MATH 8030 INTRODUCTION TO HOMOLOGICAL ALGEBRA

PETE L. CLARK

Contents

Global notation: In this course "a ring" is not necessarily commutative, but it is associative with a multiplicative identity. For a ring R, $R^\bullet$ denotes $R \setminus \{0\}$, a monoid under multiplication, and $R^\times$ denotes the group of units of R, i.e., the set of elements $x \in R$ such that there is $y \in R$ with $xy = yx = 1$. ($R^\times$ is the group of units of the monoid $R^\bullet$.)

In general my terminology follows Bourbaki. For instance compact and locally compact imply Hausdorff. The condition that every open covering has a finite subcovering is called *quasi-compact*.

1. First Steps in Homological Algebra

Exercise 1.1) Let k be a field.
a) Let

$$0 \to V' \to V \to V'' \to 0$$

be a short exact sequence of k-vector spaces (not assumed to be finite-dimensional). Show that $\dim_k V = \dim_k V' + \dim_k V''$.
b) Let

$$0 \to V_n \to V_{n-1} \to \ldots \to V_1 \to V_0 \to 0$$

be an exact sequence of finite-dimensional k-vector spaces. Show that $\sum_{i=0}^n (-1)^i \dim_k V_i = 0$.[1]
c) Let

$$0 \to A' \to A \to A'' \to 0$$

be a short exact sequence of finite $\mathbb{Z}$-modules. Show $\#A = \#A' \cdot \#A''$.
d) Let

$$0 \to A_n \to A_{n-1} \to \ldots A_1 \to A_0 \to 0$$

be an exact sequence of finite $\mathbb{Z}$-modules. Show $\prod_{i=0}^n (\#A_i)^{(-1)^i} = 1$.
e) State and prove a result which simultaneously generalizes parts b) and d).

Exercise 1.2) Let us say that a chain complex $M_\bullet$ of left R-modules is **finitely generated** if $\bigoplus_{n\in\mathbb{Z}} M_n$ is a finitely generated R-module. Show that this holds iff each M_n is a finitely generated R-module and $M_n = 0$ for all but finitely many n.

Exercise 1.3) Let $M_\bullet$ be a finite-dimensional complex of k-vector spaces. Define its **Euler characteristic**

$$\chi(M) = \sum_n (-1)^n \dim_k M_n.$$

Show that

$$\chi(M) = \sum_n (-1)^n \dim_k H_n(M_\bullet).$$

We say that the Euler characteristic is a *homological invariant* of $M_\bullet$.

Exercise 1.4) Let R be an integral domain (that is, a commutative ring without nonzero divisors of zero) with fraction field K. For a finitely generated complex $M_\bullet$ of R-modules, we define the Euler characteristic $\chi(M_\bullet)$ as $\chi(M_\bullet \otimes_R K)$. Show that

$$\chi(M) = \sum_n (-1)^n \dim_K H_n(M_\bullet) \otimes_R K.$$

Remark: If necessary, feel free to use that K is a flat R-module.

Exercise 1.5) Let k be a field, V a fixed K-vector space, and consider the following functor from the category of k-vector spaces to itself: $FM = M \otimes_k V$. a) Show that F is an **exact functor**: that is, if

$$0 \to M_1 \to M_2 \to M_3 \to 0$$

[1] We need to assume finite-dimensionality even for the statement to make sense: subtraction is not a well-defined operation on infinite cardinals. However, if we rewrote the alternating sum as "the sum of the dimensions of the even-indexed vector spaces equals the sum of the dimensoins of the odd-indexed vector spaces, then this is true without the hypothesis of finite dimensionality.

is a short exact sequence of k-vector spaces, then so is

$$0 \to F(M_1) \to F(M_2) \to F(M_3) \to 0.$$

b) Show that if $M_\bullet$ is a complex of K-vector spaces, for all $n \in \mathbb{Z}$ there is an isomorphism

$$H_n(FM_\bullet) \cong FH_n(M_\bullet).$$

Exercise 1.6) Let

$$0 \to M_1 \to M_2 \to M_3 \to 0$$

be a short exact sequence of $\mathbb{Z}$-modules. We tensor the sequence with $\mathbb{Z}/2013\mathbb{Z}$.
a) Show that

$$M_1 \otimes \mathbb{Z}/2013\mathbb{Z} \to M_2 \otimes \mathbb{Z}/2013\mathbb{Z} \to M_3 \otimes \mathbb{Z}/2013\mathbb{Z} \to 0$$

is exact.
b) Show by example that $M_1 \otimes \mathbb{Z}/2013\mathbb{Z} \to M_2 \otimes \mathbb{Z}/2013\mathbb{Z}$ need not be injective.

Exercise 1.7) Let X be the Cantor set (X is characterized up to homeomorphism by being compact, second countable, totally disconnected and without isolated points).
a) Show that there is no CW-complex with underlying topological space X.
b) Show that X is not even homotopy equivalent to the underlying topological space of a CW-complex.

Remark: Spaces homeomorphic to the Cantor set arise frequently in number theory: e.g. the ring $\mathbb{Z}_p$ of p-adic integers. (However, admittedly such spaces are not interesting from the perspective of topological homology.)

Exercise 1.8) Let F be an exact functor from the category of R-modules to the category of S-modules. Let $M_\bullet$ be a chain complex of R-modules. Show: for all $n \in \mathbb{Z}$,

$$H_n(FM_\bullet) \cong FH_nM_\bullet.$$

2. R-Modules

2.1. **Some Constructions.**

In this section we discuss various basic module-theoretic constructions. Most of them are special cases of vastly more general category-theoretic constructions, and this more general perspective will be taken later: for now, we stay concrete.

There is a common theme running through all of these constructions: namely, they all satisfy **universal mapping properties**. In general, universal mapping properties make for good definitions because the uniqueness of the associated object is assured, and they are often (though not always) useful for giving clean proofs of various properties satisfied by these objects. One still has the task of proving existence of the objects in question, which in all these cases can be done relatively straightforwardly.

For our first two examples the constructions are so simple and familiar that they are given first, followed by the universal mapping properties that they satisfy. Thereafter the approach is inverted: we give the universal mapping property, followed by the (messier) explicit construction.

2.1.1. *Direct Products.*

Let $\{M_i\}_{i\in I}$ be an indexed family of modules (here I denotes an arbitrary set). We define an R-module, the **direct product** $\prod_{i\in I} M_i$, as follows: as a set, it is the usual Cartesian product,[2] i.e., the collection of all families of elements $\{x_i \mid x_i \in I\}$. We endow it with the structure of an R-module by

$$\{x_i\} + \{y_i\} = \{x_i + y_i\},$$
$$r\{x_i\} = \{rx_i\}.$$

For each $i \in I$ there is a **projection map** $\pi_i : \prod_i M_i \to M_i$, $\{x_i\} \mapsto x_i$.

Proposition 2.1. *(Universal Property of the Direct Product) Let $\{M_i\}_{i\in I}$ be a family of R-modules, let A be an R-module, and suppose that for each $i \in I$ we are given an R-module map $\varphi_i : A \to M_i$. Then there is a unique R-module map $\Phi : A \to \prod_{i\in I} M_i$ such that for all $i \in I$, $\varphi_i = \pi_i \circ \Phi$: namely*

$$\Phi : a \in A \mapsto \{\varphi_i(a)\}.$$

Exercise: Prove it.

2.1.2. *Direct Sums.*

For a family $\{M_i\}_{i\in I}$ of R-modules, we define an R-module, the **direct sum** $\bigoplus_{i\in I} M_i$ as follows: it is the R-submodule spanned by the elements e_i, which is 1 in the ith coordinate and otherwise 0. In other words, $\bigoplus_{i\in I} M_i$ consists of all elements in the direct product which are 0 except in finitely many coordinates. For each $i \in I$, there is an injection $\iota_i : M_i \to \bigoplus_{i\in I} M_i$ given by mapping x_i to the element which has i coordinate x_i and all other coordinates 0.

Proposition 2.2. *(Universal Property of the Direct Sum) Let $\{M_i\}_{i\in I}$ be a family of R-modules, let B be an R-module, and suppose that for each $i \in I$ we are given an R-module map $\varphi_i : M_i \to B$. Then there is a unique R-module map $\Phi : \bigoplus_{i\in I} \to B$ such that or all $i \in I$, $\varphi_i = \Phi \circ \iota_i$: namely*

$$\Phi : \{x_i\} \mapsto \sum_{i\in I} \varphi_i(x_i).$$

Exercise: Prove it.

Notice that when the index set I is finite, $\bigoplus_{i\in I} M_i = \prod_{i\in I} M_i$, which is very nice: we may make use of both universal properties. However, when the index set is infinite the direct sum and direct product are quite different objects, each important in its own right and (in a sense that we will make precise later on in the language of additive categories) mutually dual. Thus for instance the abelian group $\bigoplus_{i\geq 1} \mathbb{Z}$ is very different from the abelian group $\prod_{i\geq 1} \mathbb{Z}$: the former group is countably infinite, whereas the latter is uncountably infinite. Moreover the former is (by definition: coming up soon!) a free abelian group, whereas the latter turns out not to be (a rather difficult exercise).

Exercise: We will show that $\bigoplus$ is an exact functor. Let I be a set.
a) Suppose given for all $i \in I$ an R-module map $\varphi_i : M_i \to N_i$. Show that there is

[2] Unless I is the empty set, in which case we define the direct product to be the zero module.

a naturally defined R-module map $\bigoplus_i \varphi_i : \bigoplus_i M_i \to \bigoplus_i N_i$.
b) Suppose given for each $i \in I$ a short exact sequence

$$0 \to A_i \to B_i \to C_i \to 0$$

of R-modules. Show that

$$0 \to \bigoplus_i A_i \to \bigoplus_i B_i \to \bigoplus_i C_i \to 0$$

is exact.

2.1.3. *Direct Limits.*

A **directed set** is a partially ordered set $(I, \leq)$ with the additional property that for all $i, j \in I$, there is $k \in I$ with $i \leq k$ and $j \leq k$.

Exercise: a) Show that any totally ordered set is directed.
b) Show that a totally disordered set with more than one element is not directed.
c) Show that any partially ordered set I with a top element – i.e., an element T with $x \leq T$ for all $x \in I$ – is directed. Thus for instance any power set 2^S is directed under inclusion.
d) Let G be a group. Show that the set of all subgroups of G is directed under inclusion, as is the set of all finitely generated subgroups.
e) Let M be an R-module. Show that the set of all submodules of M is directed under inclusion, as is the set of all finitely generated submodules of M.

A **direct system** of R-modules is a family of R-modules $\{M_i\}_{i \in I}$ indexed by a directed set I together with, for all pairs $i, j \in I$ with $i \leq j$, **transition maps**: R-module maps $\alpha_{i,j} : M_i \to M_j$ satisfying the following two properties:
(TM1) For all $i \in I$, $\alpha_{i,i} = 1_{M_i}$.
(TM2) For all $i \leq j \leq k$, $\alpha_{i,k} = \alpha_{j,k} \circ \alpha_{i,j}$.

Example: When $I = \mathbb{Z}^+$ with the usual ordering, to give a directed system of R-modules it is sufficient to give a sequence $\{M_i\}_{i=1}^{\infty}$ of R-modules together with maps $\alpha_i : M_i \to M_{i+1}$ for all $i \geq 1$.

Let $\{M_i\}_{i \in I}$ be a directed system of R-modules. The **direct limit** $M = \varinjlim M_i$ is an R-module together with maps $\alpha_i : M_i \to M$, satisfying the following universal mapping property: for any R-module B and R-module maps $\varphi_i : M_i \to B$ for all i in I satisfying: $\varphi_i = \varphi_j \circ \alpha_{i,j}$ for all $i \leq j$, there is a unique R-module map $\Phi : M \to B$ such that $\Phi \circ \alpha_i = \varphi_i$ for all i.

Notice that the universal mapping property of the direct limit is reminiscent of the universal mapping property of the direct sum, but more complicated because of the presence of the transition maps. This gives a clue to the construction of $\varinjlim M_i$. Namely, we start with the direct sum $\bigoplus_{i \in I}$ and mod out by the submodule generated by $\iota_i(x_i) - \iota_j(x_j)$, where $i, j \in I$, $x_i \in M_i$, $x_j \in M_j$ and there is $k \in I$ with $i \leq k$, $j \leq k$ such that $\alpha_{ik}(x_i) = \alpha_{jk}(x_j)$.

In other words, $\varinjlim M_i$ is the module generated by all the M_i's and subject to the relations that two elements which become equal under a pair of transition maps.

Exercise: Check that the above construction satisfies the universal mapping property of the direct limit. Be explicit about where the fact that I is directed is used.

Exercise: Let I be a directed set with a top element T. Show that for any I-indexed directed system $\{M_i\}_{i \in I}$, we have $\varinjlim M_i = M_T$.

Exercise: Let M be an R-module. a) Show that family of all submodules of M naturally forms a directed system, and show that the direct limit is M.
b) Actually, in view of the previous exercise, part a) is a triviality. Redo it with the family of all finitely generated submodules of M.

Exercise: Suppose we have a directed system $\{M_i\}_{i \in I}$ in which all the transition maps α_{ij} are injective. Show that $\varinjlim M_i = \bigcup_{i \in I} \alpha_i(M_i)$. (Thus in this case the direct limit can be viewed as a kind of "internally constructed union".)

Exercise: Show that $\varinjlim$ is an exact functor.

2.1.4. *Inverse Limits.*

2.1.5. *Localization.*

Let R be a commutative ring. A subset $S \subset R$ is **multiplicative** if $SS \subset S$, $1 \in S$ and $0 \notin S$.

We wish to construct a **localized ring** $S^{-1}R$ together with a ring homomorphism $\iota : R \to S^{-1}R$. The key property of $S^{-1}R$ is that for all $s \in S$, $\iota(s)$ is a unit in $S^{-1}R$, and that $S^{-1}R$ is universal for this property. More precisely, the defining uniersal mapping property of $(S^{-1}R, \iota : S^{-1}R)$ is that for any ring T and ring homomorphism $\iota_T : R \to T$ such that $\iota_T(S) \subset T^{\times}$, there is a unique ring homomorphism $\varphi : S^{-1}R \to T$ such that $\iota_T = \varphi \circ \iota$.

Exercise: Let R be an integral domain and K be its fraction field. Let $S = R^{\bullet}$. Show that K together with the natural inclusion $\iota : R \hookrightarrow K$ satisfies the universal mapping property defining $S^{-1}R$.

The construction of the fraction field K of a domain R is an entirely straightforward generalization of the construction of $\mathbb{Q}$ from $\mathbb{Z}$ via ordered pairs modulo an equivalence relation. In fact, for a domain the general case follows from this.

Exercise: Let R be a domain and let $S \subset R$ be multiplicative. Show that the subring $R[S^{-1}]$ of K – i.e., we adjoin to R the elements $\frac{1}{s}$ for $s \in S$ – satisfies the universal mapping property of $S^{-1}R$.

It is important to be able to perform the localization process for any multiplicative subset of any commutative ring R. (For instance, it is basic to modern algebraic geomety: localization allows us to glue together affine schemes to form more general schemes.) Happily, the general construction also follows the school-child construction of $\mathbb{Q}$ from $\mathbb{Z}$...with just one additional twist.

Here is the explicit construction of $S^{-1}R$: its elements are formal quotients $\frac{x}{s}$ with $x \in R$, $s \in S$ – so really, ordered pairs $(x, s) \in R \times S$ – subject to the following equivalence relation: $\frac{x}{s} \sim \frac{x'}{s'}$ if there is $t \in S$ with $t(s'x - sx') = 0$.

Exercise: a) Check that $\sim$ is indeed an equivalence relation on the set $R \times S$.
b) Suppose that we considered the more obvious relation of $\frac{x}{s} \sim \frac{x'}{s'}$ iff $s'x = sx'$. Give an example of a ring R and a multiplicative subset S for which this *is not* an equivalence relation.

Exercise: a) Show that the usual rules of addition and multiplication of fractions are well-defined on $S^{-1}R$ and endow it with the structure of a commutative ring.
b) Show that there is a ring homomorphism $\iota : R \to S^{-1}R$ given by $x \mapsto \frac{x}{1}$.
c) Show that $\ker \iota$ is the set of $x \in R$ such that $\operatorname{ann} x \cap S \neq \varnothing$. Deduce that if R is a domain, ι is injective.

Exercise: Check that the ring $S^{-1}R$ does indeed satisfy the aforementioned universal mapping property.

One can also perform the localization process on R-modules. Namely, for an R-module M, $S^{-1}M$ is an $S^{-1}R$-module, and we have an R-module map $\iota : M \to S^{-1}M$. Here is the universal mapping property: let N be any R-module such that multiplication by s is an isomorphism on N for all $s \in S$, and let $\iota_N : M \to N$ be an R-module map. Then there is a unique R-module map $\varphi : S^{-1}M \to N$ such that $\iota_N = \varphi \circ \iota$.

Exercise: a) Show that one can construct an R-module $S^{-1}M$ by taking the quotient of $M \times S$ under the equivalence relation $\frac{x}{s} \sim \frac{x'}{s'}$ if there is $t \in S$ with with $t(s'x - sx') = 0$.
b) Show that $\iota : M \to S^{-1}M$ given by $x \mapsto \frac{x}{1}$ is an R-module map, with kernel the set of $x \in M$ such that $\operatorname{ann} x \cap S \neq \varnothing$.
c) Show that $\iota : M \to S^{-1}M$ satisfies the above universal mapping property.

For more information localization in commutative rings, see [CA, § 7].

There is a theory of localization in non-commutative rings due to Oystein Ore, but this is significantly more involved and will not be treated (or needed) in this course. The following exercise does something much more modest.

Exercise: Let R be any ring, and let S be a central multiplicative subset, i.e., $S \subset Z(R)$. Show that the constructions of this section go through without change in this setting, i.e., we can still define $S^{-1}R$ and $S^{-1}M$.

2.1.6. *Pullbacks.*

A **pullback** of $f : X \to Z$, $g : Y \to Z$ is a module P and morphisms $\pi_1 : P \to X$, $\pi_2 : P \to Y$ satisfying the following universal mapping property: given $\pi_1' : P' \to X$

and $\pi_2' : P' \to Y$ with $f\pi_1' = g\pi_2'$, there is a unique morphism $\pi : P' \to P$ such that $\pi_1\pi = \pi_1'$, $\pi_2\pi = \pi_2'$.

Exercise: With notation above, let $P = \{(x,y) \in X \times Y$ such that $f(x) = g(y)$. Let π_1 and π_2 be the two coordinate projection maps. Show that this constructs the pullback.

2.1.7. *Pushouts.*

Let $f : Z \to X$ and $g : Z \to Y$ be module maps. A **pushout** of f and g is a module P and morphisms $\iota_1 : X \to P$, $\iota_2 : Y \to P$ satisfying the following universal mapping property: for any module Q and morphims: $j_1 : X \to Q$, $j_2 : Y \to Q$ such that $j_1 f = j_2 g$, there is a unique map $\iota : P \to Q$ such that $\iota\iota_1 = j_1$ and $\iota\iota_2 = j_2$.

Exercise: With notation above, let $T = \{(f(z), -g(z)) \mid z \in Z\} \subset X \oplus Y$, and let $P = X \oplus Y/T$. Let $\iota_1 : X \to P$ be $X \hookrightarrow X \oplus Y \to (X \oplus Y)/T$ and $\iota_2 : Y \to P$ be $Y \hookrightarrow X \oplus Y \to (X \oplus Y)/T$. Show that this constructs the pushout.

2.2. **Tensor and Hom.**

Exercise 2.1) Let M be a right R-module, and consider the functor F from left R-modules to abelian groups: $F(N) = M \otimes_R N$.
a) Show that F is an additive covariant functor.
b) Show that F is **right exact**: for any exact sequence

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

of left R-modules, the induced sequence

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

is exact.

Comment: Exercise 1.6) shows that when $R = \mathbb{Z}$ and $M = \mathbb{Z}/2013\mathbb{Z}$, the functor F is not exact. As we will see shortly, it is interesting and important to isolate the class of R-modules M for which tensoring with M *is* exact.

Exercise 2.2) Let M and N be left R-modules. We denote by $\mathrm{Hom}_R(M,N)$ the set of all R-module homomorphisms $\varphi : M \to N$.
a) Show that $\mathrm{Hom}_R(M,N)$ has the natural structure of a commutative group.
b) Suppose R is commutative. Show that $(r,\varphi) : m \mapsto f(rm)$ gives $\mathrm{Hom}_R(M,N)$ the structure of an R-module. What goes wrong here if R is not commutative?

Exercise 2.3) Let M be a left R-module, and consider the **covariant Hom** functor from the category of left R-modules to the category of abelian groups (or to R-modules if R is commutative): $F : N \mapsto \mathrm{Hom}_R(M,N)$.
a) Show that F is an additive covariant functor.
b) Show that F is **left exact**: for any exact sequence

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

the induced sequence

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

is exact.
c) Show that when $R = \mathbb{Z}$ and $M = \mathbb{Z}/n\mathbb{Z}$ for $n > 1$, the functor F is not exact. As we shall see shortly...

Exercise 2.4) Let N be a left R-module, and consider the **contravariant Hom** functor from the category of left R-modules to the category of abelian groups (or to R-modules if R is commutative): $F : M \mapsto \operatorname{Hom}_R(M, N)$.
a) Show that F is an additive contravariant functor.
b) Show that if

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

is exact, then

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

is exact. The standard name for a contravariant functor with this property is **left exact**, but one could also justify the name “right exact”. We will try out a new – less confusing, we hope – name: **epimonic**.
c) Show that when $R = N = \mathbb{Z}$ the functor F is not exact. As we shall see shortly...

Exercise 2.5) We work with left R-modules. Find canonical isomorphisms:
a) $\operatorname{Hom}_R(A, \prod_{i\in I} B_i) \cong \prod_{i\in I} \operatorname{Hom}_R(A, B_i)$.
b) $\operatorname{Hom}_R(\bigoplus_{i\in I} A_i, B) \cong \prod_{i\in I} \operatorname{Hom}_R(A_i, B)$.

Exercise: Let $R \to T$ be a ring homomorphism.
a) (**Associating Tensor Identity**) Let $M \in \operatorname{Mod}_T$, $N \in_T \operatorname{Mod}_R$ and $P \in_R \operatorname{Mod}$. Find a canonical isomorphism

$$M \otimes_T (N \otimes_R P) \cong (M \otimes_T N) \otimes_R P.$$

b) (**Telescoping Tensor Identity**) Deduce

$$M \otimes_T (T \otimes_R P) \cong M \otimes_R P.$$

Exercise: Let $R \to T$ be a ring homomorphism. Let $A \in_T \operatorname{Mod}$ and $B \in_R \operatorname{Mod}$. Find a canonical isomorphism, the **Telescoping Hom Identity:**

$$\operatorname{Hom}_T(A, \operatorname{Hom}_R(T, B)) \cong \operatorname{Hom}_R(A, B).$$

Exercise 2.6) (**Tensor-Hom Adjunction**) Let R and T be rings, let $X \in_R \operatorname{Mod}_T$, $Y \in \operatorname{Mod}_R$ and $Z \in_T \operatorname{Mod}$. Find a canonical isomorphism

$$\operatorname{Hom}_S(Y \otimes_R X, Z) \cong \operatorname{Hom}_R(Y, \operatorname{Hom}_S(X, Z)).$$

In other words, tensor and hom are adjoint functors.

Exercise: a) Let R be a commutative ring, $S \subset R$ a multiplicative subset, and M and R-module. Show that $M \otimes_R S^{-1}R \cong S^{-1}M$. (Suggestion: show that $M \otimes_R S^{-1}M$ also satisfies the appropriate universal mapping property.)
b) Let R be a domain with fraction field K, and let M be an R-module. Show that the kernel of $M \to M \otimes_R K$ is $M[\text{tors}]$, i.e., the set of elements $x \in M$ such that $rx = 0$ for some $r \in R^{\bullet}$.

2.3. **Splitting.**

Exercise 2.8) Let $0 \to A \xrightarrow{\iota} B \xrightarrow{p} C \to 0$ be a short exact sequence of left R-modules. We say that the sequence is **split** if there exists an R-module map $\sigma : C \to B$ such that $p \circ \sigma = 1_C$: such a σ is called a **section** of p.
a) Show that for all $a, b \in \mathbb{Z}^+$ there is a short exact sequence of $\mathbb{Z}$-modules

$$0 \to \mathbb{Z}/a\mathbb{Z} \to \mathbb{Z}/ab\mathbb{Z} \to \mathbb{Z}/b\mathbb{Z} \to 0.$$

For which values of a and b is this sequence split?
b) Show: a section σ gives a canonical isomorphism $B \cong A \oplus C$.
c) Show that the short exact sequence is split iff there is an R-module map $r : B \to A$ such that $\iota \circ r = 1_B$: such an r is called a **retraction** of ι.
d)* Suppose there is some isomorphism $B \cong A \oplus C$. Must the sequence be split? (Suggestion: see [Rot, p. 54].)

Exercise 2.9) Let R be a ring.
a) Suppose $R = \prod_{i=1}^n K_i$ is a finite product of fields. Show that every short exact sequence of R-modules splits.
b)* Suppose R is a commutative ring such that every short exact sequence of R-modules splits. Show: R is isomorphic to a finite product of fields.
c) Give necessary and sufficient conditions on a not necessarily commutative ring for every short exact sequence of left R-modules to split. (Hint: Wedderburn-Artin.)

2.4. **Free Modules.**

Proposition 2.3. *For a left R-module M, the following are equivalent:*
(i) $M \cong \bigoplus_{i \in I} R$ for some index set I.
(ii) There is a subset I of M with the following property: for any R-module N and any function $x : I \to N$, there is a unique R-module map $\Phi : M \to N$ with $\varphi(i) = x(i)$ for all $i \in I$.
A module satisfying these equivalent conditions is called a ***free module****, and a subset E satisfying the conditions of (ii) is called a* ***basis****.*

Proof. (i) $\implies$ (ii): Put $M = \bigoplus_{i \in I} R$. Let $e_i \in M$ be the element which is 1 in the ith coordinate and otherwise 0. For $i \in I$, let $\varphi_i : R \to N$ be the unique R-module homomorphism with $\varphi_i(1) = x(i)$. By the universal property of the direct sum there is a unique homomorphism $\Phi : M \to N$ with $\varphi_i = \Phi \circ \iota_i$ for all $i \in I$.

(ii) $\implies$ (i): Put $F = \bigoplus_{i \in I} R$, and once again let e_i in F be the element which is 1 in the ith coordinate and otherwise 0. By hypothesis, there is a unique R-homomorphism $\Phi : M \to F$ with $\Phi(i) = e_i$ for all i. By (i) $\implies$ (ii), there is a unique R-homomorphism $\Psi : F \to M$ with $\Psi(e_i) = i$ for all i. It follows easily from the assumed property of M and the universal property of the direct sum that $\Psi \circ \Phi = 1_M$ and $\Psi \circ \Phi = 1_F$, so Φ and Ψ are mutually inverse isomorphisms. $\square$

Exercise: a) Let R be a commutative ring, and let M be an R-module. Show that any two bases of R have the same cardinality. (Hint: let $\mathfrak{m}$ be a maximal ideal of R. Tensor from R to the field $R/\mathfrak{m}$ to reduce this to a known fact in linear algebra.
b)$*$ Find a noncommutative ring such that $R \cong R^2$ as left R-modules.

A ring R is said to have the **invariant basis number** property (or IBN) if any two bases of an R-module have the same cardinality. As the above exercise shows, every commutative ring satisfies IBN but there are non-commutative rings which do not. For more information on IBN see [NCA] and [Lam99]. In particular one finds in these sources that a left Noetherian ring satisfies IBN.

If R is an IBN ring and F is a free R-module, we define the **rank** of F to be the cardinality (well-determined by the IBN condition) of any basis of R. On the other hand, if R is a domain with fraction field K, then for any R-module M, we define the rank of M as $\dim_K M \otimes_R K$.

Exercise: Show that this terminology is consistent: i.e., for free R-modules over a domain, the two notions of rank coincide.

Exercise: Show that an R-module M is finitely generated iff there is a surjection $R^n \to M$ for some $n \in \mathbb{Z}^+$.

Exercise: a) Let I be an infinite set, and let $\{M_i\}_{i\in I}$ be a family of nonzero left R-modules. Show that $\bigoplus_{i\in I} M_i$ is *not* finitely generated.
b) Deduce that it is not possible for an R-module to have both a finite basis and an infinite basis.

Exercise 2.7) For a ring R, show the following are equivalent:
(i) Every left R-module is free.
(ii) R is a division ring.

Direct sums of free modules are free almost by definition. What about direct products? The following classic example answers this question in the negative.

Theorem 2.4 (Baer [Bae37])**.** *The group $\mathcal{B} = \prod_{n=1}^{\infty} \mathbb{Z}$ is* not *free abelian.*

Proof. We follow [Sch08]. Suppose $\mathcal{B}$ is free, and let $\{b_i\}_{i\in I}$ be a basis for $\mathcal{B}$. Since $\#\mathcal{B} = \mathfrak{c} = 2^{\aleph_0}$, we must also have $\#I = \mathfrak{c}$. For $n \in \mathbb{Z}^+$, let e_n be the element which is 1 in the nth coordinate and 0 otherwise, so that e_n is a basis not for $\mathcal{B}$ but for its subgroup $\mathfrak{b} = \bigoplus_{n=1}^{\infty} \mathbb{Z}$. For each n, write

$$e_n = \sum_{i\in I} \lambda_{n,i} b_i,$$

and let

$$J = \{i \in I \mid \lambda_{n,i} \neq 0 \text{ for some } n\}.$$

The set J is countable, and thus so is $A = \langle b_i \mid i \in J\rangle$. We have

$$\mathfrak{b} \subset A \subset \mathcal{B}.$$

Further, the images of the elements b_i for $i \in I \setminus J$ form a basis for $\mathcal{B}/A$.

Consider elements $y = \{x_n\} \in \mathcal{B}$ with $x_1 = 1$ and for all $n \geq 1$, $x_{n+1} = 2^{a_n} x^n$ for some $a_n \geq 1$. The set of all such y is in bijection with $\mathcal{B}$ so has cardinality $\mathfrak{c}$; thus there is such a $y = (x_1, x_2, \ldots) \in \mathcal{B} \setminus A$. Since $A \supset \mathfrak{b}$, for all $k \in \mathbb{Z}^+$, $y \equiv (0, \ldots, 0, x_{k+1}, x_{k+2}, \ldots) \pmod{A}$. So in the free abelian group $\mathcal{B}/A$, $0 \neq \overline{y}$ is divisible by 2^k for all positive integers k, and this is a clear contradiction. $\square$

Exercise (Goodwillie): Let R be a Noetherian domain which is not a field. Show that $\bigoplus_{i=1}^{\infty} R$ is not a free R-module. (Comment: if R is countably infinite, then the above proof goes through with 2 replaced by any element π of R which is nonzero and not a unit.)

Remark: On the other hand, Specker showed that every countable subgroup of B is free abelian [Sp50]. These two results have focused a lot of interest on the group $\mathcal{B}$, which is often called the **Baer-Specker group**.

Exercise: Let R be a domain with fraction field K. If $R \neq K$, show that K is *not* a free R-module.

Theorem 2.5. *Let R be a PID.*
a) Let M be a finitely generated module. Then M is free iff it is torsionfree.
b) If F is a free R-module and $M \subset_R F$, then F is free, and $\operatorname{rank} M \leq \operatorname{rank} F$.

Proof. Part a) is an immediate consequence of the structure theory for modules over a PID, with which we assume familiarity. Note that part b) follows immediately when F is finitely generated. The general case is a bit harder. For one proof – which is however embedded in a more general discussion which is unnecessarily intricate if one is only interested in this particular result – see [CA, Thm. 3.57]. $\square$

Exercise: a) Let R be a Notherian domain in which every finitely generated torsionfree module is free. Show that R is a PID.
b) Let R be a commutative ring in which every submodule of a free module is free. Show that R is a PID.

Proposition 2.6. *For a domain R, the following are equivalent:*
(i) Every finitely generated ideal of R is principal.
(ii) Every finitely generated torsionfree R-module is free.
A domain satisfying these equivalent conditions is called a ***Bézout domain****.*

Proof. See [CA, Thm. 3.62]. $\square$

Let R be a domain. An element $v \in R^n$ is **primitive** – or a **primitive vector** – if it is *not* of the from αw for any $\alpha \in R \setminus R^{\times}$.

Exercise: Show: $v \in (R^n)^{\bullet}$ is primitive iff $R^n/\langle v \rangle$ is torsionfree.

he following result is useful – especially in the case $R = \mathbb{Z}$ – in classical algebraic number theory and in "geometry of numbers".

Theorem 2.7. *(Hermite's Lemma) Let R be a Bézout domain, and let $e_i = (0, \ldots, 1, \ldots 0) \in R^n$ be the ith standard basis vector. For $v \in R^n$, TFAE:*
(i) There is $M \in \mathrm{GL}_n(R)$ with $M(e_1) = v$, i.e., the first column of M is v.
(ii) There is a basis for R^n containing v.
(iii) v is a primitive vector.

Proof. (i) $\implies$ (ii): If $M(e_1) = v$, then $\{M(e_i)\}_{i=1}^n\}$ is a basis for M containing v.
(ii) If $v, v_2, \ldots, v_n$ is a basis, the matrix with columns $v, v_2, \ldots, v_n$ lies in $\mathrm{GL}_n(R)$.
$\neg$ (iii) $\implies$ $\neg$ (i): Let $v = \alpha w$ for $\alpha \in R \setminus R^{\times}$, and let $M \in M_n(R)$ be a matrix with $M(e_1) = v$. Let M' be the matrix obtained from M by replacing the first column with w. Then $\det M = \alpha(\det M')$, so $\det M \notin R^{\times}$.
(iii) $\implies$ (i): Put $F = R^n/\langle v \rangle$ and consider the exact sequence

$$0 \to \langle v \rangle \to R^n \xrightarrow{q} M \to 0.$$

By Exercise X.X, M is torsionfree. It is also finitely generated, so by Theorem X.X M is free. Tensoring to the fraction field shows $\operatorname{rank} M = n-1$; let $w_2, \ldots, w_n$ be a basis. For $2 \leq i \leq n$, choose $v_i \in R^n$ mapping to w_i in M. By the universal property of free modules there is an R-module map from $\iota : M \to R^n$ mapping w_i to v_i for all i, and since $q \circ \iota = 1_M$, ι is an isomorphism onto its image. It follows that $v, v_2, \ldots, v_n$ is R-linearly independent and spans R^n. $\square$

2.5. **Projective Modules.**

A left R-module P is **projective** if every short exact sequence

$$0 \to M \to N \to P \to 0$$

splits.
A left R-module E is **injective** if every short exact sequence

$$0 \to E \to M \to N \to 0$$

splits.

Exercise 2.10) Let P be a left R-module.
a) Show that P is projective iff: whenever we have an R-module surjection $f : M \to N$ and an R-module map $a : P \to N$, there is a **lift** $A : P \to N$, i.e., an R-module map such that $f \circ A = a$.
b) Show that P is projective iff: there is a left R-module Q such that $P \oplus Q$ is a free R-module.
c) Show that P is projective iff the functor $M \mapsto \operatorname{Hom}_R(P, M)$ is exact.

Exercise 2.11) Show that free R-modules are projective.

Remark: In general it is much easier to check whether an R-module is projective than whether it is free. For instance, in 1955 Serre asked whether every finitely generated projective module over a polynomial ring $k[t_1, \ldots, t_n]$ (where k is any field) is free. This was proven in 1976 by D. Quillen and A.A. Suslin (independently). It is not a coincidence that Quillen won the Fields Medal in 1978!

Exercise 2.12) Show that every left R-module is a quotient of a projective module. (This result is described as "The category of R-modules has enough projectives." Soon enough we will understand the significance of this: it implies that every module admits a **projective resolution**.)

Exercise 2.13) Let $\{M_i\}_{i \in I}$ be a family of R-modules, and put $M = \bigoplus_{i \in I} M_i$.
a) Show: M is projective iff each M_i is projective.
b) Show that M free *does not imply* that each M_i is free.
(Suggestion: this is in fact equivalent to the existence of nonfree projective modules. As alluded to above, this is often a delicate issue. For a cheap example, try a ring like $\mathbb{C} \times \mathbb{C}$.)

Exercise: Let R be a commutative ring, and let M, N be R-modules. Show that if M and N are projective, so is $M \otimes_R N$.

Let R be an integral domain. Recall(?) that an ideal I of R is **invertible** if there exists an ideal J and $a \in R^\bullet$ such that $IJ = aR$. (Here IJ is the set of all finite sums of elements ij for $i \in I$ and $j \in J$.) It is a fact that a nonzero ideal is invertible iff it is, as an R-module, projective. An integral domain in which every nonzero finitely generated ideal is invertible is called a **Prüfer domain**. In Noetherian rings all ideals are finitely generated, so a Noetherian Prüfer domain is precisely a **Dedekind domain**.

Exercise 2.17) For a Dedekind domain R, show that the following are equivalent:
(i) Every projective R-module is free.
(ii) The ideal class group of R is trivial.
(iii) R is a PID.

In algebraic geometry, a finitely generated projective R-module P is viewed as a vector bundle over the affine scheme $\operatorname{Spec} R$. This perspective is due to Serre. Well, maybe the above means little or nothing to you, but there is an easier analogue in topology that I at least find particularly beautiful and motivational. Let X be a topological space. For a real vector bundle $\eta : E \to X$ we attach the set $\Gamma(X, E)$ of **global sections**, namely the set of all continuous maps $\sigma : X \to E$ such that $\eta \circ \sigma = 1_X$. Because each fiber $\eta^{-1}(x)$ of η has the structure of an $\mathbb{R}$-vector space, it makes sense to add two global sections and to scale any global section by any real number. This endows $\Gamma(X, E)$ with the structure of an $\mathbb{R}$-vector space. But actually it has much more structure than that: if $f : X \to \mathbb{R}$ is any continuous function and $\sigma : X \to E$ is any global section, then fx is again a global section. Now the continuous functions from X to $\mathbb{R}$ form a commutative ring $C(X, \mathbb{R})$ under pointwise addition and multiplication, and by what we have just said, $\Gamma(X)$ has the natural structure of a $C(X, \mathbb{R})$-module.

Theorem 2.8. *(Serre-Swan) Let X be a compact space. The functor $E \to X \mapsto \Gamma(X, E)$ gives a categorical equivalence from the category of real vector bundles on X to the category of finitely generated $C(X, \mathbb{R})$-modules.*

Proof. See [CA, § 6.3]. □

2.6. **Injective Modules.**

Proposition 2.9. *For a left module E over a ring R, TFAE:*
(ii) If $\iota : M \to N$ is an injective R-module homomorphism and $\varphi : M \to E$ is any homomorphism, there exists at least one extension of φ to a homomorphism $\Phi : N \to E$.
(iii) If $\iota : M \to N$ is an injection, the natural map $\operatorname{Hom}(N, E) \to \operatorname{Hom}(M, E)$ is surjective.
(iv) The (contravariant) functor $\operatorname{Hom}(\cdot, E)$ is exact.
(v) Any short exact sequence of R-modules

$$0 \to E \xrightarrow{\iota} M \to N \to 0$$

splits: there exists an R-module map $\pi : M \to E$ such that $\pi \circ \iota = 1_E$ and thus an internal direct sum decomposition $M = \iota(E) \oplus \ker(\pi) \cong E \oplus N$.
*A module satisfying these equivalent conditions is called **injective**.*

Exercise 3.1) Prove Proposition 2.9.

Exercise 3.2) Show that every module over a field is injective.

Exercise 3.3) Show that $\mathbb{Z}$ is *not* an injective $\mathbb{Z}$-module. (Thus injectivity is the first important property of modules that is not satisfied by free modules.)

Exercise 3.4) Let $\{M_i\}_{i \in I}$ be any family of R-modules and put $M = \prod_{i \in I} M_i$. Show that M is injective iff M_i is injective for all $i \in I$.

One naturally asks whether the same result holds for direct sums. This is vaguely dual to the issue of whether a product of projective modules must be projective. Given that the Baer-Specker group gives a negative answer to this even over such a nice ring as $\mathbb{Z}$, the following result is rather surprising.

Theorem 2.10 (Bass-Papp [Bas59] [Pa59])**.** *For a ring R, TFAE:*
a) A direct sum of injective left R-modules is injective.
b) A countable direct sum of injective left R-modules is injective.
c) R is left Noetherian.

Proof. See [CA, Thm. 8.29]. (The result is stated there for commutative rings, but the proof goes through in the general case.) □

Exercise 3.5) For a ring R, show TFAE:
(i) R is **absolutely projective**: every R-module is projective.
(ii) R is **absolutely injective**: every R-module is injective.
(iii) R is semisimple.

Theorem 2.11 (Baer Criterion [Bae40])**.** *For an R-module E, TFAE:*
(i) E is injective.
(ii) For every nonzero left ideal I of R, every R-module map $\varphi : I \to E$ extends to an R-module map $\Phi : R \to E$.

Proof. (i) $\implies$ (ii): In condition (ii) of Proposition 2.9, take $M = I$, $N = R$.
(ii) $\implies$ (i): Let M be an R-submodule of N and $\varphi : M \to E$ an R-module map. We must show: φ can be extended to N. Now the set $\mathcal{P}$ of pairs (N', φ') with $M \subset N' \subset N$ and $\varphi : N' \to E$ a map extending φ is nonempty and has an evident partial ordering, with respect to which the union of any chain of elements in $\mathcal{P}$ is again an element of $\mathcal{P}$. So by Zorn's Lemma, there is a maximal element $\varphi' : N' \to E$. Our task is to show that $N' = M$.

Assume not, and choose $x \in N \setminus N'$. Put

$$I = (N' : x) = \{r \in R \mid rx \subset N'\};$$

one checks immediately that I is an ideal of R. Consider the composite map

$$I \xrightarrow{\cdot x} N' \xrightarrow{\varphi} E;$$

by our hypothesis, this extends to a map $\psi : R \to E$. Now put $N'' = \langle N', x \rangle$ and define[3] $\varphi'' : N'' \to E$ by

$$\varphi''(x' + rx) = \varphi'(x') + \psi(r).$$

Thus φ'' is an extension of φ' to a strictly larger submodule of N than N', contradicting maximality. □

[3]Since N'' need not be the direct sum of N' and $\langle x \rangle$, one does need to check that φ'' is well-defined; we ask the reader to do so in an exercise following the proof.

Exercise 3.6) Verify that the map φ'' is well-defined.

A module M over a domain R is **divisible** if for all $r \in R^\bullet$ the endomorphism $r\bullet : M \to M, x \mapsto rx$, is surjective. Further, we define M to be **uniquely divisible** if for all $r \in R^\bullet$, the endomorphism $r\bullet : M \to M$ is a bijection. For example: the $\mathbb{Z}$-module $\mathbb{Q}$ is divisible; $\mathbb{Q}/\mathbb{Z}$ is divisible but not uniquely.

Exercise 3.7) Show: a divisible module is uniquely divisible iff it is torsionfree.

Exercise 3.8) a) Show that a quotient of a divisible module is divisible.
b) Show that direct sums and direct products of divisible modules are divisible.

Exercise 3.9) Let R be a domain with fraction field K.
a) Show that K is a uniquely divisible R-module.
b) Let M be any R-module. Show that the natural map $M \to M \otimes_R K$ is injective iff M is torsionfree.
c) Show that for any R-module M, $M \otimes_R K$ is uniquely divisible.
d) Show that K/R is divisible but not uniquely divisible.

Exercise 3.10)
a) Show that a $\mathbb{Z}$-module is uniquely divisible iff it can be endowed with the (compatible) structure of a $\mathbb{Q}$-module, and if so this $\mathbb{Q}$-module structure is unique.
b) Show that a $\mathbb{Z}$-module M is a subgroup of a uniquely divisible $\mathbb{Z}$-module iff it is torsionfree.

Proposition 2.12. *Let R be a domain and E an R-module.*
a) If E is injective, it is divisible.
b) If E is torsionfree and divisible, it is injective.
c) If R is a PID and E is divisible, it is injective.

Proof. a) Let $r \in R^\bullet$. For $x \in E$, consider the R-module homomorphism $\varphi : rR \to E$ given by $r \mapsto x$. Since E is injective, this extends to an R-module map $\varphi : R \to E$. Then $r\varphi(1) = \varphi(r \cdot 1) = \varphi(r) = x$, so $r\bullet$ is surjective on E.
b) Let I be a nonzero ideal of R and $\varphi : I \to E$ be an R-module map. For each $a \in I^\bullet$, there is a unique $e_a \in E$ such that $\varphi(a) = ae_a$. For $b \in I^\bullet$, we have

$$bae_a = b\varphi(a) = \varphi(ba) = a\varphi(b) = abe_b;$$

since E is torsionfree we conclude $e_a = e_b = e$, say. Thus we may extend φ to a map $\Phi : R \to E$ by $\Phi(r) = re$. Thus E is injective by Baer's Criterion.
c) As above it is enough to show that given a nonzero ideal I of R, every homomorphism $\varphi : I \to E$ extends to a homomorphism $R \to E$. Since R is a PID, we may write $I = xR$ for $x \in R^\bullet$. Then, as in part a), one checks that φ extends to Φ iff multiplication by x is surjective on M, which it is since M is divisible. $\square$

We quote the following result from [CA, § 20.7].

Theorem 2.13. *For an integral domain R, the following are equivalent:*
(i) Every divisible R-module is injective.
(ii) R is a Dedekind domain.

By combining Proposition 2.12 with Exercise 3.42, we see that if M is a torsionfree module over a domain R, then M is a submodule of the uniquely divisible – hence injective – module $M \otimes_R K$. Later we will show that in fact every left R-module is a submodule of an injective module: this is somewhat more involved.

Exercise 3.11) Let $n \in \mathbb{Z}^+$.
a) Show that as a $\mathbb{Z}$-module $\mathbb{Z}/n\mathbb{Z}$ is not divisible hence not injective.
b) Show that $\mathbb{Z}/n\mathbb{Z}$ is injective as a $\mathbb{Z}/n\mathbb{Z}$-module. (One says that $\mathbb{Z}/n\mathbb{Z}$ is a **self-injective ring**.)

Exercise 3.12) Let $R = \mathbb{Z}[t]$ and let K be its fraction field. Show that the R-module K/R is divisible but not injective.

Exercise 3.13) Let R be a domain with fraction field K.
a) If $R = K$, then all R-modules are both injective and projective.
b) If $R \neq K$, the only R-module which is both projective and injective is 0.

Let M be a *right* R-module and A a left $\mathbb{Z}$-module. We endow the abelian group $\mathrm{Hom}_{\mathbb{Z}}(M, A)$ with the structure of a *left* R-module by $(rf)(x) = f(xr)$.[4]

As a special case, we denote $\mathrm{Hom}_{\mathbb{Z}}(M, \mathbb{Q}/\mathbb{Z})$ by M^* and call it the **Pontrjagin dual** of M. Because $\mathbb{Q}/\mathbb{Z}$ is an injective $\mathbb{Z}$-module, the (contravariant) functor $M \mapsto M^*$ – or in other words $\mathrm{Hom}_{\mathbb{Z}}(\ , \mathbb{Q}/\mathbb{Z})$ – is exact.[5] In particular, if $f : M \to N$ is an R-module map, then f injective implies f^* surjective and f surjective implies f^* injective.

Exercise 3.14) a) Let M be a nonzero abelian group. Show that $M^* \neq 0$.
b) Show that for any left R-module M, there is a natural injection of R-modules $\Psi_M : M \to M^{**}$.

Lemma 2.14. *Every $\mathbb{Z}$-module M can be embedded into an injective $\mathbb{Z}$-module.*

Proof. Let $I \subset M$ be a generating set and let $\bigoplus_{i\in I} \mathbb{Z} \to M$ be the corresponding surjection, with kernel K, so $M \cong (\bigoplus_{i\in I} \mathbb{Z})/K$. The natural map $\bigoplus_{i\in I} \mathbb{Z} \hookrightarrow \bigoplus_{i\in I} \mathbb{Q}$ induces an injection $M \hookrightarrow (\bigoplus_{i\in I} \mathbb{Q})/K$, and the latter $\mathbb{Z}$-module is divisible, hence injective since $\mathbb{Z}$ is a PID. $\square$

Lemma 2.15. *(Injective Production Lemma) Let E be an injective $\mathbb{Z}$-module and F a flat R-module. Then $\mathrm{Hom}_{\mathbb{Z}}(F, E)$ is an injective R-module.*

Proof. We will show that the functor $\mathrm{Hom}_R(\ , \mathrm{Hom}_{\mathbb{Z}}(F, E))$ is exact. For any R-module M, the adjointness of $\otimes$ and Hom gives

$$\mathrm{Hom}_R(M, \mathrm{Hom}_{\mathbb{Z}}(F, E)) = \mathrm{Hom}_{\mathbb{Z}}(F \otimes_R M, E)$$

so we may look at the functor $M \mapsto \mathrm{Hom}_{\mathbb{Z}}(F \otimes_R M, E)$ instead. But this is the composition of the exact functor $M \mapsto F \otimes_R M$ with the exact functor $N \mapsto \mathrm{Hom}_{\mathbb{Z}}(N, E)$, so it is exact. $\square$

Theorem 2.16. *Every R-module can be embedded into an injective R-module.*

[4] Thanks to John Doyle for noting that this construction inverts the "handedness" of the module.

[5] Here we are using the (obvious) fact that a sequence of R-modules is exact iff it is exact when viewed merely as a sequence of $\mathbb{Z}$-modules.

Proof. Let M be an R-module. Viewing M as a $\mathbb{Z}$-module, by Lemma 2.14 there is an injective $\mathbb{Z}$-module E_1 and a $\mathbb{Z}$-module map $\varphi_1 : M \hookrightarrow E_1$. Further, by Lemma 2.15, $\mathrm{Hom}_{\mathbb{Z}}(R, E_1)$ is an injective R-module. Now consider the R-module map

$$\varphi : M \to \mathrm{Hom}_{\mathbb{Z}}(R, E_1), \ x \mapsto (r \mapsto \varphi_1(rx)).$$

We claim that φ is an injection. Indeed, if $\varphi(x) = 0$ then for all $r \in R$, $\varphi_1(rx) = 0$. In particular $\varphi_1(x) = 0$, so since φ_1 is a monomorphism, we conclude $x = 0$. $\square$

Theorem 2.17. *Every left R-module admits a right injective resolution: i.e., there is an exact sequence*

$$0 \to M \to E_0 \to E_1 \to \ldots \to E_n \to E_{n+1} \to \ldots$$

with each E_n injective.

Exercise 3.15) Prove Theorem 2.17.

2.7. **Flat Modules.**

A right R-module M is **flat** if for any short exact sequence of left R-modules

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

the complex of abelian groups

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

remains exact. In other words, M is flat if $M \otimes_R \cdot$ is an exact functor. Similarly we say that a left R-module is flat if $\cdot \otimes_R M$ is exact.

Around the 1950's it was observed that flatness is one of the central notions of commutative algebra, although it seems technical at first. On the homological algebra side flatness is an easier sell: as we will see, it is closely related to the universal coefficient theorems in co/homology.

Exercise: Let $\{M_i\}_{i \in I}$ be an indexed family of left R-modules. Show that $\bigoplus_{i \in I}$ is flat iff M_i is flat for all i.

Exercise 2.14) Show that projective modules are flat.
(Suggestion: Reduce to the case that free modules are flat.)

Let R be a domain. For an R-module M, we define the **torsion submodule**

$$M[\mathrm{tors}] = \{m \in M \mid \exists r \in R^{\bullet} \mid rm = 0\}.$$

In words, $M[\mathrm{tors}]$ consists of the elements of M which are killed by some nonzero element of R. We say M is **torsion** if $M = M[\mathrm{tors}]$ and **torsionfree** if $M[\mathrm{tors}] = 0$.

Exercise 2.15) Let R be a commutative ring.
a) Suppose R is an integral doomain. Show that flat modules are torsionfree.
b) Suppose R is not an integral domain, and suppose that we took the same definition of a torsionfree module as given above. Show that in fact no nonzero R-module is torsionfree (so this is not a good definition!).

To sum up, we have the following implications among classes of modules, in which the last holds for integral domains and the others hold on all rings:

free $\implies$ **projective** $\implies$ **flat** $\implies$ **torsionfree**

Exercise: a) Show that the following conditions on a domain are equivalent:
(i) Every finitely generated torsionfree R-module is free.
(ii) Every finitely generated ideal of R is principal (R is a **Bézout domain**).
b) Deduce that if R is a Noetherian domain in which every finitely generated torsionfree R-module is free, then R is a PID.

Exercise 2.16) Let R be a PID, and let M be an R-module.
a) Suppose M is finitely generated. Show: M is free iff it is torsionfree.
b)* Show that every projective R-module is free. (See e.g. [CA, Cor. 3.58].)
c)* Show that every torsionfree R-module is flat. (See e.g. [CA, Cor. 3.86].)
d) Show that the additive group $(\mathbb{Q}, +)$ is torsionfree but not free.

Proposition 2.18. *For a multiplicative subset S of a commutative ring R, $S^{-1}R$ is a flat R-module.*

Proof. Since $S^{-1}M = S^{-1}R \otimes_R M$, we must show that if

$$0 \to M' \to M \to M'' \to 0$$

is an exact sequence of R-modules, then so is

$$0 \to S^{-1}M' \to S^{-1}M \to S^{-1}M'' \to 0.$$

Tensor products are always right exact, so we need only show $S^{-1}M' \hookrightarrow S^{-1}M$. Suppose not: then there exists $m' \in M'$ and $s \in S$ such that $\frac{m'}{s} = 0 \in M$. Thus there is $g \in S$ such that $gm' = 0$, but if so, then $\frac{m'}{s} = 0$ in M'. $\square$

A ring R is **absolutely flat** if every left R-module is flat.

Theorem 2.19 (Harada)**.** *A ring is absolutely flat iff it is* ***von Neumann regular****: for all $a \in R$, there is $x \in R$ with $a = axa$.*

Proof. See [Rot, Thm. 4.9]. $\square$

Theorem 2.20. *For a commutative ring, the following are equivalent:*
(i) R is absolutely flat.
(ii) For every principal ideal I of R, $I^2 = I$.
(iii) Every finitely generated ideal of R is a direct summand.

Proof. See [CA, § 3.11]. $\square$

Exercise: A ring R is **Boolean** if for every $x \in R$, $x^2 = x$.
a) Show that a Boolean ring is commutative.
b) Show that a Boolean ring is absolutely flat.

Theorem 2.21. *For an integral domain R, the following are equivalent:*
(i) Every torsionfree R-module is flat.
(ii) Every finitely generated torsionfree R-module is projective.
(iii) R is a Prüfer domain.

Proof. See [CA, Thm. 21.9]. $\square$

Theorem 2.22. *Let $\{M_i\}_{i \in I}$ be a family of R-modules indexed by a direct set I. If each M_i is flat, then $\varinjlim M_i$ is flat.*

Proof. See [Rot, Prop. 5.34] for a proof using module-theoretic methods. Later we will give a proof of a more general result using categorical ideas. □

Theorem 2.23 (Govorov-Lazard [Gov65] [Laz64])**.** *For an R-module M, the following are equivalent:*
(i) M is flat.
(ii) M is a direct limit of free modules.

Proof. See [Laz64, Thm. 5.40]. □

3. The Calculus of Chain Complexes

3.1. Additive Functors.

A functor F from the category of left R-modules to the category of left S-modules is **additive** if for all $f, g \in \mathrm{Hom}_{RMod}(A, B)$, $F(f + g) = Ff + Fg$.

Exercise 4.1 ([Rot, Prop. 27]): If F is an additive functor, show that F takes the 0 object to the zero object and any zero homomorphism to the zero homomorphism.

Exercise 4.2 ([Rot, Cor. 2.21]) If F is an additive functor, $F(A \oplus B) \cong F(A) \oplus F(b)$.

3.2. Chain Complexes as a Category.

We claim that the chain complexes $M_\bullet$ of left (or right-) R-modules form an additive category in their own right. By a morphism of chain complexes $f : M_\bullet \to N_\bullet$ we mean the most obvious thing: namely, for all $n \in \mathbb{Z}$ we have an R-module map $f_n : M_n \to N_n$ and these maps commute with the differentials:

$$\forall n \in \mathbb{Z}, d_{n-1} \circ f_n = f_{n-1} \circ d_n.$$

Rather than expressing this symbolically as above, it is more perspicuous to draw a commutative ladder...but I'm going to be lazy about inserting commutative diagrams into this document, unfortunately for you.

Exercise 4.3) Give definitions for:
a) An injective morphism of chain complexes.
b) A surjective morphism of chain complexes.
c) The kernel of a morphism of chain complexes.
d) The image of a morphism of chain complexes.
e) The cokernel of a morphism of chain complexes.

3.3. Chain Homotopies.

In algebraic topology one has the important notion of a **homotopy** between continuous maps $f, g : X \to Y$: this is a continuous map $H : X \times [0, 1] \to Y$ such that $H(x, 0) = f(x)$, $H(x, 1) = g(x)$ for all $x \in X$, and we write $f \sim g$. It is often useful to regard homotopic maps as being equivalent. This leads for intance to the notion of a **homotopy equivalence** of topological spaces: we say that X and Y are homotopy equivalent if there are maps $f : X \to Y$ and $g : Y \to X$ such that

$g \circ f \sim 1_X$, $f \circ g \sim 1_Y$. Most of the standard invariants in algebraic topology do not distinguish between homotopy equivalent spaces.[6] In particular, a homotopy equivalence between spaces induces an isomorphism on the singular co/homology groups.

In homological algebra we have an analogous notion, that of a **chain homotopy** between chain complexes. As in the topological case, this leads to a notion of **chain homotopy equivalence** of chain complexes, and a chain homotopy equivalence is a **quasi-isomorphism**: that is, it induces an isomorphism on homology groups. Many of the basic uniqueness results in homological algebra come from showing that a certain complex is unique up to chain homotopy equivalence.

Two morphisms $f, g : C_\bullet \to D_\bullet$ are chain homotopic if there exists for all $n \in \mathbb{Z}^+$ a map $s_n : C_n \to D_{n+1}$ such that

$$f_n - g_n = d_{n+1} s_n + s_{n-1} d_n;$$

the sequence $\{s_n\}$ is called a chain homotopy. We write $f \sim g$.

Exercise 4.4) a) Let f be an additive functor from the category of left R-modules to the category of left S-modules. Show that there is an induced functor $\mathcal{C}(f)$ from chain complexes of R-modules to chain complexes of S-modules.
b) Let $f, g : A_\bullet \to B_\bullet$ be morphisms of chain complexes of R-modules, and let F be an additive functor from R-modules to S-modules. Show: $f \sim g \implies F(f) \sim F(g)$. (Hint: apply F to the chain homotopy between f and g!)

Proposition 3.1. *Let $f, g : C_\bullet \to D_\bullet$ be chain homotopic maps. Then $H_n(f) = H_n(g)$ for all $n \in \mathbb{Z}$.*

Proof. Replacing f and g by $f - g$ and 0, it suffices to assume that $g = 0$ and show that $H_n(f) = 0$ for all $n \in \mathbb{Z}$. We know that

$$f_n = d_{n+1} s_n + s_{n-1} d_n.$$

Let $\overline{x} \in H_n(C_\bullet)$, so $\overline{x}$ is represented by an element $x \in \operatorname{Ker} d_n : C_n \to C_{n-1}$. Then

$$f(x) = d_{n+1} s_n(x) + s_{n-1} d_n(x) = d_{n+1}(s_n(x)),$$

so x lies in the image of $d_{n+1} : C_{n+1} \to C_n$. □

Note well that chain homotopy is an equivalence relation between *maps* between chain complexes, just as in topology homotopy is an equivalence relation between *maps* between topological spaces. Just as in the topological case, we can use this relation to define an equivalence relation between chain complexes: we say that $C_\bullet$ and $D_\bullet$ are **chain homotopy equivalent** if there are maps $f : C_\bullet \to D_\bullet$, $g : D_\bullet \to C_\bullet$ such that

$$g \circ f \sim 1_{C_\bullet}, \; f \circ g \sim 1_{D_\bullet}.$$

Proposition 3.2. *Let $f : C_\bullet \to D_\bullet$. If f is a chain homotopy equivalence, it is a quasi-isomorphism. In other words, chain homotopic complexes have isomorphic homology.*

[6]The natural first reaction is to regard this as a weakness, e.g. that the methods of algebraic topology do not distinguish between $\mathbb{R}^m$ and $\mathbb{R}^n$. My algebraic topology teacher J.P. May surprised me by extolling it as a great advantage of the theory. In short, it turns out that he was right.

Proof. Let $g : D_\bullet \to C_\bullet$ be such that $g \circ f \sim 1_C$, $f \circ g \sim 1_D$. Then for all $n \in \mathbb{Z}$,

$$H_n(g) \circ H_n(f) = H_n(g \circ f) = H_n(1_C) = 1_{H_n(C)},$$
$$H_n(f) \circ H_n(g) = H_n(f \circ g) = H_n(1_D) = 1_{H_n(D)}.$$

So $H_n(f)$ and $H_n(g)$ are inverse isomorphisms between $H_n(C)$ and $H_n(D)$. □

3.4. **The Comparison Theorem.**

Theorem 3.3 (Comparison theorem for resolutions)**.**
a) Let $P_\bullet \xrightarrow{\epsilon} M$ be a projective resolution of the R-module M. Let $f_{-1} : M \to N$ be an R-module map, and let $Q_\bullet \xrightarrow{\eta} M$ be any resolution. Then there is a chain map $f : P_\bullet \to Q_\bullet$ such that $\eta f_0 = f_{-1}\epsilon$. Moreover f is unique up to chain homotopy.
b) Let $E^\bullet$ be an injective resolution of the R-module N. Let M be another R-module and $f_{-1} : M \to N$ be an R-module map. Then for every right resolution $A^\bullet$ of M there exists a homomorphism η from the chain complex $0 \to M \to A^\bullet$ to the chain complex $0 \to N \to E^\bullet$. Moreover η is unique up to chain homotopy.

Proof. a) Existence of s: By induction, suppose: for all $i \leq n$ we have $f_i : P_i \to Q_i$ such that $f_{i-1}d = df_i$. We must define $f_{n+1} : P_{n+1} \to Q_{n+1}$ such that $f_n d = df_{n+1}$.
If $n = -1$, then using the projectivity of P_0 we may lift the map $f_{-1}\epsilon : P \to N$ to a map $f_0 : P \to Q_0$: by construction this makes the rightmost square commute.
$n \geq 0$: $f_n : P_n \to Q_n$ restricts to a map $f_n : Z_n(P) \to Z_n(Q)$ on the cycles. Since $Q_\bullet$ is exact, the map $d : Q_{n+1} \to Z_n(Q)$ is a surjection. Since P_{n+1} is projective, we may lift the map $f_n|_{Z_n(P)} \circ (d : P_{n+1} \to Z_n(P))$ to a map $f_{n+1} : P_{n+1} \to Q_{n+1}$. Then $df_{n+1} = f_n|_{Z_n(P)} \circ d = f_n \circ d$.
Uniqueness of s: Let $g : P_\bullet \to Q_\bullet$ be another chain map satifying $\eta g_0 = f{-}1\epsilon$, and put $h = f - g$. We will construct a chain homotopy $s_n : P_n \to Q_{n+1}$ from h to the zero map by induction.
If $n < 0$, then $P_n = 0$, so put $s_n = 0$.
If $n = 0$, then since

$$\eta h_0 = \eta(f_0 - g_0) = f_{-1}\epsilon - f_{-1}\epsilon = 0,$$

by exactness of $Q_\bullet$ we have $h_0(P_0) \subset d(Q_1)$. Since P_0 is projective, we can lift the map $P_0 \to d(Q)$ to a map $s_0 : P_0 \to Q_1$. This satisfies $h_0 = s_0 d + ds_{-1}$.
Inductively, suppose that for all $i < n$ we have maps s_i such thta

$$ds_{n-1} = h_{n-1} - s_{n-2}d$$

and consider

$$h_n - s_{n-1}d : P_n \to Q_n.$$

Now we compute

$$d(h_n - s_{n-1}d) = dh_n - (h_{n-1} - s_{n-2}d)d = dh_n - h_{n-1}d + s_{n-2}dd = 0.$$

Therefore we get a map

$$h_n - s_{n-1}d : P_n \to Z_n(Q) = Q_{n+1}/d(Q_{n+2}).$$

By projectivity of P_n, we may lift this to a map

$$s_n : P_n \to Q_{n+1},$$

i.e., $ds_n = h_n - s_{n-1}d$. We're done.
b) This is the dual version of part a). We may safely leave it to the reader. □

Exercise 4.5) Prove part b) of the Comparison Theorem.

3.5. **The Horseshoe Lemma.**

Proposition 3.4. *(Horseshoe Lemma) Given a diagram ... where the columns are projective resolutions and the row is exact, there is a projective resolution $P_\bullet$ of A and chain maps so that the three columns form an exact sequence of complexes.*

Proof. By projectivity, the map $P_0'' \to A''$ lifts to a map $P_0'' \to A$. Taking the direct sum of this with ϵ' defines a map from $P_0' \oplus P_0''$ making the diagram commute. Applying the Snake Lemma to

$$0 \to \ker \epsilon' \to \ker \epsilon \to \ker \epsilon''$$

$$0 \to P_0' \to P_0 \to P_0'' \to 0$$

$$0 \to A' \to A \to A'' \to 0$$

shows that the first row is exact and ϵ is surjective. We proceed upwards filling in the horseshoe by induction. □

3.6. **Some Diagram Chases.**

Proposition 3.5. *(Snake Lemma) Given a commutative ladder of short exact sequences of left R-modules:*

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

$$0 \to A' \xrightarrow{f'} B' \xrightarrow{g'} C'$$

a) There is an exact sequence

$$\ker \alpha \to \ker \beta \to \ker \gamma \xrightarrow{S} \operatorname{coker} \alpha \to \operatorname{coker} \beta \to \operatorname{coker} \gamma.$$

b) If f is an injection, so is $\ker \alpha \to \ker \beta$.
c) If g is a surjection, so is $\operatorname{coker} \beta \to \operatorname{coker} \gamma$.

Proof. (K. Gunzinger, c.f. `http://www.youtube.com/watch?v=etbcKWEKnvg`)
a) Let me just show you how to construct the map S, which is the fun of the lemma anyhow, okay? So you assume you have an element in $\ker \gamma$ – that is an element $c \in C$ such that $\gamma(c) = 0$. You pull it back to $b \in B$ – i.e., by surjectivity of f, we choose $b \in B$ such that $f(b) = c$ – and note that b is unique up to addition of an element in the image of f. Then you take $\beta(b)$, which takes you to 0 in C' by the commutativity of the diagram. So $\beta(b)$ lies in the kernel of g' hence in the image of f', by exactness: there is $a' \in A'$ with $f'(a') = \beta(b)$.[7] It turns out that the class of $a' \in A'/(\alpha A) = \operatorname{coker} \alpha$ *is* well-defined, and this defines the map S.
b) and c) These follow immediately: too much so to be left as exercises. □

Exercise 4.6) a) Check that indeed the image of $a' \in \operatorname{coker} \alpha$ is well-defined: this is short case around the left-most square in the diagram.
b) Check the rest of the lemma: that the maps fit together into an exact sequence.
c) In the movie clip there is a student, Mr. Cooperman, who interrupts throughout the proof to make "objections", each of which the instructor immediately recognizes as a prompting for a justification she gives of the well-definedness of the map S. As the class ends, Mr. Cooperman says "This stuff is just garbage. It's another diagram chase. When are we going to move on to something interesting?" Do you find this comment insightful and/or appropriate? What about his interrupting

[7]The element a' depended on the choice of b lifting c, so the ambiguity is parameterized by elements of A.

objections during the proof itself (which, as it turns out, do not cause Dr. Gunzinger to break her stride)? After a further exchange suggesting that Dr. Gunzinger has gone as far as she can with her group-theoretic research and that he's exploring a whole new angle on the problem, Mr. Cooperman walks out of the room and Dr. Gunzinger mutters "fuckface." Discuss.

Lemma 3.6. *Let*

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

be a short exact sequence. If any two of the complexes are exact, so is the third.

Proof. (I acknowledge help from `http://math.stackexchange.com/questions/32841`.) We will remove subscripts from maps and non-ambiguous parentheses – as the reader will see, this helps to make reading the arguments bearable.

Step 1: Suppose $A_\bullet$ and $B_\bullet$ are exact. Let $n \in \mathbb{Z}$ and let $c \in C_n$ be such that $dc = 0$. We want to find an element of C_{n-1} which maps to c. By the surjectivity of g, there is $b \in B_n$ with

$$g(b) = c.$$

Since $0 = d(c) = d(g(b)) = g(d(b))$, by exactness there is $a \in A_{n-1}$ with

$$f(a) = db.$$

We have

$$f(d(a)) = d((a))) = d(d(b)) = 0,$$

and, since f is injective, this implies $d(a) = 0$. By exactness of $A_\bullet$, there is $a' \in A_n$ with $d(a') = a$. Consider $b - f(a') \in B_n$: we have

$$d(b - f(a')) = d(b) - d(f(a')) = d(b) - f(d(a')) = d(b) - d(b) = 0,$$

so by exactness of $B_\bullet$ there is $b' \in B_{n+1}$ with

$$d(b') = b - f(a').$$

Now we have

$$d(g(b')) = g(d(b')) = g(b) - g(f(a)) = c - 0 = c.$$

Step 2: Suppose $A_\bullet$ and $C_\bullet$ are exact. Let $n \in \mathbb{Z}$ and let $b \in B_n$ be such that $db = 0$. Let

$$c = g(b).$$

Then

$$d(c) = d(g(b)) = g(d(b)) = g(0) = 0,$$

so by exactness of $C_\bullet$ there is $\tilde{c} \in C_{n-1}$ with

$$d(\tilde{c}) = c.$$

Since $g_\bullet$ is surjective, there is $\tilde{b} \in B$ such that

$$g\tilde{b} = \tilde{c}.$$

We might hope that $d(\tilde{b}) = b$, but this is not the case. Instead we analyze the difference: let

$$b' = d\tilde{b} - b \in B_n.$$

Since

$$g(b') = gd\tilde{b} - gb = dg\tilde{b} - c = d\tilde{c} - c = c - c = 0,$$

there is $a \in A_n$ with

$$f(a) = b'.$$

Further, we have

$$fda = dfa = db' = dd\tilde{b} - db = 0.$$

Since f is injective, this means $da = 0$, and since $A_\bullet$ is exact, this means there is $\tilde{a} \in A_{n-1}$ such that

$$d\tilde{a} = a.$$

Now we calculate

$$d(\tilde{b} - f\tilde{a}) = d\tilde{b} - fd\tilde{a} = d\tilde{b} - fa = d\tilde{b} - b' = b.$$

Step 3: Suppose $B_\bullet$ and $C_\bullet$ are exact, let $n \in \mathbb{Z}$, and let $a \in A_n$ be such that $da = 0$. Then

$$dfa = fda = f0 = 0,$$

so by exactness of $B_\bullet$ there is $b \in B_{n+1}$ with $db = fa$. Since

$$dgb = gdb = gfa = 0,$$

by exactness of $C_\bullet$ there is $c \in C_{n+2}$ with $dc = gb$. By surjectivity of g there is is $\tilde{b} \in B_{n+2}$ with $g\tilde{b} = c$. Since

$$g(b - d\tilde{b}) = gb - dg\tilde{b} = gb - gb = 0,$$

there is $\tilde{a} \in A_{n+1}$ with

$$f(\tilde{a}) = b - d\tilde{b}.$$

Then

$$f(d\tilde{a} - a) = df\tilde{a} - fa = db - dd\tilde{b} - f(a) = 0.$$

Since f is injective, $d\tilde{a} = a$. $\square$

Proposition 3.7. *(3×3 Lemma) Suppose we are given a commutative diagram with exact columns of the form*

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

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

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

Then:
a) If the last two rows are exact, so is the first.
b) If the top and bottom row are exact and $gf = 0$, then the middle row is exact.
c) If the top two rows are exact, so is the bottom.

Proof. In all three cases the strategy is to show that the remaining row is a complex and apply the preceding lemma.
a) Suppose the last two rows are exact. Let $a' \in A'$. We must show $g'f'a' = 0$. Since $d : C' \to C$ is injective, it's enough to show that $dg'f'a' = 0$, but

$$dg'f'a' = g'f'da' = 0.$$

Case 2: In this case the additional hypothesis $gf = 0$ is supplied to us, so there is nothing else to show.
Case 3: Suppose the first two rows are exact, and let $a'' \in A''$. Lift a'' to $a \in A$. Then $gfa = 0$, so by commutativity of the diagram $g''f''a'' = 0$. $\square$

Proposition 3.8. *(Five Lemma) Consider a commutative ladder with exact rows:*

$$A_1 \overset{d_1}{\to} A_2 \overset{d_2}{\to} A_3 \overset{d_3}{\to} A_4 \overset{d_4}{\to} A_5$$

$$B_1 \to B_2 \to B_3 \to B_4 \to B_5.$$

a) If h_2 and h_4 are surjective and h_5 is injective, then h_3 is surjective.
b) If h_2 and h_4 are injective and h_1 is surjective, then h_3 is injective.
c) If h_1, h_2, h_4, h_5 are isomorphisms, then h_3 is an isomorphism.

Proof. a) Let $b_3 \in B_3$. Map it into B_4 via d_3. Since h_4 is surjective, there is $a_4 \in A_4$ with $h_4(a_4) = d_3(b_3)$. Furthermore, by exactness at B_4 and commutativity of the diagram we have

$$0 = d_4(d_3(b_3)) = d_4(h_4(a_4)) = h_5(d_4(a_4)).$$

Since h_5 is injective, $d_4(a_4) = 0$, so by exactness at A_4 there is $a_3 \in A_3$ such that $d_3(a_3) = a_4$. Now one's first thought is that $h_3(a_3) = b_3$, but in fact this need not be the case: what we have is that

$$d_3(b_3 - h_3(a_3)) = d_3(b_3) - h_4(d_3(a_3)) = d_3(b_3) - h_4(a_4) = 0,$$

so $b_3 - h_3(a_3) = d_2(b_2)$ for some $b_2 \in B_2$. Since h_2 is surjective, $b_2 = h_2(a_2)$ for some $a_2 \in A_2$. Now we compute

$$h_3(d_2(a_2)+a_3)) = d_2(h_2(a_2))+h_3(a_3) = d_2(b_2)+h_3(a_3) = b_3-h_3(a_3)+h_3(a_3) = b_3.$$

b) This is the dual statement to part a); we leave the proof as an exercise.
c) This follows immediately from parts a) and b). □

Exercise 4.7) Prove the **Short Five Lemma**.

Proposition 3.9. *Given a commutative diagram with exact rows*

$$A' \to A \to A'' \to 0$$

$$f \;\; g$$

$$B' \to B \to B'' \to 0,$$

(here we have $f : A' \to B'$ and $g : A'' \to B''$), there is a unique $h : A'' \to B''$ making the diagram commute. Moreover, if both f and g are isomorphisms, so is h.

Exercise: Prove Proposition 3.9.

3.7. **The Fundamental Theorem on Chain Complexes.**

Theorem 3.10. *Let $0 \to A_\bullet \to B_\bullet \to C_\bullet \to 0$ be a short exact sequence of chain complexes of left R-modules.*
a) There is a ***long exact homology sequence***

$$\ldots H_n(C) \overset{\delta}{\to} H_{n-1}(A) \to H_{n-1}(B) \to H_{n-1}(A) \overset{\delta}{\to} \ldots.$$

b) Formation of the long exact homology sequence is ***natural*** *in the sense that a commutative ladder of chain complexes gives rise to a commutative ladder of long exact homology sequences.*

Proof. a) The Snake Lemma gives us a commutative diagram with exact rows:

$$H_n(A) \to H_n(B) \to H_n(C)$$

$$A_n/d(A_{n+1}) \to B/d(B_{n+1}) \to C_n/d(C_{n+1}) \to 0$$

$$0 \to Z_{n-1}(A) \to Z_{n-1}(B) \to Z_{n-1}(C).$$

Then we take the connecting homomorphism δ to be $S : H_n(C) \to H_{n-1}(A)$. These give the connecting homomorphisms and the exactness. For later use it is convenient to record the explicit recipe for $\delta : H_n(C) \to H_{n-1}(A)$: take $z \in H_n(C)$, represent it by $c \in Z_n(C)$; lift c to $b \in B_n$ and apply d. Then db lies in $Z_{n-1}(A)$ and hence defines an element $\delta z \in H_{n-1}(A)$.
b) The functoriality of homology shows that two out of every three squares commute (the ones not involving a connecting homomorphism). For the commutativity of the third square, we use the explicit recipe for δ mentioned above. □

4. Derived Functors

4.1. **(Well)-definedness of the derived functors.**

4.1.1. *Derived functors.*

Let F be a right exact additive covariant functor on the category of R-modules. We will define a sequence $\{L_nF\}_{n\in\mathbb{N}}$ of functors, with $L_0F = F$, called the **left derived functors** of F. The idea here is that the left-derived functors quantify the failure of F to be exact.

Let M be an R-module. We define all the functors L^nM at once, as follows: first we choose any projective resolution $P_\bullet \to M \to 0$ of M. Second we take away the M, getting a complex $P_\bullet$ which is exact except at P_0, i.e.,

$$H_0(P) = P_0/\operatorname{Image}(P_1 \to P_0) = P_0/\operatorname{Ker}(P_0 \to M) = M,$$

$$\forall n > 0, H_n(P) = 0.$$

Third we apply the functor F getting a new complex $FP_\bullet$. And finally, we take homology of this new complex, defining

$$(L_nF)(M) := H_n(FP_\bullet).$$

Now there is (exactly?) one thing which is relatively clear at this point.

Proposition 4.1. *We have* $(L_0F)(M) = FM$.

Proof. Since $P_1 \to P_0 \to M \to 0$ is exact and F is right exact, $FP_1 \to FP_0 \to FM \to 0$ is exact, hence

$$\operatorname{Image}(FP_1 \to FP_0) = \operatorname{Ker}(FP_0 \to FM).$$

Thus

$$(L_0F)(M) = H_0(FP_\bullet) = \operatorname{Ker}(FP_0 \to 0)/\operatorname{Image}(FP_1 \to FP_0)$$
$$= FP_0/\operatorname{Ker}(FP_0 \to FM) = FM.$$

□

Before saying anything else about the left derived functors L_nF, there is an obvious point to be addressed: how do we know they are well-defined? On the face of it, they seem to depend upon the chosen projective resolution $P_\bullet$ of M, which is very far from being unique. To address this point we need to bring in the Comparison Theorem for Resolutions (Theorem 3.3). Namely, let $P'_\bullet \to M \to 0$ be any other projective resolution of M. By Theorem 3.3, there exists a homomorphism of chain complexes $\eta : P_\bullet \to P'_\bullet$ which is unique up to chain homotopy. Interchanging the roles of $P'_\bullet$ and $P_\bullet$, we get a homomorphism $\eta' : P'_\bullet \to P_\bullet$. Moreover, the composition $\eta' \circ \eta$ is a homomorphism from $P_\bullet$ to itself, so by the uniqueness $\eta' \circ \eta$ is chain homotopic to the identity map on $P_\bullet$. Similarly $\eta \circ \eta'$ is chain homotopic to the identity map on $P'_\bullet$, so that η is a chain homotopy equivalence. By Exercise 3.71, $F\eta : FP_\bullet \to FP'_\bullet$ is a chain homotopy equivalence, and therefore the induced maps on homology $H_n(F\eta) : H_n(FP_\bullet) \to H_n(FP'_\bullet)$ are isomorphisms. Thus we have shown that two different choices of projective resolutions for M lead to *canonically* isomorphic modules $(L_nF)(M)$.

Exercise 5.1: a) Suppose M is projective. Show that for any right exact functor F and all $n > 0$, $(L_nF)(M) = 0$.
b) Suppose M is injective. Show that for any left exact functor F and all $n > 0$, $(R^nF)(M) = 0$.

4.2. **The Long Exact Co/homology Sequence.**

The next important result shows that a short exact sequence of R-modules induces a long exact sequence involving the left-derived functors and certain connecting homomorphisms (which we have not defined and will not define here).

Theorem 4.2. *Let*

$$0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow M_3 \longrightarrow 0 \tag{1}$$

be a short exact sequence of R-modules, and let F be any left exact functor on the category of R-modules. Then:
a) There is a long exact sequence
(2)
$$\ldots \to (L_2F)(M_3) \stackrel{\partial}{\to} (L_1F)(M_1) \to (L_1F)(M_2) \to (L_1F)(M_3) \stackrel{\partial}{\to} FM_1 \to FM_2 \to FM_3 \to 0.$$

b) The above construction is functorial in the following sense: if $0 \longrightarrow N_1 \longrightarrow N_2 \longrightarrow N_3 \longrightarrow 0$ is another short exact sequence of R-modules and we have maps $M_i \to N_i$ making a "short commutative ladder", then there is an induced "long commutative latter" with top row the long exact sequence associated to the first short exact sequence and the bottom row the long exact sequence associated to the second short exact sequence.

Proof. a) Let

$$0 \to A' \to A \to A'' \to 0$$

be a short exact sequence of left R-modules. Choose projective resolutions $P'_\bullet$ of A' and $P''_\bullet$ of A'', and apply the Horseshoe Lemma to get a short exact sequence of chain complexes

$$0 \to P'_\bullet \to P_\bullet \to P''_\bullet \to 0.$$

For all n, since P''_n is projective, the sequence

$$0 \to P'_n \to P_n \to P''_n \to 0$$

splits. Additive functors preserve split exact sequences, so

$$0 \to F(P'_\bullet) \to F(P_\bullet) \to F(P''_\bullet) \to 0$$

is a short exact sequence of chain complexes. Applying the Fundamental Theorem on Chain Complexes to this short exact sequence, we get a long exact homology sequence.
b) See [W, pp. 46-47]. $\square$

Now, dually, if F is a right exact functor on the category of R-modules, we may define **right derived functors** R^nF. Namely, for an R-module M, first choose an injective resolution $0 \to M \to E^\bullet$, then take M away to get a cochain complex $E^\bullet$, then apply F to get a cochain complex $FE^\bullet$, and then finally define $(R^nF)(M) = H^n(FE^\bullet)$. In this case, a short exact sequence of modules (1) induces a **long exact cohomology sequence**
(3)

$$0 \to FM_1 \to FM_2 \to FM_3 \xrightarrow{\partial} (R^1F)(M_1) \to (R^1F)(M_2) \to (R^1F)(M_3) \xrightarrow{\partial} (R^2F)(M_1)\ldots$$

Exercise 5.2: Let F be right exact from R-modules to S-modules. Show TFAE:
(i) F is exact.
(ii) For all $n \geq 1$ and all R-modules M, $L_nF(M) = 0$.
(iii) For all R-modules M, $L_1(F)(M) = 0$.

Remark: Exercise 5.2 is our first indication that properties of L_1F imply properties of L_nF for $n \geq 1$. This will later be studied in more detail, leading to a proof technique called **dimension shifting**.

Exercise 5.3: Suppose F is an additive functor which need not be left or right exact. Note that our recipe for deining the left-derived functors $L_nF(M)$ still makes sense: choose a projective resolution $P_\bullet \to M \to 0$, and define $L_nF(M) = H_n(FP_\bullet)$.
a) Show that the L_nF are well-defined indepedent of the projective resolution.
b) Show that we still have a long exact homology sequence.
c) Show that L_0F is right exact.
d) Show that the following are equivalent:
(i) F is right exact.
(ii) $F \cong L_0F$.

Exercise 5.4: State and prove an analogue of Exercise 5.3 for right-derived functors of arbitrary additive functors.

Remark: Exercises 5.3 and 5.4 are adapted from the exposition in [Rot], whichc indeed defines left- and right-derived functors for any additive functor. This is nice to know. It would be nicer to have an example in which derived functors of a neither left nor right exact functor naturally arise. I do not know of such an example.

4.3. **Delta Functors.**

A **homological** δ-functor between abelian categories $\mathcal{A}$ and $\mathcal{B}$ is a sequence of additive functors $T_n : \mathcal{A} \to \mathcal{B}$ together with, for each short exact sequence

$$0 \to A \to B \to C \to 0 \tag{4}$$

in $\mathcal{A}$, morphisms

$$\delta_n : T_n C \to T_{n-1} A,$$

satisfying the following key properties: (DF1) Each short exact sequence(4) induces a **long exact homology sequence**

$$T_{n+1}(C) \xrightarrow{\delta} T_n(A) \to T_n(B) \to T_n(C) \xrightarrow{\delta} T_{n-1}(A) \to \dots .$$

(DF2) Functoriality: a commutative ladder of short exact sequences induces a long commutative ladder in homology.

Exercise: Write down a reasonable definition of a morphism of δ-functors and check that it is correct.

Exercise: If $T = \{T_n\}$ is a δ-functor, show that T_0 is right exact.

Exercise: A **cohomological** δ-functor $\{T_n : \mathcal{A} \to \mathcal{B}\}$ is a homological δ-functor $\{T_n : \mathcal{A}^{\mathrm{op}} \to \mathcal{B}\}$. Unwind this to get the standard definition, including the long exact **cohomology sequence**.

Exercise: Let $\mathcal{A}$ be an abelian category and let $C(\mathcal{A})$ be the category of chain complexes in $\mathcal{A}$. By the Fundamental Theorem of Homological Algebra, the homology functors $H_n : C(\mathcal{A}) \to \mathcal{A}$ form a homological δ-functor.

Key Example: For any right exact functor T_0, the left derived functors extend T_0 to a homological δ-functor.

Example: Let R be a ring, and let $r \in R$ giving a projective resolution for R/rR. We claim that there is a homological δ-functor from R-modules to R-modules with $T_0(M) = M[r]$, $T_1(M) = M/rM$ and $T_n(M) = 0$ for all $n > 1$. Indeed, to see this, apply the Snake Lemma to the diagram

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

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

where the vertical maps are multiplication by r.

On the other hand, since the function $T_0(M) = M/rM$ is right exact, we can *also* extend it to a δ-functor by taking its derived functors. Is this the same δ-functor? Note that $M/rM = M \otimes_R R/rR$, so $T_n(M) = \mathrm{Tor}_n(R/rR, M)$. Are these homological δ-functors the same?

Exercise (Doyle): Suppose r is a left non-zerodivisor in R, i.e., we have a short exact sequence

$$0 \to R \xrightarrow{r\bullet} R \to R/rR \to 0.$$

Use this to show that $\mathrm{Tor}_1(R/rR, M) = M[r]$ and $\mathrm{Tor}_n(R/rR, M) = 0$ for all $n \geq 2$ and all m, so indeed the modules are the same.

However, for a zero divisor r, $\mathrm{Tor}_1(R/rR, M)$ is the quotient of $M[r]$ by the submodule generated by $\{sm \mid rs = 0, r \in R, m \in M\}$, so they do not coincide. On the other hand, at least we have a map from one δ-functor to the other. We hope this motivates the following definition of Grothendieck.

A homological δ-functor T is **universal** if for any δ-functor S and natural transformation $f_0 : S_0 \to T_0$, there is a unique morphism $f = (f_n : S_n \to T_n)$ extending f_0.

Exercise*: Show that homology $H_\bullet : C(\mathcal{A}) \to \mathcal{A}$ is a universal δ-functor.

Theorem 4.3 (Cartan-Eilenberg)**.** *Let $\mathcal{A}, \mathcal{B}$ be abelian categories.*
a) Assume that $\mathcal{A}$ has enough projective objects. For any right exact functor $F : \mathcal{A} \to \mathcal{B}$, the left derived functors L_nF form a universal homological δ-functor.
b) Assume that $\mathcal{A}$ has enough injective objcets. For any left exact functor $F : \mathcal{A} \to \mathcal{B}$, the right derived functors R_nF form a universal cohomological δ-functor.

Proof. [W, Thm. 2.4.7]. □

In fact we mention a strengthening of this theorem. An additive functor $F : \mathcal{A} \to \mathcal{B}$ is **effaceable**[8] if for any object A of $\mathcal{A}$ there is a monomorphism $\iota : A \to I$ with $F(\iota) = 0$. Dually, an additive functor $F : \mathcal{A} \to \mathcal{B}$ is **coeffaceable** if for every A there is a surjection $u : P \to A$ with $F(u) = 0$.

Exercise: If $\mathcal{A}$ has enough projectives and F is right exact, then its left derived functors L_nF for $n \geq 1$ are coeffaceble. Dually...

Theorem 4.4 (Grothendieck)**.** *If T is a homological δ-functor with T_n coeffaceable for all $n \geq 1$, then T is universal. Dually...*

4.4. **Dimension Shifting and Acyclic Resolutions.**

Let F be an additive functor from the category of R-modules to the category of S-modules. An R-module M is **F-acyclic (for homology)** if $L_nF(M) = 0$ for all $n > 0$. (An R-module M is **F-acyclic (for cohomology)** if $R^nF(M) = 0$ for all $n > 0$. As usual, in practice we only take left-derived functors of right exact functors and right-derived functors of left exact functors, so it will be clear from the context whether we are considering acyclic objects for homology or cohomology.)

Example: Projective modules are F-acyclic for homology for any functor F. Injective modules are F-acyclic for cohomology for any functor F. is flat iff it is acyclic for $M \otimes \cdot$ for all right R-modules M.

A left resolution $J_\bullet \to M \to 0$ of M is **F-acyclic** if each J_n is F-acyclic for homology. Thus in particular projective resolutions are F-acyclic and we can use them to compute the derived functors $L_n(F)$. In fact we can use any F-acylic resolution for this purpose.

[8]This terminology comes from Grothendieck's Tohoku paper, written in French. Some anglophone authors have suggested "erasable" intead, but the majority stay with Grothendieck's terminology

Exercise 5.5: Let M, X be left R-modules, N be a submodule of M, let $q : M \to M/N$ be the quotient map, let $\overline{f} : M/N \to X$ be an R-module map, and let $f = \overline{f} \circ q$. Show:

$$(\ker f)/N = \ker \overline{f}.$$

Theorem 4.5 (Acylic Resolutions Compute Derived Functors)**.** *Let F be a right exact functor from the category of left R-modules to the category of left S-modules. Let M be a left R-module, and let $J_\bullet \to M \to 0$ be an F-acylic resolution. Then there are canonical isomorphisms*

$$L_n F(M) \cong H_n(FJ_\bullet)$$

for all $n \geq 0$.

Proof. We split the resolution $J_\bullet \to M \to 0$ into a short exact sequence

$$0 \to K \to J_0 \to M \to 0 \tag{5}$$

and a resolution $\ldots \to J_2 \to J_1 \to K \to 0$, which we denote by $I_\bullet \to K \to 0$. Now we argue by induction on n.

$n = 0$: Looking back at the proof of Proposition 4.1 we see immediately that the proof $L_0 F = F$ did not use that the resolution was a projective resolution but only the right exactness of F. So $H_0(FJ_\bullet) \cong F(M) \cong L_0 F(M)$.

$n = 1$: Applying the right exact functor F to (5) we get

$$L_1F(J_0) \to L_1F(M) \to F(K) \to F(J_0) \to F(M) \to 0.$$

Since J_0 is F-acyclic, $L_1F(J_0) = 0$, so

$$L_1F(M) = \ker F(K) \to F(J_0).$$

Since F is right exact, $F(J_0) \to F(J_1) \to F(K) \to 0$ is exact and thus

$$F(K) = F(J_1)/(\text{Image}(F(J_2) \to F(J_1)).$$

Putting these together and using Exercise 5.5, we get

$$L_1F(M) = (\ker F(J_1) \to F(J_0))/(\text{Image}\, F(J_2) \to F(J_1)) = H_1(FJ_\bullet).$$

$n \geq 2$: By induction we may assume the isomorphism of functors holds for all $i \leq n$. Since J_0 is F-acyclic, the long exact homology sequence associated to (5) has every third term vanishing and thus yields isomorphisms

$$L_{i+1}F(M) \cong L_iF(K)$$

for all $i \geq 1$. Then we get

$$L_nF(M) \cong L_{n-1}F(K) \cong H_{n-1}(FI_\bullet) \cong H_n(FJ_\bullet),$$

where the middle isomorphism is by induction. □

Remark: Once we *balance the bifunctor tor*, we will see that a left R-module N is flat iff it is acyclic for all functors $N \mapsto M \otimes_R N$, and it will follow that the tor functors can be computed using *flat resolutions*.

5. Abelian Categories

A category $\mathcal{C}$ is **pre-additive** if for all objects $A, B \in \mathcal{C}$, the set $\mathrm{Hom}(A, B)$ is endowed with the structure of a commutative group so that composition distributes over addition.

Exercise: For any object A in a pre-additive category, $\mathrm{End}\, A := \mathrm{Hom}(A, A)$ is a ring.

An **initial object** in a category $\mathcal{C}$ is an object I such that for all objects X, $\#\,\mathrm{Hom}(I, X) = 1$. A **terminal object** is an object T such that for all objects X, $\#\,\mathrm{Hom}(X, T) = 1$. That the passage from a category to its opposite category converts initial objects to terminal objects and conversely.

Exercise: a) Let I, I' be initial objects in a category. Show that there is a unique isomorphism between them.
b) Let T, T' be terminal objects in a category. Show that there is a unique isomorphism between them.

A **zero object** in a category is an object which is both initial and terminal.

Exercise: a) Find all initial and terminal objects in the category of sets.
b) Show that the category of sets does not have a zero object.
c) Show that the trivial group is a zero object in the category of groups.
d) Show that the zero module is a zero object in the category of left (or right) R-modules.

An **additive category** is a pre-additive category with a zero object and possesing finite direct products.

Exercise: In any additive category, finite products and finite coproducts coincide. (This coincidence of products and coproducts sometimes goes by the name **biproduct**.)

In a category $\mathcal{C}$, a morphism $f : B \to C$ is **monic** (noun form: a **monomorphism**) if for all objects C and all morphisms $e_1, e_2 : A \to B$, $fe_1 = fe_2 \implies e_1 = e_2$. In other words, a monic morphism is one which can be cancelled on the left.

Similarly, a morphism $f : A \to B$ is **epic** (noun form: an **epimorphism**) if for all objects C and all morphisms $e_1, e_2 : B \to C$, $e_1 f = e_2 f \implies e_1 = e_2$. In other words, an epic morphism is one which can be cancelled on the right.

Exercise: Show that in any concrete category, an injection is a monomorphism and a surjection is an epimorphism.

Exercise: Show that in any of the following concrete categories – groups, abelian groups, sets, posets, rings, R-modules – a morphism is monic iff it is injeective.

Exercise: Show that the map $\mathbb{Q} \to \mathbb{Q}/\mathbb{Z}$ is monic in the (sub)category of divisible abelian groups.

Example: The map $\mathbb{Z} \to \mathbb{Q}$ is epic in the category of commutative rings even though it is not surjective. The same holds for any nontrivial localization map on commutative rings.

Suppose our category has a zero object 0. This forces all Homsets to be nonempty: indeed we have $B \to 0 \to C$. By the **kernel** of a morphism $f : B \to C$ we mean a morphism $\iota : A \to B$ satisfying $f \circ \iota = 0$ and being universal for this: any $\iota' : A' \to B$ such that $f \circ \iota' = 0$ factors through ι. Any kernel is a monic and any two kernels of the same map are canonically isomorphic.

A **cokernel** of $f : B \to C$ is a map $p : C \to A$ such that $p \circ f = 0$ and p is universal for this property. Cokernels are epic and unique up to canonical isomorphism.

For a morphism $f : B \to C$, we define the **image** of f as $\ker \operatorname{coker} f$. Thus, when kernels and cokernels exist, we can speak of exact sequences.

Let $f, g : X \to Y$ in a category $\mathcal{C}$. An **equalizer** of f and g is a morphism $a : A \to X$ such that $fa = ga$ and a is universal for this: for any $a' : A' \to X$ with $fa' = ga'$, there is a unique morphism $\iota : a \to a'$ with $a'\iota = a$.

A **coequalizer** of f and g is a morphism $q : Y \to Q$ such that $qf = qg$ and which is universal for this property: for any $q' : Y \to Q'$ with $q'f = q'g$, there is a unique morphism $\iota : Q' \to Q$ with $\iota q' = q$.

Exercise: Let $\mathcal{C}$ be a category with a zero object.
a) Show that a kernel of $f : X \to Y$ is precisely an equalizer of f and $0 : X \to Y$.
b) Show that a cokernel of $f : X \to Y$ is precisely a coequalizer of f and $0 : X \to Y$.
c) Suppose $\mathcal{C}$ is additive, and let $f, g : X \to Y$. Show that $\operatorname{Ker} f - g = E(f - g)$. Deduce that an additive category with kernels has equalizers.
d) State and prove the analogue of part c) for coequalizers.

Exercise: For any family $\{f_i : X \to Y\}_{i \in I}$ of morphisms in a category $\mathcal{C}$, one can define the equalizer $E(\{f_i\})$ and the coequalizer $\exists(\{f_i\})$.
a) Do so.
b) Construct equalizers and coequalizers in the category of sets.

Let $f : Z \to X$ and $g : Z \to Y$ be morphisms in a category $\mathcal{C}$. A **pushout** of f and g is an object P and morphisms $\iota_1 : X \to P$, $\iota_2 : Y \to P$ satisfying the following universal mapping property: for any object Q and morphims: $j_1 : X \to Q$, $j_2 : Y \to Q$ such that $j_1 f = j_2 g$, there is a unique map $\iota : P \to Q$ such that $\iota\iota_1 = j_1$ and $\iota\iota_2 = j_2$.

Recall that in the category of groups the pushout is called the **amalgamated product**. They come up in the Seifert-van Kampen Theorem: let X be a path-connected topological space and suppose $X = U \cup V$ where U and V are path-connected open subsets. Then $\pi_1(X)$ is the pushout of $\pi_1(U \cap V) \to \pi_1(U)$ and $\pi_1(U \cap V) \to \pi_1(V)$.

Exercise: Show that the pushout in the category of commutative rings is the tensor product of algebras.

Exercise: Let $\mathcal{C}$ be a category with an initial object I.
a) Show that the coproduct of $X, Y \in \mathcal{C}$ is the pushout of $I \to X$, $I \to Y$.
b) Show that the coequalizer of $f, g : X \to Y$ is the pushout of $(f, g) : X \to Y \times Y$ and $(1, 1) : X \to X \times X$.
c) Let $f : X \to Y$ and $g : X \to Z$. Denote by $\iota_1 : X \to X \coprod Y$ and $\iota_2 : Y \to X \coprod Y$ the canonical maps into the coproduct. Show that the pushout of f and g is the coequalizer of $\iota_1 f : Z \to X \coprod Y$ and $\iota_g : Z \to X \coprod Y$.
d) Deduce that pushouts exist iff coequalizers and binary coproducts exist.

Exercise: a) Pushouts can be defined for any set of maps $f_i : X \to Y_i$. Do so.
b) Show that if an additive category has pushouts – i.e., pairwise pushouts – then it has all finite pushouts.
c) Show that a category with an initial object has arbitrary pushouts iff it has arbitrary coproducts and arbitrary coequalizers.

A **pullback** of $f : X \to Z$, $g : Y \to Z$ is an object P and morphisms $\pi_1 : P \to X$, $\pi_2 : P \to Y$ satisfying the following universal mapping property: given $\pi_1' : P' \to X$ and $\pi_2' : P' \to Y$ with $f\pi_1' = g\pi_2'$, there is a unique morphism $\pi : P' \to P$ such that $\pi_1 \pi = \pi_1'$, $\pi_2 \pi = \pi_2'$.

Example: In the category of sets, the pull back of $f : X \to Z$ and $g : Y \to Z$ is (merely?) the collection of all $(y, z) \in Y \times Z$ such that $f(y) = g(z)$.

Exercise:
a) Notice that pullbacks in $\mathbb{C}$ are pushouts in the opposite category $\mathbb{C}^{\mathrm{op}}$. Use this observation to give immediate proofs of the following:
b) A category with a terminal object admits binary pullbacks iff it admits binary equalizers and binary products.
c) Define the pullback of an arbitrary family of maps $\{f_i : X_i \to Y\}_{i \in I}$.
d) A category with a terminal object admits arbitrary pullbacks iff it admits arbitrary equalizers and arbitrary products.

Exercise: We work in an additive category with kernels. Suppose that P is the pullback of $f : X \to Z$, $g : Y \to Z$. Show that the kernel of $\pi_1 : P \to X$ is canonically isomorphic to $\ker f$.

5.1. **Definition and First Examples.**

Definition: An **abelian category** is an additive category in which
(AB1) Every morphism in $\mathcal{C}$ has a kernel and a cokernel.
(AB2) Every monic in $\mathcal{C}$ is the kernel of its cokernel.
Every epic in $\mathcal{C}$ is the cokernel of its kernel.

Example: For any ring R, the categories of left- and right- R-modules are abelian.

Exercise: Explain why this is really one example, not two. (Hint: Use the opposite ring R^{op}.

Example: The category of finite abelian groups is abelian. This is often useful as an example of an abelian category which is "too small" to have certain desirable properties.

Exercise: Let R be a left Noetherian ring. Show that the category of finitely generated left R-modules is Noetherian.

Remark: In commutative algebra and algebraic geometry one does want to do homological algebra on a category of modules with a suitable finiteness condition. When the ring R is not left-Noetherian, the condition of finite generation is too weak. A left R-module M is **finitely presented** if for some $n \in \mathbb{N}$ there is a surjection $R^n \to M$ with finitely generated kernel. (It then turns out that every such surjection has finitely generated kernel: [CA, Prop. 3.6].) Finally, a left R-module is **coherent** if it is finitely generated and every finitely generated submodule is finitely presented. Notice that when R is left-Noetherian the notions of finitely generated, finitely presented and coherent coincide.[9]

Theorem 5.1. *For any ring R, the category of coherent left R-modules is abelian.*

Example: The category of sheaves of abelian groups on a topological space X is abelian.

Example: For any locally ringed space $(X, \mathcal{O}_X)$, the category of sheaves of $\mathcal{O}_X$-modules on X is abelian. This is in fact a globalization of the commutative case of Example X.X.

Proposition 5.2. *For any abelian category $\mathcal{C}$, the category $C(\mathcal{C})$ of chain complexes in $\mathcal{C}$ is an abelian category.*

Exercise: Prove it.

5.2. **The Duality Principle.**

Proposition 5.3. *(Duality Principle) If $\mathcal{C}$ is an abelian category, so is $\mathcal{C}^{\mathrm{op}}$.*

Exercise: Prove it.

Exercise: True or false: left R-modules and right R-modules are dual categories.

The duality principle is highly useful, as it allows us to formalize the idea that two theorems and/or proofs are "the same" but one comes from the other by reversing all the arrows. Here are some examples of this.

Short exact sequences are self dual, as are split short exact sequences.

[9]All this rather technical stuff may explain to readers of Hartshorne's text why he only defines coherent modules over a Noetherian scheme, to the consternation of the hardcore EGA set.

The dual of a monic is an epic.

The dual of a kernel is a cokernel.

The dual of a projective object is an injective object. Indeed:

Proposition 5.4. *a) For an object P in any abelian category, TFAE:*
(ii) If $\pi : M \to N$ is an epimorphism and we have $\varphi : P \to N$, then there is $\Phi : P \to M$ such that $\varphi = \pi \circ \Phi$.
(iii) If $\pi : M \to N$ is an epimorphism, $\operatorname{Hom}(P, M) \to \operatorname{Hom}(P, N)$ *is surjective.*
(iv) The functor $\operatorname{Hom}(P, \cdot)$ *is exact.*
(v) Every short exact sequence $0 \to A \to B \to P \to 0$ splits.
An object satisfying these equivalent conditions is called ***projective****.*
b) For an object E in an abelian category, TFAE:
(ii') If $\iota : M \to N$ is a monomorphism and we have $\varphi : M \to E$, then there is $\Phi : N \to E$ such that $\varphi = \Phi \circ \iota$.
(iii') If $\iota : M \to N$ is a monomorphism, $\operatorname{Hom}(N, E) \to \operatorname{Hom}(N, M)$ *is surjective.*
(iv') The (contravariant) functor $\operatorname{Hom}(\cdot, E)$ *is exact.*
(v') Every short exact sequence $0 \to E \to B \to C \to 0$ splits.

Proof. a) The proofs that we gave of (ii) $\implies$ (iii) $\implies$ (iv) $\implies$ (v) go through verbatim in any abelian category. Hoewever, when working with modules we did not prove (v) $\implies$ (ii) directly but instead (v) $\implies$ (i): every projective module is a direct summand of a free module. The notion of *free module* **does not** have an analogue in an arbitrary abelian category – it is well worth thinking about this – so we need to replace this implication with a direct proof of (v) $\implies$ (ii). In a perhaps surprising development, we use (pairwise) pullbacks, which by Exercise X.X exist in any additive category with kernels hence in the abelian category $\mathcal{C}$. Let us write $K = \ker M \to N$ and $P \times_N M$ for the pullback of $M \to N$ and $P \to N$. By Exercise X.X, $\ker P \times_N M \to P = K$, and we get a ladder of short exact sequences

$$0 \to K \to P \times_N M \xrightarrow{\gamma} P \to 0,$$

$$0 \to K \to M \xrightarrow{\pi} N \to 0.$$

Let $\iota : P \to P \times_N M$ be a section of γ, and denote by π_1 the map $P \times_N M \to M$. Then $\Phi = \pi_1 \gamma : P \to M$ is such that $\varphi = \pi \circ \Phi$.
b) This follows immediately from part a) by the Duality Principle.[10] Note that if we wanted to prove it directly the only less than straightforward part is again $(\mathrm{v})'$ $\implies$ $(\mathrm{ii})'$. In the 8030 course Maren Turbow proved this using the fact that every module embeds in an injective module, which is of course a nontrivial theorem. It is *not true* that in an arbitrary abelian category every object can be embedded in an injective object, so we need to give a different proof here. The proof that we gave above dualizes to an argument involving pushouts. □

Exercise: Let $\mathcal{C}$ be the category of finite abelian groups – that is, the objects are finite abelian groups and the morphisms are group homomorphisms between them ("full subcategory").
a) Show that for $A \in \mathcal{C}$, the following are equivalent:
(i) A is projective.

[10] It is enlightening to check this carefully. Note in particular that the "surjective" in condition (iii) stays "surjective" in condition $(\mathrm{iii})'$!

(ii) A is injective.
(iii) $\# A = 1$.
(Warning: It is immediate from what we already know that no nontrivial finite abelian group is either projective or injective *in the category of abelian groups.* But the desired result does not follow immediately from this!)
b) Deduce that $\mathcal{C}$ has neither enough projectives nor enough injectives.

5.3. **Elements Regained.**

Theorem 5.5 (Freyd-Heron-Lubkin-Mitchell, 1964)**.** *A small abelian category admits a fully faithful functor to the category of abelian groups.*

Corollary 5.6. *It is permissible to "diagram chase" in an abelian category. In particular the results of* §4.6 *hold in any abelian category.*

5.4. **Limits in Abelian Categories.**

We have seen that any abelian category $\mathcal{A}$ has finite products, coproducts, equalizers and coequalizers. From this it follows that all finite limits and colimits exist in $\mathcal{A}$. We now push things further by considering colimits and limits over arbitrary (small!) diagrams.

Proposition 5.7. *Let $\mathcal{A}$ be an abelian category.*
a) The following are equivalent:
(i) Arbitrary coproducts exist in $\mathcal{A}$.
(ii) $\mathcal{A}$ is ***cocomplete****: every colimit exists.*
b) The following are equivalent:
(i) Arbitrary products exst in $\mathcal{A}$.
(ii) $\mathcal{A}$ is ***complete****: every limit exists.*

Proof. a) (i) $\implies$ (ii): Given $A : I \to \mathcal{A}$, the cokernel C of the map $\coprod_{\varphi : i \to j} \to \coprod_{i \in I}$ defined by sending the element which is a_i in the $\varphi : i \to j$ component and 0 in all other components to $\varphi(a_i) - a_i$ solves the universal mapping problem defining the colimit.
(ii) $\implies$ (i): This is immediate, since coproducts are a special kind of colimit.
b) This is immediate from the Duality Principle. □

Corollary 5.8. *For any ring R, the category of left (or of right) R-modules is complete and cocomplete.*

Exercise: Let $\mathcal{A}$ be a cocomplete abelian category. Show that the category $C(\mathcal{A})$ of chain complexes in $\mathcal{A}$ is cocomplete.

The following is an important theorem of pure category theory.

Theorem 5.9. *Let $(L : \mathcal{A} \to \mathcal{B}, R : \mathcal{B} \to \mathcal{A})$ be an adjoint pair.*[11] *Then:*
a) L preserves all colimits: if $A : I \to \mathcal{A}$ has a limit, so does $LA : I \to \mathcal{B}$ and

$$L(\operatorname{colim}_{i \in I} A_i) = \operatorname{colim}_{i \in I} L(A_i).$$

b) R preserves all limits: if $B : I \to \mathcal{B}$ has a limit, then so does $RB : I \to \mathcal{A}$ and

$$R(\lim_{i \in I} B_i) = \lim_{i \in I} R(B_i).$$

[11]Here $\mathcal{A}$ and $\mathcal{B}$ may be arbitrary categories.

Proof. See [CW]. □

Remark: One sometimes calls a functor which preserves all colimits **cocontinuous**. (Dually, a functor which preserves all limits is **continuous**.)

Corollary 5.10. *Let $\mathcal{A}$ be a cocomplete abelian category with enough projectives, and let $F : \mathcal{A} \to \mathcal{B}$ be a functor which is a left adjoint. (Recall that F must then be right exact.) Then all the derived functors preserve colimits: for all $n \geq 0$,*

$$L_nF(\bigoplus_{i \in I} A_i) \cong \bigoplus_{i \in I} L_nF(A_i).$$

Exercise: Prove Corollary 5.10. (Hint: if $\{P_{\bullet,i} \to A_i\}_{i \in I}$ are projective resolutions, then $\bigoplus_i P_\bullet \to \bigoplus_i A_i$ is a projective resolution.)

Corollary 5.11.

$$\operatorname{Tor}_*(A, \bigoplus_{i \in I} B_i) = \bigoplus_{i \in I} \operatorname{Tor}_*(A, B_i).$$

Proof. This is immediate from the two previous results: by the adjunction between tensor and hom, the functor $F(A) = A \otimes_R M$ is a left adjoint hence cocontinuous, and Corollary 5.10 applies. □

We would like to go further and show that the Tor functors commute with direct limits. On the other hand it is not true that the higher tor functors are cocontinuous, so there is some subtlety here. A key notion is that of a filtered category.

A category I is **filtered** if it satisfies both of the following:
(FC1) For all objects $x, y \in I$, there is an object $z \in I$ and maps $x \to z$, $y \to z$.
(FC2) For all morphisms $f, g : x \to y$, there is a morphism $h : y \to z$ with $hf = hg$.

Every partially ordered set X defines a category in which for all $x, y \in X$, there is a unique morphism from x to y if $x \leq y$ and no morphisms otherwise. Then the condition (FC1) becomes that of a **directed set** and condition (FC2) is vacuous.

Key Example: Consider a category with two objects x and y and a pair of morphisms between them. This satisfies (FC1) *but not* (FC2). It is this phenomenon which allows a functor which preserves filtered colimits not to be cocontinuous!

Lemma 5.12. *Let I be a small filtered category, and let A be a functor from I to the category of left R-modules. Then:*
a) Let $A = \operatorname{colim}_{i \in I} A_i$. Then every $a \in A$ is the image of some $a_i \in A_i$ under the natural map $A_i \to A$.
b) For all $i \in I$, the kernel of $A_i \to A$ is the union of the kernels of the maps $\varphi : A_i \to A_j$, where φ ranges over all arrows in I from i to j.

Exercise: Prove it.

Theorem 5.13. *Filtered colimits of R-modules are eaxct, considered as functors from $(R - Mod)^I$ to $R - Mod$.*

Proof. Step 1: The colimit functor is left adjoint to the diagonal functor $\Delta : R - Mod \to (R - Mod)^I$ given by $\Delta(A)_i = A$ for all $i \in I$. Therefore it is right exact. In fact this works in any cocomplete category.

Step 2: Let $\{t_i : A_i \to B_i\}_{i\in I}$ be a monomorphism in $(R-Mod)^I$. We need to show that the colimit of t is a monomorphism in $R-Mod$. Put $A = \operatorname{colim} A_i$, $B = \operatorname{colim} B_i$. We need to show that the induced map $t : A \to B$ is a monomorphism, so let $a \in A$ be such that $t(a) = 0$. By the preceding lemma, a is the image of a_i in some A_i. Since $t_i(a_i) \in B_i$ maps to zero in the colimit B, again by the preceding lemma there is some $\varphi : i \to j$ with

$$0 = \varphi(t_i(a_i)) = t_j(\varphi(a_i)) \in B_j,$$

and since t_j is a monomorphism this means $\varphi(a_i) = 0 \in A_j$ hence $a = 0$ in A. □

Remark: Note that in the last two results we worked in the category of R-modules. In fact the exactness of filtered colimits *does not hold* in every cocomplete abelian category. (Weibel gives as an exercise to show that it does not hold in the opposite category to the category of abelian groups.) In [T] Grothendieck explicitly considers the property of an abelian category that it is cocomplete and filtered colimits are exact: he calls in (AB5).

Exercise: Let $\mathcal{A}$ be a cocomplete abelian category. Show that the homology functors $H_n : C(\mathcal{A}) \to \mathcal{A}$ commute with filtered colimits.

Corollary 5.14. *Let $\mathcal{A}$ and $\mathcal{B}$ be (AB5) abelian categories, and suppose that $\mathcal{A}$ has enough projectives.*
a) For any left adjoint functor $F : \mathcal{A} \to \mathcal{B}$ and diagram $A : I \to \mathcal{A}$ with I filtered, for all $n \geq 0$, we have

$$L_nF(\operatorname{colim} A_i)) \cong \operatorname{colim} L_nF(A_i).$$

b) In particular, for every filtered $B : I \to \mathrm{Mod}_R$ and $A \in_R \mathrm{Mod}$, for all $n \geq 0$,

$$\mathrm{Tor}_n(A, \operatorname{colim} B_i) \cong \operatorname{colim} \mathrm{Tor}_n(A, B_i).$$

6. Tor and Ext

6.1. **Balancing Tor.**

We come now to a case where assuming our arbitrary ring R is commutative simplifies the proof of an important theorem which is valid more generally.

Theorem 6.1. *Let R be commutative. Then for all $A, B \in_R \mathrm{Mod}$ and all $n \geq 0$,*

$$\mathrm{Tor}_n^R(A, B) \cong \mathrm{Tor}_n^R(B, A).$$

Proof. Since R is commutative, we have an isomorphism $A \otimes_R B \cong B \otimes_R A$. So both $\mathrm{Tor}_*^R(A, B)$ and $\mathrm{Tor}_*^R(B, A)$ are universal δ-functors for $F : A \mapsto A \otimes_R B$. □

Theorem 6.2 (Balancing Tor)**.**

6.2. **More on Tor.**

We begin by revisiting a previous result.

Proposition 6.3. *Let $n \in \mathbb{Z}^+$. For any abelian group B, we have*

$$\mathrm{Tor}_0^{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, B) = B/nB,$$

$$\mathrm{Tor}_1^{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, B) = B[n],$$

$$\mathrm{Tor}_n^{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, B) = 0 \forall n \geq 2.$$

Proof. Since $0 \to \mathbb{Z} \stackrel{\cdot n}{\to} \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \to 0$ is a projective resolution of $\mathbb{Z}/n\mathbb{Z}$ as a $\mathbb{Z}$-module, $\mathrm{Tor}_*^{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, B)$ is the homology of the complex $0 \to B \stackrel{\cdot n}{\to} B \to 0$. □

Exercise: For finite abelian groups A, B, show $\mathrm{Tor}_1^{\mathbb{Z}}(A, B) \cong A \otimes_{\mathbb{Z}} B$.

Proposition 6.4. *For all abelian groups A and B,*
a) $\mathrm{Tor}_1^{\mathbb{Z}}(A, B)$ *is a torsion group.*
b) $\mathrm{Tor}_n^{\mathbb{Z}}(A, B) = 0$ *for all $n \geq 2$.*

Exercise: Prove Proposition 6.4.

Exercise: State and prove an analogue of Proposition XX for any PID R with fraction field K.

Proposition 6.5. *Let R be a domain with fraction field K. For any R-module B,*

$$\mathrm{Tor}_1^R(K/R, B) = B[\mathrm{tors}].$$

Exercise: Prove Proposition 6.5.

Proposition 6.6. *For finitely generated modules A, B over a Noetherian commutative ring R,* $\mathrm{Tor}_n(A, B)$ *is finitely generated for all $n \geq 0$.*

Exercise: Prove Proposition 6.6. (Hint: a finitely generated module over a Noetherian ring admits a resolution by finitely generated projective modules.)

Theorem 6.7 (Homological Criterion for Flatness)**.** *For a ring R and a left R-module B, the following are equivalent:*
(i) A is flat.
(ii) $\mathrm{Tor}_n^R(A, B) = 0$ *for all B and all $n > 0$.*
(iii) $\mathrm{Tor}_1^R(A, B) = 0$ *for all B.*

Proof. (i) $\implies$ (ii): Let $P_\bullet \to A \to 0$ be a projective resolution. Since B is flat, $P_\bullet \otimes_R A$ remains exact except at $P_0 \otimes A$, and thus for all $n > 0$, $H_n(P_\bullet \otimes A) = \mathrm{Tor}_n^R(A, B) = 0$.
(ii) $\implies$ (iii) is immediate.
(iii) $\implies$ (i): Let $0 \to M' \to M \to M'' \to 0$ be a short exact sequence of R-modules. The long exact homology sequence associated to the functor tensoring with A ends in

$$\mathrm{Tor}_1(A, M'') \to M' \otimes A \to M \otimes A \to M'' \otimes A \to 0,$$

and the result follows. □

Corollary 6.8. *Direct limits of flat modules are flat.*

Exercise: Prove Corollary 6.8.

Corollary 6.9. *The Tor functors can be computed using flat resolutions.*

Exercise: Prove Corollary 6.9.

Theorem 6.10. *Let R be a PID. For an R-module A, the following are equivalent:*
(i) A is flat.
(ii) A is torsionfree.
(iii) For all R-modules B, $\mathrm{Tor}_1^R(A, B) = 0$.

Proof. (i) $\implies$ (ii): We have already seen that this holds for modules over any integral domain.
(ii) $\implies$ (iii): Like any R-module, A is a colimit of its finitely generated submodules. Since R is a PID and A is torsionfree, A is a colimit of free modules. By swapping the arguments in Tor and applying Corollary 5.14, we deduce the result.
(iii) $\implies$ (i): We have already proved this in more generality. $\square$

Exercise: a) Let R be an integral domain with the following property: every submodule of a finitely generated free R-module is projective. Show that any torsionfree R-module is flat.
b) Show that a Dedekind domain satisfies the condition of part a) and thus torsionfree modules over a Dedekind domain are flat.
c) Show that the only integral domains satisfying the conditions of part a) are Dedekind domains.

Lemma 6.11. *Let R be a commutative ring, and let M, N be R-modules. For $r \in R$, let $\mu : M \to M$ be $x \mapsto rx$. Then for all n, the induced homomorphism μ^* on $\operatorname{Tor}_n(M,N)$ is multiplication by r.*

Exercise: a) Prove Lemma 6.11. (Suggestion: track multiplication by r through a projective resolution of M.
b) Suppose R is commutative and $r \in R$ is such that $rM = 0$, so that M is canonically an R/rR-module. Show that $\operatorname{Tor}^n(M,N)$ is an R/rR-module for all N.

Theorem 6.12 (Base Change for Tor)**.**
a) Let $R \to T$ be a ring homomorphism such that T is flat a left R-module. Then for all right R-modules M, all left T-modules N and all $n \geq 0$,

$$\operatorname{Tor}_n^T(M \otimes_R T, N) \cong \operatorname{Tor}_n^R(M,N) \cong \operatorname{Tor}_n^T(M, T \otimes_R N). \tag{6}$$

b) If R is commutative and T is a flat R-algebra, then for all R-modules M and N, the natural map

$$\operatorname{Tor}_*^R(M,N) \otimes_R T \to \operatorname{Tor}_*^T(M \otimes_R T, N \otimes_R T)$$

is an isomorphism.
c) For any multiplicative subset $S \subset R$ and all R-modules M, N, the natural map

$$\Phi : S^{-1} \operatorname{Tor}_*^R(M,N) \to \operatorname{Tor}_*^{S^{-1}R}(S^{-1}M, S^{-1}N)$$

is an isomorphism.

Proof.
a) Let $P_\bullet \to M$ be a projective resolution over R. Since T is flat over R, $P_\bullet \otimes_R T \to M \otimes_R T$ is a projective resolution over T. Using the Telescoping Tensor Identity,

$$\operatorname{Tor}_*^T(M \otimes_R T, N) \cong H_*((P_\bullet \otimes_R T) \otimes_T N) = H_*(P_\bullet \otimes_R N) = \operatorname{Tor}_*^R(M,N).$$

The second isomorphism is established in exactly the same way.
b) Applying part a) with the R-module $T \otimes_R N$ in place of N we get

$$\operatorname{Tor}_n^R(M, T \otimes_R N) \xrightarrow{\sim} \operatorname{Tor}_n^T(M \otimes_R T, T \otimes_R N) \cong \operatorname{Tor}_n^T(M \otimes_R T, N \otimes_R T).$$

Let $P_\bullet$ be a projective resolution for M over R. Since T is a flat R-module, $F = \cdot \otimes_R T$ is an exact functor and commutes with homology. Using Tensor Associativity, we get an isomorphism

$$\mathrm{Tor}_n^R(M,N)\otimes_R T = F(\mathrm{Tor}_n^R(M,N)) \cong F(H_n(P_\bullet \otimes_R N))$$
$$= H_n(F(P_\bullet \otimes_R N)) = H_n(P_\bullet \otimes_R (N \otimes_R T)) \cong \mathrm{Tor}_n^R(M, N\otimes_R T).$$

c) We need only apply Proposition X.X: $S^{-1}R$ is flat over R. ☐

Theorem 6.13. *Let R be a domain. Then for all R-modules M,N and all $n>0$, $\mathrm{Tor}_n^R(M,N)$ is a torsion R-module.*

Proof. Step 1: We make use of the fact that Tor commutes with localization (Theorem 6.12): for any multiplicatively closed subset $S \subset R$,

$$S^{-1}\,\mathrm{Tor}_n^R(M,N) = \mathrm{Tor}_n^{S^{-1}R}(S^{-1}M, S^{-1}N).$$

Step 2: Taking $S = R\setminus\{0\}$, we have $S^{-1}R = K$. Then for all $n>0$,

$$\mathrm{Tor}_n^R(M,N)\otimes_R K = \mathrm{Tor}_n^K(M\otimes_R K, N\otimes_R K) = 0.$$

Thus $\mathrm{Tor}_n^(M,N)$ lies in the kernel of $\otimes_R K$, which as we have already seen is precisely the torsion subgroup. ☐

Exercise: Let R be a ring, I a right ideal of R and J a left ideal of R. Show that

$$\mathrm{Tor}_1^R(R/I, R/J) \cong \frac{I\cap J}{IJ}.$$

Hint: apply the Snake Lemma to

$$0 \to IJ \to I \to I\otimes R/J \to 0$$
$$0 \to J \to R \to R\otimes R/J \to 0.$$

Example: Let k be a field and $R = k[x,y]$. Let $I = \langle x,y\rangle$ and view k as the R-module R/I. Then

$$0 \to R \to R^2 \to R \to k \to 0,$$

where $\alpha: f \mapsto (-yf, xf)$ and $\beta: (f,g)\mapsto xf+yg$ gives a projective resolution of k as an R-module. Using it we compute

$$\mathrm{Tor}_1^R(I,k) \cong \mathrm{Tor}_2^R(I,k) \cong k.$$

Thus I is a torsionfree but not flat, and we have a nonvanishing Tor_2.

6.3. Balancing Ext.

Theorem 6.14 (Balancing Ext)**.**

6.4. More on Ext.

Proposition 6.15. *a) For any family $\{M_i\}_{i\in I}$ of R-modules, any R-module N and all $n\geq 0$, there is a natural isomorphism*

$$\mathrm{Ext}^n(\bigoplus_{i\in I} M_i, N) = \prod_{i\in I}\mathrm{Ext}^n(M_i,N).$$

b) For any R-module M, any family $\{N_i\}_{i\in I}$ of R-modules and all $n\geq 0$, there is a natural isomorphism

$$\mathrm{Ext}^n(M, \prod_{i\in I} N_i) = \prod_{i\in I}\mathrm{Ext}^n(M,N_i).$$

Proof. We will give two proofs of part a) and then – to maintain balance in the force? – assign the analogous proof(s) of part b) as an exercice.

FIRST PROOF (WEIBEL) If $P_{\bullet,i}$ is a projective resolution of M_i for all $i \in I$, then $\bigoplus_{i\in I} P_{\bullet,i}$ is a projective resolution of $M = \bigoplus_{i\in I} M_i$. Now $\mathrm{Hom}(\bigoplus P_{\bullet,i}, N) = \prod_{i\in I} \mathrm{Hom}(P_{\bullet,i}, N)$, and the result follows.

SECOND PROOF (ROTMAN) The case $n = 0$ is an earlier seen property of Hom. We now suppose that $n > 0$, assume the result holds for $n-1$ and deduce it for n. For each $i \in I$, choose a short exact sequence

$$0 \to K_i \to P_i \to M_i \to 0$$

with P_i projective. Taking direct sums, we get

$$0 \to \bigoplus_{i\in I} K_i \to \bigoplus_{i\in I} P_i \to \bigoplus_{i\in I} M_i \to 0.$$

Case: $n = 1$. We have a commutative diagram with exact rows

$$\mathrm{Hom}(\bigoplus_i P_i, N) \to \mathrm{Hom}(\bigoplus_i L_i, N) \xrightarrow{\delta} \mathrm{Ext}^1(\bigoplus_i M_i, B) \to 0,$$

$$\prod_i \mathrm{Hom}(P_i, N) \to \prod_i \mathrm{Hom}(K_i, N) \xrightarrow{d} \prod \mathrm{Ext}^1(M_i, B) \to \prod_i \mathrm{Ext}^1(M_i, B) \to 0.$$

By Proposition 3.9 there is an isomorphism $\mathrm{Ext}^1(\bigoplus_i M_i, N) \xrightarrow{\sim} \prod_i \mathrm{Ext}^1(M_i, N)$.

Case: $n \geq 2$. We have a commutative diagram with exact rows

$$\mathrm{Ext}^{n-1}(\bigoplus_i P_i, N) \to \mathrm{Ext}^{n-1}(\bigoplus_i K_i, N) \xrightarrow{\delta} \mathrm{Ext}^n(\bigoplus_i M_i, N) \to 0$$

$$\prod_i \mathrm{Ext}^{n-1}(P_i, N) \to \prod_i \mathrm{Ext}^{n-1}(K_i, N) \xrightarrow{d} \prod_i \mathrm{Ext}^n(M_i, B) \to 0,$$

where $\sigma : \mathrm{Ext}^{n-1}(\bigoplus_i K_i, N) \to \prod_i \mathrm{Ext}^{n-1}(K_i, N)$ is the isomorphism given by the induction hypothesis. Thus

$$d\sigma\delta^{-1} : \mathrm{Ext}^n(\bigoplus_i M_i, N) \xrightarrow{\sim} \prod_i \mathrm{Ext}^n(M_i, N).$$

□

Proposition 6.16. *a) For any commutative group B, we have*

$$\mathrm{Ext}^1(\mathbb{Z}, B) = 0.$$

b) For any $n \in \mathbb{Z}^+$ and any commutative group B, we have

$$\mathrm{Ext}^1(\mathbb{Z}/n\mathbb{Z}, B) = B/nB.$$

Proof. Starting with the projective resolution

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

of $\mathbb{Z}/n\mathbb{Z}$ as a $\mathbb{Z}$-module, we get an exact sequence

$$\mathrm{Hom}(\mathbb{Z}, B) \xrightarrow{\alpha} \mathrm{Hom}(\mathbb{Z}, B) \to \mathrm{Ext}^1(\mathbb{Z}/n\mathbb{Z}, B) \to \mathrm{Ext}^1(\mathbb{Z}, N).$$

We have $\mathrm{Hom}(\mathbb{Z}, B) = B$, and the map α is multiplication by n. Since $\mathbb{Z}$ is a projective $\mathbb{Z}$-module, $\mathrm{Ext}^1(\mathbb{Z}, N) = 0$, so the exact sequence gives

$$\mathrm{Ext}^1(\mathbb{Z}/n\mathbb{Z}, B) \cong B/nB.$$

□

Exercise: Let M, N be finitely generated abelian groups. Compute $\operatorname{Ext}^1(M, N)$.

For a commutative group A, we put $A^* = \operatorname{Hom}(A, \mathbb{Q}/\mathbb{Z})$.

Proposition 6.17. *For any torsion commutative group A, $\operatorname{Ext}^1(A, \mathbb{Z}) = A^*$.*

Proof. Applying the right exact functor $\operatorname{Hom}(A, \cdot)$ to the short exact sequence

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

we get a long exact cohomology sequence, a portion of which is

$$\operatorname{Hom}(A, \mathbb{Q}) \to \operatorname{Hom}(A, \mathbb{Q}/\mathbb{Z}) \to \operatorname{Ext}^1(A, \mathbb{Z}) \to \operatorname{Ext}^1(A, \mathbb{Q}).$$

Since A is torsion and $\mathbb{Q}$ is torsionfree, $\operatorname{Hom}(A, \mathbb{Q}) = 0$, and since $\mathbb{Q}$ is injective, $\operatorname{Ext}^1(A, \mathbb{Q}) = 0$. $\square$

In particular, $\operatorname{Ext}^1(\mathbb{Q}/\mathbb{Z}, A) = \hat{\mathbb{Z}}$, $\operatorname{Ext}^1(\mathbb{Q}_p/\mathbb{Z}_p, A) = \mathbb{Z}_p$.

Exercise: Show that $\operatorname{Ext}^1(\mathbb{Z}[\frac{1}{p}], \mathbb{Z}) = \mathbb{Z}_p/\mathbb{Z} \neq 0$. Deduce that flat R-modules need not be acyclic for $\operatorname{Hom}_R(\cdot, B)$.
(Suggestion: use the short exact sequence $0 \to \mathbb{Z} \to \mathbb{Z}[\frac{1}{p}] \to \mathbb{Q}_p/\mathbb{Z}_p \to 0$.)

Exercise: Show that for any commutative group M and any positive integer n, $\operatorname{Ext}^1_{\mathbb{Z}}(M, \mathbb{Z}/n\mathbb{Z}) \cong M^*/nM^*$.

Lemma 6.18. *Let $R \to T$ be a ring map. Suppose that T is projective as a left R-module. Then any projective left T-module M is also projective as a left R-module.*

Exercise: Prove it.

Proposition 6.19. *(Base Change for Ext) Let $R \to T$ be a ring map.*
a) Suppose T is a flat right R-module. Let $M \in_R \operatorname{Mod}$, $N \in_T \operatorname{Mod}$. For $n \geq 0$,

$$\operatorname{Ext}^n_R(M, N) \cong \operatorname{Ext}^n_T(T \otimes_R M, N).$$

b) Suppose T is a projective left R-module. Let $M \in_T \operatorname{Mod}$, $N \in_R \operatorname{Mod}$. For $n \geq 0$,

$$\operatorname{Ext}^n_R(M, N) \cong \operatorname{Ext}^n_T(M, \operatorname{Hom}_R(T, N)).$$

Proof. a) Let $P_\bullet \to M$ be a projective resolution over R. Since T is flat over R, $T \otimes_R P_\bullet \to T \otimes_R M$ is a projective resolution of $T \otimes_R M$ over T. Using the Tensor-Hom Adjunction we compute

$$\operatorname{Ext}^n_T(T \otimes_R M, N) \cong H^n(\operatorname{Hom}_T(T \otimes_R P_\bullet, N)) \cong H^n(\operatorname{Hom}_R(P_\bullet, \operatorname{Hom}_T(T, N))$$
$$\cong H^n(\operatorname{Hom}_R(P_\bullet, N)) \cong \operatorname{Ext}^n_R(M, N).$$

b) Let $P_\bullet \to M$ be a projective resolution over T. Since T is projective over R, by Lemma 6.18 $P_\bullet \to M$ is also a projective resolution over R. Using the Telescoping Hom Identity we compute

$$\operatorname{Ext}^n_T(M, \operatorname{Hom}_R(T, N)) \cong H^n(\operatorname{Hom}_T(P_\bullet, \operatorname{Hom}_R(T, N)))$$
$$\cong H^n(\operatorname{Hom}_R(P_\bullet, N)) \cong \operatorname{Ext}^n_R(M, N).$$

$\square$

Lemma 6.20. *Let R be a commutative ring, and let M, N be R-modules. For $r \in R$, let $\mu : M \to M$ be $x \mapsto rx$, and let $\nu : N \to N$ be $x \mapsto rx$. Then for all n, the induced homomorphisms μ^* and ν_* on $\operatorname{Ext}^n(M, N)$ are multiplication by r.*

Exercise: a) Prove Lemma 6.20. (Suggestion: track multiplication by r through a projective (resp. injective) resolution of M (resp. N).)
b) Suppose R is commutative and $r \in R$ is such that $rM = 0$, so that M is canonically an R/rR-module. Show that $\operatorname{Ext}^n(M, N)$ is an R/rR-module for all N.
c) Let S be a multiplicatively closed subset of R, and let M be an $S^{-1}R$-module. Show that for all R-modules N and all $n \geq 0$, $\operatorname{Ext}^n(M, N)$ and $\operatorname{Ext}^n(N, M)$ are $S^{-1}R$-modules – i.e., multiplication by each $s \in S$ is invertible on them.

Our next order of business is to show that Ext functors commute with localization. This is fundamentally more delicate than the case of the Tor functors because – unlike the tensor product – it is not even unrestrictedly true that taking Hom's commutes with localization! So we proceed rather carefully.

Lemma 6.21. *Let $M \in_R \operatorname{Mod}$ be finitely presented, i.e., there is an exact sequence*

$$R^m \to R^n \to M \to 0.$$

Then for any central multiplicative subset $S \subset R$, the natural map

$$\Phi : S^{-1} \operatorname{Hom}_R(M, N) \to \operatorname{Hom}_{S^{-1}R}(S^{-1}R, S^{-1}N)$$

is an isomorphism.

Proof. Certainly Φ is an isomorphism when $M = R$; by additivity it is also an isomorphism when $M = R^n$. We finish by applying the Five Lemma to

$$0 \to S^{-1} \operatorname{Hom}_R(M, N) \to S^{-1} \operatorname{Hom}_R(R^n, N) \to S^{-1} \operatorname{Hom}_R(R^m, N)$$

$$\operatorname{Hom}(S^{-1}M, S^{-1}N) \to \operatorname{Hom}(S^{-1}R^n, S^{-1}N) \to \operatorname{Hom}(S^{-1}R^m, S^{-1}N) :$$

the last two vertical maps are isomorphisms, hence so is Φ. $\square$

Proposition 6.22. *Let R be a Noetherian commutative ring and $S \subset R$ a multiplicatively closed set. For every finitely generated R-module M, all R-modules N and all $n \geq 0$, the natural map*

$$\Phi : S^{-1} \operatorname{Ext}^n_R(M, N) \to \operatorname{Ext}^n_{S^{-1}R}(S^{-1}M, S^{-1}N)$$

is an isomorphism.

Proof. Since R is Noetherian and M is finitely generated, M admits a finite free resolution $F_\bullet \to M \to 0$. Since $S^{-1}R$ is a flat R-module, localization is an exact functor and thus $S^{-1}F_\bullet \to S^{-1}M \to 0$ is a finite free resolution over $S^{-1}R$. Because exact functor commute with co/homology and using Lemma 6.21, we get

$$S^{-1} \operatorname{Ext}^\bullet(M, N) = S^{-1}(H^\bullet \operatorname{Hom}_R(F_\bullet, N)) \cong H^\bullet S^{-1} \operatorname{Hom}_R(F_\bullet, N)$$

$$\cong H^\bullet \operatorname{Hom}_{S^{-1}R}(S^{-1}F_\bullet, S^{-1}N) = \operatorname{Ext}^\bullet_{S^{-1}R}(S^{-1}M, S^{-1}N).$$

$\square$

Theorem 6.23. *For left R-modules A, C, the following are equivalent:*
(i) Every short exact sequence

$$0 \to A \xrightarrow{i} B \xrightarrow{p} C \to 0 \tag{7}$$

splits.
(ii) $\operatorname{Ext}^1_R(C, A) = 0$.

Proof. At the moment we will prove (i) $\implies$ (ii) *only*. The other direction lies deeper and will be proved in the next section.

(i) $\implies$ (ii): We take the long exact cohomology sequence of the functor $\operatorname{Hom}(C, \cdot)$ applied to the short exact sequence (7), getting

$$\operatorname{Hom}(C, B) \stackrel{p\circ}{\to} \operatorname{Hom}(C, C) \to 0.$$

We get a homomorphism $\sigma : C \to B$ with $p \circ \sigma = 1_C$, so the sequence splits. $\square$

Application: We say that a commutative group A is **torsion split** if its torsion subgroup $A[\mathrm{tors}]$ is a direct summand.

Exercise: Show that a commutative group A is torsion split if:
(i) A is torsion.
(ii) A is torsionfree.
(iii) A is finitely generated.
(iv) $A[\mathrm{tors}]$ is divisible.
(v) $A/A[\mathrm{tors}]$ is free.

Theorem 6.24. *Let R be a Dedekind domain.*
a) If A is torsionfree, then for every R-module B, $\operatorname{Ext}^1(A, B)$ is divisible.
b) If A is torsionfree and $B = N[r]$ for some $r \in R^\bullet$, $\operatorname{Ext}^1(A, B) = 0$.
c) If $A[\mathrm{tors}] = A[r]$ for some $r \in R^\bullet$, then $A[\mathrm{tors}]$ is a direct summand of A.

Proof. a) Let $V = A \otimes_R K$. Since A is torsionfree, we have an exact sequence

$$0 \to A \to V \to V/A \to 0.$$

Applying the cofunctor $\operatorname{Hom}(\cdot, B)$, a portion of the long exact Ext sequence is

$$\operatorname{Ext}^1_R(V, B) \to \operatorname{Ext}^1_R(A, B) \to \operatorname{Ext}^2_R(V/A, B).$$

Since R is hereditary, submodules of projective modules are projective and thus $\operatorname{Ext}^2_R(A, B) = 0$,[12] so $\operatorname{Ext}^1_R(A, B)$ is a quotient of $\operatorname{Ext}^1_R(V, B)$. Since V is a K-module, so is $\operatorname{Ext}^1_R(V, B)$ and thus $\operatorname{Ext}^1_R(V, B)$ and its quotient $\operatorname{Ext}^1_R(A, B)$ is a divisible module, hence injective by Theorem 2.13.
b) Let $T = A[\mathrm{tors}] = A[r]$. We will show that the sequence

$$0 \to T \to A \to A/T \to 0$$

splits by computing $\operatorname{Ext}^1_R(A/T, T) = 0$. Since A/T is torsionfree, by part a), $\operatorname{Ext}^1_R(A/T, T)$ is divisible. On the other hand, since $T = T[r]$, by Exercise X.X, $\operatorname{Ext}^1_R(A/T, T) = \operatorname{Ext}^1_R(A/T, T)[r]$. Thus multiplication by r on $\operatorname{Ext}^1_R(A/T, T)$ is on the one hand surjective and on the other hand identically zero, so $\operatorname{Ext}^1_R(A/T, T) = 0$. By Theorem 6.23 the sequence splits. $\square$

Proposition 6.25. *There is a commutative group with torsion subgroup $T = \bigoplus_p \mathbb{Z}/p\mathbb{Z}$ which is not torsion split.*

Proof. Step 1: We claim that it is enough to show that $\operatorname{Ext}^1(\mathbb{Q}, T) \neq 0$. Indeed, if so, then there is a nonsplit extension

$$0 \to T \to A \to \mathbb{Q} \to 0.$$

[12] This is explored in more detail in § 7.2 below.

Since T is torsion and $\mathbb{Q}$ is torsionfree, $T = A[\text{tors}]$.
Step 2: Put $M = \prod_p \mathbb{Z}/p\mathbb{Z}$. Then we have a short exact sequence

$$0 \to T \to M \to D \to 0,$$

where $D = M/T$. Note that D is torsionfree, divisible and nonzero, hence is a nontrivial $\mathbb{Q}$-vector space. Using the short exact sequence

$$0 \to \bigoplus_p \mathbb{Z}/p\mathbb{Z} \to \prod_p \mathbb{Z}/p\mathbb{Z} \to D \to 0,$$

we get

$$\operatorname{Hom}(\mathbb{Q}, \prod_p \mathbb{Z}/p\mathbb{Z}) \to \operatorname{Hom}(\mathbb{Q}, D) \to \operatorname{Ext}^1(\mathbb{Q}, T) \to \operatorname{Ext}^1(\mathbb{Q}, \prod_p \mathbb{Z}/p\mathbb{Z}).$$

Now $\operatorname{Hom}(\mathbb{Q}, \prod_p \mathbb{Z}/p\mathbb{Z}) = \prod_p \operatorname{Hom}(\mathbb{Q}, \mathbb{Z}/p\mathbb{Z}) = 0$ and similarly $\operatorname{Ext}^1(\mathbb{Q}, \prod_p \mathbb{Z}/p\mathbb{Z}) = \prod_p \operatorname{Ext}^1(\mathbb{Q}, \mathbb{Z}/p\mathbb{Z}) = 0$, so

$$\operatorname{Hom}(\mathbb{Q}, D) \cong \operatorname{Ext}^1(\mathbb{Q}, T).$$

By the above remarks about D, this shows $\operatorname{Ext}^1(\mathbb{Q}, T) \neq 0$. (In fact it is easy to see that it is uncountably infinite!) □

Exercise:
a) Check that $\prod_p \mathbb{Z}/p\mathbb{Z} / \bigoplus_p \mathbb{Z}/p\mathbb{Z}$ is torsionfree, divisible and of cardinality $2^{\aleph_0}$.
b) Show that $\prod_p \mathbb{Z}/p\mathbb{Z}$ contains no nonzero divisible submodule, and deduce that the exact sequence

$$0 \to \bigoplus_p \mathbb{Z}/p\mathbb{Z} \to \prod_p \mathbb{Z}/p\mathbb{Z} \to D \to 0$$

is nonsplit and thus $\prod_p \mathbb{Z}/p\mathbb{Z}$ is not torsionsplit.

Theorem 6.26. *(Wiegold* [Wi69]*)* $\operatorname{Ext}^1(\mathbb{Q}, \mathbb{Z}) \cong (\mathbb{R}, +)$.

Proof. A (new?) proof is sketched in the following exercise. □

Exercise: We will show that $\operatorname{Ext}^1(\mathbb{Q}, \mathbb{Z}) \cong (\mathbb{R}, +)$.
a) Recall that for any commutative group G, $\operatorname{Ext}^1(\mathbb{Q}, G)$ is a $\mathbb{Q}$-vector space, and thus it remains to determine its dimension. Show that the claimed result is equivalent to $\# \operatorname{Ext}^1(\mathbb{Q}, \mathbb{Z}) = 2^{\aleph_0}$.
b) Apply the functor $\operatorname{Hom}(\cdot, \mathbb{Z})$ to the short exact sequence

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

to get

$$0 \to \mathbb{Z} \to \operatorname{Ext}^1(\mathbb{Q}/\mathbb{Z}, \mathbb{Z}) \to \operatorname{Ext}^1(\mathbb{Q}, \mathbb{Z}) \to 0.$$

Deduce that it suffices to show $\# \operatorname{Ext}^1(\mathbb{Q}/\mathbb{Z}, \mathbb{Z}) = 2^{\aleph_0}$.
c) Compute $\operatorname{Ext}^1(\mathbb{Q}/\mathbb{Z}, \mathbb{Z})$ using Proposition 6.17.

Exercise: A torsion abelian group T has **Property B** if for all abelian groups A, if $A[\text{tors}] \cong T$, then A is torsion split.
a) Show that if $T \cong B \oplus D$ with B bounded – i.e., $B = B[n]$ for some $n \in \mathbb{Z}^+$ – and D divisible, then T has property B.
c)$**$ (Baer [Bae36]) Show: if T has Property B, then $T \cong B \oplus D$ with B bounded and D divisible.

6.5. **Ext and Extensions.**

Our goal in this section is to show that $\mathrm{Ext}^1(M, N)$ parameterizes the set of *extensions* of N by M. In particular this will complete the proof of Theorem 6.23.

Let A and B be left R-modules. An **extension of B by A** is a short exact sequence

$$0 \to A \to X \to B \to 0.$$

(Note the order of A and B. This terminology is rather confusing at first, but it is quite standard, though unfortunately not strictly universal.) There is always at least one extension of B by A, namely the split extension

$$0 \to A \to A \oplus B \to B \to 0. \tag{8}$$

Previously we have worked with the dichotomy split/nonsplit for extensions, but now we want to go further and study the set of all extensions of B by A, up to a natural equivalence relation. Namely, we say that two extensions

$$0 \to A \to X \to B \to 0,$$

$$0 \to A \to X' \to B \to 0$$

are **equivalent** if there is a morphism $\alpha : X \to X'$ making the diagram

$$0 \to A \to X \to B \to 0$$

$$0 \to A \to X' \to B \to 0$$

commute. By the Five Lemma, such an α is necessarily an isomorphism. Note that this notion of equivalence is very natural, since one of our enunciations of what it means for a short exact sequence to split was that it be equivalent to one of the form (8). Let us take $\mathcal{E}(B, A)$ to be the set of equivalence classes of extensions of B by A.

Example: If $R = \mathbb{Z}$ we claim that the set $\mathcal{E}(\mathbb{Z}/p\mathbb{Z}, \mathbb{Z}/p\mathbb{Z})$ has precisely p elements. Indeed, if we have a short exact sequence

$$0 \to \mathbb{Z}/p\mathbb{Z} \to X \to \mathbb{Z}/p\mathbb{Z} \to 0$$

then X is a commutative group of order p^2, hence it is isomorphic to either $\mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}$ or to $\mathbb{Z}/p^2\mathbb{Z}$. In the first case we have indeed a short exact sequence of $\mathbb{Z}/p\mathbb{Z}$-vector spaces, so it certainly splits and thus there is exactly one equivalence class of extension with $X \cong \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}$. Now suppose $X \cong \mathbb{Z}/p^2\mathbb{Z}$. To give a surjective homomorphism $\mathbb{Z}/p^2\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ we need to – and may – send the generator 1 to any nonzero element of $\mathbb{Z}/p\mathbb{Z}$, so there are $p-1$ choices. We ask the reader to check that these $p-1$ extensions are pairwise inequivalent, *despite the fact* that the middle modules are the same for all of them.

Exercise: Complete the calculations necessary to show that $\#\mathcal{E}(\mathbb{Z}/p\mathbb{Z}, \mathbb{Z}/p\mathbb{Z}) = p$.

This example has an important moral: given two extensions of B by A, if they are isomorphic then $X \cong X'$, but the converse need not hold!

With respect to the above example, notice that $\mathrm{Ext}^1(\mathbb{Z}/p\mathbb{Z}, \mathbb{Z}/p\mathbb{Z}) = \mathbb{Z}/p\mathbb{Z}$, so

$\#\operatorname{Ext}^1(\mathbb{Z}/p\mathbb{Z},\mathbb{Z}/p\mathbb{Z}) = \#\mathcal{E}(\mathbb{Z}/p\mathbb{Z},\mathbb{Z}/p\mathbb{Z})$. We are about to vastly generalize this observation: for any left R-modules A, B, we will give a canonical isomorphism

$$\Phi : \mathcal{E}(B,A) \xrightarrow{\sim} \operatorname{Ext}^1(B,A).$$

Note that this certainly gives a proof of Theorem 6.23.

The definition of Φ is quite natural: suppose we have

$$\xi : 0 \to A \to X \to B \to 0.$$

As we did before, we take the long exact cohomology sequence of the functor $\operatorname{Hom}(\cdot, A)$, getting

$$\operatorname{Hom}(A,A) \xrightarrow{\delta} \operatorname{Ext}^1(B,A).$$

We put

$$\Phi(\xi) := \delta(1_A).$$

Using the naturality of the δ-functor Ext, it is immediate that Φ depends only on the equivalence class of the extension.

Theorem 6.27. *The above map $\Phi : \mathcal{E}(B,A) \to \operatorname{Ext}^1(B,A)$ is a bijection.*

Proof. Step 1: Let $0 \to M \xrightarrow{j} P \to B \to 0$ be an exact sequence with P projective. Applying $\operatorname{Hom}(\cdot, A)$ we get an exact sequence

$$\operatorname{Hom}(P,A) \to \operatorname{Hom}(M,A) \xrightarrow{\delta} \operatorname{Ext}^1(B,A) \to 0.$$

Let $x \in \operatorname{Ext}^1(B,A)$ and choose $\beta \in \operatorname{Hom}(M,A)$ with $\delta\beta = x$. Let X be the pushout of j and β, constructed concretely as follows: let $\alpha : M \to P \times A$ by $\alpha(x) = (j(x), -\beta(x))$, and put $X = (P \times A)/\beta(M)$. The natural surjection $P \times A \to P \to B$ induces a surjective map $X \to B$ with kernel A, and thus we have a diagram

$$0 \to M \xrightarrow{j} P \to B \to 0$$

$$\xi : 0 \to A \xrightarrow{i} X \to B \to 0.$$

Taking $\operatorname{Ext}^*(\cdot, A)$ we get a commutative diagram

$$\operatorname{Hom}(A,A) \xrightarrow{\delta} \operatorname{Ext}^1(B,A)$$

$$\operatorname{Hom}(M,A) \xrightarrow{\delta} \operatorname{Ext}^1(B,A)$$

which shows that $\delta(1_A) = x$.
Step 2: We claim that in fact the above construction gives a well-defined map $\Psi : \mathcal{E}(B,A) \to \operatorname{Ext}^1(B,A)$. Indeed, if $\beta' \in \operatorname{Hom}(M,A)$ is another lift of x, then there is $f \in \operatorname{Hom}(P,A)$ with

$$\beta' = \beta + fj.$$

If X' is the pushout of j and β', then the maps $i : A \to X$ and $\sigma + i : P \to X$ induce an isomorphism $X \to X'$ and an equivalence between σ and σ'. (Exercise!)
Step 3: Given an extension ξ of B by A, the projective lifting property gives us a commutative diagram

$$0 \to M \xrightarrow{j} P \to B \to 0$$

$$0 \to B \xrightarrow{i} X \to B \to 0.$$

Then X is the pushout of j and $\gamma : M \to A$. (Exercise!) Hence $\Psi(\Phi(\xi)) = \xi$ and Φ is injective. $\square$

There is a naturally defined addition law on $\mathcal{E}(A,B)$ with respect to which $\mathcal{E}(A,B)$ becomes a commutative group and Φ becomes an isomorphism of groups, the **Baer sum** of extensions. Given

$$\xi : 0 \to A \to X \to B \to 0,$$
$$\xi' : 0 \to A \to X' \to B \to 0,$$

let P be the fiber product of $f : X \to B$ and $g : X' \to B$. Then P is nearly an extension of B by A but it is slightly too large in that it contains two independent copies of A: indeed, using the standard concrete construction $P = \{(x,x') \in X \times X' \mid f(x) = g(x)\}$ we see that $A \times A \subset P$ and in fact $P/(A \times A) \cong B$. Let $\mathcal{S} = \{(a,-a) \mid a \in A\}$; this is a third, **antidiagonal** copy of A sitting inside P. Put $X'' = P/\mathcal{S}$ and let $q : P \to X''$ be the quotient map. Then $q : A \times \{0\} \stackrel{\sim}{\to} q(A \times \{0\}) = q(\{0\} \times A) \stackrel{\sim}{\leftarrow} \{0\} \times A$. Denoting this common copy of A in X'' simply by A, we then have an exact sequence

$$\xi'' : 0 \to A \to X'' \to B \to 0$$

and we put $\xi'' = \xi + \xi'$.

Theorem 6.28. *The Baer sum makes $\mathcal{E}(B,A)$ into a commutative goup and the map $\Phi : \mathcal{E}(B,A) \to \operatorname{Ext}^1(B,A)$ into a group isomorphism.*

Proof. Since Φ is a bijection and $\operatorname{Ext}^1(B,A)$ is a commutative group, it is enough to show that $\Phi(\xi + \xi') = \Phi(\xi) + \Phi(\xi')$. ... □

Exercise: One can certainly show directly that $(\mathcal{E}(B,A),+)$ is a commutative group, but some of the verifications required (e.g. the associativity) are unrewardingly tedious. But what is the inverse in $\mathcal{E}(B,A)$ of an extension $\xi : 0 \to A \to X \to B \to 0$? Give it explicitly.

6.6. **The Universal Coefficient Theorems.**

Theorem 6.29 (Künneth Formula)**.** *Let $P_\bullet$ be a chain complex of flat right R-modules such that for all n $d(P_n)$ is also flat. Then for all $n \in \mathbb{Z}$ and all left R-modules M, there is an exact sequence*

$$0 \to H_n(P_\bullet) \otimes_R M \to H_n(P_\bullet \otimes_R M) \to \operatorname{Tor}_1^R(H_{n-1}(P_\bullet), M) \to 0.$$

Proof. Step 1: Consider the short exact sequence

$$0 \to Z_n \to P_n \to d(P_n) \to 0.$$

Since P_n and $d(P_n)$ are assumed flat, the long exact Tor sequence shows that Z_n is also flat. Therefore

$$0 \to dP_n \to Z_n \to H_{n-1}(P_\bullet) \to 0$$

is a flat resolution of $H_{n-1}(P_\bullet)$, so that $\operatorname{Tor}_*^R(H_{n-1}(P_\bullet), M)$ is the homology of the complex

$$0 \to dP_n \otimes M \to Z_n \otimes M \to H_{n-1}P_\bullet \otimes M \to 0$$

and in particular

$$\operatorname{Tor}_1^R(H_{n-1}(P_\bullet), M) \cong \operatorname{Ker}(\mathfrak{d} : dP_n \otimes M \to Z_{n-1} \otimes M).$$

Step 2: Since dP_n is flat, we have $\operatorname{Tor}_1^R(dP_n, M) = 0$ for all n, and thus the complexes

$$0 \to Z_n \otimes M \to P_n \otimes M \to dP_n \otimes M \to 0$$

are all exact. They compile to give a short exact sequence of chain complexes, in which the differentials in $Z_\bullet$ and $dP_\bullet$ are all zero. The long exact homology sequence is

$$H_{n+1}(dP_\bullet \otimes M) \to H_n(Z_\bullet \otimes M) \to H_n(P_\bullet \otimes M) \xrightarrow{\alpha} H_n(dP_\bullet \otimes M) \xrightarrow{\delta} H_{n-1}(Z_\bullet \otimes M)$$

We have

$$H_{n-1}(Z_\bullet \otimes M) \cong Z_{n-1} \otimes M,$$
$$H_n(dP_\bullet \otimes M) \cong dP_n \otimes M,$$
$$\delta = \mathfrak{d},$$

and thus

$$dP_{n+1} \otimes M \xrightarrow{\delta \otimes 1} Z_n \otimes M \to H_n(P_\bullet \otimes M) \xrightarrow{\alpha} dP_n \otimes M \xrightarrow{\mathfrak{d}} Z_{n-1} \otimes M.$$

Therefore

$$\mathrm{Tor}_1^R(H_{n-1}(P_\bullet), M) \cong \mathrm{Ker}(\mathfrak{d}) \cong \mathrm{Image}\, \alpha \cong H_n(P_\bullet \otimes M)/H_n P_\bullet \otimes M.$$

□

Remark: The (only?) evident way to ensure the hypothesis that $d(P_n)$ is flat is to assume that R is a ring in which a submodule of a flat module is flat. Among domains these are precisely the Prüfer domains; in particular, among Noetherian domains these are precisely the Dedekind domains. In fact in the applications to algebraic topology we will have $R = \mathbb{Z}$.

Exercise (John Doyle): The above result and its proof is not really about tensor products and tor functors at all but rather a useful characterization of the difference between $F(H_n(P_\bullet))$ and $H_n(FP_\bullet)$ under certain conditions. Namely:
a) Let $F : \mathcal{A} \to \mathcal{B}$ be a right exact functor between abelian categories with enough projectives, and let $P_\bullet$ be a chain complex in $\mathcal{A}$ such that for all n both P_n and dP_n are F-ayclic. Then, for all $n \in \mathbb{Z}$, there is an exact sequence

$$0 \to H_n(F(P_\bullet)) \to F(H_n(P_\bullet)) \to L_1F(H_n(P_\bullet)) \to 0.$$

b) Deduce from part a) another proof that exact functors commute with homology.
c) Find another application of the result of part a).

There is also a more general Kunneth Formula in which the left R-module M is replaced by a chain complex. Most of the additional content of this resides in the definition of a tensor product of a chain complex $P_\bullet$ of right R-modules with a chain complex $Q_\bullet$ of left R-modules: by definition,

$$(P_\bullet \otimes_R Q_\bullet)_n = \bigoplus_{p+q=n} P_p \otimes_R Q_q,$$

and the differential is given by

$$d(a \otimes_R b) = (da) \otimes_R b + (-1)^p a \otimes_R (db)$$

for $a \in P_p$, $b \in Q_q$.

Theorem 6.30. *(Künneth for Complexes) Let $P_\bullet$ be a chain complex of right R-modules such that P_n and dP_n is flat for all n. Let $Q_\bullet$ be a chain complex of left R-modules. Then for all n there is an exact sequence*

$$0 \to \bigoplus_{p+q=n} H_p(P) \otimes_R H_q(Q) \to H_n(P_\bullet \otimes_R Q_\bullet) \to \bigoplus_{p+q=n-1} \operatorname{Tor}_1^R(H_p(P_\bullet), H_q(Q_\bullet)) \to 0.$$

Moreover, if R is a hereditary ring and $P_\bullet$ is a chain complex of projective R-modules, then the above exact sequence splits.

Exercise: Prove it. (Suggestions: [H, pp. 274-275] contains a nice treatment under the slightly stronger hypothesis that P_n and dP_n is projective for all n. This is used only to ensure that tensoring the complex $0 \to Z_\bullet \to P_\bullet \to dP_\bullet \to 0$ with $Q_\bullet$ yields a short exact sequence of chain complexes. But this can be shown in a different way: by first showing that for a complex $Q_\bullet$, tensoring any short exact sequence of complexes with $Q_\bullet$ yields a short exact sequence of complexes iff each Q_n is flat.)

Theorem 6.31 (Universal Coefficient Theorem in Homology)**.** *Let $P_\bullet$ be a chain complex of free abelian groups. Then for all n and all abelian groups M, we have*

$$H_n((P_\bullet \otimes M)) \cong (H_n(P_\bullet) \otimes M) \bigoplus \operatorname{Tor}_1^{\mathbb{Z}}(H_{n-1}(P_\bullet), M).$$

Proof. Since every subgroup of a free abelian group is free, dP_n is free abelian group for all n, and we get

$$P_n \cong Z_n \oplus dP_n.$$

Tensoring with M gives that $Z_n \otimes M$ is a direct summand of $P_n \otimes M$; it must also then be a direct summand of the intermediate group

$$K = \ker d_n \otimes 1 : P_n \otimes M \to P_{n-1} \otimes M :$$

that is, there is an abelian group B such that

$$(Z_n \otimes M) \oplus B \cong K.$$

Let K' be the image of $d_{n+1} \otimes 1$ in $P_n \otimes M$. Then $K' \subset K$ and $K' \subset Z_n \otimes M$, so

$$H_n(P_\bullet \otimes M) \cong K/K' \cong (Z_n \otimes M)/K' \oplus B \cong (H_n(P_\bullet) \otimes M) \oplus B.$$

Thus $H_n(P_\bullet) \otimes M$ is a direct summand of $H_n(P_\bullet \otimes M)$. By the Künneth Formula the complementary direct summand must be $\operatorname{Tor}_1^{\mathbb{Z}}(H_{n-1}(P_\bullet), M)$. □

Exercise: Let X be a topological space. Apply Theorem 6.31 to the singular complex $S_\bullet(X)$ to get the usual Universal Coefficient Theorem from algebraic topology.

Theorem 6.32 (Universal Coefficient Theorem for Cohomology)**.** *Let $P_\bullet$ be a chain complex of projective left R-modules such that each dP_n is projective. Then for all $n \in \mathbb{Z}$ and all R-modules M we have a* ***split exact sequence***

$$0 \to \operatorname{Ext}_R^1(H_{n-1}(P_\bullet), M) \to H^n(\operatorname{Hom}_R(P_\bullet, M)) \to \operatorname{Hom}_R(H_n(P_\bullet), M) \to 0.$$

Exercise: Prove Theorem 6.32. (Suggestion: adapt the proof of the Künneth Formula to give the existence of the short exact sequence, then adapt the proof of Theorem 6.31 to show that it is split.)

Exercise: State and prove the Universal Coefficient Theorem for singular cohomology of a topological space.

Exercise: Verify that all the results of this section work in the context of complexes $P_\bullet$ of projective left R-modules over any left hereditary ring.

7. Homological Dimension Theory

7.1. Syzygies, Cosyzygies, Dimension Shifting.

For an object M of an abelian category $\mathcal{A}$, let

$$\ldots \xrightarrow{d_{n+1}} T_n \xrightarrow{d_n} \ldots \xrightarrow{d_1} T_0 \xrightarrow{d_0} M \to 0$$

be a left resolution. Let $K_n = \ker d_n$; we call this the **nth syzygy** of the resolution.

Dually, if we have a right resolution

$$0 \to M \to T^\bullet$$

then we call $C_n = \operatorname{coker} d^n$ the **nth cosyzygy**.

The reader should stop for a moment and recall that syzygies were used to construct projective resolutions (and cosyzygies to construct injective resolutions), so the idea that they carry some important data in their own right should perhaps not be entirely surprising. On the other hand, the mind rebels against this a bit because of the apparent lack of canonicity of syzygies. Is there any sense in which the syzygies K_n of M are invariants of M and not just a chosen resolution?

Indeed there is. To get at this, we need one further (fairly natural) notion.

Two objects M and N are **projectively equivalent** if there are projective modules P_1 and P_2 such that $M \oplus P_1 \cong N \oplus P_2$. This is (clearly) an equivalence relation. Dually, M and N are **injectively equivalent** if there are injectives E_1 and E_2 such that $M \oplus E_1 \cong N \oplus E_2$.

Exercise: a) Show: M is projectively equivalent to 0 iff it is projective.
b) Show: M is injectively equivalent to 0 iff it is injective.

Lemma 7.1. *Let A, B be objects in an abelian category $\mathcal{A}$.*
a) If A and B are projectively equivalent, then for any right exact functor F and all $n > 0$, $L_n(A) \cong L_n(B)$.
b) If A and B are injectively equivalent, then or any left exact functor F and all $n > 0$, $R^n(A) \cong R^n(B)$.
c) If A and B are projectively equivalent, then for any epimonic cofunctor F and all $n > 0$, $R^n(A) \cong R^n(B)$.

Exercise: Prove Lemma 7.1.

Theorem 7.2 (Schanuel's Lemma)**.** *Let M be an object in an abelian category $\mathcal{A}$.*
a) Suppose we have two short exact sequences

$$0 \to K \to P \to M \to 0,$$

$$0 \to K' \to P' \to M \to 0,$$

with P and P' projective. Then

$$K \oplus P' \cong K' \oplus P.$$

b) More generally, suppose we have two exact sequences

$$0 \to K \to P_n \to P_{n-1} \to \ldots \to P_0 \to M \to 0,$$

$$0 \to K' \to P'_n \to P'_{n-1} \to \ldots \to P'_0 \to M \to 0.$$

Then

$$K \oplus P'_n \oplus P_{n-1} \oplus \ldots \cong K' \oplus P_n \oplus P'_{n-1} \oplus \ldots.$$

In particular, K and K' are projectively equivalent.

Proof. a) Let Q be the fiber product of $P \to M$, $P' \to M$. Consider the diagram

$$K' \xrightarrow{1} K'$$

$$0 \to K \to Q \to P' \to 0.$$

$$0 \to K \to P \to M \to 0.$$

In particular we have short exact sequences

$$0 \to K' \to Q \to P \to 0,$$

$$0 \to K \to Q \to P' \to 0.$$

Since P and P' are projective, both of these sequences split and thus

$$K' \oplus P \cong Q \cong K \oplus P'.$$

b) We leave this to the reader as an exercise. □

Exercise: Prove part b) of Theorem 7.2. (Hints: go by induction on n. Use the fact that if $0 \to A \to B \to C \to 0$ is an exact sequence then so is $0 \to A \to B \oplus D \to C \oplus D \to 0$.)

Exercise: State and prove a version of Schanuel's Lemma for injectives.

Exercise: Show that part a) of Schanuel's Lemma *need not hold* for flat resolutions. (Suggestion: compare the flat resolution $0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$ to any projective resolution.)

Corollary 7.3. *Let M be an object in an abelian category $\mathcal{A}$.*
a) If $\mathcal{A}$ has enough projectives, then the syzygies K_n of M are well-defined independent of the projective resolution, up to projective equivalence. It follows that applying left derived functors (or right derived functors of epimonic cofunctors) to syzygies is well-defined.
b) If $\mathcal{A}$ has enough injectives, then the cosyzygies C_n of M are well-defined independent of the injective resolution, up to injective equivalence. It follows that applying right derived functors to cosyzygies is well-defined.

Theorem 7.4 (Dimension Shifting)**.** *a) Let M be an object of an abelian category $\mathcal{A}$ with enough projectives, and let $F : \mathcal{A} \to \mathcal{B}$ be a right exact functor. Then for all $n > 0$,*

$$L_n F(A) \cong L_1 F(K_{n-1}),$$

where K_{n-1} is the $n-1$st (projective) syzygy of M.
b) Dually...

Proof. We prove part a) only, as part b) follows by the Duality Principle. First we choose a projective resolution $P_\bullet$ of M.
Step 0: Consider

$$0 \to K_0 \to P_0 \to M \to 0$$

with P_0 projective. Since projectives are F-acyclic, we get

$$L_n(K_0) \to L_n(P_0) \to L_n(M) \xrightarrow{\delta} L_{n-1}(K_0) \ldots,$$

and every third object is zero, so the connecting maps give isomorphisms

$$L_{n+1}(M) \cong L_n(K_0).$$

Step 1: Since the image of $P_1 \to P_0$ is K_0, we have an exact sequence

$$0 \to K_1 \to P_1 \to K_0 \to 0.$$

Now arguing as above gives

$$L_n(K_0) \cong L_{n-1}(K_1).$$

Step 2: Proceeding inductively we finally get the desired result. □

Exercise: State and prove a version of dimension shifting for epimonic cofunctors.

Exercise: State and prove a version of dimension shifting for F-acyclic resolutions.

The following exercises develop an alternate take on syzygies and projective dimension which is sometimes useful.

Exercise: For $M, N \in_R$ Mod, we write $M \sim N$ is M and N are projectively equivalent, and denote by $[M]$ the projective equivalence class of M. Let $G(R)$ be the set of projective equivalence classes of left R-modules.
a) Show that if $M_1 \sim M_2$ and $N_1 \sim N_2$, then $M_1 \oplus N_1 \sim M_2 \oplus N_2$.
b) Deduce that $[M] + [N] = [M \oplus N]$ is a well-defined binary operation on $G(R)$ which endows it with the structure of a commutative monoid.
c) Show that the only invertible element of $G(R)$ is 0 (the equivalence class of projective modules).

Exercise: For a left R-module M, we define the **projective shift** $\mathcal{P}(M) \in G(R)$ to be the projective equivalence class of the zeroth projective syzygy of M: for any short exact sequence

$$0 \to K \to P \to M,$$

we put $\mathcal{P}(M) = [K]$.
a) Show that $\mathcal{P}(M)$ is well-defined.
b) Show that $\mathcal{P}(M)$ depends only on $[M]$, thus $\mathcal{P} : G(R) \to G(R)$ is well-defined.
c) Show that $\mathcal{P}$ is an endomorphism of the monoid $G(R)$.
d) Let $\{M_i\}_{i \in I}$ be a family of left R-modules. Show that $\mathbb{P} \bigoplus_{i \in I} M_i = [\bigoplus_{i \in I} \mathbb{P}(M_i)]$.
e) Show that for any $n \in \mathbb{Z}^+$, $\mathcal{P}^n(M) = [K_{n-1}]$, the projective equivalence class of the $(n-1)$st projective syzygy of M.
f) Show that $\mathrm{pd}(M)$ is the least $n \in \mathbb{N}$ such that $\mathcal{P}^n(M) = 0 \in G(R)$, or ∞ if no such n exists.

7.2. **Finite Free Resolutions and Serre's Theorem on Projective Modules.**

A left R-module M is **stably free** if there is a finitely generated free module F such that $M \oplus F$ is free.

Exercise: Show that free modules are stably free, and stably free modules are projective.

In his 1972 Brandeis thesis, M.R. Gabel showed that an infinitely generated stably free module is necessarily free. The rather short, elementary proof can be found in [CA, Thm. 6.10]: it was taken from a treatment of K. Conrad. So from now on let us agree to only consider finitely generated stably free modules.

Stably free modules are natural from the perspective of algebraic K-theory. Indeed (although this may be a thoroughly unhelpful remark) they are precisely the finitely generated modules with trivial image in the reduced K-group $\widetilde{K_0(R)}$. They are also an interesting intermediate point between projective modules and free modules.

Recall that in the early 1950's, in the midst of a foundational study of coherent sheaves on algebraic varieties, Serre asked the question of whether every finitely generated projective module P over a ring $R_n = k[t_1, \ldots, t_n]$ – where k is an arbitrary field – must be free. Since R_n is the ring of polynomial functions on affine n-space $\mathbb{A}^n$ (by definition!; don't be scared yet), the Serre-Swan theorem leads us to think of P as an **algebraic vector bundle** on $\mathbb{A}^n$. Suppose instead that we had an ordinary topological vector bundle on $\mathbb{R}^n$ or $\mathbb{C}^n$. Then because the category of vector bundles on a paracompact space depends only on the homotopy type of the space and $\mathbb{R}^n$ and $\mathbb{C}^n (\cong \mathbb{R}^{2n})$ are contractible, it is immediate that every vector bundle on such a space is trivial.

That was for **topological vector bundles**. One can ask the same question for **smooth vector bundles** – this means that we require the transition functions to be smooth – and then it is a simple exercise using smooth partitions of unity that again every smooth vector bundle on $\mathbb{R}^n$ or $\mathbb{C}^n$ (again, smoothly $\mathbb{C}^n \cong \mathbb{R}^{2n}$) is trivial. On $\mathbb{C}^n$ one can try once again with **holomorphic vector bundles** – now the transition functions are required to be holomorphic – and we get a question that is not completely trivial for the novice in complex geometry. But there is an elementary fact, c the **d-bar Poincare Lemma**, which again swiftly implies that holomorphic vector bundles on $\mathbb{C}^n$ are trivial.

Then finally we come to algebraic vector bundles, which means roughly that the transition functions (with respect to a trivializing open covering in the Zariski topology) are quotients of polynomials. Remarkably this makes the problem incredibly more difficult, and Serre was unable to prove the result – except of course in the trivial case $n = 1$, when $k[t]$ is a PID.

FAC was published in 1955. In 1958 Serre published a proof of the weaker result that every finitely generated projective module over $k[t_1, \ldots, t_n]$ is stably free. It was not until 1976 that D. Quillen and A. Suslin (independently) were able to replace stably free with "free". To give a sense of the scope of this achievement I mention that Quillen received the Fields Medal in 1978, in part for this work.

In the remainder of this section we will prove Serre's Theorem. It is in fact a remarkable showpiece of homological algebra: the key is to study *finite free resolutions* of modules, and the proof uses no more than quite straightforward results on such things together with one piece of formal magic which will be introduced later.

7.2.1. *FFR.*

Let M be a left R-module. A **finite free resolution (FFR)** of M is a projective resolution $P_\bullet \to M$ with three additional properties:
(I) Each P_i is free.
(II) Each P_i is finitely generated.
(III) The resolution has finite length: $P_n = 0$ for all sufficiently large n.

We well know that every module admits a projective resolution. In what way do the added conditions (I) through (III) impose restrictions on M, i.e., which modules M are FFR? Let's take them in turn.

• As we know, every module is a quotient of a free module, so every module admits a free resolution: condition (I) is no restriction on M whatsoever.

• Suppose M admits a resolution by finitely generated free modules. In particular M is a homomorphic image of the finitely generated module F_0 so is itself finitely generated. What about the converse? For every finitely generated module M there is a short exact sequence

$$0 \to K_0 \to F_0 \to M \to 0$$

with F_0 finitely generated free. Consider the kernel K_0: *if* it is finitely generated, then we can find a finitely generated free module F_1, a surjection $F_1 \to K_0$, and splice to get

$$0 \to K_1 \to F_1 \to F_0 \to M \to 0.$$

Similarly, *if* K_1 happens to be finitely generated, then we can write it as a homomorphic image of a free module, splice that in, and so forth. The point is that there are rings for which not every submodule of a finitely generated free module is finitely generated: indeed this condition is equivalent to R being left Noetherian. So we get:

Proposition 7.5. *For a module M over a left Noetherian ring M, the following are equivalent: (i) M admits a resolution by finitely generated free modules.*
(iii) M admits a resolution by finitely generated projective modules.
(iii) M is finitely generated.

Over an arbitrary ring R, we say that a module M is $\mathbf{FP}_n$ if there is an exact sequence

$$P_n \to \ldots P_0 \to M \to 0$$

with each P_i finitely generated projective. We say that M is $\mathbf{FP}_\infty$ if it is FP_n for all $n \in \mathbb{N}$.

Exercise: Let R be a ring and M a left R-module.

a) Show that M is FP_0 iff it is finitely generated.
b) Show that the following conditions are equivalent:
(i) M is FP_1.
(ii) M is **finitely presented**: there is an exact sequence

$$F_1 \to F_0 \to M \to 0$$

with each F_i finitely generated free.
(iii) For every surjection $\epsilon : P \to M$ with P finitely generated projective, $\ker(\epsilon)$ is finitely generated.
c) For any $n \geq 1$, show that the following conditions are equivalent:
(i) M is FP_n.
(ii) There is an exact sequence

$$F_n \to \dots F_0 \to M \to 0$$

with each F_i finitely generated free.
(iii) For every exact sequence $P_n \stackrel{d_n}{\to} \dots \to P_0 \to M \to 0$ with each P_i finitely generated projective, $\operatorname{Ker} d_n$ is finitely generated.
(Hint for parts b) and c): Schanuel's Lemma.)
d) The following conditions are equivalent:
(i) M admits a resolution by finitely generated free modules.
(ii) M admits a resolution by finitely generated projective modules.
(iii) M is FP_∞.

From now on we will be interested only in the Noetherian case, where as we have seen conditions (I) and (II) simply mean that M is finitely generated. We move now to the full FFR property, and we begin with the following innocent, but fundamental observation of Serre.

Lemma 7.6 (Serre's Lemma)**.** *For a finitely generated projective module P, TFAE:*
(i) P is stably free.
(ii) P is FFR.

Proof. (i) $\implies$ (ii): If there are finitely generated free modules F_0, F_1 with $P \oplus F_1 \cong F_0$, then projection of F_0 onto P gives a FFR $0 \to F_1 \to F_0 \to P \to 0$.
(ii) $\implies$ (i): We go by induction on the length of the FFR. If $n = 0$ then P is free. Suppose now that every finitely generated projective module with an FFR of length $n-1$ is stably free, and let

$$0 \to F_n \to \dots \to F_0 \to P \to 0$$

be an FFR of a finitely generated projective module P. Let $K_0 = \operatorname{Ker} F_0 \to P$. Since P is projective, $F_0 \cong K_0 \oplus P$. We are left with an exact sequence

$$0 \to F_n \to \dots \to F_1 \to K_0 \to 0,$$

which shows by induction that K_0 is stably free: $K_0 \oplus R^a \cong R^b$ for some $a, b \in \mathbb{N}$. Thus $R^a \oplus F_0 \cong (K_0 \oplus R^a) \oplus P \cong R^b \oplus P$ and P is stably free. $\square$

Lemma 7.7. *If a left R-module M admits a length n resolution by finitely generated stably free modules, then M admits an FFR of length $n+1$.*

Proof. By induction on n.
$n = 0$: Then M is stably free, so there are $a, b \in \mathbb{N}$ with $M \oplus R^a \cong R^b$ and we get a length 1 FFR

$$0 \to R^a \to R^n \to M \to 0.$$

We suppose that $n > 0$ and that the result holds for modules with a length $n - 1$ resolution by finitely generated stably free modules – henceforth we abbreviate this to FSFR. Let $P_\bullet \to M \to 0$ be a length n FSFR. Choose a finitely generated free module F such that $P_0 \oplus F$ is free. We have a modified resolution

$$0 \to P_n \to \dots P_2 \stackrel{d_1 \oplus 0}{\to} P_1 \oplus F \stackrel{d_1 \oplus 1}{\to} P_0 \oplus F \stackrel{\epsilon' = \epsilon \oplus 0}{\longrightarrow} M \to 0.$$

Then

$$0 \to P_n \to \dots \to P_2 \to P_1 \oplus F \to \operatorname{Ker} \epsilon' \to 0$$

is a FSFR of length $n - 1$, so by induction $\operatorname{Ker} \epsilon'$ has a FFR of length n. Splicing this FFR with $0 \to \operatorname{Ker} \epsilon' \to P_0 \oplus F \to M \to 0$ gives a FFR of length $n + 1$. $\square$

Exercise: Let M be a left module over a left Noetherian ring. Show: if M admits an FFR of length n, then for any resolution of M by finitely generated free modules, the nth syzygy is stably free.

Proposition 7.8. *Let R be a left Noetherian ring, and let $0 \to M' \to M \to M'' \to 0$ be a short exact sequence of left R-modules. If any two of M', M, M'' are FFR, so is the third.*

Proof. Since R is Noetherian, finitely generated modules are Noetherian. Any module admitting an FFR is Noetherian, so by hypothesis two out of the three of M', M, M'' are Noetherian, hence so is the third. Thus M' and M'' admit infinite length resolutions $F'_\bullet$ and $F''_\bullet$ by finitely generated free modules. By the Horseshoe Lemma we can fill in with a projective resolution $F_\bullet$ of M to get short exact sequences

$$0 \to F'_n \to F_n \to F''_n \to 0$$

for all n. Since F''_n is projective, this sequence splits, showing that F_n is finitely generated free. For each $n \in \mathbb{N}$, we get a short exact sequence of projective syzygies

$$0 \to K'_n \to K_n \to K''_n \to 0.$$

If some K_n is stably free, then

$$0 \to K_n \to F_n \to \dots \to F_0 \to M \to 0$$

is a FSFSR, so by Lemma 7.7 M is FFR, and the same holds for M' and M''.

Case 1: Suppose M', M'' admit FFRs of length n. By Schanuel's Lemma, K'_n and K''_n are stably free. In particular K''_n is projective, so $K_n \cong K'_n \oplus K''_n$ is stably free and M is FFR.
Case 2: Suppose M, M'' admit FFRs of length n. Let L be a finitely generated free module such that $K_n \oplus L$ is free, and let L'' be a finitely generated free module such that $K''_n \oplus L''$ is free, so

$$(K_n \oplus L) \oplus L'' \cong (K'_n \oplus L) \oplus (K''_n \oplus L'')$$

shows that K'_n is stably free.
Case 3: Suppose M', M admit FFRs of length n, so K'_n and K_n are stably free. Splice

$$0 \to K'_n \to K_n \to K''_n \to 0$$

to

$$0 \to K_n'' \to F_n'' \to \ldots \to F_0'' \to M'' \to 0$$

to get a FSFR of M'', and apply Lemma 7.7. $\square$

7.2.2. *Biternary Classes.*

Let $\mathcal{X}$ be a subclass of the class of all left R-modules. We say that $\mathcal{X}$ is **biternary**[13] if given a short exact sequence

$$0 \to M' \to M \to M'' \to 0$$

of left R-modules, if any two of M', M, M'' lie in $\mathcal{X}$, so too does the third.

Exercise: Determine which of the following properties of modules determine a biternary subclass of ${}_R\,\mathrm{Mod}$ for any ring R:
(i) finitely generated modules.
(ii) Noetherian modules.
(iii) Artinian modules.
(iv) finite length (= Noetherian + Artinian) modules.
(v) free modules.
(vi) stably free module.
(vii) projective modules.
(viii) flat modules.
(ix) torsionfree modules (over any domain).
(x) injective modules.
(xi) finite length modules.

Above we proved that for any left Noetherian ring, FFR is a biternary class. This turns out to be a key idea in the proof of Serre's Theorem. First we develop a very modest formalism concerning biternary classes.

Exercise: Let R be a ring. Show that any intersection of biternary subclasses of ${}_R\,\mathrm{Mod}$ is a biternary class.

From the exercise it follows that for any subclass $\mathcal{X} \subset_R \mathrm{Mod}$ there is a unique minimal biternary subclass containing it, namely the intersection of all biternary subclasses containing it. We denote this "biternary closure" by $\mathcal{F}(\mathcal{X})$. As usual, when we define a "generated object" by this kind of top-down approach, it is useful to supplement it with a more explicit bottom-up construction. In this case this is completely straightforward: for a subclass $\mathcal{X}$ of ${}_R\,\mathrm{Mod}$, we put $\mathcal{C}(\mathcal{X})$ be the class of all R-modules lying in a short exact sequence, the other two members of which lie in $\mathcal{C}$.

Exercise: Let $\mathcal{X} \subset \mathcal{Y} \subset_R \mathrm{Mod}$ be subclasses. Show:
a) We have $\mathcal{C}(X) \subset \mathcal{C}(Y)$.
b) We have $\mathcal{X} \subset \mathcal{C}(\mathcal{X})$.

[13]We have made this name up on the spot. It is meant to suggest "two out of three" and not to stick out like a sore thumb. Our solution may nor be ideal, but in our defense J. Rotman in [Rot] calls such a subclass a **family**, which is much worse.

c) We have $\mathcal{F}(\mathcal{X}) = \bigcup_{n=1}^{\infty} \mathcal{C}^n(\mathcal{X})$.
d) We have $\mathcal{F}(\mathcal{X}) \subset \mathcal{F}(Y)$.

Lemma 7.9. *If R is left Noetherian and $\mathcal{X} \subset FFR$, then $\mathcal{F}(\mathcal{X}) \subset FFR$.*

Exercise: Prove it.

7.2.3. *Serre's Theorem.*

Theorem 7.10. *Let R be a Notherian commutative ring. If every finitely generated R-module is FFR, then every finitely generated $R[t]$-module is FFR.*

Proof. Step 1: Let $\mathcal{X}$ be the class of finitely generated $R[t]$-modules which are *extended* from M: $M \cong R[t] \otimes_R N$ for some R-module N. Let $F_\bullet$ be a FFR of N. Since $R[t]$ is flat over R, $R[t] \otimes_R F_\bullet$ is a FFR for M. By Lemma 7.9, $\mathcal{F}(\mathcal{X}) \subset FFR$. So it suffices to show: every finitely generated $R[t]$-module lies in $\mathcal{F}(\mathcal{X})$.
Step 2: Suppose $\operatorname{ann}(M) \cap R \neq \{0\}$. Let $m \in M^\bullet$; then $\operatorname{ann}(m) \cap R \supset \operatorname{ann}(M) \cap R \neq \{0\}$. Put $I = \operatorname{ann}(m) \cap R$, so $R/I \cong \langle m \rangle_R$. Since $R[t]$ is flat over R, there is a short exact sequence

$$0 \to R[t] \otimes_R I \to R[t] \to R[t] \otimes_R \langle m \rangle \to 0. \tag{9}$$

By the Tensorial Criterion for Flatness [CA, Thm. 3.83], $R[t] \otimes_R I \cong R[t]I$, so $R[t]I \neq \{0\}$. So $R[t]/R[t]I \cong R[t] \otimes_R \langle m \rangle$ is (again by flatness of $R[t]$) a cyclic $R[t]$-submodule of M, say $\langle m_1 \rangle_{R[t]}$. So $\langle m_1 \rangle_{R[t]} \in \mathcal{X}$. Since $\operatorname{ann}(m_1) = R[t]I$, $\operatorname{ann}(m_1) \cap R \neq \{0\}$. Apply the same argument to $M/\langle m_1 \rangle$: there is $m_2 \in M$ such that $\operatorname{ann}(m_2 + \langle m_1 \rangle) \cap R \neq \{0\}$ and $\langle m_1, m_2 \rangle / \langle m_1 \rangle \in \mathcal{X}$. Since M is Noetherian, eventually we get $M = \langle m_1, \ldots, m_l \rangle$ and thus $M \in \mathcal{F}(\mathcal{X})$.
Step 3: In general, by [CA, Thm. 4.31] we have a filtration

$$M = M_0 \supset M_1 \supset \ldots \supset M_n = 0$$

with $M_i/M_{i+1} \cong R/\mathfrak{p}_i$ for a prime ideal $\mathfrak{p}_i$ of $R[t]$. Thus it suffices to show that for any prime ideal $\mathfrak{p}$ of $R[t]$, $R[t]/\mathfrak{p} \in \mathcal{F}(\mathcal{X})$. By Step 2, we may assume

$$\operatorname{ann}(R[t]/\mathfrak{p}) \cap R = \mathfrak{p} \cap R = 0.$$

Since $\mathfrak{p} \cap R$ is a prime ideal of R, R and thus $R[t]$ must be domains. Let $0 \neq f \in \mathfrak{p} \subset R[t]$, and consider

$$0 \to \langle f \rangle \to \mathfrak{p} \to \mathfrak{p}/\langle f \rangle \to 0.$$

Since $R[t]$ is a domain, $\langle f \rangle \cong R[t]$, while $\operatorname{ann} \mathfrak{p}/\langle f \rangle \supset \langle f \rangle \neq \{0\}$. It follows that $\langle f \rangle,\ \mathfrak{p}/\langle f \rangle \in \mathcal{F}(\mathcal{X})$, and thus also $\mathfrak{p} \in \mathcal{F}(\mathcal{X})$. Similarly, since $\mathfrak{p},\ R[t] \in \mathcal{F}(\mathcal{X})$, we get $R[t]/\mathfrak{p} \in \mathcal{F}(\mathcal{X})$. $\square$

Theorem 7.11 (Serre's Theorem)**.** *Let k be a PID, let $n \in \mathbb{N}$, and put $R_n = k[t_1, \ldots, t_n]$. Then every finitely generated projective R_n-module is stably free.*

Proof. Note first that k is Noetherian, hence so is each R_n by the Hilbert Basis Theorem. We will show by induction on n that every finitely generated R_n-module is FFR. This suffices by Serre's Lemma.
The base case is $n = 0$, in which case $R_0 = k$ is a PID, hence a hereditary ring, so every finitely generated R-module admits an FFR of length 1. Suppose now that $n > 0$ and that every finitely generated R_{n-1}-module is FFR. Since $R_n \cong R_{n-1}[t]$, by Theorem 7.10 every finitely generated R_n-module is FFR. We're done! $\square$

7.3. **Projective, Injective and Global Dimensions.**

Let M be an R-module. The **projective dimension of M** is the minimal length of a projective resolution of M, or ∞ if there is no finite length projective resolution.

The **injective dimension of M** is the minimal length of an injective resolution of M, or ∞ if there is no finite length injective resolution.

The **projective dimension of R** is the supremum of the projective dimensions of all R-modules. The **injective dimension of R** is the supremum of the injective dimensions of all R-modules.

Exercise: Let R be a ring. Show:
a) An R-module has projective dimension 0 iff it is projective.
b) An R-module has injective dimension 0 iff it is injective.
c) R has projective dimension 0 iff it has injective dimension 0 iff it is semisimple.

Proposition 7.12. *Let $\{M_i\}_{i\in I}$ be a family of left R-modules. Then:*

$$\operatorname{pd}\bigoplus_{i\in I} M_i = \sup_{i\in I} \operatorname{pd} M_i.$$

Proof. Put $M = \bigoplus_{i\in I} M_i$ and $d = \sup_{i\in I} \operatorname{pd} M_i$. If $K_{i,n}$ is the nth projective syzygy of M_i and K_n is the projective equivalence class of the nth projective syzygy of M, then $K_n \sim \bigoplus_{i\in I} K_{i,n}$. Thus K_n is projective iff $K_{i,n}$ is projective for all i, and the result follows immediately. □

Corollary 7.13. *If R has infinite projective dimension, there is a left R-module M with $\operatorname{pd} M = \infty$.*

Exercise: Prove Corollary 7.13.

Theorem 7.14 (Short Exact Sequence Theorem)**.** *Let $0 \to A \to B \to C \to 0$ be a short exact sequence of left R-modules.*
a) If any two of $\operatorname{pd} A$, $\operatorname{pd} B$, $\operatorname{pd} C$ are finite, so is the third.
b) If $\operatorname{pd} A < \operatorname{pd} B$, then $\operatorname{pd} C = \operatorname{pd} B$.
c) If $\operatorname{pd} A > \operatorname{pd} B$, then $\operatorname{pd} C = 1 + \operatorname{pd} A$.
d) If $\operatorname{pd} A = \operatorname{pd} B$, then $\operatorname{pd} C \leq 1 + \operatorname{pd} A$.
e) We have $\operatorname{pd} B \leq \max \operatorname{pd} A, \operatorname{pd} C$, with equality unless $\operatorname{pd} C = 1 + \operatorname{pd} A$.

Proof. Step 1: First suppose C is projective, so $B \cong A \oplus C$. In this case by Proposition X.X we have $\operatorname{pd} B = \sup \operatorname{pd} A, \operatorname{pd} C = \operatorname{pd} A$, so the result holds in this case.
Next suppose B is projective, so $\operatorname{pd} A \geq \operatorname{pd} B$. Then $[A] = \mathbb{P}[C]$, so $\operatorname{pd} C = 1+\operatorname{pd} A$. Henceforth we assume that neither B nor C is projective.
Step 2: We prove part a). Write

$$0 \to K \to P \to B \to 0,$$

so $B = P/K$. Thus the submodule A is of the form Q/K for some $K \subset Q \subset P$ and we have

$$0 \to K \to Q \to A \to 0 \tag{10}$$

and $C \cong P/Q$. It follows that

$$\operatorname{pd} B = 1 + \operatorname{pd} K,$$
$$\operatorname{pd} C = 1 + \operatorname{pd} Q.$$

The result follows by induction on the sum of the two finite projective dimensions.
Step 3: If $\operatorname{pd} A = \operatorname{pd} B = \infty$, then only d) applies and the conclusion is vacuous.
If $\operatorname{pd} A = \operatorname{pd} C = \infty$, then only c) and d) apply and the conclusions hold.
If $\operatorname{pd} B = \operatorname{pd} C = \infty$, then only b) and d) apply and the conclusions hold.
Step 4: we may assume $\operatorname{pd} A, \operatorname{pd} B, \operatorname{pd} C < \infty$, and we go by induction on their sum.
Case 1: If $\operatorname{pd} K < \operatorname{pd} Q$ – hence $\operatorname{pd} B < \operatorname{pd} C$ – then by induction and using (10) we get $\operatorname{pd} A = \operatorname{pd} Q = \operatorname{pd} C - 1 \geq \operatorname{pd} B$.
Case 2: If $\operatorname{pd} K > \operatorname{pd} Q$ – hence $\operatorname{pd} B > \operatorname{pd} C$ – then by induction and using (10) we get $\operatorname{pd} A = \operatorname{pd} K + 1 = \operatorname{pd} B$.
Case 3: If $\operatorname{pd} K = \operatorname{pd} Q$ – hence $\operatorname{pd} B = \operatorname{pd} C$ – then by induction and using (10) we get $\operatorname{pd} A \leq \operatorname{pd} K + 1 = \operatorname{pd} B$.
Step 5: We prove part b): suppose $\operatorname{pd} A < \operatorname{pd} B$. By Step 4 we must be in Case 3, so $\operatorname{pd} B = \operatorname{pd} C$.
Step 6: We prove part c): suppose $\operatorname{pd} A > \operatorname{pd} B$. By Step 4 we must be in Case 1, so $\operatorname{pd} C = \operatorname{pd} A + 1$.
Step 7: We prove part d): suppose $\operatorname{pd} A = \operatorname{pd} B$.
If we are in Case 1, then $\operatorname{pd} C = \operatorname{pd} A + 1$.
If we are in either Case 2 or Case 3, then $\operatorname{pd} C \leq \operatorname{pd} B < \operatorname{pd} A + 1$.
Step 8: We prove part e).
Case b): suppose $\operatorname{pd} A < \operatorname{pd} B$. By part b), $\operatorname{pd} B = \operatorname{pd} C$ and the result holds.
Case c): suppose $\operatorname{pd} A > \operatorname{pd} B$. By part c), $\operatorname{pd} C = 1 + \operatorname{pd} A$ and the result holds.
Case d): suppose $\operatorname{pd} A = \operatorname{pd} B$. Then $\operatorname{pd} C \leq 1 + \operatorname{pd} A$. If we have equality, we're done. Otherwise, $\operatorname{pd} C \leq \operatorname{pd} A$ so $\operatorname{pd} B = \max \operatorname{pd} A, \operatorname{pd} C$. □

Proposition 7.15. *a) For an R-module M, the following are equivalent:*
(i) M is projective.
(ii) $\operatorname{Ext}^n_R(M, N) = 0$ for all $n \in \mathbb{Z}^+$ and all R-modules N.
(iii) $\operatorname{Ext}^1_R(M, N) = 0$ for all R-modules N.
b) For an R-module N, the following are equivalent:
(i) N is injective.
(ii) $\operatorname{Ext}^n_R(M, N) = 0$ for all $n \in \mathbb{Z}^+$ and all R-modules M.
(iii) $\operatorname{Ext}^1_R(M, N) = 0$ for all R-modules M.
(iv) $\operatorname{Ext}^1_R(R/I, N) = 0$ for all left ideals I of R.

Proof. a) (i) $\implies$ (ii): projective objects are acyclic for all derived functors of epimonic functors.
(ii) $\implies$ (iii) is clear.
(iii) $\implies$ (i): We use the fact that M is projective iff $N \mapsto \operatorname{Hom}(M, N)$ is exact.
b) Exercise. (Hint for (iv) $\implies$ (iii): use Baer's Criterion.) □

Theorem 7.16. *a) For an R-module M and $n \in \mathbb{N}$, the following are equivalent:*
(i) $\operatorname{pd} M \leq n$.
(ii) $\operatorname{Ext}^i_R(M, N) = 0$ for all $i > n$ and all R-modules N.
(iii) $\operatorname{Ext}^{n+1}_R(M, N) = 0$ for all R-modules N.
(iv) If $0 \to K_n \to P_{n-1} \to \ldots \to P_0 \to M \to 0$ is exact with all P_i's projective,

then the syzygy K_n is projective.
b) For an R-module N and $n \in \mathbb{N}$, the following are equivalent:
(i) $\operatorname{id} N \leq n$.
(ii) $\operatorname{Ext}^i(M, N) = 0$ *for all $i > n$ and all R-modules M.*
(iii) $\operatorname{Ext}^{n+1}(M, N) = 0$ *for all R-modules M.*
(iv) If $0 \to N \to E_0 \to \ldots E_{n-1} \to C \to 0$ is an exact sequence with all E_i's injective, then also C is injective.

Proof. a) (i) $\implies$ (ii): Using the projective resolution of M of length at most m to compute the Ext's, this is immediate.
(ii) $\implies$ (iii) is immediate.
(iii) $\implies$ (iv): Apply dimension shifting to the epimonic functor $\operatorname{Hom}(\cdot, N)$ to get

$$0 = \operatorname{Ext}_R^{n+1}(M, N) \cong \operatorname{Ext}_R^1(K_{n-1}, N).$$

Since this holds for all N, by Proposition 7.15, K_{n-1} is projective.
(iv) $\implies$ (i): Construct a projective reslution of M as usual, but stop at X_{n-1} and instead write down the kernel ("syzygy"):

$$0 \to K_n \to P_{n-1} \to \ldots \to P_0 \to M \to 0.$$

Then the hypothesis implies that K_n is projective and thus we have constructed a projective resolution of length at most n.
b) Exercise. $\square$

Corollary 7.17. *For any ring R, For every ring R, the projective dimension of R is equal to its injective dimension.*

This common quantity is called the **global dimension** of R.

Theorem 7.18 (Auslander)**.** *For any ring R, $D(R)$ is the supremum of* $\operatorname{pd} R/I$ *as I ranges over all left ideals of R.*

Proof. Just for the purposes of the proof, let us set $D_A(R)$, the "Auslander dimension" of R, to be the supremum of the projective dimensions of R/I. Clearly $D_A(R) \leq D(R)$, so if $D_A(R) = \infty$ there is nothing to show: assume $D_A(R) \leq n$ for some finite n. Let B be any left R-module, and take an injective resolution with $(n-1)$st cosyzygy C^{n-1}. By dimension shifting, we have

$$0 = \operatorname{Ext}^{n+1}(R/I, B) = \operatorname{Ext}^1(R/I, C^{n-1})$$

for all left ideals I. By Proposition 7.15b), this gives that C^{n-1} is injective, and thus we get an injective resolution of B of length n. $\square$

Remark: Our terminology "global dimension" is sloppy in the non-commutative case. We are speaking about left R-modules so that we should be speaking of the **left homological dimension** $D_\ell(R)$; there is also a **right homological dimension** $D_r(R)$ computed using right modules.

Obviously $D_\ell(R) = D_r(R)$ for all commutative rings R: must this equality hold for all rings? There is one early piece of evidence in favor of this: as we will record shortly, $D_\ell(R) = 0$ iff R is left semisimple. But it follows from Artin-Wedderburn theory that a ring is left semisimple iff it is right semisimple, and thus

$$D_\ell(R) = 0 \iff D_r(R) = 0.$$

However this is as far as it goes.

Theorem 7.19. *a) (Kaplansky* [Ka58b]*) There is a ring R with $D_\ell(R) = 1$ and $D_r(R) = 2$.*
b) (Jategaonkar [Ja69]*) For any $1 \leq m \leq n \leq \infty$ there is a ring R with $D_\ell(R) = m$, $D_r(R) = n$.*

Theorem 7.20. *For a ring R:*
a) R is semisimple iff $D(R) = 0$.
b) R is left hereditary iff $D(R) \leq 1$.

Proof. a) Exercise.
b) Suppose R is left hereditary. By [CA, Cor. 3.56], a commutative ring is hereditary iff every submodule of a projective R-moduleis projective. As the reader may check, the result works verbatim in the context of left (say) modules over arbitrary rings. Thus for any R-module M, we choose a projective module P_0 and a surjection $P_0 \to M \to 0$, and consider its kernel

$$0 \to K_0 \to P_0 \to M \to 0.$$

It follows that K_0 is projective, so we get a projective resolution o length at most 1. Apply Theorem XX.
(ii) $\implies$ (i): let I be a non-projective left ideal of R. Consider the exact sequence:

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

by Theorem 7.16, if $\operatorname{pd} R/I$ were at most one, then I would be projective. It isn't, so $D(R) \geq \operatorname{pd} R/I \geq 2$. □

Remark: Thus a commutative ring has homological dimension zero iff it is a finite product of fields. These rings are a tiny subset of the class of all zero dimensional rings: in fact they are precisely the *regular* Noetherian zero-dimensional rings. Similarly, a domain which is not a field has homological dimension one iff it is Dedekind. Dedekind domains are again a tiny subclass of the class of all domains of Krull dimension one but they are precisely the regular Noetherian ones.

Here is a result showing that the study of homological dimensions of (non-Noetherian) rings can be connected to deep issues in set theory.

Theorem 7.21 (Osborne)**.** *a) Let $m \in \mathbb{N}$, and let R be a Bézout domain of cardinality $\aleph_m$. Then $D(R) \leq m + 2$.*
b) In particular, assuming the continuum hypothesis – $\#\mathbb{R} = \aleph_1$ – the ring R of entire functions in the complex plane has homological dimension at most 3.

7.4. **Kaplansky Pairs.**

Here is an elementary construction due to Kaplansky which provides us with several important examples of rings of infinite global dimension.

Let R be a ring. A **Kaplansky pair** is a pair of elements $a, b \in R$ such that

$$\{x \in R \mid ax = 0\} = bR, \ \{x \in R \mid bx = 0\} = aR.$$

In this case we have a short exact sequence

$$0 \to bR \to R \to aR \to 0, \tag{11}$$

where the first map is inclusion and the second map is multiplication by a, and, symmetrically, a short exact sequence

$$0 \to aR \to R \to bR \to 0. \tag{12}$$

By splicing these sequences, we get an infinite free resolution of aR of the form

$$\ldots \to R \to R \to \ldots \to aR \to 0, \tag{13}$$

where the maps $R \to R$ alternate between $R \to aR \hookrightarrow R$ and $R \to bR \hookrightarrow R$. Thus for all n, $K_{2n} = bR$ and $K_{2n+1} = aR$.

Theorem 7.22. *Let $a, b \in R$ be a Kaplansky pair.*
a) The following are equivalent:
(i) aR and bR are both projective R-modules.
(ii) At least one of aR and bR is a projective R-module.
(iii) $aR \oplus bR \cong R$.
b) When R is commutative, the conditions of part a) are equivalent to
(iv) $\langle a, b\rangle = R$.
c) When the equivalent conditions of part a) ***do not hold****, we have*

$$D(R) = \operatorname{pd} aR = \operatorname{pd} bR = \infty.$$

Proof. a) Using (11) and (12), (i) $\implies$ (ii) $\implies$ (iii) $\implies$ (i) is immediate.
b) For any ideals I and J in a commutative ring R there is a natural injection of rings

$$\Phi : R/(IJ) \to R/I \times R/J.$$

Apply this with $I = aR$, $J = bR$: we have $IJ = 0$, $I \cong R/J$ and $J \cong R/I$, so

$$\Phi : R \to bR \oplus aR.$$

By the Chinese Remainder Theorem and its converse [CA, § 4.3], Φ is an isomorphism iff $I + J = R$, which is condition (iv). Thus (iv) $\implies$ (iii). Conversely, if the sequence (11) splits then Φ is surjective, so (i) $\implies$ (iv).
c) We may assume that neither aR nor bR is projective; using (13), this shows that none of the syzygies of aR are projective, so by Theorem 7.16 $\operatorname{pd} aR = \infty$. Symmetrically we get $\operatorname{pd} bR = \infty$. Either of these implies $D(R) = \infty$. □

Let us say that a Kaplansky pair is **proper** if the equivalent conditions of Theorem 7.22a) *do not hold.* Thus exhibiting a proper Kaplansky pair in a ring R shows that $D(R) = \infty$. We give four examples of this.

Proposition 7.23. *Let $n \in \mathbb{Z}^+$. Then:*
a) If n is squarefree, $D(\mathbb{Z}/n\mathbb{Z}) = 0$.
b) If n is not squarefree, $D(\mathbb{Z}/n\mathbb{Z}) = \infty$.

Proof. Exercise. □

Proposition 7.24. *Let k be a field, $n \geq 2$ and $R = k[t]/(t^n)$. Then $D(R) = \infty$.*

Proof. Exercise. □

Proposition 7.25. *Let k be a field, $R = k[x, y]/(xy)$. Then $D(R) = \infty$.*

Proof. Exercise. □

Proposition 7.26. *Let $n > 1$, let $G = \langle \sigma \mid \sigma^n = 1\rangle$, and let $R = \mathbb{Z}[G]$. Then $a = \sigma - 1$, $b = 1 + \sigma + \ldots + \sigma^{n-1}$ is a proper Kaplansky pair in R.*

Proof. Exercise. □

Exercise: Let T be a ring, and let $a, b \in Z(T)$ be non-zero-divisors. Let $R = T/\langle ab \rangle$.
a) Show that (the natural images in R of) a and b are a Kaplansky pair in R.
b) Show that the pair (a, b) is proper iff $\langle a, b \rangle \neq T$.
c) Show that in fact all four examples above are special cases of this construction.

7.5. **The Weak Dimension.**

Having considered vanishing of Ext modules as a kind of measure of the dimension of a ring R, it is natural to try to do the same thing for Tor.

Definition: The **flat dimension** $\mathrm{fd}(M)$ of a left R-module M is the minimum length of a finite flat (left) resolution of M, or ∞ if there is no finite flat resolution. The **weak dimension** $\mathrm{wD}(R)$ of a ring R is the supremum of $\mathrm{fd}(M)$ as M ranges over all left R-modules.

Exercise: a) Show that for every R-module, $\mathrm{fd}(M) \leq \mathrm{pd}(M)$.
b) Show that for every ring, $\mathrm{wD}(R) \leq D(R)$.

Theorem 7.27. *For an R-module N, the following are equivalent:*
(i) $\mathrm{fd}\, N \leq n$.
(ii) $\mathrm{Tor}_k^R(M, N) = 0$ *for all* $k \geq n + 1$ *and all modules* M.
(iii) $\mathrm{Tor}_{n+1}^R(M, N) = 0$ *for all modules* M.
(iv) Every flat resolution of N has a flat $(n-1)$st syzygy K_{n-1}.

Exercise: Prove Theorem 7.27. (Suggestion: adapt the proof of Theorem 7.16. Use the fact that tor can be computed using flat resolutions.)

Corollary 7.28. *A ring R has weak dimension at most n iff for every left R-module M and right R-module N,* $\mathrm{Tor}_{n+1}^R(M, N) = 0$. *In particular, the left weak dimension of R is equal to the right weak dimension of R.*

Exercise: Show that $\mathrm{wD}(R) = 0$ iff R is absolutely flat.

Theorem 7.29. *For any ring R, the weak dimension is the supremum of* $\mathrm{fd}\, R/I$ *as I ranges over all left ideals and also the supremum of* $\mathrm{fd}\, R/I$ *as I ranges over all right ideals.*

Proof. We recall the **Homological Criterion For Flatness** [CA, Thm. 3.82]: an R-module M is flat iff $\mathrm{Tor}_1^R(M, R/I) = 0$ for every left ideal I of R. Given this, the proof is the same as that of Theorem 7.18. □

Theorem 7.30. *a) For a ring R, the following are equivalent:*
(i) Every submodule of a flat left R-module is flat.
(ii) Every left ideal of R is a flat R-module.
b) If R is a domain, the conditions of (i) and (ii) are equivalent to:
(iii) R is a Prüfer domain: every finitely generated ideal is projective.

Proof. a) (i) $\implies$ (ii) is immediate, since R is a flat R-module.
(ii) $\implies$ (i): If every left ideal of R is flat, then

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

is a flat resolution of R/I, which shows that $\mathrm{fd}(R/I) \leq 1$. By Theorem 7.29, $\mathrm{wD}(R) \leq 1$. Now let N be a submodule of a flat R-module M. Since $\mathrm{fd}(M/N) \leq 1$, applying Theorem 7.27 to

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

shows that N is flat.
b) We use the fact [CA, Thm. 21.9] that a domain is Prüfer iff every torsionfree R-module is flat.
(iii) $\implies$ (i): A submodule of a flat module is torsionfree, hence flat since R is Prüfer.
(i) $\implies$ (iii): Let K be the fraction field of R, and let M be a torsionfree R-module. Then $M \hookrightarrow M \otimes_R K$ embeds M as a submodule of a flat R-module, so by assumption M is flat. □

Theorem 7.31. *Let R be a left Noetherian ring.*
a) If M is a finitely generated left R-module, then

$$\mathrm{fd}\, M = \mathrm{pd}\, M.$$

b) It follows that $\mathrm{wD}(R) = D(R)$.

Proof. a) Of course we have $\mathrm{fd}\, M \leq \mathrm{pd}\, M$ in general, so we may assume $\mathrm{fd}\, M = n < \infty$; our task is to construct a projective resolution of length at most n. Because R is left Noetherian and M is finitely generated, we may construct a left reslution of M by *finitely generated* left projective modules; now consider the $n-1$st syzygy of such a guy:

$$0 \to K_{n-1} \to P_{n-1} \to \ldots \to P_0 \to M.$$

In particular this is a flat resolution of M, so by Theorem 7.27 K_{n-1} is flat. Being a submodule of a finitely generated module over a left Noetherian ring, K_{n-1} is finitely generated. We finish with the fundamental result that a finitely generated flat module over a left Noetherian ring is projective: see [Rot, Cor. 3.57] for the non-commutative case. Thus we have constructed a projective resolution of M of length at most n.
b) By Theorems 7.18 and 7.29, both $\mathrm{wD}(R)$ and $D(R)$ can be computed using finitely generated modules. □

7.6. **The Change of Rings Theorems.**

I. Kaplansky gave a remarkably efficient exposition of most of the key results of homological dimension theory in a series of lectures in the 1950's (so quite soon after the theorems were first obtained). Recall that Schanuel's Lemma emerged from a graduate student taking his course. Another one of his innovations was to observe that much of the content turned on a trio of results comparing projective dimensions of modules over a ring R and over a quotient $\overline{R} = R/(x)$ where x is a non-zero-divisor in R. We give these theorems here. In the next section Change of Rings I will be used to prove the Hilbert Syzygy Theorem. Later we will use Change of Rings I and II to prove the theorem of Serre and Auslander-Buchsbaum.

Theorem 7.32. *(Change of Rings I) Let R be a ring, and let $x \in R$ be a central non zero-divisor. Put $\overline{R} = R/\langle x \rangle$, and let M be a nonzero left $\overline{R}$-module. Then*

$$\mathrm{pd}_{\overline{R}}\, M = n < \infty \implies \mathrm{pd}_R\, M = n + 1.$$

Proof. We go by induction on n.
Base Case ($n = 0$): Suppose M is $\overline{R}$-projective, hence a direct summmand of an $\overline{R}$-free module $\overline{F}$. Using the sequence

$$0 \to Rx \to R \to \overline{R} \to 0$$

and the fact that $Rx \cong R$ since x is not a zero-divisor, we see $\operatorname{pd}_R \overline{R} \le 1$ and thus

$$\operatorname{pd}_R M \le \operatorname{pd}_R \overline{F} = \operatorname{pd}_R \bigoplus_{i \in I} \overline{R} \le 1.$$

On the other hand, since $xM = 0$ and x is not a zero-divisor, M cannot be a submodule of a free R-module. In particular M is not R-projective, so $\operatorname{pd}_R M \ge 1$.
$n = 1$ Case: Choose a short exact sequence of $\overline{R}$-modules

$$0 \to K \to \overline{F} \to M \to 0, \tag{14}$$

with $\overline{F}$ a free $\overline{R}$-module. Since $\operatorname{pd}_{\overline{R}} M = 1$, $\operatorname{pd}_{\overline{R}} K = 0$. By the induction hypothesis, we get $\operatorname{pd}_R \overline{F} = \operatorname{pd}_R K = 1$, and by the Short Exact Sequence Theorem,

$$\operatorname{pd}_R M \le \max \operatorname{pd}_R \overline{F}, 1 + \operatorname{pd}_R K \le 2.$$

Conversely, let

$$0 \to T \to F \to M \to 0 \tag{15}$$

be a short exact sequence of R-modules with F free. Since $xM = 0$, $xF \subset T$, so

$$0 \to T/xF \to F/xF \to M \to 0$$

is a short exact sequence of $\overline{R}$-modules. Further, since $F/xF = F \otimes_R \overline{R}$ is a free $\overline{R}$-module, we have

$$\operatorname{pd}_{\overline{R}} T/xF = \operatorname{pd}_{\overline{R}} -1 = 0.$$

Therefore the sequence of $\overline{R}$-modules

$$0 \to xF/xT \to T/xT \to T/xF \to 0$$

splits. Since $M \cong F/T \xrightarrow{\cdot x} xF/xT$ is an isomorphism, M is a direct summand of T/xT. Now if T were R-projective, then $T/xT = T \otimes_R \overline{R}$ would be $\overline{R}$-projective and thus M would be $\overline{R}$-projective, which it isn't. Using (15) we get $\operatorname{pd}_R M = 2$.
$n \ge 2$ Case: Considering (14), we have $\operatorname{pd}_{\overline{R}} K = \operatorname{pd}_{\overline{R}} -1 = n - 1$, so by induction $\operatorname{pd}_R K = n > 1 \ge \operatorname{pd}_R \overline{F}$, so by the Short Exact Sequence Theorem we have

$$\operatorname{pd}_R M = \operatorname{pd}_R K + 1 = n + 1.$$

□

Example: Let k be a field and $R = k[t_1, \ldots, t_n]$. Applying the Change of Rings Lemma n times to the R-module $k = R/\langle t_1, \ldots, t_n \rangle$ we get $\operatorname{pd}_R k = n$. It follows that $DR \ge n$ and that Tor and Ext are not identically vanishing in degree n.

Let R be a ring. A finite sequence $x_1, \ldots, x_n$ of elements of the center of R is called a **regular sequence** if $\langle x_1, \ldots, x_n \rangle \subsetneq R$ and for all $i \ge 1$, the image of x_i is a non-zero-divisor in $R/\langle x_1, \ldots, x_{i-1} \rangle$.

Proposition 7.33. *Let $x_1, \ldots, x_n$ be a regular sequence in R, and put $I = \langle x_1, \ldots, x_n \rangle$. Then $\operatorname{pd} R/I = n$.*

Proof. We go by induction on n, the base case $n = 0$ being trivial. For $n > 0$, the images $\overline{x_2}, \ldots, \overline{x_n}$ form a regular sequence in $\overline{R} = R/\langle x_1 \rangle$. By induction,

$$\operatorname{pd}_{\overline{R}} \overline{R}/\langle \overline{x_2}, \ldots, \overline{x_n} \rangle = n - 1.$$

Now Change of Rings I gives $\operatorname{pd} R/I = n$. $\square$

Theorem 7.34. *(Change of Rings II) Let $x \in R$ be a central non-zero-divisor, and put $\overline{R} = R/(x)$. Let M be an R-module. We suppose that x is regular on M. Then*

$$\operatorname{pd}_{\overline{R}} M/xM \leq \operatorname{pd}_R M.$$

Proof. The result holds trivially if $\operatorname{pd}_R M = \infty$, so suppose $\operatorname{pd}_R M = n < \infty$; we go by induction on n.
Base Case ($n = 0$): Then M is projective, so $M/xM = M \otimes_R \overline{R}$ is $\overline{R}$-projective.
Induction Step ($n > 0$): Consider a short exact sequence

$$0 \to K \to F \xrightarrow{\alpha} M \to 0$$

with F free. Then $\operatorname{pd}_R K = n - 1$ and since x is regular on R it is also on F and thus on K. By induction, $\operatorname{pd}_{\overline{R}} K/xK \leq n - 1$. The map α induces a map $F/xF \to M/xM$, with kernel $(K + xF)/xF \cong K/(K \cap xF)$. If $a \in K \cap xF$ then $\alpha(a) = 0$ and thus $a = xb$, so $0 = \alpha(xb) = x\alpha(b)$, and since x is regular on M this implies $\alpha(b) = 0$, so $b \in K$. Thus $K \cap xF = xK$, and we get a short exact sequence

$$0 \to K/xK \to F/xF \to M/xM \to 0.$$

Since F/xF is $\overline{R}$-projective, K/xK is a syzygy of M/xM, so $\operatorname{pd}_{\overline{R}} M/xM \leq n$. $\square$

Theorem 7.35. *(Change of Rings III) Let R be left Noetherian, let $x \in R$ be a central non-zero-divisor contained in the Jacobson radical of R; put $\overline{R} = R/(x)$. Let M be a finitely generated R-module such that x is regular on M. Then*

$$\operatorname{pd}_{\overline{R}} M/xM = \operatorname{pd}_R M.$$

Proof. Let $n = \operatorname{pd}_{\overline{R}} M/xM$. We must show that $\operatorname{pd}_R M = n$. If $n = \infty$, then Change of Rings II applies, so we may assume $n < \infty$ and go by induction on n.
Step 1: We show that if M/xM is $\overline{R}$-free, then M is R-free.
Let $v_1, \ldots, v_n \in M$ map to an $\overline{R}$-basis for M/xM. We claim that $v_1, \ldots, v_n \in M$ is an R-basis. That they span M follows from aNakayama's Lemma. Suppose $\sum_{i=1}^n c_i v_i = 0$. Then since the images of $v_1, \ldots, v_n$ in M/xM are $\overline{R}$-linearly independent, there are $d_1, \ldots, d_n \in R$ such that $c_i = xd_i$ for all i. Thus we have $x\left(\sum_{i=1}^n d_i v_i\right) = 0$, and since x is regular on R, $\sum_{i=1}^n d_i v_i = 0$. Arguing as above we get that $d_i = xd_i'$, and so forth. The conclusion is that for all $1 \leq i \leq n$, $c_i \in \bigcap_{k=1}^\infty (x^k) = 0$ by the Krull Intersection Theorem.
Step 2: We show that if M/xM is $\overline{R}$-projective, then M is R-projective, which is the $n = 0$ case of the result we are trying to prove. As in the proof of Change of Rings II we have short exact sequences

$$0 \to K \to F \to M \to 0$$

and

$$0 \to K/xK \to F/xF \to M/xM \to 0. \tag{16}$$

Put $B = M \oplus K$. Since M/xM is $\overline{R}$-projective, (16) splits, so

$$B/xB \cong M/xM \oplus K/xK \cong F/xF.$$

Thus B/xB is $\overline{R}$-free, so by Step 1 B is R-free and thus M is R-projective.
Step 3: Suppose $n > 0$ and the result holds for modules of projective dimension $n-1$. By Change of Rings II it suffices to show that $\operatorname{pd}_R M \leq n$. By (16) we have $\operatorname{pd}_{\overline{R}} K/xK \leq n-1$. The hypotheses also apply to K, so by induction $\operatorname{pd}_R K \leq n-1$ and thus $\operatorname{pd}_R M \leq n$. ☐

7.7. **The Hilbert Syzygy Theorem.**

Theorem 7.36. *(Eilenberg-Rosenberg-Zelinsky* [ERZ57]*) For any ring R and $n \in \mathbb{N}$ we have $D(R[t_1, \ldots, t_n]) = D(R) + n$.*

Proof. Step 0: By an evident induction argument it is enough to take $n = 1$. Thus let us change our notation: starting with a ring A, put $R = A[x]$, and our goal is to show that $D(R) = D(A) + 1$. For any left A-module M, we write $M[x]$ for $R \otimes_A M$, and we write elements of $M[x]$ as formal finite sums $\sum_i m_i x^i$.
Step 1: We CLAIM that for any A-module M, M is projective iff $M[x]$ is projective.
PROOF OF CLAIM: As for any base change, if M is projective over A, then $R \otimes_A M$ is projective over R. Conversely, suppose $M[x]$ is $A[x]$-projective, so there is a free $A[x]$-module F with $F \cong M[x] \oplus M'$. Since $A[x]$ is A-free, F is A-free, and since M is a direct summand of $M[x]$, we conclude that M is A-projective.
Step 2: We have $\operatorname{pd}_A M = \operatorname{pd}_R M[x]$.
Indeed, consider an exact sequence

$$K_{n-1} \to P_{n-1} \to \ldots \to P_0 \to M \to 0$$

with P_i projective for all i. Then (since R is a flat A-module) we have an exact sequence

$$K_{n-1}[x] \to P_{n-1}[x] \to \ldots \to P_0[x] \to M[x] \to 0.$$

From this and Step 1 it follows that the $(n-1)$st syzygy of M is projective iff the $(n-1)$st syzygy of $M[x]$ is projective, and the result follows immediately from this.
Step 3: Suppose $D(A) = \infty$. By Corollary 7.13 there is $M \in_A \operatorname{Mod}$ with $\operatorname{pd}_A M = \infty$. By Step 2, $\operatorname{pd}_R M[x] = \infty$ and thus $D(R) = \infty$.
Step 4: We may thus assume $D(A) = d < \infty$. It follows immediately from the Change of Rings Theorem that $D(R) \geq d+1$, and it remains to show the opposite inequality. Let $M \in_R \operatorname{Mod}$. We may view M as an A-module endowed with an A-endomorphism f. It suffices to construct a short exact sequence

$$0 \to M[x] \xrightarrow{\psi} M[x] \xrightarrow{\varphi} 0.$$

Indeed, using such a sequence the Short Exact Sequence Theorem gives

$$\operatorname{pd}_R M \leq \operatorname{pd}_R M[x] + 1 = \operatorname{pd}_A M + 1 \leq d + 1.$$

Step 5: We construct φ and ψ quite explicitly. Indeed, put

$$\varphi(\sum m_i x^i) = \sum f^i(m_i).$$

This is clearly surjective. Next, $\tilde{f} = 1_R \otimes_A f$ is an R-endomorphism of $M[x]$ which maps $\sum m_i x^i$ to $\sum f(m_i) x^i$. Also we have $\tilde{x} \in \operatorname{End}_R M[x]$ which maps $\sum m_i x^i$ to $\sum m_i x^{i+1}$. Put

$$\psi = \tilde{x} - \tilde{f}.$$

Then

$$\psi(\sum m_i x^i) = -f(m_0) + (m_0 - f(m_1))x_1 + \ldots + (m_{r-1} - f(m_r))x^r + m_r x^{r+1},$$

so ψ is surjective. We leave the (routine) verification that $\varphi\psi = 0$ as an exercise, but let's show that $\ker \varphi \subset \operatorname{Image} \psi$: suppose

$$0 = \varphi(\sum m_i x^i) = \sum f^i(m_i) = 0.$$

Then

$$\sum_{i \geq 0} m_i x6i = \sum_{i \geq 0} m_i x^i - f^i(m_i) = \sum_{i \geq 1} (\tilde{x^i} - \tilde{f}^i)(m_i) \in \operatorname{Image} \psi.$$

□

Corollary 7.37. *(Hilbert Syzygy Theorem) For any field k, $D(k[t_1, \ldots, t_n]) = n$.*

8. Dimension Theory of Local Rings

It turns out that homological dimension theory simplifies considerably when the ring R is commutative, Noetherian and local. In this section we (mostly) work under these assumptions and further develop the theory. In particular we will define and study the key notion of a regular local ring and prove the following results.

• (Serre, Auslander-Buchsbaum) A Noetherian local commutative ring has finite global dimension iff it is regular, in which case its global dimension is equal to its Krull dimension.

• (Auslander-Buchsbaum) A regular local ring is a UFD.

This latter result is striking in that it is barely homological in nature. In particular, let k be an algebraically closed field (in fact it is enough if it is perfect), let $V_{/k}$ be an algebraic variety, let $P \in V$ be a closed point, and let R be the local ring of functions regular at P. Then R is a regular local ring if P is a nonsingular point on V in the sense of the Jacobian condition from multivariable calculus.

An elementary property of UFDs is that in them every height one prime ideal is principal (CITE). Because of this, the Auslander-Buchsbaum Theorem has the following basic geometric consequence: let $P \in V$, and let W be a codimension one subvariety passing through P. Then in some Zariski-open neighborhood of P, W is a hypersurface, i.e., is cut out by a single defining equation.

Another purely algebraic consequence of Auslander-Buchsbaum is:

• The localization of a regular local ring at a prime ideal is a regular local ring.

This sounds almost innocuous but in fact it had long been an open problem in the field and was resolved for the first time as a consequence of Auslander-Buchsbaum.

Throughout this section we assume that all of our rings are *commutative*. Some of the basic concepts and minor results hold in the non-commutative case, but most of the important theorems require commutativity, so we make this assumption at the outset for simplicity.

8.1. **Basics on Local Rings.**

We assume that R is (commutative and) *local*: i.e., with a unique maximal ideal $\mathfrak{m}$. We put $k = R/\mathfrak{m}$. We need the following basic (and easy) result, which we are content to state in a somewhat special case.

Proposition 8.1. *(Nakayama's Lemma) Let $(R, \mathfrak{m})$ be a local ring, M be a finitely generated R-module and N an R-submodule with $N + \mathfrak{m}M = M$. Then $M = N$.*

Proof. See e.g. [CA, §3.8]. □

Corollary 8.2. *Let M be a finitely generated R-module.*
a) If $M \neq 0$, then $M/\mathfrak{m}M \neq 0$.
b) If $x_1, \ldots, x_n \in M$ are such that their images span $M/\mathfrak{m}M$ as a k-vector space, then $M = \langle x_1, \ldots, x_n \rangle$.

Exercise: Prove it.

Proposition 8.3. *Let $(R, \mathfrak{m})$ be a local ring, and let M be a finitely generated R-module. Then there is a short exact sequence*

$$0 \to K \to F \to R \to 0$$

with F finitely generated free and $K \subset \mathfrak{m}F$.

Proof. Let $x_1, \ldots, x_n \in M$ map to an $R/\mathfrak{m}$-basis of $M/\mathfrak{m}M$. Put $F = R^n$ with standard basis $e_1, \ldots, e_n$. Let $\varphi : F \to M$ by $e_i \mapsto x_i$. By Nakayama's Lemma, φ is surjective; let $K = \operatorname{Ker} \varphi$. If $x = \sum_{i=1}^n a_i e_i \in K$, then $0 = \varphi(x) = \sum_{i=1}^n a_i x_i$, so $a_i \in \mathfrak{m}$ for all i. □

8.2. **Some Results From Commutative Algebra.**

Lemma 8.4. *(Prime Avoidance) Let R be a ring, and $I_1, \ldots, I_n, J$ be ideals of R. Suppose that all but at most two of the I_i's are prime and that $J \subset \bigcup_{i=1}^n I_i$. Then $J \subset I_i$ for some i.*

Proof. We go by induction on n, the case $n = 1$ being trivial.
$n = 2$: Seeking a contradiction, suppose there is $x_1 \in J \setminus I_2$ and $x_2 \in J \setminus I_1$. Since $J \subset I_1 \cup I_2$ we must have $x_1 \in I_1$ and $x_2 \in I_2$. Then $x_1 + x_2 \in J \subset I_1 \cup I_2$. If $x_1 + x_2 \in I_1$, then since $x_1 + x_2, x_1 \in I_1$, so is x_2, contradiction; whereas if $x_1 + x_2 \in I_2$, then since $x_1 + x_2, x_2 \in I_1$, so is x_1.[14]
$n \geq 3$: We may suppose that I_n is prime and also that for all proper subsets $S \subset \{1, \ldots, n\}$, $J \not\subset \bigcup_{i \in S} I_i$; otherwise we would be done by induction. So for $1 \leq i \leq n$, there is $x_i \in J \setminus \bigcup_{j \neq i} I_j$, and then $x_i \in I_i$. Consider $x = x_1 \cdots x_{n-1} + x_n$. Then $x \in J$, so $x \in I_i$ for some i.
Case 1: $x \in I_n$. Then since $x_n \in I_n$, $x_1 \cdot x_{n-1} \in I_n$, and since I_n is prime $x_i \in I_n$ for some $1 \leq i \leq n-1$, contradiction.
Case 2: $x \in I_j$ for some $1 \leq j \leq n-1$. Then $x_1 \cdots x_{n-1} \in I_j$, so $x_n \in I_j$, contradiction. □

Theorem 8.5 (Krull Intersection Theorem)**.** *Let I be an ideal in a Noetherian ring R. Suppose* either
(i) R is a domain and I is a proper ideal; or

[14] In fact this works for any subgroups I_1, I_2, J of a group G with $J \subset I_1 \cup I_2$.

(ii) I is contained in the Jacobson radical $J(R)$ of R.
Then $\bigcap_{n=1}^{\infty} I^n = 0$.

Proof. See [CA, § 8.12]. □

Theorem 8.6. *(Krull Hauptidealsatz) Let R be a Noetherian ring, and let $I = \langle a_1, \ldots, a_n \rangle$ be a proper ideal of R. Let $\mathfrak{p}$ be a minimal element of the set of all prime ideals containing I. Then $\mathfrak{p}$ has height at most n.*

Proof. See [CA, § 8.13]. □

For a ring R, let $\operatorname{MinSpec} R$ denote the set of minimal prime ideals, i.e., those which do not properly contain any other prime ideal. (Thus R is a domain iff $\operatorname{MinSpec} R = \{(0)\}$.

Theorem 8.7. *Let R be a Noetherian ring.* $\operatorname{MinSpec} R$ *is finite.*

Proof. [CA, § 4.6]. □

Lemma 8.8. *Let $(R, \mathfrak{m})$ be a Noetherian local ring, and let M be a finitely generated R-module. If $\Phi : \mathfrak{m} \otimes_R M \to R \otimes_R M = M$ is injective, then R is free.*

Proof. Choose $x_1, \ldots, x_n \in M$ whose images in $M/\mathfrak{m}M$ give an $R/\mathfrak{m}$-basis. Consider the short exact sequence

$$0 \to K \to F \to M \to 0$$

from Proposition 8.3: in particular $F = R^n$, the standard basis vector $e_i \in F$ gets mapped to $x_i \in M$, and $K \subset \mathfrak{m}F$. It suffices to show $\mathfrak{m}K = K$, for then by Nakayama's Lemma $K = 0$ and $M = F$ is free. Let $x = \sum_{i=1}^n a_i e_i \in K$, so $\sum_{i=1}^n a_i x_i = 0$ in M. Since $\mathfrak{m} \otimes M \hookrightarrow M$, we have $\sum_{i=1}^n a_i \otimes x_i = 0$, and thus $\sum_{i=1}^n a_i \otimes e_i \in \operatorname{Image}(\mathfrak{m} \otimes K \to \mathfrak{m} \otimes F)$. Thus $x = \sum_{i=1}^n a_i e_i \in \mathfrak{m}K$. □

Theorem 8.9. *For M finitely generated over $(R, \mathfrak{m})$ Noetherian local, TFAE:*
(i) M is free.
(ii) M is projective.
(iii) M is flat.
(iv) $\operatorname{Tor}_1^R(M, R/\mathfrak{m}) = 0$.
(v) $\operatorname{Ext}_R^1(M, R/\mathfrak{m}) = 0$.
(vi) The natural map $\Phi : \mathfrak{m} \otimes_R M \hookrightarrow M$ is an injection.

Proof. (i) $\implies$ (ii) $\implies$ (iii) $\implies$ (iv) are all immediate.
(iv) $\implies$ (vi): Indeed, applying $\cdot \otimes_R M$ to

$$0 \to \mathfrak{m} \to R \to R/\mathfrak{m} \to 0$$

shows that $\operatorname{Ker} \Phi \cong \operatorname{Tor}_1^R(R/\mathfrak{m}, M)$.
(vi) $\implies$ (i) is Lemma 8.8.
(ii) $\implies$ (v) is immediate, since projective modules are acyclic for $\operatorname{Ext}(\cdot, N)$.
(v) $\implies$ (i): By Proposition 8.3 there is an exact sequence

$$0 \to K \to F \to M \to 0$$

with F finitely generated free and $K \subset \mathfrak{m}F$. Applying $\operatorname{Hom}(\cdot, R/\mathfrak{m})$ and using $\operatorname{Ext}_R^1(M, R/\mathfrak{m}) = 0$ gives

$$0 \to \operatorname{Hom}(M, R/\mathfrak{m}) \to \operatorname{Hom}(F, R/\mathfrak{m}) \to \operatorname{Hom}(K, R/mm) \to 0.$$

Thus every homomorphism $f : K \to R/\mathfrak{m}$ is attained from restricting a homomorphism $F \to R/\mathfrak{m}$, but any such map is trivial on $\mathfrak{m}F$ and thus on K: $0 = \operatorname{Hom}(K, R/\mathfrak{m}) = \operatorname{Hom}(K/\mathfrak{m}K, R/\mathfrak{m})$; since $R/\mathfrak{m}$ is a field, this implies $K/\mathfrak{m}K = 0$. On the other hand, since R is Noetherian, K is finitely generated, and then by Nakayama's Lemma $K = 0$, so $F \overset{\sim}{\to} M$ and M is free. $\square$

The following result is a nice indication of how much homological dimension theory simplifies when we restrict to finitely generated modules over a Noetherian local commutative ring!

Theorem 8.10. *For a finitely generated module M over a Noetherian local ring $(R, \mathfrak{m})$ and $n \in \mathbb{N}$, the following are equivalent:*
(i) $\operatorname{pd} M \leq n$.
(ii) $\operatorname{Tor}_{n+1}^R(M, R/\mathfrak{m}) = 0$.
(iii) $\operatorname{Ext}_{n+1}^R(M, R/\mathfrak{m}) = 0$.

Proof. Since M is Noetherian it admits a resolution by finitely generated projective modules; let K_n be the nth syzygy. We claim that all of the conditions are equivalent to: K_n is projective. That this condition is equivalent to (i) is Theorem 7.16 (valid for any module over any ring). As for (ii): by Dimension Shifting for Tor, $\operatorname{Tor}_{n+1}^R(M, R/\mathfrak{m}) = \operatorname{Tor}_1^R(K_n, R/\mathfrak{m})$. Applying Theorem 8.9 we get that $\operatorname{Tor}_{n+1}^R(M, R/\mathfrak{m}) = 0$ iff K_n is projective. The argument for (iii) is identical. $\square$

Corollary 8.11. *Let $(R, \mathfrak{m})$ be a Noetherian local ring. Then:*
a) We have $\operatorname{id} R/\mathfrak{m} = D(R) = \operatorname{pd} R/\mathfrak{m}$.
b) For $n \in \mathbb{N}$, the following are equivalent:
(i) $D(R) \leq n$.
(ii) $\operatorname{Tor}_{n+1}^R(R/\mathfrak{m}, R/\mathfrak{m}) = 0$.
(iii) $\operatorname{Ext}_R^{n+1}(R/\mathfrak{m}, R/\mathfrak{m}) = 0$.

Proof. a) As for any module over any commutative ring, we have $\operatorname{id} R/\mathfrak{m}, \operatorname{pd} R/\mathfrak{m} \leq R$. Conversely, suppose $\operatorname{pd} R/\mathfrak{m} \leq n$. Then for all finitely generated R-modules M, $\operatorname{Tor}_{n+1}^R(M, R/\mathfrak{m}) = 0$, so by Theorem 8.10 $\operatorname{pd} M \leq n$. By Auslander's Theorem $D(R) \leq n$. Finally, suppose $\operatorname{id} R/\mathfrak{m} \leq n$. Then for all finitely generated R-modules M, $\operatorname{Ext}_R^{n+1}(M, R/\mathfrak{m}) = 0$, so again we conclude $\operatorname{pd} M \leq n$ and then $D(R) \leq n$.
b) It is clear that (i) implies both (ii) and (iii). Conversely, if either $\operatorname{Tor}_{n+1}^R(R/\mathfrak{m}, R/\mathfrak{m}) = 0$ or $\operatorname{Ext}_R^{n+1}(R/\mathfrak{m}, R/\mathfrak{m}) = 0$ then by Theorem 8.10 and part a) we have $D(R) = \operatorname{pd} R/\mathfrak{m} \leq n$. $\square$

Lemma 8.12. *Let $(R, \mathfrak{m})$ be Noetherian local. If every element of $\mathfrak{m} \setminus \mathfrak{m}^2$ is a zero-divisor, then there is $a \in R^\bullet$ with $a\mathfrak{m} = 0$.*

Proof. [CA, Cor. 10.8]. $\square$

8.3. **Regular Local Rings.**

Let $(R, \mathfrak{m})$ be a Noetherian local commutative ring.

Lemma 8.13. *Consider the R-module $\mathfrak{m}/\mathfrak{m}^2$.*
a) If $\mathfrak{m}/\mathfrak{m}^2 = 0$, then $\mathfrak{m} = 0$ (i.e., R is a field).
b) $\dim_k \mathfrak{m}/\mathfrak{m}^2$ is finite.
c) $\dim_k \mathfrak{m}/\mathfrak{m}^2$ is equal to the minimal number of generators of the ideal $\mathfrak{m}$.

Proof. a) Apply Corollary X.Xa) to the finitely generated R-module $\mathfrak{m}$.
b) Since R is Noetherian, the ideal $\mathfrak{m}$ is finitely generatd, and certainly any generating set for $\mathfrak{m}$ as an R-module is a generating set for $\mathfrak{m}/\mathfrak{m}^2$ as an $R/\mathfrak{m}$-module.
c) Nakayama's Lemma! $\square$

Definition: For our (Noetherian, local commutative) ring R we put $\dim_e R = \dim_k \mathfrak{m}/\mathfrak{m}^2$, the **embedding dimension** of R.

Corollary 8.14. *We always have* $\dim R \leq \dim_e R$.

Proof. Since $\mathfrak{m}$ is the unique maximal ideal of R, the height of $\mathfrak{m}$ is equal to $\dim R$. Now we can apply Krull's Generalized Principal Ideal Theorem. $\square$

Let M be a finitely generated R-module. An element $a \in R$ is **regular on M** if the endomorphism of M given by $x \mapsto ax$ is injective. (One also says that a is a **non-zerodivisor** on M.)

A finite sequence $a_1, \ldots, a_n$ is **regular on M** if for all $1 \leq i \leq n$, a_i is regular on $M/\langle a_1, \ldots, a_{i-1}\rangle$. A **regular sequence** is a sequence $a_1, \ldots, a_n$ which is regular on R.

Example: Let $R = k[[t_1, \ldots, t_n]]$. Then $t_1, \ldots, t_n$ is a regular sequence.

A **regular local ring** is a Noetherian, local ring $(R, \mathfrak{m})$ with $\dim R = \dim_e R$.

Exercise: a) Show that a zero-dimensional regular local ring is a field.
b) Show that a DVR is a regular local ring.
c) Show that a one-dimensional regular local *domain* is a DVR.

The hypothesis that R be a domain in Exercise X.Xc) is in fact superfluous, as the next result shows.

Theorem 8.15. *A regular local ring is a domain.*

Proof. We go by induction on n. If $n = 0$, then $\dim_e R = 0$, i.e., $\mathfrak{m}/\mathfrak{m}^2 = 0$, and then by Nakayama $\mathfrak{m} = 0$ and R is a field. So suppose that $n > 0$ and that the result holds for regular local rings of dimension $n - 1$.

Let $\operatorname{MinSpec} R = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$. Since $\dim R > 0$, $\mathfrak{m} \supsetneq \mathfrak{p}_i$ for all i; and once again, by Nakayama, $\mathfrak{m} \neq \mathfrak{m}^2$. By Prime Avoidance,[15] Since $x \in \mathfrak{m} \setminus \mathfrak{m}^2$,

$$\dim_e R/(x) = \dim_{R/\mathfrak{m}} \mathfrak{m}/\langle \mathfrak{m}^2, x\rangle = \dim_{R/\mathfrak{m}} (\mathfrak{m}/\mathfrak{m}^2)/((\langle x\rangle + \mathfrak{m}^2)/\mathfrak{m}^2 = \dim_e R - 1.$$

Since R is local and x lies in no minimal prime of R, $\dim R/(x) = \dim R - 1$. Thus $\overline{R} = R/(x)$ is regular local of dimension $n - 1$. By induction, $\overline{R}$ is a domain and thus x is prime. Since again x lie in no minimal prime of R, (x) has height at least one and thus height exactly one by the Krull Hauptidealsatz.

Choose $\mathfrak{q} \in \operatorname{MinSpec} R$ with $\mathfrak{q} \subset (x)$. Then $\mathfrak{q} = (\mathfrak{q} : x)(x)$.[16] Since $\mathfrak{q}$ is prime, we

[15] I found this clever maneuver in online lecture notes of Laura Lynch. The standard argument works with any $x \in \mathfrak{m}\setminus\mathfrak{m}^2$ and eventually succeeds, thus proving something a bit more general...but at the cost of having to develop a lot more background.

[16] Recall that for ideals I and J, $(I : J) = \{y \in R \mid yJ \subset I\}$. Armed only with this definition, verifying the above equality is extremely straightforward.

have $\mathfrak{q} = (\mathfrak{q} : x)$ or $\mathfrak{q} = (x)$;since (x) properly contains $\mathfrak{q}$, we have $\mathfrak{q} = (\mathfrak{q} : x)$. Thus $\mathfrak{q} = (x)\mathfrak{q}$ and, since $x \in \mathfrak{m}$, $\mathfrak{q} = m\mathfrak{q}$. By Nakayama, $\mathfrak{q} = 0$: R is a domain. □

Corollary 8.16. *Let $(R, \mathfrak{m})$ be a regular local ring of dimension $n > 0$. Let $a_1 \in \mathfrak{m} \setminus \mathfrak{m}^2$. Then a_1 is a regular element and $R/(a_1)$ is regular local of dimension $n-1$.*

Proof. Since R is a domain and $a_1 \neq 0$, it is a regular element. Moreover, since R is a domain the unique minimal prime is (0), so the proof of Theorem X.X goes through with any $a_1 \in \mathfrak{m} \setminus \mathfrak{m}^2$. □

Theorem 8.17. *Let $(R, \mathfrak{m})$ be Noetherian local of Krull dimension n. TFAE:*
(i) R is a regular local ring.
(ii) The maximal ideal $\mathfrak{m}$ can be generated by n elements.
(iii) The maximal ideal $\mathfrak{m}$ can be generated by a regular sequence $a_1, \ldots, a_n$.

Proof. (i) $\iff$ (ii): By X.X, $\dim_e R$ is the least number of generators of $\mathfrak{m}$. So if R is regular, $\mathfrak{m}$ can be generated by $\dim_e R = n$ elements. Conversely, by the Krull Hauptidealsatz, $\mathfrak{m}$ requires at least n generators, so if it can be generated by n elements then $n = \dim_e R$.
(i) $\implies$ (iii): The proof of Theorem X.X gives us a regular element $a_1 \in \mathfrak{m}$ such that $R/(a_1)$ is regular local of dimension $n-1$. Performing this procedure $n-1$ more times yields a regular sequence $a_1, \ldots, a_n \in \mathfrak{m}$.
(iii) $\implies$ (ii) is immediate. □

Exercise: Let $(R, \mathfrak{m})$ be a regular local ring of dimension n, and let $a_1, \ldots, a_k \in \mathfrak{m}$.
a) Show that $a_1, \ldots, a_k$ is a regular sequence in $\mathfrak{m}$ iff the images $\overline{a_1}, \ldots, \overline{a_k} \in \mathfrak{m}/\mathfrak{m}^2$ are $R/\mathfrak{m}$-linearly independent.
b) Deduce that if $a_1, \ldots, a_k$ is a regular sequence, $k \leq n$.[17]
c) Deduce that any regular sequence of length n in $\mathfrak{m}$ generates $\mathfrak{m}$.

Theorem 8.18 (Serre, Auslander-Buchsbaum)**.** *Let $(R, \mathfrak{m})$ be Noetherian local.*
a) The following are equivalent:
(i) R is a regular local ring.
(ii) $D(R) < \infty$.
b) When the equivalent conditions of part a) hold, we have $D(R) = \dim R$.

Proof. Let $d = \dim R$. Assume (i) holds. We will prove both (ii) and that $d = D(R)$.

Let $x_1, \ldots, x_d$ be a regular sequence generating $\mathfrak{m}$. Then by Corollary 8.11 and Proposition 7.33 we have

$$D(R) = \operatorname{pd} R/\mathfrak{m} = d < \infty.$$

(ii) $\implies$ (i):
Step 0: Let $n = \operatorname{pd} \mathfrak{m} < \infty$, since $D(R) < \infty$. We first handle the case $n = 0$. Then $\mathfrak{m}$ is free, i.e., is a principal ideal generated by a non-zero-divisor. By Krull's Principal Ideal Theorem, $\mathfrak{m}$ has height at most one and thus $\dim R = 1$. It is easy to see that such a ring is a DVR, hence a regular local ring: e.g. [CA, § 17.5.2].
Now suppose $n > 0$. Applying the Short Exact Sequence Theorem to

$$0 \to \mathfrak{m} \to R \to R/\mathfrak{m} \to 0$$

tells us that $d = D(R) = \operatorname{pd} R/\mathfrak{m} = \operatorname{pd} \mathfrak{m} + 1 = n + 1$.

Put $k = \dim R$. We'll go by induction on k. The case $k = 0$ is trivial: R is

[17]In fact this shows: "a regular local ring is Cohen-Macaulay".

local, commutative and semisimple hence is a field. Suppose the result holds for Noetherian local rings of finite global dimension and of Krull dimension $k-1$.
Step 1: We CLAIM $\mathfrak{m} \setminus \mathfrak{m}^2$ contains a non-zero-divisor.
PROOF OF CLAIM If not, then by Lemma 8.12 there is $a \in R^\bullet$ with $a\mathfrak{m} = 0$. Fix a finitely generated R-module N of projective dimension 1 (such a thing exists: since $n > 0$, there is a finitely generated R-module M with $\operatorname{pd} M = d \geq 1$; let N be the $(d-1)$st syzygy of M). As in Theorem X.X, consider a short exact sequence

$$0 \to K \to F \to N \to 0$$

with F finitely generated free and $K \subset \mathfrak{m}F$. Since K is a first syzygy of N, it is finitely generated projective over the local ring R, so it is free. But on the other hand $aK \subset a\mathfrak{m}F = 0$, so $a \in \operatorname{ann} K$. Nonzero free modules have zero annihilator, so $K = 0$ and $N = F$ is free: contradiction.
Step 2: Fix $x \in \mathfrak{m} \setminus \mathfrak{m}^2$ a non-zero-divisor, and put $\overline{R} = R/(x)$, a Noetherian local ring with maximal ideal $\overline{\mathfrak{m}} = \mathfrak{m}/(x)$. We CLAIM $\overline{\mathfrak{m}}$ isa direct summand of $\mathfrak{m}/x\mathfrak{m}$.
PROOF OF CLAIM Since $x \notin \mathfrak{m}^2$, by Nakayama there is a set of generators $x, y_1, \ldots, y_r$ of $\mathfrak{m}$ mapping to a basis of $\mathfrak{m}/\mathfrak{m}^2$. We now have

$$S + (x) = \mathfrak{m}. \tag{17}$$

Further, we have

$$S \cap (x) = x\mathfrak{m}. \tag{18}$$

Indeed, $x\mathfrak{m} \subset S \cap (x)$ is clear; if $z \in S \cap (x)$, then

$$z = ax = cx + b_1 y_1 + \ldots + b_r y_r, \ c \in \mathfrak{m}, b_i \in R,$$

so $ax - \sum_i b_i y_i \in \mathfrak{m}^2$. Since $x, y_1, \ldots, y_r$ are linearly independentin $\mathfrak{m}/\mathfrak{m}^2$, we get $a \in \mathfrak{m}$ so $z \in x\mathfrak{m}$.

From (18) we deduce

$$\mathfrak{m}/x\mathfrak{m} = (x)/x\mathfrak{m} \oplus S/x\mathfrak{m}$$

and

$$\mathfrak{m}/(x) \cong S/x\mathfrak{m},$$

so $\mathfrak{m}/(x)$ is isomorphic to a direct summand of $\mathfrak{m}/x\mathfrak{m}$.
Step 3: Since (x) is R-free, applying the Short Exact Sequence Theorem to

$$0 \to (x) \to \mathfrak{m} \to \overline{\mathfrak{m}} \to 0$$

shows $\operatorname{pd}_R \overline{\mathfrak{m}} = \operatorname{pd}_R \mathfrak{m} = n$. Moreover by XX and Change of Rings II we have

$$\operatorname{pd}_{\overline{R}} \overline{\mathfrak{m}} \leq \operatorname{pd}_{\overline{R}} \mathfrak{m}/x\mathfrak{m} \leq \operatorname{pd}_R \mathfrak{m} = n < \infty.$$

Thus by Change of Rings I, $\operatorname{pd}_{\overline{R}} \overline{m} = n - 1$. Applying the Short Exact Sequence Theorem again shows $\operatorname{pd}_{\overline{R}} \overline{R}/\overline{m} \leq n < \infty$, so $\overline{R}$ has finite global dimension. Since x is a non-zero-divisor, $\dim \overline{R} = \dim R - 1$, so by induction $\overline{R}$ is a regular local ring with $D(\overline{R}) = \dim \overline{R} = \dim R - 1$. It follows that R is regular local: if $\overline{x_2}, \overline{x_k}$ is a regular sequence generating $\overline{\mathfrak{m}}$, then lifting these elements to $\mathfrak{m}$ gives a regular sequence $x_1, \ldots, x_k$ for $\mathfrak{m}$. $\square$

8.4. **The Auslander-Buchsbaum Theorem.**

In this section we will give a proof – following Samuel following Kaplansky – of what is probably the single deepest result in these notes: the celebrated Auslander-Buchsbaum theorem that a regular local ring is a UFD. Apart from the main result of the previous section the proof will – not so surprisingly – require some side results on UFDs, all of which are covered in the section on UFDs in [CA]. We single out the following results.

Theorem 8.19 (Nagata's Criterion)**.** *Let R be a Noetherian domain. Suppose that $p \in R$ is a prime element such that $R[\frac{1}{p}]$ is a UFD. Then R is a UFD.*

Proof. This is (a special case of) [CA, Thm. 15.39]. □

Proposition 8.20. *For a domain R, the following are equivalent:*
(i) R satisfies the ascending chain condition on principal ideals, and the intersection of any two principal ideals is a principal ideal.
(ii) R is a UFD.

Proof. This is immediate from the results of [CA, § 15.4, 15.5]. □

Theorem 8.21. *(Auslander-Buchsbaum) Every regular local ring is a UFD.*

Proof. We go by induction on the common quantity

$$d = \dim R = D(R) = \dim_e R$$

for a regular local ring $(R, \mathfrak{m})$. As we have seen, $d = 0$ iff R is a field; this disposes of the base case. Suppose now that $d \geq 1$.
Step 1: Consider the short exact sequence

$$0 \to \mathfrak{m} \to R \to R/\mathfrak{m} \to 0.$$

Since R is projective, $\mathfrak{m}$ is the first syzygy of $R/\mathfrak{m}$, whereas by Corollay 8.11, $\operatorname{pd} R/\mathfrak{m} = d$, s $\operatorname{pd} \mathfrak{m} = d - 1$. Let $a_1, \ldots, a_d$ be a regular sequence generating $\mathfrak{m}$; as we have seen, (a_1) is prime. By Nagata's Criterion (Theorem 8.19), it is enough to show that $S = R[\frac{1}{a}]$ is a UFD. Notice that inverting a_1 kills the maximal ideal $\mathfrak{m}$ – or more precisely, makes it the unit ideal – in S, so $\dim S \leq d - 1$. Let $\mathfrak{p} \in \operatorname{MaxSpec} S$, so $S_{\mathfrak{p}} = R_{\mathfrak{p} \cap R}$. Then $\dim S_{\mathfrak{p}} \leq d - 1$, and Serre-Auslander-Buchsbaum, $S_{\mathfrak{p}}$ is a regular local ring, so by induction $S_{\mathfrak{p}}$ is a UFD.
Step 2: We will use Proposition 8.20 to show that S is a UFD. Since R is Noetherian, so is S, so certainly it satisfies ACC on principal ideals. So let $u, v \in S$ and put $\mathfrak{b} = Bu \cap Bv$: we need to show that $\mathfrak{b}$ is principal.
Step 2a: For any $\mathfrak{p} \in \operatorname{MaxSpec} B$, we saw above that $B_{\mathfrak{p}}$ is a UFD, hence by Proposition 8.20 $\mathfrak{b}_p = B_{\mathfrak{p}} u \cap B_{\mathfrak{p}} v$ is principal. By [CA, Thm. 7.21], $\mathfrak{b}$ is a projective module. On the other hand, since R is regular local it has finite global dimension and thus $\mathfrak{b} \cap R$ admits a finite free resolution (FFR). Since S is flat over R, tensoring the FFR from R to S yields a FFR of $\mathfrak{b} = S(\mathfrak{b} \cap R)$. By Serre's Lemma, the FFR projective module $\mathfrak{b}$ is stably free. But by [CA, Prop. 7.14] a stably free *ideal* is a free module, i.e., a principal ideal. Thus $\mathfrak{b}$ is a principal ideal. □

8.5. **Some "Global" Consequences.**

We state a few more important results, mostly without proof. Reasonably elementary proofs can be found in [Lam99, § 2.5].

Theorem 8.22. *Let R be a commutative ring and $S \subset R$ a multiplicatively closed subset. Then $D(S^{-1}R) \leq D(R)$.*

Proof. Suppose $D(R) = n < \infty$. Every $S^{-1}R$-module is of the form $S^{-1}M = S^{-1}R \otimes_R M$ for an R-module M. Let $P_\bullet \to M \to 0$ be a projective resolution of length at most n. Since localization preserves exact sequences and carries projective R-modules to projective $S^{-1}R$-modules (in fact the latter holds for any base change), $S^{-1}P_\bullet \to S^{-1}M \to 0$ is a projective resolution of length at most n. $\square$

Theorem 8.23. *Let R be regular local ring, and let $\mathfrak{p}$ be a prime ideal of R. Then $R_\mathfrak{p}$ is also regular local.*

Proof. By Theorem 8.18, $D(R) < \infty$, so by Theorem 8.22 $D(R_\mathfrak{p}) < \infty$. Since $R_\mathfrak{p}$ is Noetherian local, by Theorem 8.18 $R_\mathfrak{p}$ is regular local. $\square$

Lemma 8.24. *Let R be a commutative Noetherian ring. For any finitely generated R-module M, there is $\mathfrak{m} \in \operatorname{MaxSpec} R$ such that $\operatorname{pd}_R M = \operatorname{pd}_{R_\mathfrak{m}} R_\mathfrak{m}$.*

Theorem 8.25. *Let R be a commutative Noetherian ring.*
a) The following conditions are equivalent:
(i) For all $\mathfrak{p} \in \operatorname{Spec} R$, $R_\mathfrak{p}$ is a regular local ring.
(ii) For all $\mathfrak{m} \in \operatorname{MaxSpec} R$, $R_\mathfrak{m}$ is a regular local ring.
(iii) For every finitely generated R-module M, $\operatorname{pd} M < \infty$.
b) If the equivalent conditions of part a) hold then

$$D(R) = \dim R.$$

Remark: In contrast to the local case, a regular Noetherian ring may have infinite Krull dimension; examples were constructed by Nagata. However, a Noetherian ring of finite Krull dimension is regular iff it has finite global dimension. In particular:

Corollary 8.26. *Let $V_{/k}$ be an affine variety with coordinate ring $k[V]$.*
a) The following are equivalent:
(i) V is nonsingular.
(ii) $D(k[V]) < \infty$.
b) When the conditions of part a) hold, $D(k[V]) = \dim k[V] = \dim V$.

9. Cohomology (and Homology) of Groups

9.1. *G*-modules.

Let G be a monoid. A **G-module** is a commutative group M together with an action of G on M by $\mathbb{Z}$-linear maps, i.e., a homomorphism $\rho : G \to \operatorname{End}_\mathbb{Z}(M)$. We generally write this action as $(g, m) \mapsto g \cdot m$. A homomorphism of G-modules is a homomorphism of abelian groups that respects the group action:

$$gf(x) = f(g \cdot x).$$

Example: Let X be a G-set, i.e., a set X together with a homorphism from G into the monoid of all maps from X to X. There is an associated G-module: the

G-action on X extends uniquely to a G-module structure on $\mathbb{Z}[X]$, the free abelian group on X, namely $g \cdot \sum_{x \in X} n_x[x] = \sum n_x[g \cdot x]$.

Consider the monoid ring $\mathbb{Z}[G]$, which is the set of all finitely nonzero functions $f : G \to \mathbb{Z}$ with pointwise addition and convolution product:

$$(fg)(x) = \sum_{(y,z) \in G^2 \ \mid \ yz = x} f(y)g(z).$$

Equivalently one may view $\mathbb{Z}[G]$ as the collection of formal finite $\mathbb{Z}$-linear combinations of elements of G, with pointwise addition and multiplication given by $[x][y] = [xy]$ and the distributive law. Note that this notation is consistent with the previous paragraph in the sense that indeed M is a basis for the $\mathbb{Z}$-module $\mathbb{Z}[G]$.

More generally, for any commutative ring k, one can form the monoid ring $k[G]$.

Exercise: a) Prove the universal property of monoid rings: for any ring B,

$$\mathrm{Hom}_{\mathrm{Rings}}(k[G], B) = \mathrm{Hom}_{\mathrm{Monoids}}(G, (B, \cdot)).$$

b) Deduce that every G-module M has the natural structure of a left $\mathbb{Z}[G]$-module, and conversely. (Hint: apply part a) to the endomorphism ring $\mathrm{End}_{\mathbb{Z}}(M)$.)

Exercise: a) Suppose that $M \cong (\mathbb{N}, +)$. Show that $\mathbb{Z}[M] \cong \mathbb{Z}[t]$, the univariate polynomial ring.
b) Suppose $M \cong (\mathbb{Z}, +)$. Show that $\mathbb{Z}[M] \cong \mathbb{Z}[t, t^{-1}]$, the ring of univariate Laurent polynomials.
c) Let M and N be monoids. Show that as rings, $\mathbb{Z}[M \times N] \cong \mathbb{Z}[M] \otimes_{\mathbb{Z}} \mathbb{Z}[N]$.
d) Show that any polynomial ring $\mathbb{Z}[t_1, \ldots, t_n]$ is isomorphic to a monoid ring.

Henceforth we will restrict attention to the case in which G is a group!

9.2. **Introducing Group Co/homology.**

For any G-module M, we define the **G-invariants**

$$M^G = \{x \in M \mid gx = x \forall g \in G\};$$

it is the largest G-submodule of M on which G acts trivially. Similarly, we define the **G-coinvariants**

$$M_G = M / \langle gx - x \mid g \in G, \ x \in M \rangle;$$

it is the largest quotient module on which G acts trivially.

Exercise: a) Show that $M \mapsto M^G$ is a left exact covariant functor from the category of $\mathbb{Z}[G]$-modules to the category of $\mathbb{Z}$-modules.
b) Show that $M \mapsto M_G$ is a right exact covariant functor from the category of $\mathbb{Z}[G]$-modules to the category of $\mathbb{Z}$-modules.

For all $n \geq 0$, we put $H^n(G, M) = R^n F(M)$, the nth right derived functor of $F(M) = M^G$, the **nth cohomology group of G with coefficients in M**.

For all $n \geq 0$, we put $H_n(G, M) = L_n F(M)$, the nth left derived functor of

$F(M) = M_G$, the **nth homology group of G with coefficients in M**.

Group co/homology is the study of these functors. Of course the burden is on us to explain why these particular derived functors are of interest. In brief preview:
• The homology and cohomology groups $H_n(G,\mathbb{Z})$ and $H^n(G,\mathbb{Z})$ are of fundamental importance in topology, as they turn out to be nothing else than the homology and cohomology groups of the Eilenberg-MacLane space $K(G,1)$. (More generally, for a G-module M, $H_n(G,M)$ and $H^n(G,M)$ are homology and cohomology of **local systems** on the space $K(G,1)$.) This gives a beautiful and powerful connection between algebra and topology – maybe the single most beautiful and powerful one!
• We will soon see that group homology can be understood in terms of Tor functors over $\mathbb{Z}[G]$ and group cohomology can be understood in terms of Ext functors over $\mathbb{Z}[G]$. This allows us to fruitfully apply many of our earlier tools.
• Group cohomology is related to **group extensions**, one of the fundamental concepts in pure group theory.
• Galois cohomology – roughly, group cohomology with G equal to the automorphism group of a Galois extension of fields – is of the utmost importance in modern number theory. For instance, the modern formulation of **class field theory**, due to Artin and Tate, places the entire theory in the context of the cohomology theory of finite Galois groups.

9.3. More on the Group Ring.

Let G be a group, and consider $R = \mathbb{Z}[G]$.

If G is finite, we define the **norm element** $N = \sum_{g\in G}[g] \in \mathbb{Z}[G]$. Note that $N \in \mathbb{Z}[G]^G$. This is an instance of a ubiquitous trick in mathematics: when G acts on an object X, to get a subobject which is invariant under G, start with any subobject and sum (or average) it over the orbit of G. It follows that the G-submodule $\mathbb{Z}[G]N$ generated by N is simply $\{nN \mid n \in \mathbb{Z}\}$.

Exercise: a) Let G be a finite group. Show: $\mathbb{Z}[G]^G = \mathbb{Z}[G]N$.
b) Let G be an infinite group. Show: $\mathbb{Z}[G]^G = 0$.

The augmentation map: using the universal property of the group ring, there is a unique ring homomorphism $\Sigma : \mathbb{Z}[G] \to \mathbb{Z}$ with $\Sigma(g) = 1$ for all $g \in G$. If we think of the elements of $\mathbb{Z}[G]$ as formal finite $\mathbb{Z}$-linear combinations of elements of G, then Σ simply adds up the $\mathbb{Z}$-coefficients:

$$\Sigma(\sum_{g\in G} n_g[g]) = \sum_{g\in G} n_g.$$

Since $\Sigma(n[1]) = n$, Σ is surjective. Let $I = \ker \Sigma$, the **augmentation ideal**. Thus we have a short exact sequence of R-modules

$$0 \to I \to \mathbb{Z}[G] \to \mathbb{Z} \to 0 \tag{19}$$

Σ endows $\mathbb{Z}$ with the structure of a $\mathbb{Z}[G]$-module: the G-action is trivial.

Lemma 9.1. *Let $I = \operatorname{Ker}\Sigma$ be the augmentation ideal of $\mathbb{Z}[G]$.*
a) I is a free $\mathbb{Z}$-module with $\mathbb{Z}$-basis $\{[g]-[1] \mid g \in G^\bullet\}$.

b) If S is a generating set for G, then $\{[s]-[1] \mid s \in S\}$ is a spanning set for I as a $\mathbb{Z}[G]$-module.

Exercise: Prove Lemma 9.1

Proposition 9.2. *Let M be a left $\mathbb{Z}[G]$-module. Then:*
a) $M^G = \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, M)$.
b) $M_G = \mathbb{Z} \otimes_{\mathbb{Z}[G]} M$.

Proof. a) Let $\varphi : \mathbb{Z} \to M$ be a G-module map. In particular it is a $\mathbb{Z}$-module map, hence is determined by $\varphi(1)$. The condition that it be a G-map is $g\varphi(1) = \varphi(g \cdot 1) = \varphi(1)$: that is, $\varphi(1)$ must be a G-invariant element of M.
b) In view of Lemma X.X, we have

$$M_G = M/IM = \mathbb{Z}[G]/I \otimes_R M = \mathbb{Z} \otimes_R M.$$

□

We immediately deduce the following fundamental result.

Theorem 9.3. *Let M be a G-module, and let $n \in \mathbb{N}$. Then:*
a) $H^n(G, M) = \mathrm{Ext}^n_{\mathbb{Z}[G]}(\mathbb{Z}, M)$.
b) $H_n(G, M) = \mathrm{Tor}_n^{\mathbb{Z}[G]}(\mathbb{Z}, M)$.

Thus we can – in principle, at least – compute both group homology and group cohomology using a projective resolution of $\mathbb{Z}$ over $\mathbb{Z}[G]$.

The group ring construction is actually a functor from the category of groups to the category of rings: in other words, a group homomorphism $G \to G'$ naturally induces a ring homomrphism $\mathbb{Z}[G] \to \mathbb{Z}[G']$.

Lemma 9.4. *Let $H \hookrightarrow G$ be an injective group homomorphism. Let X be a set of coset representatives for H in G. Then $\mathbb{Z}[G]$ is a free $\mathbb{Z}[H]$-module with basis $\{[x] \mid x \in X\}$.*

Exercise: Prove it.

9.4. **First Examples.**

Proposition 9.5. *For any group G, $H_1(G, \mathbb{Z}) \cong I/I^2 \cong G^{\mathrm{ab}}$.*

Proof. Step 1: By X.X, $H_1(G, \mathbb{Z}) \cong \mathrm{Tor}_1^{\mathbb{Z}[G]}(\mathbb{Z}, \mathbb{Z})$. To compute this, we apply $\mathrm{Tor}_*(\cdot, \mathbb{Z})$ to the augmentation sequence, getting

$$0 = \mathrm{Tor}_1(\mathbb{Z}[G], \mathbb{Z}) \to I/I^2 \to \mathbb{Z} \stackrel{1}{\mathbb{Z}} \to 0,$$

so $\mathrm{Tor}_1(\mathbb{Z}, \mathbb{Z}) \cong I/I^2$.
Step 2: We define a map $\Phi : G \to I/I^2$ by $\Phi(g) = g - 1$. Then

$$\Phi(gh) = gh - 1 = (g-1) + (h-1) - (g-1)(h-1) \equiv \Phi(g) + \Phi(h) \pmod{I^2},$$

so it is a homomorphism.
Step 3: Since $\{[g]-[1] \mid g \neq 1 \in G\}$ is a $\mathbb{Z}$-basis for I, there is a unique $\mathbb{Z}$-module map $\Psi : I \to G^{\mathrm{ab}}$ with $\Psi([g]-[1]) = g[G, G]$. It is immediate that Φ and Ψ are mutually inverse maps, so each is an isomorphism of commutative groups. □

Theorem 9.6. *(Schur-Hopf) Let G be a group. Write G as the quotient of a free group F by a normal subgroup R. Then*

$$H_2(G, \mathbb{Z}) \cong (R \cong [F, F])/[F, R].$$

Example: Let $G = \langle \sigma \rangle$ be infinite cyclic. By Lemma X.X, I is the principal ideal generated by $[\sigma] - [1]$. Since $\mathbb{Z}[G] \cong \mathbb{Z}[t, t^{-1}]$ is a domain, we must have $I \cong \mathbb{Z}[G]$ and thus

$$0 \to \mathbb{Z}[G] \stackrel{\cdot[\sigma]-[1]}{\to} \mathbb{Z}[G] \to \mathbb{Z} \to 0$$

is a free resolution of $\mathbb{Z}$ as a $\mathbb{Z}[G]$-module. Let M be any G-module. Then $H_\bullet(G, M)$ is the homology of the complex

$$0 \to M \stackrel{[\sigma]-[1]}{\to} M \to 0,$$

so

$$H_0(G, M) = M/(\sigma - 1)M = M_G.$$

$$H_1(G, M) = M^G,$$

$$\forall n \geq 2, \ H_n(G, M) = 0.$$

Similarly, $H^\bullet(G, M)$ is the cohomology of the complex

$$0 \to \operatorname{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G], M) \stackrel{[\sigma]-[1]}{\to} \operatorname{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G], M) \to 0,$$

so

$$H^0(G, M) = M^G,$$

$$H^1(G, M) = M_G,$$

$$\forall n \geq 2, \ H^n(G, M) = 0.$$

Exercise: Let $G = \langle \sigma \rangle$.
a) Show that $\operatorname{cd} G = 1$.
b) Show that $D(\mathbb{Z}[G]) = 2$.
(Thus we have an example of $\operatorname{cd} G < D(\mathbb{Z}[G])$).

Proposition 9.7. *Let $n \in \mathbb{Z}^+$ and let $G = \langle \sigma \mid \sigma^n = 1 \rangle$. For any G-module M:*
a) $H_0(G, M) = M_G = M/(\sigma - 1)M$
b) $H_n(G, M) = M^G/NM, \ n = 1, 3, 5, 7, \ldots$
c) $H_n(G, M) = (\operatorname{Ker} N)/(\sigma - 1)M, \ n = 2, 4, 6, 8, \ldots$
d) $H^0(G, M) = M^G$.
e) $H^n(G, M) = (\operatorname{Ker} N)/(\sigma - 1)M, \ n = 1, 3, 5, 7, \ldots$
f) $H^n(G, M) = M^G/NM, \ n = 2, 4, 6, 8, \ldots$

Proof. The Kaplansky pair $(\sigma - 1, 1 + \sigma + \ldots + \sigma^{n-1} = N)$ in $\mathbb{Z}[G]$ gives us a free resolution of $\mathbb{Z}$ over $\mathbb{Z}[G]$:

$$\mathbb{Z}[G] \stackrel{N}{\to} \mathbb{Z}[G] \stackrel{\sigma-1}{\to} \mathbb{Z}[G] \stackrel{N=\Sigma}{\to} \mathbb{Z} \to 0.$$

Applying $\cdot \otimes_{\mathbb{Z}[G]} M$ and taking homology, we get that if n is odd,

$$H_n(G, M) = (\operatorname{Ker} N)/(\operatorname{Im} \sigma - 1) = (\operatorname{Ker} N)/(\sigma - 1)M,$$

as claimed, whereas if n is even,

$$H_n(G, M) = \operatorname{Ker}(\sigma - 1)/(\operatorname{Image} N) = M^G/NM,$$

as claimed. Applying $\operatorname{Hom}_{\mathbb{Z}[G]}(\cdot, M)$ and taking cohomology, we get parts a) and b). Applying $\operatorname{Hom}_{\mathbb{Z}[G]}(\cdot, M)$ we get parts c) and d). $\square$

Note that the homology and cohomology groups turned out to be the same, only with shifted indices. Also from this perspective $H_0(G, M)$ and $H^0(G, M)$ are disappointing outliers. It is natural to want to redefine them in such a way that the co/homology is truly periodic. This leads us to a definition we will explore later:

If G is a finite group and M a G-module, we define **Tate cohomology groups**:

$$\hat{H}^n(G, M) = H^n(G, M), \; n > 0,$$
$$\hat{H}^0(G, M) = M^G/NM.$$
$$\hat{H}^{-1}(G, M) = (\operatorname{Ker} N)/IM.$$
$$\hat{H}^n(G, M) = H_{1-n}(G, M), \; n \leq -2.$$

Exercise: For G finite, show that a short exact sequence of G-modules

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

leads to a doubly infinite long exact sequence in Tate cohomology.

Proposition 9.8. *Let $G = F(S)$ be the free*[18] *group on the set S. Then:*
a) The augmentation ideal I is a free $\mathbb{Z}[G]$-module, with basis $\{[s] - [1] \mid s \in S\}$.
b) Thus

$$0 \to I \to \mathbb{Z}[G] \to \mathbb{Z} \to 0$$

is a free resolution of $\mathbb{Z}$ over $\mathbb{Z}[G]$.
c) For all $n > 1$ and all G-modules M,

$$H_n(G, M) = H^n(G, M) = 0.$$

Proof. a) For a purely algebraic proof, see [W, Prop. 6.2.6]. Later we will give a topological proof!
b) and c) both follow immediately. □

9.5. **Cohomological Dimension.**

For a group G, the **cohomological dimension** $\operatorname{cd} G$ is the projective dimension of $\mathbb{Z}$ as a $\mathbb{Z}[G]$-module.

Proposition 9.9. *For a group G, the following are equivalent:*
(i) The augmentation sequence (19) splits.
(ii G is trivial.

Proof. (i) $\implies$ (ii): A section $\sigma : \mathbb{Z} \to \mathbb{Z}[G]$ of the augmentation map Σ amounts to an element $x \in \mathbb{Z}[G]^G$ with $\Sigma(x) = 1$. If G is infinite, then by Exercise X.X, $\mathbb{Z}[G]^G = 0$ and that ends that. Suppose now that G is finite of order $n > 1$. Then $\mathbb{Z}[G]^G = \mathbb{Z}[G]N$, where $N = \sum_{g \in G}[g]$ is the norm element. Thus $\Sigma(\mathbb{Z}[G]^G) = \Sigma(N)\mathbb{Z} = n\mathbb{Z}$, so there is no G-fixed element x with $\Sigma(x) = 1$.
(ii) $\implies$ (i): $\mathbb{Z}$ is a projective $\mathbb{Z}$-module. □

Exercise: a) Show that $\operatorname{cd} G \leq D(\mathbb{Z}[G])$.
b) Show that $\operatorname{cd} G = 0 \iff G$ is trivial.
(Note that if G is trivial, $0 = \operatorname{cd} G < D(\mathbb{Z}[G]) = D(\mathbb{Z}) = 1$.
c) Show that $\operatorname{cd} G$ is the supremum of the set of all natural numbers n such that $H^n(G, M) \neq 0$ for some G-module M.

[18] Not the free abelian group!

Exercise: Let G be a nontrivial finite cyclic group. Show
$$\operatorname{cd} G = D(\mathbb{Z}[G]) = \infty.$$

Exercise: Let G be an infinite cyclic group. Show
$$\operatorname{cd} G = 1 < 2 = D(\mathbb{Z}[G]).$$

Exercise: Let $G = F(S)$ be a free group.
a) Show $\operatorname{cd} G = 1$.
b) What is $D(\mathbb{Z}[G])$?

In fact the converse also holds.

Theorem 9.10. *(Stallings-Swan) If $\operatorname{cd} G \leq 1$, then G is free.*

Proof. The finitely generated case is due to J.R. Stallings [St68]. The general case is due to R.G. Swan [Sw69]. Both arguments are long and difficult. According to `http://mathoverflow.net/questions/95974` there is still no easy proof. □

Exercise: Let G be a group; let $I \subset \mathbb{Z}[G]$ be the augmentation ideal. Show TFAE:
(i) G is free (as a group).
(ii) I is free (as a $\mathbb{Z}[G]$-module).
(iii) I is projective (as a $\mathbb{Z}[G]$-module).

Theorem 9.11. *Let H be a subgroup of G.*
a) We have $\operatorname{cd} H \leq \operatorname{cd} G$.
b) If $\operatorname{cd} G < \infty$, then G is torsionfree.

Exercise:
a) Deduce from Theorems 9.10 and 9.11 that any subgroup of a free group is free. (This is ridiculous overkill. In fact it is likely that it is logically circular: I would be surprised if the proof of Stallings-Swan did not make use of this basic fact.)
b) Fill in the details for the following (rather standard) topological proof that subgroups of free groups are free.
Step 1: Let S be a set, and let X be the topological space obtained by wedging together $\#S$ circles. Show that $\pi_1(X) \cong F(S)$, the free group on S.
Step 2: Let X be a connected one-dimensional CW-complex. Show that X is homotopy equivalent to a (possibly) infinite wedge of circles. (Hint: find a maximal subtree.) Deduce that $\pi_1(X)$ is free.
Step 3: Let $Y \to X$ be a covering space of a connected one-dimensional CW-complex. Show (or notice: this is almost trivial) that Y naturally has the structure of a one-dimensional CW-complex. Deduce that $\pi(Y)$ is free.
Step 4: Conclude that any subgroup of a free group is free.

Theorem 9.12. *(Serre) Let G be a torsionfree group and H a finite index subgroup. Then $\operatorname{cd} G = \operatorname{cd} H$.*

The proof of Theorem 9.12 is beyond our means, but see e.g. [Br].

Combining the theorems of Stallings-Swan and Serre, we get the following remarkable result of pure group theory.

Corollary 9.13. *A torsionfree group admitting a finite index free subgroup is free.*

Example: The modular group $\mathrm{PSL}_2(\mathbb{Z})$ has an index 6 normal subgroup $\Gamma(2)$ which is free on 2 generators. However, $\Gamma(1) = \mathrm{PSL}_2(\mathbb{Z})$ has elements of order 2 and 3: in fact it is the free product $C_2 * C_3$. So "torsionfree" is certainly necessary in the statement of Corollary 9.13.

9.6. **Products.**

Let G_1 and G_2 be groups. If we understand the co/homology groups of G_1 and G_2, it is certainly natural to try to understand the co/homolohy groups of $G = G_1 \times G_2$ in terms of them. This is a classic application of the Künneth Formula for chain complexes, although it takes a little work to see how it applies. Here is the main result.

Theorem 9.14. *Let $P_\bullet$ be a projective resolution for $\mathbb{Z}$ over $\mathbb{Z}[G_1]$ and $Q_\bullet$ be a projective resolution for $\mathbb{Z}$ over $\mathbb{Z}[G_2]$.*
a) Then $P_\bullet \otimes_{\mathbb{Z}} Q_\bullet$ is a projective resolution for $\mathbb{Z}$ over $\mathbb{Z}[G_1 \times G_2]$.
b) For all $n \in \mathbb{N}$, we have

$$H_n(G_1 \times G_2, \mathbb{Z}) \cong \bigoplus_{p+q=n} H_p(G_1,\mathbb{Z}) \otimes_{\mathbb{Z}} H_q(G_2,\mathbb{Z}) \oplus \bigoplus_{p+q=n-1} \mathrm{Tor}_1^{\mathbb{Z}}(H_p(G_1,\mathbb{Z}), H_q(G_2,\mathbb{Z})).$$

c) For all $n \in \mathbb{N}$, we have

$$H^n(G_1 \times G_2, \mathbb{Z}) \cong \bigoplus_{p+q=n} H^p(G_1,\mathbb{Z}) \otimes_{\mathbb{Z}} H^q(G_2,\mathbb{Z}) \oplus \bigoplus_{p+q=n-1} \mathrm{Ext}_1^{\mathbb{Z}}(H^p(G_1,\mathbb{Z}), H^q(G_2,\mathbb{Z})).$$

Proof. We remind the reader of our convention on tensor products of G-modules: if we don't write any subscript, we mean tensor product over $\mathbb{Z}$.
a) Clearly our first order of business is to make sense of the claim that $P_\bullet \otimes Q_\bullet$ is a complex of $\mathbb{Z}[G]$-modules. The key observation here is that $\mathbb{Z}[G_1] \otimes \mathbb{Z}[G_2]$ is canonically isomorphic to $\mathbb{Z}[G_1 \times G_2]$: we map $[g_1] \otimes [g_2]$ to (g_1, g_2). Thus it is enough to observe that for any rings R_1 and R_2, if M_1 is an R_1-module and M_2 is an R_2-module, then $M_1 \otimes_{\mathbb{Z}} M_2$ is an $R_1 \otimes_{\mathbb{Z}} R_2$-module, where the latter tensor product has a natural ring structure. This does the job.

Next we need to see that for all $n \in \mathbb{N}$, $(P_\bullet \otimes Q_\bullet)_n$ is projective. This comes down to checking that if M_1 is a projective R_1-module and M_2 is a projective R_2-module, then $M_1 \otimes M_2$ is a projective $R_1 \otimes R_2$ module, which is very easy: using the characterization of projective modules as direct summands of free modules we reduce to the corresponding statement for free modules and then to the statement that $R_1 \otimes R_2$ is a free $R_1 \otimes R_2$-module: of course it is.

Finally we need to see that the complex $P_\bullet \otimes Q_\bullet$ is exact. For this we first observe that exactness of a complex of R-modules may be checked by considering it as a complex of $\mathbb{Z}$-modules. Then we apply the Künneth Formula for chain complexes, which gives in particular that if $P_\bullet$ is an acyclic complex of $\mathbb{Z}$-modules, then its tensor product with *any* chain complex of $\mathbb{Z}$-modules remains acyclic. (The clean way to do this is to apply it to the tensor product of the augmented complexes $P_\bullet \to \mathbb{Z} \to 0$ and $Q_\bullet \to \mathbb{Z} \to 0$; otherwise we need to check the degree zero part separately.)
b) By part a), $H_*(G, \mathbb{Z})$ is the homology of the complex

$$(P_\bullet \otimes Q_\bullet) \otimes_{\mathbb{Z}[G_1] \otimes \mathbb{Z}[G_2]} \mathbb{Z} \cong (P_\bullet \otimes_{\mathbb{Z}[G_1]} \mathbb{Z}) \otimes_{\mathbb{Z}} (Q_\bullet \otimes_{\mathbb{Z}[G_2]} \mathbb{Z}).$$

Noting that all chain complexes in sight are chain complexes of free $\mathbb{Z}$-modules, the Künneth Formula for complexes of $\mathbb{Z}$-modules applies to give the claimed result.
c) This is exactly the same as part b), but using the Künneth Formula for Cohomology. $\square$

Corollary 9.15. *For any groups G_1 and G_2, we have*

$$\mathrm{cd}(G_1 \times G_2) \leq \mathrm{cd}\, G_1 + \mathrm{cd}\, G_2.$$

Exercise: Prove it.

Corollary 9.16. *For any $d \in \mathbb{N}$, $\mathrm{cd}(\mathbb{Z}^d) = d$.*

Exercise: Prove it.

Exercise: Try to use the above ideas to explicitly compute $H_n(\mathbb{Z}^d, M)$ and $H^n(\mathbb{Z}^d, M)$ for all $d, n \in \mathbb{N}$ and all $\mathbb{Z}^d$-modules M.

Exercise: Can you find groups G_1 and G_2 with $\mathrm{cd}(G_1 \times G_2) < \mathrm{cd}\, G_1 + \mathrm{cd}\, G_2$?

10. Functorialities in Group Co/homology

10.1. **Induction, Coinduction and Eckmann-Shapiro.**

Let H be a subgroup of a group G, and let A be an H-module. We can manufacture from A a G-module in the following two important ways:

$$\mathrm{Ind}_H^G A = \mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} A.$$

Here the G-module structure comes from the left action of G on $\mathbb{Z}[G]$ (or, in more technical terms that amount to the same thing, from the fact that $\mathbb{Z}[G]$ is a $(\mathbb{Z}[G], \mathbb{Z}[G])$-bimodule). Such G-modules are said to be **induced from H**. The special case in which H is the trivial group – i.e., A is just a $\mathbb{Z}$-module – is itself of some importance, and we put

$$\mathrm{Ind}^G A = \mathbb{Z}[G] \otimes_{\mathbb{Z}} A$$

and simply say that A is **induced**.

On the other hand, we put

$$\mathrm{Coind}_H^G A = \mathrm{Hom}_{\mathbb{Z}[H]}(\mathbb{Z}[G], A).$$

The G-action here is $g \cdot f : x \mapsto f(xg)$.[19] Such modules are said to be **coinduced from H**. Again, when H is trivial we put

$$\mathrm{Coind}^G A = \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], A)$$

such modules are said to be **coinduced**.

Free $\mathbb{Z}[G]$-modules are precisely those which are induced from free $\mathbb{Z}$-modules. In general an induced G-module need not be free: for instance free $\mathbb{Z}[G]$-modules are free $\mathbb{Z}$-modules and thus $\mathbb{Z}$-torsionfree, but if A has $\mathbb{Z}$-torsion then so does $\mathrm{Ind}^G A$.

[19]Note that this is an instance of switching from a left action by g^{-1} to a right action by g.

Remark: As for most of the constructions introduced here, induction and coinduction can also be defined for $k[G]$-modules, where k is a field. We recover the key concept in representation theory: if W is a finite-dimensional k-vector space with k-linear H-action, then

$$V = \mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} W$$

is the **induced representation**. Recall that the most classical setting for reprsentation is when G is finite and $k = \mathbb{C}$. Then much of the core of the subject describes how represntations of G can be obtained as induced representations from various (simpler) subgroups. More specifically, at least to the extent of my own knowledge of the subject, the two Fundamental Theorems in this subject are the following.

Theorem 10.1. *(Artin's Induction Theorem) Let G be a finite group, and let V be a finite-dimensional $\mathbb{C}$-representation of G. Then V is a $\mathbb{Q}$-linear combination of representations of the form $\operatorname{Ind}_H^G W$, where W is a one-dimensional representation of a cyclic subgroup H of G.*

What do we mean by a $\mathbb{Q}$-linear combination of representations? The traditional answer is that a finite-dimensional complex representation (V, ρ) of a finite group G is determined by its **character** $\chi : G \to \mathbb{C}$, $\chi(g) = \operatorname{trace}(g\bullet)$. Then the $\mathbb{Q}$-linear combination business can be interpreted in terms of the corresponding characters.

However there is another way. Suppose, to fix ideas, that there are $a_1, \ldots, a_n \in \mathbb{Q}$ and representations $\chi_1, \ldots, \chi_n$ of cyclic subgroups $H_1, \ldots, H_n$ of G such that

$$\chi = \sum_{i=1}^{n} a_i \operatorname{Ind}_{H_i}^G \chi_i.$$

Let N be the least common multiple of $a_1, \ldots, a_n$. Then

$$N\chi = \sum_{i=1}^{n} N a_i \operatorname{Ind}_{H_i}^G \chi_i = \sum_{i=1}^{n} b_i \operatorname{Ind}_{H_i}^G \chi_i,$$

say, where $b_i = N a_i \in \mathbb{Z}$. Some coefficients b_i may be negative; if so we bring them to the other side, finally getting an equation of the form

$$\bigoplus_{i=1}^{r} c_i \operatorname{Ind}_{H_i}^G \chi_i \oplus N\chi = \bigoplus_{i=1}^{s} d_i \operatorname{Ind}_{H_i}^G \chi_i$$

with $c_i, d_i \in \mathbb{Z}^+$. At last we can interpret this in terms of honest direct sums of $\mathbb{C}[G]$-modules, and this is at least a consequence of Artin's Theorem whose statement is "character-free". In fact it is an equivalent version of Artin's theorem since we can solve it for the character of χ and the character determines the representation up to isomorphism. But *in fact* it is a nice exercise to prove this directly.

Exercise: Let G be a finite group, and let k be a field. We assume that $\operatorname{char} k \nmid \#G$ ("nonmodular case"). Let A, M_1, M_2 be $k[G]$-modules. Suppose that for some $n \in \mathbb{Z}^+$ we have

$$A \oplus \bigoplus_{i=1}^{n} M_1 \cong A \oplus \bigoplus_{i=1}^{n} M_2.$$

Show that $M_1 \cong M_2$. (Hint: the hypotheses on k and G are precisely those of Maschke's Theorem.)

Nevertheless it would be nicer to have a $\mathbb{Z}$-linear combination than a $\mathbb{Q}$-linear combination. A related theorem of Brauer accomplishes this. We say that a finite group is **elementary** if it is the direct product of a cyclic group and a p-group.

Theorem 10.2. *(Brauer's Induction Theorem) Let G be a finite group, and let V be a finite-dimensional $\mathbb{C}$-representation of G. Then V is a $\mathbb{Z}$-linear combination of representations of the form $\operatorname{Ind}_H^G W$, where W is a one-dimensional representation of an elementary subgroup H of G.*

Exercise: If you are a number theorist, look up the history of Brauer's Induction Theorem and in particular, how it was used to prove a special case of **Artin's Holomorphy Conjecture**.

The proverbial alert reader may have noticed that the entire discussion was about induced representations, not coinduced representations $\operatorname{Hom}_{k[H]}(k[G], W)$. Even if you know classical representation theory the term "coinduction" may not ring a bell. The following result explains why.

Lemma 10.3. *If H is a finite index subgroup of a group G and A is an H-module,*
$$\operatorname{Coind}_H^G A. \cong_{\mathbb{Z}[G]} \operatorname{Ind}_H^G A.$$

Proof. We define
$$\Phi : \operatorname{Coind}_H^G A \to \operatorname{Ind}_H^G A,\ (f : \mathbb{Z}[G] \to A) \mapsto \sum_{g \in H\backslash G} g^{-1} \otimes_{\mathbb{Z}[H]} f(g).$$
The sum extends over any system of right coset representatives for H in G. Let's check that this is well-defined. If instead of g we took hg for any $h \in H$, then we would replace $g^{-1} \otimes_{\mathbb{Z}[H]} f(g)$ with $(hg)^{-1} \otimes_{\mathbb{Z}[H]} f(hg) = g^{-1}h^{-1} \otimes_{\mathbb{Z}[H]} hf(g)$, but by bringing the h across the tensor product the latter becomes equal to the former.

Next we check the G-equivariance of Φ: for $g' \in G$,
$$\Phi(g'f) = \sum_{g \in H\backslash G} g^{-1} \otimes_{\mathbb{Z}[H]} f(gg') = g' \sum_{g \in H\backslash G} (gg')^{-1} \otimes f(gg') = g'\Phi(f).$$
On the other hand, we define a map $\Psi : \operatorname{Ind}_H^G A \to \operatorname{Coind}_H^G A$ by
$$\sum_{g \in H\backslash G} g^{-1} \otimes_{\mathbb{Z}[H]} b_g \mapsto (g \mapsto b_g).$$
Again one needs to check that this map is well-defined if we switch from g to hg, and this is very similar to the above: since
$$g^{-1} \otimes_{\mathbb{Z}[H]} b_g = g^{-1}h^{-1} \otimes_{\mathbb{Z}[H]} hb_g = (hg)^{-1}hb_g,$$
we have $b_{hg} = hb_g$, and so
$$f(hg) = b_{hg} = hb_g = hf(g)$$
as needed. To check G-equivariance of Ψ, let $x = \sum_{g \in G/H} g^{-1} \otimes_{\mathbb{Z}[H]} b_g$ and let $g' \in G$. Then
$$g'x = \sum_g g'g^{-1} \otimes b_g = \sum_{gg'} g'(gg')^{-1} \otimes b_{gg'} = \sum_g g^{-1} \otimes b_{gg'},$$
so $\Psi(g'x) : g \mapsto b_{gg'}$, while
$$g'\Psi(x) : g' \cdot (g \mapsto b_g) = g \mapsto b_{gg'}.$$
As it is evident that Φ and Ψ are mutually inverse, we're done. $\square$

Exercise: Where in the proof did we use that H has finite index in G?

Warning: When G is finite, it is unfortunately rather standard to *refer to* $\mathrm{Hom}_{\mathbb{Z}[H]}(\mathbb{Z}[G], A)$ as "induced". For instance, Serre does (the profinite analogue of) this in [S-CG, § I.2.5], but at least he mentions that this construction is what he called coinduction in [S-CL]. Some other authors are not this careful.

Theorem 10.4. *(Eckmann-Fadeev-Shapiro Lemma)*
Let $H \subset G$, let M be a G-module and let N be an H-module.
a) For all $n \geq 0$, there are canonical isomorphisms

$$\mathrm{Tor}_n^{\mathbb{Z}[G]}(M, \mathrm{Ind}_H^G N) \cong \ Tor_n^{\mathbb{Z}[H]}(M, N).$$

$$\mathrm{Ext}^n_{\mathbb{Z}[G]}(M, \mathrm{Coind}_H^G N) \cong \mathrm{Ext}^n_{\mathbb{Z}[H]}(M, N).$$

b) In particular, for all H-modules N, we have

$$H_*(G, \mathrm{Ind}_H^G N) \cong H_*(H, N),$$

$$H^*(G, \mathrm{Coind}\, N) \cong H^*(H, N)$$

Proof. Consider the ring map $\mathbb{Z}[H] \to \mathbb{Z}[G]$. Then $\mathbb{Z}[G]$ is a free $\mathbb{Z}[H]$ bimodule: in particular it is projective and flat on both sides.
a) Apply Base Change for Tor and Ext (Theorems 6.12 and 6.19) with $R = \mathbb{Z}[H]$, $T = \mathbb{Z}[G]$.
b) This follows immediately. □

Corollary 10.5. *a) An induced G-module is acyclic for group homology.*
b) A coinduced G-module is acyclic for group cohomology.

Exercise: Prove it.

Exercise: Let M be a G-module.
a) Show that M is *canonically* the quotient of an induced G-module ....
b) Show that M is *canonically* a submodule of a coinduced G-module....

Remark: Our treatment of the Eckmann-Shapiro Lemma was directly inspired by the wikipedia article `http://en.wikipedia.org/wiki/Shapiro's_lemma`. In particular in my first pass through these notes I had (following Weibel) included a treatment of Base Change for Tor but not for Ext. After reading wikipedia I went back and included this material, as well as the tensor and hom identities it requires, making it look like this was planned all along.

10.2. **The Standard Resolutions; Cocycles and Coboundaries.**

Let us record some of these formulas in low dimension.

$$B^0(G, M) = \delta(C^{-1}(G, M)) = \delta^{-1}(0) = 0.$$

$$C^0(G, M) = \mathrm{Map}(G^0, M) = M.$$

$$\delta^0 : C^0(G, M) \to C^1(G, M) : a \in M \mapsto (g \mapsto ga - a).$$

Therefore

$$Z^0(G, M) = \{a \in M \mid ga = a \forall g \in G\} = M^G,$$

so

$$H^0(G,M) = Z^0(G,M)/B^0(G,M) = M^G.$$

$$\delta^1 : C^1(G,M) \to C^2(G,M),\ (\delta^1 f)(g,h) = gf(h) - f(gh) + f(g),$$

so

$$Z^1(G,M) = \operatorname{Ker}\delta^1 = \{f : G \to M \mid f(gh) = f(g) + gf(h)\}.$$

Elements of $Z^1(G,M)$ are called **crossed homomorphisms**.

$$B^1(G,M) = \operatorname{Image}\delta^0 = \{f : G \to M \mid \exists a \in M \mid f(g) = ga - a \forall g \in G\}.$$

The resulting description of $H^1(G,M) = Z^1(G,M)/B^1(G,M)$ is extremely useful. This is especially so when M is a trivial G-module because then we get the simpler description $Z^1(G,M) = \operatorname{Hom}(G,M)$, $B^1(G,M) = 0$, so $H^1(G,M) = \operatorname{Hom}(G,M)$.

We have

$$Z^2(G,M) = \{f : G^2 \to M \mid g_1 f(g_2,g_3) - f(g_1g_2,g_3) + f(g_1,g_2g_3) - f(g_1,g_2) = 0\}.$$

Elements of $Z^2(G,M)$ are called **factor sets**: they come up naturally when one examines the set of extensions of the group G by the abelian group M.

$$B^2(G,M) = \{f : G^2 \to M \mid \exists F : G \to M \mid f(g_1,g_2) = g_1F(g_2) - F(g_1g_2) + F(g_1) \forall g_1, g_2 \in G\}.$$

The resulting description $H^2(G,M) = Z^2(G,M)/B^2(G,M)$ is often useful.

Three cocycles also come up in group theory, but are less important. To the best of my knowledge instances of n-cocycles with $n \geq 4$ "in nature" are extremely rare.

10.3. Group co/homology as bifunctors.

Proposition 10.6. *Let $\rho : G \to G'$ be a group homomorphism, let M be a G-module, M' a G'-module, and $f : M \to M'$ a G-module map.*
a) There are natural homomorphisms $H_\bullet(G,M) \to H_\bullet(G',M')$.
b) There are natural homomorphisms $H^\bullet(G',M) \to H^\bullet(G,M')$.

Proof. Let $P_\bullet$ be a projective resolution of $\mathbb{Z}$ over $\mathbb{Z}[G]$ and let $P'_\bullet$ be a projective resolution of $\mathbb{Z}$ over $\mathbb{Z}[G']$. Via the homomorphism $\mathbb{Z}[G] \to \mathbb{Z}[G']$ we may regard $P'_\bullet$ as a resolution of $\mathbb{Z}$ over $\mathbb{Z}[G]$. (If ρ is an embedding, then this is a projective resolution. In general it isn't, but that's okay: it doesn't need to be.) By the Comparson Theorem for resolutions there is a chain map $\varphi : (P_\bullet \to \mathbb{Z} \to 0) \to (Q_\bullet \to \mathbb{Z} \to 0)$ between the augented resolutions, unique up to chain homotopy. There is then an induced map

$$P_\bullet \otimes_{\mathbb{Z}[G]} M \to P'_\bullet \otimes_{\mathbb{Z}[G]} M' \to P'_\bullet \otimes_{\mathbb{Z}[G']} M',$$

and its induced maps on homology are the desired maps $H_*(G,M) \to H_*(G',M')$. Similarly, there is an induced map

$$\operatorname{Hom}_{\mathbb{Z}[G']}(P'_\bullet, M') \to \operatorname{Hom}_{\mathbb{Z}[G]}(P'_\bullet, M') \to \operatorname{Hom}_{\mathbb{Z}[G]}(P_\bullet, M)$$

and its induced maps on cohomology are the desired maps $H^*(G',M) \to H^*(G,M')$. □

Exercise: Describe the map $H^*(G',M') \to H^*(G,M)$ in terms of standard cochains.

10.4. **Inflation-Restriction.**

Let G be a group, H a normal subgroup, and M a G-module. Then M is naturally an H-module and M^H is naturally a G/H-module. As a special case of the functorial maps defined above, we get an **inflation map**

$$\text{Inf} : H^1(G/H, M^H) \to H^1(G, M)$$

and a **restriction map**

$$\text{Res} : H^1(G, M) \to H^1(H, M).$$

Each of these maps is essentially just pulling back on one-cocycles.

Theorem 10.7. *(Inflation-Restriction Sequence) Let H be a normal subgroup of a group G, and let M be a G-module. There is an exact sequence*

$$0 \to H^1(G/H, M^H) \stackrel{\text{Inf}}{\to} H^1(G, M) \stackrel{\text{Res}}{\to} H^1(H, M).$$

Proof. Step 1: We show Inf is injective. Let $f : G/H \to M^H$, and suppose that its pullback to G is cohomologous to zero: i.e., there is $a \in M$ such that $f(g) = ga - a$ for all $g \in G$. Since f is constant on cosets of H, we have $ga - a = gha - a$ for all $h \in H$. Thus $a \in M^H$ and $f \in Z^1(G/H, M^H)$ is cohomologous to 0.
Step 2: We show $\text{Res} \circ \text{Inf} = 0$. This is almost obvious. By looking at one-cocycles, we see that by pulling back a one-cocycle $f : G/H \to M$ to G and then to H we get the constant map $h \in H \mapsto f(H)$. Since every one-cocycle has $f(1) = 0$, the pulled back cocycle is constantly zero.
Step 3: We show that $\text{Ker}\,\text{Res} \subset \text{Image}\,\text{Inf}$. Let $f \in Z^1(G, M)$, and suppose there is $a \in M$ such that $f(h) = ha - a$ for all $h \in H$. Without changing the cohomology class of f we may subtract off the one-coboundary $g \mapsto ga - a$ to get a one-cocycle which vanishes identically on H. For all $g \in G$, $h \in G$ we have $f(gh) = f(g) + gf(h) = f(g)$, and thus f is constant on cosets of H. Similarly for all $g \in G$, $h \in H$ we have $f(hg) = f(h) + hf(g) = hf(g)$. Since H is normal in G there is $h' \in H$ with $hg = gh'$, and thus

$$hf(g) = f(hg) = f(gh') = f(g),$$

i.e., $f(G) \in M^H$ and thus f lies in the image of the inflation map. $\square$

10.5. **Corestriction.**

11. Galois Cohomology

11.1. **Hilbert's Satz 90.**

Theorem 11.1. *Let K/F be a finite Galois extension. Put $G = \text{Aut}(K/F)$. Then:*
a) $H^1(G, K) = 0$.
b) $H^1(G, K^\times) = 0$.

Proof. a) Let $f : G \to K$ be a 1-cocycle. Since K/F is finite separable, by [FT, § 7] there is $c \in K$ with $\text{Tr}_{K/F}(c) = 1$. Put

$$b = \sum_{\sigma \in G} f(\sigma)\sigma(c),$$

so

$$\tau(b) = \sum_{\sigma \in G} \tau(f(\sigma))(\tau\sigma)(c)$$

$$= \sum_{\sigma \in G} \left(f(\tau\sigma) - f(\tau)\right)(\tau\sigma)(c) = \sum_{\sigma \in G} f(\tau\sigma)(\tau\sigma)(c) - \sum_{\sigma \in G} f(\tau)(\tau\sigma)(c)$$

$$= b - f(\tau) \cdot \tau \left(\sum_{\sigma \in G} \sigma(c) \right) = b - f(\tau).$$

Thus $f(\tau) = b - \tau(b)$ for all $\tau \in G$, so $f \in B^1(G, K)$.
b) Let $f : G \to K^\times$ be a 1-cocycle. By independence of characters, there is $c \in K$ such that $\sum_{\sigma \in G} f(\sigma)\sigma(c) \neq 0$; fix such a c and put $b = \sum_{\sigma \in G} f(\sigma)\sigma(c)$. Then

$$\tau(b) = \sum_{\sigma \in G} \tau(f(\sigma))(\tau\sigma)(c),$$

so

$$f(\tau)\tau(b) = \sum_{\sigma \in G} f(\tau)\tau(f(\sigma)) \cdot (\tau\sigma)(c) = \sum_{\sigma \in G} f(\tau\sigma) \cdot (\tau\sigma)(c) = b,$$

i.e., $f(\tau) = b/\tau(b)$. So $f \in B^1(G, K^\times)$. □

The proof of Theorem 11.1b) is a classic one. A very similar argument works in *non-abelian cohomology* to show that $H^1(G, \mathrm{GL}_n(K)) = 0$ for any $n \in \mathbb{Z}^+$ – alas we have not given the definition of nonabelian H^1 in these notes – and becomes one of th fundamental results in this area.

In contrast, one can prove a stronger form of Theorem 11.1a) by backing away from the explicit cocycles and using some of the ideas we have developed previously.

Exercise: Let K/F be a finite Galois extension, and put $G = \mathrm{Aut}(K/F)$.
a) Show that the G-module K is induced, i.e., is of the form $\mathbb{Z}[G] \otimes_{\mathbb{Z}} A$ for some abelian group A. (Hint: apply the **Normal Basis Theorem** [FT, § 9.5].
b) Deduce that $H^i(G, K) = 0$ for all $i \geq 1$.
c) Must we have $H^2(G, K^\times) = 0$? (Hint: hell no.)

Theorem 11.2. *(Hilbert's Satz 90) Let K/F be a finite Galois extension with cyclic Galois group $G = \langle \sigma \mid \sigma^n = 1 \rangle$.*
a) For $c \in K$, the following are equivalent:
(i) $\mathrm{Tr}_{K/F}(c) = 0$.
(ii) There is $a \in K$ such that $c = a - \sigma(a)$.
b) For $c \in K$, the following are equivalent:
(i) $N_{K/F}(c) = 1$.
(ii) There is $a \in K^\times$ such that $c = \frac{a}{\sigma(a)}$.

Exercise: Deduce Theorem 11.2 immediately from Theorem 11.1 and our computation of $H^1(G, M)$ for any finite cyclic group G.

Remark: Hilbert himself did not use group cohomology to prove his Satz 90, and most field theory texts – including [FT] – give a non-cohomological proof.

Corollary 11.3. *Let $n \in \mathbb{Z}^+$. Let F be a field of characteristic not dividing n.*
a) Let $a \in F^\times$ have order n in $F^\times/F^{\times n}$, and put $K = F(\sqrt[n]{a})$. TFAE:
(i) K/F is Galois with cyclic Galois group.
(ii) K/F is Galois.
(iii) F contains a primitive nth root of unity.
b) Let K/F be a finite Galois extension with cyclic Galois group $G = \langle \sigma \mid \sigma^n = 1 \rangle$. If F contains a primitive nth root of unity ζ_n, then $K = F(\sqrt[n]{a})$ for some $a \in F$.

Proof. a) This is a standard field-theoretic exercise which we leave to the reader.
b) Since $\zeta_n \in F$, $N_{K/F}(\zeta_n) = \zeta_n^n = 1$. By Hilbert's Satz 90, there is $a \in K^\times$ with $\zeta_n = \frac{a}{\sigma(a)}$. So for all $i \in \mathbb{Z}^+$, $\sigma(\alpha^i) = \zeta_n^i \alpha^i$. In particular $\sigma(\alpha^n) = \alpha^n \in F$. Put $a = \alpha^n$. Only the identity of G fixes $F(\alpha)$ pointwise, so $K = F(\alpha) = F(\sqrt[n]{a})$. $\square$

There is also an "absolute" version of Hilbert's Satz 90 which is, e.g. from the perspective of contemporary number theory, more natural and useful.

11.2. **Topological group cohomology.**

A **topological group** is a group G endowed with a topology τ which is compatible with the group structure in the following sense: the group law $G \times G \to G,\ (x,y) \mapsto xy$ and the inversion map $G \to G,\ x \mapsto x^{-1}$ are both continuous.

A **topological G-module** is a topological abelian group M together with a continuous action of G on M, i.e., the function $G \times M \to M,\ (g,m) \mapsto gm$ is required to be continuous.

Let M be a topological G-module. For $n \in \mathbb{N}$, let $C^n_{\text{top}}(G,M)$ be the **continuous cochains**, i.e., continuous maps $G^n \to M$. Let $\delta : C^n(G,M) \to C^{n+1}(G,M)$ be the usual coboundary map. Then

$$B^{n+1}_{\text{top}}(G,M) = \delta(C^n_{\text{top}}(G,M)) \subset C^{n+1}_{\text{top}}(G,M).$$

Accordingly, we may define the **topological group cohomology**

$$H^n_{\text{top}}(G,M) = Z^n_{\text{top}}(G,M)/B^n_{\text{top}}(G,M).$$

Example: If G is any group and M is any G-module, then by endowing G and M with the discrete topologies, M becomes a topological G-module.

However, if G is a nondiscrete group then $H^n_{\text{top}}(G,M)$ is, in general, different from the ordinary group cohomology $H^n(G,M)$, and in some situations the former is more natural.

There are many questions one should ask about these topological cohomology groups, especially: do they arise via the formalism of homological algebra? Are they the derived functors of $M \mapsto M^G$? Is it even the case that the category of topological G-modules an abelian category with enough projective and/or injective objects?

The answers to these questions are generally beyond the scope of these notes. We recommend that the interested reader consult a recent paper of M. Flach [Fl08].

11.3. **Profinite Groups.**

Let $\{X_i\}_{i \in I}$ be an inverse system of topological spaces with continuous transition maps. Then $X = \varprojlim X_i$ exists in the category of topological spaces. As a set X, is the subset of $\prod_{i \in I} X_i$ consisting of compatible systems $\{x_i\}_{i \in I}$, i.e., such that whenever $i \leq j$, $\iota_{ji}(x_j) = x_i$.

Exercise: a) Suppose each X_i is Hausdorff. Show that the subset $\varprojlim X_i$ is closed

in $\prod_{i \in I} X_i$ under the product topology.
b) Deduce that an inverse limit of compact spaces is compact.
c) Show: an inverse limit of totally disconnected spaces is totally disconnected.

Now let $\{X_i\}_{i \in I}$ be an inverse system of finite sets, and put $X = \varprojlim X_i$. We say that X is a **profinite set**. We can topologize X in a natural way: give each X_i the discrete topology and X the inverse limit topology as above. Since discrete spaces are Hausdorff and finite spaces are quasi-compact, from the previous exercise we deduce that the profinite topology on X is compact and totally disconnected.

In particular this construction works if we are given an inverse system $\{G_i\}_{i \in I}$ of finite groups: this will be the case of interest to us here. Then $G = \varprojlim G_i$ is called a **profinite group**: it is a compact, totally disconnected topological group.

Exercise: Show that any profinite group is either finite or uncountably infinite. (Hint: for instance show there are no countably infinite compact topological groups.)

In fact the converse is true, as we now explain. Let G be any topological group. Then the open finite index normal subgroups $\{N_i\}_{i \in I}$ form a directed set under reverse inclusion. It follows that $\{G/N_i\}_{i \in I}$ is an inverse system of finite, discrete topological groups: if $i \leq j$, then $N_i \supset N_j$ and we take the natural quotient map $G/N_j \to G/N_i$. Let $\hat{G} = \varprojlim G/N_i$. This is a profinite group, called the **profinite completion of G**.

Exercise: a) For any topological group G, define a canonical topological group homomorphism $P : G \to \hat{G}$.
a) Suppose G is compact. Show that P is an isomorphism of topological groups iff it is bijective.
b) Exhibit a topological group G such that P is injective but not surjective.
c) Exhibit a topological group G such that P is surjective but not injective.

Exercise: For a locally compact abelian group G, let $G^\vee = \operatorname{Hom}_c(G, S^1)$ – endowed with the compact open topology – be the **Pontrajgin dual group**. Here we suppose that G is a profinite group.
a) Show that every continuous homomorphism $G \to S^1$ has image in $\mathbb{Q}/\mathbb{Z}$.
b) Show that the natural topology on $G^\vee$ is discrete.
c) Show that if $G \cong \varprojlim G_i$, then $G^\vee \cong \varinjlim G_i^\vee$.
d) Deduce that $G^\vee$ is a torsion abelian group.
e) Show that $G \mapsto G^\vee$ induces an anti-equivalence of categories from the category of profinite abelian topological groups to the category of torsion abelian groups.

Exercise (Serre): Show that any torsionfree profinite commutative group is isomorphic to a (possibly infinite) direct product of copies of $\mathbb{Z}_p$ for some prime p.

Theorem 11.4. *For a topological group G, the following are equivalent:*
(i) The canonical map $P : G \to \hat{G}$ is an isomorphism of topological groups.
(ii) G is a profinite group.
(iii) G is compact and totally disconnected.

Proof. See [Wi, Cor. 1.2.4, Thm. 1.2.5]. □

Lemma 11.5. *Let $f : G \to Y$ be a continuous map from a profinite group to a discrete space. Then there is an open finite index normal subgroup N of G such that f factors through G/N.*

Exercise: Prove it.

Proposition 11.6. *Let G be a profinite group, and let M be a G-module. TFAE:*
(i) The action $G \times M \to M$ is continuous for the discrete topology on M.
(ii) For every $x \in M$, there is an open subgroup U of G with $x \in M^U$.

Proof. The action is continuous for the discrete topology on M iff for all $x, y \in M$, $S(x, y) = \{g \in G \mid gx = y\}$ is an open subset of G. For any $x \in M$, $S(x, x)$ is the stabilizer of x in G, so (i) $\implies$ (ii). Conversely, assuming (ii) then the result holds for whenever $x = y$. Now suppose $x \neq y$. If there is no $g \in G$ with $gx = y$, then $S(x, y) = \varnothing$, which is indeed an open subset. On the other hand, if there is $g \in S(x, y)$, then $S(x, y) = gS(x, x)$ is an open subset. □

Proposition 11.7. *Let G be a profinite group acting continuously on a discrete abelian group M. For all $n \geq 0$, we have $H^n_{\text{top}}(G, M) = \varinjlim H^n(G/N, M^N)$, where the limit is taken over the directed system of open normal subgroups of G and for $N_2 \supset N_1$, $H^n(G/N_2, M^{N_2}) \to H^n(G/N_1, M^{N_1})$ is inflation.*

Proof. One checks that the canonical map $\varinjlim C^*(G/N_i, M^{N_i}) \to C^*_{\text{top}}(G, M)$ is an isomorphism, and the result follows upon passage to cohomology. □

Exercise: More generally, suppose we are given an inverse system $\{G_i\}_{i \in I}$ of profinite groups and a direct system $\{M_i\}_{i \in I}$ of discrete G_i-modules satisfying the natural compatibility condition: if $i \leq j$, then viewing A_i is a G_j-module via $G_j \to G_i$, then $A_i \to A_j$ is a G_j-module map. Show that there is a natural isomorphism

$$H^q_{\text{top}}(\varprojlim G_i, \varinjlim A_i) \cong \varinjlim H^q_{\text{top}}(G_i, A_i).$$

11.4. **The Krull Topology on** $\mathrm{Aut}(K/F)$.

Recall that a field extension K/F is **Galois** if it is algebraic, normal and separable. However, it is entirely possible for a Galois extension to be infinite.

Example: Let $\{K_i/F\}_{i \in I}$ be any family of finite Galois extensions inside a fixed algebraic closure $\overline{F}$ of F. If I is infinite, then the field extension K generated by all the K_i's is an infinite Galois extension.

If in the previous example we take the family of *all* finite Galois subextensions of $\overline{F}/F$, then we get F^{sep}, the maximal separable algebraic subextension of $\overline{F}$. This is a Galois extension, and its automorphim group $G_F = \mathrm{Aut}(F^{\text{sep}}/F)$ is called the **absolute Galois group of F**.

Exercise: Let K/F be a Galois extension.
a) Show that K is the direct limit of its finite Galois subextensions.
b) Show that $\mathrm{Aut}(K/F)$ is the inverse limit of the automorphism groups of its finite Galois subextensions.
c) Deduce that $\mathrm{Aut}(K/F)$ is a profinite group.

Recall that the main content of finite Galois theory is this: if K/F is a finite Galois extension, then

$$L \mapsto \mathrm{Aut}(K/L)$$

and

$$H \mapsto K^H$$

are mutually inverse inclusion-reversing bijections from the lattice of subextensions of K/F to the lattice of subgroups of $G = \mathrm{Aut}(K/F)$. However, if K/F is infinite Galois with $G = \mathrm{Aut}(K/F)$, this result requires modification: there are (always) more subgroups of G than subextensions of K/F. For a simple example, let $F = \mathbb{F}_p$ a finite field, and let $K = \overline{\mathbb{F}_p} = \lim \mathbb{F}_{p^n}$ be its algebraic closure. The Frobenius map $f : x \mapsto x^p$ is an element of $\mathrm{Aut}(K/F)$, of infinite order. Let $\mathbb{Z} = \langle f \rangle \subset \mathrm{Aut}(K/F)$. Then $K^{\mathbb{Z}} = F$. Thus $\mathrm{Aut}(K/F)$ is infinite; but a profinite group cannot be countably infinite, so $\mathrm{Aut}(K/F)$ must be uncountable. (In fact it is clearly isomorphic to $\varprojlim \mathrm{Aut}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \varprojlim \mathbb{Z}/n\mathbb{Z} = \hat{\mathbb{Z}}$.) Thus the countable subgroup $\mathbb{Z}$ of $\mathrm{Aut}(K/F)$ and the full uncountably infinite group $\mathrm{Aut}(K/F)$ have the same fixed field, and hence so does any group lying in between them...of which there must be uncountably infinitely many!

To recover the Galois correspondence we must take note of the profinite structure on $\mathrm{Aut}(K/F)$. This is a profinite group, hence carries a canonical compact, totally disconnected topology, called the **Krull Topology**. Then:

Theorem 11.8. *(Krull) Let K/F be a Galois extension. The maps*

$$L \mapsto \mathrm{Aut}(K/L)$$

and

$$H \mapsto K^H$$

give inclusion-reversing bijections from the lattice of subextensions of K/F to the lattice of Krull-closed subgroups of $\mathrm{Aut}(K/F)$.

Proof. See [FT]. □

11.5. **Galois Cohomology.**

Let K a field. Changing our notation slightly from above, let us denote by $\overline{K}$ a separable algebraic closure of K, i.e., a maximal algebraic, normal, separable extension of K. Let $G = \mathrm{Aut}(\overline{K}/K)$ be the **absolute Galois group** of K.

There are many natural examples of G-modules, including $\overline{K}$, $\overline{K}^{\times}$ and $\mu(\overline{K})$, the group of roots of unity in $\overline{K}$. In fact these are all instances of a more general construction: let A/K be a **commutative algebraic group**. This is an algebraic variety defined over K endowed with morphisms $\cdot : A \times A \to A$ and $- : A \to A$ making $A(R)$ into a commutative group for any commutative K-algebra R. Then G naturally acts on $A(\overline{K})$.
Here is the concrete perspective: embed $A \hookrightarrow \mathbb{P}^n$ into projective space over K. (There are algebraic varieties which cannot be so embedded – i.e., are not quasi-projective – but by a rather deep theorem, every group variety is quasi-projective.) Then G simply acts on projective coordinates, um, coordinatewise:

$$\sigma \cdot [x_0 : \ldots : x_n] = [\sigma(x_0) : \ldots : \sigma(x_n)]$$

and the action preserves $A(\overline{K})$.
Here is the abtract perspective: an $\overline{K}$-valued point on any K-scheme X is simply an embedding $P : \operatorname{Spec}\overline{K} \to X$ compatible with the K-scheme structure (explain this!). Then $\sigma \in \operatorname{Aut} G$ gives a map $\sigma^* : \operatorname{Spec}\overline{K} \to \operatorname{Spec}\overline{K}$, and we define $\sigma(P) = \sigma^* \circ P$.

Anyway, now you are probably expecting us to define the Galois cohomology as the group cohomology of G and the G-module $A(\overline{K})$. This is the wrong definition! It ignores the (Krull) topology on G.

Exercise: Show that if $A(\overline{K})$ is given the discrete topology, the action of G on $A(\overline{K})$ is continuous. (Hint: use Proposition X.X.)

Thus the correct definition is via topological group cohomology:

$$H^n(K, A) = H^n_{\text{top}}(G, A(\overline{K})),$$

or, equivalently, by Proposition X.X above,

$$H^n(K, A) = \lim_{L/K} H^n(\operatorname{Aut}(L/K), A(L)).$$

The Galois cohomology group $H^1(K, A)$ is called the **Weil-Châtelet group** of A. (To be honest, others call it this only when A is an abelian variety. But why not extend the terminology to the general case?)

Proposition 11.9. *(Absolute Hilbert 90) For any field K we have*

$$H^i(K, \mathbb{G}_a) = 0 \forall i \geq 1$$

and

$$H^1(K, \mathbb{G}_m) = 0.$$

Exercise: Prove it.

Corollary 11.10. *(Cohomological Kummer Theory) Let $n \in \mathbb{Z}^+$, and let K be a field of characteristic not dividing n (e.g. characteristic zero!). Let μ_n be the Galois module of nth roots of unity in $\overline{K}$. Then:*
a) We have $H^1(K, \mu_n) = K^\times / K^{\times n}$.
b) Suppose that $\#\mu_n(K) = n$. Then

$$\operatorname{Hom}(G_K, \mathbb{Z}/n\mathbb{Z}) = K^\times / K^{\times n}.$$

This gives a classification of cyclic Galois extensions of K of exponent dividing n.

Proof. a) Take Galois Cohomology of the short exact sequence of Galois modules

$$1 \to \mu_n(\overline{K}) \to \overline{K}^\times \xrightarrow{n} \overline{K}^\times \to 1$$

and apply Absolute Hilbert 90.
b) When all the nth roots of unity of $\overline{K}$ lie in K, the Galois module structure on $\mu_n(\overline{K})$ is trivial, so $\mu_n(\overline{K})$ is just the abelian group $\mathbb{Z}/n\mathbb{Z}$ and thus

$$K^\times / K^{\times n} = H^1(K, \mu_n) = \operatorname{Hom}(G_K, \mathbb{Z}/n\mathbb{Z}).$$

∎

Exercise: A Galois extension L/K is said to be **abelian of exponent dividng n** if $\mathrm{Aut}(L/K)$ is an n-torsion abelian group. Suppose that K contains n nth roots of unity.
a) Show that the compositum of all finite abelian extensions of exponent dividing n is a (usually infinite) abelian extension of exponent dividing n: call it L/K.
b) Show that L is obtained by adjoining to K the nth root of every element of $K^\times$.
c) Show that $\mathrm{Aut}(L/K) \cong K^\times/K^{\times n}$.

12. Applications to Topology

12.1. **Some Reminders.**

Recall that to any topological space X we have attached a sequence $\{\pi_n(X)\}_{n\geq 0}$ of **homotopy groups**. Actually there are a couple of minor inaccuracies in the above description. Let's be a bit more careful:

$n = 0$: For any space X, $\pi_0(X)$ is the set of homotopy classes of maps from the one-point space into X. In other words, $\pi_0(X)$ is the collection of path components of X. In particular, $\pi_0(X)$ consists of a single point iff X is path connected. Let us agree to write this condition as $\pi_0(X) = 0$ in order to create notational consistency. Note that $\pi_0(X)$ is just a set: it does not have the structure of a group. For many natural applications the assumption $\pi_0(X) = 0$ is a natural one. In particular, any CW-complex X is locally contractible – so the path components are precisely the connected components – and is the direct sum of its connected components.

$n \geq 1$: For any space X and any point $x \in X$, the homotopy group $\pi_n(X, x)$ is the set of continuous maps $f : I^n = [0, 1]^n \to X$ with the proprety that f maps every boundary point to x, modulo the equivalence relation $\sim$: $f \sim g$ if there is a continuous map $H : I^{n+1} \to X$ such that for all $x \in I^n$ and all $t \in [0, 1]$:
• $H(x, 0) = f(x)$, $H(x, 1) = g(x)$, and
• if $x \in \partial I^n$, then $H(x, y) = x$.

Note that a continuous map $f : I^n \to X$ which maps ∂I^n to a fixed point x is equivalent to a continuous map $S^n \to X$ which maps a fixed point – say the north pole $p = (0, \ldots, 0, 1)$ – to x. Thus $\pi_n(X, x)$ is also the set of homotopy classes of maps $(S^n, p) \to (X, x)$. The previous descrption though is valuable because it allowsu us to define a group law on $\pi_n(X, x)$: we linearly smush f and g to maps on (respectively) the half boxes $I^{n-1} \times [0, \frac{1}{2}]$ and $I^{n-1} \times [\frac{1}{2}, 1]$ and then define $f \cdot g$ as the resulting map on I^n, which is well-defined and continuous because both f and g map every point on the common border $I^{n-1} \times \frac{1}{2}$ to x.

It is not hard to see that this product makes $\pi_n(X, x)$ into a group. The dependence on the base point x is not serious and can often be suppressed. More precisely, if x and x' lie in the same path component, then $\pi_n(X, x) \cong \pi_n(X, x')$. To get an isomorphism one chooses a path from $xtox'$, and the isomorphism depends only on the homotopy class of this path. It follows that the isomorphism is canonical up to an outer automorphism – i.e., a conjugation – of $\pi_n(X, x')$. As we shall shortly see, when $n \geq 2$ this means the isomorphisms are fully canonical. In the $n = 1$ case the philosophy that one should try to phrase results about the fundamental group in a conjugacy-invariant way is a useful one, which comes up e.g. in covering space theory. The most fully satisfactory solution to this non-canonicity issue is to replace the fundamental group with a larger structure, the **fundamental groupoid** of X: this is well beyond the scope of our intentions (or needs).

For $n \geq 2$, the group is commutative – this is actually an easy exercise involving continuously deforming half-boxes. Thus it is completely safe to write $\pi_n(X)$ for $n \geq 2$. The group $\pi_1(X, x)$, the so-called **fundamental group of X**, need not be commutative. For instance, it follows from the Seifert-van Kampen theorem that the fundamental group of a wedge of S circles is the free group $F(S)$ on the set S.

Theorem 12.1. *(Cellular Approximation) If X and Y are CW-complexes, then any continuous map $f : X \to Y$ is homotopic to a cellular map $g : X \to Y$. Moreover, if there is a subcomplex $Z \subset X$ on which f is already cellular, then the homotopy H can be chosen such that $H(z, t) = f(z)$ for all $z \in Z$ and $t \in [0, 1]$.*

From this result one can deduce the following (though we do not give the details, which make use of the homotopy groups of a pair) important one.

Theorem 12.2. *Let X be a connected CW-complex. Let $k, n \in \mathbb{N}$, and let $\iota_n : X_n \to X$ be the natural inclusion map from the n-skeleton into X. Consider the induced map*

$$\pi_k(\iota_n) : \pi_k(X_n) \to \pi_k(X).$$

a) If $k < n$, then π_k is an isomorpism.
b) If $k = n$, then π_k is surjective.

Theorem 12.3. *Let X be a connected CW-complex with universal covering space $p : \tilde{X} \to X$. Then for all $k \geq 2$, $\pi_k(p) : \pi_k(\tilde{X}) \to \pi_k(X)$ is an isomorphism.*

Proof. See e.g. [H, Prop. 4.1]. □

Theorem 12.4. *(Hurewicz) Let X be a path-connected topological space.*
*a) For all positive integers k, there is a natural **Hurewicz map***

$$h_k : \pi_k(X) \to H_k(X).$$

b) Suppose that X is $(n-1)$-connected, i.e., $\pi_k(X) = 0 \forall k \leq n-1$. Then:
- *h_1 is the abelianization map.*
- *h_1 is an isomorphism, if $2 \leq k \leq n$.*
- *h_1 is surjective, if $2 \leq k = n + 1$.*

Proof. See e.g. [H, Thm. 4.32]. □

Theorem 12.5. *(Whitehead) Let (X, x) and (Y, y) be connected, pointed CW-complexes. For a continuous map $f : (X, x) \to (Y, y)$, the following are equivalent:*
(i) $f : X \sim Y$ is a homotopy equivalence.
*(ii) f is a **weak equivalence**: for all $n \geq 0$, $\pi_n(f) : \pi_n(X) \xrightarrow{\sim} \pi_n(Y)$.*

Proof. See e.g. [H, Thm. 4.5]. □

Tournant Dangereux: Whitehead's Theorem *does not say* that if two CW-complexes have isomorphic homotopy groups then they are homotopy equivalent! In fact this is very false.

Exercise: Let $X = S^2 \times \mathbb{RP}^3$ and $Y = \mathbb{RP}^2 \times S^3$.
a) Show that $\pi_k(X) \cong \pi_k(Y)$ for all k.

b) Show that X and Y do not have identical homology groups. (In fact, because X is a closed orientable manifold and Y is a closed nonorientable manifold, this follows from Poincaré Duality.)
c) Deduce that X and Y are not homotopy equivalent.

In fact it is possible for complexes to have isomorphic homotopy, homology and cohomology groups but not be homotopy equivalent. The canonical example uses **Lens spaces**, which we will define in a special case later on. Of course the proof that such spaces cannot be homotopy equivalent must lie deeper, as we must find some other invariant to distinguish between them! (It is also possible for two lens spaces to be homotopy equivalent but not homeomorphic, and this lies deeper still.)

Corollary 12.6. *For a connected CW-complex X, the following are equivalent:*
(i) X is contractible, i.e., homotopy equivalent to I^0.
(ii) $\pi_n(X) = 0$ for all $n \geq 0$.
*(iii) X is **acyclic**: $H_n(X, \mathbb{Z}) = 0$ for all $n \geq 1$.*
(iv) For all abelian groups M, $H_n(X, M) = 0$ for all $n \geq 1$.

Proof. It is clear that (i) implies all the other conditions are (iv) $\implies$ (iii). The Hurewicz Theorem gives (ii) $\iff$ (iii), and the Whitehead Theorem gives (ii) $\implies$ (i): note that any map between two spaces with all homotopy groups nonzero is a weak equivalence! □

12.2. **Introducing Eilenberg-MacLane Spaces.**

Theorem 12.7. *For any group G, there is a connected CW-complex X such that:*
(EM1) $\pi_1(X) \cong G$.
(EM2) For all $k \geq 2$, $\pi_1(X) = 0$.

Proof. Write $G = F(S)/R$ as the quotient of a free group $F(S)$ by a normal subgroup R of relations. We take X_1 to be the wedge of S circles, so $\pi_1(X_1) \cong F(S)$. We build X_2 by adding one 2-cell for each word $x \in R$ we add a 2-cell whose attaching map on the boundary is given by the word x. This gives $\pi_2(X_2) \cong F(S)/R \cong G$. By Theorem X.X, any CW-complex with this 2-skeleton has fundamental group isomorphic to G; the only remaining issue is that by adding 2-cells we may have introduced a nontrivial π_2. If so, for each element of π_2 we attach a 3-cell so as to kill that element, getting X_3 with $\pi_1(X_3) \cong G$ and $\pi_2(X_3) \cong 0$. Now we may have introduced nontrivial π_3: if so we remedy it by adding 4-cells to kill those elements. And so on: in the end we get a – possibly infinite-dimensional – CW-complex X satisfying (EM1) and (EM2). □

A CW-complex X satisfying (EM1) and (EM2) is called an **Eilenberg-MacLane space**, or $K(G, 1)$-**space**, for the group G.

Theorem 12.8. *Any two Eilbenberg-MacLane spaces for a given group G are homotopy equivalent.*

Proof. Step 1: We need the following technical result, to which we refer the reader to [H, Lemma 4.31] for the proof: fix $n \in \mathbb{Z}^+$. Let X be a CW-complex obtained from a wedge of copies of S^n by attaching $(n+1)$-cells $\{e_\beta\}$. Then if Y is a path-connected space, every homomorphism $\psi : \pi_n(X) \to \pi_n(Y)$ is $\pi_k(f)$ for some continuous map $f : X \to Y$.
Step 2: Let G be a group. Let (X, x) be the $K(G, 1)$-space we constructed as in the

proof of Theorem X.X above (endowed with some base point: n'importe quelle). Let (Y, y) be a connected pointed CW-complex with $\pi_k(Y) = 0$ for all $k \geq 3$. We CLAIM every group homomorphism $\psi : \pi_1(X) \to \pi_1(Y)$ is of the form $\pi_1(f)$ for some continuous map $f : X \to Y$.
PROOF OF CLAIM Consider first X_2, the 2-skeleton of X. Then the hypotheses of Step 1 apply with $n = 1$: there is a continuous map $f : X_2 \to Y$. It remains to extend f over each k-cell for $k \geq 3$, but since $\pi_k(Y) = 0$ this is trivial.
Step 3: Now suppose that (X, x) and (Y, y) are both $K(G, 1)$-complexes. In particular they have isomorphic fundamental groups: choose an isomorphism $\psi : \pi_1(X, x) \to \pi_1(Y, y)$. By Step 2, ψ is realized by a continuous map $f : X \to Y$. Because all the other homotopy groups are trivial, f must be a weak equivalence and thus, by Whitehead's Theorem, a homotopy equivalence. □

Exercise: a) Show that for groups G_1 and G_2, we have

$$K(G_1, 1) \times K(G_2, 1) = K(G_1 \times G_2, 1).$$

(Here the "equality" really means homotopy equivalence.)
b) Show that the natural generalization of part a) holds for arbitrary (infinite) products.

Actually our proof of Theorem 12.8 was fairly anemic. By more careful arguments one can establish the following better result. For spaces X and Y, write $[X, Y]$ for the set of homotopy classes of continuous maps from X to Y.

Theorem 12.9. *Let G be a group, (X, x) a connected CW-complex, and let Y be an Eilenberg-MacLane space for G. Fix $y \in Y$. Let $\varphi : \pi_1(X) \to \pi_1(Y, y)$ be a homomorphism. Then:*
a) There is a continuous map $\Phi : (X, x) \to (Y, y)$ with $\pi_1(\Phi) = \varphi$.
b) If $\Psi : (X, x) \to (Y, y)$ is another map with $\pi_1(\Psi) = \varphi$, then there is a homotopy H between Φ and Ψ with $H(x, t) = y$ for all $t \in [0, 1]$.
c) In other words, for any connected complex X, we have

$$[X, K(G, 1)] \cong \mathrm{Hom}(\pi_1(X), G).$$

In categorical language, part c) says that the functor $X \mapsto \mathrm{Hom}(\pi_1(X), G)$ from the homotopy category of connected, pointed CW-complexes to the category of sets is *represented* by the Eilenberg-MacLane space $K(G, 1)$. The uniqueness of $K(G, 1)$ in the homotopy category now follows from general nonsense: the **Yoneda Lemma**.[20]

Higher Eilenberg-MacLane Spaces: you may have wondered about the "1" in $K(G, 1)$. For any commutative group G and $n \geq 2$, a $K(G, n)$-space is a connected CW-complex X with $\pi_n(X) \cong G$ and all other homotopy groups trivial. The above discussion applies equally well to these higher Eilenberg-MacLane spaces.

Exercise: Let G be a commutative group.
a) Modify our construction to construct a $K(G, n)$-complex starting in dimension n with a wedge of n-spheres.

[20] One might have thought that this piece of general nonsense would come up in a first course on homological algebra before now. Oh well.

b) Show that $K(G,n)$ is unique up to homotopy type.
c)* Show that for any connected complex X we have

$$[X, K(G,n)] \cong \mathrm{Hom}(\pi_n(X), G).$$

d)* Show that for any connected complex X we have

$$[X, K(G,n)] \cong H^n(X, G).$$

In other words, Eilenberg-MacLane spaces represent cohomology.

12.3. **Recognizing Eilenberg-MacLane Spaces.**

An action of a group G on a CW-complex X is **cellular** if for all $g \in G$, the homeomorphism $g\cdot : X \to X$ is a cellular map. In particular,a cellular action permutes the n-cells for all $n \geq 0$.

Exercise: Show that a free, cellular G-action on a CW-complex is properly discontinuous, and thus $X \to G\backslash X$ is a Galois covering map.

Our construction of $K(G,1)$-spaces is not really very explicit. The following criterion is much more helpful in practice.

Theorem 12.10. *Let G be a group which acts freely and cellularly on a CW-complex Y. Put $X = G\backslash Y$, so that $q : Y \to X$ is a covering map. TFAE:*
(i) X is an Eilenberg-MacLane space for G.
(ii) Y is contractible.

Exercise: Prove it.

12.4. **Examples of Eilenberg-MacLane Spaces.**

Although we have in a sense constructed all possible Eilenberg-MacLane spaces, given a particular group G of interest, our construction of $K(G,1)$ is not especially informative. For instance, *a priori* the construction yields an infinite-dimensional complex, but in many cases one can find a finite-dimensional Eilenberg-MacLane space for G.

Theorem XX is very useful for identifying and constructing Eilenberg-MacLane spaces: a connected space X as an Eilenberg-MacLane space for its fundamental group iff its universal cover is contractible. Conversely, given G, to construct $K(G,1)$ it is sufficient to find a free, cellular G-action on a contractible space.

Example: The circle S^1 has universal cover $\mathbb{R}$ and fundamental group $\mathbb{Z}$, so $S^1 = K(\mathbb{Z}, 1)$.

Example: For $d \geq 0$, the torus $T = (S^1)^d$ has universal cover $\mathbb{R}^d$ and fundamental group $\mathbb{Z}^d$, so $T = K(\mathbb{Z}^d, 1)$. Of course this follows from the previous example and Exercise X.X, but it is a basic example worth contemplating.

Example/Exercise: Let A be any free abelian group. Let $Y = A \otimes_{\mathbb{Z}} \mathbb{R}$ and give it the topology which is the direct limit of the usual Euclidean topologies on its finite-dimensional subspaces.

a) Show that Y is contractible.
b) We have naturally $A \hookrightarrow Y$ by $x \mapsto x \otimes 1$. (This map is injective because A is torsionfree.) Thus A acts on Y by translation. Show that this action is freely and properly discontinuous.
c) Deduce that $X = Y/A$ is an Eilenberg-MacLane space for A.

Remark: This construction was given to me by Tyler Lawson in an answer to my request for a topological proof that subgroups of free abelian groups are free abelian: see `http://mathoverflow.net/questions/4578`.

Example: Let X be a connected graph, i.e., a connected one-dimensional CW-complex. Then $\tilde{X}$ is a tree, hence contractible, so X is an Eilenberg-MacLane space for its fundamental group. Further, X is homotopy equivalent to a wedge of circles, so its fundamental group is a free group. Precisely, $H_1(X, \mathbb{Z}) = \pi(X)^{\mathrm{ab}}$ is a free abelian group; let S be a basis. Then $\pi_1(X) \cong F(S)$. In particular, if $S = 1$ we get that the

Example/Exercise: For $n \geq 1$, we have real projective space $\mathbb{RP}^n$, given for instance as the quotient of S^n under the antipodal map $x \mapsto -x$.
a) Show that $\mathbb{RP}^1 \cong S^1$.
b) Show that for $n \geq 2$, $\pi_1(\mathbb{RP}^n) = \mathbb{Z}/2\mathbb{Z}$.
c) Show that $\mathbb{RP}^n$ admits a CW-complex structure in which $(\mathbb{RP}^n)_{n-1} = \mathbb{RP}^{n-1}$ and $(\mathbb{RP}^n)_n$ consists of a single cell D_n, in which the attaching map $S^{n-1} \rightarrow \mathbb{RP}^{n-1}$ is a twofold covering map. Deduce new proofs of parts a) and b).
d) By definition, $\mathbb{RP}^\infty$ is the CW-complex with n-skeleton $\mathbb{RP}^n$ for all n. Show that $\mathbb{RP}^\infty$ is an Eilenberg-MacLane space for $\mathbb{Z}/2\mathbb{Z}$.

Exercise: Is $\mathbb{CP}^\infty$ an Eilenberg-MacLane space?

Exercise: For any $a \geq 1$, show that there is an Eilenberg-MacLane L_a space for $C_a = \langle \sigma \mid \sigma^n = 1 \rangle$ which has exactly one n-cell for each n. Hint: the group C_a acts freely on the unit sphere S^{2n-1} in $\mathbb{C}^n$, e.g. one can map the generator σ to $(z_1, \ldots, z_n) \mapsto (e^{2\pi i} a z_1, \ldots, e^{2\pi i} a z_n)$. Show that the quotient S^{2n-1}/C_a admits a CW-complex $L_{a,n}$ with a single k-cell for all $k \leq 2n-1$. Then show that $(L_{a,n-1})_k = (L_{a,n})_k$ for all $k \leq 2n-1$.

Example: We study topological surfaces, which we always assume to be connected and paracompact.

It is a basic – and rather deep fact – that there are precisely two simply connected (paracompact!) topological surfaces, namely S^2 and $\mathbb{R}^2$. Thus these are the two possible universal covers of any surface. Further, the only two surfaces with universal cover S^2 are S^2 and $\mathbb{RP}^2$. (Note that since $\chi(S^2) = 2$, any covering map $S^2 \rightarrow X$ is at most a 2-fold covering. This comes close to giving the latter result.) It follows that any surface other than S^2 or $\mathbb{RP}^2$ is an **Eilenberg-MacLane manifold**. In particular this shows that there is a 2-dimensional Eilenberg-MacLane space for the group

$$\Pi(g) = \langle a_1, \ldots, a_g, b_1, b_g \mid [a_1, b_1] \cdots [a_g, b_g] = 1 \rangle$$

for all $g \geq 0$.

Example: The following construction yields many, many interesting examples. Let G be a connected real Lie group. Then G admits a maximal compact connected subgroup O, any two such are conjugate, and $G/O \cong \mathbb{R}^d$ is homeomorphic to a Euclidean space, hence contractible. Now let $\Gamma \subset G$ be a **lattice**: i.e., a subgroup which is discrete and of finite covolume with respect to the Haar measure on G. Then $\Gamma \cap O$ is discrete and compact, hence finite. It follows that there is a finite index normal subgroup N of Γ such that the quotient $\overline{\Gamma} = \Gamma/N$ acts freely on $Y = G/O$. It can be shown that the action is also **properly discontinuous** and thus $Y \to \overline{\Gamma}\backslash Y$ is a covering map with contractible universal cover: $\overline{\Gamma}\backslash G/O$ is an Eilenberg-MacLane space for $\overline{\Gamma}$.

This construction is already interesting when G is nilpotent, in which case O is trivial. If we do this with $G = \mathbb{R}^n$ we get **Bieberbach Groups**, each of which has a finite index normal subgroup isomorphic to $\mathbb{Z}^n$. We can also do it with the Heisenberg group $H_3(\mathbb{R})$ and realize $H_3(\mathbb{R})/H_3(\mathbb{Z})$ as an Eilenberg-MacLane space for $H_3(\mathbb{Z})$.

12.5. Eilenberg-MacLane spaces and Group Co/homology.

Let Y be a (nonempty!) CW-complex. Let $C_\bullet(Y)$ be the associated cellular complex, such that $C_n(Y) = \mathbb{Z}[Y_n]$ is the free abelian group on Y_n and the differentials are defined using the attaching maps. Then there is a map $d_0 : C_0(Y) \to \mathbb{Z}$ obtained by sending every 0-cell to 1.

For the following exercise we will only need part b) in our application, so if you don't know about reduced homology groups then you can skip part a) and prove part b) directly.

Exercise: a) Show that the homology of the complex $C_\bullet(Y) \stackrel{d_0}{\to} \mathbb{Z} \to 0$ computes the **reduced homology groups** of X.
b) In particular, if Y is connected then $\ker d_0 = \operatorname{Im} d_1$.

Theorem 12.11. *Let G be a group. Then for all $n \geq 0$, we have*

$$H_n(K(G,1), \mathbb{Z}) \cong H_n(G, \mathbb{Z}),$$

$$H^n(K(G,1), \mathbb{Z}) \cong H^n(G, \mathbb{Z}).$$

Proof. Step 1: Let $X = K(G,1)$ and let $Y \to X$ be the universal covering map. For all $n \geq 0$, Y_n is a free G-set, hence the associated G-module $F_n = \mathbb{Z}[Y_n]$ is a free $\mathbb{Z}[G]$-module. To give a basis for F_n we may take one element from each G-orbit in Y_n. But because Y is the universal cover of $K(G,1)$, the G-orbits on Y_n correspond to the elements of X_n. Thus

$$F_n \cong_{\mathbb{Z}[G]} \bigoplus_{C \in X_n} \mathbb{Z}[G]C. \tag{20}$$

Step 2: As for any CW-complex, we have a boundary map $d_n : F_n \to F_{n-1}$ and thus a complex $F_\bullet$, whose homology computes the topological homology of Y. Because Y is contractible, by Exercise X.X the augmented complex $F_\bullet \stackrel{d_0}{\to} \mathbb{Z} \to 0$ is acyclic.

Thus it gives a free resolution of $\mathbb{Z}$ over $\mathbb{Z}[G]$!
Step 3: It follows that for all $n \geq 0$,

$$H_n(G, \mathbb{Z}) = H_n(F_\bullet \otimes_{\mathbb{Z}[G]} \mathbb{Z}).$$

Since $F_n \cong \bigoplus_{C \in X_n} \mathbb{Z}[G]C$, $F_n \otimes_{\mathbb{Z}[G]} \mathbb{Z} \cong \bigoplus_{C \in X_n} \mathbb{Z}$. It follows that $F_\bullet \otimes_{\mathbb{Z}[G]} \mathbb{Z} \cong C_\bullet(X)$ is precisely the singular complex of X, so its homology is the integral homology of X! This proves part a).
Step 4: Part b) is proved similarly using $\mathrm{Hom}_{\mathbb{Z}[G]}(\cdot, \mathbb{Z})$ in place of $\cdot \otimes_{\mathbb{Z}[G]} \mathbb{Z}$. $\square$

Exercise: Let M be an abelian group, viewed as a trivial G-module. Show that

$$H_*(K(G,1), M) \cong H_*(G, M),$$
$$H^*(K(G,1), M) \cong H^*(G, M).$$

Remark: It is natural to want to push things even farther. If M is a nontrivial G-module, can $H_*(G, M)$ and $H^*(G, M)$ be interpreted topologically? The answer is *yes*: they can be so interpreted in terms of more general objects on $K(G,1)$ called **local systems**. However, exactly what these things are is a bit technical. A nice modern take on this is that $H^*(G, M) = H^*(K(G,1), \mathcal{M})$ where $\mathcal{M}$ is an associated **locally constant sheaf** and the cohomology is sheaf cohomology. Unfortunately, as usual, except for annoying isolated remarks, sheaves and their cohomology are beyond the scope of this course.

References

[AB59] M. Auslander and D.A. Buchsbaum, *Unique factorization in regular local rings.* Proc. Nat. Acad. Sci. U.S.A. 45 (1959), 733-734.

[At89] M.F. Atiyah, *K-theory.* Notes by D. W. Anderson. Second edition. Advanced Book Classics. Addison-Wesley Publishing Company, Redwood City, CA, 1989.

[AM] M.F. Atiyah and I.G. Macdonald, *Introduction to commutative algebra.* Addison-Wesley Publishing Co., Reading Mass.-London-Don Mills, Ont. 1969.

[Bae36] R. Baer, *The Subgroup of the Elements of Finite Order of an Abelian Group.* Annals of Mathematics, Second Series, Vol. 37, No. 4 (Oct., 1936), pp. 766–781.

[Bae37] R. Baer, *Abelian groups without elements of finite order.* Duke Math. J. 3 (1937), 68-122.

[Bae40] R. Baer, *Abelian groups that are direct summands of every containing abelian group.* Bull. Amer. Math. Soc. 46 (1940), 800-806.

[Bas59] H. Bass, *Global dimension of rings*, Ph.D. Thesis, University of Chicago, 1959.

[Br] K.S. Brown, *Cohomology of groups.* Corrected reprint of the 1982 original. Graduate Texts in Mathematics, 87. Springer-Verlag, New York, 1994.

[B] N. Bourbaki, *Commutative algebra. Chapters 1-7.* Translated from the French. Reprint of the 1989 English translation. Elements of Mathematics (Berlin). Springer-Verlag, Berlin, 1998.

[CA] P.L. Clark, *Commutative Algebra.*

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

[CW] S. Mac Lane, *Categories for the working mathematician.*

[DM71] F. DeMeyer and E. Ingraham, *Separable algebras over commutative rings.* Lecture Notes in Mathematics, Vol. 181 Springer-Verlag, Berlin-New York 1971.

[Ec53] B. Eckmann, *Cohomology of groups and transfer.* Ann. of Math. (2) 58 (1953), 481-493.

[ES53] B. Eckmann and A. Schopf, *Über injektive Moduln.* Arch. Math. (Basel) 4 (1953), 75-78.

[Eis] D. Eisenbud, *Commutative algebra. With a view toward algebraic geometry.* Graduate Texts in Mathematics, 150. Springer-Verlag, New York, 1995.

[ERZ57] S. Eilenberg, A. Rosenberg and D. Zelinsky, *On the dimension of modules and algebras. VIII. Dimension of tensor products.* Nagoya Math. J. 12 (1957), 71-93.

[Fl08] M. Flach, *Cohomology of topological groups with applications to the Weil group* Compos. Math. 144 (2008), no. 3, 633-656.

[FT] *Field Theory*, notes by P.L. Clark, available at `http://www.math.uga.edu/~pete/FieldTheory.pdf`

[FW67] C. Faith and E.A. Walker, *Direct-sum representations of injective modules.* J. Algebra 5 (1967), 203-221.

[Gov65] V.E. Govorov, *On flat modules.* (Russian) Sibirsk. Mat. Ž. 6 (1965), 300-304.

[H] A. Hatcher, *Algebraic Topology.*

[Hel40] O. Helmer, *Divisibility properties of integral functions.* Duke Math. J. 6 (1940), 345-356.

[J1] N. Jacobson, *Basic algebra. I.* Second edition. W. H. Freeman and Company, New York, 1985.

[J2] N. Jacobson, *Basic algebra. II.* Second edition. W. H. Freeman and Company, New York, 1989.

[Ja69] A.V. Jategaonkar, *A counter-example in ring theory and homological algebra.* J. Algebra 12 (1969), 418-440.

[Ka58] I. Kaplansky, *Projective modules.* Ann. of Math. 68 (1958), 372-377.

[Ka58b] I. Kaplansky, *On the dimension of modules and algebras. X. A right hereditary ring which is not left hereditary.* Nagoya Math. J. 13 (1958), 85-88.

[K] I. Kaplansky, *Commutative rings.* Allyn and Bacon, Inc., Boston, Mass. 1970.

[Ka08] M. Karoubi, *K-theory. An introduction.* Reprint of the 1978 edition. With a new postface by the author and a list of errata. Classics in Mathematics. Springer-Verlag, Berlin, 2008.

[Lam99] T.Y. Lam, *Lectures on modules and rings.* Graduate Texts in Mathematics, 189. Springer-Verlag, New York, 1999.

[Lam06] T.Y. Lam, *Serre's problem on projective modules.* Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2006.

[Lan02] S. Lang, *Algebra.* Revised third edition. Graduate Texts in Mathematics, 211. Springer-Verlag, New York, 2002.

[LM] M.D. Larsen and P.J. McCarthy, *Multiplicative theory of ideals.* Pure and Applied Mathematics, Vol. 43. Academic Press, New York-London, 1971.

[Laz64] D. Lazard, *Sur les modules plats.* C. R. Acad. Sci. Paris 258 (1964), 6313-6316.

[M] H. Matsumura, *Commutative ring theory.* Translated from the Japanese by M. Reid. Second edition. Cambridge Studies in Advanced Mathematics, 8. Cambridge University Press, Cambridge, 1989.

[NCA] P.L. Clark, *Noncommutative Algebra.* Notes available at `http://math.uga.edu/~pete/noncommutativealgebra.pdf`

[Pa59] Z. Papp, *On algebraically closed modules.* Publ. Math. Debrecen 6 (1959), 311-327.

[Qui76] D. Quillen, *Projective modules over polynomial rings.* Invent. Math. 36 (1976), 167-171.

[Rot] J.J. Rotman, *An introduction to homological algebra.* Second edition. Universitext. Springer, New York, 2009.

[Sch08] S. Schröer, *Baer's result: the infinite product of the integers has no basis.* Amer. Math. Monthly 115 (2008), 660-663.

[S-CG] J.-P. Serre, *Cohomologie Galoisienne.*

[S-CL] J.-P. Serre, *Corps Locaux.*

[Sp50] E. Specker, *Additive Gruppen von Folgen ganzer Zahlen.* Portugal. Math. 9 (1950), 131-140.

[St68] J.R. Stallings, *On torsion-free groups with infinitely many ends.* Ann. of Math. (2) 88 (1968), 312-334.

[Su76] A.A. Suslin, *Projective modules over polynomial rings are free.* Dokl. Akad. Nauk SSSR 229 (1976), 1063-1066.

[Sw62] R.G. Swan, *Vector bundles and projective modules.* Trans. Amer. Math. Soc. 105 (1962), 264-277.

[Sw69] R.G. Swan, *Groups of cohomological dimension one.* J. Algebra 12 (1969), 585-610.

[T] Grothendieck, Tohoku...

[W] C.A. Weibel, *An introduction to homological algebra.* Cambridge Studies in Advanced Mathematics, 38. Cambridge University Press, Cambridge, 1994.

[We80] R.O. Wells Jr., *Differential analysis on complex manifolds.* Second edition. Graduate Texts in Mathematics, 65. Springer-Verlag, New York-Berlin, 1980.

[Wi69] J. Wiegold, $\mathrm{Ext}(\mathbb{Q}, \mathbb{Z})$ *is the additive group of real numbers.* Bull. Austral. Math. Soc. 1 (1969), 341-343.

[Wi] J.S. Wilson, *Profinite Groups.*