Chapter 5

Projective and Injective Modules

While the beginning of the book is a general introduction to homological algebra, in this chapter we start to see the ramifications of homological methods in the realm of commutative algebra. In particular, we begin by understanding the structure of projective and injective *modules*, and use them as a tool to understand modules in general. While usually the theory is developed for noncommutative rings, we will confine ourselves to the commutative case, leaving the general case for some exercises.

The simplest to understand are projective modules. In Section 5.1, we see that they are not far from being the same as locally free modules. This gives us some geometric intuition on the behavior of projective modules. As an application of the techniques of this section, we also prove a theorem of Vasconcelos about finite generation of ideals. In Section 5.2, we define the projective dimension of a module as the length of the shortest projective resolution. This is a fairly well-behaved notion, and we obtain results that allow us to link the projective dimension of modules across various operations, such as quotients, localizations and polynomial rings.

In Section 5.3 we turn to injective modules. These are much less intuitive objects. Our workhorse is Baer's criterion, this allows us to test for injectivity of a module using only monomorphisms of the form $I \to A$, where I is an ideal of the ring A. We use this to prove the celebrated theorem of Bass-Papp, that states that a ring A is Noetherian if and only if injective objects are stable under direct sum. This brings an unexpected link between homological techniques and finiteness conditions. In the rest of the section, we use the notion of injective hull from Section 2.7 to develop a classification theorem for injective modules over Noetherian rings, due to Matlis.

In Section 5.4, we define the notion of injective dimension, which is dual to that of projective dimension. Most of the results are analogous to those of Section 5.2. The main point of departure is the use of Baer's criterion, which allows us to prove a theorem of Kaplansky's that states that the injective dimension of a module M over a local Noetherian ring $A, \mathcal{M}$ can be computed just by looking at the groups $\operatorname{Ext}^i_A(A/\mathcal{M}, M)$.

In Section 5.5 we define the global dimension of a ring as the supremum of the projective dimensions of its modules, or equivalently as the supremum of the injective dimensions of its modules. Many results on global dimension are immediate consequences of the previous sections. The main result of the section is Theorem 5.5.7, which states that the global dimension grows by one when passing from a ring A to the polynomial ring $A[x]$. This is as an abstract version of the famous Hilbert syzygy theorem, which can be seen as the first result of homological algebra.

Hilbert's theorem, though, is concerned with free resolutions (over the ring $k[x_1, \ldots, x_n]$), while the bounds on global dimension only produce projective resolutions. To link the two, one needs to know that a finitely generated projective module over $k[x_1, \ldots, x_n]$) is free. This was conjectured by Serre, who proved a weaker version, and finally proved by Quillen and Suslin. Section 5.7 is devoted to the proof of Serre's theorem, and more generally to the concept of stably free modules. The main result is Theorem 5.7.12, which allows us to produce finite free resolutions in polynomial rings. As a consequence, we also prove Hilbert's syzygy theorem. Of course, Hilbert's original proof did not use all of this machinery, and was in fact quite elementary. We present it in the exercises. Finally, in Section 5.8 we prove the theorem of Quillen and Suslin.

5.1. Projective and free modules

In this section, we investigate the basic properties of projective modules. Recall from Proposition 2.6.4 that an A-module P is projective if and only if it is a direct summand of a free module. In particular, all free modules are projective. The converse is not true, save in simple cases.

Example 5.1.1.

(a) Let A be a principal ideal domain. Then every submodule of a free A-module is free—in particular every projective A-module. This is Theorem A.2.4, and we quickly recall the proof. Let $F = \bigoplus_{s \in S} A_s$ be a free A-module, where each A_s is just a copy of A, and let $N \subset F$ be a submodule. We can prove that N is free by transfinite induction. Namely, take a well-ordering of S and for $s \in S$ define

$$F_{\leq s} := \bigoplus_{t \leq s} F_t$$
$$F_{<s} := \bigoplus_{t<s} F_t.$$

Similarly, let $N_{\leq s} := N \cap F_{\leq s}$ and $N_{<s} := N \cap F_{<s}$. The quotient $N_{\leq s}/N_{<s}$ is a submodule of A_s, so it is either 0 or generated by a single element n_s. If $S' \subset S$ is the set for which this quotient is not 0, we claim that $\{n_s\}_{s \in S'}$ is a basis of N.

To check this, we have to prove that the $\{n_s\}_{s \in S'}$ are linearly independent, and that they generate N. Both of these claims are easy to verify; for details, see [**Fer20**, Theorem 2.1.5].

Conversely, an integral domain having the property that every submodule of a free module is itself free is a principle ideal domain (PID). To see this, let A be an integral domain with this property, and let $I \subset A$ be an ideal. Then I is a free A-module. If I had at least two generators $a, b \in I$, there there would be a nontrivial relation $ab - ba = 0$, hence I can have at most one generator, and A is a PID.

(b) Let A be a Dedekind ring. By Theorem A.5.5, a finitely generated A-module M is projective if and only if it is torsion-free. The details of the argument are fleshed out in the first volume, but since it is an important example, we briefly review them here.

First, take two different nonzero ideals $I, J \subset A$. If $I + J = A$, then $I \cap J = I \cdot J$, and the exact sequence

$$0 \longrightarrow IJ \longrightarrow I \oplus J \longrightarrow A \longrightarrow 0$$

splits, since A is free. It follows that $I \oplus J \cong A \oplus IJ$ as A-modules. The same is true for *any* pair of ideals I, J. To see this, it is enough to switch J for an ideal J' which has the same class in the class group $G(A)$, but having the property that $I + J' = A$.

Given a nonzero ideal $I \subset A$ and $x \in I$, $x \neq 0$, one can find an ideal J such that $I \cdot J = (x)$ by Theorem A.5.4. In this case, we obtain the isomorphism $I \oplus J \cong A \oplus (x) \cong A \oplus A$, showing that I is a direct summand of a free A-module, hence I is projective.

Now let M be a finitely generated A-module that is a direct sum of ideals, and $N \subset M$ a submodule. By induction on the rank of M, one can find ideals $J_k \subset I_k$ and elements $m_1, \ldots, m_r \in M$ such that

$$M \cong I_1 m_1 \oplus \cdots \oplus I_k m_k,$$
$$N \cong J_1 m_1 \oplus \cdots \oplus J_k m_k.$$

It follows that a finitely generated A-module M can be written as $M = T \oplus P$, where T is a direct sum of modules of the form I/J, where $0 \neq J \subset I \subset A$ are ideals, and P is a direct sum of ideals. In the first case, one can find $x \in I \setminus J$ such that $I \cong J + (x)$, and then

$$\frac{I}{J} \cong \frac{J + (x)}{J} \cong \frac{(x)}{(x) \cap J};$$

this is a quotient of (x), so it is isomorphic to a quotient of A. Hence $T \cong A/I_1 \oplus \cdots \oplus A/I_k$ for some ideals $I_1, \ldots, I_k$. In particular, T is torsion. In contrast, P is a direct sum of ideals, hence it is projective.

Thus, for Dedekind rings, torsion is the only obstruction to being projective, at least for finitely generated modules. For modules that are not finitely generated, all of this fails. For instance, $\mathbb{Q}$ is torsion-free, but it is not a free $\mathbb{Z}$-module, hence it is not projective. Notice that in this case, any ideal which is not principal will be a projective A-module that is not free. (Why?)

(c) Actually, projective modules that are not free are quite common. For instance, let A be any ring and consider the $A \times A$-module $A \oplus 0$. This is clearly a direct summand of $A \oplus A$, but it is usually not free. For instance, if A is finite, this is not free for cardinality reasons.

(d) Let X be a topological space, $A = C(X)$ the ring of (real-valued) continuous functions on X. If $E \to X$ is a real vector bundle of dimension n, we can multiply the sections of E by functions in $C(X)$ pointwise, this gives $M = C(E)$ the structure of an A-module. M is in general not free, but by the definition of vector bundle, E is locally isomorphic to a product $\mathbb{R}^n \times U \to U$, where $U \subset X$ is an open set. It follows that $C(E|_U)$ is a free $C(U)$-module of rank n.

Now assume that X is compact and paracompact. Then we can cover X with finitely many such open sets where E is trivial. By extending each of them and taking the direct sum, it follows that E is a subvector bundle of a trivial vector bundle $F \to X$. By taking a Riemannian metric on F, we can write $F = E \oplus E'$, where $E' = E^{\perp}$ is the orthogonal vector bundle. It follows that $C(E)$ is a *projective* $C(X)$-module. You are asked to flesh out this argument more precisely in Exercise 15.

Taking the last example as a guide, one can get a decent intuition on projective modules by thinking of projective modules as vector bundles, and free modules as trivial vector bundles. This suggests that projective modules should be locally free, in other words, that projective modules over local rings should be free. This turns out to be true.

Theorem 5.1.2 (Kaplansky). *Let A be a local ring, P a projective A-module. Then P is free.*

The above theorem has an easy proof when we assume that P is finitely generated (Exercise 1). The general case is more subtle; our approach follows [**Mat86**, Theorem 2.5]. The proof reduces to the case of countably generated modules via the following

Lemma 5.1.3. *Let A be a ring, M an A-module which is the direct sum of countably generated submodules, N a direct summand of M. Then N is itself a direct sum of countably generated submodules.*

Proof. Write $M = N \oplus P$. By hypothesis, $M = \bigoplus_{i\in I} M_i$, where the M_i are countably generated submodules of M. Given a set $J \subset I$, write $M_J = \bigoplus_{i\in J} M_i$, $N_J = M_J \cap N$, and $P_J = M_J \cap P$.

Consider all sets $J \subset I$ such that $M_J = N_J \oplus P_J$ and N_J, P_J are direct sums of countably generated submodules. By Zorn's lemma, we can take a maximal such J, and we only need to show that $J = I$. If this is not the case, we can find $i_1 \in I \setminus J$. Let $I_1 = \{i_1\}$ and $J_1 = J \cup I_1$. In general, $M_{J_1} \supset N_{J_1} \oplus P_{J_1}$, and the inclusion can be strict. But since M_{i_1} is countably generated, there is a countable set $I_2 \supset I_1$ such that $M_{J_1} \subset N_{J_2} \oplus P_{J_2}$, where $J_2 = J \cup I_2$. Recursively, we can find an increasing chain $I_1 \subset I_2 \subset I_3 \subset \cdots$ of countable sets disjoint from J such that, letting $J_k := J \cup I_k$, we have the inclusions $M_{J_k} \subset N_{J_{k+1}} \oplus P_{J_{k+1}}$ for all k.

If we let $I_\infty = \bigcup_{k=1}^{\infty} I_k$ and $J_\infty = J \cup I_\infty$, we obtain the equality $M_{J_\infty} = N_{J_\infty} \oplus P_{J_\infty}$. Since N_J is a direct summand of M_J, we can write $M = N_J \oplus M'$, whence $N_{J\infty} = N_J \oplus (M' \cap N_{J_\infty})$. Let $N'_{J_\infty} = N_{J_\infty} \cap M'$, and define P'_{J_∞} similarly. Using these, we can write

$$M_{J_\infty} = N_J \oplus P_J \oplus N'_{J_\infty} \oplus P'_{J_\infty}.$$

From this we deduce that

$$N'_{J_\infty} \oplus P'_{J_\infty} \cong \frac{M_{J_\infty}}{M_J} \cong M_{I_\infty}.$$

By construction, M_{I_∞} is countably generated, hence the same is true for N'_{J_∞} and P'_{J_∞}, which are its summands. It follows that N_{J_∞} and P_{J_∞} are the direct sum of countably generated modules, and this a contradiction, since J_∞ is strictly larger than J. □

Lemma 5.1.4. *Let $(A, \mathcal{M})$ be a local ring, P a projective A-module, and $x \in P$. Then there exists a free module F which is a direct summand of P, such that $x \in F$.*

Proof. Since P is projective, we can find a free module G such that $G \cong P \oplus Q$. Given a basis $B = \{g_i\}$ of G, we can write $x = \sum_{i=1}^n a_i g_i$, where $a_i \in A$. Choose such a basis B and a representation of x such that n is minimal. Writing $g_i = p_i + q_i$, where $p_i \in P$ and $q_i \in Q$, we obtain $x = \sum_{i=1}^n a_i p_i$. In turn, we can express

$$p_i = \sum_{j=1}^n b_{ij} g_j + c_i,$$

where $b_{ij} \in A$ and c_i is a linear combination of elements of B which are not one of $g_1, \dots, g_n$. This allows us to write

$$x = \sum_{i=1}^n \sum_{j=1}^n a_i b_{ij} g_j.$$

Since the expression for x is unique, we obtain relations $a_i = \sum_{j=1}^n a_j b_{ji}$ for $i = 1, \dots n$.

If for any such relation we had an invertible coefficient, we could write one of the a_i as a combination of the other ones, and in turn we could write x using less than n elements of B. By minimality, it follows that $1 - b_{ii} \in \mathcal{M}$ for all i and $b_{ij} \in \mathcal{M}$ for all $i \neq j$. This entails that the determinant of the matrix (b_{ij}) is $\equiv 1 \pmod{\mathcal{M}}$, and so $\det(b_{ij}) \in A^*$. We can then define an inverse of the matrix (b_{ij}) by Cramer's rule, and this inverse has coefficients in A as well. Using the inverse allows us to write $g_1, \dots, g_n$ as linear combinations of $p_1, \dots, p_n$ and other elements of B other than $g_1, \dots, g_n$.

The conclusion of all this is that if we replace $g_1, \dots, g_n$ by $p_1, \dots, p_n$ inside B, we obtain another basis of G. We can then take F to be the free module generated by $p_1, \dots, p_n$: it contains x and it is a direct summand of G, hence of P. □

Remark 5.1.5. The argument in the lemma is essentially the determinant trick that is used in one proof of Nakayama's lemma; see [**Fer20**, Theorem 5.1.8]. One cannot resort directly to Nakayama's lemma, though, without a hypothesis of finite generation.

Proof of Theorem 5.1.2. Since P is projective, it is a direct summand of a free module, so Lemma 5.1.3 applies, and P is a direct sum of countably generated modules, which are then projective. Hence, it is enough to prove the theorem for a countably generated projective module P. Let $p_1, p_2, \dots$ be generators of P. Using Lemma 5.1.4 we find a free module $F_1 \ni p_1$ such that $P \cong F_1 \oplus P_1$. We let p_i' be the projection of p_i in P_1 for $i \geq 2$. Since P_1 is again projective, we can find a free module $F_2 \ni p_2'$ such that $P_1 \cong F_2 \oplus P_2$. By continuing in this fashion we find free modules F_i such that $p_i \in F_1 \oplus \cdots \oplus F_i$ for all i, which implies that $P \cong F_1 \oplus F_2 \oplus \cdots$ is free as well. □

Remark 5.1.6. With a little care, the proof of Theorem 5.1.2 also works for noncommutative rings, where a noncommutative ring A is called local if for all $x \in A$ either x or $1 - x$ is invertible [**AF12**, Corollary 26.7].

Kaplansky's theorem reinforces the intuition that projective modules can be seen as an algebraic analogue of vector bundles. Still, one may want to be able to say a little more: that projective modules are actually locally free.

Definition 5.1.7. Let M be an A-module. We say that M is *locally free* if M_P is a free A_P-module for all prime ideals $P \subset A$.

To discuss the relation between projective and locally free modules, we need to understand how projective modules behave under localization. This, in turn, prompts us to understand the behavior of Ext under localization.

Definition 5.1.8. Let M be an A-module. A *presentation* of M is an exact sequence

$$F_1 \longrightarrow F_0 \longrightarrow M \longrightarrow 0,$$

where F_0 and F_1 are free A-modules. If M admits such a presentation with F_0 and F_1 finite free, we say that M is *finitely presented*. More generally, if M admits an exact sequence

$$F_k \longrightarrow F_{k-1} \longrightarrow \cdots \longrightarrow F_0 \longrightarrow M \longrightarrow 0$$

with $F_0, \ldots, F_k$ finite free, we say that M is *k-finitely presented*.

A presentation of M is just a way to give explicit generators $\{m_i\}$ for M and explicit generators for the relations between the $\{m_i\}$.

Remark 5.1.9. A module M is 0-finitely presented if and only if it is finitely generated, and 1-finitely presented if and only if it is finitely presented. If A is Noetherian and M is finitely generated, then M is k-finitely presented for all k (can you see why?).

Proposition 5.1.10. *Let A be a ring, M a k-finitely presented A-module. Then, for all multiplicative subsets $S \subset A$ and all A-modules N,*

$$S^{-1} \operatorname{Ext}^i_A(M, N) \cong \operatorname{Ext}^i_{S^{-1}A}(S^{-1}M, S^{-1}N)$$

for $i < k$.

Proof. Denote, for reasons of space, $A' = S^{-1}A$, $M' = S^{-1}M$ and so on. For $k = 1$ we have a commutative diagram

$$\begin{array}{ccccccc} 0 \longrightarrow & \mathrm{Hom}_A(M,N)' & \longrightarrow & \mathrm{Hom}_A(F_0,N)' & \longrightarrow & \mathrm{Hom}_A(F_1,N)' \\ & \downarrow & & \downarrow & & \downarrow \\ 0 \longrightarrow & \mathrm{Hom}_{A'}(M',N') & \longrightarrow & \mathrm{Hom}_{A'}(F_0',N') & \longrightarrow & \mathrm{Hom}_{A'}(F_1',N'), \end{array}$$

which is exact on the left because h^N is left exact and localization is exact. The two vertical arrows on the right are isomorphisms, because F_0 and F_1 are finite free, hence the left arrow is an isomorphism as well by the five lemma (Lemma 2.5.1).

For $k > 1$ the result follows by dimension shifting (Proposition 3.3.2), because the F_i and $S^{-1}F_i$ are acyclic for Hom. □

By Remark 5.1.9 we immediately obtain:

Corollary 5.1.11. *Let A be a Noetherian ring, M a finitely generated A-module. Then, for all multiplicative subsets $S \subset A$ and all A-modules N,*

$$S^{-1}\,\mathrm{Ext}^i_A(M,N) \cong \mathrm{Ext}^i_{S^{-1}A}(S^{-1}M, S^{-1}N)$$

for all $i \in \mathbb{N}$.

Remark 5.1.12. Since an A-module P is projective if and only if $\mathrm{Ext}^1(P,-)$ vanishes, we also obtain that if P if a finitely generated, projective A-module and A is Noetherian, then $S^{-1}P$ is a projective $S^{-1}A$-module for all multiplicative subsets $S \subset A$. With a slightly different proof, this can be stated in more generality:

Proposition 5.1.13. *Let $f\colon A \to B$ be a ring homomorphism, P a projective A-module. Then $B \otimes_A P$ is a projective B-module.*

Proof. The adjunction of Example 1.5.2(f) gives an isomorphism

$$\mathrm{Hom}_B(B \otimes_A P, N) \cong \mathrm{Hom}_A(P,N)$$

for all B-modules N. This means that $h^{B\otimes_A P}$ is the composition of h^P and the forgetful functor $\mathrm{Mod}_B \to \mathrm{Mod}_A$, both of which are exact. □

In particular, this applies to the localization map $A \to A_P$ for a prime ideal P. Combining this with Kaplansky's theorem, Theorem 5.1.2, we finally get:

Corollary 5.1.14. *Let A be a ring, M a projective A-module. Then M is locally free, that is, for all prime ideals $P \subset A$, the A_P-module M_P is free.*

Under some finiteness conditions, the converse holds. These finiteness conditions are necessary, see Exercise 4.

Proposition 5.1.15. *Let M be a finitely presented A-module. Then M is projective if and only if it is locally free.*

Proof. We only need to prove one implication. Fix a free module F with a surjection $F \to M$, and let $P \subset A$ be a prime. Assuming that M_P is free, $\mathrm{Hom}(M_P, F_P) \to \mathrm{Hom}(M_P, M_P)$ is surjective as well. Since M is finitely presented, Proposition 5.1.10 gives isomorphisms

$$\mathrm{Hom}_{A_P}(M_P, F_P) \cong \mathrm{Hom}_A(M, F)_P \text{ and}$$
$$\mathrm{Hom}_{A_P}(M_P, M_P) \cong \mathrm{Hom}_A(M, M)_P.$$

If this holds for all primes P, Proposition 2.2.21, implies that $\mathrm{Hom}(M, F) \to \mathrm{Hom}(M, M)$ is surjective, and in particular id_M is in the image. This shows that the surjection $F \to M$ splits, hence M is a direct summand of F. □

Remark 5.1.16. A finitely generated projective A-module is finitely presented. In fact, assume that M is projective and that we have a surjection $\phi\colon A^k \to M$. Then ϕ splits, so if we let $K = \ker \phi$, we get an isomorphism $A^k \cong K \oplus M$, showing that K is finitely generated as well.

A nice application of the result of Kaplansky is the following criterion of Vasconcelos, who uses it to derive a finiteness result [**Vas73**].

Proposition 5.1.17 (Vasconcelos)**.** *Let A be a ring, $I \subset A$ a projective ideal. If I is not contained in any minimal prime of A, I is finitely generated.*

The connection with Kaplansky's theorem passes through the following notion.

Definition 5.1.18. Let P be a projective A-module. The *trace* of P is the ideal $\tau_A(P)$ (or simply $\tau(P)$ when the ring is fixed) generated by $f(P)$ for all homomorphisms $f\colon P \to A$. In other words, $\tau(P)$ is the image of the evaluation morphism $\mathrm{Hom}(P, A) \otimes_A P \to A$.

Exercise 18 clarifies the reason for the name "trace." To better understand this ideal, assume that we have a decomposition $F = P \oplus Q$, where F is a free A-module, and that we have chosen a basis $\{v_i\}_{i \in I}$ of F. Then we have corresponding coordinate functions c_i defined by $c_i(\sum_j a_j v_j) = a_i \in A$, and we can restrict them to P.

On the other hand, any homomorphism $f\colon P \to A$ can be extended to F. Consider the free module $F' = F \oplus A$, and let u be a generator of the last summand. Then a basis for F' is $\{u\} \cup \{v_i - f(v_i)u\}_{i \in I}$. With this choice, $f(v_i)$ is the u-coordinate of v_i for all $i \in I$, so that the u-coordinate function agrees with f on F.

We conclude that $\tau(P)$ is generated by the coordinates of elements of P for all decompositions $F = P \oplus Q$ of a free module and all choices of bases for F. Using this characterization, we can prove a change of ring result.

Proposition 5.1.19. *Let $g\colon A \to B$ be a ring homomorphism, M a projective A-module. Then $\tau_B(B \otimes_A M) = g(\tau_A(M)) \cdot B$.*

Notice that $B \otimes_A M$ is in fact a projective B-module by Proposition 5.1.13.

Proof. The diagram

$$\begin{array}{ccc} \mathrm{Hom}_A(M, A) \otimes_A M & \longrightarrow & A \\ \downarrow & & \downarrow g \\ \mathrm{Hom}_B(M, B) \otimes_B (B \otimes_A M) & \longrightarrow & B \end{array}$$

shows that $g(\tau_A(M)) \subset \tau_B(B \otimes_A M)$.

On the other hand, choose a decomposition of A-modules $F \cong M \oplus N$, where F is free with basis $\{v_i\}$. Then

$$F_B := B \otimes_A F \cong B \otimes_A M \oplus B \otimes_A N,$$

and it is enough to check that for any choice of basis of F_B, the corresponding coordinate functions send $B \otimes_A M$ into $g(\tau_A(M)) \cdot B$. Let $\{w_i\}$ be such a basis, and choose $m \in M, b \in B$. With a small abuse of notation, denote g the induced map $F \to F_B$. For each i write

$$g(v_i) = \sum_j b_{ij} w_j,$$

where the sum is finite. Then if a_i are the coordinates of m in the basis $\{v_i\}$,

$$b \otimes m = b \sum_i g(a_i) g(v_i) = \sum_{i,j} b b_{ij} g(a_i) w_j,$$

so the w_j-coordinate of $b \otimes m$ is $\sum_i b b_{ij} g(a_i) \in g(\tau_A(M)) \cdot B$. □

Corollary 5.1.20. *Let $P \subset A$ be a prime ideal, M a projective A-module, $J = \tau_A(M)$ the trace ideal.*

(i) *If $J \subset P$, $J_P = 0$; and*

(ii) *If $J \not\subset P$, $J_P = A_P$.*

Proof. By the proposition, $J_P = \tau_{A_P}(A_P \otimes_A M) = \tau_{A_P}(M_P)$. The A_P-module M_P is projective, hence free by Theorem 5.1.2. It follows that $J_P = A_P$, unless $M_P = 0$, in which case $J_P = 0$. On the other hand, $J_P = A_P$ happens if and only if $J \not\subset P$. □

Proof of Proposition 5.1.17. Let $J = \tau_A(I)$ be the trace ideal of I. By construction, $I \subset J$. First, assume that J is not all of A, and take a maximal ideal $\mathcal{M} \supset J$. By hypothesis, $\mathcal{M}$ is not a minimal prime, hence by Theorem A.1.2, $\mathcal{M}$ contains a minimal prime P.

In the ring A/P, the ideal $I/PI = A/P \otimes_A I$ has trace

$$\tau_{A/P}(I/PI) = A/P \otimes_A J = (J + P)/P.$$

But the latter is contained in $\mathcal{M}/P$, hence it is not the whole A/P. On the other hand, A/P is an integral domain, hence all localizations of $(J+P)/P$ are different from 0. By Corollary 5.1.20, this means that $(J + P)/P$ is not contained in any prime ideal of A/P, a contradiction.

We conclude that $\tau_A(I) = A$, which means that we can find n homomorphisms $f_i \colon I \to A$ and elements $a_i \in I$ such that $\sum_{i=1}^{n} f_i(a_i) = 1$. Given any element $x \in I$, we can use this to write

$$x = \sum_{i=1}^{n} x f_i(a_i) = \sum_{i=1}^{n} f_i(x) a_i,$$

which shows that $a_1, \ldots, a_n$ generate I. □

5.2. Projective dimension

In this section, we are going to study A-modules via their projective resolutions. The starting point is the following observation about the length of projective resolutions.

Proposition 5.2.1. *Let $\mathcal{A}$ be an Abelian category with enough projectives, A an object of $\mathcal{A}$. The following are equivalent:*

(i) *there exists a projective resolution*

$$0 \longrightarrow P_n \longrightarrow \cdots \longrightarrow P_1 \longrightarrow P_0 \longrightarrow A \longrightarrow 0$$

of length n; and

(ii) $\mathrm{Ext}^i(A, B) = 0$ *for all $i > n$ and all $B \in \mathcal{A}$.*

Proof. That (i) implies (ii) is clear, since we can use the resolution $P_\bullet$ to compute the Ext groups.

Conversely, assume (ii) and take any projective resolution $P_\bullet \to A$. If $K = \ker(P_{n-1} \to P_{n-2})$, then $\mathrm{Ext}^1(K, -) = 0$ by Proposition 3.3.2. Hence, K is projective and we can substitute K for P_n and get a projective resolution of length n. □

Definition 5.2.2. Let $\mathcal{A}$ be an Abelian category with enough projectives, $X \in \mathcal{A}$. The minimal length of a projective resolution of X will be called the *projective dimension* of X, and denoted $\operatorname{pd} X$. If X does not admit any projective resolution of finite length, we set $\operatorname{pd} X = \infty$.

When $\mathcal{A} = \mathrm{Mod}_A$ is the category of modules over the ring A, we sometimes denote projective dimension by pd_A for clarity.

By the above result, $\operatorname{pd} X$ is the also minimum n (if any) such that $\operatorname{Ext}^i(X, -) = 0$ for $i > n$.

Example 5.2.3.

(a) Let A be a principal ideal domain. By Example 5.1.1(a), every A-module has projective dimension at most 1. In fact, let M be an A-module, and take an epimorphism $f\colon F \to M$ with F free. Since $K := \ker f$ is free, M admits a free resolution

$$0 \longrightarrow K \longrightarrow F \longrightarrow M \longrightarrow 0$$

with two terms.

(b) Let A be a Dedekind ring, M a finitely generated A-module. By Theorem A.5.5 it follows immediately that $\operatorname{pd}_A M \leq 1$. In fact, the same is true for arbitrary A-modules, as will follow for instance by Proposition 5.5.3.

(c) Let $A = \mathbb{Z}/4\mathbb{Z}$, and consider the A-module $M = \mathbb{Z}/2\mathbb{Z}$. Seeing M as a quotient of A, we get an exact sequence

$$0 \longrightarrow \tfrac{\mathbb{Z}}{2\mathbb{Z}} \longrightarrow \tfrac{\mathbb{Z}}{4\mathbb{Z}} \longrightarrow \tfrac{\mathbb{Z}}{2\mathbb{Z}} \longrightarrow 0\ .$$

The first term in this sequence can also be seen as quotient of A, and so on. This leads us the the following infinite free resolution of M:

$$\cdots \longrightarrow \tfrac{\mathbb{Z}}{4\mathbb{Z}} \longrightarrow \tfrac{\mathbb{Z}}{4\mathbb{Z}} \longrightarrow \tfrac{\mathbb{Z}}{2\mathbb{Z}} \longrightarrow 0.$$

Applying $\operatorname{Hom}(-, \mathbb{Z}/2\mathbb{Z})$, we can compute that

$$\operatorname{Ext}^i_{\mathbb{Z}/4\mathbb{Z}}\left(\frac{\mathbb{Z}}{2\mathbb{Z}}, \frac{\mathbb{Z}}{2\mathbb{Z}}\right) = \frac{\mathbb{Z}}{2\mathbb{Z}}$$

for all $i \geq 0$. In particular, $\operatorname{pd}_{\mathbb{Z}/4\mathbb{Z}} \mathbb{Z}/2\mathbb{Z} = \infty$.

Remark 5.2.4. Let G be an Abelian group, so that $\operatorname{pd}_{\mathbb{Z}} G \leq 1$. If we assume that $\operatorname{Ext}^1(G, H) = 0$ for all other Abelian groups H, then G is projective, hence free. One may ask whether the condition $\operatorname{Ext}^1(G, \mathbb{Z}) = 0$ suffices. This is known as the Whitehead problem. Shelah proved in [**She74**] that this question is actually independent from the ZFC axioms!

We will be mostly interested in the notion of projective dimension in a category of modules. In particular, we want to understand how the projective dimension of modules changes under various operations. We start by discussing the graded case.

Recall from Definition 1.1.4(d) that when A is a graded ring, we distinguish between the category Mod_A of graded A-modules and the category Mod^u_A of ungraded ones. The functor that forgets the grading is denoted by $U\colon \mathrm{Mod}_A \to \mathrm{Mod}^u_A$.

We can use Proposition 2.6.8 to link the projective dimension in the graded and ungraded case. We state the result in slightly more generality.

Proposition 5.2.5. *Let $\mathcal{A}, \mathcal{B}$ be two Abelian categories with enough projectives, and $U\colon \mathcal{A} \to \mathcal{B}$ an exact functor such that for all $P \in \mathcal{A}$, P is projective if and only if $U(P)$ is. Then $\operatorname{pd} M = \operatorname{pd} U(M)$ for all $M \in \mathcal{A}$. In particular, for a graded A-module the projective dimensions in Mod_A and in Mod^u_A are the same.*

Proof. From a projective resolution

$$0 \longrightarrow P_n \longrightarrow \cdots \longrightarrow P_1 \longrightarrow P_0 \longrightarrow M \longrightarrow 0$$

of M of length n in $\mathcal{A}$, we get a projective resolution

$$0 \longrightarrow U(P_n) \longrightarrow \cdots \longrightarrow U(P_1) \longrightarrow U(P_0) \longrightarrow U(M) \longrightarrow 0$$

of $U(M)$ of length n, hence $\operatorname{pd} U(M) \leq \operatorname{pd} M$.

For the opposite inequality, assume that $\operatorname{pd} U(M) \leq n$, and consider a truncated resolution

$$P_{n-1} \longrightarrow \cdots \longrightarrow P_1 \longrightarrow P_0 \longrightarrow M \longrightarrow 0$$

of M. Denote $K := \ker P_{n-1} \to P_{n-2}$. Applying U we get a truncated resolution

$$U(P_{n-1}) \longrightarrow \cdots \longrightarrow U(P_1) \longrightarrow U(P_0) \longrightarrow U(M) \longrightarrow 0$$

of $U(M)$, and by Proposition 3.3.2, $U(K)$ is projective. It follows that K is projective as well, hence $\operatorname{pd} M \leq n$.

The final statement follows from Proposition 2.6.8. □

To relate the projective dimension of various modules, we start with a general result, known as the *change of ring* theorem for projective dimension.

Theorem 5.2.6. *Let $f\colon A \to B$ a homomorphism of rings, and M a B-module. Then*

$$\operatorname{pd}_A M \leq \operatorname{pd}_A B + \operatorname{pd}_B M.$$

Proof. This follows at once from the base change spectral sequence of Theorem 4.5.5. □

Taking appropriate choices of A and B, we find many useful specializations of this result, also known as change of ring theorems. In particular, we will investigate what happens under quotients, localization, and polynomial rings. We will follow the approach of [**Wei95**, Section 4.3].

Localization is the easiest case. If $P \subset A$ is a prime ideal, the localization functor $\mathrm{Mod}_A \to \mathrm{Mod}_{A_P}$ is exact, and for any projective A-module M, the localized A-module M_P is again projective by Proposition 5.1.13. The first part of the proof of Proposition 5.2.5 shows that for all A-modules M, $\operatorname{pd}_{A_P} M_P \leq \operatorname{pd}_A M$. In fact, we can state a little more under some finite generation assumptions.

Proposition 5.2.7. *Let A be a Noetherian ring, M a finitely generated A-module. Then there exists a maximal ideal $\mathcal{M} \subset A$ such that $\operatorname{pd}_A M = \operatorname{pd}_{A_\mathcal{M}} M_\mathcal{M}$, so*

$$\operatorname{pd}_A M = \sup_{\substack{P \subset A \\ prime}} \operatorname{pd}_{A_P} M_P = \sup_{\substack{\mathcal{M} \subset A \\ maximal}} \operatorname{pd}_{A_\mathcal{M}} M_\mathcal{M}.$$

Proof. Define $d(\mathcal{M}) := \operatorname{pd}_{A_\mathcal{M}} M_\mathcal{M}$. We can assume that $d(\mathcal{M}) < \infty$ for all maximal ideals $\mathcal{M}$, otherwise the result follows from the previous remark.

Consider a projective resolution

$$\cdots \longrightarrow P_2 \longrightarrow P_1 \longrightarrow P_0 \longrightarrow M \longrightarrow 0$$

and let $K_n := \ker P_{n-1} \to P_{n-2}$. Since A is Noetherian, we can choose the resolution so that all P_i are finitely generated. It follows that all K_i are finitely generated as well.

Since localization is exact, we get a projective resolution of $M_\mathcal{M}$ for all $\mathcal{M}$, and moreover $(K_n)_\mathcal{M} = \ker(P_n)_\mathcal{M} \to (P_{n-1})_\mathcal{M}$. By definition of $d(\mathcal{M})$, $(K_{d(\mathcal{M})})_\mathcal{M}$ is projective, hence free by Kaplansky's theorem, Theorem 5.1.2. Let $r(\mathcal{M})$ be the rank of this free $A_\mathcal{M}$-module.

We can choose a homomorphism $f_\mathcal{M} \colon A^{r(\mathcal{M})} \to K_{d(\mathcal{M})}$ such that the localization at $\mathcal{M}$ becomes an isomorphism. In other words, $\ker f_\mathcal{M}$ and $\operatorname{coker} f_\mathcal{M}$ become 0 in the localization at $\mathcal{M}$. Since they are finitely generated, there exists a single element $a_\mathcal{M} \notin \mathcal{M}$ such that $a_\mathcal{M} \cdot \ker f_\mathcal{M} = 0$ and $a_\mathcal{M} \cdot \operatorname{coker} f_\mathcal{M} = 0$.

The set of elements $\{a_\mathcal{M}\}$ generates the whole ring, hence we can choose a *finite* subset $\{a_{\mathcal{M}_1}, \ldots, a_{\mathcal{M}_t}\}$ that generates the whole ring. Let

$$d = \max\{d_{\mathcal{M}_1}, \cdots, d_{\mathcal{M}_t}\}.$$

We claim that $(K_d)_{\mathcal{M}}$ is free for all maximal ideals $\mathcal{M}$. To see this, choose i such that $a_{\mathcal{M}_i} \notin \mathcal{M}$. Then $f_{\mathcal{M}_i}$ becomes an isomorphism when localized at $\mathcal{M}$, that is to say, $(K_{d(\mathcal{M}_i)})_{\mathcal{M}}$ is free. But then, since $d \geq d(\mathcal{M}_i)$, $(K_d)_{\mathcal{M}}$ is projective. (Why?) Again, by Theorem 5.1.2, it is free.

By Proposition 5.1.15, we conclude that K_d is projective. But then $\operatorname{pd}_A M \leq d = d(\mathcal{M}_i)$ for one of the maximal ideals $\mathcal{M}_i$. □

The case of quotients is more subtle, and is handled by the following three results. All of them are proved by induction, based on the following observation.

Remark 5.2.8. Given an A-module M, we can choose a projective module P with a surjection $P \to M$. Let K be the kernel, so that we have the exact sequence

$$0 \longrightarrow K \longrightarrow P \longrightarrow M \longrightarrow 0 \ .$$

By Proposition 3.3.2, it follows immediately that $\operatorname{pd}_A M = 1 + \operatorname{pd}_A K$.

To state our change of rings results, it is convenient to introduce some terminology.

Definition 5.2.9. Let M be an A-module, $a \in A$. We say that a is *weakly M-regular* if it is not a divisor of 0 in M, that is, if $am = 0$ for some $m \in M$, then $m = 0$. If moreover $aM \subsetneq M$, a is called M-regular. In the case where $M = A$, we will simply speak of (weakly) regular elements.

Theorem 5.2.10 (First change of rings theorem)**.** *Let A be a ring, $a \in A$ a regular element, and let M be an $A/(a)$-module. Assume that $\operatorname{pd}_{A/(a)} M < \infty$. Then*

$$\operatorname{pd}_A M = 1 + \operatorname{pd}_{A/(a)} M.$$

Proof. We start with the remark that any module over $A/(a)$ cannot be projective as an A-module. Otherwise, it would be a direct summand of a free A-module, which is a contradiction since multiplication by a is injective on a free A-module.

The exact sequence

$$0 \longrightarrow A \xrightarrow{\cdot a} A \longrightarrow \frac{A}{(a)} \longrightarrow 0$$

gives us $\operatorname{pd}_A A/(a) \leq 1$, so in fact $\operatorname{pd}_A A/(a) = 1$. By Theorem 5.2.6, $\operatorname{pd}_A M \leq 1 + \operatorname{pd}_{A/(a)} M$.

We prove equality by induction on $\operatorname{pd}_{A/(a)} M$. If $\operatorname{pd}_{A/(a)} M = 0$, we have $\operatorname{pd}_A M = 1$, since we have excluded that $\operatorname{pd}_A M = 0$.

For the inductive step, take an epimorphism $P \to M$, where P is a projective $A/(a)$-module, and let K be the kernel. By Remark 5.2.8,

$\operatorname{pd}_{A/(a)} M = 1 + \operatorname{pd}_{A/(a)} K$, and by the inductive hypothesis $\operatorname{pd}_{A/(a)} K = \operatorname{pd}_A K - 1$. We finish the proof if we can show that $\operatorname{pd}_A M = 1 + \operatorname{pd}_A K$. This does *not* follow from Remark 5.2.8 because P is not projective as an A-module.

Still, the exact sequence

$$0 \longrightarrow K \longrightarrow P \longrightarrow M \longrightarrow 0$$

gives us a long exact sequence of $\operatorname{Ext}_A(-, N)$ groups for all A-modules N. Since $\operatorname{pd}_A P = 1$, from that sequence we conclude that $\operatorname{pd}_A M = 1 + \operatorname{pd}_A K$, *unless* $\operatorname{pd}_A M = \operatorname{pd}_A K = 1$ (in which case we know that $\operatorname{pd}_{A/(a)} K = 0$ and $\operatorname{pd}_{A/(a)} M = 1$).

To exclude this case, take another short exact sequence

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

this time of A-modules, with P' projective. If $\operatorname{pd}_A M = 1$, then K' is projective as well. By tensoring with $A/(a)$, we obtain

$$0 \longrightarrow \operatorname{Tor}_1^A(M, A/(a)) \longrightarrow \tfrac{K'}{aK'} \longrightarrow \tfrac{P'}{aP'} \longrightarrow M \longrightarrow 0.$$

Since $\operatorname{pd}_{A/(a)} M = 1$, by dimension shifting (Proposition 3.3.2) we obtain that $\operatorname{Tor}_1^A(M, A/(a))$ is projective. By Example 3.4.12(a),

$$\operatorname{Tor}_1^A(M, A/(a)) = \{m \in M \mid am = 0\} = M,$$

hence M is projective, a contradiction. □

Our second theorem is similar to the previous one, but starts from an A-module.

Theorem 5.2.11 (Second change of rings theorem)**.** *Let A be a ring, M an A-module and $a \in A$ an M-regular element. Then*

$$\operatorname{pd}_A M \geq \operatorname{pd}_{A/(a)} \frac{M}{aM}.$$

Proof. We can assume that $\operatorname{pd}_A M$ is finite, so the proof will be by induction on $\operatorname{pd}_A M$. The base case is $\operatorname{pd}_A M = 0$, in which case M is projective over A, hence M/aM is projective over $A/(a)$ by Proposition 5.1.13.

For the inductive case, consider an exact sequence

$$0 \longrightarrow K \longrightarrow P \longrightarrow M \longrightarrow 0 ,$$

where P is projective, so that $\operatorname{pd}_A K = \operatorname{pd}_A M - 1$. By induction, we know that $\operatorname{pd}_{A/(a)} K/aK \leq \operatorname{pd}_A K$. As in the previous proof, we tensor with $A/(a)$ to find the exact sequence

$$0 \longrightarrow \operatorname{Tor}_1^A(M, A/(a)) \longrightarrow \tfrac{K}{aK} \longrightarrow \tfrac{P}{aP} \longrightarrow \tfrac{M}{aM} \longrightarrow 0.$$

Our hypothesis tells us that a is not torsion on M, hence $\operatorname{Tor}_1^A(M, A/(a)) = 0$. We conclude that either M/aM is projective as an $A/(a)$-module, or

$$\operatorname{pd}_{A/(a)} \frac{M}{aM} = 1 + \operatorname{pd}_{A/(a)} \frac{K}{aK} \leq pd_A M,$$

and in both cases we are done. □

The last change of rings theorem deals with the case of a local ring.

Lemma 5.2.12. *Let A be a Noetherian ring, M a finitely generated A-module and $I \subset \mathcal{J}(A)$ an ideal. If M/IM is free as an A/I-module, then M is free.*

Proof. Choose a set $S \subset M$ of n elements such that its image is a basis of M/IM. This defines a map $f\colon A^n \to M$, which is surjective by Nakayama's lemma, and injective by Nakayama's lemma applied to $\ker f$. □

Theorem 5.2.13 (Third change of rings theorem)**.** *Let A be a Noetherian local ring with maximal ideal $\mathcal{M}$, $a \in \mathcal{M}$, and let M be a finitely generated A-module. If a is regular and M-regular, then*

$$\operatorname{pd}_A M = \operatorname{pd}_{A/(a)} \frac{M}{aM}.$$

Proof. If $\operatorname{pd}_{A/(a)} \frac{M}{aM} = \infty$, the equality follows from Theorem 5.2.11. Otherwise, we can prove the result by induction on $\operatorname{pd}_{A/(a)} \frac{M}{aM}$.

The base case is $\operatorname{pd}_{A/(a)} \frac{M}{aM} = 0$, in which case $\frac{M}{aM}$ is projective. Since $A/(a)$ is a local ring, $\frac{M}{aM}$ is free by Theorem 5.1.2. In this case, M is free by Lemma 5.2.12, hence $\operatorname{pd}_A M = 0$ as well.

For the inductive step, consider an exact sequence

$$0 \longrightarrow K \longrightarrow P \longrightarrow M \longrightarrow 0$$

where P is projective, so that $\operatorname{pd}_A K = \operatorname{pd}_A M - 1$. As in the previous proof, we tensor it with $A/(a)$ and use the vanishing of $\operatorname{Tor}_1^A(M, A/(a))$ to obtain the exact sequence

$$0 \longrightarrow \frac{K}{aK} \longrightarrow \frac{P}{aP} \longrightarrow \frac{M}{aM} \longrightarrow 0\ ,$$

from which we get $\operatorname{pd}_{A/(a)} K/aK = \operatorname{pd}_{A/(a)} M/aM - 1$.

We can choose P to be finitely generated (for instance a finitely generated free A-module). Since A is Noetherian, K is finitely generated as well. By induction, $\operatorname{pd}_A K = \operatorname{pd}_{A/(a)} K/aK$, hence $\operatorname{pd}_A M = \operatorname{pd}_{A/(a)} M/aM$. □

Remark 5.2.14. Since Theorem 5.2.13 requires an element that is both regular and M-regular, it is interesting to understand when such elements exist. Of course, a necessary condition is that there exist, separately, a regular element and an M-regular one. In the local case, this is sufficient as well. Indeed, by Theorem A.3.6, the divisors of zero in M are the union of its associated primes (and similarly for A). If M and A have regular elements, none of these associated primes is the whole $\mathcal{M}$, hence by prime avoidance there is an element of $\mathcal{M}$ that does not lie in any of these associated primes. Such element is regular and M-regular at the same time.

The second change of rings theorem, Theorem 5.2.11, can also be used to link the projective dimension of an A-module M to that of the $A[x]$-module $M[x]$.

Proposition 5.2.15. *Let A be a ring, M an A-module. Then*

$$\operatorname{pd}_A M = \operatorname{pd}_{A[x]} M[x].$$

Proof. The indeterminate $x \in A[x]$ clearly satisfies the hypothesis of Theorem 5.2.11, hence $\operatorname{pd}_{A[x]} M[x] \geq \operatorname{pd}_A M$.

For the converse inequality, notice that a projective resolution $P_\bullet \to M$ as A-modules gives a projective resolution $P_\bullet[x] \to M[x]$ as $A[x]$-modules. □

5.3. Injective modules

We now turn to the study of injective modules. Recall from Baer's criterion (Theorem 2.6.12) that an A-module M is injective if and only if every morphism $I \to M$, where I is an ideal of A, can be extended to the whole of A. In particular, when A is a PID, an A-module is injective if and only if it is divisible.

An immediate consequence of this is that the category Ab has enough injectives, and we have used this to derive the more general fact that Mod_A has enough injectives for all rings A (Corollary 2.6.18).

Recall from Remark 2.6.2 that a direct product of injective modules is itself injective. A consequence of Baer's criterion is the following surprising connection between direct sums of injective modules and the Noetherian property. The result appeared independently in [**Bas59**] and [**Pap59**]; our proof is taken from [**Cla15**, Section 8.9].

Theorem 5.3.1 (Bass–Papp). *Let A be a ring. Then the following are equivalent:*

(i) *A is Noetherian,*

(ii) *any direct limit of injective A-modules is injective, and*

(iii) *the countable direct sum of injective A-modules is injective.*

Proof. Assume that A is Noetherian and let $\{M_i\}$ be a direct system of A-modules, indexed over a directed set, with morphisms $f_{ij}\colon M_i \to M_j$ for $i \leq j$. Let $M = \varinjlim M_i$, with maps $f_i\colon M_i \to M$. To prove (
refbass-papp direct limit) by Theorem 2.6.12, we only need to consider a homomorphism $g\colon I \to M$, where $I \subset A$ is an ideal.

Since A is Noetherian, I is finitely generated, hence $g(I)$ is contained in $f_i(M_i)$ for some i. Moreover, there is a finitely generated submodule of M_i, call it N such that $g(I) = f_i(N)$. Letting K be the kernel of $N \to g(I)$, we obtain an exact sequence

$$0 \longrightarrow K \longrightarrow N \longrightarrow g(I) \longrightarrow 0\ .$$

Since $K \subset N$ and A is Noetherian, K is finitely generated. Since $f_i(K) = 0$ and the set is directed, there exists an index $j \geq i$ such that $f_{ij}(K) = 0$. If we let $N' = f_{ij}(N)$, it follows that $f_j\colon N' \to g(I)$ is an isomorphism. By inverting it, we get a homomorphism

$$I \to g(I) \to N' \subset M_j,$$

which we can extend to a map $h\colon A \to M_j$. The composition $f_j \circ h\colon A \to M$ is then an extension of g. Since this holds for all morphisms g, M is injective, or in other words (i) implies (ii).

Since (iii) is a special case of (ii), it remains to prove that (iii) implies (i), or better its contrapositive. Assuming that A is not Noetherian, we can find an infinite increasing chain of ideals $I_0 \subset I_1 \subset \cdots$. For each ideal I_k, choose an injective module J_k with an injection $A/I_k \to J_k$.

Consider the ideal $I := \bigcup_k I_k$, and the morphism

$$f_k\colon I \to I/I_k \to J_k.$$

All these morphisms together give a map $f\colon I \to \prod_k J_k$. For an element $a \in I$, $f_k(a) = 0$ except for finitely many k, hence $f(I)$ actually lies in $J := \bigoplus_k J_k$. We claim that f does not extend to a homomorphism $\tilde{f}\colon A \to J$, hence J is not injective.

In fact, assume that the extension $\tilde{f}$ exists. Then

$$f(a) = \tilde{f}(a \cdot 1) = a \cdot \tilde{f}(1)$$

for all $a \in I$. Since $\tilde{f}(1)$ has only finitely many nonzero coordinates, the image $f(I)$ lies in a finite direct sum of the J_k, which is a contradiction since $f_k(a) \neq 0$ for $a \in I \setminus I_k$. □

Corollary 5.3.2. *Let A be a Noetherian ring, M an A-module. Then M has a maximal injective submodule, and we can decompose $M = I \oplus N$, where N has no nontrivial injective submodules.*

Proof. The union of an increasing chain of injective submodules of M is injective by Theorem 5.3.1, hence the first claim follows by Zorn's lemma. If $I \subset M$ is a maximal injective submodule, then the inclusion $I \to M$ splits, and this implies the second claim. □

Theorem 5.3.1 should be compared with the following result from [**Cha60**], which looks exactly like its dual, even though the proof is very different.

Theorem (Chase). *Let A be a ring. Then the following are equivalent:*

(i) *A is Artinian,*

(ii) *any inverse limit of projective A-modules is projective, and*

(iii) *the direct product of projective A-modules is projective.*

In the rest of the section, we are going to study A-modules by means of their injective hull. Recall from Definition 2.7.1 that an inclusion of A-modules $M \subset E$ is called an essential extension if $M \cap M' \neq 0$ for all nonzero submodules $M' \subset E$. If moreover E is injective, E is called the injective hull of M. By Theorem 2.7.7, injective hulls exist in Mod_A, and they are unique up to an isomorphism that is the identity on M. The injective hull of M is denoted $E(M)$, or $E_A(M)$ if multiple rings are involved.

Example 5.3.3. Let A be an integral domain, $k = \mathcal{F}(A)$ its fraction field. Then k is injective as an A-module. To see this, we use Theorem 2.6.12. Let $I \subset A$ be an ideal and $f\colon I \to k$ a homomorphism of A-modules. For any nonzero $a \in I$, let $e = f(a)/a \in k$. It is easy to see that e is independent of the choice of a, so we can extend f to the whole of A by writing $f(1) = e$.

Moreover, k is the injective hull of A, regarded as an A-module over itself. Since k is injective, we know that $A \subset E(A) \subset k$. By Remark 2.6.14, every injective A-module is divisible, so $E(A)$ must be the whole fraction field k.

For injective modules over Noetherian rings, there is a nice structure theory due to Matlis [**Mat58**], based on primary decomposition (see Section A.3 to review).

Definition 5.3.4. Let M be an A-module. If M cannot be written as a direct sum $M = N_1 \oplus N_2$ with $N_1, N_2 \neq 0$, then we say that M is *indecomposable.*

The following result is the reason that primary decomposition appears here.

Proposition 5.3.5. *Let I be an ideal of the ring A, and assume that I has an irredundant decomposition $I = J_1 \cap \cdots \cap J_k$. Assume that $E(A/J_i)$ is* *indecomposable for each i. Then there is a natural isomorphism*

$$E(A/I) \cong E(A/J_1) \oplus \cdots \oplus E(A/J_k).$$

Proof. To start with, the natural map

$$\iota\colon \frac{A}{I} \to \frac{A}{J_1} \oplus \cdots \oplus \frac{A}{J_k}$$

is injective, and this allows us to identify A/I with a submodule of $E(A/J_1)\oplus \cdots \oplus E(A/J_k)$. Since the latter is injective, we only have to check that this is an essential extension.

Since the decomposition is irredundant, for every $i = 1, \dots, k$ we can find $a \in A$ such that $a \in J_t$ for $t \neq i$ but $a \notin J_i$. It follows that the class of a is nonzero in A/I, and $\iota(\overline{a}) \in A/J_i$. In other words, $A/I \cap A/J_i \neq 0$ when both are regarded as submodules of $E(A/J_1) \oplus \cdots \oplus E(A/J_k)$.

By Proposition 2.7.10, we can regard $E(A/I \cap A/J_i)$ as a submodule of $E(A/J_i)$. The inclusion splits because $E(A/I \cap A/J_i)$ is injective, and the hypothesis that $E(A/J_i)$ is indecomposable implies that $E(A/I \cap A/J_i) = E(A/J_i)$.

Now choose any nonzero element

$$m = (m_1, \dots, m_k) \in E(A/J_1) \oplus \cdots \oplus E(A/J_k),$$

and assume without loss of generality that $m_1 \neq 0$. Since $E(A/J_1)$ is an essential extension of $A/I \cap A/J_1$, the intersection

$$(A/I \cap A/J_1) \cap Am_1 \neq 0.$$

In other words, $0 \neq am_1 \in A/I$ for some $a \in A$.

We now repeat the procedure with am in place of m, for the first index i such that $am_i \neq 0$, and so on. At the end, we find some $b \in A$ such that $0 \neq bm \in A/I$. It follows that all submodules of $E(A/J_1) \oplus \cdots \oplus E(A/J_k)$ meet A/I—in other words, $E(A/J_1)\oplus\cdots\oplus E(A/J_k)$ is an essential extension of A/I. □

In view of this result, it is natural to ask for which ideals $J \subset A$, the injective hull $E(A/J)$ is indecomposable. We can answer in slightly more generality.

Let E be an injective A-module. For all $e \in E$, we have a natural monomorphism $A/\operatorname{Ann}(e) \to E$, which we can extend to an embedding $E(A/\operatorname{Ann}(e)) \to E$ by Proposition 2.7.10. If moreover E is indecomposable and $e \neq 0$, we must have the equality $E(A/\operatorname{Ann}(e)) = E$. It follows that all indecomposable injective A-modules appear as the injective hull of a module of the form A/J, where J is an ideal (namely, $J = \operatorname{Ann}(e)$ for any $e \neq 0$). This construction is the basis of the following result.

Theorem 5.3.6. *Let A be a ring, E an A-module. Then E is injective and indecomposable if, and only if, $E \cong E(A/J)$ for some irreducible ideal J.*

Proof. Assume that J is an irreducible ideal. This can be rephrased by saying that any two nontrivial submodules $M_1, M_2 \subset A/J$ have nonzero intersection. If $E(A/J) = N_1 \oplus N_2$ is decomposable, we must have $A/J \cap N_i = 0$ for $i = 1$ or 2, which contradicts the fact that $E(A/J)$ is an essential extension of A/J.

To prove the converse, let E be an indecomposable injective A-module. By the above discussion, we can take $E = E(A/J)$ for some ideal $J \subset A$, and we only need to prove that J is irreducible. If not, we can write $J = J_1 \cap J_2$, where $J \subsetneq J_i$ for $i = 1, 2$, and the decomposition is irredundant.

As in the proof of Proposition 5.3.5, consider A/J as a submodule of $E(A/J_1) \oplus E(A/J_2)$. Following the same proof, we have $A/J \cap A/J_1 \neq 0$. By Lemma 2.7.2, the map $E(A/J \cap A/J_1) \to E(A/J) = E$ is injective, hence an isomorphism because E is indecomposable. Similarly, the map $E(A/J \cap A/J_1) \to E(A/J_1)$ is injective, which is a contradiction since already $A/J \to A/J_1$ is not injective. □

All results so far apply to any ring. In the Noetherian case, we have more precise results thanks to primary decomposition.

Proposition 5.3.7. *Let A be a Noetherian ring, E an injective A-module. Then E is the direct sum of indecomposable, injective modules.*

Proof. By Zorn's lemma (check that it applies!), there is a maximal submodule $F \subset E$ which is the direct sum of indecomposable injective modules; moreover it is injective by Theorem 5.3.1. If $F \subsetneq E$, write $E = F \oplus G$. If $g \in G$ is any nonzero element, we have an embedding $E(A/\operatorname{Ann}(g)) \hookrightarrow G$ by Lemma 2.7.2.

Let

$$\operatorname{Ann}(g) = Q_1 \cap \cdots \cap Q_k$$

be an irreducible decomposition of $\operatorname{Ann}(g)$. Since each Q_i is irreducible, $E(A/Q_i)$ is indecomposable by Theorem 5.3.6. By Proposition 5.3.5,

$$E(A/\operatorname{Ann}(g)) = E(A/Q_1) \oplus \cdots \oplus E(A/Q_k),$$

hence $F \oplus E(A/\operatorname{Ann}(g))$ is a larger submodule of E which is the direct sum of indecomposable injective modules. □

In the Noetherian case, we can also sharpen Theorem 5.3.6. An injective indecomposable A-module has the form $E(A/Q)$, where $Q \subset A$ is irreducible, hence primary. We can reduce to the prime case thanks to the following lemma.

Lemma 5.3.8. *Let A be a Noetherian ring, Q a primary ideal of A, $P := \sqrt{Q}$. Then $E(A/Q) \cong E(A/P)$.*

Proof. Let n be the smallest integer such that $P^n \subset Q$ - we can assume that $n > 1$. Choose any $a \in P^{n-1} \setminus Q$, and let $\overline{a} \neq 0$ be its image in $E(A/Q)$. Since Q is primary, $\mathrm{Ann}(\overline{a}) = P$. The conclusion follows from the discussion before Theorem 5.3.6. ☐

In conclusion, we can completely classify injective modules over a Noetherian ring.

Theorem 5.3.9. *Let A be a Noetherian ring. Then every injective A-module is the direct sum of indecomposable injective modules. Every indecomposable injective module has the form $E(A/P)$ for some prime ideal $P \subset A$, and all such A-modules are pairwise nonisomorphic.*

Proof. We have already proved all statements but the last. Let P, Q be two prime ideals, and assume that $E = E(A/P) \cong E(A/Q)$. Inside E, we have $A/P \cap A/Q \neq 0$. (Why?) As in the previous proof, for any nonzero $m \in A/P \cap A/Q$ we have $P = \mathrm{Ann}(m) = Q$. ☐

Remark 5.3.10. Keep the assumption that A is Noetherian. Let $P \subset A$ be a prime, $E = E(A/P)$, and take a nonzero $e \in E$. Letting $J = \mathrm{Ann}(e)$, we know that $E = E(A/J)$, so J is primary by Proposition 5.3.5 and primary decomposition. Letting $Q = \sqrt{J}$, we have $E \cong E(A/Q)$ by Lemma 5.3.8, so ultimately $Q = P$ by Theorem 5.3.9. We deduce that P is the only associated prime of E. Moreover, there exists a k such that $P^k \subset J$ since P is finitely generated. It follows that $P^k e = 0$; in other words, every element of $E(A/P)$ is annihilated by a power of P.

Example 5.3.11. Every injective $\mathbb{Z}$-module is the direct sum of modules of the form $E(\mathbb{Z}/P)$ for some prime ideal P. Let us compute these modules.

When $P = 0$, we get the $\mathbb{Z}$-module $E(\mathbb{Z}) = \mathbb{Q}$. When $P = (p)$ is generated by a prime number, we notice that we can embed

$$\frac{\mathbb{Z}}{p\mathbb{Z}} \cong \frac{\frac{1}{p}\mathbb{Z}}{\mathbb{Z}} \subset \frac{\mathbb{Q}}{\mathbb{Z}}.$$

The subgroup $\frac{1}{p}\mathbb{Z}/\mathbb{Z}$ is divisible by all primes $q \neq p$. To get the injective hull, we only need to guarantee divisibility by powers of p. It follows that

$$E(\mathbb{Z}/p\mathbb{Z}) \cong \frac{\mathbb{Z}[p^{-1}]}{\mathbb{Z}},$$

where $\mathbb{Z}[p^{-1}]$ is the localization of $\mathbb{Z}$ at the powers of p.

5.4. Injective dimension

In this section we introduce the notion of injective dimension of a module, which is the obvious analogue of the projective dimension that we studied in Section 5.2. We start with the analogue of Proposition 5.2.1, whose proof follows immediately from dualization.

Proposition 5.4.1. *Let $\mathcal{A}$ be an Abelian category with enough injectives, and let A be an object of $\mathcal{A}$. The following are equivalent:*

(i) *there exists an injective resolution*

$$0 \longrightarrow A \longrightarrow I_0 \longrightarrow I_1 \longrightarrow \cdots \longrightarrow I_n \longrightarrow 0$$

of length n, and

(ii) $\mathrm{Ext}^i(B, A) = 0$ *for all $i > n$ and all $B \in \mathcal{A}$.*

Definition 5.4.2. Let $\mathcal{A}$ be an Abelian category with enough injectives, $X \in \mathcal{A}$. The minimal length of an injective resolution of X will be called the *injective dimension* of X, and denoted $\mathrm{id}\, X$. If X does not admit any injective resolution of finite length, we set $\mathrm{id}\, X = \infty$. When $\mathcal{A} = \mathrm{Mod}_A$ is the category of modules over the ring A, we sometimes denote injective dimension by id_A for clarity.

By the above result, $\mathrm{id}\, X$ is the also minimum n (if any) such that $\mathrm{Ext}^i(-, X) = 0$ for $i > n$. As in the case of projective dimension, we want to establish some change of ring theorems. Before doing so, we notice one simple consequence of Baer's criterion.

Proposition 5.4.3. *Let A be a ring, M an A-module. Then $\mathrm{id}\, M$ is the minimum n (if any) such that $\mathrm{Ext}^i(A/I, M) = 0$ for $i > n$ and for all ideals $I \subset A$.*

Proof. First assume that $\mathrm{Ext}^1(A/I, M) = 0$ for all ideals I. Then all homomorphisms $I \to M$ can be extended to A by the long exact sequence of Ext, hence M is injective by Theorem 2.6.12.

Assuming $\mathrm{Ext}^{n+1}(A/I, M) = 0$ for all ideals I, take a truncated injective resolution

$$0 \longrightarrow M \longrightarrow I_0 \longrightarrow \cdots \longrightarrow I_{n-1} \longrightarrow N \longrightarrow 0,$$

where $N := \mathrm{coker}\, I_{n-2} \to I_{n-1}$. Then $\mathrm{Ext}^1(A/I, N) = 0$ for all ideals I by Proposition 3.3.2, hence N is injective and $\mathrm{id}\, M \leq n$. □

For local Noetherian rings, we can give a sharper version.

Theorem 5.4.4 (Kaplansky)**.** *Let A be a local Noetherian ring with maximal ideal $\mathcal{M}$, $k = A/\mathcal{M}$, M a finitely generated A-module. Then $\mathrm{id}_A\, M \leq n$ if and only if $\mathrm{Ext}^i(k, M) = 0$ for all $i > n$.*

Lemma 5.4.5. *Let $A, \mathcal{M}$ be a local Noetherian ring with $k = A/\mathcal{M}$, M a finitely generated A-module, and P a prime ideal of A distinct from $\mathcal{M}$. Assume that* $\mathrm{Ext}_A^{i+1}(A/Q, M) = 0$ *for all primes Q properly containing P; then* $\mathrm{Ext}_A^i(A/P, M) = 0$.

Proof. Choose any element $a \in \mathcal{M} \setminus P$, and denote $B = A/P$. Notice that $\overline{a}$ is not a zero divisor on B, hence we get the exact sequence

$$0 \longrightarrow B \xrightarrow{\cdot a} B \longrightarrow \frac{B}{\overline{a}B} \longrightarrow 0.$$

Applying the functor $\mathrm{Hom}_A(-, M)$ to it, we get a piece of the associated long exact sequence

$$\mathrm{Ext}_A^i(B, M) \xrightarrow{\cdot a} \mathrm{Ext}_A^i(B, M) \longrightarrow \mathrm{Ext}_A^{i+1}\left(\frac{B}{\overline{a}B}, M\right).$$

Since $B/\overline{a}B$ is a finitely generated B-module, by Theorem A.3.7 we get a chain of submodules having quotients isomorphic to B/Q'_j for some primes Q'_j of B. These, in turn, are isomorphic to A/Q_j, where Q_j is the prime of A corresponding to Q'_j in B. By hypothesis, $\mathrm{Ext}_A^{i+1}(A/Q_j, M) = \mathrm{Ext}_A^{i+1}(B/Q'_j, M) = 0$ for all j. By induction, $\mathrm{Ext}_A^{i+1}(B/\overline{a}B, M) = 0$.

It follows that multiplication by $\overline{a}$ is surjective on $\mathrm{Ext}_A^i(B, M)$. Since this is finitely generated, it is 0 by Nakayama's lemma. □

Proof of Theorem 5.4.4. By Theorem A.8.5, A has finite dimension. We can then apply the lemma recursively to prove that $\mathrm{Ext}^i(A/P, M) = 0$ for all primes $P \subset A$, for $i > n$. If N is a finitely generated A-module, we can find a chain of submodules of N having quotients isomorphic to A/P for some prime P. By induction, it follows that $\mathrm{Ext}^i(N, M) = 0$ for all finitely generated A-modules N and all $i > n$—in particular, taking $N = A/I$, the conclusion follows from Proposition 5.4.3. □

We end this section with the change of ring theorems for injective dimension. Notice that they are similar, but not identical, to their projective counterparts. For one thing, the general change of rings theorem involves the *projective* dimension of B.

Theorem 5.4.6. *Let $f: A \to B$ a homomorphism of rings, and N a B-module. Then*

$$\mathrm{id}_A N \leq \mathrm{pd}_A B + \mathrm{id}_B N.$$

Proof. Apply the base change spectral sequence of Theorem 4.5.7. □

As in the projective case, we specialize this to the important case of quotient rings.

Theorem 5.4.7 (First change of rings theorem)**.** *Let A be a ring, $a \in A$ a regular element, and let M be an $A/(a)$-module. Assume that $\operatorname{id}_{A/(a)} M < \infty$. Then*

$$\operatorname{id}_A M = 1 + \operatorname{id}_{A/(a)} M.$$

Proof. We prove the result by induction on $\operatorname{id}_{A/(a)} M$. First, any $A/(a)$-module cannot be injective as an A-module, for instance, 1 is not divisible by a. If $\operatorname{id}_{A/(a)} M = 0$, then $\operatorname{id}_A M \leq 1$ by Theorem 5.4.6, and in fact $\operatorname{id}_A M = 1$ because M is not injective over A.

For the inductive step, we consider an exact sequence of $A/(a)$-modules

$$0 \longrightarrow M \longrightarrow I \longrightarrow C \longrightarrow 0\ ,$$

where I is injective. Then $\operatorname{id}_{A/(a)} C = \operatorname{id}_{A/(a)} M - 1$.

By the previous step, $\operatorname{id}_A I = 1$. If we regard the same exact sequence as a sequence of A-modules and consider the associated long exact sequence of $\operatorname{Ext}(N, -)$ groups for all A-modules N, we conclude that either $\operatorname{id}_A C = \operatorname{id}_A M - 1$—in which case we are done—or $\operatorname{id}_A M = \operatorname{id}_A C = 1$ (in which case, $\operatorname{id}_{A/(a)} C = 0$ and $\operatorname{id}_{A/(a)} M = 1$).

To exclude the latter case, consider an exact sequence of A-modules

$$0 \longrightarrow M \longrightarrow I' \longrightarrow C' \longrightarrow 0\ ,$$

with I' and C' injective. We can apply the functor $F = \operatorname{Hom}_A(A/(a), -)$ to get the long exact sequence

$$0 \longrightarrow F(M) \longrightarrow F(I') \longrightarrow F(C') \longrightarrow \operatorname{Ext}^1_A(A/(a), M) \longrightarrow 0,$$

which is actually a sequence of $A/(a)$-modules. Since F preserves injectives (see the proof of Theorem 4.5.5), $F(I')$ and $F(C')$ are injective over $A/(a)$, hence so is $\operatorname{Ext}^1_A(A/(a), M)$.

By Example 3.4.11(c), $\operatorname{Ext}^1_A(A/(a), M) = M/aM = M$, which is a contradiction, since $\operatorname{id}_{A/(a)} M = 1$. □

For the second theorem, we need a lemma that is of independent interest. Recall that $(0 :_M a)$ denotes the elements of the A-module M annihilated by a. This is a module over $A/(a)$ that can be identified with $\operatorname{Hom}_A(A/(a), M)$.

Lemma 5.4.8. *Let A be a ring, M an A-module and $a \in A$ such that $M = aM$. Then*

$$\operatorname{id}_{A/(a)}(0 :_M a) \leq \operatorname{id}_A M.$$

Proof. We can assume that $\operatorname{id}_A M < \infty$, and so prove the result by induction on it. For the case $\operatorname{id}_A M{=}0$, we notice that the functor $\operatorname{Hom}_A(A/(a), -)$

preserves injectives. For the inductive step, take an exact sequence of A-modules

$$0 \longrightarrow M \xrightarrow{f} I \xrightarrow{g} C \longrightarrow 0,$$

with I injective, so that $\operatorname{id}_A C = \operatorname{id}_A M - 1$. We claim that

$$0 \longrightarrow (0 :_M a) \longrightarrow (0 :_I a) \longrightarrow (0 :_C a) \longrightarrow 0$$

is exact as well. We can check exactness on the right directly: given $c \in C$ such that $ac = 0$, choose $x \in I$ such that $g(x) = c$. Then $ax \in \ker g = \operatorname{im} f$, so we can write $ax = f(am)$ for some $m \in M$. Then $x - f(m) \in (0 :_I a)$ and maps to c, as required.

Since $(0 :_I a)$ is injective over $A/(a)$, we have

$$\operatorname{id}_{A/(a)}(0 :_C a) = \operatorname{id}_{A/(a)}(0 :_M a) - 1. \tag{5.4.1}$$

Since I is divisible, $aC = C$. By induction, C satisfies the conclusion of the lemma, and hence so does M. □

Theorem 5.4.9 (Second change of rings theorem)**.** *Let A be a ring, M be an A-module, and let a be weakly regular and weakly M-regular. Then either*

(i) *M is injective and $M/aM = 0$, or*

(ii) $\operatorname{id}_A M \geq 1 + \operatorname{id}_{A/(a)} \frac{M}{aM}$.

Proof. We can assume that $\operatorname{id}_A M$ is finite. If $\operatorname{id}_A M = 0$, M is injective. Moreover, the exact sequence

$$0 \longrightarrow M \longrightarrow M \longrightarrow \frac{M}{aM} \longrightarrow 0$$

splits, hence M/aM is a direct summand of M. But multiplication by a is injective on M, hence $M/aM = 0$.

If $\operatorname{id}_A M > 0$, consider an exact sequence of A-modules

$$0 \longrightarrow M \longrightarrow I \longrightarrow C \longrightarrow 0\ ,$$

with I injective, so that $\operatorname{id}_A C = \operatorname{id}_A M - 1$. We apply the functor $F = \operatorname{Hom}_A(A/(a), -)$ to get a long exact sequence. Using Example 3.4.11(c) and the fact that a is not a zero divisor on M, this reads

$$0 \longrightarrow \operatorname{Hom}_A(A/(a), I) \longrightarrow \operatorname{Hom}_A(A/(a), C) \longrightarrow \frac{M}{aM} \longrightarrow 0\ .$$

Since F preserves injectives, $\operatorname{Hom}_A(A/(a), I)$ is injective over $A/(a)$; moreover $\operatorname{id}_{A/(a)} \operatorname{Hom}_A(A/(a), C) \leq \operatorname{id}_A C$ by Lemma 5.4.8. It follows that

$$\operatorname{id}_{A/(a)} \frac{M}{aM} = \operatorname{id}_{A/(a)} \operatorname{Hom}_A(A/(a), C) \leq \operatorname{id}_A C = \operatorname{id}_A M - 1.$$

□

Theorem 5.4.10 (Third change of rings theorem). *Let A be a Noetherian local ring with maximal ideal $\mathcal{M}$, M a finitely generated A-module, and let $a \in A$ be regular and M-regular. Then*

$$\operatorname{id}_A M = \operatorname{id}_A \frac{M}{aM} = 1 + \operatorname{id}_{A/(a)} \frac{M}{aM}.$$

Proof. For the first equality, we consider the exact sequence

$$0 \longrightarrow M \longrightarrow M \longrightarrow \tfrac{M}{aM} \longrightarrow 0$$

given by multiplication by a. Considering the associated long exact sequence of $\operatorname{Ext}(A/I, -)$ groups, for ideals $I \subset A$, we conclude that $\operatorname{id}_A M = \operatorname{id}_A \frac{M}{aM}$ unless $\operatorname{id}_A M = n$ is finite and

$$\operatorname{Ext}^n_A\left(\tfrac{A}{I}, M\right) \xrightarrow{a\cdot} \operatorname{Ext}^n_A\left(\tfrac{A}{I}, M\right)$$

is surjective. Since A/I and M are both finitely generated and A is Noetherian, the group $\operatorname{Ext}^n_A(A/I, M)$ is finitely generated as well (why?), hence it is 0 by Nakayama's lemma, a contradiction.

The second equality is Theorem 5.4.7, assuming $\operatorname{id}_{A/(a)} \frac{M}{aM}$ is finite. Otherwise, the equality holds anyway: $\operatorname{id}_A M = \infty$ as well by Theorem 5.4.9. □

5.5. Global dimension of rings

As the reader may imagine, projective and injective dimension are strictly related, and they can be combined to yield an invariant of rings.

Definition 5.5.1. Let A be a ring. The number

$$\sup_{M \in \operatorname{Mod}_A} \operatorname{pd}_A M = \sup_{N \in \operatorname{Mod}_A} \operatorname{id}_A N = \sup_{M,N \in \operatorname{Mod}_A} \{n \mid \operatorname{Ext}^n_A(M, N) \neq 0\}$$

is called the *global dimension* (or *homological dimension*) of A, and denoted $\operatorname{gl.dim} A$. As it happens for the injective and projective dimensions, this number can also be ∞.

We can easily translate some results about projective and injective dimension. From Kaplansky's theorem (Theorem 5.4.4) we immediately get

Proposition 5.5.2. *Let $A, \mathcal{M}$ be a local Noetherian ring, $k = A/\mathcal{M}$. Then* $\operatorname{gl.dim} A = \operatorname{pd}_A k$.

More generally, Proposition 5.4.3 gives us

Proposition 5.5.3. *For any ring A,*

$$\operatorname{gl.dim} A = \sup_{I \subset A} \operatorname{pd}_A(A/I).$$

We can also relate the global dimension of A to that of its localizations.

Theorem 5.5.4. *For any ring A,*

$$\operatorname{gl.dim} A \geq \sup_{\substack{P \subset A \\ \textit{prime}}} \operatorname{gl.dim} A_P.$$

If moreover A is Noetherian, then we have the equalities

$$\operatorname{gl.dim} A = \sup_{\substack{P \subset A \\ \textit{prime}}} \operatorname{gl.dim} A_P = \sup_{\substack{\mathcal{M} \subset A \\ \textit{maximal}}} \operatorname{gl.dim} A_{\mathcal{M}}.$$

Proof. For the first claim, we can assume that $\operatorname{gl.dim} A < \infty$. Consider any A_P-module M. Regarding M as an A-module, we have $M_P = M$. By the remark before Proposition 5.2.7 and the fact that $\operatorname{pd}_A M < \infty$, we get $\operatorname{pd}_A M \geq \operatorname{pd}_{A_P} M$. We conclude that $\operatorname{gl.dim} A \geq \operatorname{gl.dim} A_P$.

Then, assume that A is Noetherian. By Proposition 5.5.3, $\operatorname{gl.dim} A$ can be computed by considering only cyclic modules A/I. By Proposition 5.2.7, for all finitely generated A-modules M there is a maximal ideal $\mathcal{M}$ such that $\operatorname{pd}_A M = \operatorname{pd}_{A_{\mathcal{M}}} M_{\mathcal{M}}$, and we get the desired conclusion. □

We can develop the same notions in the graded context. Let A be a graded ring, Mod_A its category of graded modules, and Mod^u_A the category of modules over A, when regarded as an ungraded ring. As usual, denote $U\colon \operatorname{Mod}_A \to \operatorname{Mod}^u_A$ the forgetful functor.

Definition 5.5.5. Let A be a graded ring. The number

$$\sup_{M,N \in \operatorname{Mod}_A} \{n \mid \operatorname{Ext}^n_A(M,N) \neq 0\}$$

is called the *graded global dimension* of A, and denoted $\operatorname{gr.gl.dim} A$.

Notice that the supremum is taken among graded modules, and that Ext is computed in the category Mod_A of graded modules. It is a simple verification, that, as it happens in the ungraded case,

$$\operatorname{gr.gl.dim} A = \sup_{M \in \operatorname{Mod}_A} \operatorname{pd}_A M.$$

Notice that by Proposition 5.2.5, the projective dimension $\operatorname{pd}_A M$ is the same, whether it is computed in Mod_A or in Mod^u_A. A priori, the ungraded global dimension $\operatorname{gl.dim} A$ is the supremum of the same quantity, computed over a larger family of modules, and this immediately implies the following fact.

Proposition 5.5.6. *Let A be a graded ring. Then* $\operatorname{gr.gl.dim} A \leq \operatorname{gl.dim} A$.

We will shortly see in Theorem 5.5.12 that there is a closer relation, and in fact $\operatorname{gl.dim} A \leq 1 + \operatorname{gr.gl.dim} A$. Before doing so, we need to relate the global dimension of a ring A to that of the polynomial ring $A[x]$.

Theorem 5.5.7. *Let A be a ring. Then* $\operatorname{gl.dim} A[x] = 1 + \operatorname{gl.dim} A$. *If moreover A is graded over $\mathbb{Z}$ and $A[x]$ is graded with* $\deg x = 1$*, then* $\operatorname{gr.gl.dim} A[x] = 1 + \operatorname{gr.gl.dim} A$.

Proof. We prove the case of ungraded rings, and leave it to the reader to check that all arguments generalize to the graded case. If $\operatorname{gl.dim} A = \infty$, then $\operatorname{gl.dim} A[x] = \infty$ as well by Proposition 5.2.15, so we can assume that $\operatorname{gl.dim} A$ is finite.

By Theorem 5.2.10, $\operatorname{pd}_{A[x]} M = 1 + \operatorname{pd}_A M$ for any A-module M such that $\operatorname{pd}_A M < \infty$, hence $\operatorname{gl.dim} A[x] \geq 1 + \operatorname{gl.dim} A$.

To get the other inequality, take an $A[x]$-module M, and denote M_A the module M regarded as an A-module. Then we have an exact sequence of $A[x]$-modules

$$0 \longrightarrow M_A[x] \xrightarrow{f} M_A[x] \xrightarrow{g} M \longrightarrow 0. \tag{5.5.1}$$

To define the maps f and g, it is simpler to think of $M_A[x]$ as $A[x] \otimes_A M_A$. Then

$$f(a \otimes m) := ax \otimes m - a \otimes xm,$$

and $g(a \otimes m) := a \cdot m$, where multiplication by scalars in $A[x]$ happens in M. It is immediate that (5.5.1) is a complex and that g is surjective so we only need to prove that f is injective and $\operatorname{im} f = \ker g$. To see that f is injective, write an element $p \neq 0$ of $A[x] \otimes M_A$ as a sum

$$p = x^k \otimes m_k + \cdots + x \otimes m_1 + 1 \otimes m_0,$$

where $m_k \neq 0$, and notice that the only term of degree $k+1$ in $f(p)$ is $x^{k+1} \otimes m_k \neq 0$. We prove that $g(p) = 0$ implies $p \in \operatorname{im} f$ by induction on k. If $k = 0$, then $p = 1 \otimes m_0$, so that $g(p) = m_0$. If $g(p) = 0$, then $p = 0$ as well. For $k > 0$, notice that we can find a polynomial $q \in \operatorname{im} f$ such that $p - q$ has lower degree, namely $q = f(x^{k-1} \otimes m_k)$. By induction, $p - q \in \operatorname{im} f$, so $p \in \operatorname{im} f$ as well.

From the exactness of (5.5.1) and Proposition 5.2.15, we get the inequality

$$\operatorname{pd}_{A[x]} M \leq 1 + \operatorname{pd}_{A[x]} M_A[x] = 1 + \operatorname{pd}_A M_A \leq 1 + \operatorname{gl.dim} A,$$

and the conclusion follows by taking the supremum. □

Corollary 5.5.8. *If k is a field, then*

$$\operatorname{gr.gl.dim} k[x_1, \ldots, x_n] = \operatorname{gl.dim} k[x_1, \ldots, x_n] = n.$$

Notice that a similar result holds for power series as well.

Proposition 5.5.9. *If k is a field, then* $\operatorname{gl.dim} k[[x_1, \dots, x_n]] = n$.

Proof. The ring $A = k[[x_1, \dots, x_n]]$ is local and Noetherian (Theorem A.2.2), hence $\operatorname{gl.dim} A = \operatorname{pd}_A k$ by Proposition 5.5.2. The equality $\operatorname{pd}_A k = n$ follows by induction from the first change of rings theorem, Theorem 5.2.10. □

The attentive reader has surely noticed that the global dimension of a ring has many properties in common with its Krull dimension. In particular, the above result should be compared with Theorem A.7.2. Moreover, the reader should compare Theorem 5.5.4 with the fact that for all rings A,

$$\dim A = \sup_{\substack{P \subset A \\ \text{prime}}} \dim A_P = \sup_{\substack{\mathcal{M} \subset A \\ \text{maximal}}} \dim A_{\mathcal{M}},$$

which is obvious from the definition. In the following example we compute some global dimensions, showing that the two notions do not always agree.

Example 5.5.10.

(a) Let $A = \mathbb{Z}/4\mathbb{Z}$. By Example 5.2.3(c), we know that $\operatorname{gl.dim} \mathbb{Z}/4\mathbb{Z} = \infty$. On the other hand, $\dim \mathbb{Z}/4\mathbb{Z} = 0$.

(b) More generally, we have $\dim A = 0$ for all Artinian rings. The condition $\operatorname{gl.dim} A = 0$ only holds if all A-modules are projective (in which case A is called *semisimple*). It is easy to see (check this!) that this implies that every A-module is a direct sum of simple modules, that is, modules that have no nontrivial submodules.

Applying this to the ring A itself, we find a decomposition $A = \bigoplus_{i \in I} A_i$ for some simple submodules A_i. The projection $\pi_i \colon A \to A_i$ is surjective, hence we can give A_i a ring structure so that π_i is a ring homomorphism. Since A_i is simple, it has no nontrivial ideals, hence it is a field.

Moreover, every ideal of A is principal (why?), hence A is Noetherian. Since an infinite direct sum of fields is not Noetherian, the index set I must be finite. In conclusion, every semisimple commutative ring is a finite product of fields. This is a very special case of a result for noncommutative rings, called the Artin–Wedderburn theorem [**Lam01**, Theorem 3.5].

In particular, every Artinian ring that is not a direct product of fields has $\dim A = 0$ but $\operatorname{gl.dim} A > 0$.

(c) On the other hand, let A be a principal ideal domain that is not a field. Then $\dim A = 1$, and by Example 5.2.3(a), $\operatorname{gl.dim} A = 1$ as well.

(d) More generally, let A be a Dedekind ring. By Proposition 5.5.3,

$$\operatorname{gl.dim} A = \sup_{I \subset A} \operatorname{pd} A/I.$$

By Example 5.1.1(b), every ideal $I \subset A$ is projective, and the exact sequence

$$0 \longrightarrow I \longrightarrow A \longrightarrow A/I \longrightarrow 0$$

shows that $\operatorname{pd} A/I \leq 1$, hence $\operatorname{gl.dim} A = 1 = \dim A$.

Remark 5.5.11. Let A be a Noetherian ring. Then either $\operatorname{gl.dim} A = \infty$ or else $\operatorname{gl.dim} A \leq \dim A$. By Theorem 5.5.4, it is enough to prove this in the case where A is local. We will do this in Theorem 8.2.1.

We end the section by using Theorem 5.5.7 to derive a connection between the graded and the ungraded global dimension. This result appears as [**NvO82**, Theorem II.8.2].

Theorem 5.5.12. *Let A be a ring graded over $\mathbb{Z}$. Then* $\operatorname{gl.dim} A \leq 1 + \operatorname{gr.gl.dim} A$.

To prove it, we will need the concept of (de)homogeneization.

Definition 5.5.13. Let A be a $\mathbb{Z}$-graded ring, $M = \bigoplus_{i \in \mathbb{Z}} M_i$ a graded A-module. Given a nonzero element $m = \sum_{i=a}^{b} m_i$, where $m_i \in M_i$, and $m_b \neq 0$, the element $m^* \in M[x]$ defined as

$$m^* := \sum_{i=a}^{b} m_i x^{b-i}$$

is called the *external homogeneization* of m. Notice that m^* is always a homogeneous element of $M[x]$. If $N \subset M$ is an ungraded submodule, the graded module $N^* \subset M[x]$ generated by n^* for $n \in N$ is called the *external homogeneization* of N.

In the opposite direction, given a homogeneous element of degree d in $M[x]$, say $m = \sum_{i=a}^{b} m_i x^{d-i}$, where $m_i \in M_i$, the element $m_* \in M$ defined as

$$m_* := \sum_{i=a}^{b} m_i$$

is called the *dehomogeneization* of m. In other words, m_* is obtained by evaluating m at $x = 1$. Given a graded submodule $N \subset M[x]$, the set $N_* = \{0\} \cup \{n_* \mid n \in N\} \subset M$ is an ungraded submodule, called the *dehomogeneization* of N.

We can use these operations to relate graded $A[x]$-modules and ungraded A-modules. Define a functor $E\colon \operatorname{Mod}_{A[x]} \to \operatorname{Mod}^u_A$ by

$$E(M) = \frac{M}{(x-1)M} = \frac{A[x]}{(x-1)} \otimes_{A[x]} M.$$

Notice that $A[x]/(x-1) \cong A$, hence $E(M)$ is an A-module.

Lemma 5.5.14. *The functor E is exact and essentially surjective.*

Proof. The definition of E as a tensor product shows that E is right exact.

Assume that $N \subset M$ is a graded $A[x]$-submodule. Take $n \in N \cap (x-1)M$, say $n = (1-x)m$ with $m = \sum_{i=a}^{b} m_i$ and $m_i \in M_i$. Then

$$n = m_a + (m_{a+1} - xm_a) + \cdots + (m_b - xm_{b-1}) - xm_b.$$

Since N is graded, we find that $m_a \in N$ and recursively $m_i \in N$ for all $i = a, \ldots, b$. In other words, $N \cap (x-1)M = (x-1)N$, and this implies that E is exact.

To check that E is essentially surjective, we start with an ungraded A-module M and we need to find a graded module N over $A[x]$ such that $E(N) \cong M$. Take a presentation

$$0 \longrightarrow K \longrightarrow F \longrightarrow M \longrightarrow 0\ ,$$

where F is free. Then we claim that $N = F[x]/K^*$ will do. First notice that for $0 \neq m \in F$, $(m^*)_* = m$. Hence $(K^*)_* = K$, and the result follows by exactness of E and the exact sequence

$$0 \longrightarrow K^* \longrightarrow F[x] \longrightarrow N \longrightarrow 0\ . \qquad \square$$

Proof of Theorem 5.5.12. Let M be an ungraded A-module. By Lemma 5.5.14, we can find a graded $A[x]$-module N such that $E(N) \cong M$. Let P be a graded projective $A[x]$-module. By Corollary 2.6.8, P is a direct summand of a free $A[x]$-module, hence $E(P)$ is projective as well.

It follows that if $P_\bullet \to N$ is a projective resolution of N, $E(P_\bullet) \to E(M)$ is a projective resolution of M. In particular,

$$\operatorname{pd}_A M \leq \operatorname{pd}_{A[x]} N \leq \operatorname{gr.gl.dim} A[x] = 1 + \operatorname{gr.gl.dim} A,$$

where the last equality is Theorem 5.5.7. $\square$

5.6. Free resolutions

Corollary 5.5.8 has a reformulation in classical language, that was already known to Hilbert in 1890 [**Hil90**]. Hilbert formulated his celebrated result in terms of syzygies.

Definition 5.6.1. Let $A = k[x_1, \ldots, x_n]$ be a polynomial ring over a field, M a finitely generated A-module, and choose generators $m_1, \ldots, m_d$. A (first order) *syzygy*[1] between $m_1, \ldots, m_d$ is a relation

$$a_1 m_1 + \cdots + a_d m_d = 0$$

for some $a_1, \ldots, a_d \in A$. The syzygies between $m_1, \ldots, m_d$ form an A-module that we can recognize as the kernel of the map $A^d \to M$ that sends the i-th basis vector e_i to m_i. Recursively, k-th order syzygies are defined as syzygies on the module of $(k-1)$-th order syzygies.

The terminology is more complex than necessary—in our language, Hilbert was looking at presentations

$$F_k \longrightarrow \cdots \longrightarrow F_1 \longrightarrow F_0 \longrightarrow M \longrightarrow 0,$$

where each F_i is a finitely generated, free A-module. The celebrated theorem of Hilbert on syzygies then states:

Theorem 5.6.2 (Hilbert)**.** *Every finitely generated module over the ring $A = k[x_1, \ldots, x_n]$ admits a finite free resolution*

$$0 \longrightarrow F_k \longrightarrow \cdots \longrightarrow F_1 \longrightarrow F_0 \longrightarrow M \longrightarrow 0,$$

of length $k \leq n$.

In other words, if one keeps taking syzygies, at most at the n-th step one ends up with a free A-module. Theorem 5.6.2 is almost equivalent to Corollary 5.5.8, but for one crucial and highly nontrivial fact. Corollary 5.5.8 guarantees that every A-module has a *projective* resolution of length at most n. The missing ingredient is the Quillen–Suslin theorem, stating that every finitely generated projective module over $k[x_1, \ldots, x_n]$ is in fact free. Of course, the original proof of Hilbert did not use neither the Quillen–Suslin theorem, nor the machinery of homological algebra, which did not exist at the time; in fact, Hilbert's theorem can be seen as a forerunner of that machinery. We present Hilbert's elementary proof in Exercise 19. In the next section, we are going to prove Hilbert's syzygy theorem using the theory of stably free modules.

Remark 5.6.3. We can reformulate a special case of Hilbert's theorem as follows. Let k be a field, and $f_1, \ldots, f_k$ be homogeneous polynomials in $A = k[x_1, \ldots, x_n]$, of degrees $d_1, \ldots, d_k$. Then

$$\operatorname{pd}_A A/(f_1, \ldots, f_k) \leq n.$$

---

[1]The word syzygy comes from the Greek, and in astronomy denotes an alignment of three celestial bodies. It was then borrowed for usage in mathematics to denote a more general linear relation.

In [**PS09**], Stillman conjectured that there exists a number p, depending only on $d_1, \dots, d_k$ such that

$$\operatorname{pd}_A A/(f_1, \dots, f_k) \le p.$$

The crucial point is that p does *not* depend on the number n of variables. This is a much deeper result, that was proved by Ananya and Hochster in [**AH19**].

We end this section by studying a particularly simple way to construct free resolutions. Let A be a Noetherian ring, M a finitely generated A-module. By definition, we have a surjective homomorphism $f_0 \colon A^{n_0} \to M$, and we can choose n_0 to be minimal. If we let $K_0 = \ker f_0$, then K_0 is finitely generated as well, and we can repeat the construction with a homomorphism $f_1 \colon A^{n_1} \to K_0$, where n_1 is as small as possible. Continuing in this way, we obtain a (possibly infinite) free resolution of M

$$\cdots \longrightarrow A^{n_k} \xrightarrow{f_k} \cdots \xrightarrow{f_1} A^{n_0} \xrightarrow{f_0} M \longrightarrow 0. \tag{5.6.1}$$

Definition 5.6.4. A free resolution as in (5.6.1), where each n_i is as small as possible, is called a *minimal* free resolution.

The main result on minimal free resolutions is the following characterization in the local case.

Proposition 5.6.5. *Let $A, \mathcal{M}$ be local Noetherian ring, $k = A/\mathcal{M}$ the residue field, M a finitely generated A-module. Take a free resolution of M as in* (5.6.1)*. The following are equivalent:*

(i) *the resolution is minimal;*

(ii) *for each $i \ge 1$, $f_i(A^{n_i}) \subset \mathcal{M}A^{n_{i-1}}$, and $f_0(A^{n_0}) \subset \mathcal{M}M$; and*

(iii) *for each $i \ge 1$, the matrix representing f_i has coefficients in $\mathcal{M}$, and $f_0(A^{n_0}) \subset \mathcal{M}M$.*

Proof. Denote $F_i = A^{n_i}$, and notice that $n_i = \dim_k F_i \otimes_A k = \dim_k F_i/\mathcal{M}F_i$. Let $K_i = \ker f_i$, and for simplicity of notation let $K_{-1} = M$. When constructing the minimal F_i, we take a surjective map $f_i \colon A^{n_i} \to K_{i-1}$, where n_i is minimal. By Nakayama's lemma, such map is surjective if and only if the map $k^{n_i} \to K_{i-1} \otimes_A k$ is, so the smallest n_i that we can choose is

$$n_i = \dim_k K_{i-1} \otimes_A k.$$

If n_i is chosen in this way and the map of vector spaces $k^{n_i} \to K_{i-1} \otimes_A k$ is surjective, it must be an isomorphism.

Rewrite this as an isomorphism $F_i/\mathcal{M}F_i \cong K_{i-1}/\mathcal{M}K_{i-1}$. It follows that

$$\ker(F_i \to F_{i-1}) = \ker(F_i \to K_{i-1}) \subset \mathcal{M}F_i,$$

thereby showing that (i) implies (ii).

Conversely, if (ii) holds, the map $F_i/\mathcal{M}F_i \cong K_{i-1}/\mathcal{M}K_{i-1}$ is injective. Since it is also surjective, it must be an isomorphism, hence n_i is as small as possible, proving (i).

Finally, (ii) and (iii) are both equivalent to the condition that the tensored complex $F_\bullet \otimes_A k$ has 0 maps, and thus equivalent to each other. $\square$

Corollary 5.6.6. *Let $A, \mathcal{M}$ be a local Noetherian ring, M a finitely generated A-module. Then the numbers n_i in a minimal free resolution* (5.6.1) *are uniquely determined by M. In fact, $n_i = \dim_k \operatorname{Tor}_i^A(k, M)$, where $k = A/\mathcal{M}$.*

Proof. Let $K_i = \ker f_i$. The number n_i is the dimension of the vector space $K_i/\mathcal{M}K_i$. The result then follows from the fact that if $F_\bullet \to M$ is a minimal resolution, then $F_\bullet \otimes_A k$ has 0 differentials by Proposition 5.6.5(ii). $\square$

Definition 5.6.7. The numbers n_i in (5.6.1) are called the *Betti numbers* of M.

5.7. Stably free modules

In Example 5.1.1(d), we have seen that for a compact and paracompact topological space X, finitely generated projective modules over the ring $A = C(X)$ are the same as locally free modules, and they all arise as the modules of sections of a suitable vector bundle $E \to X$. This led us to investigate the relation between projective and locally free modules for a general ring.

Following this analogy, one can take inspiration from topological K-theory [**Hat17**], which is a cohomology theory that studies spaces by analyzing the category of vector bundles over them. One can hope to translate results in topological K-theory into results about projective modules over general rings. This eventually leads to the study of algebraic K-theory. We will not pursue this in general; instead we will limit ourselves to the simplest example.

If X is a contractible space, all vector bundles on X are actually trivial. In algebraic geometry, one does not have a notion of contractible space, but surely the affine space $\mathbb{A}^n(k)$ over a field k is a natural candidate. This line of reasoning leads to the conjecture that a finitely generated projective module over $k[x_1, \ldots, x_n]$ is in fact free.

This was posed as a problem by Serre in his seminal paper [**Ser55**], and resolved affirmatively by Quillen in [**Qui76**] and Suslin in [**Sus76**] at the same time. The account that we give will follow a simplified proof by Vaserstein in [**VS74**]. For much more on the history of Serre's problem and the development that followed, see the book [**Lam06**].

We start with a result that is slightly weaker, already proved by Serre.

Definition 5.7.1. Let A be a ring, M an A-module. We say that M is *stably free* if there exists a finitely generated free module F such that $M \oplus F$ is free. More generally, two A-modules M, N are *stably isomorphic* if there exist finitely generated free modules F, G such that $M \oplus F \cong N \oplus G$. Hence M is stably free if and only if it is stably isomorphic to a free module.

Remark 5.7.2. A stably free module is projective by Proposition 2.6.4. Moreover, notice that the condition that F is finitely generated is crucial in the definition. Otherwise, according to Exercise 2, *every* projective module would be stably free.

We see that *stably free* is a convenient intermediate notion between *projective* and *free*. These notions are actually distinct, as the next example shows.

Example 5.7.3.

(a) Let $A = \mathbb{Z}/pq\mathbb{Z}$ for two distinct primes p, q, and consider the A-module $M = \mathbb{Z}/p\mathbb{Z}$. Then M is a direct summand of A, hence it is projective, but it is not stably free for cardinality reasons.

(b) Let $S^n \subset \mathbb{R}^{n+1}$ be the n-sphere, and T_{S^n} its tangent bundle. The normal bundle of S^n is trivial, hence there is an exact sequence of vector bundles

$$0 \longrightarrow T_{S^n} \longrightarrow S^n \times \mathbb{R}^{n+1} \longrightarrow S^n \times \mathbb{R} \longrightarrow 0 \ .$$

Letting $A = C(S^n)$, this gives an exact sequence of the A-modules of sections

$$0 \longrightarrow C(T_{S^n}) \longrightarrow A^{n+1} \longrightarrow A \longrightarrow 0 \ .$$

This sequence splits, showing that $C(T_{S^n})$ is stably free. On the other hand, $C(T_{S^n})$ is free if and only if T_{S^n} is trivial, which happens only for $n = 1, 3, 7$ by a theorem of Adams [**Hat17**, Theorem 2.16]. Without using the full strength of this result, the hairy ball theorem [**Hat02**, Theorem 2.28] shows that T_{S^n} does not even admit a nonvanishing section for n even, so it is certainly not trivial.

Our aim in the first part of the section is to prove the following result. Our approch follows [**Lan02**, Section XXI.2] with some simplifications.

Theorem 5.7.4 (Serre)**.** *Let M be a finitely generated projective module over $A = k[x_1, \ldots, x_n]$, where k is a field or a Dedekind ring. Then M is stably free.*

This will be easy to prove once we have some general results on stably free modules.

Proposition 5.7.5. *Let A be a Noetherian ring, M a finitely generated, projective A-module. Then M is stably free if and only if it admits a finite free resolution.*

Proof. Assume that M has a finite free resolution of length n, say

$$0 \longrightarrow F_n \longrightarrow \cdots \longrightarrow F_1 \longrightarrow F_0 \longrightarrow M \longrightarrow 0.$$

By the Noetherian hypothesis, we can assume that all F_i are finitely generated. We prove that M is stably free by induction on n, the case $n = 0$ being obvious. Letting $K = \ker F_0 \to M$, we get the exact sequence

$$0 \longrightarrow K \longrightarrow F_0 \longrightarrow M \longrightarrow 0 \ ,$$

which splits because M is projective. Then K is projective as well, hence stably free by induction, say $K \oplus G \cong H$, where G, H are finitely generated free modules. Hence

$$M \oplus H \cong M \oplus K \oplus G \cong F_0 \oplus G,$$

which is free. The other direction is obvious. □

Notice that this result, together with Hilbert's theorem, Theorem 5.6.2, is already enough to prove Theorem 5.7.4. Of course, this would be circular, so there is still some work to do. Instead, what we are going to do is to prove a weaker version of Hilbert's syzygy theorem, namely that every finitely generated module over $k[x_1, \ldots, x_n]$ has a finite free resolution, which is in any case enough to prove Serre's theorem. We will then obtain Hilbert's syzygy theorem by combining this result with our computation of the global dimension of $k[x_1, \ldots, x_n]$ (Corollary 5.5.8). This allows us to decouple the problem of existence of finite free resolutions from the problem of finding a bound on their length.

We will prove the existence of finite free resolutions by induction. The following result allows the induction step to go through.

Proposition 5.7.6. *Let A be a ring,*

$$0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow M_3 \longrightarrow 0$$

an exact sequence of A-modules. If two of the modules admit a finite resolution by free finitely generated modules, so does the third.

In order to prove this, we need to introduce the concept of stably free dimension.

Definition 5.7.7. Let A be a ring, M an A-module. The *stably free dimension* of M, denoted $\operatorname{sfd} M$, is the smallest length of a left resolution of M by *finitely generated* stably free modules. If no such resolution exists, we set $\operatorname{sfd} M = \infty$.

Remark 5.7.8. Given a stably free resolution of M

$$0 \longrightarrow S_n \longrightarrow \cdots \longrightarrow S_1 \longrightarrow S_0 \longrightarrow M \longrightarrow 0,$$

of length $n > 0$, we can alter it to make it a free resolution by adding suitable pairs of free modules to consecutive terms. In other words, if $\operatorname{sfd} M = n > 0$, then M admits a finite free resolution of length n, hence the length of the shortest (finitely generated) free and stably free resolutions of M are the same. It follows that M admits a finite resolution by finitely generated, free modules, if and only if $\operatorname{sfd} M < \infty$.

Of course, the above remark does not hold for $n = 0$: a stably free module is not necessarily free. What we need to make the notion of stably free dimension workable is an analogue of Remark 5.2.8. Unfortunately, we cannot leverage the machinery of the Ext functors and dimension shifting, so we will need to produce a more explicit proof.

Lemma 5.7.9. *Let M, N be stably isomorphic A-modules. Then* $\operatorname{sfd} M = \operatorname{sfd} N$.

Proof. We can assume that $N = M \oplus F$ for some finitely generated free module F. Clearly, a finite free resolution of M gives rise to a finite free resolution of N of the same length.

Conversely, assume there is a finite resolution

$$0 \longrightarrow S_n \longrightarrow \cdots \longrightarrow S_1 \longrightarrow S_0 \longrightarrow M \oplus F \longrightarrow 0,$$

where the modules S_i are stably free. The surjection $S_0 \to F$ splits, hence we can write $S_0 = R_0 \oplus F$, and $R_0 \to M$ is still surjective. Then

$$\ker(R_0 \to M) = \ker(S_0 \to M \oplus F) = \operatorname{coker}(S_2 \to S_1),$$

and we get a stably free resolution of M of length n. □

We can now prove the analogue of Remark 5.2.8. Notice that this approach would also work to develop the theory of projective dimension, although using Ext functors is much more convenient.

Proposition 5.7.10. *Let M be an A-module with* $\operatorname{sfd} M = n > 0$*, and consider an exact sequence*

$$0 \longrightarrow K \longrightarrow S \longrightarrow M \longrightarrow 0\ ,$$

where S is finitely generated and stably free. Then $\operatorname{sfd} K = n - 1$.

Proof. A stably free resolution of K of length k gives a stably free resolution of M of length $k+1$, hence $\operatorname{sfd} M \leq \operatorname{sfd} K + 1$. For the converse inequality, take a stably free resolution

$$0 \longrightarrow S_n \longrightarrow \cdots \longrightarrow S_1 \longrightarrow S_0 \longrightarrow M \longrightarrow 0$$

of length n. Since S is projective, we can lift the map $S \to M$ to a map $S \to S_0$, giving rise to a diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & K & \longrightarrow & S & \longrightarrow & M & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow{\scriptstyle \mathrm{id}_M} & & \\ 0 & \longrightarrow & K_0 & \longrightarrow & S_0 & \longrightarrow & M & \longrightarrow & 0, \end{array}$$

where $K_0 = \ker S_0 \to M$. Clearly, $\operatorname{sfd} K_0 = n - 1$.

By Schanuel's lemma (Proposition 4.4.1), there is an isomorphism $K_0 \oplus S \cong K \oplus S_0$. Hence, K and K_0 are stably isomorphic, and the conclusion follows from Lemma 5.7.9. □

Lemma 5.7.11. *Let*

$$0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow M_3 \longrightarrow 0$$

be an exact sequence of A-modules, where M_2 is finitely generated and M_3 is finitely presented. Then M_1 is finitely generated.

Proof. First, assume that M_2 is actually free, and take an exact sequence

$$0 \longrightarrow K \longrightarrow F \longrightarrow M_3 \longrightarrow 0 ,$$

where K, F are finitely generated and F is free. By Schanuel's lemma (Proposition 4.4.1), $K \oplus M_2 \cong M_1 \oplus F$, from which we conclude that M_1 is finitely generated.

In general, take a finitely generated free module G with a surjection $G \to M_2$, and let $H = \ker G \to M_3$. Then there is a surjection $H \to M_1$, and H is finitely generated by the first part of the proof. □

Proof of Proposition 5.7.6. There are three cases, according to which pair among (M_1, M_2), (M_1, M_3) and (M_2, M_3) we assume to have finite stably free dimension. In all cases, we will produce a commutative diagram of the form

(5.7.1)
$$\begin{array}{ccccccccc} & & 0 & & 0 & & 0 & & \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & K_1 & \longrightarrow & K_2 & \longrightarrow & K_3 & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & S_1 & \longrightarrow & S_2 & \longrightarrow & S_3 & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & M_1 & \longrightarrow & M_2 & \longrightarrow & M_3 & \longrightarrow & 0, \\ & & \downarrow & & \downarrow & & \downarrow & & \\ & & 0 & & 0 & & 0 & & \end{array}$$

where S_1, S_2, and S_3 are stably free (in fact, finitely generated free).

The first thing to prove is that all of M_1, M_2 and M_3 are finitely generated. This is clear, except in the case where we assume that M_2 and M_3 have finite stably free dimension, where it follows by Lemma 5.7.11.

To obtain diagram (5.7.1), take S_i to be a finitely generated free module with a surjection to M_i for $i = 1, 3$, and let $S_2 = S_1 \oplus S_3$. The map $S_2 \to M_2$ results by letting it restrict to $S_1 \to M_1$ on the summand S_1, and choosing a lift $S_3 \to M_2$ on the other one. Finally, choose $K_i = \ker S_i \to M_i$. By construction, all columns and the bottom two rows are exact, and the top row is exact by the nine lemma.

The proof then splits into two cases. In the first one, we assume that $\operatorname{sfd} M_2 < \infty$ and either $\operatorname{sfd} M_1 < \infty$ or $\operatorname{sfd} M_3 < \infty$—we want to prove that the other one holds. If $\operatorname{sfd} M_2 = 0$, M_2 is stably free and the conclusion follows by Proposition 5.7.10. Otherwise, the same Proposition gives us $\operatorname{sfd} K_2 = \operatorname{sfd} M_2 - 1$, and we finish the proof by induction on $\operatorname{sfd} M_2$.

The remaining case has $\operatorname{sfd} M_1 < \infty$ and $\operatorname{sfd} M_3 < \infty$. In this case, we argue by induction on $\max\{\operatorname{sfd} M_1, \operatorname{sfd} M_3\}$. If both M_1 and M_3 are stably free, the exact sequence between the M_i splits, hence $M_2 = M_1 \oplus M_3$ is stably free as well. Otherwise, Proposition 5.7.10 gives us $\operatorname{sfd} K_i = \operatorname{sfd} M_i - 1$ for $i = 1, 3$, and we reduce to a smaller case. □

We can now prove the main result of this section.

Theorem 5.7.12. *Let A be a Noetherian ring such that every finitely generated A-module has a finite free resolution. Then every finitely generated $A[x]$-module has a finite free resolution.*

Notice that we do not specify whether the free modules in the resolution are finitely generated, but over a Noetherian ring, a finitely generated module that has a finite resolution by free modules also has a finite resolution by finitely generated free modules.

Proof. We need to prove that every module M over $A[x]$ has a finite free resolution. By Theorem A.3.7 and Proposition 5.7.6, it is enough to prove the result for $M = A/P$ for some prime ideal P. By another application of Proposition 5.7.6, we can prove the result for $M = P$.

Let $Q = P \cap A$. By hypothesis, Q has a finite free resolution, hence so does $Q[x] = Q \cdot A[x]$. Let $A' = A/Q$, $P' = P/(Q \cdot A[x])$. By Proposition 5.7.6, P has a finite free resolution if and only if P' does.

To find such a resolution for P', we first work over $A'[x]$, where we have the convenience that A' is an integral domain. Let $k = \mathcal{F}(A')$ be its field of fractions. Choose generators $f_1, \ldots, f_d$ for P', and an element $f \in P'$ of minimal degree. Then we can perform the division over k to get $f_i = q_i \cdot f + r_i$, where $q_i, r_i \in k[x]$. By clearing denominators, we find $a' f_i = a' q_i \cdot f + a' r_i$ for some $a' \in A'$ such that $a' q_i \in A'[x]$ and $a' r_i \in A'[x]$. Since f has minimal degree, $a' r_i = 0$, whence $a' \cdot P' \subset (f)$.

Lifting a' to some $a \in A$, we have the exact sequence of $A[x]$-modules

$$0 \longrightarrow a \cdot P' \longrightarrow f \cdot A'[x] \longrightarrow N \longrightarrow 0 \ ,$$

where N is the quotient. Since A' is integral, as $A[x]$-modules, $a \cdot P' \cong P'$ and $f \cdot A'[x] \cong A'[x]$, so we read this exaxct sequence as

$$0 \longrightarrow P' \longrightarrow A'[x] \longrightarrow N \longrightarrow 0 \ .$$

Since $A'[x] = A[x]/(Q \cdot A[x])$, by another application of Proposition 5.7.6, we reduce to proving that N has a finite free resolution.

As in the first part of the proof, N has a filtration by $A[x]$-modules of the form $A[x]/R$, for some prime ideals $R \subset A[x]$, and we can reduce to proving that each of them has a finite free resolution. Moreover, by Theorem A.3.7, such primes R are exactly the associated primes of N. We claim that each associated prime R of N is strictly larger than P. Clearly, $P \subset \operatorname{Ann}(n)$ for all $n \in N$. Moreover, $a \in \operatorname{Ann}(n)$ as well, and $a \notin P$, since $a' \neq 0$ in A'.

All of the above works for any prime P. Now, assuming that a prime without a finite free resolution exists at all, we can choose P to be maximal with respect to this condition, since $A[x]$ is Noetherian. With this choice, every associated prime R of N has a finite free resolution, hence the same holds for N, and eventually for P' and P, which is a contradiction. □

As corollaries, we derive Serre's theorem on stably free modules and Hilbert's syzygy theorem.

Proof of Theorem 5.7.4. Combine Theorem 5.7.12 and Proposition 5.7.5. □

Proof of Theorem 5.6.2. By Corollary 5.5.8, $\operatorname{gl.dim} k[x_1, \ldots, x_n] = n$, hence every module over $k[x_1, \ldots, x_n]$ has a projective resolution of length n. If the module is finitely generated, one can choose the projectives to be finitely generated as well. By Theorem 5.7.4, this is a stably free resolution. By Remark 5.7.8, we can alter this resolution to produce a resolution of length n by finitely generated free modules. □

We end this section with a result of Gabel [**Gab72**], showing that stably free modules are interesting only in the finitely generated case. The proof is from [**Con13**].

Theorem 5.7.13 (Gabel)**.** *Let M be a stably free A-module. If M is* not *finitely generated, then M is free.*

Proof. Let $M \oplus A^k \cong F$, with F free, and choose a basis $\mathcal{B}$ for F. Since $F \to A^k$ is surjective, we can choose a finite subset $\mathcal{B}' \subset \mathcal{B}$ such that the free module F' generated by $\mathcal{B}'$ surjects onto A^k.

Then we have $M + F' = F$, hence, letting $N = M \cap F'$,

$$\frac{F}{F'} \cong \frac{M + F'}{F'} \cong \frac{M}{M \cap F'} = \frac{M}{N}.$$

Moreover, the exact sequence

$$0 \longrightarrow N \longrightarrow F' \longrightarrow A^k \longrightarrow 0$$

splits, so $N \oplus A^k \cong F'$. Since F/F' is free of infinite rank, we can write $F/F' \cong A^k \oplus F''$, with F'' free.

Finally, since $M/N \cong F/F'$ is projective,

$$M \cong N \oplus \frac{M}{N} \cong N \oplus \frac{F}{F'} \cong N \oplus A^k \oplus F'' \cong F' \oplus F''. \qquad \square$$

A result in the same spirit is the following from [**Bas63a**].

Theorem (Bass)**.** *Let A be a Noetherian ring, M a projective module, and assume that the only elements $a \in A$ such that $a^2 = a$ are 0 and 1. If M is* not *finitely generated, then M is free.*

Remark 5.7.14. The hypothesis on idempotent elements is necessary to avoid trivial examples, such as the module A over $A \times B$ for any two rings A, B. Less obviously, the Noetherian hypothesis is also necessary; see Exercise 16.

One can also obtain results in the finitely generated case, as long as the rank of the module is big enough with respect to the dimension of the ring. A nice result from [**Yen11**] is

Theorem (Yengui). *Let A be a ring with $\dim A < \infty$, and M a stably free module over $A[x]$, so that $M \oplus A[x]^m \cong A[x]^n$. If $n - m > \dim A$, then M is free.*

5.8. The Quillen–Suslin theorem

We now take the decisive step towards the solution of Serre's problem, passing from stably free to free modules. Our aim is to prove the following result.

Theorem 5.8.1 (Quillen–Suslin). *Let $A = k[x_1, \dots, x_n]$, where k is a field or a principal ideal domain. If M is a finitely generated projective module over A, then M is free.*

Of course, we have already done the passage from projective to stably free in the previous section. For reasons that will become apparent in a moment, we rephrase the question of freeness of a stably free module in the following way.

Assume that M is a stably free, finitely generated A-module, so that $M \oplus A^m \cong A^n$ for some $m, n \in \mathbb{N}$. Here $m \leq n$, as can be seen by taking the quotient with respect to any maximal ideal. We can see M as the cokernel of a morphism $f \colon A^m \to A^n$, which happens to split. Then f is given by a matrix with coefficients in A. We are free to change the bases for the two free A-modules, which corresponds to multiplication by an element of $\mathrm{GL}_m(A)$ on the left and $\mathrm{GL}_n(A)$ on the right. If, applying these operations, we can choose a matrix for f which represents the standard inclusion $A^m \to A^n$ by the first m coordinates, then the cokernel of f is manifestly free, isomorphic to A^{n-m}. Hence the question can be rephrased by starting from a $m \times n$ matrix that represents a split monomorphism, and checking whether a particular matrix lies in its orbit under the action of these groups.

Now, one can easily see that if this always holds for $m = 1$, then it holds for any m, by a simple induction. We are thus going to study morphisms $f \colon A \to A^n$ such that f is a split monomorphism. Such f is uniquely determined by the vector $v = f(1) \in A^n$.

Definition 5.8.2. The vector $v \in A^n$ is called *unimodular* if its coordinates $v_1, \dots, v_n$ generate the unit ideal in A.

Lemma 5.8.3. *Let $f \colon A \to A^n$ be a homomorphism. Then f is a split monomorphism if and only if $v = f(1)$ is unimodular.*

Proof. The condition that f is a split monomorphism amounts to saying that there exists a homomorphism $g\colon A^n \to A$ such that $g(v) = 1$. Representing g by a $n \times 1$ matrix with entries $g_1, \ldots, g_n$, this can be written as $\sum_{i=1}^n g_i v_i = 1$, which means exactly that v is unimodular. □

In light of the above lemma and the discussion preceding it, we are going to study unimodular vectors in A^n modulo the action of $\mathrm{GL}_n(A)$ on the right. Actually, we will transpose everything, turning our vectors into column vectors, and changing the action of $\mathrm{GL}_n(A)$ to be an action on the left. We will simply say that two unimodular vectors v, w are equivalent if there is a matrix $M \in \mathrm{GL}_n(A)$ such that $M \cdot v = w$, in which case we write $v \sim w$. We aim to find conditions for a ring A that guarantee that every unimodular vector is equivalent to the standard basis vector e_1, or, in other words, that every two unimodular vectors are equivalent.

Remark 5.8.4. Over a PID or a local ring, every projective module is free (the latter is Theorem 5.1.2). Hence, if A is a PID or local, every two unimodular vectors are equivalent.

We will prove the result for polynomial rings by localization. Hence, our point of departure is the following result for local rings.

Theorem 5.8.5 (Horrocks)**.** *Let $A, \mathcal{M}$ be a local ring,*

$$v = (v_1(x), \ldots, v_n(x)) \in A[x]^n$$

a unimodular vector such that one of the elements v_i is monic. Then $v \sim e_1$.

Lemma 5.8.6. *Let A be a ring, $v \in A^n$ a unimodular vector for $n = 1, 2$. Then $v \sim e_1$.*

Proof. The result is obvious for $n = 1$. For $n = 2$, we have an equation $av_1 + bv_2 = 1$. Then the matrix $M = \begin{pmatrix} a & b \\ -v_2 & v_1 \end{pmatrix}$ has $\det M = 1$, so M is invertible over A, and $M \cdot v = e_1$. □

Proof of Theorem 5.8.5. By Lemma 5.8.6, we can assume that $n \geq 3$. Say v_1 is monic, and let $d = \deg v_1$. We will prove the result by induction on d, the case $d = 0$ being obvious (check it!).

By row operations, we can assume that $\deg v_i < d$ for $i \geq 2$. If all coefficients of all v_i lie in $\mathcal{M}$ for $i \geq 2$, v is not unimodular. In fact, reduction modulo $\mathcal{M}$ kills all coordinates but v_1, and v_1 does not generate the unit ideal in $k[x]$, for $k = A/\mathcal{M}$. We can then assume that v_2 has a coefficient outside $\mathcal{M}$, which is thus a unit of A.

We claim that there exists a monic polynomial

$$h(x) = a(x)v_1(x) + b(x)v_2(x) \tag{5.8.1}$$

such that $\deg h < d$. To see this, let $I \subset A$ be the ideal generated by all leading coefficients of polynomials h of the form (5.8.1) where $\deg h < d$. It is easy to see that all coefficients of v_2 belong to I (use descending induction starting from the highest coefficient), hence $I = A$. In particular, $1 \in A$, which is our claim.

We can now use row operations to replace v_3 by $v_3' = v_3 - c \cdot h$ for some $c \in A[x]$, in such a way that v_3' is monic and $\deg v_3' < d$. The proof is then finished by the induction hypothesis. □

Corollary 5.8.7. *Let $A, \mathcal{M}$ be a local ring,*

$$v = (v_1(x), \ldots, v_n(x)) \in A[x]^n$$

a unimodular vector such that one of the elements v_i is monic. Then $v \sim v(0) \in A^n$.

This is obvious, since both v and $v(0)$ are equivalent to e_1 (the latter because of Remark 5.8.4), but it will turn out to be a convenient reformulation, since it allows induction from A to $A[x]$.

One can also formally derive other relations. Assume that $v \sim v(0)$, so that there is an $n \times n$ matrix $M(x)$ over $A[x]$ such that $M(x) \cdot v(x) = v(0)$. By replacing formally x with $x+y$ we end up with $M(x+y) \cdot v(x+y) = v(0)$. Combining the two relations we get

$$M(x)^{-1} M(x+y) \cdot v(x+y) = v(x),$$

so that $v(x+y) \sim v(x)$ over $A[x, y]$.

Our next task is to generalize Corollary 5.8.7 to arbitrary rings.

Proposition 5.8.8. *Let A be a ring,*

$$v = (v_1(x), \ldots, v_n(x)) \in A[x]^n$$

a unimodular vector such that one of the elements v_i is monic. Then $v \sim v(0) \in A^n$.

The key is the following localization result.

Lemma 5.8.9. *Let A be a ring, $S \subset A$ a multiplicative set, $v \in A[x]^n$, and assume that $v \sim v(0)$ over $S^{-1}A[x]$. Then $v(x) \sim v(x+sy)$ over $A[x, y]$, for some $s \in S$.*

Proof. We have seen that $v(x) \sim v(x+y)$ over $S^{-1}A[x, y]$, so there is a matrix M over $S^{-1}A[x, y]$ such that $M(x, y) \cdot v(x+y) = v(x)$. Replacing y by sy we get

$$M(x, sy) \cdot v(x+sy) = v(x),$$

so it is enough to check that $M(x, sy)$ has coefficients in A for some $s \in S$.

By construction, $M(x, 0)$ is the identity, hence $M(x, y) = I + yN$ for some matrix N. Then $M(x, sy) = I + syN$, and it is enough to choose $s \in S$ to clear the denominators in N. □

Proof of Proposition 5.8.8. Reversing what we have done before, it is enough to show that $v(x+y) \sim v(x)$ over $A[x, y]$, and then substitute $x = 0$ (and rename y to x).

This leads us to define

$$I := \{a \in A \mid v(x + ay) \sim v(x) \text{ over } A[x, y]\}.$$

It will be enough to prove that $1 \in I$. It is easy to check that I is an ideal. For instance, if $a, b \in I$, then $v(x + ay) \sim v(x)$ and $v(x + by) \sim v(x)$. Changing x into $x+ay$ in the latter, we get $v(x+ay+by) \sim v(x+ay) \sim v(x)$. Similarly, I is closed under multiplication for an element of A.

Knowing that I is an ideal, we can rely on our local results. If $I \subsetneq A$, then $I \subset \mathcal{M}$ for some maximal ideal $\mathcal{M}$. Corollary 5.8.7 then guarantees that $v(x) \sim v(0)$ over $A_{\mathcal{M}}[x]$, and by Lemma 5.8.9 there is $s \notin \mathcal{M}$ such that $v(x) \sim v(x + sy)$ over $A[x, y]$, hence $I \not\subset \mathcal{M}$. □

Proposition 5.8.8 is the crucial inductive step to prove the following formulation of the Quillen–Suslin theorem.

Theorem 5.8.10 (Quillen–Suslin)**.** *Let $A = k[x_1, \dots, x_n]$, where k is a field or a principal ideal domain. If $v \in A^n$ is unimodular, then $v \sim e_1$.*

Proof. We perform induction on n, the case $n = 0$ being Remark 5.8.4. We look at A as the ring $B[x_n]$, where $B = k[x_1, \dots, x_{n-1}]$.

We can perform the following invertible change of variables over A. Replace x_i by $x_i - x_n^{M^i}$ for $i < n$, for some $M \gg 0$ (compare the proof of Noether's normalization lemma in [**Fer20**, Theorem 5.3.1]). Then we can guarantee that the entries v_i of v become monic, as polynomials in x_n.

By Proposition 5.8.8, $v \sim v(0) \in A^n$, and since $v(0) \in B^n$, we are done by induction. □

Proof of Theorem 5.8.1. By Serre's theorem, Theorem 5.7.4, M is stably free. Hence $M \oplus A^m \cong A^n$ for some $m, n \in \mathbb{N}$. By induction over m, we only need to prove the case $m = 1$. In this case, there is a split monomorphism $f\colon A \to A^n$ such that $M \cong \operatorname{coker} f$.

The vector $v = f(1) \in A^n$ is unimodular, and by Theorem 5.8.10, $v \sim e_1$. Hence, we can perform a change of variables in A^n such that f becomes the standard inclusion in the first coordinate, and then $M \cong A^{n-1}$. □

Remark 5.8.11. A ring A such that all stably free A-modules are free is called a *Hermite ring*. One may be tempted to strengthen the above result to say that if A is Hermite, then $A[x]$ is Hermite. But the proof of Theorem 5.8.10 uses a crucial change of variables that is only available in polynomial rings to achieve the condition that one of the components v_i is monic. In fact, the question of whether being Hermite is inherited from A to $A[x]$ is known as the Hermite ring conjecture by Lam [**Lam78**], and is currently still open.

5.9. Exercises

1. Give a proof of Theorem 5.1.2 under the assumption that P is finitely generated, as follows. Let $\mathcal{M}$ be the maximal ideal of A, and choose a set $\{p_1, \dots, p_n\} \subset P$ such that the classes $\{\overline{p_1}, \dots, \overline{p_n}\}$ are a basis of the vector space $P/\mathcal{M}P$. Consider the map $f\colon A^n \to P$ defined by $f(e_i) = p_i$ and apply Nakayama's lemma.

2. Let P be a projective A-module. Show that there exists a free A-module F such that $P \oplus F \cong F$. The construction you will probably come up with is called the Eilenberg swindle.

3. Let A be a Boolean ring, that is, a ring such that $a^2 = 2$ for all $a \in A$. Prove that all localizations of A are isomorphic to $\mathbb{Z}/2\mathbb{Z}$, and conclude that every module over A is locally free.

4. Let A be a direct product of countably many copies of $\mathbb{Z}/2\mathbb{Z}$, and $I \subset A$ their direct sum. Prove that A is Boolean ring (see Exercise 3), and that I is an ideal. Show that I is not principal and conclude that A/I is a locally free, finitely generated A-module that is not projective.

Exercises 5–10, discuss the notion of locally free module in the following strong sense. We say that M is *locally free in the strong sense* if there exist elements $a_1, \dots, a_n \in A$ that generate the whole ring as an ideal such that M_{a_i} is free for all i. We will provide an example from [**dJea20**, Tag $05WG$] of a projective module that is not locally free in the strong sense.

5. Show that if M is locally free in the strong sense, then it is locally free with the usual definition.

6. Let A be a Noetherian ring, M a finitely generated, projective A-module. Show that M is locally free in the strong sense.

7. Let A be a ring, $\{a_i\}_{i\in\mathbb{N}}$ elements of A satisfying $a_i^2 = a_i$, and let $I = (a_1, a_2, \dots)$ be the ideal that they generate. Show that I is projective. (Up to changing the a_i, one can assume that $(a_i) \subset (a_{i+1})$, so that $I = \operatorname{colim}(a_i)$. Then show that h^I is exact by Theorem 3.5.9.)

8. Let A be a ring, and assume that there is an injective map $f\colon A^n \to M$ for some A-module M. Then M cannot be generated by less that n elements.

(Reduce to the case of M free, and consider the matrix S associated to f. If one of the elements of S is a unit, one can reason by induction. Reduce to this case by localization, unless all elements of S are nilpotent, in which case prove the claim directly.)

9. Let A be a ring $M \subset N$ two A-modules. Show that if N is finitely generated and M is locally free in the strong sense, then M is finitely generated. (Use the previous exercise.)

10. Let $A = \prod_{i=1}^{\infty} \mathbb{Z}/2\mathbb{Z}$ be an infinite product of copies of $\mathbb{Z}/2\mathbb{Z}$. Use the previous exercises to find an ideal $I \subset A$ that is projective but not locally free in the strong sense.

11. Let I be an ideal of A. If A/I is a projective A-module, prove that I is principal.

12. Find a counterexample to Theorem 5.2.10 if we drop the assumption that $\operatorname{pd}_{A/(a)} M < \infty$. Namely, find a ring A, an element $a \in A$, which is not a zero divisor, and a module M over $A/(a)$ such that $\operatorname{pd}_{A/(a)} M = \infty$ but $\operatorname{pd}_A M < \infty$.

13. Show that for a ring A all A-modules are injective if, and only if, all A-modules are projective. In this case, we say that A is *semisimple*.

14. Let M, N be two A-modules such that $M \oplus P \cong N \oplus Q$, with P, Q projective A-modules. Prove that $\operatorname{pd} M = \operatorname{pd} N$.

15. Let X be a compact and paracompact topological space. Prove that the category of continuous vector bundles over X is equivalent to the category of finitely generated projective modules over the ring $A = C(X)$. This result is known as *Swan's theorem* [**Swa62**].

16. Let $A = C([0,1])$, and consider the ideal $I \subset A$ of functions f such that $f|_{[0,\epsilon]} = 0$ for some $\epsilon > 0$. Show that the only elements $f \in A$ such that $f^2 = f$ are the constants 0 and 1. Prove that I is projective, but I is not free. Conclude that I is *not* finitely generated.

17. Let P, Q be projective A-modules. Prove that $P \otimes_A Q$ is projective. Is the same true for injective modules?

18. Let P be a finitely generated projective A-module. Prove that there is a canonical isomorphism $\operatorname{Hom}(P, A) \otimes P \cong \operatorname{End}_A(P)$. If P is moreover free, prove that the composition

$$\operatorname{End}_A(P) \cong \operatorname{Hom}(P, A) \otimes P \to A,$$

where the latter is the evaluation morphism, is the usual trace (that is, if $f\colon P \to P$ is represented by a matrix M, this is the sum of the diagonal entries of M).

19. Let k be a field, $A = k[x_1, \ldots, x_n]$. Show that if

$$0 \longrightarrow F_0 \longrightarrow F_1 \longrightarrow \cdots \longrightarrow F_n$$

is an exact sequence of graded A-modules and $F_1, \ldots, F_n$ are finitely generated free, then so is F_0. Deduce the graded version of Hilbert's syzygy theorem (Theorem 5.6.2). (Show that the sequence remains exact up to F_{n-1} when taking the quotient with respect to x_n.)

20. Derive from the previous exercise another proof of the existence of the Hilbert polynomial for finitely generated graded modules over $A = k[x_1, \ldots, x_n]$. Namely, if M is such a module, there exists a polynomial $p_M \in \mathbb{Q}[x]$ such that $\dim_k M_i = p_M(i)$ for all i big enough.

21. Let M be an A-module. We say that a morphism $f\colon P \to M$ is a *projective cover* if P is projective, f is surjective, and no proper submodule of P maps surjectively onto M. Show that this is the same as saying $M \to P$ is an injective hull in Mod_A^{op}, and that the projective cover, if it exists, is unique up to isomorphism.

22. Show that $\mathbb{Z}/2\mathbb{Z}$ does not admit a projective cover as a $\mathbb{Z}$-module.

Quite surprisingly, every A-module M admits a *flat cover*, that is, a morphism $F \to M$ as in Exercise 21, where F is only assumed flat (that is, acyclic for Tor, see Chapter 6). This used to be called the *flat cover conjecture*, now a theorem thanks to [**BEBE01**] (see also [**EEE01**]).

23. Let $A, \mathcal{M}$ be a local Artinian ring, with $\mathcal{M}$ principal, and M a finitely generated A-module. Show that M is a direct sum of cyclic modules. (Replace A by $A/\operatorname{Ann} M$, then show that A is injective over itself.)

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

$$T = \{(a, b, c) \in A^3 \mid xa + yb + zc = 0\}.$$

Show that T is a stably free A-module, but is not free.

Starting from this ring, Hochster has given an example of two non-isomorphic rings B, C such that $B[t] \cong C[t]$ [**Hoc72**]. We give his construction in Exercises 25–27. We will need some notation: given an A-module M, we denote by $\operatorname{Sym}^n M$ its n-th symmetric power (see Definition 6.5.4). We also denote $\operatorname{Sym} M = \bigoplus_{n=0}^{\infty} \operatorname{Sym}^n M$, which has the structure of a commutative ring.

25. Let A, T be as in Exercise 24, so that $A^3 \cong A \oplus T$. Show that

$$\operatorname{Sym}(A^3) \cong \operatorname{Sym}(T) \otimes \operatorname{Sym}(A) \cong \operatorname{Sym}(T)[t],$$

where t is an indeterminate. Also show that

$$\operatorname{Sym}(T) \cong \frac{A[a,b,c]}{(xa+yb+zc)}.$$

Hence, if we let $B = A[u,v]$ and $C = \operatorname{Sym}(T)$, we have $B[t] \cong C[t]$ as rings.

26. Keep the notation of the previous exercise. Assume that there is an isomorphism $f\colon B \to C$. Show that f is an isomorphism of $\mathbb{R}$-algebras. Moreover, show that the only solutions to $X^2+Y^2+Z^2=1$ in B actually lie in A. Deduce that the same holds for C, so $f(A) \subset A$ and $f^{-1}(A) \subset A$. Thus, up to composing with an automorphism of A, f is an isomorphism of A-algebras.

27. Keep the notation of the previous exercise. Show that there is no isomorphism of A-algebras $f\colon B \to C$. (Assume that there is one, and let $c = f(u)$ and $d = f(v)$. Obtain from them two generators of T as an A-module and prove that $T \cong A^2$, a contradiction.)

28. By Example 5.3.11 and Theorem 5.3.9, we know that $\mathbb{Q}/\mathbb{Z}$ must be a direct sum of factors, all of which are either $\mathbb{Q}$ or $\mathbb{Z}[p^{-1}]/\mathbb{Z}$ for some prime p. Find explicitly such a decomposition.

29. Let A be a Noetherian ring, $\mathcal{M}$ a maximal ideal. Prove that $\operatorname{gl.dim} A_{\mathcal{M}} = \operatorname{pd}_A A/\mathcal{M}$.

30 (**[AHRT02]**)**.** Prove that injective hulls cannot be made functorial. Namely, assume $E\colon \operatorname{Mod}_A \to \operatorname{Mod}_A$ is a functor with a natural transformation $\iota\colon \mathrm{id} \to E$ such that for all A-modules M, $\iota_M\colon M \to E(M)$ is an injective hull. Prove that all A-modules are injective and E is isomorphic to the identity. (Show that $E(\iota_M)$ is an isomorphism, then use the following diagram

$$\begin{array}{ccccc}
M & \xrightarrow{\iota_M} & E(M) & \overset{f}{\underset{g}{\rightrightarrows}} & N \\
{\scriptstyle \iota_M}\downarrow & & {\scriptstyle \iota_{E(M)}}\downarrow & & {\scriptstyle \iota_N}\downarrow \\
E(M) & \xrightarrow{E(\iota_M)} & E(E(M)) & \overset{E(f)}{\underset{E(g)}{\rightrightarrows}} & E(N)
\end{array}$$

to show that if $f \circ \iota_M = g \circ \iota_M$, then $f = g$.)

31. Let $A, \mathcal{M}$ be a local ring with $\operatorname{gl.dim} A = 2$. Assuming that $\mathcal{M}$ is principal, show that A is a valuation domain.

32. Let P be a finitely generated projective A-module. Show that for all maximal ideals $\mathcal{M} \subset A$, there exists $a \notin \mathcal{M}$ such that P_a is free over A_a. Deduce that if Q_1, Q_2 are two prime ideals such that $Q_1 + Q_2 \subsetneq A$, then P_{Q_1} and P_{Q_2} are free of the same rank (for readers familiar with the terminology, the rank function is locally constant for the Zariski topology). Show that if the only solutions to $a^2 = a$ in A are 0 and 1, then the rank of P_Q is the same regardless of the prime $Q \subset A$. Show that all these properties can fail for nonprojective modules.