UNIVERSITÀ DEGLI STUDI DI GENOVA

DIPARTIMENTO DI MATEMATICA

CORSO DI LAUREA MAGISTRALE IN MATEMATICA

Tesi di Laurea Magistrale

Basic element theory and applications

Candidato
Matteo Pardo

Relatore
Prof. Alessandro De Stefani

Correlatore
Prof. Alessio Caminata

Anno accademico 2025/2026

Contents

Introduction

This thesis mainly deals with basic elements, which are simply minimal generators of an R-module M which remains minimal under localization in primes. Formally, the element $x \in M$ is $\mathfrak{p}$-basic, where $\mathfrak{p}$ is a prime ideal of R, if $\frac{x}{1}$ is a minimal generator of $M_{\mathfrak{p}}$. This definition can be extended to a finite subset of M, in which case we say that $S \subseteq M$ is a $\mathfrak{p}$-basic set.

The first chapter of the thesis and the subsequent section mostly focus on these definitions, together with some elementary properties, which are preliminary to the proof of the Eisenbud-Evans' Theorem, that is covered in the second chapter. Under assumptions regarding specific primes of R, the theorem provides us with a $\mathfrak{p}$-basic element, for all such primes $\mathfrak{p}$.

Basic elements are instrumental in proving theorems which are not apparently related to them. For this reason, being able to obtain a basic element will be useful to prove those results, since it will allow us to make use of the theory developed in the first chapters. A first corollary of the Eisenbud-Evans' Theorem states that every ideal of a Noetherian ring of dimension d, is generated, up to radical, by $d+1$ elements. This result can also be proved without basic elements, however this is one of the reasons for their versatile applicability.

Chapter 3 opens with a discussion about basic elements in projective modules. After various remarks, we conclude that $z \in P$ is $\mathfrak{q}$-basic if and only if its localization at $\mathfrak{q}$ is part of a basis of $P_{\mathfrak{q}}$. Since in the free case, the rank coincides with the minimum number of generators, this fact confirms again that the concept of basic element is an extension of the notion of basis.

At the end of the first section of this chapter, we find a very important result, that is the Serre's Theorem. If P is a finitely generated projective R-module, under further assumptions on its localizations at prime ideals, we obtain that $P \cong R \oplus Q$, with Q a finitely generated module. Again, by examining the localizations, we deduce global information about the starting module. Under similar assumptions, we can also prove the Bass' Cancellation Theorem, which allows to derive from the expression $Q \oplus P \cong Q \oplus M$ the isomorphism $P \cong M$, where P, Q are projective modules.

This local to global process through basic elements is best expressed by the Forster-Swan's Theorem, which is in the last section of chapter 3. Only assuming that R is Noetherian and M is finitely generated, we conclude that:

$$\mu_{R_{\mathfrak{p}}}(M_{\mathfrak{p}}) \leq \mu_R(M) \leq \sup_{\mathfrak{q}\in \operatorname{Spec}(R)} \left\{\mu_{R_{\mathfrak{q}}}(M_{\mathfrak{q}})\right\} + d, \quad \forall \mathfrak{p} \in \operatorname{Spec}(R),$$

where $d = \dim(R)$ and $\mu_R(-)$ denotes the minimal number of generators of a module. The upper bound on the right further explains that the localizations of a module give us global information about it.

Chapter 4 deals with the concept of stable range, which regards the general linear group $GL(R)$. The most important result of the second section claims that if $n \in \mathbb{N}$ defines a stable range for $GL(R)$, then we have that the map $\dfrac{GL_m(R)}{E_m(R)} \longrightarrow \dfrac{GL(R)}{E(R)}$ is surjective, for every $m \geq n$. Here, $E_m(R)$ denotes the group of the elementary matrices. The last section of the chapter presents the Bass' Stable Range Theorem, which claims that $\dim(j - \operatorname{Spec}(R)) + 1$ defines a stable range for $GL(R)$, where $j - \operatorname{Spec}(R)$ is a specific subset of $\operatorname{Spec}(R)$. This part of the chapter is the one in which we use the basic element theory.

Finally, chapter 5 deals with the Bourbaki's Theorem, which lies in the setting of torsion-free modules over normal domains. If M satisfies this assumption and has rank r, the theorem claims that there exists a short exact sequence

$$\begin{tikzcd} 0 \arrow[r] & R^{r-1} \arrow[r] & M \arrow[r] & I \arrow[r] & 0, \end{tikzcd}$$

with $I \subseteq R$ an ideal. The first section provides several results concerning both normal domains and torsion-free modules. The second section proves the theorem, while the third one gives a useful application of that statement in case of Gorenstein rings. The last section presents some corollaries of the Forster-Swan's Theorem, which rely on R being a Dedekind domain.

Chapter 1

Basic elements

1.1 Zariski Topology on $\operatorname{Spec}(R)$

Most of this work, excluding some preliminaries and results, is based on the notes from a course taught by C. Huneke (see [1]).

Throughout the thesis, R will denote a commutative ring with unity. Unless otherwise stated, all homomorphisms are unital. We will denote by $\operatorname{Spec}(R)$ the set of prime ideals of R, and by $\langle x_1, \dots, x_n \rangle_R \subseteq M$ the R-submodule of the R-module M generated by the elements $\{x_1, \dots, x_n\}$.

The definition of basic elements first requires the notion of basic set, which in turn relies on some concepts from the Zariski topology on $\operatorname{Spec}(R)$.

Definition 1.1.1. Let $E \subseteq R$ be a subset, we denote by

$$V(E) = \{\mathfrak{p} \in \operatorname{Spec}(R) \mid \mathfrak{p} \supseteq E\} \subseteq \operatorname{Spec}(R)$$

the set of all prime ideals that contain E.

We have that $\{V(E) \mid E \subseteq R\}$ defines a topology of closed sets on $\operatorname{Spec}(R)$, called the **Zariski topology**. This can be easily proved, for example the condition stating that the space itself must be a closed set follows from the fact that $V(0) = \operatorname{Spec}(R)$, because every prime ideal of R contains 0.
We now consider some useful properties.

Proposition 1.1.2. *Let E_1, E_2, E be subsets of R, and I_1, I_2, I ideals of R, then:*
(1) If $E_1 \subseteq E_2$, then $V(E_1) \supseteq V(E_2)$.
(2) $V(E) = V((E))$.
(3) $V(I) = V(\sqrt{I})$.
(4) If $V(I_1) \supseteq V(I_2)$, then $\sqrt{I_1} \subseteq \sqrt{I_2}$.

Proof. (1) This follows from the fact that if an ideal contains E_2, then it also contains E_1.
(2) This is also immediate, since if a prime ideal $\mathfrak{p}$ contains a set E, then, being an ideal, it also contains the ideal generated by E. The converse follows from (1), because $E \subseteq (E)$.
(3) Concerning the first inclusion, we have that $I \subseteq \sqrt{I}$, then $V(I) \supseteq V(\sqrt{I})$. For the other one, the argument is similar to the previous one, because if $\mathfrak{p} \in V(I)$, then $\mathfrak{p} \supseteq I$, but then, being $\mathfrak{p}$ a prime ideal and hence a radical one, we have that $\mathfrak{p} = \sqrt{\mathfrak{p}} \supseteq \sqrt{I}$, from which $\mathfrak{p} \in V(\sqrt{I})$.
(4) We first use the fact that $\sqrt{I_1} = \bigcap\limits_{\mathfrak{p} \supseteq I_1} \mathfrak{p}$ and $\sqrt{I_2} = \bigcap\limits_{\mathfrak{p} \supseteq I_2} \mathfrak{p}$.

Our assumptions guarantee that, for every prime ideal $\mathfrak{p}$ such that $\mathfrak{p} \supseteq I_2$, we have $\mathfrak{p} \supseteq I_1$. It follows that the first intersection, i.e. the one taken over all primes $\mathfrak{p} \supseteq I_1$, also includes those with $\mathfrak{p} \supseteq I_2$, which are further intersected with other prime ideals, so that:

$$\sqrt{I_1} = \left(\bigcap_{\mathfrak{p} \supseteq I_2} \mathfrak{p} \right) \cap (\cdots) = \sqrt{I_2} \cap (\cdots) \subseteq \sqrt{I_2}.$$

□

Therefore, the first point shows that inclusions between sets are reversed. On the other hand, (2) shows that one can always reduce to considering ideals, while by (3) we can consider only radical ideals.

The second point shows a very simple but important fact, that is the Zariski topology can be defined only using closed sets related to ideals, not necessarily to general subsets; thus a general closed set of this topology will be $V(I)$, with I an ideal of R, which can further assumed to be radical.

It is immediate to notice that if I is an ideal of R, then $V(I) \longleftrightarrow \mathrm{Spec}(R/I)$. It can also be proved that the Zariski topology is the weakest topology that makes ring homomorphism continuous.

Definition 1.1.3. A topological space X is called **Noetherian** if every descending chain of closed subsets of X stabilizes.

Proposition 1.1.4. *If Y is a Noetherian topological space and $X \subseteq Y$, then X with the subspace topology is also Noetherian.*

Proof. Let $X \cap F_1 \supseteq X \cap F_2 \supseteq \cdots$ be a descending chain of closed sets in X, so that every F_i is a closed set in Y.
We define $F'_i = \bigcap\limits_{k \leq i} F_k$, these are arbitrary intersections of closed sets in Y, which

therefore are still closed sets in Y. Compared to using F_i, we have the advantage that $F'_1 \supseteq F'_2 \supseteq \cdots$

We note that $X \cap F'_i = X \cap \left(F'_i = \bigcap_{k \leq i} F_k \right) = \bigcap_{k \leq i} (X \cap F_k) = X \cap F_i$, this because $X \cap F_1 \supseteq X \cap F_2 \supseteq \cdots \supseteq X \cap F_i \supseteq \cdots$, thus $X \cap F_i$ is in fact the smallest set in that intersection. It follows that intersecting X with F_i is the same as doing it with F'_i.

We know that Y is Noetherian, hence the descending chain consisting of the sets F'_i stabilizes at some $F'_N = F'_n$, for every $n \geq N$.

It follows that $F_N \cap X = F'_N \cap X = F'_n \cap X = F_n \cap X$, for every $n \geq N$, therefore the chain consisting of the sets $F_i \cap X$ also stabilizes.

□

Remark 1.1.5. If R is a Noetherian ring, then $\operatorname{Spec}(R)$ with the Zariski topology is Noetherian, as a topological space.

This follows immediately from the previous properties, since if

$$\operatorname{Spec}(R) \supseteq V(I_1) \supseteq V(I_2) \supseteq \cdots \supseteq V(I_n) \supseteq V(I_{n+1}) \supseteq \cdots$$

is a descending chain of closed sets of $\operatorname{Spec}(R)$, then using (4) of the previous proposition we obtain the following ascending chain of ideals of R:

$$\sqrt{(0)} \subseteq \sqrt{I_1} \subseteq \sqrt{I_2} \subseteq \cdots \subseteq \sqrt{I_n} \subseteq \sqrt{I_{n+1}} \subseteq \cdots,$$

which however must stabilize at a certain ideal $\sqrt{I_N} = \sqrt{I_{N+1}}$.

Now, using the above (3), we obtain:

$$V(I_N) = V(\sqrt{I_N}) = V(\sqrt{I_{N+1}}) = V(I_{N+1}),$$

so the chain of $V(I_k)$ also stabilizes at $V(I_N)$.

Remark 1.1.6. The converse does not hold in general. For example, let K be a field and $K[x_1, x_2, \ldots]$ the ring of polynomials in infinite variables with coefficients in K. Take $R = \dfrac{K[x_1, x_2, \ldots]}{(x_1^2, x_2^2, \ldots)}$. This is not a Noetherian ring, because the chain $(\overline{x_1}) \subsetneq (\overline{x_1}, \overline{x_2}) \subsetneq \cdots$ does not stabilize.

However $\operatorname{Spec}(R) = \{(\overline{x_1}, \overline{x_2}, \ldots)\}$, because if $\mathfrak{p}$ is a prime of R, then we have that $\mathfrak{p} = \dfrac{\mathfrak{p}'}{(x_1^2, x_2^2, \ldots)}$, with $\mathfrak{p}'$ a prime of $K[x_1, x_2, \ldots]$ containing the ideal $(x_1^2, x_2^2, \ldots)$. This implies that $\mathfrak{p}' \supseteq \sqrt{(x_1^2, x_2^2, \ldots)} = (x_1, x_2, \ldots)$, which is maximal, so $\mathfrak{p}' = (x_1, x_2, \ldots)$. Hence $\operatorname{Spec}(R)$ is Noetherian.

If $X \subseteq \mathrm{Spec}(R)$ is a subset, we can define the Zariski topology induced by $\mathrm{Spec}(R)$ on X, i.e. the topology whose closed sets will be of the form $X \cap V(I)$, with $I \subseteq R$ an ideal. Therefore, stating that X is Noetherian means that it is a subspace of $\mathrm{Spec}(R)$ whose descending chains of closed subsets stabilize.

1.2 Basic sets

Now we are ready to give the definition of basic set.

Definition 1.2.1. Let $X \subseteq \mathrm{Spec}(R)$ be a subset, equipped with the Zariski topology. We say that X is **basic** if

(i) X is Noetherian.

(ii) If Λ is an index set, such that for every $\alpha \in \Lambda$ we have $\mathfrak{p}_\alpha \in X$, and if we know that $\bigcap_{\alpha \in \Lambda} \mathfrak{p}_\alpha \in \mathrm{Spec}(R)$ is still a prime ideal, then $\bigcap_{\alpha \in \Lambda} \mathfrak{p}_\alpha \in X$.

In other words, a Noetherian subspace X of $\mathrm{Spec}(R)$ is basic if it is closed under arbitrary intersections.

Remark 1.2.2. Clearly, the intersection to consider is actually the one of the primes that are not nested, because if $\mathfrak{p} \subseteq \mathfrak{q}$, then $\mathfrak{q}$ does not contribute to the intersection. If we examine only the case in which primes are not nested, we obtain that if Λ is finite, then the intersection is never a prime ideal.

Proof. We assume that the intersection is $\mathfrak{p_1} \cap \cdots \cap \mathfrak{p_n}$. For every i, we take an element $x_i \in \mathfrak{p_i}$, such that $x_i \notin \mathfrak{p}_j$, for $j \neq i$. We can certainly find it because $\mathfrak{p_i} \nsubseteq \mathfrak{p_j}$, $\forall i \neq j$.

Let us consider the product $x = x_1 \cdot \ldots \cdot x_n \in \bigcap_i \mathfrak{p_i}$. If the previous intersection is a prime ideal, then a given x_j will be in $\bigcap_i \mathfrak{p_i}$, however this is a contradiction, because $x_j \in \mathfrak{p_j}$, but it does not lie in the other primes $\mathfrak{p_i}$.

□

We understand that the interesting case in (ii) of the definition of basic element happens when Λ is infinite.

Example 1.2.3. If R is a Noetherian ring, then $\mathrm{Spec}(R)$ is as well (refer to Remark 1.1.5), hence property (i) holds, whereas (ii) is trivially satisfied.

We conclude that $\mathrm{Spec}(R)$ is a basic set.

Example 1.2.4. If R is Noetherian, then

$$X = j - \mathrm{Spec}(R) = \left\{ \mathfrak{p} \in \mathrm{Spec}(R) \;\middle|\; \mathfrak{p} = \bigcap_{\substack{\mathfrak{p} \subseteq \mathfrak{m} \\ \mathfrak{m} \text{ maximal}}} \mathfrak{m} \right\}$$

is basic.

Thus X is the set of all the prime ideals of R which are equal to the intersection of all the maximal ideals containing them.

We immediately note that $\mathrm{Max}(R) \subseteq X$, because no maximal ideal is contained in another maximal ideal, therefore if $\mathfrak{p} = \mathfrak{m}$ is maximal, then the intersection above is indeed equal to $\mathfrak{m}$, hence $\mathfrak{m} \in X$.

Condition (i) is satisfied thanks to the previous remark, since $\mathrm{Spec}(R)$ is Noetherian. Let us check condition (ii).

Given a family of $\mathfrak{p}_\alpha \in X$, i.e. $\mathfrak{p}_\alpha = \bigcap_{\substack{\mathfrak{p}_\alpha \subseteq \mathfrak{m}_\alpha \\ \mathfrak{m}_\alpha \text{ maximal}}} \mathfrak{m}_\alpha$, for $\alpha \in \Lambda$. Also assume that $\bigcap_{\alpha \in \Lambda} \mathfrak{p}_\alpha \in \mathrm{Spec}(R)$.

Let $\mathfrak{q} = \bigcap_{\alpha \in \Lambda} \mathfrak{p}_\alpha$, our goal is to show that $\mathfrak{q} = \bigcap_{\mathfrak{q} \subseteq \mathfrak{m}} \mathfrak{m}$. Obviously $\mathfrak{q} \subseteq \mathfrak{p}_\alpha$, for every α; therefore if $\mathfrak{m}_\alpha \supseteq \mathfrak{p}_\alpha$, for some α, then $\mathfrak{m}_\alpha \supseteq \mathfrak{q}$. We then have that

$$\mathfrak{q} = \bigcap_{\alpha \in \Lambda} \left(\bigcap_{\mathfrak{p}_\alpha \subseteq \mathfrak{m}_\alpha} \mathfrak{m}_\alpha \right) \supseteq \bigcap_{\mathfrak{q} \subseteq \mathfrak{m}} \mathfrak{m} \supseteq \mathfrak{q};$$

as a consequence equality holds, hence $\mathfrak{q} \in X$.

Example 1.2.5. If R is Noetherian, then

$$X^i = \{\mathfrak{p} \in \mathrm{Spec}(R) \mid \mathrm{ht}(\mathfrak{p}) \leq i\}$$

is basic.

Again, condition (i) is trivially satisfied. Concerning (ii), if $\mathfrak{p}_\alpha \in X^i$ and $\bigcap_{\alpha \in \Lambda} \mathfrak{p}_\alpha \in \mathrm{Spec}(R)$, then from $\mathfrak{p}_\alpha \supseteq \bigcap_{\alpha \in \Lambda} \mathfrak{p}_\alpha$, we obtain:

$$i \;\geq\; \mathrm{ht}(\mathfrak{p}_\alpha) \;\geq\; \mathrm{ht}\left(\bigcap_{\alpha \in \Lambda} \mathfrak{p}_\alpha \right)$$

It follows that $\left(\bigcap_{\alpha\in\Lambda}\mathfrak{p}_\alpha\right) \in X^i$.

Proposition 1.2.6. *If X is basic and $F \subseteq \operatorname{Spec}(R)$ is closed, then $X \cap F$ is still basic.*

Proof. We know that if X is Noetherian, then $X \cap F \subseteq X$ is too.

Given $\bigcap_{\alpha\in\Lambda}\mathfrak{p}_\alpha \in \operatorname{Spec}(R)$, with every $\mathfrak{p}_\alpha \in X \cap F$, then $\bigcap_{\alpha\in\Lambda}\mathfrak{p}_\alpha \in X$, because $\mathfrak{p}_\alpha \in X$ and X is basic.

Being F a closed set, it may be written as $V(I)$, with $I \subseteq R$ an ideal. Moreover, since $\mathfrak{p}_\alpha \in F$, we have $\mathfrak{p}_\alpha \supseteq I$, for every $\alpha \in \Lambda$, consequently $\bigcap_{\alpha\in\Lambda}\mathfrak{p}_\alpha \supseteq I$, that is $\bigcap_{\alpha\in\Lambda}\mathfrak{p}_\alpha \in F$.

□

Definition 1.2.7. Let $X \subseteq \operatorname{Spec}(R)$ be a basic set and let $\mathfrak{p} \in X$ be a prime ideal. Define:

$$\dim_X \mathfrak{p} = \sup\{n \mid \exists \mathfrak{p} = \mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n,\ \text{con}\, \mathfrak{p}_i \in X,\ \forall i\}$$

Therefore, this notion of dimension is the length of the longest chain of prime ideals starting at $\mathfrak{p}$ and contained in X.

We immediately note that if $X = \operatorname{Spec}(R)$, then $\dim_X \mathfrak{p} = \dim(R/\mathfrak{p})$, that is the Krull dimension of the quotient by $\mathfrak{p}$, since chains of primes in the quotient correspond to chains of primes in R starting at $\mathfrak{p}_0 = \mathfrak{p}$.

Definition 1.2.8. A topological space Y is called **irreducible** if it cannot be written as the union of two proper closed subsets.

Proposition 1.2.9. *Let X be basic, then:*

(1) Every closed subset $F \subseteq X$ is a finite union of irreducible closed sets in X.

(2) If $F \subseteq X$ is a non empty, closed and irreducible subset, then F has a generic point in X, i.e. $F = V(\mathfrak{p}) \cap X$, for some $\mathfrak{p} \in X$.

Proof. (1) Let $F \subseteq X$ be a closed subset, if it is irreducible we are done.

If is not, then $F = F_1 \cup F_2$, with $F_i \subsetneq F$ two proper closed sets. In this case, if both F_i are irreducible we are done, otherwise assume for example that F_1 is reducible, then similarly $F_1 = F_{11} \cup F_{12}$, with $F_{1i} \subsetneq F_1$ closed sets.

If we continue with this process, at a certain point it will stop, because otherwise we would obtain a descending chain of closed sets, however X is Noetherian, so it must stabilize at a finite chain.

(2) From F being a closed set, we deduce that it is of the following form: $V(I) \cap X$, with $I \subseteq R$ an ideal. This is very close to our goal, except that we would like I to be a prime ideal. We proceed by steps.

(a) Let $\mathfrak{p}_0 = \bigcap\limits_{\mathfrak{p} \in F} \mathfrak{p}$. Let us first show that $F = V(\mathfrak{p}_0) \cap X$.

Clearly $F \subseteq V(\mathfrak{p}_0) \cap X$, because if $\mathfrak{p} \in F$, then $\mathfrak{p} \supseteq \bigcap\limits_{\mathfrak{p} \in F} \mathfrak{p} = \mathfrak{p}_0$, thus this means that $\mathfrak{p} \in V(\mathfrak{p}_0)$; moreover we already know that $F \subseteq X$, hence $\mathfrak{p} \in X$.

On the other hand $V(\mathfrak{p}_0) \subseteq V(I)$; in fact, we have that $F = V(I) \cap X$, consequently every $\mathfrak{p} \in F$ is such that $\mathfrak{p} \in V(I)$, and therefore $\mathfrak{p} \supseteq I$. It follows from this that $\mathfrak{p}_0 = \bigcap\limits_{\mathfrak{p} \in F} \mathfrak{p} \supseteq I$, from which $V(\mathfrak{p}_0) \subseteq V(I)$, by (1) of Proposition 1.1.2. It follows that $V(\mathfrak{p}_0) \cap X \subseteq V(I) \cap X = F$, hence $V(\mathfrak{p}_0) \cap X = F$.

(b) We now show that $\mathfrak{p}_0$ is a prime ideal.

By way of contradiction assume that it is not prime, then there exists a product $c \cdot d \in \mathfrak{p}_0$, con $c, d \notin \mathfrak{p}_0$. Let $F_1 = V(\mathfrak{p}_0, c) \cap X$ e $F_2 = V(\mathfrak{p}_0, d) \cap X$. Let us show that $F = F_1 \cup F_2$.

Regarding "$\supseteq$", if $\mathfrak{p} \in V(\mathfrak{p}_0, c) \cap X$, then $\mathfrak{p} \supseteq \mathfrak{p}_0 \cup (c)$, from which $\mathfrak{p} \supseteq \mathfrak{p}_0$, thus $\mathfrak{p} \in V(\mathfrak{p}_0)$. The same property holds for F_2, hence $F_1 \cup F_2 \subseteq F$, since, by (a), we have $F = V(\mathfrak{p}_0) \cap X$.

On the other hand, if $\mathfrak{p} \in F$, then $\mathfrak{p} \supseteq \mathfrak{p}_0$ and hence $c \cdot d \in \mathfrak{p}$, which is a prime ideal, therefore either $c \in \mathfrak{p}$ or $d \in \mathfrak{p}$, thus either $\mathfrak{p} \supseteq \mathfrak{p}_0 \cup (c)$ or $\mathfrak{p} \supseteq \mathfrak{p}_0 \cup (d)$, that is $\mathfrak{p} \in V(\mathfrak{p}_0, c) \cup V(\mathfrak{p}_0, d) = F_1 \cup F_2$, hence $F = F_1 \cup F_2$.

Both F_1 and F_2 are closed sets in F (which however is irreducible), so they cannot be both proper closed subsets. Assume for instance that $F_1 = F$. This is equivalent to $X \cap V(\mathfrak{p}_0) = X \cap V(\mathfrak{p}_0, c)$.

It follows that $c \in \mathfrak{p}_0$, since if $\mathfrak{p} \in F = V(\mathfrak{p}_0, c) \cap X$, then $\mathfrak{p} \in X$ and also $\mathfrak{p} \supseteq (\mathfrak{p}_0, c)$, from which we get that $c \in \mathfrak{p}$, for all $\mathfrak{p} \in F$. Consequently $c \in \bigcap\limits_{\mathfrak{p} \in F} \mathfrak{p} = \mathfrak{p}_0$, therefore $\mathfrak{p}_0$ is a prime ideal.

(c) Point (b) says that $\mathfrak{p}_0 = \bigcap\limits_{\mathfrak{p} \in F} \mathfrak{p} \in \operatorname{Spec}(R)$. Moreover, all the primes in the intersection are in F, hence in X. Since X is basic, it follows that $\mathfrak{p}_0 \in X$.

□

1.3 Basic elements

Definition 1.3.1. Let M be a finitely generated R-module, denote with $\mu_R(M)$ the minimum number of generators of M.

The definition of basic elements is closely related to this idea of minimal generators, for this reason we first give an important property concerning them. The following lemma is a consequence of Nakayama's Lemma, hence for the rest of the thesis we will refer to it as "Nakayama's Corollary".

Corollary 1.3.2 (of Nakayama). *Let $(R, \mathfrak{m}, \kappa)$ be a local ring, let M be a finitely generated R-module, the following conditions are equivalent:*

(1) $x_1, \dots, x_n$ are minimal generators of M.

(2) $\overline{x_1}, \dots, \overline{x_n} \in M/\mathfrak{m}M$ form a basis of $M/\mathfrak{m}M$ as $R/\mathfrak{m} = \kappa$-vector space.

Proof. (1) $\Rightarrow$ (2). We know that $M = \langle x_1, \dots, x_n \rangle_R$, as a consequence $M/\mathfrak{m}M = \langle \overline{x_1}, \dots, \overline{x_n} \rangle$. If by contradiction these classes were not linearly independent over κ, it would mean that one of them could be written as a combination of the other $n-1$, assume for instance $\overline{x_1} = \tilde{a}_2 \, \overline{x_2} + \dots + \tilde{a}_n \, \overline{x_n}$, with $\tilde{a}_i \in R/\mathfrak{m} = \kappa$.

It follows that $\overline{x_1 - (a_2 x_2 + \dots a_n x_n)} = \overline{0}$ in $M/\mathfrak{m}M$, thus

$$x_1 - (a_2 x_2 + \dots a_n x_n) = y \in \mathfrak{m}M.$$

Set $N = \langle x_2, \dots, x_n \rangle_R$, from which we obtain $M \subseteq N + \mathfrak{m}M$, because $x_1 = y + (a_2 x_2 + \dots + a_n x_n)$, where the first lies in $\mathfrak{m}M$ and the second in N, while the other $x_i \in N$. However, at the same time $N + \mathfrak{m}M \subseteq M$, from which it follows that they are equal. Now we can use Nakayama's Lemma and obtain $N = M$, but this is a contradiction, since $x_1, \dots, x_n$ are minimal generators of M, and now we are stating instead that we can remove one of them and the remaining $n-1$ still generate M.

(2) $\Rightarrow$ (1). Let us now assume that $\overline{x}_1, \dots, \overline{x}_n$ form a basis of $M/\mathfrak{m}M$. By way of contradiction, if $x_1, \dots, x_n$ were not minimal, we would obtain for example $x_1 = a_2 x_2 + \dots + a_n x_n$, with $a_i \in R$.

It follows that $\overline{x_1} = \tilde{a}_2 \, \overline{x_2} + \dots + \tilde{a}_n \, \overline{x_n}$, with $\tilde{a}_i \in R/\mathfrak{m}$, hence $\overline{x}_1, \dots, \overline{x}_n$ are not linearly independent, however this is a contradiction, because they are a basis.

We now prove that for every $x \in M$, $x = \sum_{i=1}^{n} a_i x_i$.

Let $x \in M$, consider $\overline{x} \in M/\mathfrak{m}M$, then $\overline{x} = \sum_{i=1}^{n} \tilde{a}_i \overline{x}_i$, with $\tilde{a}_i \in \kappa$. It follows that $x = a_1 x_1 + \dots + a_n x_n + y$, with $y \in \mathfrak{m}M$, hence:

$$M \subseteq \langle x_1, \dots, x_n \rangle_R + \mathfrak{m}M \ \subseteq \ M.$$

Using again Nakayama's Lemma, we deduce $M = \langle x_1, \dots, x_n \rangle_R$, and this concludes the proof. ☐

Given an R-module M, we now want to analyse the minimum number of generators of the various localizations of M at prime ideals $\mathfrak{p}$.

Notation. Let R be a ring and M a finitely generated R-module. Given $\mathfrak{p} \in \operatorname{Spec}(R)$, define

$$\mu_{\mathfrak{p}}(M) = \mu_{R_{\mathfrak{p}}}(M_{\mathfrak{p}}) = \dim_{\kappa(\mathfrak{p})}(M_{\mathfrak{p}}/\mathfrak{p}M_{\mathfrak{p}}).$$

Therefore this quantity is the minimum number of generators of the localization $M_{\mathfrak{p}}$ as an $R_{\mathfrak{p}}$-module, which, by Nakayama's Corollary, is equal to the dimension of the quotient $M_{\mathfrak{p}}/(\mathfrak{p}R_{\mathfrak{p}})M_{\mathfrak{p}}$ (which is the same as $M_{\mathfrak{p}}/\mathfrak{p}M_{\mathfrak{p}}$), as $\kappa(\mathfrak{p}) = (R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}})$-vector space.

Given this notation, we now see the definition of basic element.

Definition 1.3.3. Let R be a ring, $\mathfrak{p} \in \operatorname{Spec}(R)$ and M an R-module, then $x \in M$ is called a **$\mathfrak{p}$-basic element** if

$$\mu_{\mathfrak{p}}(M) > \mu_{\mathfrak{p}}(M/\langle x\rangle_R).$$

Therefore x is $\mathfrak{p}$-basic if after quotienting $M_{\mathfrak{p}}$ by the $R_{\mathfrak{p}}$-submodule generated by $x_{\mathfrak{p}}$ (meaning by the localization of x, i.e. $\frac{x}{1}$), then the minimum number of generators decreases. This means that $x_{\mathfrak{p}}$ was part of a system of minimal generators of $M_{\mathfrak{p}}$.

Definition 1.3.4. Now, if $X \subseteq \operatorname{Spec}(R)$, an element $x \in M$ is said to be X-basic if it is $\mathfrak{p}$-basic, for every $\mathfrak{p} \in X$.

We now present two lemmas concerning some properties of $\mu_{\mathfrak{p}}(M)$, which will be useful in the next chapter.

Lemma 1.3.5. *Let M a finitely generated R-module, then the set*

$$F_n = \{\mathfrak{q} \in \operatorname{Spec}(R) \mid \mu_{\mathfrak{q}}(M) \geq n\} \subseteq \operatorname{Spec}(R)$$

is closed, for every $n \in \mathbb{N}$.

Proof. The case $n = 0$ is obvious, since $\mu_{\mathfrak{q}}(M) \geq 0,\ \forall \mathfrak{q} \in \operatorname{Spec}(R)$, consequently $F_0 = \operatorname{Spec}(R)$, that is closed.

Let us now take $n \in \mathbb{N}^*$, consider the ideal

$$I_n = \sum_{x_{i_1},\dots,x_{i_{n-1}} \in M} [\langle x_{i_1}, \dots, x_{i_{n-1}}\rangle :_R M].$$

This ideal is the sum of the colon ideals of M inside any submodule generated by $n-1$ elements.

(i) Suppose now that $\mathfrak{p} \in \operatorname{Spec}(R)$ is such that $\mathfrak{p} \supseteq I_n$, we show that $\mu_{\mathfrak{p}}(M) \geq n$.

By way of contradiction, if this is false, then we know that $M_{\mathfrak{p}}$ is generated by $n-1$ elements, i.e. $M_{\mathfrak{p}} = \left\langle \frac{x_1}{s_1}, \ldots, \frac{x_{n-1}}{s_{n-1}} \right\rangle_{R_{\mathfrak{p}}}$, where $x_i \in M$ and $s_i \in S = R \setminus \mathfrak{p}$, however this is the same as taking the $R_{\mathfrak{p}}$-submodule generated by the localizations of $x_1, \ldots, x_{n-1}$, which are elements of M itself, whose submodule in $M_{\mathfrak{p}}$ we will denote by $\langle x_1, \ldots, x_{n-1} \rangle_{\mathfrak{p}} = \left\langle \frac{x_1}{1}, \ldots, \frac{x_{n-1}}{1} \right\rangle_{R_{\mathfrak{p}}} = M_{\mathfrak{p}}$.

We know from the assumptions that M is finitely generated, hence $M = \langle m_1, \ldots, m_v \rangle_R$. Since every $\frac{m_i}{1} \in \left\langle \frac{x_1}{1}, \ldots, \frac{x_{n-1}}{1} \right\rangle_{R_{\mathfrak{p}}}$, there exist an expression of the form

$$\forall i = 1, \ldots, v, \qquad \frac{m_i}{1} = \sum_{j=1}^{n-1} \left(\frac{a_j^i}{s_j^i} \cdot \frac{x_j}{1} \right).$$

Thus for every $i = 1, \ldots v$ there exists $s_i' \in R \backslash \mathfrak{p}$ such that $s_i' m_i \in \langle x_1, \ldots, x_{n-1} \rangle_R$. Setting $s = s_1' \cdot \ldots \cdot s_v' \in R \setminus \mathfrak{p}$, we get $s \cdot m_i \in \langle x_1, \ldots, x_{n-1} \rangle_R$, $\forall i = 1, \ldots, v$, hence $s \cdot M \subseteq \langle x_1, \ldots, x_{n-1} \rangle_R$.

Thus $s \in \langle x_1, \ldots, x_{n-1} \rangle :_R M$ and $s \notin \mathfrak{p}$, consequently $\langle x_1, \ldots, x_{n-1} \rangle :_R M \nsubseteq \mathfrak{p}$, and this contradicts the assumption that $I_n \subseteq \mathfrak{p}$.

Thus if $\mathfrak{p} \supseteq I_n$, then $\mu_{\mathfrak{p}}(M) \geq n$, which means that $\mathfrak{p} \in F_n$. This gives the containment $V(I_n) \subseteq F_n$.

(ii) Let us show the converse, i.e. $V(I_n) \supseteq F_n$. Suppose that $\mathfrak{p} \in \operatorname{Spec}(R)$ is such that $\mu_{\mathfrak{p}}(M) \geq n$ and suppose, for the sake of contradiction, that $\mathfrak{p} \notin V(I_n)$, that is, $\mathfrak{p} \nsupseteq I_n$.
It follows that there exist $x_1, \ldots, x_{n-1} \in M$, such that $\langle x_1, \ldots, x_{n-1} \rangle :_R M \nsubseteq \mathfrak{p}$. In particular, there exists $a \in \langle x_1, \ldots, x_{n-1} \rangle :_R M$, such that $a \notin \mathfrak{p}$.

This implies that $a \cdot M \subseteq \langle x_1, \ldots, x_{n-1} \rangle_R$, which implies, by passing to localizations, that $\frac{a}{1} \cdot M_{\mathfrak{p}} \subseteq \langle x_1, \ldots, x_{n-1} \rangle_{\mathfrak{p}}$. However, we know that $a \notin \mathfrak{p}$, therefore $\frac{a}{1}$ is a unit of $R_{\mathfrak{p}}$, and then $\frac{a}{1} \cdot M_{\mathfrak{p}} = M_{\mathfrak{p}}$. It follows that $M_{\mathfrak{p}} = \langle x_1, \ldots, x_{n-1} \rangle_{\mathfrak{p}}$, thus $\mu_{\mathfrak{p}}(M) \leq n-1$, and this is a contradiction, because $\mathfrak{p} \in F_n$.

(iii) We have concluded that $F_n = V(I_n)$, which is a closed set.

□

Lemma 1.3.6. *Let M be a finitely generated R-module and let $X \subseteq \operatorname{Spec}(R)$ be basic. Then there exists a finite set of primes $\Lambda \subseteq X$ such that, if $\mathfrak{p} \in X \setminus \Lambda$, there exists a prime ideal $\mathfrak{q} \subsetneq \mathfrak{p}$ in X such that $\mu_{\mathfrak{q}}(M) = \mu_{\mathfrak{p}}(M)$.*

The fact that Λ can be chosen to be a finite set is crucial in what follows; this set Λ, and this lemma, will be recalled several times in the rest of the thesis.

Proof. The previous lemma states that $F_n = \{\mathfrak{q} \in \operatorname{Spec}(R) \mid \mu_{\mathfrak{q}}(M) \geq n\}$ is closed in $\operatorname{Spec}(R)$. Then by (1) of Proposition 1.2.9, since $X \cap F_n$ is a closed set of X, which is basic, it can be written as a finite union of closed and irreducible sets of X.

Using this time the item (2) of the same proposition, we obtain that these closed sets can be written in the following form: $V(\mathfrak{p}) \cap X$, with $\mathfrak{p} \in X$. However, if all of these sets are contained in $X \cap F_n$, in particular this means that the prime $\mathfrak{p} \in V(\mathfrak{p}) \cap X$ also belongs to F_n. Ultimately:

$$X \cap F_n = \bigcup_{i \in \Lambda_n} V(\mathfrak{p}_{i,n}) \cap X,$$

with $\mathfrak{p}_{i,n} \in X \cap F_n$ prime ideals and Λ_n a finite set of indices. We define

$$\Lambda = \bigcup \{\mathfrak{p}_{i,n} \mid n = 0, \dots, \mu_R(M),\ i \in \Lambda_n\} \subseteq X.$$

Since $\mu_R(M)$ is finite, and each Λ_n is finite as well, we have that Λ is a finite subset of X.

Let now $\mathfrak{p} \in X \setminus \Lambda$, in order to simplify we set $n = \mu_{\mathfrak{p}}(M)$. We have that $\mathfrak{p} \in X \cap F_n$. Thus $\mathfrak{p}$ lies in some $V(\mathfrak{p}_{i,n})$ listed in the union that defines $X \cap F_n$, say $\mathfrak{p} \in V(\mathfrak{p}_{i,n})$, so that $\mathfrak{p} \supseteq \mathfrak{p}_{i,n}$. Note that $\mathfrak{p}_{i,n} \neq \mathfrak{p}$, since $\mathfrak{p}_{i,n} \in \Lambda$, while $\mathfrak{p} \notin \Lambda$.

Since $\mathfrak{p} \supseteq \mathfrak{p}_{i,n}$ we have $\mu_{\mathfrak{p}}(M) \geq \mu_{\mathfrak{p}_{i,n}}(M)$. This follows from the fact that a set of generators of M localized at $R \setminus \mathfrak{p}$ still generates after we further localize to the multiplicative closed set $R \setminus \mathfrak{p}_{i,n}$.

On the other hand, $\mathfrak{p}_{i,n} \in F_n$, hence $\mu_{\mathfrak{p}_{i,n}}(M) \geq n$; it follows that $\mu_{\mathfrak{p}_{i,n}}(M) = \mu_{\mathfrak{p}}(M)$, therefore $\mathfrak{p}_{i,n} \in \Lambda$ is the prime we were searching for.

□

Remark 1.3.7. During the proof we have also shown that if $\mathfrak{p}, \mathfrak{q}$ are two prime ideals, with $\mathfrak{p} \supseteq \mathfrak{q}$, then $\mu_{\mathfrak{p}}(M) \geq \mu_{\mathfrak{q}}(M)$. This holds because if $\{x_1, \dots, x_n\}$ generate M, then $\{\frac{x_1}{1}, \dots, \frac{x_n}{1}\}$ generate M_S, for every multiplicative set $S \subseteq M$.

Chapter 2

Eisenbud-Evans' Theorem

2.1 Preliminaries

First of all we state the Eisenbud-Evans' Theorem, later in this section we will give some definitions which will be useful for the rest of thesis, in addition to some preliminary lemmas for the proof of the theorem. The latter will be the subject of the second section, which also includes some corollaries.

Theorem 2.1.1 (Eisenbud-Evans). *Let R be a ring, M a finitely generated R-module and $X \subseteq \operatorname{Spec}(R)$ basic, assume that:*

(i) $(a, y) \in R \oplus M$ is X-basic.

(ii) For every $\mathfrak{p} \in X$, we have $\mu_{\mathfrak{p}}(M) \geq 1 + \dim_X(\mathfrak{p})$.

Then there exists $z \in M$, such that $y + a \cdot z \in M$ is X-basic.

Let us examine condition (i): $R \oplus M$ is an R-module, therefore it can be localized at the primes of $X \subseteq \operatorname{Spec}(R)$, hence if we assume that (a, y) is for instance $\mathfrak{p}$-basic, our assumption refers to $(R \oplus M)_{\mathfrak{p}}$, which is well-defined. The theorem allows us to move from a pair in $R \oplus M$ to an element of M itself, while preserving basicity.

Definition 2.1.2. Under the same assumptions, let $\mathfrak{p} \in X$ and $S \subseteq M$ be a subset, we set

$$\delta_{\mathfrak{p}}(S) = \mu_{\mathfrak{p}}(M) - \mu_{\mathfrak{p}}(M/\langle S \rangle_R).$$

The purpose of $\delta_{\mathfrak{p}}(S)$ is to measure the number of minimal generators of $M_{\mathfrak{p}}$ which lie in S: for example, if they are 2, then by quotienting by S that number will decrease by 2, and hence $\delta_{\mathfrak{p}}(S) = 2$; if instead there are not any of them, that number will be 0. We formalize this argument through the following remark.

Remark 2.1.3. Consider the following short exact sequence

$$\begin{tikzcd} 0 \arrow[r] & \langle S\rangle_R \arrow[r, "i"] & M \arrow[r, "\pi"] & M/\langle S\rangle_R \arrow[r] & 0. \end{tikzcd}$$

We now localize at $\mathfrak{p}$ and obtain a further exact sequence:

$$\begin{tikzcd} 0 \arrow[r] & \langle S\rangle_{R_\mathfrak{p}} \arrow[r] & M_\mathfrak{p} \arrow[r] & M_\mathfrak{p}/\langle S\rangle_{R_\mathfrak{p}} \arrow[r] & 0. \end{tikzcd}$$

Tensoring over $R_\mathfrak{p}$ with $\kappa(\mathfrak{p}) = R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p}$, we get the exact sequence:

$$\begin{tikzcd} \dfrac{\langle S\rangle_{R_\mathfrak{p}}}{\mathfrak{p}\langle S\rangle_{R_\mathfrak{p}}} \arrow[r, "\alpha"] & \dfrac{M_\mathfrak{p}}{\mathfrak{p}M_\mathfrak{p}} \arrow[r, "\beta"] & \dfrac{M_\mathfrak{p}}{\langle S\rangle_{R_\mathfrak{p}} + \mathfrak{p}M_\mathfrak{p}} \arrow[r] & 0. \end{tikzcd}$$

(We denote with (1) the fact that the codomain of β is in the form above, we will prove it later). Recall the Nakayama's Corollary, from which it follows that $\mu_\mathfrak{p}(M) = \mu_{R_\mathfrak{p}}(M_\mathfrak{p}) = \dim_{\kappa(\mathfrak{p})}(M_\mathfrak{p}/\mathfrak{p}M_\mathfrak{p})$.

By examining $\mu_\mathfrak{p}(M/\langle S\rangle_R)$, we obtain that it is equal to

$$\mu_{R_\mathfrak{p}}(M_\mathfrak{p}/\langle S\rangle_\mathfrak{p}) = \dim_{\kappa(\mathfrak{p})}\left(\frac{M_\mathfrak{p}}{\langle S\rangle_{R_\mathfrak{p}} + \mathfrak{p}M_\mathfrak{p}}\right),$$

thanks to (1).

Since β is surjective, we have $\dfrac{M_\mathfrak{p}}{\langle S\rangle_{R_\mathfrak{p}} + \mathfrak{p}M_\mathfrak{p}} \cong \dfrac{\frac{M_\mathfrak{p}}{\mathfrak{p}M_\mathfrak{p}}}{\ker(\beta) = \mathrm{Im}(\alpha)}$, then:

$$\dim_{\kappa(\mathfrak{p})}\left(\frac{M_\mathfrak{p}}{\langle S\rangle_{R_\mathfrak{p}} + \mathfrak{p}M_\mathfrak{p}}\right) = \dim_{\kappa(\mathfrak{p})}\left(\frac{M_\mathfrak{p}}{\mathfrak{p}M_\mathfrak{p}}\right) - \dim_{\kappa(\mathfrak{p})}(\mathrm{Im}(\alpha)).$$

We can now conclude this remark with the following result:

$$\delta_\mathfrak{p}(S) = \dim_{\kappa(\mathfrak{p})}(\mathrm{Im}(\alpha)).$$

In fact α is the map induced by the natural inclusion of $\langle S\rangle_R$ into M.

Proof. Let us prove (1).

First of all, (1) represents the following isomorphism:

$$\frac{M_\mathfrak{p}}{\langle S\rangle_{R_\mathfrak{p}}} \otimes_{R_\mathfrak{p}} \frac{R_\mathfrak{p}}{\mathfrak{p}R_\mathfrak{p}} \cong \frac{M_\mathfrak{p}}{\langle S\rangle_{R_\mathfrak{p}} + \mathfrak{p}M_\mathfrak{p}}.$$

This holds because

$$\frac{M_{\mathfrak{p}}}{\langle S\rangle_{R_{\mathfrak{p}}}}\otimes_{R_{\mathfrak{p}}}\frac{R_{\mathfrak{p}}}{\mathfrak{p}R_{\mathfrak{p}}}\cong\frac{M_{\mathfrak{p}}/\langle S\rangle_{R_{\mathfrak{p}}}}{(\mathfrak{p}R_{\mathfrak{p}})\cdot M_{\mathfrak{p}}/\langle S\rangle_{R_{\mathfrak{p}}}}\cong\frac{M_{\mathfrak{p}}/\langle S\rangle_{R_{\mathfrak{p}}}}{(\langle S\rangle_{R_{\mathfrak{p}}}+\mathfrak{p}M_{\mathfrak{p}})/\langle S\rangle_{R_{\mathfrak{p}}}}\cong\frac{M_{\mathfrak{p}}}{\langle S\rangle_{R_{\mathfrak{p}}}+\mathfrak{p}M_{\mathfrak{p}}},$$

where the last equivalence holds by the Third Isomorphism Theorem. This proves (1) and in particular the fact that the codomain of β is in the aforementioned form.

□

Remark 2.1.4. Let $X \subseteq \operatorname{Spec}(R)$ be basic and let $S \subseteq M$ be a subset, with M a finitely generated R-module. Then there exists a finite set $\Lambda' \subseteq X$, such that for every $\mathfrak{p} \in X \setminus \Lambda'$, there exists a prime ideal $\mathfrak{q} \in X$, such that $\mathfrak{q} \subsetneq \mathfrak{p}$ and $\mu_{\mathfrak{q}}(M) = \mu_{\mathfrak{p}}(M)$, and it follows that $\delta_{\mathfrak{q}}(S) \leq \delta_{\mathfrak{p}}(S)$.

Proof. Denote with $M' = \dfrac{M}{\langle S\rangle_R}$, it is still a finitely generated R-module, therefore we can apply Lemma 1.3.6 to M', and we obtain a finite set Λ', such that for all primes $\mathfrak{p} \in X \setminus \Lambda'$, there exists $\mathfrak{q} \in X$, such that $\mathfrak{q} \subsetneq \mathfrak{p}$ and $\mu_{\mathfrak{q}}(M') = \mu_{\mathfrak{p}}(M')$. Moreover, as stated in Remark 1.3.7, we have that $\mu_{\mathfrak{q}}(M) \leq \mu_{\mathfrak{p}}(M)$. It follows:

$$\delta_{\mathfrak{q}}(S) = \mu_{\mathfrak{q}}(M) - \mu_{\mathfrak{q}}(M') \ \leq\ \mu_{\mathfrak{p}}(M) - \mu_{\mathfrak{q}}(M') = \mu_{\mathfrak{p}}(M) - \mu_{\mathfrak{p}}(M') = \delta_{\mathfrak{p}}(S).$$

All of this holds for every $\mathfrak{p} \in X \setminus \Lambda'$, thus for every $\mathfrak{p} \in X$, except for a finite number of them.

□

Definition 2.1.5. Let $X \subseteq \operatorname{Spec}(R)$ be basic and let $\mathfrak{p} \in X$ be a prime ideal. A finite subset $S = \{x_1, \ldots, x_n\} \subseteq M$ is called a **$\mathfrak{p}$-basic subset** if

$$\delta_{\mathfrak{p}}(S) \geq \min\{n,\ 1 + \dim_X(\mathfrak{p})\}.$$

If S is $\mathfrak{p}$-basic for every $\mathfrak{p} \in X$, then S is X-basic.

We examine this concept first in an intuitive way and then provide more details about the case in which S is a single element. As we have stated before, the quantity $\delta_{\mathfrak{p}}(S)$ measures how many minimal generators of $M_{\mathfrak{p}}$ lie in S, therefore, if S consists of n elements, clearly this number must be less or equal than n.

Thus, the actual comparison made in this definition is with the quantity $1 + \dim_X(\mathfrak{p})$, if it is less than n, then we compare it with $\delta_{\mathfrak{p}}(S)$; if instead the minimum occurs at n, then requiring that S is basic is equivalent to requiring that $\delta_{\mathfrak{p}}(S) = n$, so that $S_{\mathfrak{p}}$ itself is part of a minimal generating set for $M_{\mathfrak{p}}$.

Remark 2.1.6. Assume that $S = \{x\}$ consists of a single element. Given $\mathfrak{p} \in X$, then:

$$S \text{ is } \mathfrak{p}\text{-basic} \iff x \text{ is } \mathfrak{p}\text{-basic}.$$

Before seeing the proof, we can understand this fact by analyzing the previous definition of $\delta_{\mathfrak{p}}(S)$: if $S = x$ is a single element, then we have by definition that $\delta_{\mathfrak{p}}(\{x\}) = \mu_{\mathfrak{p}}(M) - \mu_{\mathfrak{p}}(M/\langle x \rangle_R)$, hence we have only two cases: either $x_{\mathfrak{p}}$ was among the minimal generators of $M_{\mathfrak{p}}$, and thus the generators decrease by quotienting by $x_{\mathfrak{p}}$, i.e. $\delta_{\mathfrak{p}}(\{x\}) = 1$; or $x_{\mathfrak{p}}$ was not a minimal generator, hence $\delta_{\mathfrak{p}}(\{x\}) = 0$. The first case is the one in which x is $\mathfrak{p}$-basic.

Thus, the two definitions coincide in the case where S is a singleton. We now understand that the definition for a general S is nothing but an extension of the one for $x \in M$. Observe however that requiring that S is $\mathfrak{p}$-basic is not the same as requiring that all of its elements are $\mathfrak{p}$-basics. For example, let $M = (x) \subseteq \mathbb{R}[x, y] = R$, so M is an R-module. It is clear that both x and $2x$ are minimal generators of M, the same holds in $M_{\mathfrak{p}}$, where $\mathfrak{p} = (x)$, hence x and $2x$ are both $\mathfrak{p}$-basics. However, if we take $S = \{x, 2x\}$, then this set is not $\mathfrak{p}$-basic, because $\dim_{\mathrm{Spec}(R)}((x)) = 1$, so $\min\{n,\ 1 + \dim_{\mathrm{Spec}(R)}(\mathfrak{p})\} = 2$. However $\delta_{\mathfrak{p}}(S) = 1 < 2$, because the elements of $S_{\mathfrak{p}}$ can be written in terms of each other, so, viewed in the same system of generators of $M_{\mathfrak{p}}$, only one is necessary, the other is not.

Proof. $\Longrightarrow$. Assume that S is $\mathfrak{p}$-basic, then

$$\delta_{\mathfrak{p}}(S) \geq \min\{1,\ 1 + \dim_X(\mathfrak{p})\} = 1,$$

that is, $\mu_{\mathfrak{p}}(M) - \mu_{\mathfrak{p}}(M/\langle x \rangle_R) \geq 1$, hence $\mu_{\mathfrak{p}}(M) \geq 1 + \mu_{\mathfrak{p}}(M/\langle x \rangle_R)$, from which $\mu_{\mathfrak{p}}(M) > \mu_{\mathfrak{p}}(M/\langle x \rangle_R)$, which precisely means that x is $\mathfrak{p}$-basic.

$\Longleftarrow$. If x is $\mathfrak{p}$-basic, then $\mu_{\mathfrak{p}}(M) - \mu_{\mathfrak{p}}(M/\langle x \rangle_R) \geq 1$, i.e.

$$\delta_{\mathfrak{p}}(S) \geq 1 = \min\{1,\ 1 + \dim_X(\mathfrak{p})\},$$

thus $S = \{x\}$ is $\mathfrak{p}$-basic.

□

Remark 2.1.7. Assume that $X \subseteq \mathrm{Spec}(R)$ is basic and M satisfies condition (ii) of the Eisenbud-Evans' Theorem, i.e. we have $\mu_{\mathfrak{p}}(M) \geq 1 + \dim_X(\mathfrak{p})$, for every $\mathfrak{p} \in X$. With the previous definition in mind, this condition is very similar to the condition of S being basic. In fact, choosing S a finite set of generators of

M, then for every $\mathfrak{p} \in X$ we have that:

$$\begin{aligned}\delta_{\mathfrak{p}}(S) = \mu_{\mathfrak{p}}(M) - \mu_{\mathfrak{p}}(M/\langle S\rangle_R = M/M = 0) = \mu_{\mathfrak{p}}(M) \geq 1 + \dim_X(\mathfrak{p})\\ \geq \min\{|S|,\ 1 + \dim_X(\mathfrak{p})\}.\end{aligned}$$

From this it follows that S is X-basic. Therefore if M satisfies the assumptions of the theorem, we obtain that every system of generators of M is X-basic.

We have just examined the second condition of the theorem; now we state an important lemma which gives us more information regarding the first one.

Lemma 2.1.8. *Let $S = \{x_1, \dots, x_n\} \subseteq M$ be an X-basic subset, suppose that $(a, x_1) \in R \oplus M$ is an X-basic element, then there exist $a_1, \dots, a_{n-1} \in R$, such that:*

$$S' = \{x'_1, \dots, x'_{n-1}\} = \{x_1 + aa_1x_n,\ x_2 + a_2x_n,\ \dots,\ x_{n-1} + a_{n-1}x_n\}$$

is X-basic.

From S basic and (a, x_1) basic in $R \oplus M$, we obtain a basic set, again in M, but with one element less than S.

Proof. We claim that $\langle S\rangle_R = \langle S' \cup \{x_n\}\rangle_R$, in fact: clearly $\supseteq$ holds, because S consists of $x_1, \dots, x_n$ and the elements of S' are nothing but linear combinations of those elements. On the other hand, for every $i \neq 1$, we have the equality $x_i = [(x_i + a_ix_n) - a_ix_n] \in \langle S' \cup \{x_n\}\rangle_R$. Similarly, $x_1 \in \langle S' \cup \{x_n\}\rangle_R$.

It follows that:

$$\mu_{\mathfrak{p}}(M/\langle S\rangle_R) = \mu_{\mathfrak{p}}(M/\langle S' \cup \{x_n\}\rangle_R) \geq \mu_{\mathfrak{p}}(M/\langle S'\rangle_R) - 1,$$

where the last step holds because $\dfrac{M}{\langle S' \cup \{x_n\}\rangle_R} = \dfrac{\frac{M}{\langle S'\rangle_R}}{\langle \overline{x_n}\rangle_R}$. Therefore if $\overline{x_n}$ is not a minimal generator of $\dfrac{M}{\langle S'\rangle_R}$, then $\mu_{\mathfrak{p}}$ remains invariant under quotienting by $\overline{x_n}$; whereas in the other case it decreases by 1.

It follows that

$$\delta_{\mathfrak{p}}(S) = \mu_{\mathfrak{p}}(M) - \mu_{\mathfrak{p}}(M/\langle S\rangle_R) \leq \mu_{\mathfrak{p}}(M) - \mu_{\mathfrak{p}}(M/\langle S'\rangle_R) + 1 = \delta_{\mathfrak{p}}(S') + 1.$$

From this, we get that $\delta_{\mathfrak{p}}(S') \geq \delta_{\mathfrak{p}}(S) - 1$.

Remark 2.1.4 states that, if $\Lambda \subseteq X$ is the finite set defined in Lemma 1.3.6 and $\mathfrak{p} \in X \setminus \Lambda$, then there exists a prime ideal $\mathfrak{q} \in X$, such that $\mathfrak{q} \subsetneq \mathfrak{p}$ and $\delta_{\mathfrak{q}}(S) \leq \delta_{\mathfrak{p}}(S)$. Putting all together:

$$\delta_{\mathfrak{p}}(S') \geq \delta_{\mathfrak{p}}(S) - 1 \geq \delta_{\mathfrak{q}}(S) - 1 \geq \min\{n,\ 1 + \dim_X(\mathfrak{q})\} - 1,$$

where the last step holds because S is X-basic and $\mathfrak{q} \in X$.

(a) In general, it holds that $\min\{n,\ 1+\dim_X(\mathfrak{q})\}-1 = \min\{n-1,\ \dim_X(\mathfrak{q})\}$.

(b) We now prove that $\min\{n-1,\ \dim_X(\mathfrak{q})\} \geq \min\{n-1,\ 1+\dim_X(\mathfrak{p})\}$.

We know that $\mathfrak{q} \subsetneq \mathfrak{p}$, hence if $\mathfrak{p} \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n$ is a chain starting from $\mathfrak{p}$, then $\mathfrak{q} \subsetneq \mathfrak{p} \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n$ is a chain starting from $\mathfrak{q}$, as a consequence we have $\dim_X(\mathfrak{q}) \geq \dim_X(\mathfrak{p}) + 1$.

We obtain the same inequality involving minima.

Joining (a) and (b) to previous inequalities, we obtain:

$$\delta_{\mathfrak{p}}(S') \geq \min\{n-1,\ 1+\dim_X(\mathfrak{p})\},$$

which means that S' is $\mathfrak{p}$-basic, since S' consists of $n-1$ elements.

We have proved the thesis for all $\mathfrak{p} \in X \setminus \Lambda$, in particular for any choice of $a_1, \ldots, a_{n-1} \in R$. We now show the statement for the remaining prime ideals of $\Lambda = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$.

Assume that the last one of them, i.e. $\mathfrak{p}_r$, is minimal compared to the others, i.e. it does not contain any of the other $\mathfrak{p}_i$ (Λ is finite, so we can certainly find a minimal prime in it; it does not matter if it is not the last one, because in this case we can always reorder the indices).

We proceed by induction on r, that is, the cardinality of Λ. If $\Lambda = \emptyset$, there is nothing to prove. Let us suppose that if $|\Lambda| = r-1$, then the lemma holds, i.e. $\exists a_1, \ldots, a_{n-1} \in R$, such that S' is $\mathfrak{p}_i$-basic, for every $i = 1, \ldots, r-1$. We now construct a new set S'' and we use it as S' in the statement.

By the minimality of $\mathfrak{p}_r$, we can choose $c \in \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_{r-1}$, such that $c \notin \mathfrak{p}_r$. Recall that:

$$S' = \{x'_1, \ldots, x'_{n-1}\} = \{x_1 + aa_1x_n,\ x_2 + a_2x_n,\ \ldots,\ x_{n-1} + a_{n-1}x_n\}.$$

We set:

$$\begin{cases} x''_1 = x'_1 + acb_1 x_n = x_1 + a(cb_1 + a_1)x_n \\ x''_2 = x'_2 + cb_2 x_n = x_2 + (a_2 + cb_2)x_n \\ \vdots \\ x''_{n-1} = x'_{n-1} + cb_{n-1}x_n = x_{n-1} + (a_{n-1} + cb_{n-1})x_n, \end{cases}$$

with $b_1, \dots, b_{n-1} \in R$ coefficients to be determined. Our goal is to prove that the set $S'' = \{x''_1, \dots, x''_{n-1}\}$ is $\mathfrak{p}_i$-basic, $\forall i = 1, \dots, r$.

Let then $i \in \{1, \dots, r-1\}$, we set $M(\mathfrak{p}_i) = M \otimes_R \kappa(\mathfrak{p}_i) \cong \dfrac{M_{\mathfrak{p}_i}}{\mathfrak{p}_i M_{\mathfrak{p}_i}}$, this isomorphism holds because

$$M \otimes_R \frac{R_{\mathfrak{p}_i}}{\mathfrak{p}_i R_{\mathfrak{p}_i}} \cong M \otimes_R (R/\mathfrak{p}_i)_{\mathfrak{p}_i} \cong (M \otimes_R R/\mathfrak{p}_i)_{\mathfrak{p}_i} \cong (M/\mathfrak{p}_i M)_{\mathfrak{p}_i} \cong \frac{M_{\mathfrak{p}_i}}{\mathfrak{p}_i M_{\mathfrak{p}_i}}.$$

We know that $c \in \mathfrak{p}_i$, consequently in $M(\mathfrak{p}_i)$ we have $\overline{x''_j} = \overline{x'_j}$, for every j, since the component $cb_j x_n \in \mathfrak{p}_i M_{\mathfrak{p}_i}$.

Recall Remark 2.1.3, which stated that $\delta_{\mathfrak{p}_i}(S') = \dim_{\kappa(\mathfrak{p}_i)}(\mathrm{Im}(\alpha'))$, where $\alpha' \colon \dfrac{\langle S' \rangle_{R_{\mathfrak{p}_i}}}{\mathfrak{p}_i \langle S' \rangle_{R_{\mathfrak{p}_i}}} \longrightarrow \dfrac{M_{\mathfrak{p}_i}}{\mathfrak{p}_i M_{\mathfrak{p}_i}}$ is the map induced by the natural inclusion of $\langle S' \rangle_R$ into M.

Similarly, if we consider the map α'' induced by the inclusion of $\langle S'' \rangle_R$ into M, we have that α' and α'' have the same image, because the codomain is in both cases $M(\mathfrak{p}_i)$, where $S' = S''$. It follows that $\delta_{\mathfrak{p}_i}(S') = \delta_{\mathfrak{p}_i}(S'')$, for every $i = 1, \dots, r-1$. In particular, since S' is $\mathfrak{p}_i$-basic, also S'' is $\mathfrak{p}_i$-basic, for every $i = 1, \dots, r-1$.

It remains to choose $b_1, \dots, b_{n-1}$ to ensure that S'' is $\mathfrak{p}_r$-basic. In order to do that, we distinguish three cases.

(1) The first case is where $\overline{x'_1}, \dots, \overline{x'_{n-1}}$ are linearly independent in $M_{\mathfrak{p}_r}$. Thus, we have the following short exact sequence:

$$\begin{tikzcd} 0 \arrow[r] & \displaystyle\sum_{i=1}^{n-1} \kappa(\mathfrak{p}_r)\, \overline{x'_i} \arrow[r, "i"] & M(\mathfrak{p}_r) \arrow[r, "\pi"] & \dfrac{M(\mathfrak{p}_r)}{\displaystyle\sum_{i=1}^{n-1} \kappa(\mathfrak{p}_r)\, \overline{x'_i}} \arrow[r] & 0. \end{tikzcd}$$

Let us examine the members of this sequence. The first one is nothing but the $\kappa(\mathfrak{p}_r)$- vector space generated by $\{\overline{x'_1}, \dots, \overline{x'_{n-1}}\}$ in $M(\mathfrak{p}_r)$, hence i is its natural inclusion. Similarly the map π is the canonical projection onto the quotient.

Let us now prove that the third member is $\dfrac{M(\mathfrak{p}_r)}{\displaystyle\sum_{i=1}^{n-1} \kappa(\mathfrak{p}_r)\, \overline{x'_i}} \cong \dfrac{M}{\langle S' \rangle_R}(\mathfrak{p}_r)$. As already seen before, we have that:

$$\frac{M}{\langle S'\rangle_R} \otimes_R \kappa(\mathfrak{p}_r) \cong \frac{M_{\mathfrak{p}_r}/\langle S'\rangle_{\mathfrak{p}_r}}{\mathfrak{p}_r(M_{\mathfrak{p}_r}/\langle S'\rangle_{\mathfrak{p}_r})} \cong \frac{M_{\mathfrak{p}_r}}{\mathfrak{p}_r M_{\mathfrak{p}_r} + \langle S'\rangle_{\mathfrak{p}_r}} \cong \frac{M(\mathfrak{p}_r)}{\langle S'\rangle_{\kappa(\mathfrak{p}_r)}}.$$

This helps us to understand that the inclusion map i is nothing but the map α' above described, therefore $\delta_{\mathfrak{p}_r}(S') = \dim_{\kappa(\mathfrak{p}_r)}(\mathrm{Im}(i)) = n-1$, since $\overline{x'_j}$ are $n-1$ and are linearly independent. Then $\delta_{\mathfrak{p}_r}(S') = n-1 \geq \min\{n-1,\ 1+\dim_X(\mathfrak{p}_r)\}$.

Note that, in this case, the set S' did not require any change, since it is already $\mathfrak{p}_i$-basic, for every i, hence it is enough to set $b_1 = \ldots = b_{n-1} = 0$, so that $S' = S''$ is $\mathfrak{p}_r$-basic.

(2) Next, assume that $\overline{x'_1} = \overline{0}$ in $M(\mathfrak{p}_r)$. Since (a, x_1) is X-basic, we know that:

$$\mu_{\mathfrak{p}}(R \oplus M) = \mu_{\mathfrak{p}}\left(\frac{R \oplus M}{\langle (a, x_1)\rangle_R}\right) + 1.$$

Here the quantity $\mu_{\mathfrak{p}}(R \oplus M)$ refers to the minimum number of generators of the module $(R \oplus M)_{\mathfrak{p}} \cong (R \oplus M) \otimes_R R_{\mathfrak{p}} \cong (R \otimes_R R_{\mathfrak{p}}) \oplus (M \otimes_R R_{\mathfrak{p}}) \cong R_{\mathfrak{p}} \oplus M_{\mathfrak{p}}$, whereas $\left(\frac{R \oplus M}{\langle (a, x_1)\rangle_R}\right)_{\mathfrak{p}} \cong \frac{R_{\mathfrak{p}} \oplus M_{\mathfrak{p}}}{\langle (a, x_1)\rangle_{R_{\mathfrak{p}}}}$. All this holds for every $\mathfrak{p} \in X$.

Stating that (a, x_1) is basic implies that $\delta_{\mathfrak{p}_r}(\{(a, x_1)\}) = \dim_{\kappa(\mathfrak{p}_r)}(\mathrm{Im}(\gamma))$, where γ is the application $\gamma\colon \frac{\langle (a, x_1)\rangle_{R_{\mathfrak{p}_r}}}{\mathfrak{p}_r\langle (a, x_1)\rangle_{R_{\mathfrak{p}_r}}} \longrightarrow \frac{R_{\mathfrak{p}_r} \oplus M_{\mathfrak{p}_r}}{\mathfrak{p}_r(R_{\mathfrak{p}_r} \oplus M_{\mathfrak{p}_r})}$ induced by the natural inclusion.

If $a \in \mathfrak{p}_r$, it follows that $x_1 \in \mathfrak{p}_r M_{\mathfrak{p}_r}$, since the fact that $\overline{x'_1} = \overline{0}$ implies that $x_1 = (x'_1 - aa_1x_n) \in \mathfrak{p}_r M_{\mathfrak{p}_r}$. Therefore

$$(a, x_1) = (a, 0) + (0, x_1) \in \mathfrak{p}_r(R \oplus M)_{\mathfrak{p}_r},$$

but then $\gamma(\overline{(a, x_1)}) = \tilde{0}$, hence the dimension of $\mathrm{Im}(\gamma)$ is equal to 0, but this is a contradiction.

Therefore $a \notin \mathfrak{p}_r$. We set $b_1 = 1,\ b_2 = \ldots = b_{n-1} = 0$. As a consequence:

$$S'' = \{x'_1 + acx_n,\ x'_2,\ \ldots,\ x'_{n-1}\}.$$

The image under α'' is $\langle \overline{acx_n},\ \overline{x'_2},\ \ldots,\ \overline{x'_{n-1}}\rangle_{\kappa(\mathfrak{p}_r)}$, which denotes the $\kappa(\mathfrak{p}_r)$-vector space generated by those elements. We know that $a, c \notin \mathfrak{p}_r$, hence $a \cdot c \notin \mathfrak{p}_r$, because $\mathfrak{p}_r$ is prime, then $a \cdot c$ is a unit in $R_{\mathfrak{p}_r}$, thus its class is a unit in $\kappa(\mathfrak{p}_r)$, therefore:

$$\mathrm{Im}(\alpha'') = \langle \overline{x'_2},\ \ldots,\ \overline{x'_{n-1}},\ \overline{x_n}\rangle_{\kappa(\mathfrak{p}_r)}.$$

Using that $x_i' = x_i + a_i x_n$, we obtain:

$$\operatorname{Im}(\alpha'') = \langle \overline{x_2},\ \dots,\ \overline{x_{n-1}},\ \overline{x_n} \rangle_{\kappa(\mathfrak{p}_r)}.$$

We now note that $\overline{0} = \overline{x_1'} = \overline{x_1 + \lambda x_n}$, with $\lambda = aa_1$, it follows that $\overline{x_1} = \overline{\lambda x_n}$ in $\kappa(\mathfrak{p}_r)$, therefore:

$$\operatorname{Im}(\alpha'') = \langle \overline{x_1},\ \overline{x_2},\ \dots,\ \ \overline{x_n} \rangle_{\kappa(\mathfrak{p}_r)} = \operatorname{Im}(\alpha),$$

where α is the map induced by the natural inclusion of $\langle S \rangle_R$ into M, i.e., the map whose image has dimension equal to $\delta_{\mathfrak{p}_r}(S)$. Finally, we have

$$\delta_{\mathfrak{p}_r}(S'') = \delta_{\mathfrak{p}_r}(S) \geq \min\{n,\ 1 + \dim_X(\mathfrak{p}_r)\} \geq \min\{n-1,\ 1 + \dim_X(\mathfrak{p}_r)\},$$

hence S'' is $\mathfrak{p}_r$-basic.

(3) The third and final case is when $\overline{x_1'} \neq \overline{0}$ and $\overline{x_1'}, \dots, \overline{x_{n-1}'}$ are linearly dependent in $\kappa(\mathfrak{p}_r)$.

From linear dependence it follows that there is some i, such that $\overline{x_i'}$ can be expressed as a $\kappa(\mathfrak{p}_r)$-linear combination of the other $\overline{x_j'}$. Set $b_i = 1$ for that specific i and $b_j = 0$ for the others.

It results:

$$\begin{aligned}\operatorname{Im}(\alpha'') &= \langle \overline{x_1'},\ \dots,\ \overline{x_i' + cx_n},\ \dots,\ \overline{x_{n-1}'} \rangle_{\kappa(\mathfrak{p}_r)} \\ &= \langle \overline{x_1'},\ \dots,\ \overline{x_{i-1}'}, \overline{x_{i+1}'},\ \dots,\ \overline{x_{n-1}'},\ \overline{cx_n} \rangle_{\kappa(\mathfrak{p}_r)},\end{aligned}$$

because $\overline{x_i'}$ can be written as a linear combination of the remaining vectors.

As above, $c \notin \mathfrak{p}_r$, thus is a unit in $\kappa(\mathfrak{p}_r)$, hence the image becomes

$$\begin{aligned}\operatorname{Im}(\alpha'') &= \langle \overline{x_1'},\ \dots,\ \overline{x_{i-1}'}, \overline{x_{i+1}'},\ \dots,\ \overline{x_{n-1}'},\ \overline{x_n} \rangle_{\kappa(\mathfrak{p}_r)} \\ &= \langle \overline{x_1},\ \dots,\ \overline{x_{i-1}}, \overline{x_{i+1}},\ \dots,\ \overline{x_{n-1}},\ \overline{x_n} \rangle_{\kappa(\mathfrak{p}_r)}.\end{aligned}$$

We know that

$$\begin{aligned}\overline{x_i'} = \overline{x_i} + \overline{\lambda x_n} \in &\langle \overline{x_1'},\ \dots,\ \overline{x_{i-1}'}, \overline{x_{i+1}'},\ \dots,\ \overline{x_{n-1}'},\ \overline{x_n} \rangle_{\kappa(\mathfrak{p}_r)} \\ &= \langle \overline{x_1},\ \dots,\ \overline{x_{i-1}}, \overline{x_{i+1}},\ \dots,\ \overline{x_{n-1}},\ \overline{x_n} \rangle_{\kappa(\mathfrak{p}_r)},\end{aligned}$$

thus we also have that $\overline{x_i} \in \langle \overline{x_1},\ \dots,\ \overline{x_{i-1}}, \overline{x_{i+1}},\ \dots,\ \overline{x_{n-1}},\ \overline{x_n} \rangle_{\kappa(\mathfrak{p}_r)}$, so

$$\mathrm{Im}(\alpha'') = \langle \overline{x_1},\ \dots,\ \overline{x_i},\ \dots,\ \overline{x_n} \rangle_{\kappa(\mathfrak{p}_r)} = \mathrm{Im}(\alpha).$$

Therefore, as above, since S is X-basic, we obtain that S'' is $\mathfrak{p}_r$-basic.

□

2.2 Theorem's proof and corollaries

We are now ready to prove the Eisenbud-Evans Theorem, whose statement is briefly recalled below.

Theorem 2.2.1 (Eisenbud-Evans). *Let R be a ring, M a finitely generated R-module and $X \subseteq \mathrm{Spec}(R)$ basic, assume that:*

(i) $(a, y) \in R \oplus M$ is X-basic.

(ii) For every $\mathfrak{p} \in X$, we have $\mu_{\mathfrak{p}}(M) \geq 1 + \dim_X(\mathfrak{p})$.

Then there exists $z \in M$, such that $y + a \cdot z \in M$ is X-basic.

Proof. We complete y to a system of generators of M, say $S = \{y, x_2, \dots, x_n\}$, we call $y = x_1$. Thanks to assumption (ii), we can apply Remark 2.1.7, which implies that S is X-basic.

Using assumption (i), we apply Lemma 2.1.8, which states that there exist $a_1, \dots, a_{n-1} \in R$, such that:

$$S' = \{x'_1, \dots, x'_{n-1}\} = \{x_1 + aa_1x_n,\ x_2 + a_2x_n,\ \dots,\ x_{n-1} + a_{n-1}x_n\}$$

is X-basic. As already discussed immediately after the statement of the lemma, the cardinality of S' has decreased by one with respect to S.

Let us now take S', we want to apply again Lemma 2.1.8, hence we need that S' is X-basic (which already is), and also that $(a, x_1 + aa_1x_n) \in R \oplus M$ is X-basic. Fix $\mathfrak{p} \in X$, we know that (a, x_1) is $\mathfrak{p}$-basic, i.e. $(a, x_1) \notin \mathfrak{p}\,(R \oplus M)_{\mathfrak{p}}$, for the Nakayama's Corollary.

From $(a, x_1) \notin \mathfrak{p}\,(R \oplus M)_{\mathfrak{p}} = \mathfrak{p}(R_{\mathfrak{p}} \oplus M_{\mathfrak{p}}) = \mathfrak{p}R_{\mathfrak{p}} \oplus \mathfrak{p}M_{\mathfrak{p}}$ it follows that either $a \notin \mathfrak{p}R_{\mathfrak{p}}$, or $x_1 \notin \mathfrak{p}M_{\mathfrak{p}}$.

If $(a, x_1 + aa_1x_n)$ is not $\mathfrak{p}$-basic, then similarly we have $a \in \mathfrak{p}R_{\mathfrak{p}}$ and at the same time $(x_1 + aa_1x_n) \in \mathfrak{p}M_{\mathfrak{p}}$. If before we had $a \notin \mathfrak{p}R_{\mathfrak{p}}$, then we now have a contradiction. If instead we had $x_1 \notin \mathfrak{p}M_{\mathfrak{p}}$, then since $a \in \mathfrak{p}R_{\mathfrak{p}}$, one has $aa_1x_n \in \mathfrak{p}M_{\mathfrak{p}}$, hence $x_1 = (x_1 + aa_1x_n) - aa_1x_n$, which is the difference between elements of $\mathfrak{p}M_{\mathfrak{p}}$, thus $x_1 \in \mathfrak{p}M_{\mathfrak{p}}$, which is a contradiction. Therefore $(a, x_1 + aa_1x_n)$ is $\mathfrak{p}$-basic, for every $\mathfrak{p} \in X$.

We use again Lemma 2.1.8, so we obtain S'', which is a set with cardinality equal to $n-2$, that is still X-basic, of the form:

$$S'' = \{\, x_1 + aa_1x_n + ab_1x'_{n-1},\ x''_2,\ \dots,\ x''_{n-2} \,\}.$$

We proceed with this argument until we obtain a set consisting of a single element, which will be of the form

$$\{x_1 + az\} = \{y + az\},$$

where $z \in M$. This set is X-basic, which is equivalent to claiming that the element $y + az$ itself is X-basic, due to Remark 2.1.6 This concludes the proof.

□

Corollary 2.2.2. *Let R a ring, $X \subseteq \operatorname{Spec}(R)$ basic, M a finitely generated R-module, such that $\mu_{\mathfrak{p}}(M) \geq 1 + \dim_X(\mathfrak{p})$, for every $\mathfrak{p} \in X$. Then there exists $z \in M$ an X-basic element.*

The corollary is formulated similarly to the theorem, in fact the assumptions on M are exactly condition (ii) of the Eisenbud-Evans' result. We will recall this statement more frequently in the course of the thesis, since it allows us to obtain an X-basic element of M, without having to go through the direct sum $R \oplus M$.

Proof. Consider $(a, y) = (1, 0) \in R \oplus M$, it is X-basic, because $\dfrac{R \oplus M}{\langle (1,0) \rangle_R} \cong 0 \oplus M$, hence if $\{(1,0), (0,x_1), \dots, (0,x_n)\}$ is a minimal system of generators of $R \oplus M$, then $\{(0,x_1), \dots, (0,x_n)\}$ is a minimal system of generators in the quotient module. Under localization the same holds, thus $\mu_{\mathfrak{p}}(R \oplus M)$ decreases by 1, i.e. $(1,0)$ is $\mathfrak{p}$-basic, for every $\mathfrak{p} \in X$.

We now apply Eisenbud-Evans' Theorem, to obtain an element $z \in M$, such that $y + az = z$ is X-basic.

□

Corollary 2.2.3. *Let R a Noetherian ring of dimension d, let $I \subseteq R$ an ideal, then there exist $d+1$ elements $a_1, \dots, a_{d+1} \in I$, such that*

$$I \subseteq \sqrt{(a_1, \dots, a_{d+1})}.$$

Therefore, up to radicals, I is generated by $d+1$ elements.

Proof. Let $M = I^{\oplus(d+1)}$. It is a finitely generated R-module, because R is Noetherian, hence if $I = (f_1, \dots, f_n)$, it is enough to take

$$\{\, (f_1, 0, \dots, 0), (f_2, 0, \dots, 0), \dots, (f_n, 0, \dots, 0), (0, f_1, 0, \dots, 0), \dots \},$$

which is a system of generators for M.

Take $X = \operatorname{Supp}_R(M)$ the support of M, i.e. the set of primes $\mathfrak{p} \in \operatorname{Spec}(R)$, such that $M_\mathfrak{p} \neq 0$. Since M is finitely generated, we obtain $\operatorname{Supp}_R(M) = V(\operatorname{ann}_R(M))$, which is a closed set. We have that R is Noetherian, so $\operatorname{Spec}(R)$ is as well, thus it is basic, while X is a closed set within a basic one, hence it is basic, due to Proposition 1.2.6.

Now, let $\mathfrak{p} \in X$, the following inequalities hold

$$\mu_\mathfrak{p}(M) \overset{(1)}{\geq} (d+1)\,\mu_\mathfrak{p}(I) \overset{(2)}{\geq} d+1 \overset{(3)}{\geq} 1 + \dim_X(\mathfrak{p}).$$

(1) Upon localizing we obtain $M_\mathfrak{p} \cong \displaystyle\bigoplus_{i=1}^{d+1} I_\mathfrak{p}$, and upon taking the quotient $\dfrac{M_\mathfrak{p}}{\mathfrak{p}M_\mathfrak{p}} \cong \displaystyle\bigoplus_{i=1}^{d+1} \dfrac{I_\mathfrak{p}}{\mathfrak{p}I_\mathfrak{p}}$. These are $\kappa(\mathfrak{p})$-vector spaces, if $I = (f_1, \dots, f_{\mu_\mathfrak{p}(I)})$ minimally, then a basis of $\dfrac{I_\mathfrak{p}}{\mathfrak{p}I_\mathfrak{p}}$ is given by these generators, first localized and then taken to the quotient, while a basis for the direct sum is in the form described at the beginning of the proof, which consists of $(d+1)\,\mu_\mathfrak{p}(I)$ elements. Therefore even equality holds.

(2) We assumed that $\mathfrak{p} \in \operatorname{Supp}_R(M)$, hence $M_\mathfrak{p} \neq 0$, in particular $I_\mathfrak{p} \neq 0$, thus $\mu_\mathfrak{p}(I) = \mu_{R_\mathfrak{p}}(I_\mathfrak{p}) \geq 1$.

(3) We have $\dim_X(\mathfrak{p}) \leq \dim(R) = d$, because $\dim(R)$ is the length of the longest possible chain of primes, whereas $\dim_X(\mathfrak{p})$ is the length of the longest chain of primes starting from $\mathfrak{p}$.

As per Corollary 2.2.2 there exists $z = (a_1, \dots, a_{d+1}) \in M$, which is X-basic. We show that $I \subseteq \sqrt{(a_1, \dots, a_{d+1})}$ and we are done.

Recall that $\sqrt{(a_1, \dots, a_{d+1})} = \displaystyle\bigcap_{\mathfrak{p} \supseteq (a_1, \dots, a_{d+1})} \mathfrak{p}$, with $\mathfrak{p}$ primes. For the sake of contradiction, assume that the statement does not hold, this implies that there exists a prime ideal $\mathfrak{p} \supseteq (a_1, \dots, a_{d+1})$, such that $\mathfrak{p} \not\supseteq I$, i.e. $I \cap (R \setminus \mathfrak{p}) \neq \emptyset$, hence at least one element in I becomes a unit under localization at $\mathfrak{p}$, hence $I_\mathfrak{p} = R_\mathfrak{p}$, therefore

$$M_\mathfrak{p} \;\cong\; \bigoplus_{i=1}^{d+1} I_\mathfrak{p} \;=\; \bigoplus_{i=1}^{d+1} R_\mathfrak{p}.$$

We know that every a_i (localized) is in $\mathfrak{p}R_\mathfrak{p}$, as a consequence we have that $(a_1, \dots, a_{d+1}) \in \mathfrak{p}R_\mathfrak{p}^{d+1} \cong \mathfrak{p}M_\mathfrak{p}$, however this is a contradiction, because then $\overline{(a_1, \dots, a_{d+1})} = \overline{0}$ in $\dfrac{M_\mathfrak{p}}{\mathfrak{p}M_\mathfrak{p}}$, i.e. $(a_1, \dots, a_{d+1})$ is not basic, since it cannot be part of a minimal system of generators. $\square$

Chapter 3

Applications

3.1 Basic elements in projective modules

Recall that if R is a ring, then an R-module P is called **projective** if for every $f : M \to N$ surjective and $g : P \to N$, with M, N two R-modules and f, g two R-module homomorphisms, there exists an another R-module homomorphism $h : P \to M$, such that $g = f \circ h$. The definition can be summarized by the following commutative diagram:

$$\begin{tikzcd}
 & P \arrow[dl, dotted, "\exists h"'] \arrow[d, "g"] & \\
M \arrow[r, "f"'] & N \arrow[r] & 0.
\end{tikzcd}$$

We then examine some useful properties of projective modules.

Remark 3.1.1. If P is free then P is projective.

In fact: let $P \cong R^I$, with I a set of index, let then $\{e_i \mid i \in I\}$ a basis of P. Take two R-module homomorphisms $f : M \to N$ (surjective) and $g : P \to N$. Observe that $g(e_i) \in N$, so for every $i \in I$, there exists $x_i \in M$, such that $g(e_i) = f(x_i)$. Define $\begin{tikzcd} h : P \arrow[r] & M \\ e_i \arrow[r, mapsto] & x_i \end{tikzcd}$, then extended by linearity. It is clear that $f \circ h = g$.

Remark 3.1.2. If we have an exact sequence of R-modules

$$\begin{tikzcd}
0 \arrow[r] & N \arrow[r] & M \arrow[r, "f"] & P \arrow[r] & 0,
\end{tikzcd}$$

where P is projective, then the sequence splits. As a consequence, we have that $M \cong N \oplus P$. In fact, we have the following commutative diagram

$$\begin{tikzcd}
& P \arrow[dl, dotted, "\exists h"'] \arrow[d, "\mathrm{id}_P"] & \\
M \arrow[r, "f"'] & P \arrow[r] & 0.
\end{tikzcd}$$

This means that there exists $h : P \to M$, such that $f \circ h = \mathrm{id}_P$, i.e. the previous sequence splits.

Lemma 3.1.3. *An R-module P is projective if and only if is a direct summand of a free R-module.*

Proof. $\Leftarrow$. If P is a direct summand of a free module, there exist $i : P \to F$ and $\pi : F \to P$, such that $\pi \circ i = \mathrm{id}_P$. Let $f : M \to N$ (surjective) and $g : P \to N$, we need $h : P \to M$, such that $f \circ h = g$.

Apply Remark 3.1.1, hence F is a projective module, so we have the following commutative diagram

$$\begin{tikzcd}
& F \arrow[dl, dotted, "\exists h'"'] \arrow[d, "g \circ \pi"] & \\
M \arrow[r, "f"'] & N \arrow[r] & 0.
\end{tikzcd}$$

So we have $h' : F \to M$, such that $f \circ h' = g \circ \pi$. Let us define $h = h' \circ i : P \to M$, hence we have

$$f \circ h = f \circ h' \circ i = g \circ \pi \circ i = g \circ \mathrm{id}_P = g.$$

$\Rightarrow$. Let P be projective and $\{p_i \mid i \in I\}$ a system of generators for P, with I an index set. Take $F = R^{|I|}$ and the map $f : \begin{array}{ccc} F & \longrightarrow & P \\ e_i & \longmapsto & p_i \end{array}$, then extended by linearity (the elements e_i form a basis for F). We have that f is surjective, hence we can construct the following commutative diagram

$$\begin{tikzcd}
& P \arrow[dl, dotted, "\exists h"'] \arrow[d, "\mathrm{id}_P"] & \\
F \arrow[r, "f"'] & P \arrow[r] & 0.
\end{tikzcd}$$

The map h is such that $f \circ h = \mathrm{id}_P$, so P is a direct summand of the free module F.

□

Remark 3.1.4. If M is a finitely generated projective R-module, $\mathfrak{p} \in \operatorname{Spec}(R)$, then $M_\mathfrak{p}$ is still projective.

Proof. Let $n = \mu_R(M)$. As we have discussed before, since M is finitely generated we have the following short exact sequence

$$\begin{tikzcd}0 \arrow[r] & N = \ker(f) \arrow[r] & R^n \arrow[r, "f"] & M \arrow[r] & 0,\end{tikzcd}$$

where f is the map such that $f(e_i) = x_i$, with $x_1, \dots, x_n$ minimal generators of M. By Remark 3.1.2, we know that this sequence splits, since M is projective, so we have that $R^n \cong N \oplus M$. We now localize in $\mathfrak{p} \in \operatorname{Spec}(R)$ and we have $R^n_\mathfrak{p} \cong N_\mathfrak{p} \oplus M_\mathfrak{p}$, so $M_\mathfrak{p}$ is a direct summand of a free $R_\mathfrak{p}$-module and by Lemma 3.1.3, this implies that it is a projective $R_\mathfrak{p}$-module.

□

Lemma 3.1.5. *Assume R is Noetherian, M, N two R-modules, with M finitely generated. Then we have an isomorphism:*

$$(\operatorname{Hom}_R(M, N))_\mathfrak{p} \cong \operatorname{Hom}_{R_\mathfrak{p}}(M_\mathfrak{p}, N_\mathfrak{p}),$$

for every $\mathfrak{p} \in \operatorname{Spec}(R)$.

Proof. Take $\mathfrak{p} \in \operatorname{Spec}(R)$ and $\frac{f}{s} \in \operatorname{Hom}_R(M, N)_\mathfrak{p}$, so $f \in \operatorname{Hom}_R(M, N)$ and $s \notin \mathfrak{p}$. We map this element into the $R_\mathfrak{p}$-homomorphism

$$\begin{tikzcd}\frac{f_\mathfrak{p}}{s} : M_\mathfrak{p} \arrow[r] & N_\mathfrak{p} \\ \frac{x}{s'} \arrow[r, mapsto] & \frac{f(x)}{ss'}.\end{tikzcd}$$

This assignment is both injective and surjective. Let us prove that is injective. If $\frac{f_\mathfrak{p}}{s} = 0$, then for every $x \in M$, we have that $\frac{f_\mathfrak{p}}{s}\left(\frac{x}{1}\right) = \frac{f(x)}{s} = 0$, so there exists $s_x \notin \mathfrak{p}$, such that $f(x)s_x = 0$ in N. Take $s' = s_{x_1} \cdot \ldots \cdot s_{x_n}$, with $M = \langle x_1, \dots, x_n \rangle_R$.

It follows that $\frac{f}{s} = 0$ in $\operatorname{Hom}_R(M, N)_\mathfrak{p}$, because $\frac{f}{s} = \frac{s'f}{s's}$ in $\operatorname{Hom}_R(M, N)_\mathfrak{p}$ and $s' \cdot f = 0$ in $\operatorname{Hom}_R(M, N)$.

Let us prove the surjectivity. Take $g : M_\mathfrak{p} \to N_\mathfrak{p}$ an $R_\mathfrak{p}$-homomorphism. Assume again that $M = \langle x_1, \dots, x_n \rangle_R$, hence $M_\mathfrak{p} = \langle \frac{x_1}{1}, \dots, \frac{x_n}{1} \rangle_{R_\mathfrak{p}}$. We choose one representative element for every $g(\frac{x_i}{1})$, say $g(\frac{x_i}{1}) = \frac{n_i}{s_i}$, with every $n_i \in N$ and

$s_i \notin \mathfrak{p}$. Make the common denominator $s = s_1 \cdot \ldots \cdot s_n$ and, instead of renaming those elements, set $g(\frac{x_i}{1}) = \frac{n_i}{s}$. We define the map

$$\begin{tikzcd} f : M \arrow[r] & N \\ x_i \arrow[r, mapsto] & n_i, \end{tikzcd}$$

then extended by linearity. We want to prove that it is well-defined. We have from the assumptions that M is finitely presented, i.e. if we take the map $\varphi : R^n \to M$, sending every element of the canonical basis e_i into x_i, then its kernel is finitely generated. Suppose $K = \ker\varphi = \langle y_1, \ldots, y_m \rangle_R \subseteq R^n$; so we have that every y_i is such that $\sum_{j=1}^{n} (y_i)_j x_j = 0$.

Taken two different expressions of the same element of M, say $\sum_{j=1}^{n} r_j x_j = \sum_{j=1}^{n} r'_j x_j$, if we want to prove that f is well-defined, we had to show that $\sum_{j=1}^{n} r_j n_j = \sum_{j=1}^{n} r'_j n_j$. Since f is linear, it is enough to show that if $\sum_{j=1}^{n} r_j x_j = 0$, then $\sum_{j=1}^{n} r_j n_j = 0$.

If $\sum_{j=1}^{n} r_j x_j = 0$, then $(r_1, \ldots, r_n) \in \ker\varphi$, assume for instance that $(r_1, \ldots, r_n) = y_i$. If we localize, we obtain $\sum_{j=1}^{n} \frac{r_j x_j}{1} = 0$. Since g is well defined, this implies that $\sum_{j=1}^{n} \frac{r_j n_j}{s} = 0$, so there exists $s_i \notin \mathfrak{p}$, such that $s_i \cdot \sum_{j=1}^{n} r_j n_j = 0$. Take $s'' = s_1 \cdot \ldots \cdot s_m$, and finally take the application:

$$\begin{tikzcd} f' : M \arrow[r] & N \\ x_i \arrow[r, mapsto] & s'' n_i. \end{tikzcd}$$

The previous f was not well-defined, while f' is so, because if $\sum_{j=1}^{n} r_j x_j = 0$, for $(r_1, \ldots, r_n) = y_i$, then $f'\left(\sum_{j=1}^{n} r_j x_j\right) = s'' \cdot \sum_{j=1}^{n} r_j n_j = 0$. Since the y_i generate $\ker\varphi$, we have proved that f' is well-defined.

Finally, take $\frac{f'}{ss''} \in \mathrm{Hom}_R(M,N)_{\mathfrak{p}}$. We have that $\frac{f'}{ss''}$ is mapped into

$$\begin{tikzcd}
\frac{f'_{\mathfrak{p}}}{ss''} : M_{\mathfrak{p}} \arrow[r] & N_{\mathfrak{p}} \\
\frac{x_i}{1} \arrow[r, mapsto] & \frac{f'(x_i)}{ss''} = \frac{s''n_i}{ss''} = \frac{n_i}{s} = g\left(\frac{x_i}{1}\right),
\end{tikzcd}$$

which is exactly g. $\square$

Lemma 3.1.6. *Let R be a Noetherian ring, M a finitely generated R-module. Then M is projective if and only if it is locally free, i.e. $M_{\mathfrak{p}}$ is a free $R_{\mathfrak{p}}$-module, for every $\mathfrak{p} \in \mathrm{Spec}(R)$.*

Proof. $\Rightarrow$. By virtue of the Remark 3.1.4, it is enough to prove the statement with M a finitely generated projective module over a local Noetherian ring $(R,\mathfrak{m})$. Let $x_1,\ldots,x_n$ be minimal generators for M. Let then f be the map $f : R^n \to M$, such that $f(e_i) = x_i$, and let $N = \ker(f)$. We have the exact sequence

$$\begin{tikzcd}
0 \arrow[r] & N \arrow[r] & R^n \arrow[r, "f"] & M \arrow[r] & 0.
\end{tikzcd}$$

We can now apply the functor $- \otimes_R R/\mathfrak{m}$ to the previous sequence, which was split exact, so the new one will be also split exact:

$$\begin{tikzcd}
0 \arrow[r] & N/\mathfrak{m}N \arrow[r] & (R/\mathfrak{m})^n \arrow[r, "\overline{f}"] & M/\mathfrak{m}M \arrow[r] & 0,
\end{tikzcd}$$

where $\overline{f}(\overline{e_i}) = \overline{x_i}$. By Nakayama's Corollary, we have that $\overline{x_1},\ldots,\overline{x_n}$ form a basis for $M/\mathfrak{m}M$, since they form a system of minimal generators for M. It follows that $\overline{f}$ send a basis into a basis, so it is an isomorphism, thus $N/\mathfrak{m}N = 0$, hence $N = \mathfrak{m}N$ and, by Nakayama's Lemma we have $N = 0$. However $N = \ker(f)$, so f itself is an isomorphism, then $M \cong R^n$, so M is free.

$\Leftarrow$. Let M be locally free. We know that M is a projective module if and only if the functor $\mathrm{Hom}_R(M,-)$ is exact. Since this functor is already left exact, we only have to prove that if $A \longrightarrow B \longrightarrow 0$ is exact, then the sequence

$$\begin{tikzcd}
\mathrm{Hom}_R(M,A) \arrow[r, "f"] & \mathrm{Hom}_R(M,B) \arrow[r] & 0
\end{tikzcd}$$

is exact. Assume that is not, so the map is not surjective, so we have the exact sequence:

$$\begin{tikzcd}
\mathrm{Hom}_R(M,A) \arrow[r] & \mathrm{Hom}_R(M,B) \arrow[r] & C \arrow[r] & 0,
\end{tikzcd}$$

with $C = \mathrm{coker}(f)$. We can now localize at a prime $\mathfrak{p} \in \mathrm{Spec}(R)$, in order to obtain the exact sequence:

$$\mathrm{Hom}_R(M,A)_{\mathfrak{p}} \longrightarrow \mathrm{Hom}_R(M,B)_{\mathfrak{p}} \longrightarrow C_{\mathfrak{p}} \longrightarrow 0.$$

As we have proved in Lemma 3.1.5, we have an isomorphism $\mathrm{Hom}_R(M,A)_{\mathfrak{p}} \cong \mathrm{Hom}_{R_{\mathfrak{p}}}(M_{\mathfrak{p}}, A_{\mathfrak{p}})$, when M is a finitely generated module over a Noetherian space. We then obtain the equivalent exact sequence:

$$\mathrm{Hom}_{R_{\mathfrak{p}}}(M_{\mathfrak{p}},A_{\mathfrak{p}}) \longrightarrow \mathrm{Hom}_{R_{\mathfrak{p}}}(M_{\mathfrak{p}},B_{\mathfrak{p}}) \longrightarrow C_{\mathfrak{p}} \longrightarrow 0.$$

Notice that the functor $\mathrm{Hom}_{R_{\mathfrak{p}}}(M_{\mathfrak{p}}, -)$ is exact, because $M_{\mathfrak{p}}$ is free, hence projective. If we first localize the sequence $A \longrightarrow B \longrightarrow 0$ and then apply the functor $\mathrm{Hom}_{R_{\mathfrak{p}}}(M_{\mathfrak{p}}, -)$, we obtain the exact sequence:

$$\mathrm{Hom}_{R_{\mathfrak{p}}}(M_{\mathfrak{p}},A_{\mathfrak{p}}) \longrightarrow \mathrm{Hom}_{R_{\mathfrak{p}}}(M_{\mathfrak{p}},B_{\mathfrak{p}}) \longrightarrow 0.$$

The first map of both sequences is the same, so the second sequence implies that it is surjective, hence $C_{\mathfrak{p}} = 0$, for every prime $\mathfrak{p}$. We conclude by the local to global theorem, that $C = 0$.

□

Before dealing with basic elements in projective modules, we also discuss the notion of unimodular row, which will be useful in this chapter.

Definition 3.1.7. Let R be a ring, a row vector $(a_1, \dots, a_n)$, with $a_i \in R$, is called **unimodular row** if there exist $b_1, \dots, b_n \in R$, such that $\sum_i a_i \cdot b_i = 1$. In other words, if there exists an R-linear combination of a_i resulting in 1. Equivalently, if $(a_1, \dots, a_n) = R$, i.e. if the ideal generated by the elements composing the vector is equal to R.

Proposition 3.1.8. *If $(a_1, \dots, a_n)$ is a unimodular row, consider the following homomorphisms of R-modules:*

$$\begin{aligned} i\colon R &\longrightarrow R^n \\ 1 &\mapsto (a_1,\dots,a_n) \\ r &\mapsto (ra_1,\dots,ra_n) \end{aligned} \qquad \begin{aligned} \pi\colon R^n &\longrightarrow R \\ (x_1,\dots,x_n) &\mapsto b_1x_1+\ldots+b_nx_n, \end{aligned}$$

where $b_1, \dots, b_n$ are such that $\sum_i a_ib_i = 1$. Then $\pi \circ i = \mathrm{id}_R$ and

$$R^n = i(R) \oplus \ker(\pi) = \langle (a_1,\dots,a_n)\rangle_R \oplus \ker(\pi).$$

Proof. Let $r \in R$, then:

$$(\pi \circ i)(r) = \pi(r(a_1, \dots, a_n)) = r(a_1 b_1 + \dots + a_n b_n) = r.$$

Hence we indeed obtain $\pi \circ i = \mathrm{id}_R$.

Now, we show that $i(R) \cap \ker(\pi) = \{0\}$. By way of contradiction, if there is an element $x \in i(R) \cap \ker(\pi)$, then $x = i(r)$, with $r \in R$ and $\pi(x) = 0$. However $\pi(x) = \pi(i(r)) = \mathrm{id}_R(r) = r$, hence $r = 0$ and therefore $x = i(0) = 0$. Thus $i(R) \cap \ker(\pi) = \{0\}$, and so the above sum is a direct sum.

Let us take $m \in R^n$, we can express it as

$$m = i(\pi(m)) + (m - i(\pi(m))),$$

where the first part $i(\pi(m)) \in i(R)$, while concerning the second:

$$\pi(m - i(\pi(m))) = \pi(m) - (\pi \circ i)(\pi(m)) = \pi(m) - \mathrm{id}_R(\pi(m)) = \pi(m) - \pi(m) = 0.$$

Hence $(m - i(\pi(m))) \in \ker(\pi)$. In conclusion we obtain $R^n = i(R) \oplus \ker(\pi)$.

□

Remark 3.1.9. From the previous proposition, it follows that if $a = (a_1, \dots, a_n)$ is a unimodular row for R, then a is an element of a basis of R^n. Let us prove the converse, so

$$a \in R^n \text{ is a unimodular row for } R \iff a \text{ is an element of a basis of } R^n.$$

Proof. If $(a_1, \dots, a_n)$ is an element of a basis of R^n, say $\{a, f_2, \dots, f_n\}$, then we can express a and every f_i in terms of the canonical base $\{e_1, \dots, e_n\}$. We obtain the transition matrix from the first basis to the second, say B. The first column of B will be exactly the vector $(a_1, \dots, a_n)$. We know that B is invertible, so there exists a matrix $A \in GL_n(R)$, such that $A \cdot B = I_n$, which denotes the identity matrix of size n. The product of the first row of A and the first column of B gives:

$$b_1 a_1 + \dots b_n a_n = 1, \text{ with } b_1, \dots, b_n \in R.$$

This is the definition of a being a unimodular row for R.

□

Now, we examine what is the meaning for an element to be $\mathfrak{q}$-basic in a projective module, instead of a general one.

Remark 3.1.10. We start with the free case, hence suppose that $P = R^t$ is a finitely generated free R-module, consider $z = (z_1, \dots, z_t) \in P$. Stating that z is $\mathfrak{q}$-basic means claiming that z is a minimal generator of $P_\mathfrak{q} = (R^t)_\mathfrak{q} \cong (R_\mathfrak{q})^t$, i.e. $z \notin \mathfrak{q}R^t_\mathfrak{q} \cong (\mathfrak{q}R_\mathfrak{q})^t$. This implies that $z_i \notin \mathfrak{q}$, for some i, which is equivalent to $(z_1, \dots, z_t) \not\subseteq \mathfrak{q}$, where this time $(z_1, \dots, z_t)$ denotes the ideal generated by the various z_i in R.

So far our remark can be summarized as follows:

$$(z_1, \dots, z_t) \in R^t \text{ is } \mathfrak{q}\text{-basic} \iff (z_1, \dots, z_t) \not\subseteq \mathfrak{q}.$$

This is equivalent to claiming that the ideal $(z_1, \dots, z_t)$ localized at $\mathfrak{q}$ contains a unit, i.e. $(z_1, \dots, z_t)_\mathfrak{q} = R_\mathfrak{q}$; this means that $(z_1, \dots, z_t)_\mathfrak{q}$ is a unimodular row for $R_\mathfrak{q}$. So

$$(z_1, \dots, z_t) \in R^t \text{ is } \mathfrak{q}\text{-basic} \iff (z_1, \dots, z_t)_\mathfrak{q} \text{ is a unimodular row for } R_\mathfrak{q}.$$

By virtue of Proposition 3.1.8, and with the same notation used therein, the above argument implies that

$$R^t_\mathfrak{q} = \langle\ z\ \rangle_{R_\mathfrak{q}} \oplus \ker(\pi).$$

In addition, note that the homomorphism i defined in Proposition 3.1.8 is injective, because if $r(z_1, \dots, z_t) = 0$, then $r \cdot z_i = 0$, for every i, hence also

$$r = r \cdot \sum_i z_i b_i = \sum_i (r z_i) b_i = 0,$$

which is a contradiction, unless $r = 0$. This holds in general, with z a unimodular row for a ring R. In our setting, the map i is

$$\begin{tikzcd} i : R_\mathfrak{q} \arrow[r] & R_\mathfrak{q} \\ r \arrow[r, mapsto] & r \cdot z_\mathfrak{q} \end{tikzcd},$$

which is injective.

It follows that $\langle\ z\ \rangle_{R_\mathfrak{q}} \cong R_\mathfrak{q}$ via i, so it is a free $R_\mathfrak{q}$-module of rank 1.

Let us now examine the other member of the direct sum, i.e. $\ker(\pi)$. We know that $R^t_\mathfrak{q}$ is a free $R_\mathfrak{q}$-module generated by the t elements of the canonical basis $\{e_1, \dots, e_t\}$. Since $\ker(\pi)$ is a submodule of $R_\mathfrak{q}$, it is finitely generated as well. More specifically, if

$$\begin{tikzcd} \mathrm{pr} : R^t_\mathfrak{q} \cong R_\mathfrak{q} \oplus \ker(\pi) \arrow[r] & \ker(\pi) \\ (x, y) \arrow[r, mapsto] & y \end{tikzcd}$$

is the projection onto the second component, we obtain $\{\mathrm{pr}(e_1), \ldots, \mathrm{pr}(e_t)\}$ generates $\ker(\pi)$.

We have just proved that $\ker(\pi)$ is a finitely generated $R_{\mathfrak{q}}$-module, with $R_{\mathfrak{q}}$ a local ring. Moreover, it is a direct summand of a free module, hence it is projective. We deduce by Lemma 3.1.6 that $\ker(\pi)$ is a free $R_{\mathfrak{q}}$-module.

If we examine the ranks:

$$\mathrm{rk}_{R_{\mathfrak{q}}}(\ker(\pi)) + \mathrm{rk}_{R_{\mathfrak{q}}}(R_{\mathfrak{q}}) = \mathrm{rk}_{R_{\mathfrak{q}}}(R_{\mathfrak{q}}^t) = t,$$

thus $\mathrm{rk}_{R_{\mathfrak{q}}}(\ker(\pi)) = t-1$, i.e. $\ker(\pi) \cong R_{\mathfrak{q}}^{t-1}$. In conclusion

$$R_{\mathfrak{q}}^t \cong \langle\ z\ \rangle_{R_{\mathfrak{q}}} \oplus R_{\mathfrak{q}}^{t-1}$$

If we unify all the previous statements, we obtain:

$$z \text{ is } \mathfrak{q}\text{-basic} \iff z_{\mathfrak{q}} \text{ is an element of a basis of } R_{\mathfrak{q}}^t \iff R_{\mathfrak{q}}^t = \langle\ z\ \rangle_{R_{\mathfrak{q}}} \oplus Q,$$

with Q a free $R_{\mathfrak{q}}$-module of rank $t-1$. If z is $\mathfrak{q}$-basic, then $Q = \ker(\pi) \cong R_{\mathfrak{q}}^{t-1}$ and $\langle\ z\ \rangle_{R_{\mathfrak{q}}} \cong R_{\mathfrak{q}}$.

Remark 3.1.11. Remark 3.1.10 handles the case in which z is in a finitely generated free module. Now we examine the case in which $z \in P$, with P a finitely generated projective R-module. We have from Remark 3.1.4 that $P_{\mathfrak{q}}$ is a finitely generated free $R_{\mathfrak{q}}$-module, for every prime $\mathfrak{q}$.

Then $P_{\mathfrak{q}} \cong R_{\mathfrak{q}}^t$, for some $t \in \mathbb{N}$. Since all the previous discussion was based on the statement: $z \in P$ is $\mathfrak{q}$-basic if and only if $z_{\mathfrak{q}}$ is a unimodular row for $R_{\mathfrak{q}}$ (and this still holds, because projective modules are locally free, hence we only need P to be projective as an assumption), we obtain the same result as before, that is:

$$z \in P \text{ is } \mathfrak{q}\text{-basic} \iff z_{\mathfrak{q}} \text{ is an element of a basis of } P_{\mathfrak{q}} \iff P_{\mathfrak{q}} = \langle\ z\ \rangle_{R_{\mathfrak{q}}} \oplus Q,$$

with Q a free $R_{\mathfrak{q}}$-module of rank equal to $\mathrm{rk}(P_{\mathfrak{q}}) - 1$.

We now take a different approach: instead of fixing a prime $\mathfrak{q}$ and searching for all the elements that are $\mathfrak{q}$-basics, we fix an element $z \in P$ and search for all the prime ideals $\mathfrak{q}$, such that this z is $\mathfrak{q}$-basic. In order to do that, we introduce the following definition.

Definition 3.1.12. Given P a finitely generated projective R-module, and given $z \in P$, define

$$\mathcal{U}_z = \{\mathfrak{q} \in \operatorname{Spec}(R) \mid z \text{ is } \mathfrak{q}\text{-basic}\} \subseteq \operatorname{Spec}(R).$$

Exactly as before, we divide our discussion in two remarks, the first regarding free modules, the second projective ones.

Remark 3.1.13. Let P be a free and finitely generated R-module, i.e. $P \cong R^t$, at the beginning of Remark 3.1.10 we stated that $z = (z_1, \dots, z_t) \in R^t$ is $\mathfrak{q}$-basic if and only if $(z_1, \dots, z_t) \nsubseteq \mathfrak{q}$, therefore in this case finding $\mathcal{U}_z$ is particularly simple:

$$\mathcal{U}_z = \operatorname{Spec}(R) \setminus V((z_1, \dots, z_t)),$$

that is the set of all primes that do not contain the ideal $(z_1, \dots, z_t)$.

Before studying $\mathcal{U}_z$ in the projective case, we have to talk about the dual of a module. We recall the dual of an R-module M, denoted with M^*, defined as follows:

$$M^* = \operatorname{Hom}_R(M, R) = \{\, f : M \to R \mid f \text{ is a homomorphism of } R\text{-modules}\,\}.$$

Definition 3.1.14. Let M be a finitely generated R-module and let $z \in M$. Define

$$M^*(z) = \{f(z) \mid f \in M^*\} \subseteq R.$$

Our goal is to prove that $\mathcal{U}_z = \operatorname{Spec}(R) \setminus V(P^*(z))$, when P is finitely generated projective. In order to do that, we study the set $M^*(z)$, starting with the free case. As we will prove later, $M^*(z)$ is not only a set, but an ideal of R.

Remark 3.1.15. We study this set in the case in which $P \cong R^t$ is a finitely generated free module. In this case we have an explicit expression for the dual module P^*, in fact:

$$\operatorname{Hom}_R(R^t, R) \cong R^t.$$

One possible isomorphism takes $(f\colon R^t \to R)$ and maps it to $(f(e_1), \dots, f(e_t))$, with $\{e_1, \dots, e_t\}$ the canonical basis of R^t. The inverse function takes the element $x = (x_1, \dots, x_t) \in R^t$ and maps it to the homomorphism

$$\begin{tikzcd} f_x : R^t \arrow[r] & R , \\ e_i \arrow[r, mapsto] & x_i \end{tikzcd}$$

which then is extended by linearity. It is easy to prove that they are inverses of each other.

Now we show that, if $M \cong R^t$ is free and $z = (z_1, \dots, z_t) \in M$, then

$$M^*(z) = (z_1, \dots, z_t).$$

Proof. ($\supseteq$). First of all, $M^*(z)$ is always an ideal of R, for every module M, since if $f(z), g(z) \in M^*(z)$, then $f(z) + g(z) = (f+g)(z) \in M^*(z)$. If instead $r \in R$ and $f(z) \in M^*(z)$, then $r \cdot f(z) = (r \cdot f)(z) \in M^*(z)$.

Next, consider the component $z_i \in R$ of z, which, viewed in R^t, corresponds to the element $z_i \cdot e_i = (0, \dots, 0, \underset{(i)}{z_i}, 0, \dots, 0)$, then we can define the R-module homomorphism:

$$\begin{aligned} f^i \colon R^t &\longrightarrow R \\ e_j &\longmapsto \begin{cases} 1 & \text{if } j = i \\ 0 & \text{if } j \neq i, \end{cases} \end{aligned}$$

then extended by linearity. We obtain $f^i \in P^*(z)$, moreover:

$$f^i(z) = f^i\left(\sum_{k=1}^{t} z_k e_k\right) = z_i.$$

Therefore we have proved that $z_i \in P^*(z)$, for every $i = 1, \dots, t$, hence $\{z_1, \dots, z_t\} \subseteq P^*(z)$, however we have that $P^*(z)$ is an ideal, so it follows that $(z_1, \dots, z_t) \subseteq P^*(z)$.

($\subseteq$). Given an element $f(z) \in P^*(z)$, then

$$f(z) = f\left(\sum_{k=1}^{t} z_k e_k\right) = \left[\sum_{k=1}^{t} z_k f(e_k)\right] \in (z_1, \dots, z_t).$$

□

We have understood that, in the free case, given $z = (z_1, \dots, z_t) \in R^t \cong P$, the following equality holds

$$\mathcal{U}_z = \mathrm{Spec}(R) \setminus V(P^*(z)) = \mathrm{Spec}(R) \setminus V((z_1, \dots, z_t)),$$

and the reason is that $P^*(z) = (z_1, \dots, z_t)$.

Remark 3.1.16. We now prove that if P is a finitely generated projective module, given $z \in P$, we have

$$\mathcal{U}_z = \operatorname{Spec}(R) \setminus V(P^*(z)).$$

Proof. Assume R Noetherian, then Lemma 3.1.5 holds, because P is finitely generated, as R-module. Consequently, given $\mathfrak{q} \in \operatorname{Spec}(R)$, we have:

$$(\operatorname{Hom}_R(P, R))_{\mathfrak{q}} \cong \operatorname{Hom}_{R_{\mathfrak{q}}}(P_{\mathfrak{q}}, R_{\mathfrak{q}}).$$

Using again Remark 3.1.10, adjusted to P projective via Remark 3.1.11, we have that z is $\mathfrak{q}$-basic if and only if $z_{\mathfrak{q}}$ is a unimodular row for $R_{\mathfrak{q}}$, i.e. if $(z_1, \dots, z_t)_{\mathfrak{q}} = R_{\mathfrak{q}}$, in other words, if $1 \in (z_1, \dots, z_t)_{\mathfrak{q}}$. Here we denote with $z_{\mathfrak{q}} = (z_1, \dots, z_t) \in R_{\mathfrak{q}}^t$ and with $(z_1, \dots, z_t)_{\mathfrak{q}} \subseteq R_{\mathfrak{q}}$ the ideal generated by $z_1, \dots, z_t$ in $R_{\mathfrak{q}}$. However, we have previously shown that, in the free case (which is the case for $P_{\mathfrak{q}}$) we have $(z_1, \dots, z_t)_{\mathfrak{q}} = P_{\mathfrak{q}}^*(z_{\mathfrak{q}})$. Combining everything:

$$z \text{ is } \mathfrak{q}\text{-basic} \iff 1 \in P_{\mathfrak{q}}^*(z_{\mathfrak{q}}) \overset{(1)}{\iff} 1 \in (P^*(z))_{\mathfrak{q}} \iff P^*(z) \not\subseteq \mathfrak{q}.$$

It follows that $\mathcal{U}_z = \operatorname{Spec}(R) \setminus V(P^*(z))$. If we prove (1) we are done.

(1) Consider the evaluation map at z:

$$\begin{aligned} \operatorname{ev}_z : \operatorname{Hom}_R(P, R) &\longrightarrow R \\ f &\longmapsto f(z). \end{aligned}$$

We observe that $P^*(z) = \operatorname{Im}(ev_z)$. Now we localize this map, obtaining the new map:

$$\begin{aligned} (\operatorname{ev}_z)_{\mathfrak{q}} : (\operatorname{Hom}_R(P, R))_{\mathfrak{q}} &\longrightarrow R_{\mathfrak{q}} \\ \frac{g}{s} &\longmapsto \frac{ev_z(g)}{s} = \frac{g(z)}{s}. \end{aligned}$$

Consider now the map

$$\begin{aligned} \operatorname{ev}_{z_{\mathfrak{q}}} : \operatorname{Hom}_{R_{\mathfrak{q}}}(P_{\mathfrak{q}}, R_{\mathfrak{q}}) &\longrightarrow R_{\mathfrak{q}} \\ f &\longmapsto f(z_{\mathfrak{q}}). \end{aligned}$$

The following diagram commutes

$$\begin{tikzcd}
(\operatorname{Hom}_R(P, R))_{\mathfrak{q}} \arrow[r, "(\operatorname{ev}_z)_{\mathfrak{q}}"] \arrow[d, "\varphi"'] & R_{\mathfrak{q}} \arrow[d, equal] \\
\operatorname{Hom}_{R_{\mathfrak{q}}}(P_{\mathfrak{q}}, R_{\mathfrak{q}}) \arrow[r, "\operatorname{ev}_{z_{\mathfrak{q}}}"'] & R_{\mathfrak{q}},
\end{tikzcd}$$

where the map φ is the isomorphism mentioned earlier, that takes $\dfrac{g}{s} \in (\mathrm{Hom}_R(P,R))_{\mathfrak{q}}$ and maps it to the homomorphism $f\colon \dfrac{m}{t} \mapsto \dfrac{g(m)}{st}$ in $\mathrm{Hom}_{R_{\mathfrak{q}}}(P_{\mathfrak{q}}, R_{\mathfrak{q}})$. This diagram commutes since, if we take $\dfrac{g}{s} \in (\mathrm{Hom}_R(P,R))_{\mathfrak{q}}$ and then apply $(\mathrm{ev}_z)_{\mathfrak{q}}$, we obtain $\dfrac{g(z)}{s}$, while if we apply φ and evaluate the resulting f at $z_{\mathfrak{q}}$, we obtain $f(z_{\mathfrak{q}}) = f\left(\dfrac{z}{1}\right) = \dfrac{g(z)}{1 \cdot s}$, which is the same as before. We conclude that $(\mathrm{ev}_z)_{\mathfrak{q}} = \mathrm{ev}_{z_{\mathfrak{q}}} \circ \varphi$, from which:

$$P_{\mathfrak{q}}^*(z_{\mathfrak{q}}) = \mathrm{Im}(\mathrm{ev}_{z_{\mathfrak{q}}}) \cong \mathrm{Im}((\mathrm{ev}_z)_{\mathfrak{q}}) = (P^*(z))_{\mathfrak{q}},$$

and (1) follows.

□

We are now ready to state an important corollary of the Eisenbud-Evans' Theorem from the previous chapter, namely Serre's Theorem. Before doing that, recall that

$$j - \mathrm{Spec}(R) = \left\{ \mathfrak{p} \in \mathrm{Spec}(R) \;\middle|\; \mathfrak{p} = \bigcap_{\substack{\mathfrak{p} \subseteq \mathfrak{m} \\ \mathfrak{m} \text{ maximal}}} \mathfrak{m} \right\},$$

which is a basic set. We then notice that, if P is a projective module, then $P_{\mathfrak{q}}$ is free, for every prime $\mathfrak{q}$, so is well-defined $\mathrm{rk}(P_{\mathfrak{q}})$.

Theorem 3.1.17 (Serre's Theorem)**.** *Let R be a Noetherian ring, $X = j - \mathrm{Spec}(R)$ and $d = \dim(X)$. Let P a finitely generated projective R-module, with $\mathrm{rk}_{R_{\mathfrak{m}}}(P_{\mathfrak{m}}) > d$, for every $\mathfrak{m} \in \mathrm{Max}(R)$. Then*

$$P \cong R \oplus Q,$$

with Q a finitely generated R-module.

Proof. First of all, note that in the case of a free module, the minimum number of generators coincides with the cardinality of a basis (i.e. the rank of the module). In fact, if $M = R^t$ is free, we know that $\mu_R(M) \leq \mathrm{rk}(M)$, since a basis (with cardinality t) is in particular a system of generators. Assume by contradiction that $\mu_R(M) < t$. Consider $R^t/\mathfrak{m}R^t \cong (R/\mathfrak{m})^t$, with $\mathfrak{m} \in \mathrm{Max}(R)$; this is an $(R/\mathfrak{m})$-vector space, with dimension t. However, if S is a minimal system of generators of M, with cardinality $t-1$, we have that $S/\mathfrak{m}$ is still a system of generators of $(R/\mathfrak{m})^t$. This is a contradiction, since we know that for vector spaces it cannot exists a system of generators with cardinality less than the dimension.

The dimension of $j-\operatorname{Spec}(R)$ is defined as the length of the longest chain of primes inside $j-\operatorname{Spec}(R)$.

Given $\mathfrak{q} \in X$, then, for every $\mathfrak{m} \in \operatorname{Max}(R),$ such that $\mathfrak{q} \subseteq \mathfrak{m}$, we have:

$$\mu_{\mathfrak{q}}(P) = \mu_{R_{\mathfrak{q}}}(P_{\mathfrak{q}}) \overset{(1)}{=} \operatorname{rk}(P_{\mathfrak{q}}) \overset{(2)}{=} \operatorname{rk}(P_{\mathfrak{m}}) \geq d+1 \overset{(3)}{\geq} \dim_X(\mathfrak{q})+1.$$

We have that (1) follows from the fact that $P_{\mathfrak{q}}$ is free and from what stated above. While (2) holds because $\mathfrak{q} \subseteq \mathfrak{m}$, hence we can consider $P_{\mathfrak{q}}$ as $(P_{\mathfrak{m}})_{\mathfrak{q}}$, but then, since $P_{\mathfrak{m}}$ is free, it follows that $P_{\mathfrak{m}} \cong R_{\mathfrak{m}}^t$, thus $P_{\mathfrak{q}} = (P_{\mathfrak{m}})_{\mathfrak{q}} \cong (R_{\mathfrak{m}})_{\mathfrak{q}}^t = R_{\mathfrak{q}}^t$. Finally, (3) holds because d is the length of the longest chain of primes inside X, while $\dim_X(\mathfrak{q})$ is the length of the longest chain inside X starting from $\mathfrak{q}$.

We are under the assumptions of Corollary 2.2.2, so we obtain an element $z \in P$ that is X-basic. This means that for every $\mathfrak{q} \in X$, we have that $\mathfrak{q} \in \mathcal{U}_z = \operatorname{Spec}(R) \setminus V(P^*(z))$, but we can observe that every maximal ideal $\mathfrak{m} \in X$, because $\mathfrak{m} = \bigcap_{\mathfrak{m}' \supseteq \mathfrak{m}} \mathfrak{m}'$, being $\mathfrak{m}$ itself the only $\mathfrak{m}' \supseteq \mathfrak{m}$, since it is maximal. It follows that $\mathfrak{m} \notin V(P^*(z))$, for every $\mathfrak{m}$ maximal ideal of R, i.e. $P^*(z)$ is not contained in any maximal ideal of R, and this necessarily implies that $P^*(z) = R$.

This means that there exists $f\colon P \to R$, such that $f(z) = 1$. Consider now the map

$$\begin{tikzcd} g : R \arrow[r] & P \\ 1 \arrow[r, mapsto] & z, \end{tikzcd}$$

then extended by linearity. We clearly have that $f \circ g = \mathrm{id}_R$, because $(f \circ g)(1) = f(z) = 1$.

By the same argument as in the Proposition 3.1.8, we conclude that $P = g(R) \oplus \ker(f)$.

Being g injective and having $\operatorname{Im}(g) = \langle\ z\ \rangle_R \cong R$, we conclude that

$$P = \langle\ z\ \rangle_R \oplus \ker(f) \cong R \oplus Q,$$

where we set $Q = \ker(f)$.

□

3.2 Bass' Cancellation Theorem

We briefly recall the following definition: let $X \subseteq \operatorname{Spec}(R)$ be basic and let $\mathfrak{p} \in X$ be a prime ideal. A finite subset $S = \{x_1, \dots, x_n\} \subseteq M$ is a $\mathfrak{p}$-basic subset if

$$\delta_{\mathfrak{p}}(S) \geq \min\{n,\ 1 + \dim_X(\mathfrak{p})\},$$

where $\delta_{\mathfrak{p}}(S) = \mu_{\mathfrak{p}}(M) - \mu_{\mathfrak{p}}(M/\langle S \rangle_R)$.

Theorem 3.2.1 (Bass' Cancellation Theorem)**.** *Let R be a Noetherian ring, $X = j - \operatorname{Spec}(R)$ (which is basic), let $d = \dim(X)$. Let then M, P, Q be finitely generated R-modules, with P and Q projective modules. Assume that $\mu_{\mathfrak{q}}(P) = \operatorname{rk}(P_{\mathfrak{q}}) \geq d + 1$, for every $\mathfrak{q} \in X$, then:*

$$Q \oplus P \cong Q \oplus M \ \Rightarrow\ P \cong M.$$

This result would be immediate if all modules were free, but the theorem states a stronger version of it, extending it to projective modules, even when one of them is just finitely generated. Although this theorem does not appear to be related to the basic element theory, we will make a large use of it, as we will see during the proof.

Proof. We start by proving some preliminaries.

(A) The direct sum of projective modules is still a projective module. We show this using the definition. Consider the following diagram:

$$\begin{tikzcd}
 & P_1 \oplus P_2 \arrow[d, "g"] & \\
M \arrow[r, "f"] & N \arrow[r] & 0.
\end{tikzcd}$$

We can then consider the inclusions

$$\begin{aligned} i_1 : P_1 &\longrightarrow P_1 \oplus P_2 & \qquad i_2 : P_2 &\longrightarrow P_1 \oplus P_2 \\ x &\longmapsto (x, 0) & y &\longmapsto (0, y). \end{aligned}$$

Every P_j is projective, hence we have

$$\begin{tikzcd}
 & P_j \arrow[dl, dashed, "\exists h_j"'] \arrow[d, "g \circ i_j"] & \\
M \arrow[r, "f"] & N \arrow[r] & 0,
\end{tikzcd}$$

where the triangle commutes, i.e. $f \circ h_1 = g \circ i_1$ and $f \circ h_2 = g \circ i_2$. We then define:

$$\begin{aligned} h = h_1 \oplus h_2 : P_1 \oplus P_2 &\longrightarrow N \\ (x, y) &\longmapsto h_1(x) + h_2(y). \end{aligned}$$

We prove that $f \circ h = g$. Let $(x, y) \in P_1 \oplus P_2$, then:

$$\begin{aligned} f(h)((x, y)) &= f(h_1(x) + h_2(y)) = f(h_1(x)) + f(h_2(y)) \\ &= (g \circ i_1)(x) + (g \circ i_2)(y) = g((x, 0)) + g((0, y)) = g(x, y). \end{aligned}$$

Therefore, under our assumptions, we have that $P \oplus Q$ is projective, i.e. there exist a free R-module F and an R-module N, such that:

$$F \cong N \oplus P \oplus Q \cong N \oplus P \oplus M.$$

Then, also M is a direct summand of a free module, consequently it is projective.

(B) Since Q is projective, there exists a finitely generated projective R-module Q', such that $Q \oplus Q' \cong R^n$, for some $n \in \mathbb{N}$. It follows that:

$$Q \oplus M \cong Q \oplus P \Rightarrow Q' \oplus Q \oplus M \cong Q' \oplus Q \oplus P \Rightarrow R^n \oplus M \cong R^n \oplus P.$$

(C) Therefore, if we prove the following version of the theorem:

$$R^n \oplus M \cong R^n \oplus P, \text{for some } n \in \mathbb{N} \;\Rightarrow\; M \cong P$$

we are done, because thanks to (B), from the starting assumption of the theorem, i.e. $Q \oplus M \cong Q \oplus P$, we deduce that $R^n \oplus M \cong R^n \oplus P$.

We proceed by induction on n.

If $n = 0$ we are done, since the assumption becomes $M \cong P$.

If $n = 1$, we have to prove that from $R \oplus M \cong R \oplus P$ it follows $M \cong P$. We will discuss this case later.

It remains to prove the inductive step. We temporarily assume the cases $n = 1$ and $n - 1$ as true, then we have $R^n \oplus M \cong R^n \oplus P$, from this it follows:

$$R^{n-1} \oplus (R \oplus M) \cong R^{n-1} \oplus (R \oplus P)$$

We notice that $R \oplus M$ is still finitely generated, as well as $R \oplus P$, moreover $(R \oplus P)_{\mathfrak{q}} \cong R_{\mathfrak{q}} \oplus P_{\mathfrak{q}}$, hence if $t = \mu_{\mathfrak{q}}(P) = \operatorname{rk}(P_{\mathfrak{q}})$, it follows that $R_{\mathfrak{q}} \oplus P_{\mathfrak{q}} \cong R_{\mathfrak{q}} \oplus R_{\mathfrak{q}}^t \cong R_{\mathfrak{q}}^{t+1}$, i.e. $\operatorname{rk}((R \oplus P)_{\mathfrak{q}}) = t + 1 > \operatorname{rk}(P_{\mathfrak{q}}) \geq d + 1$. Finally, R, P being projective implies that $R \oplus P$ is projective. The same holds for R and M, thus we can apply the inductive hypothesis:

$$R^{n-1} \oplus (R \oplus M) \cong R^{n-1} \oplus (R \oplus P) \Rightarrow R \oplus M \cong R \oplus P,$$

which implies that $M \cong P$ thanks to the case $n = 1$. In order to conclude the proof we now show the case $n = 1$.

(D) Assume that $R \oplus M \cong R \oplus P$, we distinguish two cases.

(D1) Denote with α the given isomorphism $R \oplus M \xrightarrow{\sim} R \oplus P$. In this first case, we assume that $\alpha((1, 0)) = (1, 0)$. We then define the function $g = \mathrm{pr}_P \circ \alpha \circ i_M$

$$\begin{tikzcd}
g = \mathrm{pr}_P \circ \alpha \circ i_M : M \arrow[r, "i_M"] & R \oplus M \arrow[r, "\alpha"] & R \oplus P \arrow[r, "\mathrm{pr}_P"] & P \\
x \arrow[r, mapsto] & (0, x) \arrow[r, mapsto] & \alpha((0, x)) = (\alpha_{1,x}, \alpha_{2,x}) \arrow[r, mapsto] & \alpha_{2,x}.
\end{tikzcd}$$

We show that g is an isomorphism.

Let us begin with proving that g is injective. Let $\alpha_{2,x} = 0$, then it follows

$$\alpha((0, x)) = (\alpha_{1,x}, 0) = \alpha_{1,x} \cdot (1, 0) = \alpha_{1,x} \cdot \alpha((1, 0)) = \alpha((\alpha_{1,x}, 0)),$$

thus we have $\alpha((0, x)) = \alpha((\alpha_{1,x}, 0))$, so, being α injective, we get $(0, x) = (\alpha_{1,x}, 0)$, so that $x = 0$.

We now show that g is also surjective. Let $y \in P$, all its preimages via pr_P are of the form (r, y). Let us try to obtain the element $(0, y) \in R \oplus P$ as a preimage via $\alpha \circ i_M$. We know that α is surjective, so there exists $(s, x) \in R \oplus M$, such that $\alpha((s, x)) = (0, y)$. We have that

$$\alpha((s, x)) = \alpha(s(1, 0) + (0, x)) = s(1, 0) + \alpha((0, x)) = (s, 0) + \alpha((0, x)) = (0, y),$$

therefore $\alpha((0, x)) = (0, y) - (s, 0) = (-s, y)$. Then

$$g : x \mapsto (0, x) \mapsto \alpha((0, x)) = (-s, y) \mapsto y,$$

hence $g(x) = y$. Finally, we obtain $M \overset{g}{\cong} P$.

(D2) In the general case, we have $\alpha((1, 0)) = (a, x_1)$, with $a \in R$ and $x_1 \in P$. We want to reduce to (D1). In order to do so, we consider the following sequence of homomorphisms

$$\begin{tikzcd}
R \oplus M \arrow[r, "\alpha"] & R \oplus P \arrow[r, "\beta"] & R \oplus P \arrow[r, "\gamma"] & R \oplus P \arrow[r, "\eta"] & R \oplus P \\
(1, 0) \arrow[r, mapsto] & (a, x_1) \arrow[r, mapsto] & \cdots \arrow[r, mapsto] & (1, z) \arrow[r, mapsto] & (1, 0),
\end{tikzcd}$$

where β, γ, η are isomorphisms to be specified later, so we obtain an isomorphism

$h\colon R\oplus M \longrightarrow R\oplus P$, such that $h((1,0)) = (1,0)$, and then, proceeding as in the case (D1), we conclude $M \cong P$.

The element $(1,0) \in R \oplus M$ is always basic, α is an isomorphism and $\alpha((1,0)) = (a, x_1)$, so (a, x_1) is a basic element of $R \oplus P$. This holds because $(1,0)$ being basic implies that $(1,0) \notin \mathfrak{q}(R\oplus M)_{\mathfrak{q}}$, therefore $\alpha((1,0)) \notin \mathfrak{q}(R\oplus P)_{\mathfrak{q}}$, since α is an isomorphism.
Let $P = \langle x_1, \dots, x_n\rangle_R$ and let $\mathfrak{q} \in X$. We have:

$$\mathrm{rk}_{R_{\mathfrak{q}}}(P_{\mathfrak{q}}) = \mu_{\mathfrak{q}}(P) \geq d+1 \geq \dim_X(\mathfrak{q}) + 1, \ \forall \mathfrak{q} \in X.$$

We are under the assumptions of Eisenbud-Evans' Theorem, so there exists $z = x_1 + ax \in P$, which is X-basic. We write $x = \sum_{i=1}^{n} r_i x_i$ and define

$$\begin{tikzcd} f : R \arrow[r] & P \\ 1 \arrow[r, mapsto] & x, \end{tikzcd}$$

which is a R-module homomorphism. We then set $\beta\colon R\oplus P \longrightarrow R\oplus P$ the map defined by the matrix

$$\begin{pmatrix} 1_R & 0 \\ f & 1_P \end{pmatrix}$$

and this is an isomorphism, because $\det(\beta) = 1$. We notice that:

$$\beta(\alpha((1,0))) = \begin{pmatrix} 1_R & 0 \\ f & 1_P \end{pmatrix} \cdot \begin{pmatrix} a \\ x_1 \end{pmatrix} = \begin{pmatrix} a \\ f(a) + x_1 \end{pmatrix} = \begin{pmatrix} a \\ ax + x_1 \end{pmatrix} = (a, z),$$

hence $\beta(\alpha((1,0))) = (a, z)$. As seen in the proof of Serre's Theorem, we have that $z \in P$ being basic implies that $P^*(z)$ is not contained in any maximal ideal. It follows that $P^*(z) = R$, so $1 - a \in R = P^*(z)$, therefore there exists $\varphi\colon P \longrightarrow R$, such that $\varphi(z) = 1 - a$. We define the R-module homomorphism $\gamma\colon R\oplus P \longrightarrow R\oplus P$ as the map given by the matrix:

$$\begin{pmatrix} 1_R & \varphi \\ 0 & 1_P \end{pmatrix},$$

which is an isomorphism, since the determinant is again equal to 1. We then notice that

$$\gamma(\beta(\alpha((1,0)))) = \gamma((a,z)) = \begin{pmatrix} 1_R & \varphi \\ 0 & 1_P \end{pmatrix} \cdot \begin{pmatrix} a \\ z \end{pmatrix} = \begin{pmatrix} a + \varphi(z) \\ z \end{pmatrix} = (1, z)$$

Finally, let

$$\begin{tikzcd} g : R \arrow[r] & P \\ 1 \arrow[r, mapsto] & z, \end{tikzcd}$$

we define $\eta\colon R\oplus P \longrightarrow R\oplus P$ as the map represented by the matrix $\begin{pmatrix} 1_R & 0 \\ -g & 1_P \end{pmatrix}$, that is an isomorphism, for the same reason as before. We have:

$$\eta(\gamma(\beta(\alpha((1,0)))) = \eta((1,z)) = \begin{pmatrix} 1_R & 0 \\ -g & 1_P \end{pmatrix} \cdot \begin{pmatrix} 1 \\ z \end{pmatrix} = \begin{pmatrix} 1 \\ -g(1)+z \end{pmatrix} = (1,0)$$

and this concludes the proof.

□

3.3 Forster-Swan's Theorem

The Forster-Swan's Theorem is an application of the basic element theory that allows us to transfer information regarding the minimal number of generators in the localizations of M, to information regarding the minimal number of generators of M itself. We already know that if $\mu_R(M) = t$, then for every $\mathfrak{p} \in \operatorname{Spec}(R)$, we have that $\mu_{\mathfrak{p}}(M) \leq t$, because the t generators of M, when localized, still generate the localization $M_{\mathfrak{p}}$. The Forster-Swan's Theorem gives us an opposite upper bound.

Theorem 3.3.1 (Forster-Swan's Theorem)**.** *Let R be a Noetherian ring, M a finitely generated R-module and let $X = j-\operatorname{Spec}(R) \cap \operatorname{Supp}(M)$, which is basic (since $j-\operatorname{Spec}(R)$ is basic and $\operatorname{Supp}(M)$ is closed). We then have:*

$$\mu(M) \ \leq \ \sup_{\mathfrak{p}\in X} \{\dim_X(\mathfrak{p}) + \mu_{\mathfrak{p}}(M)\}$$

If we combine everything we said about the minimum number of generators, we obtain:

$$\mu_{\mathfrak{p}}(M) \ \leq \ \mu(M) \ \leq \ \sup_{\mathfrak{q}\in X} \{\dim_X(\mathfrak{q}) + \mu_{\mathfrak{q}}(M)\},$$

for all $\mathfrak{p} \in \operatorname{Spec}(R)$.

Proof. We set $n = \mu(M)$ and $t = \sup_{\mathfrak{p}\in X} \{\dim_X(\mathfrak{p}) + \mu_{\mathfrak{p}}(M)\}$. We have to prove $n \leq t$.

(1) First of all, we show that we can prove the theorem by considering M as an $(R/\operatorname{ann}_R(M))$-module, instead of as an R-module.

We first notice that if M is an R-module, it is well defined its structure as $(R/\operatorname{ann}_R(M))$-module. In our case, it immediately follows that M is finitely generated also as $(R/\operatorname{ann}_R(M))$-module. In fact: if $M = \langle x_1, \dots, x_n \rangle_R$ and $x \in M$, then $x = \displaystyle\sum_{i=1}^{n} r_i \cdot x_i$, with $r_i \in R$. Consider the following expression:

$$x = \sum_{i=1}^{n} \overline{r_i} \cdot x_i,$$

with $\overline{r_i} \in R/\operatorname{ann}_R(M)$. We have that if $b \in \operatorname{ann}_R(M)$, then $\overline{r_i + b} = \overline{r_i}$ and $(r_i + b)x_i = r_i x_i$, hence the previous expression is well-defined, so the x_i generate M as an $(R/\operatorname{ann}_R(M))$-module. This does not influence the minimum number of generators, because if $M = \langle x_1, \dots, x_n \rangle_R$ minimally, then $M = \langle x_1, \dots, x_n \rangle_{R/\operatorname{ann}(M)}$ still minimally; because if by contradiction we can write $x_1 = \overline{r_2}x_2 + \ldots + \overline{r_n}x_n$, this means that $x_1 = r_2x_2 + \ldots + r_nx_n$, so x_1 was not minimal in M as an R-module, but this is a contradiction. So

$$\mu_R(M) = \mu_{R/\operatorname{ann}(M)}(M).$$

and this holds also for the localization in $\mathfrak{p}$.

Moreover, $R/\operatorname{ann}_R(M)$ is still a Noetherian ring, because is the quotient of a Noetherian ring. Finally, we have:

$$\operatorname{Spec}(R/\operatorname{ann}_R(M)) \cong \operatorname{Spec}(R) \cap V(\operatorname{ann}_R(M)).$$

It follows that also:

$$j\text{−}\operatorname{Spec}(R/\operatorname{ann}_R(M)) \cong j\text{−}\operatorname{Spec}(R) \cap V(\operatorname{ann}_R(M)) = j\text{−}\operatorname{Spec}(R) \cap \operatorname{Supp}(M) = X.$$

It follows that $\dim_X(\mathfrak{p}) = \dim_{j-\operatorname{Spec}(R/\operatorname{ann}(M))}(\mathfrak{p}/\operatorname{ann}(M))$. Combining with the fact that $\mu_{\mathfrak{p}}(M) = \mu_{\mathfrak{p}/\operatorname{ann}(M)}(M)$, for every $\mathfrak{p} \in X$, we obtain that, if we prove the theorem for M as an $(R/\operatorname{ann}(M))$-module, it follows

$$\begin{aligned} \mu_R(M) &= \mu_{R/\operatorname{ann}(M)}(M) \\ &\le \sup_{\{\mathfrak{p}/\operatorname{ann}(M) \mid \mathfrak{p} \in X\}} \left\{ \dim_{j-\operatorname{Spec}(R/\operatorname{ann}(M))}(\mathfrak{p}/\operatorname{ann}(M)) + \mu_{\mathfrak{p}/\operatorname{ann}(M)}(M) \right\} \\ &= \sup_{\mathfrak{p} \in X} \{ \dim_X(\mathfrak{p}) + \mu_{\mathfrak{p}}(M) \} \end{aligned}$$

and this is the statement of the theorem. So, under the assumption of the theorem, we have that M is a finitely generated $(R/\operatorname{ann}_R(M))$-module, with

$R/\operatorname{ann}_R(M)$ a Noetherian ring. Moreover, setting $R = R/\operatorname{ann}_R(M)$, we can directly assume $X = j - \operatorname{Spec}(R)$ and it is enough to prove the theorem for R of this form. With this change of notation, our goal is exactly the same.

(2) Assume by contradiction that $n > t$. Since M is finitely generated, we know that $n = \mu(M) < \infty$, so $t < \infty$. Since $M = \langle x_1, \dots, x_n \rangle_R$, we have the following short exact sequence

$$\begin{tikzcd} 0 \arrow[r] & M' \arrow[r, "i"] & R^n \arrow[r, "f"] & M \arrow[r] & 0, \end{tikzcd}$$

where $\begin{array}{l} f : R^n \longrightarrow M, \\ \quad e_i \longmapsto x_i \end{array}$ $M' = \ker(f)$ and i is the natural inclusion. We can now apply the functor $- \otimes_R \kappa(\mathfrak{p})$ (with $\mathfrak{p} \in X$) and we obtain the exact sequence:

$$\begin{tikzcd} M' \otimes_R \kappa(\mathfrak{p}) \arrow[r, "\tilde{i}"] & \kappa(\mathfrak{p})^n \arrow[r, "\tilde{f}"] & M \otimes_R \kappa(p) \arrow[r] & 0, \end{tikzcd}$$

which is equivalent to the exact sequence

$$\begin{tikzcd} \dfrac{(M')_\mathfrak{p}}{\mathfrak{p}(M')_\mathfrak{p}} \arrow[r, "\tilde{i}"] & \kappa(\mathfrak{p})^n \arrow[r, "\tilde{f}"] & \dfrac{M_\mathfrak{p}}{\mathfrak{p}M_\mathfrak{p}} \arrow[r] & 0. \end{tikzcd}$$

This is a sequence consisting of $\kappa(\mathfrak{p})$-vector spaces, since it is exact we have that $\dim_{\kappa(\mathfrak{p})}(\operatorname{Im}(\tilde{i})) = \dim_{\kappa(\mathfrak{p})}(\ker(\tilde{f}))$ and from the Rank–Nullity Theorem, it follows:

$$\dim_{\kappa(\mathfrak{p})}(\operatorname{Im}(\tilde{i})) = \dim_{\kappa(\mathfrak{p})}(\ker(\tilde{f})) = \dim_{\kappa(\mathfrak{p})}(\kappa(\mathfrak{p})^n) - \dim_{\kappa(\mathfrak{p})}(\operatorname{Im}(\tilde{f})).$$

However, $\dim_{\kappa(\mathfrak{p})}(\kappa(\mathfrak{p})^n) = n$ and $\operatorname{Im}(\tilde{f}) = \dfrac{M_\mathfrak{p}}{\mathfrak{p}M_\mathfrak{p}}$, which has dimension $= \mu_\mathfrak{p}(M)$. So we have

$$\dim_{\kappa(\mathfrak{p})}(\operatorname{Im}(\tilde{i})) = n - \mu_\mathfrak{p}(M) > t - \mu_\mathfrak{p}(M) \geq (\dim_X(\mathfrak{p}) + \mu_\mathfrak{p}(M)) - \mu_\mathfrak{p}(M) = \dim_X(\mathfrak{p})$$

and this holds for all $\mathfrak{p} \in X$. It follows that $\dim_{\kappa(\mathfrak{p})}(\operatorname{Im}(\tilde{i})) \geq \dim_X(\mathfrak{p}) + 1$, for every $\mathfrak{p} \in X$. Since M' is a submodule of R^n and $\tilde{i}$ is the map induced by the natural inclusion of the former into the latter, we deduce that

$$\dim_{\kappa(\mathfrak{p})}(\operatorname{Im}(\tilde{i})) = \delta_\mathfrak{p}(M') \geq \dim_X(\mathfrak{p}) + 1, \forall \mathfrak{p} \in X.$$

Take S a system of generators of M', we have just proved that S is an X-basic set. Apply Corollary 2.2.2 in order to obtain an element $z \in R^n$ which is X-basic. We can see from the proof of the Eisenbud-Evans' Theorem that $z \in \langle S \rangle_R = M'$. By proceeding exactly as in the proof of Serre's Theorem, we obtain that z is a unimodular row for R, so $R^n = \langle z\rangle_R \oplus P$, with P a finitely generated projective module, and $\langle z\rangle_R \cong R$. Finally, we have that $R^n \cong R \oplus P$ and the same holds under localization, so that $(R_{\mathfrak{q}})^n \cong R_q \oplus P_q$, with P_q a finitely generated free module, whose rank must be $n-1 \geq t$. This holds for every $\mathfrak{q} \in X$.

Bass' Cancellation theorem requires that $\operatorname{rk}(P_{\mathfrak{q}}) \geq d+1$, for every $\mathfrak{q} \in X$, where $d = \dim(X)$. However, we have that $t \geq d+1$, in fact: if $\mathfrak{p} \in X$ is the prime ideal achieving $d = \dim(X) = \sup\limits_{\mathfrak{q}\in X}\{\dim_X(\mathfrak{q})\}$, then $\dim_X(\mathfrak{p}) = d$ and we have

$$\dim_X(\mathfrak{p}) + \mu_{\mathfrak{p}}(M) = d + \mu_{\mathfrak{p}}(M) \overset{(3)}{\geq} d+1.$$

It follows

$$t = \sup_{\mathfrak{q}\in X}\{\dim_X(\mathfrak{q}) + \mu_{\mathfrak{q}}(M)\} \geq \dim_X(\mathfrak{p}) + \mu_{\mathfrak{p}}(M) \geq d+1.$$

Clearly, this holds also in the case of infinite dimension. We can now use Bass' Cancellation Theorem to obtain $P \cong R^{n-1}$.

Since $z \in M' = \ker(f)$, we have a surjective map $\overline{f} : \dfrac{R^n}{\langle z\rangle_R} \longrightarrow M$ induced by f. Since $R^n = \langle z\rangle_R \oplus P$, it results $\dfrac{R^n}{\langle z\rangle_R} \cong P \cong R^{n-1}$. As a consequence, we have another surjective map

$$\begin{tikzcd} g : R^{n-1} \arrow[r] & M, \\ e_i \arrow[r, mapsto] & x_i. \end{tikzcd}$$

But this means that one of the minimal generators of M was not necessary, i.e. $\mu(M) < n$, and this is a contradiction, so $t \leq n$.

(3) Recall that our ring is $R/\operatorname{ann}(M)$ and this implies that

$$\operatorname{Supp}_{R/\operatorname{ann}(M)}(M) = V(\operatorname{ann}_{R/\operatorname{ann}(M)}(M)) = V(0) = \operatorname{Spec}(R/\operatorname{ann}(M)),$$

because if $\overline{a} \in R/\operatorname{ann}(M)$ is such that $\overline{a}\cdot x = 0$, for every $x \in M$, that is $a \cdot x = 0$, for every $x \in M$, it means that $a \in \operatorname{ann}_R(M)$, so $\overline{a} = \overline{0}$ in $R/\operatorname{ann}(M)$. It follows that $X \subseteq \operatorname{Spec}(R/\operatorname{ann}(M)) = \operatorname{Supp}_{R/\operatorname{ann}(M)}(M)$, so in particular $\mathfrak{p} \in \operatorname{Supp}_{R/\operatorname{ann}(M)}(M)$, hence $M_{\mathfrak{p}} \neq 0$ and $\mu_{\mathfrak{p}}(M) \geq 1$.

□

Corollary 3.3.2. *Under the same assumptions of the previous theorem, with* $d = \dim(R)$ *finite, we have*

$$\mu_{\mathfrak{p}}(M) \leq \mu(M) \leq \sup_{\mathfrak{q} \in X} \{\mu_{\mathfrak{q}}(M)\} + d, \quad \forall \mathfrak{p} \in \operatorname{Spec}(R).$$

These two inequalities better clarify the relationship between the minimum number of generators of M and that of its localizations. If we know the dimension of the ring, the upper bound discovered in the Forster-Swans' Theorem becomes much easier, because $\dim(R)$ is an upper bound for every $\dim_X(\mathfrak{q})$.

Proof. It follows directly from the theorem that

$$\mu(M) \leq \sup_{\mathfrak{q} \in X} \{\dim_X(\mathfrak{q}) + \mu_{\mathfrak{q}}(M)\} \leq \sup_{\mathfrak{q} \in X} \{d + \mu_{\mathfrak{q}}(M)\} = \sup_{\mathfrak{q} \in X} \{\mu_{\mathfrak{q}}(M)\} + d.$$

□

Since in general $X \subseteq \operatorname{Spec}(R)$, it holds that

$$\mu_{\mathfrak{p}}(M) \leq \mu(M) \leq \sup_{\mathfrak{q} \in \operatorname{Spec}(R)} \{\mu_{\mathfrak{q}}(M)\} + d, \quad \forall \mathfrak{p} \in \operatorname{Spec}(R),$$

which is a weaker than the previous one.

Example 3.3.3. Let $R = k[x_1, \dots, x_n]$, with k a field, and let $M = \mathfrak{m} \subseteq R$ be a maximal ideal. We know from Hilbert Nullstellensatz that $\operatorname{Spec}(R) = j - \operatorname{Spec}(R)$.

If $\mathfrak{p} \neq \mathfrak{m}$ is a prime ideal, then we have

$$\dim_X(\mathfrak{p}) + \mu_{\mathfrak{p}}(\mathfrak{m}) = \dim(R/\mathfrak{p}) + \mu_{R_{\mathfrak{p}}}(R_{\mathfrak{p}}) = \dim(R/\mathfrak{p}) + 1.$$

If instead $\mathfrak{p} = \mathfrak{m}$, then

$$\dim_X(\mathfrak{m}) + \mu_{\mathfrak{m}}(\mathfrak{m}) = \dim(R/\mathfrak{m}) + n = n.$$

Therefore

$$\mu(\mathfrak{m}) \leq \sup_{\mathfrak{p} \in \operatorname{Spec}(R)} \{\dim_X(\mathfrak{p}) + \mu_{\mathfrak{p}}(\mathfrak{m})\} = \dim(R/(0)) + 1 = n + 1,$$

which is off by one, since we know that $\mu(\mathfrak{m}) = n$.

Chapter 4

Bass' Stable Range Theorem

4.1 The General Linear Group GL(R)

Definition 4.1.1. We denote with $GL_m(R)$ the group of invertible $m \times m$ matrices with entries in R. We set then

$$\begin{tikzcd} i_{m,m+1} : GL_m(R) \arrow[r] & GL_{m+1}(R) \\ A \arrow[r, mapsto] & \begin{pmatrix} A & 0 \\ 0 & 1 \end{pmatrix} \end{tikzcd}$$

and similarly, for every $k > m$, we have

$$\begin{tikzcd} i_{m,k} : GL_m(R) \arrow[r] & GL_k(R) \\ A \arrow[r, mapsto] & \begin{pmatrix} A & 0 & \cdots & 0 \\ 0 & 1 & & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}. \end{tikzcd}$$

So we map an invertible $m \times m$ matrix in itself, surrounded by rows and columns of the identity matrix. So we complete A to an invertible $k \times k$ matrix, because if we add 1 only on the diagonal and 0 everywhere else, the determinant of the new matrix remains the same as before, in particular it is still invertible. We set $i_{m,m} = \mathrm{id}_{GL_m(R)}$. It is immediate to show that these applications are compatible with composition, so that $i_{k,h} \circ i_{m,k} = i_{m,h}$, because the effect is the same: we add $h-m$ rows and columns of the identity to the matrix A. Moreover, these are all group homomorphisms. Therefore $\{GL_m(R), i_{m,k}\}_{k \geq m \in \mathbb{N}}$ is a direct system of groups. Finally, we define the **General Linear Group**

$$GL(R) = \varinjlim_{m\in\mathbb{N}} (GL_m(R))$$

Remark 4.1.2. From the properties of the direct limit, it follows that

$$GL(R) = \left(\bigsqcup_{m\in\mathbb{N}} GL_m(R) \right) /\!\sim$$

and $A \in GL_m(R) \sim B \in GL_n(R)$ if and only if there exists $k \in \mathbb{N}$, such that $k \geq m, k \geq n$ and $i_{m,k}(A) = i_{n,k}(B)$, i.e. the matrices A e B are equal, except for some number of rows and columns of the identity matrix. If for example $m \geq n$, this is the same thing as asking that $i_{n,m}(B) = A$, i.e. the matrix A is equal to B, if we add $m - n$ rows and columns of the identity matrix to B.

The direct limit $GL(R)$ is still a group, because if $A \in GL_m(R)$ and $B \in GL_n(R)$, with for instance $m \geq n$ then their product is defined as

$$A \cdot B = A \cdot i_{n,m}(B) = A \cdot \begin{pmatrix} B & 0 & \cdots & 0 \\ 0 & 1 & & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}.$$

As in the direct limits in general, we bring both A and B in the same level group, in this case $GL_m(R)$, and we use that $GL_m(R)$ is a group, so here the product is well-defined.

We now see the definition of the subgroup of $GL(R)$ generated by all elementary matrices.

Definition 4.1.3. Let $r \in \mathbb{N}$. An **elementary $r \times r$ matrix** is the result of the identity matrix I_r, after applying one of the following operation: interchanging two rows, multiplying a row by a unit, and adding a multiple of one row to another. We denote with $E_r(R)$ the subgroup of $GL_r(R)$ generated by all elementary $r \times r$ matrices.

Remark 4.1.4. First of all, it is clear that the elementary matrices are invertible.

If we take a matrix $A \in GL_r(R)$ and an elementary $r \times r$ matrix E; then multiplying A on the left by E applies to A the same operations that were applied to I_r. For example, if $E = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$, that is the identity I_3 with the second and the third rows interchanged, and then we take the matrix $A = \begin{pmatrix} 2 & 3 & 0 \\ 0 & 5 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, if we take the product we obtain

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 2 & 3 & 0 \\ 0 & 5 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 3 & 0 \\ 0 & 0 & 1 \\ 0 & 5 & 0 \end{pmatrix},$$

which is exactly the matrix A with the second and the third rows interchanged.

We have also that if we multiply A on the right by E, we apply the same operations defining E to the columns instead of the rows. We can easily see this fact in the previous example:

$$\begin{pmatrix} 2 & 3 & 0 \\ 0 & 5 & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 2 & 0 & 3 \\ 0 & 0 & 5 \\ 0 & 1 & 0 \end{pmatrix},$$

which is the matrix A with the second and the third columns interchanged.

Definition 4.1.5. We can define the same group homomorphisms as before by restricting the previous ones to every $E_r(R)$. In fact $i_{m,k}(E)$ is still an elementary matrix if E is, because if E is for example the interchange of the first and second rows of I_m, then $i_{m,k}(E)$ will be the interchange of the same rows, but of the matrix I_k. So we can define

$$E(R) = \varinjlim_{m \in \mathbb{N}} (E_m(R)).$$

Analogous considerations apply as in the previous case. Since every $E_r(R)$ is a subgroup of $GL_r(R)$, and also the operation defined in $E(R)$ is the same as the one in $GL(R)$, it follows that $E(R)$ is a subgroup of $GL(R)$.

4.2 Stable range

Recall that $a = (a_1, \dots, a_n) \in R^n$ is a unimodular row if the ideal $(a_1, \dots, a_n) = R$.

Definition 4.2.1. Let $n \in \mathbb{N}$. We say that n **defines a stable range** for $GL(R)$ if for every $r > n$ and $(a_1, \dots, a_r)$ unimodular row for R, there exist elements $b_1, \dots, b_{r-1} \in R$, such that $(a_1 + a_r b_1, a_2 + a_r b_2, \dots, a_{r-1} + a_r b_{r-1})$ is still unimodular.

Therefore n defines a stable range if every unimodular row longer than n can be reduced to a row of length one less. We can proceed with this argument until we obtain a unimodular row of length n.

We now see some results regarding the relation between the concept of stable range and the elementary matrices seen in the previous section.

Lemma 4.2.2. *Assume that n defines a stable for $GL(R)$ and let $r > n$. If $(a_1, \dots, a_r)$ is a unimodular row, then there exists $A \in E_r(R)$, such that*

$$((a_1, \dots, a_r) \cdot A)^t = (0, \dots, 0, 1)^t,$$

or, in other words:

$$A^t \cdot \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_r \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}.$$

Proof. We know that n defines a stable range, $r > n$ and $(a_1, \dots, a_r)$ is unimodular, so there exist $b_1, \dots, b_{r-1} \in R$, such that $(a_1 + a_r b_1, a_2 + a_r b_2, \dots, a_{r-1} + a_r b_{r-1})$ is unimodular. Denote $c_i = (a_i + a_r b_i) \in R$, so that $(c_1, \dots, c_{r-1})$ is a unimodular row. This means that there exist $\lambda_1, \dots, \lambda_{r-1} \in R$, such that $\lambda_1 c_1 + \dots + \lambda_{r-1} c_{r-1} = 1 - a_r \in R$.

Let us now consider the following operations over the vector $(a_1, \dots, a_r)^t$:

$$\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_r \end{pmatrix} \xrightarrow{R_1 + b_1 \cdot R_r} \begin{pmatrix} a_1 + a_r \cdot b_1 = c_1 \\ a_2 \\ \vdots \\ a_r \end{pmatrix} \to \dots \to \begin{pmatrix} c_1 \\ \vdots \\ c_{r-1} \\ a_r \end{pmatrix}.$$

Then we do the followings:

$$\begin{pmatrix} c_1 \\ \vdots \\ c_{r-1} \\ a_r \end{pmatrix} \xrightarrow{R_r + \lambda_1 \cdot R_1} \begin{pmatrix} c_1 \\ \vdots \\ c_{r-1} \\ \lambda_1 c_1 + a_r \end{pmatrix} \to \dots \to \begin{pmatrix} c_1 \\ \vdots \\ c_{r-1} \\ \lambda_1 c_1 + \ldots + \lambda_{r-1} c_{r-1} + a_r = 1 \end{pmatrix}.$$

We have obtained the column vector $(c_1, \dots, c_{r-1}, 1)^t$ starting from the column vector $(a_1, \dots, a_r)^t$, applying elementary row operations, so, step by step, multiplying the vector $(a_1, \dots, a_r)^t$ on the left by the elementary matrices associated with these operations. The result is of the following form:

$$A' \cdot \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_r \end{pmatrix} = \begin{pmatrix} c_1 \\ \vdots \\ c_{r-1} \\ 1 \end{pmatrix},$$

where A' is the product of all the elementary matrices involved in the process, representing the composition of all these operations. So $A' \in E_r(R)$. Next,

$$\begin{pmatrix} c_1 \\ \vdots \\ c_{r-1} \\ 1 \end{pmatrix} \xrightarrow{R_1 - c_1 R_r} \begin{pmatrix} 0 \\ \vdots \\ c_{r-1} \\ 1 \end{pmatrix} \to \cdots \to \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix},$$

so, if we call A the matrix obtained by multiplying A' on the left by the last elementary matrices, then $A \in E_r(R)$ and

$$A \cdot \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_r \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}$$

and this is the same as:

$$((a_1, \ldots, a_r) \cdot A^t)^t = (0, \ldots, 0, 1)^t,$$

with $A^t \in E_r(R)$, since it can be proved that the transpose of an elementary matrix is still an elementary matrix.

□

Lemma 4.2.3. *Under the same assumptions as the lemma before, if $r > n$, then:*

$$GL_r(R) \cdot E_{r+1}(R) = GL_{r+1}(R).$$

This product means to denote:

$$\begin{pmatrix} GL_r(R) & 0 \\ 0 & 1 \end{pmatrix} \cdot E_{r+1}(R).$$

Proof. Clearly, $GL_r(R) \cdot E_{r+1}(R) \subseteq GL_{r+1}(R)$, because if $A \in GL_r(R)$, then

$i_{r,r+1}(A) = \begin{pmatrix} A & 0 \\ 0 & 1 \end{pmatrix}$ is still invertible, as discussed before; moreover $E \in E_{r+1}(R)$ is invertible, so $A \cdot E \in GL_{r+1}(R)$.

Let us now take $A \in GL_{r+1}(R)$, we want to show that $A \in GL_r(R) \cdot E_{r+1}(R)$. We first show that the last row of A is unimodular.

Let it be $(a_1, \dots, a_{r+1})$. Let then $1 \in R$, we consider the column vector of length $r+1$: $\begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix}$, then it follows

$$A \cdot A^{-1} \cdot \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix}.$$

We set $B = A^{-1} \cdot \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix}$, this is a column vector of length $r+1$, say $\begin{pmatrix} b_1 \\ \vdots \\ b_{r+1} \end{pmatrix}$. Then we have

$$A \cdot \begin{pmatrix} b_1 \\ \vdots \\ b_{r+1} \end{pmatrix} = \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix} \Rightarrow \begin{pmatrix} \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots \\ a_1 & \cdots & a_{r+1} \end{pmatrix} \cdot \begin{pmatrix} b_1 \\ \vdots \\ b_{r+1} \end{pmatrix} = \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix}.$$

This implies that the last row of A multiplied by the vector B is equal to 1, but this is $a_1 b_1 + \ldots + a_{r+1} b_{r+1} = 1$, so $(a_1, \dots, a_{r+1})$ is a unimodular row.

We can now apply the previous lemma, hence there exists an elementary matrix $E \in E_{r+1}(R)$, such that $(a_1, \dots, a_{r+1}) \cdot E = (0, \dots, 0, 1)$ (we have taken the transpose). The expression $(a_1, \dots, a_{r+1}) \cdot E$ represents the product of E and the last row of A, that is the last row of the resulting matrix AE. So the final result of this multiplication will be

$$A \cdot E = \begin{pmatrix} A' & f \\ 0 & 1 \end{pmatrix},$$

where f is a column vector of size $r \times 1$, while $A' \in GL_r(R)$, because the determinant of AE depends only on the block A', since the contribution of the block f is annihilated by the 0 block, and the resulting matrix AE must be invertible, hence also A' must be invertible.

Notice then a matrix of the form $\begin{pmatrix} I_r & g \\ 0 & 1 \end{pmatrix} \in E_{r+1}(R)$, since $g = (v_1, \dots, v_r)^t$ is a column vector of size $r \times 1$, representing the following r elementary operations:

$$I_{r+1} = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \cdots & 0 & 1 \end{pmatrix} \xrightarrow{R_1 + v_1 R_{r+1}} \begin{pmatrix} 1 & 0 & \cdots & v_1 \\ 0 & 1 & & 0 \\ \vdots & & \ddots & \vdots \\ 0 & \cdots & 0 & 1 \end{pmatrix} \to \cdots \to \begin{pmatrix} I_r & g \\ 0 & 1 \end{pmatrix}.$$

The size of the matrix A' is $r \times r$, the same holds for its inverse, while f has size $r \times 1$, so we can create a column vector of size $r \times 1$ by taking $g = (-A')^{-1} \cdot f$. Denote $E' = E \cdot \begin{pmatrix} I_r & g \\ 0 & 1 \end{pmatrix} \in E_{r+1}(R)$, with this specific column vector g. We then have:

$$A \cdot E' = A \cdot E \cdot \begin{pmatrix} I_r & (-A')^{-1} f \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} A' & f \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} I_r & (-A')^{-1} f \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} A' & 0 \\ 0 & 1 \end{pmatrix}.$$

We finally have

$$A = \begin{pmatrix} A' & 0 \\ 0 & 1 \end{pmatrix} \cdot (E')^{-1} = i_{r,r+1}(A') \cdot (E')^{-1} \in GL_r(R) \cdot E_{r+1}(R).$$

□

We are now ready to prove the following theorem, which makes us understand how useful the concept of stable range is.

Theorem 4.2.4. *If n defines a stable range for $GL(R)$, then*

(1) $\dfrac{GL_m(R)}{E_m(R)} \longrightarrow \dfrac{GL(R)}{E(R)}$ *is surjective, for every $m \geq n$.*

(2) $E_r(R) \trianglelefteq GL_r(R)$ *and $GL_r(R)/E_r(R)$ is abelian, for every $r \geq 2n$.*

In other words, (1) shows that the quotient at level m is sufficient to cover all levels of the disjoint union forming the quotient $GL(R)/E(R)$, if $m \geq n$.

Proof. (1) The map is the canonical projection

$$\begin{tikzcd} \pi : \dfrac{GL_m(R)}{E_m(R)} \arrow[r] & \dfrac{GL(R)}{E(R)} \\ \overline{A} \arrow[r, mapsto] & \tilde{A} \end{tikzcd}$$

. Let us show that this map is well-defined.

Let $E \in E_m(R)$, then $\pi(\overline{E}) = \tilde{E} \in E(R)$, so it is well-defined.

Given now $B \in GL(R)$, suppose that $B \in GL_k(R)$, for some $k \in \mathbb{N}$, we distinguish two cases.

(a) This is the case when $k > m \geq n$, then by Lemma 4.2.3, we have

$$GL_k(R) = GL_{k-1}(R) \cdot E_k(R) = \cdots = GL_m(R) \cdot E_{m+1}(R) \cdot \ldots \cdot E_k(R).$$

Therefore $B = B' \cdot E_{m+1} \cdot \ldots \cdot E_k$, with $E_i \in E_i(R)$ and $B' \in GL_m(R)$. It follows that $\pi(\overline{B'}) = \tilde{B}' = \tilde{B}' \cdot \tilde{E}_{m+1} \cdot \ldots \cdot \tilde{E}_k = \tilde{B}$, because every $E_i \in E(R)$. This case is concluded.

(b) If instead $k \leq m$, we know that $\widetilde{B} = \widetilde{i_{k,k+1}(B)} = \cdots = \widetilde{i_{k,m}(B)}$, this follows from the definition of $GL(R)$ as a direct limit, as seen in Remark 4.1.2, where we defined $i_{k,m}(B) = \begin{pmatrix} B & 0 & \cdots & 0 \\ 0 & 1 & & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix} \in GL_m(R)$. Hence we have that $\pi(\overline{i_{k,m}(B)}) = \widetilde{i_{k,m}(B)} = \widetilde{B}$, thus π is surjective.

(2) The normality of $E_r(R)$ follows from Suslin's Theorem. We will prove only the abelianity of the quotient group. We proceed by induction on r. First, we prove the case $r = 2n$. Given two matrices $A, B \in GL_{2n}(R)$, since $2n > n$ and n defines a stable range, we can use Lemma4.2.3, as we have done in (1a), and obtain

$$A = A' \cdot E_{n+1} \cdot \ldots \cdot E_{2n},$$

with $E_i \in E_i(R)$ and $A' \in GL_n(R)$. It follows that in the quotient $GL_r(R)/E_r(R)$ we have

$$\overline{A} = \overline{A'} \cdot \overline{I_{n+1}} \cdot \ldots \cdot \overline{I_{2n}} = \overline{i_{n,2n}(A')} = \begin{pmatrix} A' & 0 \\ 0 & I_n \end{pmatrix},$$

where this matrix is seen in the same quotient, but we denote it without the class, to simplify notation. Similarly we have $\overline{B} = \begin{pmatrix} B' & 0 \\ 0 & I_n \end{pmatrix}$, with $B' \in GL_n(R)$. In the quotient we have that $\begin{pmatrix} B' & 0 \\ 0 & I_n \end{pmatrix} = \begin{pmatrix} 0 & B' \\ I_n & 0 \end{pmatrix}$, because the second matrix is obtained from the first one by multiplying it by n elementary matrices corresponding, to the n column interchanges performed. Following the exact same argument for the n rows, we obtain $\begin{pmatrix} 0 & B' \\ I_n & 0 \end{pmatrix} = \begin{pmatrix} I_n & 0 \\ 0 & B' \end{pmatrix}$. We finally have:

$$\overline{A} \cdot \overline{B} = \begin{pmatrix} A' & 0 \\ 0 & I_n \end{pmatrix} \cdot \begin{pmatrix} I_n & 0 \\ 0 & B' \end{pmatrix} = \begin{pmatrix} A' & 0 \\ 0 & B' \end{pmatrix} \text{ and}$$

$$\overline{B} \cdot \overline{A} = \begin{pmatrix} I_n & 0 \\ 0 & B' \end{pmatrix} \cdot \begin{pmatrix} A' & 0 \\ 0 & I_n \end{pmatrix} = \begin{pmatrix} A' & 0 \\ 0 & B' \end{pmatrix}.$$

Therefore, the base case $r = 2n$ is proved.

Suppose now that $r > 2n$ and that the theorem holds for every $2n \leq k < r$, we have to prove that also the case r is true. Let $A, B \in GL_r(R)$, we again use Lemma 4.2.3 and obtain $A = A' \cdot E_r$ and $B = B' \cdot E'_r$, with $A', B' \in GL_{r-1}(R)$ and $E_r, E'_r \in E_r(R)$, so that

$$\overline{A} = \overline{i_{r-1,r}(A')} \text{ and } \overline{B} = \overline{i_{r-1,r}(B')}.$$

We then have:

$$\overline{A} \cdot \overline{B} = \begin{pmatrix} A' & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} B' & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} A'B' & 0 \\ 0 & 1 \end{pmatrix} \overset{(I)}{=} \begin{pmatrix} B'A' & 0 \\ 0 & 1 \end{pmatrix} = \overline{B} \cdot \overline{A},$$

where (I) follows by the inductive hypothesis.

□

4.3 Bass' Stable Range Theorem

This theorem is a direct application of the Eisenbud-Evans Theorem, and gives us an example of a quantity that defines a stable range for $GL(R)$.

Theorem 4.3.1 (Bass' Stable Range Theorem)**.** *Let R be a Noetherian ring, then $n = \dim(j - \operatorname{Spec}(R)) + 1$ defines a stable range for $GL(R)$.*

Proof. Let $r > n$ and let $(a_1, \ldots, a_r)$ be a unimodular row for R. We then set $M = R^{r-1}$ and $y = (a_1, \ldots, a_{r-1}) \in M$. Moreover, set $a = a_r$. It follows that $(y, a) \in M \oplus R$ is X-basic, where X can be either $\operatorname{Spec}(R)$ or $j - \operatorname{Spec}(R)$.

Let $X = j$-$\operatorname{Spec}(R)$ and let $\mathfrak{q} \in X$. We have $M_\mathfrak{q} \cong R_\mathfrak{q}^{r-1}$, which is free, so

$$\mu_\mathfrak{q}(M) = \operatorname{rk}(M_\mathfrak{q}) = r - 1 \geq n = \dim(X) + 1 \geq \dim_X(\mathfrak{q}) + 1.$$

Thus, we are under the assumptions of the Eisenbud-Evans Theorem, so there exists $z = (b_1, \ldots, b_{r-1}) \in M = R^{r-1}$, such that

$$y + az = (a_1 + a_r b_1, \ldots, a_{r-1} + a_r b_{r-1}) \text{ is } X\text{-basic.}$$

This is equivalent to $y + az$ being a unimodular row. Hence n defines a stable range for $GL(R)$.

$\square$

Chapter 5

Bourbaki's Theorem

5.1 Preliminaries

Definition 5.1.1. Let A be a subring of a ring B. An element $b \in B$ is said to be **integral** over A if there exists a monic polynomial $p(x) \in A[x]$, such that $p(b) = 0$.

Notation. Denote

$$\overline{A}^B = \{b \in B \mid b \text{ is integral over } A\},$$

so this is the set of all the integral elements in B over A, it is called the **integral closure** of A in B. In general, $A \subseteq \overline{A}^B \subseteq B$.

Definition 5.1.2. If D is a domain, then we define the **field of fractions** of D as

$$Q(D) = \left\{ \frac{a}{b} \mid a, b \in D, \text{ with } b \neq 0 \right\}.$$

As the name suggests, this is a field containing D.

Definition 5.1.3. A domain D is said to be **integrally closed** (or **normal**) if $\overline{D} := \overline{D}^{Q(D)} = D$, i.e. if the integral closure of D in its field of fractions $Q(D)$ is equal to D itself.

We want to give a characterization of normal domains which are Noetherian and local. In order to do that, we first need the definition of DVR and a further characterization of this concept, which will lead us to our final goal.

Definition 5.1.4. Let $(G, +, \leq)$ be a totally ordered abelian group and K be a field. A K-**valuation** is a group homomorphism $v : K^* = K \setminus \{0\} \longrightarrow G$, such that

$$v(x + y) \geq \min\{v(x), v(y)\}, \ \forall x, y \in K^*, \text{with } x + y \neq 0.$$

If we define $\overline{G} = G \cup \{\infty\}$, we can extend the K-valuation to a new K-valuation $v : K \longrightarrow \overline{G}$, such that $v(0) = \infty$. The element ∞ is such that $g + \infty = \infty$, for every $g \in G$, $\infty + \infty = \infty$ and $\infty > g$, for all $g \in G$.

Definition 5.1.5. If $v : K^* \longrightarrow G$ is a K-valuation, then we denote $\mathrm{Im}(v) = \Gamma_v$, which is a totally ordered subgroup of G, called **value group of** G.

Definition 5.1.6. Let K be a field, a K-**valuation ring** is a subring $V \subseteq K$ (in particular it is a domain), such that $Q(V) = K$ and for every $x \in K^*$, we have that $x \in V$ or $x^{-1} \in V$.

Proposition 5.1.7. *Let V be a K-valuation ring, then:*

(1) The ideals of V are totally ordered by inclusion, i.e. if there exists $x \in I \setminus J$, then $J \subseteq I$.

(2) If I is a finitely generated ideal, then it is principal, i.e. generated by only one element.

(3) The ring V is local, with maximal ideal $\mathfrak{m}_V = \{x \in V \mid x^{-1} \notin V\} \cup \{0\}$.

(4) We can define a K-valuation $v : K \longrightarrow \overline{G}$, such that $A_v = \{x \in K \mid v(x) \geq 0_G\} = V$ and $\mathfrak{m}_V = \mathfrak{m}_v = \{x \in K \mid v(x) > 0_G\}$. Moreover, we have that $\Gamma_v \cong K^*/U(V)$, with $U(V)$ the multiplicative group of the units of V.

Proof. (1) We know that $x \in I$ and $x \notin J$. Let $y \in J$, with $y \neq 0$, then if $xy^{-1} \in V$, then $x \in (y) \subseteq J$, but this is a contradiction. So $yx^{-1} \in V$, that is $y \in (x) \subseteq I$. Finally, $J \subseteq I$.

(2) Let us suppose $I \neq 0$ and take $G = \{x_1, \dots, x_n\}$ a system of generators for I with minimal cardinality. By (1) we have that either $(x_2, \dots, x_n) \subseteq (x_1)$, or $(x_1) \subseteq (x_2, \dots, x_n)$.

In the first case, it follows that $I = (x_1)$, so $n = 1$ and I is generated by one element, as stated. In the second case, we have $I = (x_2, \dots, x_n)$, so I is generated by $n-1$ elements, however this is a contradiction, because n was the minimal number of generators.

(3) First of all, $\mathfrak{m}_V$ is an ideal of V, because if $x \in \mathfrak{m}_V, y \in V$, then if by contradiction $xy \notin \mathfrak{m}_V$, it follows that $(xy)^{-1} = y^{-1}x^{-1} \in V$, so also $y(y^{-1}x^{-1}) = x^{-1} \in V$. This implies that $x \notin \mathfrak{m}_V$, which is a contradiction.

Let us take now $z \in V \setminus \mathfrak{m}_V$, we have that $z, z^{-1} \in V$, so z is a unit. We have proved that $\mathfrak{m}_V = V \setminus U(V)$, so V is a local ring, with $\mathfrak{m}_V$ as maximal ideal.

(4) Let us define $\Gamma = K^*/U(V)$. Moreover, we define an order on Γ, that is:

$$\overline{x} \geq \overline{y} \iff xy^{-1} \in V.$$

It is well-defined because $\overline{x} = \overline{y}$ if and only if $xy^{-1} \in U(V)$, and:

$$\overline{x} = \overline{y} \iff \overline{x} \geq \overline{y} \text{ and } \overline{x} \leq \overline{y} \iff xy^{-1}, x^{-1}y \in V \iff xy^{-1} \in U(V).$$

We show that it is a total order on Γ. Given $\overline{x}, \overline{y} \in \Gamma$, if $xy^{-1} \in V$, then $\overline{x} \geq \overline{y}$ and we have finished.

If instead $xy^{-1} \notin V$, then $x^{-1}y \in V$, so $\overline{y} \geq \overline{x}$. We conclude that $\geq$ is a total order.

Let us define $v : K^* \longrightarrow \Gamma$ as the canonical projection onto the quotient group. We have that it is a surjective group homomorphism, so $\Gamma_v = \Gamma$. We now prove that $v(x+y) \geq \min\{v(x), v(y)\}$.

If for instance $v(x+y) \geq v(x)$, there is nothing to prove. Assume that $v(x+y) < v(x)$, i.e. $v(x+y) \ngeq v(x)$, so $(x+y)x^{-1} = (1+yx^{-1}) \notin V$. We know that $1 \in V$, so $yx^{-1} \notin V$, hence $xy^{-1} \in V$, therefore $(x+y)y^{-1} = (xy^{-1}+1) \in V$ and this means that $v(x+y) \geq v(y)$. We conclude that v is a K-valuation.

Now we observe that:

$$A_v \setminus \{0\} = \{x \in K^* \mid \overline{x} \geq \overline{1}\} = \{x \in K^* \mid x \cdot 1 \in V\} = V \setminus \{0\}.$$

Similarly:

$$\mathfrak{m}_v \setminus \{0\} = \{x \in K^* \mid \overline{x} > \overline{1}\} = \{x \in K^* \mid x \in V, x^{-1} \notin V\} = \mathfrak{m}_V \setminus \{0\}.$$

□

Notation. Let V be a K-valuation ring, we denote $\Gamma_V = \Gamma_v (= K^*/U(V))$, where v is the valuation of (4).

Definition 5.1.8. A K-valuation ring V is said to be **discrete**, denoted with DVR, if $\Gamma_V \cong \mathbb{Z}$.

So a DVR is a valuation ring, where the image of the natural valuation can be seen as $\mathbb{Z}$.

Theorem 5.1.9. *Let $(R, \mathfrak{m})$ be a local domain, set $K = Q(R)$, with $R \neq K$, the following statements are equivalent:*

(1) R is a DVR.

(2) R is a Noetherian valuation ring.

(3) R is a PID.

(4) R is Noetherian and $\mathfrak{m}$ is principal.

(5) R is regular and $\dim(R) = 1$.

This is the characterization of DVR we wanted; after proving this, we will show that a local and normal Noetherian domain, with dimension 1, is regular, hence is all of the previous conditions.

Proof. (1) $\Rightarrow$ (2). Let $v : K^* \longrightarrow \mathbb{Z}$ be the valuation of the previous proposition, with $\Gamma_R \cong \mathbb{Z}$. Let then $0 \subsetneq I \subsetneq R$ be an ideal and $X = \{v(y) \mid y \in I \setminus \{0\}\} \subseteq \mathbb{Z}$.

Let $z \in I$, such that $v(z) = \min(X)$. Let $0 \neq x \in I$, then we have that $v(xz^{-1}) = v(x) - v(z) \geq 0$, hence $xz^{-1} \in A_v = R$, so $x \in (z) \subseteq R$. Therefore $I \subseteq (z) \subseteq I$, consequently $I = (z)$, so R is Noetherian.

(2) $\Rightarrow$ (3). By (2) of Proposition 5.1.7 we have that every ideal is principal, since every ideal is finitely generated, under our assumptions.

(3) $\Rightarrow$ (4). It is straightforward.

(4) $\Rightarrow$ (5). If the maximal ideal $\mathfrak{m}$ is principal, then $\operatorname{ht}(\mathfrak{m}) \leq \mu_R(\mathfrak{m}) = 1$. We know that R is not a field, so there exists one ideal other than (0), and this implies that $\operatorname{ht}(\mathfrak{m}) \geq 1$. We conclude that

$$\operatorname{ht}(\mathfrak{m}) = \dim(R) = \mu_R(\mathfrak{m}) = 1,$$

so R is regular.

(5) $\Rightarrow$ (1). By the Auslander-Buchsbaum Theorem, we know that a regular and local ring is a UFD. We have that $\mu(\mathfrak{m}) = 1$, so $\mathfrak{m} = (a)$, with $a \in R$ an irreducible element. This a is the only irreducible element in R (up to units), because those elements generate prime ideals, but they all must be contained in $\mathfrak{m}$, hence they must have height at most 1, so they must be equal to $\mathfrak{m}$.

Take $0 \neq b = \frac{x}{y} \in Q(R)$, with $b \notin R$. We have to prove that $b^{-1} \in R$.

Write $x = u \cdot a^n$ and $y = w \cdot a^t$, with $u, w \in U(R)$ and $n, t \in \mathbb{N}$. We have these expressions since R is a UFD and a is the only irreducible element. It follows that $\frac{x}{y} = b = (uw^{-1})a^{n-t}$, where uw^{-1} is a unit of R.

Since $b \notin R$, we must have $n - t < 0$, hence

$$b^{-1} = (u^{-1}w)a^{t-n} \in R.$$

This proves that R is a $Q(R)$-valuation ring. We have to prove that is discrete. The elements in $Q(R)$ are of the form $b = u \cdot a^n$, for some $u \in U(R)$ and $n \in \mathbb{Z}$, as discussed before. The valuation associated to R is again the canonical projection

$$\begin{tikzcd}
v : Q(R)^* \arrow[r] & Q(R)^*/U(R) \\
ux^n \arrow[r, mapsto] & \overline{ux^n}.
\end{tikzcd}$$

We notice that in the image of v we have $\overline{ux^n} = \overline{x^n}$, so we can define an isomorphism

$$\begin{tikzcd} h : Q(R)^*/U(R) \arrow[r] & \mathbb{Z} \\ \overline{x^n} \arrow[r, mapsto] & n. \end{tikzcd}$$

Therefore R is a DVR.

□

Now, our goal is to show that, in the local Noetherian case with dimension 1, regular is equivalent to integrally closed.

The part involving the proof of the previous statement is mainly taken from Section 10.119 of [2].

Lemma 5.1.10. *Let* $(R, \mathfrak{m})$ *be a local Noetherian ring, then one of the following conditions is satisfied:*

(1) R is Artinian.

(2) R is regular of dimension 1.

(3) $\operatorname{depth}(R) \geq 2$.

(4) There exists a finite ring homomorphism $f : R \to R'$, i.e. such that R' is a finitely generated R-module, via f, which is not an isomorphism, also $\ker(f)$ *and* $\operatorname{coker}(f)$ *are annihilated by a power of* $\mathfrak{m}$. *Moreover,* $R' \neq 0$ *and* $\mathfrak{m} \notin \operatorname{Ass}_R(R')$.

Proof. First of all, R Artinian is equivalent to R Noetherian with dimension 0. We have two cases: R is Artinian. i.e. (1) holds, or R is not Artinian, that is $\dim(R) > 0$, since R is Noetherian.

Assume that $\dim(R) > 0$, we have to prove that one of the other three conditions is satisfied.

Denote with J the largest ideal of R which is annihilated by a certain power of $\mathfrak{m}$. Let us suppose that $J \neq 0$, then we can define the canonical projection $f : R \to R/J$. We prove that f satisfies (4).

Since J is a proper ideal, we have that $R/J \neq 0$. Note that $\ker(f) = J$, which is annihilated by a power of $\mathfrak{m}$, by definition of J. This also proves that f is not an isomorphism, since $\ker(f) \neq 0$. The map is finite, because $R/J = \langle \overline{1} \rangle_R$. Morevoer, $\operatorname{coker}(f) = 0$, since f is surjective, so is trivially annihilated by $\mathfrak{m}$.

Finally, $\mathfrak{m} \notin \operatorname{Ass}_R(R/J)$, because if by contradiction $\mathfrak{m} = \operatorname{ann}_R(\overline{v})$, with $\overline{v} \in R/J$, $\overline{v} \neq \overline{0}$, it follows that $v \notin J$ and $\mathfrak{m} \cdot \overline{v} = \overline{0}$, so $\mathfrak{m} \cdot v \subseteq J$. Therefore $\mathfrak{m} \cdot v$ is annihilated by a power of $\mathfrak{m}$, so also $J + (v) \supsetneq J$ is annihilated by a power of

$\mathfrak{m}$, but this is a contradiction, because J was the largest ideal among the ideals like that.

We have proved that if $J \neq 0$, then (4) holds. Assume that $J = 0$. It follows that $\mathfrak{m} \notin \operatorname{Ass}_R(R)$, because if $\mathfrak{m} = \operatorname{ann}_R(w)$, with $0 \neq w \in R$, then $\mathfrak{m} \cdot w = 0$. This means that (w) is an ideal annihilated by a power of $\mathfrak{m}$, so $J \supseteq (w) \supsetneq 0$, which is a contradiction.

Since $\{\text{zero divisors of } R\} = \bigcup\limits_{\mathfrak{p} \in \operatorname{Ass}_R(R)} \mathfrak{p}$, there exists $x \in \mathfrak{m}$ a non-zero divisor of R. Hence $\operatorname{depth}(R) \geq 1$.

Let us again distinguish in two cases. If $\mathfrak{m} \notin \operatorname{Ass}_R(R/(x))$, then we can find a non-zero divisor of $R/(x)$ in $\mathfrak{m}$, thus depth ≥ 2, which is condition (3).

Assume now that $\mathfrak{m} \in \operatorname{Ass}_R(R/(x))$, so $\mathfrak{m} = \operatorname{ann}_R(\overline{y})$, with $y \notin (x)$. It follows that $\mathfrak{m} \cdot y \subseteq (x)$.

If $\mathfrak{m} \cdot y \subseteq \mathfrak{m} \cdot x$, then we can we can consider the endomorphism

$$\begin{tikzcd}
\varphi : \mathfrak{m} \arrow[r] & \mathfrak{m} \, , \\
f \arrow[r, mapsto] & \frac{yf}{x}
\end{tikzcd}$$

which is well-defined because x is a non-zero divisor. By a consequence of the Cayley-Hamilton's Theorem, there exists a monic polynomial $P \in R[T]$, such that $P(\varphi) = 0$. Consider now the ring R_x, where it lies the element $\frac{y}{x}$. We know that $x \in \mathfrak{m}$, so choosing $f = x$, we have that $P(\varphi(x)) = P(\frac{yx}{x}) = P(y) = 0$. It easy to prove that by manipulating fractions in R_x, it follows that $P(\frac{y}{x}) = 0$.

Consider now $R' = R[\frac{y}{x}] \subseteq R_x$ the R-algebra generated by the element $\frac{y}{x}$. This is the set of the algebraic R-combinations of $\frac{y}{x}$. It is clear that $R \subseteq R'$, so we can take the inclusion map $i : R \hookrightarrow R'$. Let us prove that i satisfies (4).

We know that x is a non-zero divisor of R, so the localization map $g : R \to R_x$ is injective, hence also i is injective. Therefore $\ker(i) = 0$ is annihilated by $\mathfrak{m}$. We know that $\frac{y}{x}$ is integral over R, since it is a root of a monic polynomial with coefficients in R (that is P). It follows that $R \subseteq R'$ is finite, so R' is a finitely generated R-module, so i is finite.

Let us examine $\operatorname{coker}(i) = R'/R$; we want to prove that it is annihilated by a power of $\mathfrak{m}$. Without denoting classes, an element of this quotient ring is of the form

$$p = a_n \left(\frac{y}{x}\right)^n + a_{n-1} \left(\frac{y}{x}\right)^{n-1} + \cdots + a_1 \left(\frac{y}{x}\right).$$

Since $\mathfrak{m} \cdot y \subseteq (x)$, we have $\mathfrak{m} \cdot \frac{y}{x} \subseteq R$, so $\mathfrak{m}^n \cdot (\frac{y}{x})^n \subseteq R$ and the same holds for every other $i = 1, \ldots, n-1$. Hence $\mathfrak{m}^n \cdot p \subseteq R$. If $p_1, \ldots, p_l$ generate R'/R, then take $k = \max\limits_i \{\deg(p_i)\}$. It follows that $\mathfrak{m}^k \cdot p_i = 0$ in R'/R, for every i, that is $\mathfrak{m}^k \cdot R'/R = 0$.

The map i is not an isomorphism because it is not surjective. For the sake of contradiction, if $i(v) = \frac{v}{1} = \frac{y}{x}$, then there exists $n \in \mathbb{N}^*$, such that $x^n(vx - y) = 0$. Using that x is a non-zero divisor, we obtain $y = vx$, so $y \in (x)$, and this is a contradiction.

Let us finally prove that $\mathfrak{m} \notin \operatorname{Ass}_R(R')$. Assume by contradiction $\mathfrak{m} = \operatorname{ann}_R(q)$, with $0 \neq q = a_n \left(\frac{y}{x}\right)^n + a_{n-1}\left(\frac{y}{x}\right)^{n-1} + \cdots + a_1\left(\frac{y}{x}\right) + a_0 \in R'$. If we put everything over a common denominator, we can write $q = \frac{c}{x^n}$, with $c \in R,\ c \neq 0$, since $\frac{c}{x^n} \neq 0$. We have that $\mathfrak{m} \cdot q = 0$, so $x^m(\mathfrak{m} \cdot c) = 0$, for some $m \in \mathbb{N}^*$. Since x is non-zero divisor, we have $\mathfrak{m} \cdot c = 0$; consequently $\mathfrak{m} = \operatorname{ann}_R(c)$, which is a contradiction, because $\mathfrak{m} \notin \operatorname{Ass}_R(R)$.

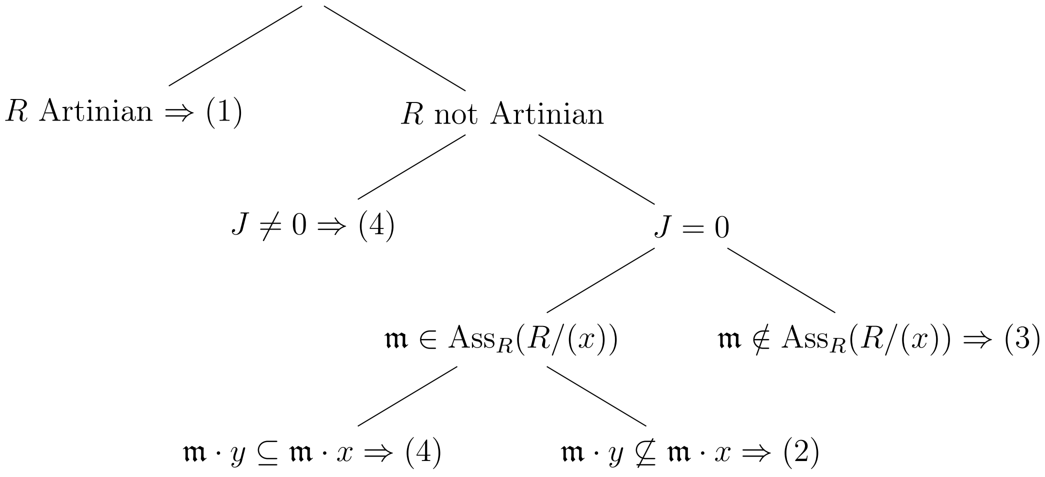
Our last case is when $\mathfrak{m} \cdot y \subseteq (x)$, but $\mathfrak{m} \cdot y \nsubseteq \mathfrak{m} \cdot x$. Hence there exist $t \in \mathfrak{m}$ and $u \in R \setminus \mathfrak{m} = U(R)$, such that $t \cdot y = u \cdot x$. It follows that $x = u^{-1}t \cdot y$, in particular y is a non-zero divisor. Rename $t = u^{-1}t$.

Let $t' \in \mathfrak{m}$, we know that $yt' = xs$, for some $s \in R$, therefore

$$y(t' - st) = xs - xs = 0 \Rightarrow t' = st \in (t),$$

hence $\mathfrak{m} = (t)$. It follows that $(R, \mathfrak{m})$ is a regular ring of dimension 1, because $\dim(R) > 0$ and $1 \leq \operatorname{ht}(\mathfrak{m}) \leq \mu(\mathfrak{m}) = 1$, so $\mu(\mathfrak{m}) = \dim(R) = 1$. This is condition (2).

Let us summarize:



So we have proved that one of the four conditions always holds.

□

From the previous tree, we can notice that (4) occurs in two different cases. We will refer to the case when $J \neq 0$ as (4S), S for surjective, since the map is the canonical projection $\pi : R \to R/J$. We will refer to the case when $J = 0$ and $\mathfrak{m} \cdot y \subseteq \mathfrak{m} \cdot x$ as (4I), I for injective, since the map is the natural inclusion $i : R \hookrightarrow R' = R[\frac{y}{x}] \subseteq R_x$, with $x \in \mathfrak{m}$ a non-zero divisor of R and $y \in R \setminus (x)$.

The following lemma proves that equivalence between regular and normal, in dimension one.

Lemma 5.1.11. *Let $(R, \mathfrak{m})$ be a local Noetherian domain of dimension 1, then*

$$R \text{ is normal} \iff R \text{ is regular.}$$

Proof. $\Rightarrow$. If R is a regular ring of dimension 1, it follows that $\operatorname{ht}(\mathfrak{m}) = \mu(\mathfrak{m}) = 1$. Assume by contradiction that $\mathfrak{m}$ cannot be generated by only one element (i.e. R not regular). By applying the previous lemma, we know that one of the four conditions is satisfied. Clearly, (2) is not satisfied, nor is (1), because $\dim(R) = 1 \neq 0$. Also (3) is excluded, because $2 \leq \operatorname{depth}(R) \leq \dim(R) = 1$, which is a contradiction. So condition (4) is satisfied.

We know that R is a domain, thus, within the notation of the discussion after the lemma, we are not in the case (4S), where $J \neq 0$ (because no element of R can be annihilated by some $\mathfrak{m}^n$). We are in the case (4I), so $R' = R[\frac{y}{x}]$ and the map f is the inclusion $i : R \hookrightarrow R'$.

It follows that $R' \subseteq R_x \subseteq Q(R)$. We also know that $R \subseteq R'$ is finite, so is an integral extension, i.e. $\overline{R}^{R'} = R'$. As a consequence:

$$R' = \overline{R}^{R'} \subseteq \overline{R}^{Q(R)} = R,$$

where the last equality holds because R is normal. Therefore $R = R'$, but this is a contradiction, since i cannot be an isomorphism.

$\Leftarrow$. It follows from Theorem 5.1.9 that if R is a regular local Noetherian domain of dimension 1, then it is a PID. Therefore it is a UFD. Let us prove that if R is a UFD, then R is normal.

Suppose $w = \frac{a}{b} \in \overline{R}$, then there exists a polynomial $f(x) = x^n + c_{n-1}x^{n-1} \dots c_1 x + c_0$ with coefficients in R, having w as a root. Assume that $MCD(a, b) = 1$. We know that $w^n + c_{n-1}w^{n-1} \dots c_1 w + c_0 = 0$, so:

$$a^n + c_{n-1}a^{n-1}b \dots c_1 ab^{n-1} + c_0 b^n = 0.$$

Therefore b divides a^n, which is a contradiction, unless b is invertible in R, because $MCD(a, b) = 1$. We conclude that $w \in R$, so $\overline{R} = R$.

□

Lemma 5.1.12. *If R is a normal domain, then also $R_{\mathfrak{p}}$ is a normal domain, for every $\mathfrak{p} \in \operatorname{Spec}(R)$.*

Proof. First of all, note that $R_{(0)} = Q(R)$ and $Q(R_\mathfrak{p}) = (R_\mathfrak{p})_{(0)} = R_{(0)}$, so that $Q(R) = Q(R_\mathfrak{p})$, for every $\mathfrak{p} \in \operatorname{Spec}(R)$. Take $\frac{a}{b} \in Q(R)$ an integral element over $R_\mathfrak{p}$. Then there exists a monic polynomial $p(x) = x^n + \frac{a_{n-1}}{s_{n-1}}x^{n-1} + \ldots + \frac{a_1}{s_1}x_1 + \frac{a_0}{s_0}$ in $R_\mathfrak{p}[x]$, such that

$$\frac{a^n}{b^n} + \frac{a_{n-1}}{s_{n-1}}\frac{a^{n-1}}{b^{n-1}} + \ldots + \frac{a_1}{s_1}\frac{a}{b} + \frac{a_0}{s_0} = 0.$$

Set $s = s_0 \cdot \ldots \cdot s_{n-1} \in R \setminus \mathfrak{p}$. Then multiply by s^n the previous equation; we obtain

$$s^n\frac{a^n}{b^n} + \left(s\frac{a_{n-1}}{s_{n-1}}\right)s^{n-1}\frac{a^{n-1}}{b^{n-1}} + \ldots + \left(s^{n-1}\frac{a_1}{s_1}\right)s\frac{a}{b} + \left(s^n\frac{a_0}{s_0}\right) = 0,$$

where the terms in parentheses belong to R. Let us define a new polynomial $\tilde{p}(x) = x^n + \left(s\frac{a_{n-1}}{s_{n-1}}\right)x^{n-1} + \ldots + \left(s^{n-1}\frac{a_1}{s_1}\right)x + \left(s^n\frac{a_0}{s_0}\right)$. This is a monic polynomial in $R[x]$ and has $s\frac{a}{b}$ as a root. We know that R is normal, so $\overline{R}^{Q(R)} = R$, hence $s\frac{a}{b} \in R$, therefore $\frac{a}{b} = \frac{1}{s} \cdot \left(s\frac{a}{b}\right) \in R_\mathfrak{p}$.

We have proved that $\overline{R_\mathfrak{p}}^{Q(R_\mathfrak{p})} = R_\mathfrak{p}$, so that $R_\mathfrak{p}$ is normal.

□

We are now ready to prove one implication of Serre's Criterion for normality, which is the one we will use in the proof of the Bourbaki's Theorem. See Section 10.157 of [2].

Definition 5.1.13. Let R be a Noetherian ring, $k \geq 0$, we say that:

(1) R has property (R_k) if for every prime $\mathfrak{p} \in \operatorname{Spec}(R)$, such that $\operatorname{ht}(\mathfrak{p}) \leq k$, then $R_\mathfrak{p}$ is regular.

(2) R has the property (S_k) if for every prime $\mathfrak{p} \in \operatorname{Spec}(R)$, we have that $\operatorname{depth}(R_\mathfrak{p}) \geq \min\{k, \dim(R_\mathfrak{p})\}$.

Theorem 5.1.14. *If R is a Noetherian integrally closed domain, then R has properties (R_1) and (S_2).*

Proof. Observe that R is a domain, so the only prime ideal with height equal to 0 is (0). Then, note that $R_{(0)} = Q(R)$, which is a field, so it is regular. Condition (R_1) is proved for primes of height 0.

Now, take a prime ideal $\mathfrak{p}$ with $\operatorname{ht}(\mathfrak{p}) = 1$. Then $\dim(R_\mathfrak{p}) = 1$. By using Lemma 5.1.12, we know that $R_\mathfrak{p}$ is still a normal domain, which is also local, and then, applying Lemma 5.1.11, we conclude that $R_\mathfrak{p}$ is regular. We have proved that R has property (R_1).

Let us show that R has property (S_2). Let $\mathfrak{p} \in \mathrm{Spec}(R)$, and rename $R = R_{\mathfrak{p}}$, which is a Noetherian normal domain of dimension $d = \dim(R_{\mathfrak{p}})$. We have to prove that $\mathrm{depth}(R) \geq \min\{2, d\}$. If $d \leq 1$, then we use property (R_1) and we are done. Assume that $d \geq 2$, so that $\min\{2, d\} = 2$.

Let $\mathfrak{m}$ be the maximal ideal of R. We apply Lemma 5.1.10, so we examine which one of the four cases occurs. Clearly is not (1), because $\dim(R) > 1$, nor (2), for the same reason. For the sake of contradiction, assume that condition (4) holds.

As observed in the proof of Lemma 5.1.11, since R is a domain, the fact that condition (4) is satisfied implies that we are in the case (4I), i.e. $J = 0$ and the map $f : R \hookrightarrow R'$ is the natural inclusion. We know that $\mathfrak{m} \notin \mathrm{Ass}_R(R')$, so we can find a non-zero divisor of R', say $z \in \mathfrak{m}$. We prove that $R_z = R'_z$.

Clearly, $R_z \subseteq R'_z$, because $R \subseteq R'$. Take $\frac{r}{z^n} \in R'_z$, with $r \in R'$ and $n \in \mathbb{N}$. Suppose that $r \in R' \setminus R$, otherwise $\frac{r}{z^n} \in R_z$ and we are done. By condition (4I), we know that there exists $k \in \mathbb{N}^*$, such that $\mathfrak{m}^k \cdot R'/R = 0$. Being z in $\mathfrak{m}$, this implies that $z^k \cdot r \in R$, so $z^k \cdot \frac{r}{z^n} \in R_z$. Finally, we obtain $\frac{r}{z^n} = \frac{rz^k}{z^{n+k}} \in R_z$.

We know that $Q(R) = Q(R_z) = Q(R'_z) = Q(R')$, therefore R and R' have the same field of fractions. We also know that $R \subseteq R'$ is finite, so it is integral, hence $\overline{R}^{R'} = R'$. It follows that

$$R \subseteq \overline{R}^{R'} \subseteq \overline{R}^{Q(R)=Q(R')} = R,$$

hence $R = \overline{R}^{R'} = R'$, and this is a contradiction, because f is not an isomorphism.

We conclude that condition (3) of Lemma 5.1.10 holds, that is $\mathrm{depth}(R) \geq 2$.

□

Corollary 5.1.15. *Let R be a Noetherian integrally closed domain, $0 \neq z \in R$, let then $\mathfrak{p} \in \mathrm{Ass}_R(R/(z))$. Then $\mathrm{ht}(\mathfrak{p}) = 1$.*

Proof. Assume by contradiction that $\mathrm{ht}(\mathfrak{p}) \geq 2$, hence $\dim(R_{\mathfrak{p}}) \geq 2$ and therefore $\min\{2, \dim(R_{\mathfrak{p}})\} = 2$. Since R has property (S_2), it follows that $\mathrm{depth}(R_{\mathfrak{p}}) \geq 2$.

We know that $z \in \mathfrak{p}$, hence $0 \neq \frac{z}{1} \in \mathfrak{p}R_{\mathfrak{p}}$ is a non-zero divisor of $R_{\mathfrak{p}}$. This means that $\mathrm{depth}(R_{\mathfrak{p}}) \geq 1$.

We also know that $\mathfrak{p}R_{\mathfrak{p}} \in \mathrm{Ass}_{R_{\mathfrak{p}}}(R_{\mathfrak{p}}/(z_{\mathfrak{p}}))$, so we cannot find a non-zero divisor of $R_{\mathfrak{p}}/(z_{\mathfrak{p}})$ in $\mathfrak{p}R_{\mathfrak{p}}$, hence $\mathrm{depth}(R_{\mathfrak{p}}) = 1 < 2$, which is a contradiction.

□

We have proved everything we need about normal domains. The assumptions of the Bourbaki's Theorem are: R being a Noetherian normal domain and M a finitely generated torsion-free R-module. In the following part, we focus on the concept of torsion-free module.

Definition 5.1.16. Let R be a domain. An R-module M is said to be **torsion-free** if there is no element $0 \neq r \in R$, such that $r \cdot x = 0$, for some element $0 \neq x \in M$.

Definition 5.1.17. Let R be a domain, with field of fractions $Q(R) = K$, let then M be a finitely generated R-module. We define $\operatorname{rank}(M) = \dim_K(M \otimes_R K)$.

Remark 5.1.18. Assume that M is a torsion-free R-module. First of all, notice that the natural map $\begin{aligned} \varphi : M &\longrightarrow M \otimes_R K \\ x &\longmapsto x \otimes 1 \end{aligned}$ is injective. In fact, we have that $M \otimes_R K = M \otimes_R R_{(0)} \cong M_{(0)}$, hence $x \otimes 1$ can be seen as $\frac{x}{1}$. If we ask that $\frac{x}{1} = 0$ in $M_{(0)}$, then there exists $0 \neq s \in R$, such that $s \cdot x = 0$. However, M is torsion-free, so this implies $x = 0$. Therefore, φ is injective.

Remark 5.1.19. Let us the examine the case $\operatorname{rank}(M) = 1$ and M torsion-free. This means that $M \otimes_R K \cong K$. So we can see M as a submodule of K, since we have the composition of maps: $h : M \xrightarrow{\varphi} M \otimes_R K \xrightarrow{\cong} K$, so $M \cong \varphi(M) \subseteq K$. We know that M is finitely generated, assume that $x_1, \ldots, x_n$ is a system of generators for M. Then $h(M) = \langle h(x_1), \ldots, h(x_n) \rangle_R = \langle \frac{a_1}{b_1}, \ldots, \frac{a_n}{b_n} \rangle_R \subseteq K$. If we take the common denominator $d = b_1 \cdot \ldots \cdot b_n$, then

$$h(M) = \left\langle \frac{a'_1}{d}, \ldots, \frac{a'_n}{d} \right\rangle_R .$$

We conclude that $I = d \cdot h(M) \subseteq R$, this is a submodule of R, hence an ideal. If we then take the map

$$\begin{aligned} \cdot d : M &\longrightarrow I \\ x &\longmapsto d \cdot h(x) \end{aligned} ,$$

we have that this map is surjective, by definition. Moreover, it is injective, because h is injective, so if $d \cdot h(x) = 0$, then $h(dx) = 0$, thus $d \cdot x = 0$. The module M is torsion-free, $d \neq 0$, hence $x = 0$. We have proved that $M \cong I$, so M is isomorphic to an ideal of R.

The following lemmas can be found in Section 15.22 of [2].

Lemma 5.1.20. *Let R be a domain and M a finitely generated R-module. Then M is torsion-free if and only if M is a submodule of some finitely generated free R-module.*

Proof. $\Leftarrow$. If $M \subseteq R^n$, for some $n \in \mathbb{N}^*$, then M is torsion-free, since R^n is. In fact, if $0 \neq r \in R$ and $r \cdot (a_1, \dots, a_n) = 0$, then $r \cdot a_i = 0$, for every i. However, R is a domain, so this implies that $(a_1, \dots, a_n) = (0, \dots, 0)$.

$\Rightarrow$. Let $K = Q(R)$. Since M is finitely generated, $M \otimes_R K$ is a finitely generated K-vector space, with $\{e_1, \dots, e_r\}$ as a basis. Let $x_1, \dots, x_n$ be generators of M, we proceed as in Remark 5.1.19, denoting with h the same map of the Remark (in our case $M \otimes_R K \cong K^r$).

We then write $h(x_i) = \displaystyle\sum_{j=1}^{r} \frac{a_{ij}}{b_{ij}} e_j \in K^r$. Then, if we take $b = \displaystyle\prod_{i,j} b_{ij}$, we have that $b \cdot h(M) \subseteq R^r$. As in the remark, the map $\cdot b$ is an isomorphism, so $M \cong b \cdot h(M) \subseteq R^r$.

□

Corollary 5.1.21. *If M is a finitely generated torsion-free R-module, then $M_{\mathfrak{p}}$ is a finitely generated torsion-free $R_{\mathfrak{p}}$-module*

Proof. Apply Lemma 5.1.20 in order to obtain $M \subseteq R^n$. Then $M_{\mathfrak{p}} \subseteq R^n_{\mathfrak{p}}$. Hence $M_{\mathfrak{p}}$ is torsion-free.

□

Lemma 5.1.22. *Let R be a PID and M a finitely generated torsion-free R-module. Then M is free.*

Proof. By applying Lemma 5.1.20, we obtain that $M \subseteq R^n$, for some $n \geq 1$. We proceed by induction on n.

If $n = 1$, then up to isomorphism we may assume that $M \subseteq R$ is a submodule, so is an ideal of R, which is a PID; hence $M = (r)$. If we then take the map $\begin{aligned} f : (r) &\longrightarrow R \\ r &\longmapsto 1 \end{aligned}$, we conclude that this is an isomorphism (since M is torsion-free), so $M \cong R$ is free.

Assume $n > 1$. Let then $\begin{aligned} \pi : R^n &\longrightarrow R^{n-1} \\ (a_1, \dots, a_n) &\longmapsto (a_2, \dots, a_n) \end{aligned}$ the projection onto the last $n-1$ coordinates. Denote $M' = \operatorname{Im}(\pi) \subseteq R^{n-1}$ and $I = M \cap R$, where this R is the first component of R^n. We obtain the following short exact sequence

$$\begin{tikzcd} 0 \arrow[r] & I \arrow[r] & M \arrow[r, "\pi"] & M' \arrow[r] & 0, \end{tikzcd}$$

where the map between I and M is the natural inclusion. We have that $I \subseteq M$ and $I \subseteq R$, so I is an ideal of R and it is also torsion-free. We can apply the case $n = 1$ and conclude that I is a free R-module. We then apply the inductive step to M', and obtain that also M' is free.

Therefore M' is projective, thus, by Remark 3.1.2, it follows that the previous exact sequence splits, hence $M \cong I \oplus M'$, which is free.

$\square$

Corollary 5.1.23. *Let R be an integrally closed Noetherian domain, let then M be a finitely generated torsion-free R-module. Then $M_{\mathfrak{p}}$ is free, for every $\mathfrak{p} \in \operatorname{Spec}(R)$ with $\operatorname{ht}(\mathfrak{p}) \leq 1$.*

Proof. Apply Theorem 5.1.14, R has property (R_1), so $R_{\mathfrak{p}}$ is a regular domain of dimension 1. Now apply Theorem 5.1.9, we obtain that $R_{\mathfrak{p}}$ is a PID. Finally, apply Lemma 5.1.22 to conclude that $M_{\mathfrak{p}}$ is free, since it is a finitely generated torsion-free $R_{\mathfrak{p}}$-module.

$\square$

5.2 Theorem's proof

Theorem 5.2.1 (Bourbaki's Theorem). *Let R be an integrally closed Noetherian domain, let then M be a finitely generated torsion-free R-module of rank r. Then there exists an ideal $I \subseteq R$ and a short exact sequence*

$$\begin{tikzcd} 0 \arrow[r] & R^{r-1} \arrow[r] & M \arrow[r] & I \arrow[r] & 0. \end{tikzcd}$$

Proof. We proceed by induction on $r = \operatorname{rank}(M)$.

(1) The case $r = 1$ is straightforward (see Remark 5.1.19). From that result it follows that $M \cong I$. The exact sequence in the thesis is

$$\begin{tikzcd} 0 \arrow[r] & 0 \arrow[r] & M \arrow[r] & I \arrow[r] & 0, \end{tikzcd}$$

which is equivalent to saying that $M \cong I$.

(2) Let now $r > 1$. We know from Corollary 5.1.21 that, under these assumptions, also $M_{\mathfrak{q}}$ is torsion-free, for every prime $\mathfrak{q}$. Notice that if $\mathfrak{q} \in \operatorname{Spec}(R)$, then $\operatorname{rank}(M) = \operatorname{rank}(M_{\mathfrak{q}})$. In fact, as discussed before, $M \otimes_R K \cong M \otimes_R R_S \cong M_S$, with $S = R \setminus (0)$. Note that $R \setminus (0) \supseteq R \setminus \mathfrak{q}$, for $\mathfrak{q} \in \operatorname{Spec}(R)$, so $M_S = (M_{\mathfrak{q}})_S$, and for the same reason $K = (R_q)_S$, so K is also the field of fractions of the domain $R_{\mathfrak{q}}$. Therefore

$$\begin{aligned} \operatorname{rank}(M_{\mathfrak{q}}) &= \dim_K(M_{\mathfrak{q}} \otimes_{R_{\mathfrak{q}}} K) = \dim_K(M_{\mathfrak{q}} \otimes_{R_{\mathfrak{q}}} (R_{\mathfrak{q}})_S) = \dim_K((M_{\mathfrak{q}})_S) \\ &= \dim_K(M_S) = \operatorname{rank}(M). \end{aligned}$$

We then notice that $\mu_{\mathfrak{q}}(M) = \mu_{R_{\mathfrak{q}}}(M_{\mathfrak{q}}) \geq \operatorname{rank}(M_{\mathfrak{q}})$, because if $x_1, \ldots, x_n$ form a minimal system of generators for $M_{\mathfrak{q}}$, then $\{x_1, \ldots, x_n\}_S$ is a system of generators for $(M_{\mathfrak{q}})_S$, hence the cardinality of a basis of it will be $\leq r$, but this number is the rank of $M_{\mathfrak{q}}$. Then we have

$$\mu_{\mathfrak{q}}(M) \geq \operatorname{rank}(M_{\mathfrak{q}}) = \operatorname{rank}(M) = r \geq 2, \ \forall \mathfrak{q} \in \operatorname{Spec}(R).$$

Let now $X = X^1 = \{\mathfrak{q} \in \operatorname{Spec}(R) \mid \operatorname{ht}(\mathfrak{q}) \leq 1\}$, we know from Example 1.2.5 that is basic. Our goal is to apply Corollary 2.2.2, hence we need the condition $\mu_{\mathfrak{q}}(M) \geq \dim_X(\mathfrak{q}) + 1$, for every $\mathfrak{q} \in X$.

By way of contradiction, if we have a chain $\mathfrak{q} \subsetneq \mathfrak{q}_1 \subsetneq \mathfrak{q}_2$ in X, we have in particular that $\mathfrak{q}_2 \in X$, so $\operatorname{ht}(\mathfrak{q}_2) \leq 1$, however we have just written a chain of three prime ideals finishing in $\mathfrak{q}_2$, and this is a contradiction. So it results $\dim_X(\mathfrak{q}) \leq 1$ and therefore $\dim_X(\mathfrak{q}) + 1 \leq 2$.

We then use Corollary 2.2.2 in order to obtain an element $x \in M$, which is X-basic.

If we take the map $\begin{aligned}\varphi : R &\longrightarrow M \\ 1 &\longmapsto x\end{aligned}$, we notice that this is injective, because if $r \cdot x = 0$, since M is torsion-free, this means that r is a zero divisor in R, however R is a domain, so the only zero divisor is 0, hence $r = 0$ and φ is injective. This implies that $R \cong \langle x \rangle_R \subseteq M$.

(3) Denote with $N = M/R$, which implicitly represents $M/\langle x \rangle_R$. We claim that N is still torsion-free.

Let us take $z \in R, z \neq 0$, we have to prove that it is N-regular, i.e. there is no $n \in N, n \neq 0$, such that $z \cdot n = 0$. Consider the following commutative diagram with exact rows and columns:

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & & \\
0 \arrow[r] & R \arrow[r, "\varphi"] \arrow[d, "\cdot z"] & M \arrow[r, "\pi"] \arrow[d, "\cdot z"] & N \arrow[r] \arrow[d, "\cdot z = \mu_z"] & 0 \\
0 \arrow[r] & R \arrow[r, "\varphi"'] & M \arrow[r, "\pi"'] & N \arrow[r] & 0,
\end{tikzcd}$$

where the first column is exact because z is a non-zero divisor in R, the second one because M is torsion-free, φ is the previous map and π is the canonical projection.

The map μ_z is nothing but $\begin{aligned}\cdot z : N &\longrightarrow N \\ \overline{n} &\longmapsto \overline{z \cdot n}\end{aligned}$, which is well-defined, because if we take $rx \in \langle x \rangle_R$, then $zrx \in \langle x \rangle_R$.

We can now use the Snake Lemma and obtain the exact sequence

$$\begin{tikzcd} 0 \arrow[r] & \ker(\cdot z) = 0 \arrow[r] & \ker(\cdot z) = 0 \arrow[r] & \ker(\mu_z) \arrow[r] & \operatorname{coker}(\cdot z \colon R \to R) \arrow[r] & \cdots, \end{tikzcd}$$

since $\operatorname{coker}(\cdot z \colon R \to R) = R/(z)$, we have an inclusion

$$\begin{tikzcd} 0 \arrow[r] & \ker(\mu_z) \arrow[r] & R/(z). \end{tikzcd}$$

We want to prove that z is N-regular, which is the same as stating that μ_z is injective, so that $\ker \mu_z = 0$. Let us take $\mathfrak{p} \in \operatorname{Ass}(\ker(\mu_z))$, so we automatically have an injection $R/\mathfrak{p} \hookrightarrow \ker(\mu_z)$. Hence we have the composition

$$R/\mathfrak{p} \hookrightarrow \ker(\mu_z) \hookrightarrow R/(z),$$

therefore we get an inclusion $R/\mathfrak{p} \hookrightarrow R/(z)$, so that $\mathfrak{p} \in \operatorname{Ass}(R/(z))$. We know from Corollary 5.1.15 that $\operatorname{ht}(\mathfrak{p}) = 1$.

Therefore, using Corollary 5.1.23, $R_\mathfrak{p}$ is a DVR and $M_\mathfrak{p}$ is free. We know that $x \in M$ is X^1-basic, $\mathfrak{p} \in X^1$, thus x is $\mathfrak{p}$-basic. This means that it is a unimodular row for $R_\mathfrak{p}$, i.e. $\langle x \rangle_\mathfrak{p} \cong R_\mathfrak{p}$ and $M_\mathfrak{p} = \langle x \rangle_\mathfrak{p} \oplus Q$, where Q is a free $R_\mathfrak{p}$-module whose rank is one less than the rank of $M_\mathfrak{p}$. It follows that $N_\mathfrak{p} \cong M_\mathfrak{p}/\langle x \rangle_\mathfrak{p} \cong Q$, then also $N_\mathfrak{p}$ is a free module, so is torsion-free, as a module over the domain $R_\mathfrak{p}$. This is equivalent to stating that for every non-zero $\frac{r}{s} \in R_\mathfrak{p}$, we have that the map $\begin{array}{rcl} \varphi' : N_\mathfrak{p} & \longrightarrow & N_\mathfrak{p} \\ \frac{n}{s'} & \longmapsto & \frac{r}{s} \cdot \frac{n}{s'} \end{array}$ is injective. This holds in particular for $\frac{z}{1} \in R_\mathfrak{p}$ (which is non-zero), with φ' being the map such that $\varphi'(\frac{n}{s'}) = \frac{z}{1} \cdot \frac{n}{s'} = \frac{zn}{s'}$. However, if we localize the map μ_z we obtain the new function $\begin{array}{rcl} (\mu_z)_\mathfrak{p} : N_\mathfrak{p} & \longrightarrow & N_\mathfrak{p} \\ \frac{n}{s'} & \longmapsto & \frac{\mu_z(n)}{s'} = \frac{zn}{s'} \end{array}$, so $\varphi' = (\mu_z)_\mathfrak{p}$, hence $(\mu_z)_\mathfrak{p}$ is also injective, that means $\ker((\mu_z)_\mathfrak{p}) = (\ker \mu_z)_\mathfrak{p} = \{0\}$, this holds for every $\mathfrak{p} \in \operatorname{Ass}_R(\ker \mu_z)$.

We now consider a variant of the local to global principle, that is, under our assumptions, the following statement:

$$M = 0 \iff M_\mathfrak{p} = 0, \ \forall \mathfrak{p} \in \operatorname{Ass}(M).$$

We have to prove only the left arrow. Assume by contradiction that $M \neq 0$, then $\operatorname{Ass}(M) \neq \emptyset$, so there exists $\mathfrak{p} = \operatorname{ann}_R(x)$ a prime ideal, with $x \in M$. In particular, we have $\operatorname{ann}_R(x) \subsetneq R$. Consider $\frac{x}{1} \in M_\mathfrak{p} = 0$, then $\frac{x}{1} = 0$, so that there exists $s \in R \setminus \mathfrak{p}$, such that $s \cdot x = 0$, but this means that $s \in \operatorname{ann}(x) = \mathfrak{p}$, and this is a contradiction.

We then conclude that $\ker(\mu_z) = 0$, so N is torsion-free.

(4) We have $N = M/R$, so $N \otimes_R K \cong \dfrac{M \otimes_R K}{K}$, therefore $N \otimes_R K$ has a dimension as K-vector space one less than $\operatorname{rank}(M)$, i.e. $\operatorname{rank}(N) = r-1$. Hence we can use the inductive step: we get an ideal $I \subseteq R$ and a short exact sequence

$$\begin{tikzcd} 0 \arrow[r] & R^{r-2} \arrow[r, "f"] & M/R \arrow[r, "g"] & I \arrow[r] & 0. \end{tikzcd}$$

We want to lift the map f to a map $f'\colon R^{r-1} \longrightarrow M$. Our goal is to make the following diagram commute

$$\begin{tikzcd} R^{r-1} \arrow[r, "f'"] \arrow[d, "\mathrm{pr}"'] & M \arrow[d, "\pi"] \\ R^{r-2} \arrow[r, "f"'] & M/R. \end{tikzcd}$$

The map pr is the projection onto the last $r-2$ coordinates of R^{r-1}, while π is the canonical projection. One first attempt could be to take $(a_1, a_2, \ldots, a_{r-1})$ and send it into $\pi^{-1}(f(a_2, \ldots, a_{r-1}))$, however we have to choose one of the preimages of $f(a_2, \ldots, a_{r-1})$ via π. Since we cannot do it for every element of R^{r-2}, we first examine the canonical basis $e_2, \ldots, e_{r-1}$. We call $f(e_i) = m_i \in M/R$ and for every i we fix a preimage $n_i \in M$, such that $\pi(n_i) = m_i$. In this way, we take $(a_1, a_2, \ldots, a_{r-1})$, we then write $(a_2, \ldots, a_{r-1})$ in function of the basis, so $(a_2, \ldots, a_{r-1}) = \sum_{i=2}^{r-1} a_i e_i$, then we apply f and obtain the following expression: $\sum_{i=2}^{r-1} a_i f(e_i) = \sum_{i=2}^{r-1} a_i m_i$. Finally, we send this element into $\sum_{i=2}^{r-1} a_i n_i$, which is unique. The diagram now commutes, however f' is no longer injective, because if $(a_1, a_2, \ldots, a_{r-1}) \neq (a_1', a_2, \ldots, a_{r-1})$, then $f'(a_1, a_2, \ldots, a_{r-1}) = f'(a_1', a_2, \ldots, a_{r-1})$, because the value of f (hence of f') is determined only by the last $r-2$ coordinates. To resolve this problem, we define

$$\begin{tikzcd} f' : R^{r-1} \arrow[r] & M \\ (a_1, a_2, \ldots, a_{r-1}) \arrow[r, mapsto] & \sum_{i=2}^{r-1} a_i n_i + a_1 \cdot x. \end{tikzcd}$$

The diagram commutes and f' is injective, because if $a = (a_1, \ldots, a_{r-1}) \in R^{r-1}$ is such that $f'(a_1, \ldots, a_{r-1}) = a_1 x + \sum_{i=2}^{r-1} a_i n_i = 0$ in M, then we have the following relation in the quotient $M/\langle x\rangle_R$:

$$\sum_{i=2}^{r-1} a_i m_i = f(a_2,\dots,a_{r-1}) = \overline{0}.$$

We know that f is injective, so this implies that $(a_2,\dots,a_{r-1}) = (0,\dots,0)$. Hence the original relation in M becomes $a_1 x = 0$, which implies $a_1 = 0$, because M is torsion-free. We conclude that $a = 0$, so f' is injective.

Let us now lift the map g to a surjective map $g'\colon M \longrightarrow I$. We define

$$\begin{tikzcd} g' : M \arrow[r] & I \\ m \arrow[r, mapsto] & g(\overline{m}). \end{tikzcd}$$

This map is clearly surjective, because if $y \in I$, then there exists $\overline{m} \in M/R$, such that $g(\overline{m}) = g'(m) = y$, since g is surjective. We finally prove that $\mathrm{Im}(f') = \ker(g')$.

We first show that $\ker(g') = \pi^{-1}(\ker g)$. We have that

$$m \in \ker(g') \iff g(\overline{m}) = \overline{0} \iff \overline{m} = \pi(m) \in \ker(g) \iff m \in \pi^{-1}(\ker g).$$

Then, we show that $\mathrm{Im}(f') = \pi^{-1}(\mathrm{Im}\, f)$, and this concludes the proof, because $\mathrm{Im}(f) = \ker(g)$, since the previous sequence is exact. We have

$$\overline{m} \in \mathrm{Im}(f) \iff \overline{m} = f(a_2,\dots,a_{r-1}) = f\left(\sum_{i=2}^{r-1} a_i e_i\right) = \sum_{i=2}^{r-1} a_i m_i$$

$$= \sum_{i=2}^{r-1} a_i \pi(n_i) = \pi\left(\sum_{i=2}^{r-1} a_i n_i\right) = \pi\left(\sum_{i=2}^{r-1} a_i n_i + a_1 x\right) \iff \overline{m} \in \pi(\mathrm{Im}\, f').$$

So $\mathrm{Im}(f') = \pi(\mathrm{Im}\, f)$, then $\mathrm{Im}(f') \subseteq \pi^{-1}(\mathrm{Im}\, f)$.

On the other hand, let $n \in \pi^{-1}(\mathrm{Im}\, f)$, then $\overline{n} \in \mathrm{Im}(f)$ and we repeat the same argument, so we conclude that $\overline{n} = \overline{\sum_{i=2}^{r-1} a_i n_i}$ in $M/\langle x\rangle_R$, hence $n = \sum_{i=2}^{r-1} a_i n_i + a_1 x \in \mathrm{Im}(f')$.

We finally obtain the short exact sequence

$$0 \longrightarrow R^{r-1} \xrightarrow{f'} M \xrightarrow{g'} I \longrightarrow 0.$$

$\square$

5.3 Application of the theorem to Gorenstein rings

In this section we will give an application of Bourbaki's Theorem to modules over Gorenstein rings, which is a theorem by Auslander (see [3]). We first recall some definitions regarding injective modules and injective resolutions. We will give also some properties, without proofs, since the only purpose of this section is to view a Corollary of Bourbaki's Theorem. We will prove only the statements strongly connected with the final result. Throughout this section, R will be a Noetherian local ring, with $\mathfrak{m}$ as maximal ideal.

Recall that if R is a ring, then an R-module E is called **injective** if for every $f : N \to M$ injective and $g : N \to E$, with M, N two R-modules and f, g two R-module homomorphisms, there exists an R-module homomorphism $h : M \to E$, such that $g = h \circ f$. The definition can be summarized by the following commutative diagram:

$$\begin{tikzcd}
 & E & \\
M \arrow[ru, dotted, "\exists h"] & N \arrow[l, "f"] \arrow[u, "g"'] & 0. \arrow[l]
\end{tikzcd}$$

Definition 5.3.1. An injective homomorphism of R-modules $i : M \hookrightarrow N$ is said to be an **essential extension** of M if for every submodule $0 \neq L \subseteq N$, we have $i(M) \cap L \neq 0$.

It can be proved that for every inclusion $i : M \hookrightarrow N$, there exists a submodule $H \subseteq N$, such that $i : M \hookrightarrow H$ is maximal among the essential extensions of M contained in N.

An essential extension $M \hookrightarrow N$ is said to be a **maximal essential extension** of M if every essential extension $N \hookrightarrow N'$ is an isomorphism. Such a module N is unique, up to isomorphism. We will denote with $E_R(M)$, or $E(M)$ if R is clear, the maximal essential extension of M. It is called **injective hull** of M and it is an injective module.

Definition 5.3.2. A complex of R-modules $E^\bullet$ is an **injective resolution** of an R-module M if every module E^i of the complex is injective and if we have the following exact sequence:

$$\begin{tikzcd}
0 \arrow[r] & M \arrow[r, "d^{-1}"] & E^0 \arrow[r, "d^0"] & E^1 \arrow[r, "d^1"] & E^2 \arrow[r] & \cdots .
\end{tikzcd}$$

Definition 5.3.3. An injective resolution is said to be a **minimal injective resolution** if $E^0 \cong E(M)$ and $E^i \cong E(\mathrm{coker}(d^{i-2}))$, for every $i \geq 1$.

Two minimal injective resolutions are always isomorphic. We denote with $\mathrm{injdim}_R(M)$ (or without R if it is clear) the length of the shortest injective resolution of M. It is called **injective dimension** of M and it can be proved that it is the length of any minimal injective resolution of M.

So if $E^\bullet$ is a minimal injective resolution of M, and $n = \mathrm{injdim}(M)$, then $E^i = 0$, for every $i > n$.

Proposition 5.3.4. *Every injective R-module E can be written in the following form:*

$$E \cong \bigoplus_{\mathfrak{p} \in \mathrm{Spec}(R)} E(R/\mathfrak{p})^{a(\mathfrak{p})},$$

where $a(\mathfrak{p}) \in \mathbb{N} \cup \{\infty\}$.

If $E^\bullet$ is a minimal resolution of M, we can then decompose any module E^i in the same way, so that

$$E^i \cong \bigoplus_{\mathfrak{p} \in \mathrm{Spec}(R)} E(R/\mathfrak{p})^{\mu_i(\mathfrak{p},M)},$$

where $\mu_i(\mathfrak{p}, M) \in \mathbb{N} \cup \{\infty\}$ and it is called **the i-th Bass number of M with respect to $\mathfrak{p}$**. It indicates how many times the injective hull of $R/\mathfrak{p}$ appears in the expression of E^i.

Definition 5.3.5. A ring R is said to be **Gorenstein** if $\mu_i(\mathfrak{p}, M) = \delta_{i,\mathrm{ht}(\mathfrak{p})}$, for every $i \geq 0$ and $\mathfrak{p} \in \mathrm{Spec}(R)$.

It follows that

$$E^i \cong \bigoplus_{\substack{\mathfrak{p} \in \mathrm{Spec}(R), \\ \mathrm{ht}(\mathfrak{p})=i}} E(R/\mathfrak{p}).$$

Therefore, we have that the only injective hulls composing E^i are the ones associated with the primes of height exactly i, and all of them with multiplicity equal to one.

It follows that if $n = \dim(R)$, then $E^n \cong E(R/\mathfrak{m})$, because R is local and $\mathfrak{m}$ is the only ideal of R of height n.

Theorem 5.3.6. *Let $n = \dim(R)$, then R is a Gorenstein ring if and only if $n = \mathrm{injdim}(R)$.*

Proposition 5.3.7. *Denote with $K = R/\mathfrak{m}$, then $\mathrm{Hom}_R(K, E(K)) \cong K$ and $\mathrm{Hom}_R(K, E(R/\mathfrak{q})) = 0$, for every prime $\mathfrak{q} \subsetneq \mathfrak{m}$.*

Let us now examine the concept of finite length module. Recall that a **composition series with simple factors** is a chain of the form

$$0 = M_0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_t = M,$$

where M_i are submodules of M and every composition factor M_{i+1}/M_i is **simple**, i.e. it has only M_{i+1}/M_i and 0 as submodules.

Definition 5.3.8. The **length** of the R-module M is the minimal length of a composition series with simple factors. It is denoted by $l(M)$.

Proposition 5.3.9. *If M is a simple R-module, then $M \cong R/\mathfrak{m}$.*

Therefore, if M has a composition series with simple factors, denoted as above, then $M_{i+1}/M_i \cong R/\mathfrak{m}$, for every i.

Theorem 5.3.10 (Matlis' duality)**.** *If M is an R-module of finite length and $E = E(R/\mathfrak{m})$, then*

$$M \cong \operatorname{Hom}_R(\operatorname{Hom}_R(M, E), E).$$

Now that we have recalled all the properties and definitions we needed, we can prove other preliminary results, leading to the theorem that provides the desired application of Bourbaki's Theorem.

Proposition 5.3.11. *Let R be a Gorenstein ring, M an R-module of finite length and $n = \dim(R) = \operatorname{injdim}(R)$. Let then*

$$\begin{tikzcd} 0 \arrow[r] & R \arrow[r] & E^0 \arrow[r] & \cdots \arrow[r] & E^h \arrow[r] & \cdots \arrow[r] & E^n \arrow[r] & 0 \end{tikzcd}$$

be a minimal injective resolution of R. We have that:

(1) $\operatorname{Hom}_R(M, E^h) = 0$*, for every $h < n$.*

(2) $\operatorname{Ext}^i_R(M, R) = 0$*, for every $0 \leq i < n$ and* $\operatorname{Ext}^n_R(M, R) \cong \operatorname{Hom}_R(M, E(R/\mathfrak{m}))$.

Proof. (1) Let us proceed by induction on $t = l(M)$.

If $l(M) = 0$, then $M = 0$ and (1) is proved. Suppose $t > 0$, then there exists a submodule $N \subsetneq M$, such that $M/N \cong R/\mathfrak{m}$ and $l(N) = t - 1$. We have the short exact sequence:

$$\begin{tikzcd} 0 \arrow[r] & N \arrow[r] & M \arrow[r] & M/N \arrow[r] & 0. \end{tikzcd}$$

Apply the contravariant functor $\operatorname{Hom}_R(-, E^h)$, for $h < n$, which is exact, because E^h is an injective module. So we obtain the exact sequence

$$\begin{tikzcd} 0 \arrow[r] & \operatorname{Hom}_R(R/\mathfrak{m}, E^h) \arrow[r] & \operatorname{Hom}_R(M, E^h) \arrow[r] & \operatorname{Hom}_R(N, E^h) \arrow[r] & 0. \end{tikzcd}$$

By induction hypothesis, we have $\mathrm{Hom}_R(N, E^h) = 0$. By the definition of Gorenstein ring, we have

$$\mathrm{Hom}_R(R/\mathfrak{m}, E^h) \cong \bigoplus_{\substack{\mathfrak{p}\in\mathrm{Spec}(R),\\ \mathrm{ht}(\mathfrak{p})=h}} \mathrm{Hom}_R(R/\mathfrak{m}, E(R/\mathfrak{p})),$$

which is zero, by Proposition 5.3.7. It follows that $\mathrm{Hom}_R(M, E^h) = 0$, for every $h < n$.

(2) In order to determine $\mathrm{Ext}^i_R(M, R)$ we need an injective resolution of R, so let us take the one in the statement of the theorem. Then we apply the covariant functor $\mathrm{Hom}_R(M, -)$ and obtain the complex

$$\begin{tikzcd} 0 \arrow[r] & \mathrm{Hom}_R(M,R) \arrow[r] & 0 \arrow[r] & \cdots \arrow[r] & 0 \arrow[r] & \mathrm{Hom}_R(M, E(R/\mathfrak{m})) \arrow[r, "f"] & 0, \end{tikzcd}$$

where we have applied again Proposition 5.3.7 to middle terms and the fact that $E^n = E(R/\mathfrak{m})$, if n is the injective dimension of R and R is Gorenstein.

It follows that $\mathrm{Ext}^n_R(M, R) = \ker(f)/\{0\} = \mathrm{Hom}_R(M, E(R/\mathfrak{m}))$ and also $\mathrm{Ext}^i_R(M, R) = 0$ for every other i.

$\square$

Under the same assumptions, it follows from Matlis' Duality that:

$$\mathrm{Ext}^i_R(\mathrm{Ext}^i_R(M,R),R) = 0,\ \forall i < n \text{ and } \mathrm{Ext}^n_R(\mathrm{Ext}^n_R(M,R),R) \cong M.$$

Proposition 5.3.12 ([3], Proposition 7)**.** *Let R be a Gorenstein ring, with* $\dim(R) = n$*, let* $0 \neq M$ *be a finitely generated R-module, with* $\mathrm{depth}_R(M) = t$*. Then*

$$n - t = \max\{i \mid \mathrm{Ext}^i_R(M, R) \neq 0\}.$$

Since $n = \mathrm{injdim}(R)$, we already know that $\mathrm{Ext}^i_R(M, R) = 0$, for every $i \geq n+1$. This proposition states that $\mathrm{Ext}^i_R(M, R) = 0$, for every $i \geq n - t + 1$.

Proof. Let us proceed by induction on t. If $t = 0$, it means that we cannot find a non-zero divisor for M inside $\mathfrak{m}$, so that $\mathfrak{m}$ is an associated prime of M. It follows that we have an inclusion $0 \longrightarrow R/\mathfrak{m} \xrightarrow{f} M$. If we call $N = M/\operatorname{Im} f$, we obtain the short exact sequence

$$\begin{tikzcd} 0 \arrow[r] & R/\mathfrak{m} \arrow[r, "f"] & M \arrow[r] & N \arrow[r] & 0. \end{tikzcd}$$

As observed above, since $n = \mathrm{injdim}(R)$, we have $\mathrm{Ext}^i_R(M, R) = 0$, for every $i > n$. Hence, if we write the long exact sequence associated to $\mathrm{Ext}_R(-, R)$, we obtain

$$\cdots \longrightarrow \operatorname{Ext}^n_R(M,R) \xrightarrow{\tilde{f}} \operatorname{Ext}^n_R(R/\mathfrak{m},R) \longrightarrow \operatorname{Ext}^{n+1}_R(N,R) \longrightarrow \cdots .$$

It follows that $\operatorname{Ext}^n_R(M,R) \xrightarrow{\tilde{f}} \operatorname{Ext}^n_R(R/\mathfrak{m},R)$ is surjective. By (2) of Proposition 5.3.11, we know that

$$\operatorname{Ext}^n_R(R/\mathfrak{m},R) \cong \operatorname{Hom}_R(R/\mathfrak{m},E(R/\mathfrak{m})) \cong R/\mathfrak{m} \neq 0,$$

where the last isomorphism is given by Proposition 5.3.7. We conclude that $\operatorname{Ext}^n_R(M,R) \neq 0$. Note that $n = n - t = n - 0$ and also $\operatorname{Ext}^i_R(M,R) = 0$, for every $i > n$; so n is the maximum we needed.

Assume the thesis holds for every $0 \leq s < t$. As just said, $t > 0$, so there exists $x \in \mathfrak{m}$ a non-zero divisor for M. Then we have that $\operatorname{depth}_R(M/xM) = t-1$. Using the inductive hypothesis, we obtain $\operatorname{Ext}^{n-t+1}_R(M,R) \neq 0$ and $\operatorname{Ext}^j_R(M,R) = 0$, for every $j > n-t+1$. Since x is a non-zero divisor for M, we have the short exact sequence

$$0 \longrightarrow M \xrightarrow{\cdot x} M \longrightarrow M/xM \longrightarrow 0.$$

Let us write the long exact sequence for $\operatorname{Ext}_R(-,R)$:

$$\cdots \longrightarrow \operatorname{Ext}^i_R(M,R) \xrightarrow{\cdot x} \operatorname{Ext}^i_R(M,R) \longrightarrow \operatorname{Ext}^{i+1}_R(M/xM,R) \longrightarrow \cdots .$$

We have that, for every $i \geq n-t+1$ (i.e. $i+1 > n-t+1$), $\operatorname{Ext}^{i+1}_R(M/xM,R) = 0$, hence $\operatorname{Ext}^i_R(M,R) \xrightarrow{\cdot x} \operatorname{Ext}^i_R(M,R)$ is surjective. Therefore $\operatorname{Ext}^i_R(M,R) = (x) \cdot \operatorname{Ext}^i_R(M,R)$. However, $\operatorname{Ext}^i_R(M,R)$ is a finitely generated module over a local Noetherian ring, hence by Nakayama's Lemma it follows that $\operatorname{Ext}^i_R(M,R) = 0$, for every $i \geq n-t+1$.

It remains to prove that $\operatorname{Ext}^{n-t}_R(M,R) \neq 0$, then we have that $n-t$ is the desired maximum. Let us rewrite the long sequence for $i = n-t$:

$$\cdots \longrightarrow \operatorname{Ext}^{n-t}_R(M,R) \longrightarrow \operatorname{Ext}^{n-t+1}_R(M/xM,R) \longrightarrow \operatorname{Ext}^{n-t+1}_R(M,R) \longrightarrow \cdots .$$

However, $\operatorname{Ext}^{n-t+1}_R(M,R) = 0$ and then $\operatorname{Ext}^{n-t}_R(M,R) \longrightarrow \operatorname{Ext}^{n-t+1}_R(M/xM,R)$ is surjective, with $\operatorname{Ext}^{n-t+1}_R(M/xM,R) \neq 0$. We conclude that $\operatorname{Ext}^{n-t}_R(M,R) \neq 0$.

□

We obtain a corollary from the previous proposition, however before stating it, we need the notion of maximal submodule of finite length. Let us give two lemmas, in order to understand the definition (see Section 10.52 of [2]).

Lemma 5.3.13. *Let M be a finitely generated R-module, such that $M \neq 0$ and $\mathfrak{m}^n \cdot M = 0$, for some $n \in \mathbb{N}^*$. Then M has finite length.*

Proof. We can write the following composition series for M:

$$0 = \mathfrak{m}^n M \subsetneq \mathfrak{m}^{n-1} M \subsetneq \cdots \subsetneq \mathfrak{m} M \subsetneq M.$$

This composition series is not necessarily with simple factors. We notice that $\mathfrak{m} \cdot \dfrac{\mathfrak{m}^k M}{\mathfrak{m}^{k+1} M} = \overline{0}$, so every quotient module is a finitely generated $(R/\mathfrak{m})-$vector space. It follows that every $\dfrac{\mathfrak{m}^k M}{\mathfrak{m}^{k+1} M}$ has finite length (equal to its dimension). It also follows that

$$l(M) = \sum_{k=0}^{n-1} l\left(\frac{\mathfrak{m}^k M}{\mathfrak{m}^{k+1} M}\right) < \infty.$$

□

Lemma 5.3.14. *Let M be an R-module with finite length. Then $\mathfrak{m}^n \cdot M = 0$, for some $n \in \mathbb{N}$.*

Proof. Suppose by contradiction that $\mathfrak{m}^n \cdot M \neq 0$, for every $n \in \mathbb{N}$. Take $x \in M$, $f_1, \ldots, f_n \in \mathfrak{m}$, such that $f_1 \cdot \ldots \cdot f_n \cdot x \neq 0$. We can construct the following chain:

$$0 \subsetneq \langle f_1 \cdot \ldots \cdot f_n \cdot x \rangle_R \subsetneq \langle f_1 \cdot \ldots \cdot f_{n-1} \cdot x \rangle_R \subsetneq \cdots \subsetneq \langle x \rangle_R \subseteq M.$$

All containments are strict because if for example $\langle f_1 f_2 x \rangle_R = \langle f_1 x \rangle_R$, there exists $g \in R$, such that $f_1 x = g f_1 f_2 x$. Consequently $(1 - g f_2) f_1 x = 0$. However, $(1 - g f_2) \in U(R)$, because otherwise $(1 - g f_2),\ g f_2 \in \mathfrak{m}$, so $1 \in \mathfrak{m}$. which is a contradiction.

We obtain $f_1 x = 0$, but this is a contradiction, by definition of x and f_i. We can repeat this process for every n and so obtain an arbitrarily long composition series with simple factors. We conclude that $l(M) = \infty$, which is a contradiction.

□

We discover that, if M is finitely generated, its submodules of finite length are the ones annihilated by some power of the maximal ideal $\mathfrak{m}$. We then define the following submodule:

$$M' = \{x \in M \mid \mathfrak{m}^n \cdot x = 0, \text{ for some } n \in \mathbb{N}\}.$$

Hence this is the set of all the elements of M which are $\mathfrak{m}$-torsion.

Remark 5.3.15. Let us prove that M' is the **maximal submodule of finite length** of M.

Proof. First of all, since M' is finitely generated, assume $M' = \langle x_1, \dots, x_n \rangle_R$, we can consider $N = \max_i \{n \mid \mathfrak{m}^n \cdot x_i = 0\}$. It follows that $\mathfrak{m}^N \cdot M' = 0$, hence, by Lemma 5.3.13 we conclude that M' has finite length.

Let us now prove that M' is maximal among the submodules of M with finite length. Assume that $N \subseteq M$ has finite length. By Lemma 5.3.14 we know that $\mathfrak{m}^n \cdot N = 0$, for some n. It follows that $N \subseteq M'$.

□

We are now ready for the Corollary of Proposition 5.3.12.

Corollary 5.3.16 ([3], Corollary 8)**.** *Let R be a Gorenstein ring of dimension n, M be a finitely generated R-module. Let denote with M' the maximal submodule of finite length of M. Then the natural map:* $\operatorname{Ext}^n_R(M,R) \to \operatorname{Ext}^n_R(M',R)$ *is an isomorphism.*

Proof. Let denote $M'' = M/M'$, then $\operatorname{depth}_R(M'') > 0$. In fact, if by contradiction there is no non-zero divisor for M'' inside $\mathfrak{m}$, it means that $\mathfrak{m} \in \operatorname{Ass}_R(M'')$. Therefore $\mathfrak{m} = \operatorname{ann}_R(\overline{x})$, with $\overline{x} \in M/M'$, $x \notin M'$. It immediately follows that $\mathfrak{m} \cdot x \subseteq M'$, hence $x \in M'$, by definition of the latter. However, this is a contradiction, so $\operatorname{depth}_R(M'') > 0$.

The natural map between Ext_R modules in the statement of the corollary is the one induced by the inclusion: $M' \to M$. This arrow is part of the short exact sequence:

$$\begin{tikzcd} 0 \arrow[r] & M' \arrow[r] & M \arrow[r] & M'' \arrow[r] & 0. \end{tikzcd}$$

We know that $\operatorname{depth}_R(M'') = t > 0$, so, if we apply Proposition 5.3.12 to M'', we obtain that

$$n - t = \max\{i \mid \operatorname{Ext}^i_R(M'',R) \neq 0\} < n,$$

hence $\operatorname{Ext}^n_R(M'',R) = 0$.

Let us write the long exact sequence derived from the short one above, associated to $\operatorname{Ext}_R(-,R)$:

$$\begin{tikzcd} \cdots \operatorname{Ext}^n_R(M'',R) \arrow[r] & \operatorname{Ext}^n_R(M,R) \arrow[r] & \operatorname{Ext}^n_R(M',R) \arrow[r] & \operatorname{Ext}^{n+1}_R(M'',R) \cdots \end{tikzcd}$$

We have that $\operatorname{Ext}^n_R(M'',R) = \operatorname{Ext}^{n+1}_R(M'',R) = 0$, so we have concluded, since $\operatorname{Ext}^n_R(M,R) \cong \operatorname{Ext}^n_R(M',R)$.

□

We are finally ready to give the application of Bourbaki's Theorem.

Theorem 5.3.17 ([3], Theorem C'). *Let* $(R, \mathfrak{m})$ *be a local Noetherian domain, which is also Gorenstein and integrally closed, with* $\dim(R) = n \geq 2$*; let then* M *be an* R*-module of finite length. We have that* M *can be embedded in a cyclic* R*-module of finite length.*

Proof. First of all, M of finite length implies that M is finitely generated, otherwise, if $\{x_i\}_{i\in I}$ is a system of minimal generators for M, then we have the composition series:

$$0 \subsetneq \langle x_1 \rangle_R \subsetneq \langle x_1, x_2 \rangle_R \subsetneq \cdots ,$$

so $l(M)$ cannot be finite.

So M is finitely generated, hence we have a presentation of M:

$$\begin{tikzcd} 0 \arrow[r] & K \arrow[r] & G \arrow[r] & M \arrow[r] & 0, \end{tikzcd}$$

where G is a finitely generated free R-module, $K \subseteq G$. The R-module K is a submodule of a free one, so it is torsion-free (besides being finitely generated); hence we can apply Bourbaki's Theorem to it. We then obtain an ideal $I \subseteq R$ and a short exact sequence

$$\begin{tikzcd} 0 \arrow[r] & F \arrow[r] & K \arrow[r] & I \arrow[r] & 0, \end{tikzcd}$$

with F free. Consequently $\operatorname{Ext}^i_R(F, R) = 0$, for every $i \geq 1$, since we need a projective resolution of F in order to determine the Ext, however F is free, hence projective. So we can choose the trivial resolution of F, which concludes the argument. Now, we write the long exact sequence associated to $\operatorname{Ext}_R(-, R)$, relative to the second short sequence:

$$\begin{tikzcd} \cdots \arrow[r] & \operatorname{Ext}^{n-1}_R(I, R) \arrow[r] & \operatorname{Ext}^{n-1}_R(K, R) \arrow[r] & \operatorname{Ext}^{n-1}_R(F, R) \arrow[r] & \cdots . \end{tikzcd}$$

We know from the assumptions that $n \geq 2$, so $n - 1 \geq 1$, thus $\operatorname{Ext}^{n-1}_R(F, R) = 0$ and $\begin{tikzcd} \operatorname{Ext}^{n-1}_R(I, R) \arrow[r] & \operatorname{Ext}^{n-1}_R(K, R) \end{tikzcd}$ is surjective.

Now, we write the same long exact sequence, but relative to the firs short sequence:

$$\begin{tikzcd} \cdots \operatorname{Ext}^{n-1}_R(G, R) \arrow[r] & \operatorname{Ext}^{n-1}_R(K, R) \arrow[r] & \operatorname{Ext}^{n}_R(M, R) \arrow[r] & \operatorname{Ext}^{n}_R(G, R) \cdots . \end{tikzcd}$$

For the same reason as above, $\operatorname{Ext}^{n-1}_R(G, R) = \operatorname{Ext}^n_R(G, R) = 0$, since also G is free. This yields to $\operatorname{Ext}^{n-1}_R(K, R) \cong \operatorname{Ext}^n_R(M, R)$.

Finally, given the following short exact sequence

$$\begin{tikzcd} 0 \arrow[r] & I \arrow[r] & R \arrow[r] & R/I \arrow[r] & 0, \end{tikzcd}$$

we obtain, by the same argument, $\mathrm{Ext}_R^{n-1}(I,R) \cong \mathrm{Ext}_R^n(R/I,R)$, since R is free. We conclude that we can find a surjective map $\mathrm{Ext}_R^n(R/I,R) \longrightarrow \mathrm{Ext}_R^n(M,R)$.

Let $I = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_t$ be an irredundant primary decomposition for I. We can assume that $M \neq 0$ (if $M = 0$, M itself is cyclic); therefore $\mathrm{Ext}_R^n(M,R) \neq 0$. In fact, if $\mathrm{Ext}_R^n(M,R) = 0$, then

$$M \cong \mathrm{Ext}_R^n(\mathrm{Ext}_R^n(M,R),R) = 0,$$

which contradicts the assumption.

We conclude that $\mathrm{Ext}_R^n(R/I,R) \neq 0$. Denote $\mathrm{depth}_R(R/I) = s$, we know that R/I is finitely generated, so by Proposition 5.3.12 we obtain:

$$n - s = \max\{i \mid \mathrm{Ext}_R^i(R/I,R) \neq 0\}.$$

However we know that this maximum is already equal to n, since $\mathrm{Ext}_R^n(R/I,R) \neq 0$. Thus $n - s = n$, so $s = \mathrm{depth}_R(R/I) = 0$. This means that $\mathfrak{m} \in \mathrm{Ass}_R(R/I)$, hence one of the $\mathfrak{q}_i$ in the primary decomposition of I is such that $\sqrt{\mathfrak{q}_i} = \mathfrak{m}$. Assume for instance that $\sqrt{\mathfrak{q}_1} = \mathfrak{m}$.

We claim that the maximal submodule of finite length of $H = \displaystyle\bigoplus_{i=1}^{t} R/\mathfrak{q}_i$ is $R/\mathfrak{q}_1$. Set M' that maximal submodule.

Since R is Noetherian, there exists $N \in \mathbb{N}^*$, such that $(\sqrt{\mathfrak{q}_1})^N = \mathfrak{m}^N \subseteq \mathfrak{q}_1$. Thus $\mathfrak{m}^N \cdot R/\mathfrak{q}_1 = \overline{0}$, so $R/\mathfrak{q}_1 \subseteq M'$.

On the other hand, suppose that $\overline{x} \in H$ is such that $\mathfrak{m}^k \cdot \overline{x} = \overline{0}$, in H, for some $k \in \mathbb{N}^*$. Write $\overline{x} = (\overline{x_1}^1, \ldots, \overline{x_t}^t)$, where $\overline{x_i}^i \in R/\mathfrak{q}_i$. Fix $i \neq 1$ and denote $\overline{x_i}^i = \overline{x_i}$. We have that:

$$\mathfrak{m}^k \subseteq \mathrm{ann}_R(\overline{x_i}) \ \Rightarrow \ \mathfrak{m} = \sqrt{\mathfrak{m}^k} \subseteq \sqrt{\mathrm{ann}_R(\overline{x_i})},$$

hence $\mathfrak{m} \subseteq \sqrt{\mathrm{ann}_R(\overline{x_i})}$. It follows that $\mathrm{Supp}_R(\langle \overline{x_i} \rangle_R) = V(\mathrm{ann}_R(\overline{x_i})) \subseteq \{\mathfrak{m}\}$, because if $\mathfrak{p}$ is a prime such that $\mathfrak{p} \supseteq \mathrm{ann}_R(\overline{x_i})$, then $\mathfrak{p} \supseteq \sqrt{\mathrm{ann}_R(\overline{x_i})} \supseteq \mathfrak{m}$, so $\mathfrak{p} = \mathfrak{m}$.

Since the primary decomposition of I is irredundant, we have that if $j \neq 1$, then $\sqrt{q_j} \neq \mathfrak{m}$. Set $\sqrt{q_i} = \mathfrak{p}$ $(\neq \mathfrak{m})$. We have that $\langle \overline{x_i} \rangle_{\mathfrak{p}} = 0$, so $\frac{\overline{x_i}}{1} = 0$ in $(R/\mathfrak{q}_i)_{\mathfrak{p}}$. This implies that there exists $s \notin \mathfrak{p}$, such that $\overline{x_i} \cdot s = \overline{0}$ in $R/\mathfrak{q}_i$. Hence $x_i \cdot s \in \mathfrak{q}_i$, but $s \notin \mathfrak{p}$ and $\mathfrak{q}_i$ is $\mathfrak{p}$-primary, so $x_i \in \mathfrak{q}_i$. We conclude that $\overline{x_i}^i = \overline{0}^i$, hence $\overline{x} = (\overline{x_1}^1, 0, \dots, 0) \in R/\mathfrak{q}_1$. We have proved that $M' \subseteq R/\mathfrak{q}_1$, hence they are equal.

It follows by Corollary 5.3.16 that $\mathrm{Ext}^n_R(\bigoplus_i R/\mathfrak{q}_i, R) \cong \mathrm{Ext}^n_R(R/\mathfrak{q}_1, R)$. Define the map

$$\begin{tikzcd}
0 \arrow[r] & R/I \arrow[r] & \bigoplus_i R/\mathfrak{q}_i \\
& \overline{x} \arrow[r, mapsto] & (\overline{x}^1, \dots, \overline{x}^t).
\end{tikzcd}$$

This is injective, because if $(\overline{x}^1, \dots, \overline{x}^t) = \overline{0}$, then $x \in \mathfrak{q}_1 \cap \dots \cap \mathfrak{q}_t = I$. We can complete this map to a short exact sequence and then write the long exact sequence associated to it, and obtain a map:

$$\begin{tikzcd}
\mathrm{Ext}^n_R(R/\mathfrak{q}_1, R) \arrow[r] & \mathrm{Ext}^n_R(R/I, R) \arrow[r] & 0,
\end{tikzcd}$$

which is surjective and also give us a surjective map

$$\begin{tikzcd}
\mathrm{Ext}^n_R(R/\mathfrak{q}_1, R) \arrow[r] & \mathrm{Ext}^n_R(M, R) \arrow[r] & 0.
\end{tikzcd}$$

By (2) of Proposition 5.3.11, this is the same as having a surjective map:

$$\begin{tikzcd}
\mathrm{Hom}_R(R/\mathfrak{q}_1, E(R/\mathfrak{m})) \arrow[r] & \mathrm{Hom}_R(M, E(R/\mathfrak{m})) \arrow[r] & 0.
\end{tikzcd}$$

Now, apply the exact functor $\mathrm{Hom}_R(-, E)$, with $E = E(R/\mathfrak{m})$, in order to obtain:

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Hom}_R(\mathrm{Hom}_R(M, E), E) \arrow[r] & \mathrm{Hom}_R(\mathrm{Hom}(R/\mathfrak{q}_1, E), E),
\end{tikzcd}$$

which by Matlis' Duality is equivalent to

$$\begin{tikzcd}
0 \arrow[r] & M \arrow[r] & R/\mathfrak{q}_1.
\end{tikzcd}$$

We note that $R/\mathfrak{q}_1 = \langle \overline{1} \rangle_R$, so it is a cyclic R-module of finite length, and this concludes the proof.

$\square$

5.4 Corollaries of Forster-Swan in Dedekind domains

In this section we examine Dedekind domains, which are a specific type of integrally closed domains. In particular, we give some consequences of the Forster-Swan Theorem.

Definition 5.4.1. Let D be an integrally closed Noetherian domain, with Krull dimension d. It is called a **Dedekind domain** if $d \leq 1$.

Corollary 5.4.2 (of Forster-Swan)**.** *Let D be a Dedekind domain, $I \subseteq D$ an ideal, then I is minimally generated by at most two elements.*

A Dedekind domain D is locally a PID, where every ideal is generated by only one element; this result partially extend this property to the global case, stating that two elements are enough to generate every ideal in D.

Proof. Set $X = j - \operatorname{Spec}(D)$, as in the proof of the Forster-Swan' Theorem.

If $\dim(D) = 0$, then D is a field, because it is also a domain, so the statement is trivially true. Assume $\dim(D) = 1$. So, as we have seen before, we have that $D_{\mathfrak{p}}$ is a PID, for every $\mathfrak{p} \in \operatorname{Spec}(D)$, hence $I_{\mathfrak{p}}$ is a principal ideal, which implies that $\mu_{\mathfrak{p}}(I) = 1$.

If $\mathfrak{p} \neq (0)$, then $\dim_X(\mathfrak{p}) = 0$, because it cannot exists a chain of the form $(0) \subsetneq \mathfrak{p} \subsetneq \mathfrak{p}_1$ in X, since $\dim(D) \leq 1$ and this is a chain of two primes. Therefore, in this case, $\mu_{\mathfrak{p}}(I) + \dim_X(\mathfrak{p}) = 1$.

If instead $\mathfrak{p} = (0)$, then for the same reason $\dim_X(\mathfrak{p}) \leq 1$ and $\mu_{\mathfrak{p}}(I) = 1$, so $\mu_{\mathfrak{p}}(I) + \dim_X(\mathfrak{p}) \leq 2$. We apply the Forster-Swan Theorem, so that

$$\mu(I) \leq \sup_{\mathfrak{p} \in X} \{\dim_X(\mathfrak{p}) + \mu_{\mathfrak{p}}(M)\} \leq 2.$$

□

Remark 5.4.3. If a Dedekind domain D is also semi-local, i.e. $|\operatorname{Max}(D)| < \infty$, then $(0) \notin X = j - \operatorname{Spec}(D)$, in fact: if $(0) = \bigcap_{\substack{(0) \subseteq \mathfrak{m} \\ \mathfrak{m} \text{ maximal}}} \mathfrak{m}$, however this is a finite intersection of prime ideals, which cannot be prime, and (0) is prime, so this is a contradiction.

By retracing the proof of the corollary, if $I \subsetneq D$ is an ideal, we conclude that

$$\mu(I) \leq \sup_{\mathfrak{p} \in X} \{\dim_X(\mathfrak{p}) + \mu_{\mathfrak{p}}(M)\} = 1,$$

since (0) was the only ideal of D with $\dim_X((0)) > 0$ (unless $D = 0$).

We conclude that D is a PID.

Bibliography

[1] Craig Huneke. *Commutative Algebra Notes*. Available at `http://people.kth.se/ads/commalg-notes/notes3.pdf`. 2011.

[2] The Stacks Project Authors. *Stacks Project*. 2026. URL: `https://stacks.math.columbia.edu`.

[3] M. Auslander. «Remarks on a theorem of Bourbaki». In: *Nagoya Math. J.* 27 (1966), pp. 361–369. ISSN: 0027-7630,2152-6842. URL: `http://projecteuclid.org/euclid.nmj/1118801639`.

Ringraziamenti

Primo fra tutti naturalmente tengo a ringraziare il mio relatore, il Professor De Stefani, per la sua estrema disponibilità e cortesia, per avermi seguito costantemente durante questo anno, per le repentine risposte sia a questioni concettuali che pratiche; oltre che per la sua pazienza, probabilmente necessaria per le peculiari e frenetiche tempistiche di lavoro da me perpetrate nello svolgimento del mio elaborato.

Ringrazio il mio correlatore, il Professor Caminata, il Dipartimento e tutti i Professori che mi hanno accompagnato nel mio percorso, per la disponibilità mostratami e per aver enormemente accresciuto la mia passione nei confronti della matematica.

Ringrazio i miei genitori per avermi sempre sostenuto, per le opportunità e l'affetto che mi hanno donato negli anni e per essere sempre stati al mio fianco, in ogni occasione.

Ringrazio tutti i miei amici e compagni di avventure, di lunga, lunghissima o nuova data, per aver ascoltato e condiviso con me i nostri differenti percorsi di crescita, per le esperienze indimenticabili e il copioso divertimento.

Ringrazio Paola per avermi supportato in ogni ora e in ogni luogo, per aver ciecamente creduto in me, per aver costellato questi anni di splendidi ricordi e sorrisi, preziosi specialmente in questi ultimi mesi particolarmente impegnativi.

Ringrazio i miei compagni di corso, con i quali ho condiviso il mio intero percorso di studio, grazie in particolare per una cosa: nonostante talvolta potessi sembrare come quel fratello che arriva a casa, appoggia lo zaino e subito dopo esce di nuovo, voi mi avete sempre tenuto un posto a tavola, come una grande famiglia quale io reputo che noi studenti rappresentiamo.

Giunto a questo punto cruciale del mio percorso, ci tengo infine a ringraziare un'ultima persona, sebbene io sia convinto che egli conosca già la teoria dei basic elements e dubito che avrà mai bisogno di leggere queste righe. Grazie ad Andrew Wiles, che con la sua instancabile determinazione ha ispirato e acceso in me la scintilla per questa meravigliosa materia.

Grazie a tutti, di cuore.