Universitat de Barcelona
Facultat de Matemàtiques i Informàtica

GRAU DE MATEMÀTIQUES

Treball final de grau

Decomposition theorems of modules over commutative rings

Autor: Guillem Sedó i Torres

Director: Dr. Santiago Zarzuela Armengou
Realitzat a: Departament de Matemàtiques i Informàtica

Barcelona, January 24, 2022

Abstract

The Fundamental Theorem of Finitely Generated Abelian Groups is a very important result that allows us to describe explicitly the finitely generated abelian groups. This theorem can naturally be generalized to finitely generated modules over principal ideal domains. The difficulty arises when we try to extend it to other types of rings. In this work we prove a generalization of this, the decomposition theorem of finitely generated modules over Dedekind domains. We also explore other similar decomposition and we characterize the rings such that all their modules have a decomposition of simple and cyclic modules.

Resum

El Teorema Fonamental dels Grups Abelians Finitament Generats és un resultat molt important que permet descriure de froma explícita com és qualsevol grup abelià finitament generat. Aquest teorema, de manera força natural es pot generalitzar per a mòduls finitament generats sobre dominis d'ideals principals. La dificultat apareix quan l'intentem estendre a altres tipus d'anells. En aquest treball provem una generalització d'aquest, el teorema de descomposició de mòduls finitament generats sobre dominis de Dedekind. A més explorem altres descomposicions similars i caracteritzarem els anells tals que tots els seus mòduls descomposen en simples i en cíclics.

Acknowledgements

I want to thank my tutor Dr. Santiago Zarzuela for his helpful advises and patience. Also for his interest and guidance in this work. Thanks for introducing me to this topic and providing me any reference and answer that I needed.

Also I would like to thank to my family and my friends, who have gave me the motivational support to complete this work, specially to Irene.

Thanks to all of you.

Contents

Introduction

The Fundamental Theorem of Finitely Generated Abelian Groups also known as the Structure Theorem of Finitely Generated Abelian Groups, affirms that: Every finitely generated abelian group can be expressed uniquely as the product of $\mathbb{Z}^n$ and the product of finite number of groups of the form $\mathbb{Z}/p_i^{e_i}\mathbb{Z}$ where $p_i \in Z$ are prime numbers and $e_i \geq 1$.

The history of this theorem is complicated because the theory of groups was not yet well-established when this result was proved. The first apparition of the actual group definition was in 1882. Group theory begins in the mid 19th century with Lagrange, Galois and Cauchy and the first proof of the finite case is credited to Leopold Kronecker in 1870, but did not use a language of groups. The first one who prove it with this language was Ferdinand Georg Frobenius and Ludwig Stickelberger in 1878. Poincaré did the finitely generated case with a matrix approach proof that is easily adaptable for proving the Fundamental Theorem of Finitely Generated Modules over a Principal Ideal Domain.

The natural generalization of the abelian case is when we consider a module over a principal ideal domain. Since every abelian group is a $\mathbb{Z}$-module this generalization makes sense. It is not very hard to prove that every finitely generated module over a PID is the finite direct sum of cyclic modules. In most cases the proof is just an adaptation of the abelian groups proof. In this case the PID rings are characterized, as we will see, by the property that every finitely generated module over this ring is a direct sum of cyclic modules.

Now we can ask that if there is some generalization of the Fundamental Theorem of Finitely Generated Modules over PID. It is credited to Steinitz that he proved a similar result for the finitely generated modules over a Dedekind domain but in 1951 Irving Kaplansky gave a new proof of this result using more general concepts. The decomposition is not as elegant neither simple as in the PID case but gives a good characterization of these modules. At first sight it may seem the same as in the case of PID, but the most notorious difference is that there are modules that can not be decomposed as a direct sum of cyclic modules. In addition this decomposition loses the uniqueness. There is a part that depends on the ideal class group.

At this point we can ask which decomposition of modules in direct sums are, or what are the type of rings that every module decomposes into a direct sum of modules of a specific type.

The main goal of this work is to prove the Decomposition of finitely generated modules over a Dedekind Domain. For doing this we need the Fundamental Theorem of Finitely Generated Modules over PID that we will also prove. We will study the Dedekind domains and we will do some characterizations of this ring.

Memoir Structure

In general, the whole text is mostly self-contained with the exception of the Krull-Schmidt-Remak-Azumaya Theorem and the chapter 5 due to the extension of the proofs of these results. Every ring R in the text is commutative and unitary unless otherwise specified.

In chapter 1 we give the first decomposition of modules. The type of modules that intervenes in the direct sum are the simple modules. This ones are the most facile modules since does not have any nonzero proper submodule. We prove several results with these modules and we reach the characterization when a ring has that every module is the direct sum of simple modules. Finally we state the Krull-Schmidt-Remak-Azumaya Theorem that gives the unicity of the direct sums of simple modules.

In chapter 2 we begin with a wide vision of the various types of modules when the ring is a PID. From these results and characterizations we can prove tha Fundamental Theorem of finitely generated modules over PID. This is the theorem that we will generalize over Dedekind domains.

In chapter 3 we study the Dedekind domains. First of all we begin with a shortly theory of valuations ring that will end with the first characterization of a Dedekind ring. We give various characterisations of these rings to have a better vision of this new object. Finally we do a brief section about the ideal class group that later will have an important role.

Once we have worked with the Dedekind domains we are able to prove the theorem about the decomposition of finitely generated modules over a Dedekind domain. That is what we do in chapter 4. First we give properties and characterizations of some modules types when the ring is a Dedekind domain. From here we can do the theorem. We have to remark that this decomposition is nearly to be cyclic, because when we have a finitely generated module over a Dedekind domain this module is isomorphic to a finite direct sum of cyclic modules except one, that is generated by two elements.

In our last chapter, to close this work, we ask what is the ring that every module is the direct sum of cyclic modules. These rings are very special, they are Artinian principal ideal rings. For proving this theorem we choose a proof where the main tool are the injective modules.

In the appendix we state the basic concepts about the theory of rings and modules. Most of these results will be used in the work. The notion of projective, Noetherianity, tensor product, localisation will be very recurrent throughout the memoir.

Chapter 1

Semisimple Modules and Rings

In this section we begin with the most facile modules type, that is the simple modules. These modules have the most basic and facile structure as a module since do not have any submodules except 0 and himself. Then we explore which modules can be described as a direct sum of simple modules. This gives us a nice characterization.

1.1 Definitions and Properties

Definition 1.1.1 An nonzero R-module S is simple if does not have any nonzero proper submodule. Equivalently S is simple if 0 and S are the only submodules of S.

Proposition 1.1.2 *Let M be a simple R-module. Then $M \cong R/I$ where I is some maximal ideal of R.*

PROOF: Let $x \in M$ a nonzero element. Then $\langle x \rangle \subseteq M$ is a submodule of M but we suposed that M was a simple module. Hence M does not have any proper submodule thus $\langle x \rangle = M$. We can consider the next morphism $p : R \longrightarrow \langle x \rangle = M$ where $p(r) = rx$. It is a epimorphism and by the First Isomorphism Theorem we have that $M \cong R/\ker(p)$. If $\ker(p)$ is not a maximal ideal we have a contradiction because it will exist a maximal ideal $I \supsetneq \ker(p)$. Then $I/\ker(p)$ will be a proper submodule of $R/\ker(p)$. □

Proposition 1.1.3 *Let M be a nonzero Artinian R-module. Then it possesses a simple submodule.*

PROOF: We can consider the collection of all nonzero submodules of M. Since M is Artinian we have that this collection has a minimal element, this will be simple. □

Observation 1.1.4 If R is an Artinian ring we have that every nonzero R-module M has a simple submodule because we can choose a nonzero $m \in M$ and $\langle m \rangle$ it is a finitely generated submodule of M. Hence $\langle m \rangle$ is an Artinian R-module (by Proposition A.3.8) and by the previous proposition it has a simple submodule.

Definition 1.1.5 A nonzero R-module that is the direct sum of simple R-modules is called semisimple. A ring is said to be semisimple if it is semisimple as a module over itself.

Proposition 1.1.6 *Let M be a nonzero R-module. Then M is semisimple if and only if every submodule* *of M is a direct summand of M.*

Proof: First suppose that M is semisimple, that is $M = \bigoplus_{i\in I} S_i$ where S_i are simple modules. Let $N \subseteq M$ be a submodule and let $J \subseteq I$ (by Zorn's lemma) be a maximal subset of I such that $\big(\bigoplus_{i\in J} S_i\big) \cap N = 0$. We denote S by $\bigoplus_{i\in J} S_i$. If $i \in I\backslash J$ then $(S + S_i) \cap N \neq 0$ (by definition of S) hence $(S + N) \cap S_i \neq 0$. Since S_i is simple we have that

$$(S + N) \cap S_i = S_i \quad \Rightarrow \quad S_i \subseteq S + N$$

This is true for every $i \in I\backslash J$, thus $M = S + N$ and $S \cap N = 0$. it follows that N is a direct sumand of M.

For the other implication first we show that every nonzero submodule of M contains a simple module. Let $C \subseteq M$ be a submodule and $c \in C$ any nonzero element. There exists a maximal submodule $D \subseteq C$ which does not contain the element c (by Zorn's lemma). By hypothesis we have that D is a direct summand of C, that is, there exist a submdoule E that $D \oplus E = C$. If E is not simple, then is the direct sum of F and G, two nonzero submodules of E. Thus $C = D \oplus F \oplus G$ and either $D \oplus F$ of $D \oplus G$ does not contain c (otherwise $c \in D = (D \oplus F) \cap (D \oplus G)$ because $F \cap G = 0$). Hence E is simple.

Now let B be a maximal submodule that is the direct sum of simple submodules of M. By hypothesis B is a direct summand and then there exist a submodule N such that $B \oplus N = M$. But N contains a simple module S, and $S \cap B \subseteq N \cap B = \{0\}$. Hence $B \subsetneq B \oplus S$ contradicts the maximality of B. Thus $B = M$ and M is semisimple. □

Theorem 1.1.7 *Let M be a semisimple R-module. Then the following statements are equivalent:*

i) *M is the direct sum of a finite number of simple submodules.*

ii) *M is Noetherian.*

iii) *M is Artinian.*

iv) *M is finitely generated.*

Proof: i)⇒ii) and i)⇒ iii): We know that a simple R-module is Noetherian and Artinian (because does not have any proper submodule). By the Corollary A.3.7 we have that a finite direct sum of simple modules is Noetherian and Artinian. If M is the direct sum of a finite number of simple submodules, these simple submodules are generated by one element, hence M is finitely generated. This establish i)⇒iv).

Now we proceed by contradiction. Suppose that M is not the direct sum of finitely many simple submodules, that is, is the direct sum of infinitely many. Then M has a strictly ascending and descending chains that does not end in a finite number of steps. So if i) is false, then ii) and iii) are false too. Now suppose that M is finitely generated and is semisimple. Then $M = \langle m_1, \ldots, m_n\rangle$ and $M = \bigoplus_{j\in J} S_i$ where S_i are simple R-modules. Then $m_i \in \bigoplus_{j\in J} S_i$ that is, there exists finitely many S_i such that $m_i \in S_{1_i} \oplus \cdots \oplus S_{r_i}$. Hence M is the direct sum of finitely many simple modules because $M = \langle m_1\rangle + \cdots + \langle m_n\rangle$. □

Corollary 1.1.8 *A semisimple ring is the direct sum of a finite number of simple ideals.*

Proof: Since R is generated by one element as an R-module we can apply the previous proposition and get that it is the direct sum of finitely many simple submodules (ideals in this case). □

Proposition 1.1.9 *Every nonzero submodule of a semisimple module is a semisimple module.*

Proof: Let M be a semisimple R-module and N a submodule of N. Let be $H \subseteq N$ a submodule of N, we know that H is also a submodule of M. By the proposition 1.1.6 we have that there exists a submodule $H' \subseteq M$ such that $H \oplus H' = M$. Let $p : M \longrightarrow H$ be the projection defined by $p(h, h') = h$. Since $H \subseteq N$ we can consider $p_{|_N} : N \longrightarrow H$. Now

$$\ker(p_{|_N}) = H' \cap N \quad \text{and} \quad \mathrm{im}\,(p_{|_N}) = H \cap N = H.$$

Hence, the following sequence splits:

$$0 \longrightarrow H' \cap N \xrightarrow{inc} N \xrightarrow{p_{|_N}} H \longrightarrow 0$$

because $p_{|_N} \circ j = \mathrm{Id}_H$ where $j : H \longrightarrow N$ is the inclusion morphism. We can conclude that $N = inc(H' \cap N) \oplus j(H) = (H' \cap N) \oplus H$, that is, H is a direct summand of N. Hence, N is semisimple. □

Proposition 1.1.10 *Any image of a nonzero morphism of a semisimple module is a semisimple module.*

Proof: Let M be a semisimple R-module and $\varphi : M \longrightarrow M'$ a morphsim of R-modules. Then $\mathrm{im}\,(\varphi) \cong M/\ker(\varphi)$, but by Theorem 1.1.7 we have that $\ker(\varphi)$ is a direct summand of M. That is $M = \ker(\varphi) \oplus N$ and then

$$\mathrm{im}\,(\varphi) \cong M/\ker(var) = \big(\ker(\varphi) \oplus N\big)/\ker(var) \cong N$$

Hence $\mathrm{im}\,(\varphi)$ is semisimple by the previous proposition.

Theorem 1.1.11 *Let R be a ring. Then the following conditions on R are equivalent:*

i) *R is semisimple.*

ii) *Every R-module is semisimple.*

iii) *Every R-module is injectve.*

iv) *Every short exact sequence of R-modules splits.*

v) *Every R-module is projective.*

Proof: i)⇒ii): Suppose that R is semisimple. For any R-module M we have the following surjective R-moprhism $\varphi : \bigoplus_{m \in M} R \longrightarrow M$. Since R is semisimple, $\bigoplus_{m \in M} R$ is semisimple too and by the previous Proposition $\mathrm{im}\,(\varphi) = M$ is semisimple.
ii)⇒iii): Suppose that every R-module is semisimple, then for every R-module E and exact sequence $0 \longrightarrow E \xrightarrow{i} A \xrightarrow{p} B \longrightarrow 0$ we have that $i(E) \cong E$ is a direct summand of A (by Proposition 1.1.6). Hence $A \cong E \oplus N$ for some R-module N and $A/\ker(p) \cong B$. But $\ker(p) = \mathrm{im}\,(i) \cong E$, so

$$A/\ker(p) \cong \big(E \oplus N\big)/\mathrm{im}\,(i) \cong \big(E \oplus N\big)/E \cong N \cong B$$

Thus $A \cong E \oplus B$ and the exact sequence is split. By Proposition A.4.10 we have that E is injective.
The implication iii) to iv) is immediate because if every R-module is injective, then every exact sequence splits. The same thing occurs with iv)⇒v) by the Proposition A.4.2.
v)⇒i): Suppose that every R-module is projective, then the following exact sequence is split:

$$0 \longrightarrow I \longrightarrow R \longrightarrow R/I \longrightarrow 0$$

where $I \subseteq R$ is a nonzero ideal of R. Then $R \cong I \oplus R/I$, that is every ideal of R is a direct summand of R. This is a characterization of semisimple modules (done at the Propostion 1.1.6), therefore R is semisimple. □

Remember that the Jacobson radical of a ring R denoted by $J(R)$ is the intersection of all the maximal ideals of R.

Proposition 1.1.12 *Let R be a ring. Then the Jacobson radical of $R/J(R)$ is* 0.

Proof: We have that the maximal ideals of $R/J(R)$ are the maximal ideals of R that contains $J(R)$. But by definition $J(R)$ is the intersection of all the maximal ideals of R, hence every maximal ideal contains $J(R)$. Therefore $J\big(R/J(R)\big) = J(R)/J(R) = 0$. $\square$

Proposition 1.1.13 *A ring R that is Artinian and $J(R) = 0$ it is also semisimple.*

Proof: By the Proposition 1.1.3 we have that R has a nonzero simple ideal I_1. If $I_1 = R$ then we have finished. Otherwise I_1 is a proper ideal of R, so $I_1 \nsubseteq J(R) = 0$, therefore there is a maximal ideal A_1 not containing I_1. Since I_1 is simple, $I_1 \cap A_1$ is either I_1 or 0. If $I_1 \cap A_1 = I_1$ then $I_1 \subseteq A_1$, a contradiction, and so $I_1 \cap A_1 = 0$. Since A_1 is maximal we have that $A_1 \oplus I_1 = R$.
Now if A_1 is simple, then we have finished because R is a direct sum of simple submodules. Otherwise A_1 is Artinian (because is a submodule of an Artinian module) and hence it have a simple ideal $I_2 \subseteq A$. By the previous argument there exists $A_1' \subseteq R$ such that $I_2 \oplus A_1' = R$. With the same argument as the proof of Proposition 1.1.9 we have that $I_2 \oplus A_2 = A_1$ where $A_2 = A_1 \cap A_1'$. This construction can be iterated to produce a strictly decreasing chain of ideals $R \supsetneq A_1 \supsetneq A_2 \supsetneq \cdots$. This chain has to end because R is Artinian. Therefore $R = I_1 \oplus I_2 \oplus \cdots I_n$ and R is semisimple. $\square$

1.2 Krull-Schmidt-Remak-Azumaya Theorem

Now we may ask if a decomposition using simple modules is unique. The answer is affirmative and the theorem of this section is what it says. The proof of this theorem is quite large, by a lack of space, we will not prove it. We have to remark that the proof of this result uses Schröder-Bernstein Theorem, therefore is not an easy demostration. It can be found at [12], Theorem 3.13.

Definition 1.2.1 An R-module M is said to be indecomposable if $M \neq 0$ and the only direct summand of M are 0 and M.

Definition 1.2.2 Let R be a ring (not necessary commutative). Then is said to be quasi local if the set of non units is nonempty and is closed under addition.

Theorem 1.2.3 (Krull-Schmidt-Remak-Azumaya) *Let M be an R-module and suppose that $\{M_i\}_{i\in I}$ and $\{N_j\}_{j\in J}$ are families of submodules of M such that*

$$\bigoplus_{i\in I} M_i = M = \bigoplus_{j\in J} N_j$$

Suppose further that each M_i and N_j has a quasi local ring of endomorphisms. Then there is a one to one correspondence between the families of $\{M_i\}_{i\in I}$ and $\{N_j\}_{j\in J}$ such that corresponding modules are isomorphic.

Proposition 1.2.4 *Let S be a simple R-module. Then the ring of endomorphism of S is a division ring, that is, every element has inverse.*

Proof: Suppose that $S \neq 0$ is a simple R-module. Then its ring of endomorphisms is nontrivial. Let f be a nonzero element of $\mathrm{Hom}_R(S,S)$. Then $f(S)$ is a nonzero submodule of S, so it has to be S (because S is simple). Also $\ker(f)$ is a submodule of S and it can not be S, so it must be 0. Hence f is an isomorphism and so it has inverse. In particular it is quasi local. □

Corollary 1.2.5 *Let $\{E_i\}_{i\in I}$ and $\{F_j\}_{j\in J}$ be families of simple R-modules such that*

$$\bigoplus_{i\in I} E_i \cong \bigoplus_{j\in J} F_j$$

Then there is a one to one correspondence between the two families such that corresponding modules are isomorphic.

Proof: It is immediate after the previous considerations. □

The following concepts will be used in chapter 5, but we will introduce it now because they have a strong relation to Krull-Schmidt-Remak-Azumaya Theorem.

Definition 1.2.6 Let M be an R-module. We denote by $S(M)$ the sum of all the simple submodules of M and is called the socle of M. In the case when M has no simple submodules, then $S(M)$ becomes the zero submodule of M, it is a convention.

Observation 1.2.7 The socle $S(M)$ of a module M is semisimple. Moreover it is the unique maximal semisimple submodule of M. Also, an isomorphism between modules restricts to an isomorphism of their socles. Then given any module M we can express the socle of M as follows

$$S(M) = \bigoplus_{i\in I} S_i$$

where S_i are simple submodules of M.

Corollary 1.2.8 *Let M be an R-module. Then the cardinal number $|I|$ only depends on the module, where I is the set such that $S(M) = \bigoplus_{i\in I} S_i$.*

Proof: Suppose that $S(M) = \bigoplus_{i\in I} S_i = \bigoplus_{j\in J} S'_j$ where S_i, S'_j are simple submodules of M. Then by the Corollary 1.2.5 we have that the cardinal of I and J are equal. Therefore the cardinal number $|I|$ only depends on M. □

Definition 1.2.9 Let M be an R-module and I be the set defined on the previous Corollary. Since the cardinal number $|I|$ only depends on M we denote this cardinal number by $c(M)$, in other words $c(M) = |I|$. Note that $c(M) = 0$ if and only if $S(M) = 0$.

Chapter 2

Modules over PID

In this section we will prove a generalization of the classification theorem of finitely generated abelian groups. The natural way to do this it is through modules (since a $\mathbb{Z}$-module is an abelian group). We will work with modules over PID rings (principal ideal domain) and lately we will be able to extend to Dedekind rings. In particular we will see that all finitely generated modules over a PID ring can be decomposed in a unique way, very similar to the abelian groups one.
To prove this result will we will divide the module in two parts, that is, we will show that every module is the direct sum of a torsion-free module and a torsion module. Then we will prove that the torsion-free modules are free and finally that the torsion modules can be decomposed in a unique way, first in to direct sum of (p)-primary modules, and then in to direct sum of cyclic (p)-primary modules.

Definition 2.0.1 A ring R is said to be a principal ideal domain if every ideal of R is singly generated and is a domain. Usually a principal ideal domain it is denoted by PID (it is an acronym).

Example 2.0.2 The ring of integers $\mathbb{Z}$ is a PID ring. The proof lies in the fact that the ideal generated by two integers is the same as the ideal generated by its greatest common divisor.
Another example of a PID ring is the ring of polynomials in one variable over a field. In general every euclidean domain is a principal ideal domain. But there are many PID that are not euclidean, like the ring $\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$.

Now we give some elemental results about the PID rings. These propositions will be used without any mention. The proofs of these can be found at reference [11].

Proposition 2.0.3 *Let R be a PID ring. The every nonzero prime ideal is maximal and its generator is an irreducible element.*

Proposition 2.0.4 *Let R be a PID ring. Then R is also a UFD (unique factorization domain).*

Definition 2.0.5 Let R be a commutative ring, and let M be an R-module. If $m \in M$, then its annihilator (or order ideal) is

$$\operatorname{ann}(m) = \{r \in R : rm = 0\}$$

We say that m is a torsion element (or has finite order) if $\operatorname{ann}(m) \neq (0)$; otherwise, m is a torsion-free element (or has infinite order).

Proposition 2.0.6 *If $M = \langle m \rangle$ is a cyclic R-module then $M \cong R/\text{ann}(m)$.*

PROOF: We can define $\varphi : R \longrightarrow M$ by $r \mapsto rm$, then φ is an R-epimorphism and $\ker(\varphi) = \{r \in R : rm = 0\} = \text{ann}(m)$. The First Isomorphism Theorem gives

$$M = \langle m \rangle \cong R/\ker(\varphi) = R/\text{ann}(m)$$

□

Let R be a ring, then it is an R-module and it is cyclic since $\langle 1 \rangle = R$. When R is a PID then all the ideals (submodules of R) are cyclic too. This property can be generalized to modules over PID.

Proposition 2.0.7 *If R is a PID ring then every submodule S of a cyclic R-module $M = \langle m \rangle$ is cyclic.*

PROOF: Let $I = \{a \in R : am \in S\} \subseteq R$, then it is an ideal of R since if $a, b \in I$ then

$$am,\, bm \in S \Rightarrow (a+b)m = am + bm \in S \quad \text{hence} \quad a + b \in I$$

and the scalar multiplication is clear too because if $a \in I$ and $\lambda \in R$ then

$$am \in S \Rightarrow (\lambda a)m = \lambda(am) \in S \Rightarrow \lambda a \in I.$$

We know that R is a PID, this implies $I = dR$ for some $d \in R$ and we will prove that $S = \langle dm \rangle$. This inclusion $\langle dm \rangle \subseteq S$ is trivial, and the other is easy too. Let $x \in S$ then

$$x \in S \Rightarrow x = am \Rightarrow a \in I = dR \Rightarrow a = bd \Rightarrow x = bdm$$

thus $x \in \langle dm \rangle$. □

2.1 Torsion-free, Projective, Injective, Free and Flat Modules over PID

In this section we will characterize and study the modules that are mentioned in the title. We will see that the fact that the ring is a PID makes the properties behaves very well.

Definition 2.1.1 If M is an R-module, where R is a domain, then its torsion submodule tM is defined by

$$tM = \{m \in M : m \text{ is a torsion element, that is, } \text{ann}(m) \neq (0)\}$$

Observation 2.1.2 We can assert that tM is a submodule because R is a domain. Let $m_1, m_2 \in tM$, then there exists $r_1, r_2 \in R$ nonzero such that $r_1 m_1 = 0$ and $r_2 m_2 = 0$. This implies that $r_1 r_2(m_1 + m_2) = 0$ and $r_1 r_2$ is nonzero because R is a domain. Hence $m_1 + m_2 \in tM$. The scalar multiplication property is very similar. Let $m_1 \in tM$ and $r \in R$, then there exists $r_1 \in R$ nonzero such that $r_1 m = 0$. Therefore $r_1 \cdot (rm) = r \cdot (r_1 m) = r \cdot 0 = 0 \Rightarrow rm \in tM$.

Definition 2.1.3 Let R be a domain and let M be an R-module. Then M is torsion if $tM = M$, while M is torsion-free if $tM = \{0\}$.

Examples 2.1.4

i) If R is an integral domain, then $tR = \{0\}$, thus it is a torsion-free module.

ii) If $M = \mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$ where $n > 1$ then it is a $\mathbb{Z}$-module and $tM = \{0\} \oplus \mathbb{Z}/n\mathbb{Z}$.

Proposition 2.1.5 *Let M be an R-module, where R is a domain. Then M/tM is torsion-free.*

Proof: Let $m + tM \neq 0$ in M/tM, in other words that is $m \notin tM$ so that m is a torsion-free element. If $\operatorname{ann}(m + tM) \neq (0)$, then there exists some $r \in R$ with $r \neq 0$ such that $0 = r(m + tM) = rm + tM$, that is $rm \in tM$. Thus, there exists $s \in R$ with $s \neq 0$ and $0 = s(rm) = (sr)m$. Since R is a domain we have $sr \neq 0$ and so $\operatorname{ann}(m) \neq (0)$, this contradicts m being a torsion-free element.

The next theorem characterizes the finitely generated torsion-free modules over PIDs, it is important because all these modules are free. First we prove a little result that will be useful lately.

Proposition 2.1.6 *Let R be a PID ring and $Q = \mathrm{Frac}(R)$. If D is a finitely generated R-submodule of Q then it is cyclic.*

Proof: Since D is finitely generated, there exists $b_i, c_i \in R$ such that $D = \langle b_1/c_1, \ldots, b_m/c_m \rangle$.
Let $c = \prod_i c_i$ and define $f : D \longrightarrow R$ by $f(d) = cd$ for all $d \in D$. Since D is torsion-free, f is an injective R-map, and so D is isomorphic to a submodule of R, that is D is isomorphic to an ideal of R. But R is a PID, so every nonzero ideal in R is isomorphic to R (since they are cyclic torsion-free) or is 0. Hence $D \cong \operatorname{im} \varphi \cong R$ or $D = 0$. □

Theorem 2.1.7 *If R is a PID, then every finitely generated torsion-free R-module M is free of finite rank.*

Proof: We prove the theorem by induction on n where $M = \langle v_1, \ldots, v_n \rangle$.
If $n = 1$, then M is a cyclic R-module then by Proposition 2.0.6 we have $M \cong R/\operatorname{ann}(v_1)$. Since M is torsion-free, $\operatorname{ann}(v_1) = (0)$, so that $M \cong R$ and M is free of rank 1.
For the inductive step, let $M = \langle v_1, \ldots, v_{n+1} \rangle$ and let π be the projection map

$$\pi : M \longrightarrow M/\langle v_{n+1} \rangle$$

and consider $N = t\big(M/\langle v_{n+1} \rangle\big)$. We can define $S = \pi^{-1}(N)$ and applying the First Theores of Isomorphism it follows that

$$M/S \cong \big(M/\langle v_{n+1} \rangle\big)/N \cong \big(M/\langle v_{n+1} \rangle\big)/t\big(M/\langle v_{n+1} \rangle\big).$$

That is, M/S is a torsion-free R-module.

Plainly, M/S can be generated by n elements ($\pi : M \longrightarrow M/S$ the projection map is surjective, then M/S is generated by $v_1 + S, \ldots, v_{n+1} + S$, but $v_{n+1} + S = 0 + S$), since M/S is torsion free then is free with finite rank by the inductive hypothesis. Since free modules are projective, Corollary A.4.4 gives

$$M \cong S \oplus (M/S)$$

Thus, it suffices to prove that $S \cong R$ or $S = \{0\}$. We can observe that S can be described as follows:

$$S = \big\{ m \in M : \overline{m} \in N \big\} = \big\{ m \in M : r\overline{m} = 0 \text{ for some } r \in R \big\} = \big\{ m \in M : rm \in \langle v_{n+1} \rangle \big\}.$$

If $x \in S$, then there is some nonzero $r \in R$ with $rx \in \langle v_{n+1} \rangle$, that is, there is $a \in R$ with $rx = av_{n+1}$. Define $\varphi : S \longrightarrow Q = \mathrm{Frac}(R)$ the fraction field of R, by $x \mapsto a/r$, this map is well defined because if $rx = av_{n+1}$ and $r'x = a'v_{n+1}$ then $a'rx = a'av_{n+1}$ and $ar'x = aa'v_{n+1}$ hence $(a'r - ar')x = a'av_{n+1} -$

$a'av_{n+1} = 0$. Since M is torsion-free we have $a'r - ar' = 0$, in other words, $a/r = a'/r'$ in Q. It is a R-map because if $x, x' \in S$ then we have $rx = av_{n+1}$ and $r'x' = a'v_{n+1}$ for some $a, a' \in R$, thus

$$rr'(x + x') = r'av_{n+1} + ra'v_{n+1} = (r'a + ra')v_{n+1}$$

hence

$$\varphi(x + x') = (r'a + ra')/rr' = a/r + a'/r' = \varphi(x) + \varphi(x')$$

If $x \in S$ and $\lambda \in R$ then $rx = av_{n+1}$ for some $a \in R$ and $r(\lambda x) = \lambda(rx) = \lambda av_{n+1}$ thus $\varphi(\lambda x) = (\lambda a)/r = \lambda\varphi(x)$.
This map is injective since if $\varphi(x) = 0$ then $a/r = 0 \Leftrightarrow r \cdot 0 - a \cdot 1 = 0 \Leftrightarrow a = 0$. But $r \neq 0$ and $rx = av_{n+1} = 0$, this implies that $x = 0$. Now $\operatorname{im}(\varphi) \cong S$ and $S \subseteq M$ then by Proposition A.3.2 S is finitely generated. The proof is completed with the previous Proposition that says that every finitely generated submodule of Q is cyclic. Hence $S \cong \operatorname{im}(\varphi)$ is cyclic. □

Observation 2.1.8 Let $R = k[X, Y]$ where k is a field and $M = \langle X, Y\rangle$. It is an R-module finitely generated and torsion-free but it is not free over R because M needs to be generated by two elements and these are linearly dependent. The hypothesis that M does not satisfy is that R is not a PID ring.

Now we keep doing results about these modules. First we will prove that every submodule of a finitely generated free module is itself free. This gives a first characterization of the finitely generated projective modules.

Corollary 2.1.9 *Let R be a PID. Then the following statements are true:*

i) *Every submodule H of a finitely generated free R-module F is itself free and* $\operatorname{rank}(H) \leq \operatorname{rank}(F)$.

ii) *Every finitely generated projective R-module P is free.*

Proof:

i) Let $H \subseteq F$ a submodule of a finitely generated free R-module $F \cong R^m$. Then H is torsion-free (because F is torsion-free) and is finitely generated (because F is Noetherian, Proposition A.3.2). Now Theorem 2.1.7 says that H is free of finite rank. Let $H \cong R^n$ then we have the following exact chain

$$0 \longrightarrow H \xrightarrow{i} F$$

where i is the inculsion morphism, then $Q = \operatorname{Frac}(R)$ is R-flat, that is

$$0 \otimes_R Q \longrightarrow H \otimes_R Q \longrightarrow F \otimes_R Q$$

is an exact sequence, but $H \otimes_R Q \cong Q^n$ and $F \otimes_R Q \cong Q^m$ are Q-vector spaces of dimension n and m respectively. Since the sequence is exact Q^n is a subspace of Q^m this implies that $n \leq m$.

ii) By Theorem A.4.6, P is a direct summand of a free R-module F. Since P is finitely generated, we may choose F to be finitely generated too. Thus, P is isomorphic to a submodule of F, which is free by the first part of this corollary. □

Corollary 2.1.10 *If an R-module M can be generated by n elements and R is a PID. Then every submodule $S \subseteq M$ can be generated by n or fewer elements.*

Proof: Supose that $M = \langle m_1, \ldots, m_n \rangle$ and $N \subseteq M$ then the following sequence is exact

$$R^n \xrightarrow{\pi} M \longrightarrow 0$$

where π is defined by $\pi(e_i) = m_i$ and $\{e_i\}_{1 \leq i \leq n}$ is the canonical basis of R^n. Since $N \subseteq M$, then we have that $\pi^{-1}(N) \subseteq R^n$. Hence the following sequence is exact:

$$\pi^{-1}(N) \longrightarrow N \longrightarrow 0$$

By the previous corollary we have that $\pi^{-1}(N) \cong R^m$ where $m \leq n$. Then $N = \big\langle \pi(e_1), \ldots, \pi(e_m) \big\rangle$. □

Note that the previous proposition gives a strong property on the submodules of a finitely generated module. This is not true when the ring R is not a PID because R is a module over istelf, so R is singly generated (generated by 1 element). But if R is not a PID then it would have an ideal that it can not be generated with only one element. This example contradicts the previous corollary. Now we characterize the flat modules over a PID ring:

Proposition 2.1.11 *If R is a domain, then every flat R-module M is torsion-free.*

Proof: If M is not torsion-free, then there is a nonzero $m \in M$ with $rm = 0$ for some nonzero $r \in R$. Let $0 \longrightarrow R \xrightarrow{i} \text{Frac}(R)$ be the inclusion. Now $m \otimes 1 \neq 0$ in $M \otimes_R R$, for the map $m \otimes 1 \mapsto m$ is an isomorphism $M \otimes_R R \longrightarrow M$. On the other hand,

$$(1_M \otimes i)(m \otimes 1) = m \otimes 1 = m \otimes \frac{r}{r} = rm \otimes \frac{1}{r} = 0$$

in $M \otimes_R \text{Frac}(R)$, therefore $m \otimes 1$ is a nonzero element in $\ker(1_M \otimes i)$, so that M is not flat. □

Proposition 2.1.12 *If R is a PID, then an R-module M is flat if and only if it is torsion-free.*

Proof: If M is torsion free, then every finitely generated submodule S is torsion-free, hence, free (Theorem 2.1.7), hence flat. Therefore, M itself is flat by [11], Lemma 6.139 (elemental proof) or [11], Corollary 6.162. The converse is the previous proposition. □

Observation 2.1.13 We can apply the Theorem 2.1.7 to this last proposition and we get that a finitely generated module over a PID is flat if and only if it is free.
There are flat modules over a PID that are not free, equivalently, there are torsion-free modules that are not free. One example is the $\mathbb{Z}$-module $\mathbb{Q}$, is torsion-free but is not free since every two elements of $\mathbb{Q}$ are dependent.

Now we prove Corollary 2.1.9 without the finitely generated condition, that is the free module can have infinite rank. The fact that every projective module over PID is free it comes off from the next Theorem.

Theorem 2.1.14 *Let R be a PID.*

i) *Every submodule H of a free R-module F is free and* $\text{rank}(H) \leq \text{rank}(F)$.

ii) *Every projective R-module H is free.*

Proof:

i) We are going to use the statement equivalent to the Axiom of Choice and to Zorn's Lemma, that every set can be well-ordered. In particular, we may assume that $\{x_k : k \in K\}$ is a basis of F having a well-ordered index set K. For each $k \in K$ define

$$F'_k = \langle x_j : j \prec k \rangle \quad \text{and} \quad F_k = \langle x_j : j \preceq k \rangle = F'_k \oplus \langle x_k \rangle$$

note that $F = \bigcup_k F_k$. Define

$$H'_k = H \cap F'_k \quad \text{and} \quad H_k = H \cap F_k$$

Now $H'_k = H \cap F'_k = H_k \cap F'_k$ since $H'_k \subseteq H_k$ and $H_k \subseteq H$, so that

$$H_k/H'_k = H_k/(H_k \cap F'_k) \cong (H_k + F'_k)/F'_k \subseteq F_k/F'_k \cong R$$

Since R is a free R-module and R is a PID, H_k/H'_k is free too, then by the proof of Theorem 2.1.7 we know that $H_k = H'_k$ or $H_k = H'_k \oplus \langle h_k \rangle$, where $h_k \in H_k \subseteq H$ and $\langle h_k \rangle \cong R$. We claim that H is a free R-module with basis the set of all h_k. It will then follow that $\operatorname{rank}(H) \leq \operatorname{rank}(F)$.
Since $F = \bigcup F_k$, each $f \in F$ lies in some F_k. Since K is well-ordered, there is a smallest index $k \in K$ with $f \in F_k$ and we denote this smallest index by $\mu(f)$.
Note that if $h \in H'_k \subseteq F'_k$ then $\mu(h) \prec k$. Let H^* be the submodule of H generated by all the h_k. Suppose that H^* is a proper submodule of H. Let j be the smallest index in

$$\{\mu(h) : h \in H \text{ and } h \notin H^*\}$$

and choose $h' \in H$ to be such an element having index j, that is $h' \notin H^*$ and $\mu(h') = j$. Now $h' \in H \cap F_j = H_j$ because $\mu(h') = j$ and so

$$h' = a + rh_j \quad \text{where } a \in H'_j \text{ and } r \in R$$

Because $H_j = H'_j$ or $H_j = H'_j \oplus \langle h_j \rangle$ (and r can be 0). Thus $a = h' - rh_j \in H'_j$ and $a \notin H^*$, otherwise $h' \in H^*$ (because $h_j \in H^*$). Since $\mu(a) \prec j$ we have contradicted j being the smallest index of an element in H not in H^*. We conclude that $H = H^*$, that is every $h \in H$ is a linear combination of h_k's.
It remains to prove that an expression of any $h \in H$ as a linear combination of h_k is unique. By subtracting two such expressions, it suffices to prove that if

$$0 = r_1 h_{k_1} + \cdots + r_n h_{k_n}$$

then all the coefficients $r_i = 0$. Arrange the terms so that $k_1 \prec \cdots \prec k_n$. If $r_n \neq 0$ then $r_n h_{k_n} \in \langle h_{k_n} \rangle \cap H'_{k_n} = \{0\}$, a contradiction. Therefore, all $r_i = 0$ and so H is a free module with basis $\{h_j : j \in K\}$.

ii) By Theorem A.4.6, P is a direct summand of a free R-module F. Thus P is isomorphic to a submodule of F, which is free by the previous part of this theorem. □

Corollary 2.1.15 *Let R be a PID ring and M an R-module. Then M is free if and only if is projective.*

Proof: One implication is the previous theorem and the other is the Theorem A.4.5. □

At this point, we achieved the characterization of projective modules over PID. This property can be extended over another type of ring. Here we have to mention the work done by Quillen and Suslin for proving that every projective module is free over any polynomial ring $k[X_1, \dots, X_n]$ where k is a field. This result can be thought of as a generalization of the PID case because the ring of polynomials in one variable is a PID ring.

Also, we can explore the injective modules over PID. Here we do a characterization that is motivated in the first chapter, proving that a module is injective if and only if it is divisible. We have to remark that previously in Proposition A.4.16 we saw that every torsion-free divisible R-module is injective where R is a domain. Here we delete the extra condition to the module but we add a condition to the ring.

Proposition 2.1.16 *Let R be a PID ring and M an R-module. Then M is injective if and only if it is divisible.*

Proof: One implication is done in the Proposition A.4.14. Now let's suppose that M is a divisible R-module and let $I \subseteq R$ be any ideal of R. By the Proposition A.4.9 it will be enough to prove that for every R-morphism $h : I \longrightarrow M$ there exists a morphism $g : R \longrightarrow M$ making the following diagram commutative:

$$\begin{tikzcd}
0 \arrow[r] & I \arrow[r, "inc"] \arrow[d, "h"'] & R \arrow[dl, "g"] \\
 & E &
\end{tikzcd}$$

Observe that $I = aR$ for some $a \in R$ because R is a PID. Since M is divisible there exists $m \in M$ such that $h(a) = am$. Now we can define the morphism $g : R \longrightarrow M$ by $g(r) = rm$. Note that if $t \in R$ then $g(t \cdot a) = t \cdot am = t \cdot h(a) = h(t \cdot a)$. So we have $h = g \circ inc$. □

Observation 2.1.17 With the previous proposition we can conclude that if R is a PID then Frac(R) is injective. This is done also in the appendix Example A.4.17. But we have a more strong result that is: every direct sum, product and quotient of injective modules over a PID ring is injective. This is true because any direct sum, product and quotient of divisible modules is a divisible module.

The Proposition 2.1.16 can be generalized to modules over a more wide rings type. We can see at [12], Proposition 2.10, that every divisible module is an injective module when the ring is a Dedekind domain. These rings are a natural generalization of PID rings.

In this section we have seen that a finitely generated torsion-free module is free and is projective. This will be an essential result for the decomposition and it simplifies a lot. The next chapter investigates the torsion part of a module introducing the (p)-primary components.

2.2 Torsion Modules over PID

We remember the definition of torsion module

Definition 2.2.1 Let M be an R-module, where R is a domain. Then its torsion submodule tM is defined by

$$tM = \{m \in M : m \text{ is a torsion element, that is, } \operatorname{ann}(m) \neq (0)\}$$

We say that M is torsion if $tM = M$, while M is torsion-free if $tM = 0$.

Definition 2.2.2 Let M be an R-module and $E \subseteq M$ a submodule then

$$(E : M) = \big\{ r \in R : r \cdot M \subseteq E \big\}$$

is an ideal of R called colon ideal.

Definition 2.2.3 Let R be a PID, M an R-module and (p) a nonzero prime ideal in R. Then M is said to be (p)-primary if for each $m \in M$ there is $n \geq 1$ with $p^n m = 0$.
If M is any R-module, then its (p)-primary component is

$$M_{(p)} = \{ m \in M \mid (0 : m) = (p^n) \text{ for some } n \geq 0 \} = \{ m \in M \mid \operatorname{ann}(m) = (p^n) \text{ for some } n \geq 0 \}$$

Lemma 2.2.4 *Let R be a PID, M an R-module and (p) a nonzero prime ideal of R. Let $m \in M$ such that $(p)^n m = 0$, then $m \in M_{(p)}$.*

Proof: We have to note that if $(p)^n m = 0$ then $(p)^n \subseteq \operatorname{ann}(m)$. That is $(p)^n = \operatorname{ann}(m) \cdot I$ where I is another ideal, but in PIDs we have a divisibility theory for ideals (very similar with the divisibility theory of the elements). Since (p) is a prime ideal it follows that $\operatorname{ann}(m)$ and I are powers of the ideal (p). Therefore $\operatorname{ann}(m) = (p^r) \Rightarrow m \in M_{(p)}$.

With this lemma we note that we can express $M_{(p)}$ by the following way since R is a PID:

$$M_{(p)} = \{ m \in M \mid (p)^n m = 0 \text{ for some } n \geq 1 \} = \{ m \in M \mid p^n m = 0 \text{ for some } n \geq 1 \}$$

Observation 2.2.5 With the notation of the previous lemma we have that the (p)-primary components are submodules of M. This is because if $m_1, m_2 \in M_{(p)}$ then there exist $n_1, n_2 \geq 1$ such that $p^{n_1} m_1 = 0$ and $p^{n_2} m_2 = 0$. Then note that $p^n(m_1 + m_2) = 0$ where $n = \max\{n_1, n_2\}$. Hence $m_1 + m_2 \in M_{(p)}$ by the previous lemma. The proof of the scalar multiplication property is very similar. Let $m \in M_{(p)}$ and $r \in R$, then there exists $n \geq 1$ such that $p^n m = 0$. Therefore $p^n(rm) = rp^n m = r0 = 0$, hence $rm \in M_{(p)}$.

Observation 2.2.6 Let M be a finitely generated (p)-primary module, then $(0 : M) = (p^n)$ for some $n \geq 1$. This is because if $x_1, x_2 \in M$, $\operatorname{ann}(x_1) = (p^{r_1})$ and $\operatorname{ann}(x_2) = (p^{r_2})$ then $(p^r) \subseteq \operatorname{ann}(x_1 + x_2)$ where $r = \max\{r_1, r_2\}$. Also we have that $\operatorname{ann}(x) \subseteq \operatorname{ann}(\lambda x)$ for all $x \in M$ and $\lambda \in R$. Since M is finitely generated we conclude that there is an element with minimal annihilator, and this element is one generator of M.

Proposition 2.2.7 *Let R be a PID, M an R-module and (p) a prime ideal of R. We can consider M_p (the localization of M by p) and the canonical morphism $\varphi_p : M \longrightarrow M_p$. Then we have the following results:*

i) $\ker(\varphi_p) \cap M_{(p)} = \{0\}$.

ii) *For every prime $q \neq p$ then $M_{(q)} \subseteq \ker(\varphi_p)$ and $(M_{(q)})_p = \{0\}$*

iii) *Let $N = \sum_{(q)} M_{(q)}$ where q are prime elements of R then* $\displaystyle\sum_{(q)\neq(p)} M_{(q)} \cap M_{(p)} = \{0\}$

Proof:

i) Note that $\varphi_p(x) = x/1$ is the canonical map, then

$$\begin{aligned}\ker(\varphi_p) = \big\{ m \in M : \varphi_p(m) = 0 \big\} = \big\{ m \in M : m/1 = 0/1 \big\} = \\ = \big\{ m \in M : rm = 0 \text{ where } r \in R \backslash (p) \big\}\end{aligned}$$

If $m \in \ker(\varphi_p) \cap M_{(p)}$ then $p^n m = 0$ and $rm = 0$ for some $n \geq 1$ and $r \in R \backslash (p)$. The greatest common divisor of r and p^n is 1 thus there exists $a, b \in R$ such that $ap^n + br = 1$. It follows that $m = 0$ because

$$m = 1 \cdot m = (ap^n + br)m = ap^n m + brm = 0 + 0 = 0$$

ii) Let $m \in M_{(q)}$ then there exists $n \geq 1$ such that $q^n m = 0$ but $q^n \notin (p)$ thus $q^n \in R \backslash (p)$. Now it follows immediately that $m \in \ker(\varphi_p)$ by the previous result.
The fact that $(M_{(q)})_p = 0$ is because the localization of a submodule of M is isomorphic to the image of the submodule by φ_p. Since $M_{(q)} \subseteq \ker(\varphi_p)$ then

$$\{0\} = \varphi_p(M_{(q)}) \cong (M_{(q)})_p$$

iii) By ii) we have that $M_{(q)} \subseteq \ker(\varphi_p)$ and $\ker(\varphi_p) \cap M_{(p)} = \{0\}$ thus

$$\sum_{(q) \neq (p)} M_{(q)} \subseteq \ker(\varphi_p) \quad \Rightarrow \quad \sum_{(q) \neq (p)} M_{(q)} \cap M_{(p)} = \{0\}$$

□

Theorem 2.2.8 (Primary Decomposition) *Every torsion R-module M over a PID R is a direct sum of its (p)-primary components:*

$$M = \bigoplus_{(p)} M_{(p)}$$

Proof: If $m \in M$ is nonzero, its order ideal $\operatorname{ann}(m) = (d)$ for some $d \in R$. By unique factorization, there are irreducible elements $p_1, \dots, p_n$ no two of which are associates, and positive exponents $e_1, \dots, e_n$ with

$$d = p_1^{e_1} \cdots p_n^{e_n}$$

Since R is a PID then (p_i) is a prime ideal for each i. Define $r_i = d/p_i^{e_i}$, so that $p_i^{e_i} r_i = d$. It follows that $r_i m \in M_{(p_i)}$ for each i. But the gcd of the elements $r_1, \dots, r_n$ is 1 and so there are elements $s_1, \dots, s_n \in R$ with $1 = \sum_i s_i r_i$. Therefore

$$m = \sum_i s_i r_i \in \left\langle \bigcup_{(p)} M_{(p)} \right\rangle$$

With the previous proposition we have that the sum of $M_{(p)}$ is a direct sum, thus

$$M = \bigoplus_{(p)} M_{(p)}$$

□

Now we have that every torsion module over a PID ring can be expressed by the direct sum of its (p)-primary components. This decomposition preserves isomorphisms.

Proposition 2.2.9 *Two torsion modules M and M' over PID are isomorphic if and only if $M_{(p)} \cong M'_{(p)}$ for every nonzero prime ideal (p).*

Proof: If $f : M \longrightarrow M'$ is an R-map, then $f(M_{(p)}) \subseteq M'_{(p)}$ for every prime ideal (p). If f is an isomorphism, then so is f^{-1}, it follows that the restriction $f_{|M_{(p)}} : M_{(p)} \longrightarrow M'_{(p)}$ is an isomorphism.
Conversely, if there are isomorphism $f_{(p)} : M_{(p)} \longrightarrow M'_{(p)}$ for all (p), then there is an ismomorpgism $\varphi : \bigoplus_{(p)} M_{(p)} \longrightarrow \bigoplus_{(p)} M'_{(p)}$ given by $\bigoplus_{(p)} f_{(p)}$. □

2.3 Fundamental Theorem of Finitely Generated Modules

The following result is the first step of the decomposition.

Proposition 2.3.1 *Let R be a PID.*

i) *Every finitely generated R-module M is a direct sum,*

$$M = tM \oplus F$$

where F is a finitely generated free R-module.

ii) *If M and M' are finitely generated R-modules, then $M \cong M'$ if and only if $tM \cong tM'$ and* $\operatorname{rank}(M/tM) = \operatorname{rank}(M'/tM')$

Proof:

i) The quotient module M/tM is finitely generated because M is finitely generated, and it is torsion-free by Proposition 2.1.5(i). Therefore, M/tM is free by Theorem 2.1.7, and hence M/tM is projective. Finally $M \cong tM \oplus (M/tM)$ by Corollary A.4.4.

ii) If $\varphi : M \longrightarrow M'$ is an isomorphism, then $\varphi(tM) \subseteq tM'$ because if $rm = 0$ with $r \neq 0$ then $r\varphi(m) = \varphi(rm) = \varphi(0) = 0$. Hence, $\varphi_{|tM} : tM \longrightarrow tM'$ is an isomorphism with inverse $\varphi^{-1}_{|tM'}$. For the second statement, the map $\overline{\varphi} : M/tM \longrightarrow M'/tM'$ defined by $\overline{\varphi}(m + tM) = \varphi(m) + tM'$ is an isomorphism. Since M/tM is finitely generated torsion-free, it is a free module of finite rank, as is M'/tM' and these are isomorphic if they have the same rank (this is the IBN property that every commutative ring satisfies).
Conversely, if $tM \cong tM'$ by f_1 and $\operatorname{rank}(M/tM) = \operatorname{rank}(M'/tM')$, that is $M/tM \cong M'/tM'$ by f_2. Since $M \cong tM \oplus (M/tM)$ and $M' \cong tM' \oplus (M'/tM')$ then

$$M \cong tM \oplus (M/tM) \cong tM' \oplus (M'/tM') \cong M'$$

where the isomorphism is $f = f_1 \oplus f_2$. □

This proposition allows us to decompose a finitely generated module over a PID in two parts. The torsion-free part and the torsion part. In the previous section we have studied each part but it remains to prove that all (p)-primary module can be expressed by a direct sum of cyclic modules. First of all we will define what a pure submodule is in this context (there are other definitions in other texts).

Definition 2.3.2 Let R be a PID, (p) be a prime ideal of R and let M be a (p)-primary R-module (that is $M = M_{(p)}$). A submodule $S \subseteq M$ is a pure submodule if, for all $n \geq 0$,

$$S \cap p^n M = p^n S$$

Observation 2.3.3 The inclusion $p^n S \subseteq S \cap p^n M$ is true for every submodule $S \subseteq M$, and so it is the reverse inclusion $S \cap p^n M \subseteq p^n S$ that is significant. It says that if $s \in S$ satifies an equation $s = p^n m$ for some $m \in M$ then there exists $s' \in S$ with $s = p^n s'$.

These pure submodules will have an important role on the proof of the Basis Theorem (the theorem that says that every finitely generated R-module is the direct sum of cyclic submodules). The proof of the Basis Theorem is by induction of a dimension defined later. The pure submodules will be the key for proving the induction step. Now we will see that every R-module has a pure submodule when R is a PID.

Lemma 2.3.4 *Let R be a PID, (p) a prime ideal of R and M a (p)-primary finitely generated R-module. Then M has a nonzero pure cyclic submodule. Indeed, if $m \in M$ is an element that has a minimal* $\operatorname{ann}(m)$ *on the set of annihilators, then $\langle m \rangle$ is a pure submodule of M.*

Proof: Since M is finitely generated we can apply the Observation 2.2.6 and we have $(0 : M) = (p^l)$ for some $l \geq 1$, thus there exists some $m \in M$ with $\operatorname{ann}(m) = (p^l)$. This element has the minimal annihilator on the set of annihilators, otherwise $(0 : M) \subsetneq (p^l)$.
Now we claim that $S = \langle m \rangle$ is a pure submodule.
If $s \in S$ then $s = \lambda p^t m$, where $t \geq 0$ and $p \nmid \lambda$, suppose that

$$s = p^n m' \in p^n M$$

for some $m' \in M$, then an element $s' \in S$ with $s = \lambda p^t m = p^n s'$ must be found (if $s = 0$ then $s' = 0$). First note that $n \leq t$ otherwise, if $n > t$ we have a contradiction because

$$0 = p^l m' = p^{l-n} p^n m' = p^{l-n} s = p^{l-n} \lambda p^t m = \lambda p^{l-n+t} m \neq 0$$

since $p \nmid \lambda$, $l - n + t \leq l$ and $(0 : M) = (p^l)$. Hence we can define $s' = \lambda p^{t-n} m \in S$ and

$$p^n s' = p^n \lambda p^{t-n} m = \lambda p^t m = s$$

so that S is a pure submodule. □

Definition 2.3.5 Let M be an R-module with R a PID, then M/pM is a vector space over $R/(p)$ where (p) is a prime ideal of R, we define

$$d(M) = \dim(M/pM)$$

In particular, $d(pM) = \dim(pM/p^2M)$ and more generally

$$d(p^n M) = \dim(p^n M/p^{n+1} M)$$

The next lemma is the base step of the induction of the Basis Theorem. This induction will be on the dimension defined previously.

Lemma 2.3.6 *If M is a finitely generated (p)-primary R-module where R is a PID and (p) a prime ideal, then $d(M) = 1$ if and only if M is a nonzero cyclic R-module.*

Proof: If M is a nonzero cyclic R-module and (p)-primary then $M = \langle m \rangle$ and M/pM is cyclic. Since $\operatorname{ann}(m) = (p^n)$ we have that $p^n M = 0$ but $p^{n-1} M \neq 0$, if we suppose that $M = pM$ then implies that $p^{n-1} M = p^n M = \{0\}$, a contradiction. Hence $M/pM \neq \{0\}$, and so $d(M) = \dim(M/pM) = 1$.
Conversely, if $d(M) = 1$ then $M/pM \cong R/(p)$, hence M/pM is cyclic, say

$$M/pM = \langle m + pM \rangle = pM + \langle m \rangle$$

then

$$p\Big(M/\langle m \rangle\Big) = \big(pM + \langle m \rangle\big)/\langle m \rangle = M/\langle m \rangle$$

now we can do the previous argument. Since M is a (p)-primary R-module then $M/\langle m \rangle$ is also a (p)-primary R-module. It satisfies $p\big(M/\langle m \rangle\big) = M/\langle m \rangle$ and this implies that $M/\langle m \rangle = \{0\}$ hence $M = \langle m \rangle$ then M is cyclic. □

Lemma 2.3.7 *Let M be a finitely generated (p)-primary R-module where R is a PID.*

i) *If $S \subseteq M$, then $d(M/S) \leq d(M)$.*

ii) *If S is a pure submodule of M, then $d(M) = d(S) + d(M/S)$.*

Proof:

i) First we note that $M \otimes_R R/(p) \cong M/pM$ hence the following exact sequence

$$0 \longrightarrow S \xrightarrow{i} M \xrightarrow{p} M/S \longrightarrow 0$$

tensoring by $R/(p)$ it becomes an exact sequence of $R/(p)$-vectorial spaces

$$S/pS \longrightarrow M/pM \longrightarrow (M/S)/p(M/S) \longrightarrow 0$$

thus we have $\dim(M/pM) \geq \dim\Big((M/S)/p(M/S)\Big) \Rightarrow d(M/S) \leq d(M)$.

ii) If S is pure then the inclusion morphism $i : S/pS \longrightarrow M/pM$ is injective. Let $\overline{s} \in \ker(i) \subseteq S/pS \Rightarrow \overline{s} = 0$ in M/pM this implies that $s \in pM \cap S$. Since S is a pure submodule we have that $pM \cap S = pS$ hence $s \in pS \Rightarrow \overline{s} = 0$ in S/pS.
We can conclude that the following sequence of $R/(p)$-vector spaces is exact

$$0 \longrightarrow S/pS \longrightarrow M/pM \longrightarrow (M/S)/p(M/S) \longrightarrow 0$$

and it satisfies $d(M) = d(S) + d(M/S)$. □

The previous lemma gives the tool that we will use to prove the induction step on the Basis Theorem. Now we are able to prove it.

Theorem 2.3.8 (Basis Theorem) *If R is a PID, then every finitely generated R-module M is a direct sum of cyclic modules in which each cyclic summand is either primary or is isomorphic to R.*

Proof: By Proposition 2.3.1, $M = tM \oplus F$ where F is finitely generated free submodule. Then we may assume that $M = tM$ and by the Primary Decomposition, Theorem 2.2.8, we may assume that M is (p)-primary for some prime p. We prove that M is a direct sum of cyclic submodules by induction on $d(M) \geq 1$. The base step is Lemma 2.3.6, which shows that M must be cyclic in this case.
For the inductive step, Lemma 2.3.4 says that there exists a nonzero pure cyclic submodule $S \subseteq M$ and Lemma 2.3.7 says that

$$d(M/S) = d(M) - d(S) = d(M) - 1 < d(M)$$

By induction, M/S is a direct sum of cyclic groups, say

$$M/S = \bigoplus_{i=1}^{q} \langle\, \overline{x}_i \,\rangle$$

where $\overline{x}_i = x_i + S$.
Let $m \in M$ and let $\overline{m} = m + S$ in M/S have order p^l, now m has order p^n, where $n \geq l$. But $p^l(m + S) = p^l\overline{m} = 0$ in M/S, so there is some $s \in S$ with $p^l m = s$. By purity, there is $s' \in S$ such that $p^l m = p^l s'$, now we define $z = m - s'$, then $p^l z = 0$ and $z + S = m + S = \overline{m}$. This implies that z can't have order less than p^l, but then the order of z is equal to p^l.

For each i we can choose a $z_i \in M$ with $\text{order}(z_1) = \text{order}(\overline{x}_i)$ and $\overline{x_i} = \overline{z_i}$. Then following exact sequence splits

$$0 \longrightarrow S \xrightarrow{i} M \xrightarrow{p} M/S \longrightarrow 0$$

because we have the following morphism $j : M/S \longrightarrow M$ where $j(\overline{x_i}) = z_i$. This application satisfies $p \circ j = \text{Id}_{M/S}$ and by the Proposition A.1.8 the sequence splits

$$M \cong M/S \oplus S = \bigoplus_{i=1}^{q} \langle \overline{x}_i \rangle \oplus S$$

□

Now, the next result that we want to prove is the Fundamental Theorem of Finitely Generated Modules over PID. It remains to be shown the uniqueness of the decomposition given in the Basis Theorem. The main idea of the proof is to study the invariant elements of the decomposition of a finitely generated (p)-primary module into cyclic submodules. In this case, the dimension described previously of the submodules $p^n M$ will be these invariant that we are searching.

Lemma 2.3.9 *Let R be a PID ring and M be a finitely generated (p)-primary R-module, where (p) is a prime ideal. Let $M = \bigoplus_i C_i$ where each C_i is cyclic. If $b_n \geq 0$ is the number of summands C_j having order p^n, then there is an integer t with*

$$d(p^n M) = b_{n+1} + b_{n+2} + \cdots + b_t$$

Proof: Let B_n be the direct sum of all C_j, if any, of order p^n. Since M is finitely generated, there is some t with

$$M = B_1 \oplus B_2 \oplus \cdots \oplus B_t$$

now

$$p^n M = p^n B_{n+1} \oplus \cdots \oplus p^n B_t$$

Because $p^b B_j = \{0\}$ for all $j \leq n$, similary

$$p^{n+1} M = p^{n+1} B_{n+2} \oplus \cdots \oplus p^{n+1} B_t$$

then we have

$$\begin{aligned}(p^n M)/(p^{n+1} M) &= (p^n B_{n+1} \oplus \cdots \oplus p^n B_t)/(p^{n+1} B_{n+1} \oplus \cdots \oplus p^{n+1} B_t) \cong \\ &\cong (p^n B_{n+1})/(p^{n+1} B_{n+1}) \oplus \cdots \oplus (p^n B_t)/(p^{n+1} B_t)\end{aligned}$$

since each B_j is the direct sum of b_j cyclic modules this implies that $p^n B_j / p^{n+1} B_j$ is the direct sum of b_j cyclic modules (when $j > n$), hence $d(p^n B_j) = \dim(p^n B_j / p^{n+1} B_j) = b_j$. Since d is additive over direct sums, we have $d(p^n M) = b_{n+1} + \cdots + b_t$. □

The numbers b_n can be described in terms of M, that is, they are independent of the cyclic decomposition (they are invariant).

Definition 2.3.10 Let R be a PID ring and M be a finitely generated (p)-primary R-module. For $n \geq 0$, define

$$U_p(n, M) = d(p^n M) - d(p^{n+1} M)$$

The previous lemma shows that $d(p^n M) = b_{n+1} + \cdots + b_t$ and $d(p^{m+1} M) = b_{n+2} + \cdots + b_t$ so that $U_p(n, M) = b_{n+1}$.

Theorem 2.3.11 *Let R be a PID ring and M a finitely generated (p)-primary R-module. Then any two decompositions of M into direct sums of cyclic modules, have the same number of cyclic summands of each type. More precisely, for each $n \geq 0$, the number of cyclic summands having order p^{n+1} is $U_p(n, M)$.*

Proof: By the Basis Theorem, there exist cyclic submodules c_i with $M = \bigoplus_i C_i$. Lemma 2.3.9 shows that is the number of c_i having order p^{n+1} is $U_p(n, M)$, a number that is defined without any mention of the given decomposition. Thus if $M = \bigoplus_j D_j$ is another decomposition of M, where each D_j is cyclic, then the number of D_j having order p^{n+1} is $U_p(n, M)$. □

Corollary 2.3.12 *If M and M' are finitely generated (p)-primary modules over a PID, then $M \cong M'$ if and only if $U_p(n, M) = U_p(n, M')$ for all $n \geq 0$.*

Proof: If $\varphi : M \longrightarrow M'$ is and isomorphism, then $\varphi(p^n M) = p^n M'$ for all $n \geq 0$ and so φ induces isomorphisms of the $R/(p)$ spaces $p^n M/p^{n+1}M \cong p^n M'/p^{n+1}M'$. Thus, their dimension are the same, that is $U_p(n, M) = U_p(n, M')$.
Conversely, assume that $U_p(n, M) = U_p(n, M')$ for all $n \geq 0$. If $M = \bigoplus_i C_i$ and $M' = \bigoplus_j C'_j$ where C_i and C_j are cyclic, then Lemma 2.3.9 shows that the number of summands of each type is the same, that is M and M' are isomorphic. □

Definition 2.3.13 If M is a finitely generated (p)-primary module over a PID, then its elementary divisors are the numbers in the sequence

$$U_p(0, M)\,,\, U_p(1, M)\,, \ldots, U_p(t-1, M)$$

where p^t is the largest order of a cyclic summand of M.

With this notation we announce and prove the Fundamental Theorem:

Theorem 2.3.14 (Fundamental Theorem of Finitely Generated Modules) *Let R be a PID ring and M a finitely generated R-module. Then M can be expressed as a finite direct sum of cyclic modules of the form R and $R/(p_i^n)$ where p_i is a prime element of R.*
Furthermore, two finitely generated R-modules are isomorphic if and only if their torsion submodules have the same elementary divisors and their free parts have the same rank.

Proof: The decomposition is very clear, is just the application of the Theorem 2.3.8 and Theorem 2.3.11. Let M and M' two isomorphic modules. We know that $M = tM \oplus F$ where F is a free module and $M' = tM' \oplus F'$. By Proposition 2.3.1 ii) we only have to prove the of the torsion, because the free part is immediate. By the Proposition 2.2.9 we know that $tM \cong tM'$ if and only if $M_p \cong M'_p$ for every prime $p \in R$, but the last corollary says that $M_p \cong M'_p$ if and only if $U_p(n, M) = U_p(n, M')$ for all $n \geq 0$, that is, they have the same elementary divisors. □

Observation 2.3.15 In the same way as for the finitely generated abelian groups, we have another way to decompose. Instead of decomposing the torsion part into elementary divisors we can do it through invariant factors. This decomposition is very similar and can be obtained from the elementary divisors. With the elementary divisors we have the following:

$$tM_{p_i} \cong R/\big(p_i^{e_{i1}}\big) \oplus R/\big(p_i^{e_{i2}}\big) \oplus \cdots \oplus R/\big(p_i^{e_{ir_i}}\big)$$

Then the invariant factors are:

$$c_j = p_1^{e_{1j}} \cdot p_2^{e_{2j}} \cdots p_n^{e_{nj}}$$

where $1 \leq j \leq \max\{r_i\} = r$ and if some e_{ij} does not exist then its value is 0. Therefore we have that $c_1 \,|\, c_2 \,|\, \cdots \,|\, c_r$ and $tM \cong \bigoplus_{j=1}^{r} R/\big(c_j\big)$ by the Chinese Remainder Theorem.

Example 2.3.16 One application of the Fundamental Theorem of Finitely Generated Modules over PID is the classification of endomorphisms of vector spaces. The relation is the following: Let $T : V \longrightarrow V$ a linear transformation between a k-vector space. Then V can be thought as a $k[X]$-module, where the multiplication $f(X) \cdot v$ is defined as $\big(f(T)\big)(v)$. It is not difficult to see that if V has finite dimension as a k-vector space then V is a torsion finitely generated $k[X]$-module. We can decompose the $k[X]$-module V by its invariant factors. Now T can be restricted to each cyclic module and these new restricted linear maps have a much simpler matrix expression. Hence we end with a simpler matrix of the linear map T. This form is called Rational Canonical Form of the endomorphism T.
If we do the same but decomposing the $k[X]$-module V with the elemenatry divisors we end with the Jordan Canonical Form of the endomorphism T.
These two forms are very relevant in the study of linear algebra and have many applications.

Finally we end this chapter with a characterization of PID rings. This one is very special because it relates the fact that every finitely generated module over a PID is the direct sum of cyclic modules.

Theorem 2.3.17 *Let R be a Noetherian domain. Then the following statements are equivalent:*

i) *R is a PID ring.*

ii) *Every finitely generated R-modules is the direct sum of cyclic R-modules.*

Proof: i)⇒ii): This implication is the Basis Theorem (Theorem 2.3.8).
Now let's suppose that every finitely generated R-module is the direct sum of cyclic R-modules. Then R is an R-module finitely generated, so every ideal of R is finitely generated because R is Noetherian. By hypothesis we have that every ideal of R is the direct sum of cyclic R-modules. If $I = J \oplus K$ where I is a nonzero ideal and J, K are nonzero cyclic R-modules, then $J \oplus 0$ and $0 \oplus K$ are R-module of I. Note that there are nonzero elements $a \in J \oplus 0$ and $b \in 0 \oplus K$. This implies that $a \cdot b \in (J \oplus 0) \cap (0 \oplus K) = 0$. Since R is a domain $a \cdot b = 0 \Rightarrow a = 0$ or $b = 0$, a contradiction. Therefore every ideal is cyclic, in other words R is a PID. □

This Theorem can be generalized for non-domains and it is still true. This is done by A. I. Uzkov in [14].

Chapter 3

Dedekind Rings

Up until now we have worked with PID rings. These rings are comfortable to work with them because this property make things easier (like every ideal is a product of prime ideals). We can consider a much simpler ring, like a local PID, and we can ask ourselves what ring is such that all its localizations are local PID. We will see that such a ring is very rich and can be characterized in many ways. They are the Dedekind domains. We can think that these domains are a generalization of PID rings. The approach that we will do to Dedekind domains in this work is, as mentioned above, looking its localisation.

3.1 Valuation Rings

The valuation rings arises from considering a function from a field to a totally ordered abelian group that satisfies two properties. Then the set of all the elements of the field including the 0 that their image is greater than 0 form a ring. This ring is called the valuation ring. But in this section we will have a idealistic pint of view towards these rings because at this work the valuation are not relevant.

Definition 3.1.1 A valuation ring is an integral domain R with the property that if I and J are ideals of R then either $I \subseteq J$ or $J \subseteq I$.

Proposition 3.1.2 *Let R be an integral domain. Then the following statements are equivalent:*

i) *R is a valuation ring.*

ii) *If $a, b \in R$ then either $(a) \subseteq (b)$ or $(b) \subseteq (a)$.*

iii) *If $x \in K = \text{Frac}(R)$ then either $x \in R$ or $x^{-1} \in R$.*

PROOF: (i)⇒(ii) is clear. Assume that (ii) holds and let $x \in K$. Then $x = a/b$ where $a, b \in R$. If $(a) \subseteq (b)$ then $a = br$ for some $r \in R$, hence $x = a/b = r \in R$. If $(b) \subseteq (a)$ then $b = ar$ and $x^{-1} = b/a = r \in R$. Finally, suppose that (iii) holds and let $I, J \subseteq R$ ideals. If $I \nsubseteq J$ then we can choose $a \in I$ that $a \notin J$. Let $b \in J$ be any nonzero element, then $a/b \notin R$ (if $a/b \in R$ then $a \in (b) \subseteq J$). Hence $b/a \in R$ and $b \in (a) \subseteq I$. Thus $J \subseteq I$. □

With the previous proposition we obtained different characterization of this type of rings. We want to reach another characterization more powerful that describes the discrete valuation rings (that will be introduced later). First note that every valuation ring is quasi local.

Proposition 3.1.3 *Let R be a valuation ring. Then the non-units of R form an ideal of R, which is the unique maximal ideal of R.*

PROOF: Let S be the set of nonunits of R. Let $a, b \in S$ and $c \in R$ then ac is not a unit of R, hence $ac \in S$. For the previous proposition we can assume that $a/b \in R$. Then $a + b = (a/b + 1)b \in S$ because $a/b + 1 \in R$ and $b \in S$. Thus S is an ideal of R and if A is a proper ideal of R then every element of A is a non-unit so $A \subseteq S$. We can conclude that S is the unique maximal ideal of R. □

Definition 3.1.4 Let $R' \,|\, R$ be a ring extension ($R \subseteq R'$), an element $a \in R'$ is integral over R if it is a root of a monic polynomial in $R[x]$. Now we can define

$$\mathcal{O}_{R'|R} = \big\{a \in R' \,:\, a \text{ is integral over } R\big\}$$

If R is a domain, $R' = \mathrm{Frac}(R)$ and $\mathcal{O}_{R'|R} = R$, then R is called integrally closed. Some authors call these rings by normal domains.

The concept of integral element is very useful on algebraic number theory. Usually $\mathcal{O}_{R'|R}$ is called the ring of integers when $R = \mathbb{Z}$ and R' is a finite field extension of $\mathbb{Q}$. For example $\mathbb{Z}[i]$ is the ring of integers of the field $\mathbb{Q}[i]$.

Example 3.1.5 Every UFD (unique factorization domain) is integrally closed, in particular every PID is integrally closed.

Proposition 3.1.6 *Let R be a valuation ring. Then it is integrally closed.*

PROOF: Let K be its quotient field and $x \in K$ an integral element over R, then

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$$

for $a_i \in R$. If $x \notin R$ then $x^{-1} \in R$ hence

$$x = -(a_{n-1} + a_{n-2}x^{-1} + \cdots + a_0 x^{-n+1})$$

and thus $x \in R$, a contradiction. □

Definition 3.1.7 Let R be a ring. Then the Krull dimension of R is:

$$\dim(R) = \sup\Big\{n \,:\, \mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n\,,\ \text{where } \mathfrak{p}_i \text{ is a prime ideal of } R \text{ for each } i\Big\}$$

Definition 3.1.8 A discrete valuation ring is a Noetherian valuation ring of dimension 1. In other words a discrete valuation ring is a Noetherian valuation ring that every nonzero prime ideal is maximal. Usually we denote these rings by the abbreviation DVR (it is an acronym).

Before we prove the theorem that characterizes the DVR rings we have to enunciate a very standard result that can be found at [2].

Proposition 3.1.9 (determinantal) *Let M a finitely generated R-module, $I \subseteq A$ an ideal and $\phi \in \mathrm{End}_A(M)$ such that $\phi(M) \subseteq IM$. Then ϕ satisfies an equation like the next one*

$$\phi^n + \alpha_{n-1}\phi^{n-1} + \cdots + \alpha_1\phi + \alpha_0 = 0$$

where $\alpha_i \in I$ and n is the number of elements that a system of generators of M has.

Theorem 3.1.10 *Let R be a domain then the following properties are equivalent:*

i) *R is a DVR.*

ii) *R is Noetherian, integrally closed and has a unique nonzero prime ideal.*

iii) *R is a local PID that is not a field.*

Proof: i)⇒ii). If R is a DVR, then it does have all the required properties, since R is a local ring and integrally closed by the previous propositions.

ii)⇒iii). This requires us to show that R is a PID. Let $\mathfrak{p}$ be the nonzero prime ideal and choose a nonzero $a \in \mathfrak{p}$. Define $M = R/aR$ and consider the family A of all the annihilators $\operatorname{ann}(m)$ as m varies over all the nonzero elements of M. Since R is noetherian, it satisfies the maximum condition, and so there is a nonzero element $b + aR \in M$ such that $\mathfrak{q} = \operatorname{ann}(b + aR)$ is maximal in A.

We claim that $\mathfrak{q}$ is a prime ideal. Suppose that $x, y \in R$, $xy \in \mathfrak{q}$ and $x, y \notin \mathfrak{q}$, then $y(b + aR) = yb + aR$ is a nonzero element of M because $y \notin \mathfrak{q}$. But $\operatorname{ann}(b+aR) \subsetneq \operatorname{ann}(yb+Ra)$ because $x \notin \operatorname{ann}(b+aR)$ and this contradicts the maximality property of $\mathfrak{q}$. Therefore $\mathfrak{q}$ is a prime ideal, since R has a unique nonzero ideal $\mathfrak{p}$ we have

$$\mathfrak{q} = \operatorname{ann}(b + aR) = \mathfrak{p}$$

We note that $b/a \notin R$ otherwise $b + aR = 0 + aR$ contradicting $b + aR$ being a nonzero element of $M = R/aR$.

Now we will show that $\mathfrak{p}$ is principal, with generator a/b (we do not yet know if a/b lies in R or not). First we have $b\mathfrak{p} = b\mathfrak{q} \subseteq aR$ so that $(b/a)\mathfrak{p} \subseteq R$. If $(b/a)\mathfrak{p} \subseteq \mathfrak{p}$, since $\mathfrak{p}$ is a R-module we can apply Proposition 3.1.9 (determinantal) with $\phi(x) = (b/a) \cdot x$. Then we get that b/a is integral over $\mathfrak{p}$, that is, over R but R is integrally closed this puts $b/a \in R$ a contradiction. Therefore $(b/a)\mathfrak{p} = R$, thus $\mathfrak{p} = (a/b)R$, that is $a/b \in R$ and $\mathfrak{p}$ is principal.

Denote a/b by t, we will show that every ideal in R is principal and generated by t^n for $n > 0$. Let I be a nonzero ideal of R, and consider the chain of submodules of $\operatorname{Frac}(R)$

$$I \subseteq t^{-1}I \subseteq t^{-2}I \subseteq \cdots$$

we claim that this chain is strictly increasing. If $t^{-n}I = t^{-n-1}I$ then the finitely generated R-module $t^{-n}I$ satisfies $t^{-1}(t^{-n}I) \subseteq t^{-n}I$ so that $t^{-1} = b/a$ is integral over R (by the determinantal). As above, R is integrally closed, this forces $b/a \in R$, a contradiction. Since R is noetherian, this chain can contain only finitely many ideals in R. Thus, there exist an n such that $t^{-n}I \subseteq R$ and $t^{-n-1}I \nsubseteq R$. If $t^{-n}I \subseteq \mathfrak{p} = tR$ then $t^{-n-1}I \subseteq R$, therefore $t^{-n}I = R$ and $I = t^nR$ is a principal ideal.

iii)⇒i). If R is a local PID that is not a field, then it is Noetherian. Since R is local we have a unique maximal ideal (p) and is prime also. Hence R has only one irreducible element named p (remember that a PID is a UFD). If $a, b \in R$ then $a = up^n$ and $b = sp^m$ where $u, s \in R$ are units hence $(a) \subseteq (b)$ or $(b) \subseteq (a)$. Thus R is a discrete valuation. □

Example 3.1.11 By the previous theorem we have that ring of formal power series $k[[x]]$ where k is a field is a DVR. This is because is a PID and it only has one maximal ideal (x).

Observe that the Theorem 3.1.10 gives a nice characterization of DVR rings, it allows us to characterize the Dedekind rings that will be defined in the next section.

3.2 Characterizations of Dedekind domains

Historically the Dedekind domains arises from algebraic number theory. When we have a finite field extension of $\mathbb{Q}$, then its ring of integers is a Dedekind domain (it is a basic result of algebraic number theory). The structure and properties of these rings can be useful for solving some Diophantine equations. Thanks to the previous section we are able to show that the localization of a Dedekind domain is a DVR and vice versa.

Definition 3.2.1 A domain R is a Dedekind ring if it is integrally closed, noetherian, and all its nonzero prime ideals are maximals.

Proposition 3.2.2 *Let R be a domain that is integrally closed. Then every localisation $S^{-1}R$ where S is a multiplicative set is integrally closed.*

With the previous proposition we can prove our first characterization of Dedekind domains.

Proposition 3.2.3 *Let R be a noetherian domain. Then R is a Dedekind ring if and only if the localizations $R_{\mathfrak{p}}$ are DVRs for every nonzero prime ideal $\mathfrak{p}$.*

Proof: If R is a Dedekind ring and $\mathfrak{p}$ is a maximal ideal, then $R_{\mathfrak{p}}$ has a unique nonzero prime ideal. Moreover $R_{\mathfrak{p}}$ is Noetherian, a domain and integrally closed by the previous proposition. By Theorem 3.1.10 we get that $R_{\mathfrak{p}}$ is a DVR since it.
For the converse, we must show that R is integrally closed and that its nonzero prime ideals are maximal. Let $u/v \in \operatorname{Frac}(R)$ be integral over R, for every nonzero prime ideal $\mathfrak{p}$, the element u/v is integral over $R_{\mathfrak{p}}$. But $R_{\mathfrak{p}}$ is a PID, hence is integrally closed, so $u/v \in R_{\mathfrak{p}}$ for all $\mathfrak{p}$ prime ideal of R. We conclude that $u/v \in \cap_{\mathfrak{p}} R_{\mathfrak{p}} = R$ by Proposition A.1.6, therefore R is integrally closed.
Suppose that there are nonzero prime ideals $\mathfrak{p} \subsetneq \mathfrak{q}$ in R. Then $\mathfrak{p}_{\mathfrak{q}} \subsetneq \mathfrak{q}_{\mathfrak{q}}$ in $R_{\mathfrak{q}}$, contradicting the fact that DVRs have a unique nonzero prime ideal. Therefore nonzero prime ideals are maximal, and R is a Dedekind ring. □

Observation 3.2.4 Note that if R is a Dedekind domain and $\mathfrak{p}$ a prime ideal then $R_{\mathfrak{p}}$ is also a Dedekind domain. The reverse is also true, that is if $R_{\mathfrak{p}}$ is a Dedekind domain for every prime ideal $\mathfrak{p}$ then R is a Dedekind domain. This can be stated as follows: The property of being Dedekind domain is local.

Now we will approach these rings by studying its ideals. But first we have to define a more general concept of an ideal.

Definition 3.2.5 If R is a domain with $Q = \operatorname{Frac}(R)$ then a fractional ideal I is a nonzero R-submodule of Q such that there exists a nonzero $a \in R$ such that $aI \subseteq R$.
If I is a fractional ideal we can define another fractional ideal

$$I^{-1} = \{v \in Q : vI \subseteq R\}$$

it is always true that $I^{-1}I \subseteq R$, a fractional ideal I is invertible if $I^{-1}I = R$.

With this new concept we will explore which properties have an invertible ideal. The next propositions answer this question.

Proposition 3.2.6 *Let R be a domain and I a fractional ideal. If there exists another fractional ideal*

$J \subseteq \mathrm{Frac}(I)$ such that $IJ = R$ then $J = I^{-1}$. In other words the inverse of a fractional ideal, if it exists, is unique.

Proof: By definition we have that $J \subseteq I^{-1}$, this implies $R = IJ \subseteq II^{-1} \subseteq R$, hence $II^{-1} = R$, then I is invertible. Finally

$$IJ = R \Rightarrow I^{-1}IJ = I^{-1} \Rightarrow J = I^{-1}$$

□

Proposition 3.2.7 *Let R be a domain. Then every invertible ideal of R is finitely generated.*

Proof: Let I be an invertible ideal, then $I^{-1}I = R$ this implies the existence of elements $c_i \in I^{-1}$ and $b_i \in I$ such that $\sum_i c_i b_i = 1$. Now let $b \in I$, then $b = b1 = \sum (bc_i)b_i$ and $a_i = bc_i \in R$ for every i, since $b \in I$ and $c_i \in I^{-1}$.
Thus $I = b_1R + \cdots + b_nR$ and $\{b_1, \dots, b_n\}$ is a set of generators of I. □

The previous propositions say that if an ideal is invertible then it has a unique inverse and it is finitely generated. We can think that the property of being invertible is strong. Well, this is true. It is strong enough that if all the ideals of a domain are invertibles then this domain is a Dedekind ring. The next theorem affirm that.

Lemma 3.2.8 *Let R be a domain. Then all the ideals of R are invertible if and only if all the fractional ideals of are invertible.*

Proof: One implication is trivial because an ideal of R is a fractional ideal.
Let J be a fractional ideal of R, then there exists an $r \in R$ such that $rJ \subseteq R$, that is $r \cdot J = I \subseteq R$. Now I is an ideal of R thus I is invertible. Then

$$I \cdot I^{-1} = R \quad \Rightarrow \quad J \cdot I^{-1} = R \quad \Rightarrow \quad J \cdot rI^{-1} = R$$

hence J is invertible and $J^{-1} = rI^{-1}$. □

Theorem 3.2.9 *Let R be a domain. Then R is a Dedekind ring if and only if all the ideals of R are invertible.*

Proof: Suppose that R is a Dedekind ring and let J be a fractional ideal in R, since R is a Dedekind ring, its localization $R_{\mathfrak{p}}$ is a PID. So $J_{\mathfrak{p}}$, as every nonzero principal ideal, is invertible (in Proposition 2.1.6 we proved that every fractional ideal of a PID is principal).

$$(J^{-1}J)_{\mathfrak{p}} = (J^{-1})_{\mathfrak{p}} J_{\mathfrak{p}} = (J_{\mathfrak{p}})^{-1} J_{\mathfrak{p}} = R_{\mathfrak{p}}$$

Proposition A.1.5 gives $J^{-1}J = R$ and so J is invertible.
Now we have to prove the other direction. Since all the ideals of R are fractional, they are invertible and by Proposition 3.2.7 they are finitely generated. Thus R is noetherian by the Corollay A.3.3.
We must show that every nonzero prime ideal $\mathfrak{p}$ is a maximal ideal. Let I be an ideal with $\mathfrak{p} \subsetneq I$ (we allow $I = R$), then $\mathfrak{p}I^{-1} \subseteq II^{-1} = R$, so that $\mathfrak{p}I^{-1}$ is an ideal in R. Now $(\mathfrak{p}I^{-1})I = \mathfrak{p}$ because the multiplication is associative, since $\mathfrak{p}$ is a prime ideal, we must have $\mathfrak{p}I^{-1} \subseteq \mathfrak{p}$ or $I \subseteq \mathfrak{p}$. The second option does not hold, so that $\mathfrak{p}I^{-1} \subseteq \mathfrak{p}$. Multiplying by $\mathfrak{p}^{-1}I$ gives $R \subseteq I$. Therefore $I = R$ and so $\mathfrak{p}$ is a maximal ideal.

Now we have to prove that R is integrally closed, let $a \in \mathrm{Frac}(R)$ be integral over R, then $J = \langle a, \dots, a^n \rangle$ is a finitely generated R-submodule of $\mathrm{Frac}(R)$, equivalently, a fractional ideal, with $aJ \subseteq J$. By the previous lemma J is invertible and this implies that there are $c_1, \dots, c_n \in J^{-1}$ and $b_1, \dots, b_n \in J$ with $1 = \sum_i c_i b_i$ (like in Proposition 3.2.7). Hence $a = \sum_i c_i b_i a$, but $b_i a \in J$ and $c_i \in J^{-1}$ gives us $a = \sum_i c_i (b_i a) \in R$. Therefore R is integrally closed and hence it is a Dedekind ring. □

This Theorem allows us to work with the fractional ideals of a Dedekind domain because they have good properties since they are invertible. The next propositions will study the semilocal Dedekind rings and the UFD Dedekind rings.

Proposition 3.2.10 *Let R be a Dedekind domain with a finite number of prime ideals, then R is a PID.*

Proof: Since R is a Dedekind domain, all the prime ideals are maximal, let $\mathfrak{m}_1, \dots, \mathfrak{m}_n$ denote the maximal ideals in R and let I be an ideal (is invertible since R is Dedekind). Since $II^{-1} = R$, then for each i from 1 to n we can choose $a_i \in I$ and $b_i \in I^{-1}$ such that $a_i b_i \notin \mathfrak{m}_i$. Moreover $\mathfrak{m}_i$ cannot contain the intersection of the remaining maximal ideals (lemma A.1.4), hence we can find an element u_i that is not in $\mathfrak{m}_i$ but does lie in all the other maximal ideals.
Set $v = u_1 b_i + \cdots + u_n b_n$, note that $v \in I^{-1}$ so that vI is an ideal in R. We claim that vI lies in no maximal ideal. Suppose, that $vI \subseteq M_i$ for some i, then $va_i \in M_i$, however

$$va_i = (u_1 b_1 + \cdots + u_n b_n) a_i$$

and $u_i b_i a_i \notin M_i$ but all the other terms lies in $\mathfrak{m}_i$. Hence $va_i \notin \mathfrak{m}_i$ and this is a contradiction because we supposed that $vI \subseteq \mathfrak{m}_i$. We have proved that $vI = R$ and $I = v^{-1}R$ is principal. □

Proposition 3.2.11 *A Dedekind ring R is a UFD if and only if it is a PID.*

Proof: First we know that if R is a PID ring then it is UFD (this is true for any ring).
Now suppose that R is a UFD Dedekind ring and let I be an invertible ideal. Then there are $a_1 \dots, a_n \in I$ and $q_1, \dots, q_n \in \mathrm{Frac}(R)$ such that $1 = \sum_i q_i a_i$ and $q_i I \subseteq R$ for all i. Let $q_i = b_i / c_i$ where $b_i, c_i \in R$, since R is a UFD we can assume that $(b_i, c_i) = 1$. But we have that $(b_i/c_i) a_j \in R$ (because $q_i \in I^{-1}$ and $a_j \in I$), thus c_i divides $b_i a_j$ so that c_i divides a_j for all i, j.
Let $c = lcm c_i, \dots, c_n$ then $c = \sum_i (cb_i/c_i) a_i$ and $cb_i/c_i \in R$. Hence $cR \subseteq I$. By the definition of c we have also that c divides a_j for all j, so that $a_j \in cR$ and so $I \subseteq cR$, that is $I = cR$ is principal. By the previous theorem we have that all the ideals of R are invertible therefore are principal. □

We have to remark that in general the UFD rings are quite complex (in spite of the simplicity of their definition). For example it is not true that the power series ring over a UFD is a UFD. But if the ring is a Dedekind domain then the UFD property is well characterized.
The next goal is to characterize the Dedekind domains with the fact that every invertible fractional ideal is projective. We begin with a characterization of the morphisms that go from a fractional ideal to the ring.

Proposition 3.2.12 *Let R be a domain, I a fractional ideal and $f : I \longrightarrow R$ an R-homomorphism. Let b be any nonzero element of I, then $f(a) = b^{-1} f(b) a$ for all $a \in I$.*

Proof: Since I is a fractional ideal, we can choose a $d \in R$ such that $dI \subseteq R$, then $db \in R$ and $da \in R$

for any $a \in I$. We have

$$(da)f(b) = f(dab) = (db)f(a)$$

Hence $af(b) = bf(a)$, this implies that $f(a) = b^{-1}f(b)a$. □

Now with the previous proposition and the dual basis lemma (Theorem A.4.7) we will characterize the Dedekind domains by the property that all its ideals are projective. This result will be important lately because we will see that all finitely generated torsion-free R-module can be decomposed by a direct sum of ideals in R and the fact that this ideals are projective simplifies and helps a lot.

Theorem 3.2.13

i) *A nonzero ideal I in a domain R is invertible if and only if I is projective.*

ii) *A domain R is a Dedekind ring if and only if every ideal in R is projective.*

Proof:

i) First we suppose that I is an invertible ideal. Then there exists $c_i \in I^{-1}$ and $b_i \in I$ such that $1 = \sum_i c_i b_i$. The maps $f_i : I \longrightarrow R$ defined by $f_i(a) = ac_i$ are in $\operatorname{Hom}_R(I, R)$ and $a = \sum_i (ac_i)b_i = \sum_i f_i(a)b_i$. By the dual basis lemma (Theorem A.4.7) the ideal I is a projective R-module.
The other implication begins with the same dual basis lemma, let $\{b_i\}_{i\geq 1}$ a set of generators of I and $f_i \in \operatorname{Hom}_R(I, R)$ such that $a = \sum_i f_i(a)b_i$ for all $a \in I$. The previous proposition ensures that $f_i(a) = b^{-1}f_i(b)a$ for any b nonzero element of I. Then if we fix $b \in I$ we have that $f_i(b) = 0$ for all i except $i = 1, \dots, m$, thus

$$a = \sum_i f_i(a)b_i \quad \Rightarrow \quad a = \sum_{i=1}^{m} b^{-1}f_i(b)ab_i \quad \Rightarrow \quad 1 = \sum_{i=1}^{m} b^{-1}f_i(b)b_i.$$

Since $f_i(a) \in R \Rightarrow b^{-1}f_i(b)a \in R$ for all $a \in I$ then $c_i = b^{-1}f_i(b) \in I^{-1}$. Therefore $1 = \sum_i c_i b_i$ and $c_i \in I^{-1}$, $b_i \in I$ hence $I^{-1}I = R$.

ii) This follows from the previous part and the Theorem 3.2.9. □

The next goal is to characterize the Dedekind domains by their primes ideals. We will see that every ideal of a Dedekind domain is a product of prime ideals. Moreover this is a sufficient and necessary condition for a domain to be Dedekind.

Lemma 3.2.14 *Let R be a domain and $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ ideals of R. If $\mathfrak{p}_1 \cdots \mathfrak{p}_n$ is invertible then each $\mathfrak{p}_i$ is invertible.*

Proof: Let $I = \mathfrak{p}_1 \cdots \mathfrak{p}_n$, then we have that $II^{-1} = R$ and $I^{-1}\prod \mathfrak{p}_i = R$. This implies $\mathfrak{p}_i\left(I^{-1}\prod_{j\neq i}\mathfrak{p}_j\right) = R$. Thus $I^{-1}\prod_{j\neq i}\mathfrak{p}_j$ is the inverse of $\mathfrak{p}_i$. □

Theorem 3.2.15 *For any domain R, the following properties are equivalent*

i) *R is a Dedekind domain.*

ii) *Every ideal of R can be expressed uniquely as a finite product of maximal ideals.*

iii) *Every ideal of R can be expressed as a finite product of prime ideals.*

Proof: (i)⇒(ii). Let R be a Dedekind domain and S the set of ideals of R wich can not be expressed as a finite product of maximal ideals. If S is empty, then all the ideals can be expressed in such way and it is done. If S is not empty then there exists some ideal $I \in S$ that is maximal in this set (this exists because R is Noetherian).

Since $I \neq R$ then $I \subseteq \mathfrak{m} \subsetneq R$ for some maximal ideal $\mathfrak{m}$. By the Theorem 3.2.9 we know that all the ideals are invertible, thus $I = \mathfrak{m}J$ where $J = \mathfrak{m}^{-1}I \subsetneq \mathfrak{m}^{-1}\mathfrak{m} = R$. If $I = J$ then $R = II^{-1} = \mathfrak{m}JJ^{-1} = \mathfrak{m}$, a contradiction, thus $I \subsetneq J$. Therefore $J \notin S$ by maximality and $\mathfrak{m} \notin S$ then $I = \mathfrak{m}J \in S$ is a contradiction. We conlude that every ideal can be expressed as a finite product of maximal ideals.

Any such expression is unique, if $\mathfrak{p}_1 \cdots \mathfrak{p}_n = \mathfrak{q}_1 \cdots \mathfrak{q}_r$, since $\mathfrak{q}_1 \cdots \mathfrak{q}_r \subseteq \mathfrak{p}_1$ and $\mathfrak{p}_1$ is prime, we have $\mathfrak{q}_i \subseteq \mathfrak{p}_1$ for some i. But $\mathfrak{q}_i$ is maximal, so $\mathfrak{p}_1 = \mathfrak{q}_i$ and we cancel these terms. Now we apply induction and follows that $n = r$ and the expression is unique up to the order of the factors.

(ii)⇒(iii) is clear. To prove (iii)⇒(i) we first show that every invertible prime ideal $\mathfrak{p}$ of R is maximal. If $\mathfrak{p}$ is not maximal, then there exists an element $a \in R$ such that $\mathfrak{p} \subsetneq \mathfrak{p} + aR \subsetneq R$ and by the hypothesis we can write

$$\mathfrak{p} + aR = \mathfrak{p}_1 \cdots \mathfrak{p}_n \quad \text{and} \quad \mathfrak{p} + a^2R = \mathfrak{q}_1 \cdots \mathfrak{q}_r$$

where $\mathfrak{p}_i$ and $\mathfrak{q}_j$ are prime ideals containing $\mathfrak{p}$. In $\overline{R} = R/\mathfrak{p}$ we have that

$$\overline{a}\overline{R} = \overline{\mathfrak{p}_1} \cdots \overline{\mathfrak{p}_n} \quad \text{and} \quad \left(\overline{a}\overline{R}\right)^2 = \overline{a}^2\overline{R} = \overline{\mathfrak{q}_1} \cdots \overline{\mathfrak{q}_r} = \overline{\mathfrak{p}_1}^2 \cdots \overline{\mathfrak{p}_n}^2$$

where $\overline{a}$ is the class of a in $R/\mathfrak{p}$ and the same for $\mathfrak{p}_i, \mathfrak{q}_j$. Let $\overline{\mathfrak{p}_1}$ be the minimal ideal among the prime ideals $\overline{\mathfrak{p}_i}, \overline{\mathfrak{q}_j}$. Since $\overline{\mathfrak{q}_j} \subseteq \overline{\mathfrak{p}_1}$ for some j, we find that $\overline{\mathfrak{p}_1} = \overline{\mathfrak{q}_j}$ because $\overline{\mathfrak{p}_1}$ is minimal. Now we can apply the Correspondence Theorem and we get that $\mathfrak{p}_1 = \mathfrak{p}_j$. These prime ideals are invertible (by hypothesis) and with induction it follows that $n = 2r$ and each $\mathfrak{p}_i$ is equal to two of the $\mathfrak{q}_j$. Therefore

$$\mathfrak{p} \subseteq \mathfrak{p} + a^2R = \left(\mathfrak{p} + aR\right)^2 \subseteq \mathfrak{p}^2 + aR$$

Thus any element x of $\mathfrak{p}$ can be written in the form $x = y + za$ with $y \in \mathfrak{p}^2$ and $z \in R$. Then we have that $za \in \mathfrak{p}$, hence $z \in \mathfrak{p}$ because $a \notin \mathfrak{p}$. This implies that $\mathfrak{p} \subseteq \mathfrak{p}^2 + \mathfrak{p} \cdot aR$. Since $\mathfrak{p}$ is invertible, we can cancel it and find $\mathfrak{p} + aR = R$, wich is a contradiction. This shows that $\mathfrak{p}$ is maximal.

Now let $\mathfrak{m}$ be any nonzero prime ideal of R. If $0 \neq a \in \mathfrak{m}$, then $aR = \mathfrak{p}_1 \cdots \mathfrak{p}_n \subseteq \mathfrak{m}$, hence $\mathfrak{p}_i \subseteq \mathfrak{m}$ for some i. Since aR is invertible (because it is a principal ideal) and $\mathfrak{p}_i$ is a factor, by the previous Lemma $\mathfrak{p}_i$ is invertible too. Hence $\mathfrak{p}_i$ is maximal by the first part of this proof and so $\mathfrak{m} = \mathfrak{p}_i$ which shows that $\mathfrak{m}$ is invertible. Since every nonzero ideal I of R can be expressed as a finite product of prime ideals and these are invertible, the ideal I is invertible too. □

This theorem is very important as it says that the behavior of prime ideals on a Dedekind ring is similar to the behavior of prime elements on a PID ring. Because every ideal (element) can be expressed uniquely as a finite product of prime ideals (elements). At this point we note that the Dedekind domains have a divisibility ideal theory. The following results are properties of this divisibility theory for ideals.

Proposition 3.2.16 *Let I and J be nonzero ideals in a Dedekind ring R, and let their prime factorization be*

$$I = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_n^{e_n} \quad \textit{and} \quad J = \mathfrak{p}_1^{f_1} \cdots \mathfrak{p}_n^{f_n}$$

where $e_i \geq 0$ and $f_i \geq 0$ for all i. Then the following statements are true:

i) *$I \subseteq J$ if and only if $I = JL$ for some ideal L.*

ii) *$I \subseteq J$ if and only if $f_i \leq e_i$ for all i.*

iii) *If $m_i = \min\{e_i, f_i\}$ and $M_i = \max\{e_i, f_i\}$ then*

$$I \cap J = \mathfrak{p}_1^{M_1} \cdots \mathfrak{p}_n^{M_n} \quad \text{and} \quad I + J = \mathfrak{p}_1^{m_1} \cdots \mathfrak{p}_n^{m_n}$$

iv) $R/I = R/(\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_n^{e_n}) \cong \left(R/\mathfrak{p}_1^{e_1}\right) \times \cdots \times \left(R/\mathfrak{p}_n^{e_n}\right)$

Proof:

i) If $I \subseteq J$ then $J^{-1}I \subseteq R$ and $J(J^{-1}I) = J$ thus $L = J^{-1}I$.
Conversely, if $I = JL$, since $L \subseteq R$ is an ideal then $I = JL \subseteq JR = J$.

ii) This is immediate by the previous result and the unique factorization of ideals as product of prime ideals.

iii) Let $I + J = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_n^{r_n}$ and let $A = \mathfrak{p}_1^{m_1} \cdots \mathfrak{p}_n^{m_n}$. Since $I \subseteq I + J$ and $J \subseteq I + J$ we have that $r_i \leq e_i$ and $r_i \leq f_i$, so $r_i \leq \min\{e_i, f_i\} = m_i$. Hence $A \subseteq I + J$.
For the other inclusion we have that $I \subseteq A$ and $J \subseteq A$ by ii), then $I + J \subseteq A$.

iv) This is just the Chinese Remainder Theorem because if $i \neq j$ then $\mathfrak{p}_i^{e_i}$ and $\mathfrak{p}_j^{e_j}$ are coprime. We can prove that first observing that $\mathfrak{p}_i + \mathfrak{p}_j = R \Rightarrow (\mathfrak{p}_i + \mathfrak{p}_j)^n = R$ then expanding this expression by the binomal theorem for $n = e_i + e_j$ we have that $p_i^{e_i} + p_j^{e_j} = R$. □

Corollary 3.2.17 *Let R be a Dedekind ring, and let $\mathfrak{p}$ be a nonzero prime ideal in R.*

i) *If $a \in \mathfrak{p}$ then $\mathfrak{p}$ occurs in the prime factorization of Ra.*

ii) *If $a \in \mathfrak{p}^e$ and $a \notin \mathfrak{p}^{e+1}$ then $\mathfrak{p}^e$ occurs in the prime factorization of Ra, but $\mathfrak{p}^{e+1}$ does not occur.*

Proof:

i) If $a \in \mathfrak{p}$ then $Ra \subseteq \mathfrak{p}$ this implies that $Ra = \mathfrak{p}L$ by the previous proposition.

ii) If we suppose that $\mathfrak{p}^{e+1}$ occurs in the prime factorization of Ra then $Ra = \mathfrak{p}^{e+1}L$ and so $a \in \mathfrak{p}^{e+1}L \subseteq \mathfrak{p}^{e+1}$. □

3.3 Ideal Class Group

Once we have proved that every fractional ideal of a Dedekind domain is invertible, we can observe that the set of all the fractional ideals of R is a group under multiplication. This group is commutative and the set of principal ideals form a subgroup. Then we can consider the quotient group by this subgroup and the result is a group that haves a lot of information. This group can be thought of as a group that measures how close or far the ring is to being PID.

Proposition 3.3.1 *Let R be a Dedekind domain. Then the set of all fractional ideals $\mathcal{F}(R)$ forms an abelian group under multiplication.*

Proof: Let $I, J \in \mathcal{F}(R)$ be two fractional ideals of R. Then $I \cdot J$ is a fractional ideal, hence $I \cdot J \in \mathcal{F}(R)$. The associative property comes off from the fact that the multiplication of elements from R is associative. It is immediate that the neutral element is R and every fractional ideal is invertible because R is a Dedekind domain (Theorem 3.2.9). This group is abelian because the ring is commutative, that is, the multiplication is commutative in R. □

Proposition 3.3.2 *Let R be a Dedekind domain. Then $\mathcal{F}(R)$ is a free abelian group with basis all the nonzero prime ideals.*

Proof: By Theorem 3.2.15 we have that every ideal of R. This can be extended to fractional ideals since if I is a fractional ideal then there exists $a \in R$ such that $aR \cdot I$ is an ideal of R. This ideal has a unique prime factorization as well as the ideal aR. Then $I = (aR)^{-1}(aR \cdot I)$ has a unique prime factorization (where the exponents of the prime ideals can be negative).
This implies that the group $\mathcal{F}(R)$ is a free abelian group with the set of prime ideals as a basis. □

Definition 3.3.3 Let R be a Dedekind domain. Then its class group $\mathcal{C}(R)$ is defined by

$$\mathcal{C}(R) = \mathcal{F}(R)/\mathcal{P}(R)$$

where $\mathcal{P}(R)$ is the set of all principal fractional ideals of R.

Observation 3.3.4 We remember that if G is a group and S a normal subgroup of G then the equivalence relation that gives G/S is the following: $g, f \in G$ are related if and only if $g \cdot f^{-1} \in S$. Then applying this to our class group gives that the fractional ideals I, J are related if and only if $I \cdot J^{-1} \in \mathcal{P}(R)$. This is the same as say that here exists some principal ideal aR such that $I \cdot J^{-1} = aR \Leftrightarrow I = aJ$ (because we are in a Dedekind domain). Hence if we have two fractional ideals I, J such that $I = rJ$ for some $r \in R$, then I and J are in the same equivalence class on the quotient group $\mathcal{C}(R)$.

In general the study of this group is difficult. There is a very important result about the ideal class group of a number field that says: If K is a number field, then $\mathcal{C}(\mathcal{O}_{K|\mathbb{Z}})$ is a finite abelian group. The order $|\mathcal{C}(\mathcal{O}_{K|\mathbb{Z}})|$ is called the class number of $\mathcal{O}_{K|\mathbb{Z}}$. Dirichlet was the first who proved this result but the usual proof of this theorem uses a geometric theorem of Minkowski wich says that sufficiently large parallelepipeds in Euclidean space must contain lattice points. These theorems are done in the subject *Algebraic Methods for Number Theory.*

Observation 3.3.5 Let R be a Dedekind domain that is UFD. By the Proposition 3.2.11 we have that R is a PID, hence $\mathcal{F}(R) = \mathcal{P}(R)$. Therefore $\mathcal{C}(R) \cong \{1\}$. If R is obtained through a number field then the class number of R would be 1. That is, the ring of integers is a UFD if and only if it class number is 1. This problem is very important and is not solved in general. When the number field is a quadratic imaginary extension of $\mathbb{Q}$, in other words is of the form $\mathbb{Q}(\sqrt{D})$ where $D < 0$ is an integer. Then it is know that there are only finitely many values of D satisfying this property and the list of these numbers is also known.

Example 3.3.6 It is known that the class number of the field extension $\mathbb{Q}[\sqrt{-5}]$ is 2. That is, $\left|\mathcal{C}(\mathbb{Z}[\sqrt{-5}])\right| = 2$. As we will see in Example 4.2.2, the ideal $(2, \sqrt{-5})$ is not principal. Hence is not trivial at the class group, therefore $\mathcal{C}(\mathbb{Z}[\sqrt{-5}]) = \left\{\overline{R}, \overline{(2, \sqrt{-5})}\right\}$

Chapter 4

Modules over a Dedekind Domain

We saw in the Section 2.1 that every finitely generated module over PID has a nice form, specifically, can be described by a direct sum of the torsion part and the torsion-free part. The torsion part is a direct sum of cyclic modules and the torsion-free part is a free module. Now in this chapter we will try to do the same but with Dedekind rings. This generalization of the ring changes the decomposition and the proofs of it, specially the results about the torsion-free part.

4.1 Finitely Generated Modules over a Dedekind Domain

We will begin this section proving some properties of torsion-free, projective and torsion modules over a Dedekind domain that are finitely generated. The first result gives a way to decompose finitely generated torsion-free modules, but as we will see later, this form is not unique.

Proposition 4.1.1 *Let R be a Dedekind ring and M a finitely generated torsion-free R-module. Then we have that $M \cong I_1 \oplus \cdots \oplus I_n$ where I_i is an ideal of R for each i.*

PROOF: The proof is by induction on $\operatorname{rank}(M) \geq 0$. If $\operatorname{rank}(M) = 0$ then M is torsion, thus $M = 0$ by Proposition A.2.6 since M is torsion-free. Assume now that $\operatorname{rank}(M) = n + 1 \geq 1$ and choose a nonzero $m \in M$, so that $\operatorname{rank}(Rm) = 1$. Then

$$0 \longrightarrow Rm \xrightarrow{i} M \xrightarrow{p} M'' \longrightarrow 0$$

is an exact sequence, where $M'' = M/Rm$ and p is the projection map. Note that by Proposition A.2.6 we have that $\operatorname{rank}(M'') = n$ because it is exact, $\operatorname{rank}(M) = n + 1$ and $\operatorname{rank}(Rm) = 1$. Now M is finitely generated, this implies that M'' is also finitely generated. Let $T = t(M'')$ the torsion submodule of M'' then M''/T is a finitely generated torsion-free R-module with $\operatorname{rank}(M''/T) = \operatorname{rank}(M'') = n$, because $\operatorname{rank}(T) = 0$. By induction M''/T is a direct sum of ideals of R, since R is a Dedekind domain its ideals are projective (by the Theorem 3.2.13) and hence M''/T is projective. Define

$$M' = p^{-1}(T) = \{x \in M \,:\, rx \in Rm \text{ for some } r \neq 0\} \subseteq M$$

There is an exact sequence $0 \longrightarrow M' \longrightarrow M \longrightarrow M''/T \longrightarrow 0$ and splits (because M''/T is projective) that is $M \cong M' \oplus (M''/T)$. Hence

$$\operatorname{rank}(M') = \operatorname{rank}(M) - \operatorname{rank}(M''/T) = 1.$$

Since R is noetherian, every submodule of a finitely generated R-module is itself finitely generated, hence M' is finitely generated. Therefore M' is isomorphic to an ideal by Proposition A.2.6 and this completes the proof. □

The next result characterizes the torsion-free modules over a Dedekind ring thanks to Proposition 4.1.1 and the fact that the sum of projective modules is a projective module.

Proposition 4.1.2 *Let R be a Dedekind ring and M a finite generated R-module. Then M is torsion-free if and only if M is projective.*

Proof: By the Theorem 3.2.13 we know that every ideal in a Dedekind ring is projective. By the Proposition 4.1.1 we have that M is a direct sum of ideals, then it is a direct sum of projective modules. Hence a projective module.
Conversely, if M is projective then there exists $n \in \mathbb{N}$ such that $M \subseteq R^n$, this implies that it is torsion-free (since R is a domain). □

Corollary 4.1.3 *Let R be a Dedekind ring and M a finitely generated R-module. Then we have that $M = P \oplus tM$ where P is a projective submodule of M isomorphic to M/tM.*

Proof: First note that the quotient module M/tM is a finitely generated torsion-free R-module, so it is projective by the previous proposition. Therefore the following exact sequence splits by Proposition A.4.3

$$0 \longrightarrow tM \longrightarrow M \longrightarrow M/tM \longrightarrow 0$$

Therefore $M \cong \big(M/tM\big) \oplus tM$ and the result is proved. □

Proposition 4.1.4 *Let R be a Dedekind ring and let M, M' be finitely generated R-modules. Then $M \cong M'$ if and only if $tM \cong tM'$ and $M/tM \cong M'/tM'$.*

Proof: The argument is very similar to the proof of the Proposition 2.3.1 ii). □

We have reached the "basic" decomposition, that is, every finitely generated module over a Dedekind rings is the direct sum of the torsion part and the torsion-free part. Moreover we proved that this decomposition is unique up to isomorphism. Also we proved that this torsion-free part has a nice form, it is the direct sum of ideals of R. Now we do the same for the torsion part. We will see that it is the direct sum of cyclic torsion modules. First we begin showing that there is an isomorphism between a $\mathfrak{p}$-primary module and its localisation at the prime $\mathfrak{p}$.

Definition 4.1.5 Let R be a Dedekind ring and T a finitely generated torsion R-module. Let $\mathfrak{p}_i$ be a prime ideal of R, then the $\mathfrak{p}_i$-primary component of T is

$$T[\mathfrak{p}_i] = \big\{ m \in T \, : \, \mathrm{ann}(m) \text{ is a power of } \mathfrak{p}_i \big\}.$$

In the case where $M = T[\mathfrak{p}_i]$ then the module is called $\mathfrak{p}$-primary.

Observation 4.1.6 By the Observation 2.2.5 we have that $T[\mathfrak{p}_i]$ are submodules of M because the ideals of a Dedekind domain have a divisibility theory as we remark at the Proposition 3.2.16. Also we have the property that when M is finitely generated $\mathfrak{p}$-primary then $\mathrm{ann}(M) = \mathfrak{p}^n$ for some $n \geq 1$. The proof is done in the Observation 2.2.6.

Proposition 4.1.7 *Let $\mathfrak{p}$ be a nonzero prime ideal in a Dedekind ring R and M an R-module with* $\operatorname{ann}(M) = \mathfrak{p}^e$ *for some $e > 0$. Then the localization map $M \longrightarrow M_{\mathfrak{p}}$ is an isomorphism (and hence M may be regarded as an $R_{\mathfrak{p}}$ module).*

Proof: It suffices to prove that $M \cong R_{\mathfrak{p}} \otimes_R M$. If $m \in M$ is nonzero and $s \in R \backslash \mathfrak{p}$ then

$$\mathfrak{p}^e + Rs = R$$

Hence there exist $u \in \mathfrak{p}^e$ and $r \in R$ with $1 = u + rs$ and so $m = rm + rsm = rsm$ because $\operatorname{ann}(M) = \mathfrak{p}^e$. Then we see that $s^{-1}m = rm \in M$, thus we can define $s^{-1}m$ in M. We have to see that this is well defined. If $1 = u' + r's$ where $u' \in \mathfrak{p}^e$ and $r' \in R$ then $s(r - r')m = 0$, so that

$$s(r - r') \in \operatorname{ann}(M) = \mathfrak{p}^e$$

Now by Corollary 3.2.17 since $s \notin \mathfrak{p}^e$ it follows that $\mathfrak{p}^e$ is not in the prime factorization of Rs. If $r - r' \notin \mathfrak{p}^e$ then $\mathfrak{p}^e$ does not appear on the prime factorization of $Rs(r - r')$, this is a contradiction because $s(r - r') \in \mathfrak{p}^e$. Thus $r - r' \in \mathfrak{p}^e$, this implies that $rm = r'm$ and since $m = rsm$ we have that $s^{-1}m$ is well defined.

Let $f : R_{\mathfrak{p}} \times M \longrightarrow M$ be the map defined by $f(r/s, m) = rs^{-1}m$. This map is R-bilinear and so there is an R-map $\tilde{f} : R_{\mathfrak{p}} \otimes M \longrightarrow M$, it is surjective and has inverse, $h_M : M \longrightarrow R_{\mathfrak{p}} \otimes M$ defined by $h_M(m) = 1 \otimes m$. □

The next goal is to prove the Primary Decomposition Theorem when the ring is a Dedekind Domain. For the proof, we have to use the following lemma that is a consequence from the divisibility ideal theory of the Dedekind Domains.

Lemma 4.1.8 *Let $I_1, \ldots, I_n$ be ideals in a Dedekind ring R. If there is no nonzero prime ideal $\mathfrak{p}$ with $I_i = \mathfrak{p}L_i$ for all i for some ideals L_i then $I_1 + \cdots + I_n = R$.*

Proof: First we factorize every ideal I_i in to product of prime ideals, then we proceed to calculate the first sum $I_1 + I_2$ with the help of Proposition 3.2.16 iii). We keep doing this, since all the ideals I_i does not have a common prime, this sum finalize with all the primes exponent equals to 0. □

Theorem 4.1.9 (Primary Decomposition) *Let R be a Dedekind ring and T a finitely generated torsion R-module. If $I = \operatorname{ann}(T) = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_n^{e_n}$, then $T = T[\mathfrak{p}_1] \oplus \cdots \oplus T[\mathfrak{p}_n]$.*

Proof: We now check that the sum is direct. Let W_i the submodule of T generated by all $T[\mathfrak{p}_j]$ with $j \neq i$ and $I_i = \prod_{j \neq i} \mathfrak{p}_j^{e_j}$ then $\mathfrak{p}_i$ and I_i are coprime. Hence there are $a_i \in \mathfrak{p}_i$ and $r_i \in I$ with $1 = a_i + r_i$. Let $x \in T[\mathfrak{p}_i] \cap W_i$ then $x = a_i x + r_i x$ but $a_i x = 0$ and $r_i x = 0$ this implies $x = 0$. Therefore $T[\mathfrak{p}_i] \cap W = \{0\}$, then $T[\mathfrak{p}_i]$ are in direct sum.

By the previous Lemma we have

$$I_1 + \cdots + I_n = R$$

thus there are $b_i \in I_i$ with $b_1 + \cdots b_n = 1$. If $t \in T$, then $t = b_1 t + \cdots b_n t$, but if $c_i \in \mathfrak{p}_i^{e_i}$ then $c_i b_i \in \mathfrak{p}_i^{e_i} I_i = I = \operatorname{ann}(T)$ and so $c_i(b_i t) = 0$. Hence $\mathfrak{p}_i^{e_i} \subseteq \operatorname{ann}(b_i t)$ so that $\operatorname{ann}(b_i t) = \mathfrak{p}_i^e$ for some $e > 0$ (because $\mathfrak{p}_i^{e_i} \subseteq \operatorname{ann}(b_i t) \subseteq \mathfrak{p}_i$). Therefore $b_i t \in T[\mathfrak{p}_i]$ and so

$$T = T[\mathfrak{p}_1] \oplus \cdots \oplus T[\mathfrak{p}_n]$$

□

Now we have a decomposition of finitely generated modules over a Dedekind domain. That is, with the results from this section we know that a module can be expressed as a direct sum of a torsion-free submodule and a torsion and these ones decomposes too. The torsion-free submodules is the direct sum of ideals of R and the torsion submodule can be expressed as a direct sum of their $\mathfrak{p}$-primary components.

4.2 Decompositon of Finitely Generated Modules over a Dedekind Domain

The objective of this section is to show the unicity of the decomposition described in the previous section. We will see first of all that the $\mathfrak{p}$-primary modules can be decomposed with a direct sum of cyclic modules and this is unique (as in the PID case). And then we will study the unicity of the torsion-free part that will be more difficult.

Theorem 4.2.1 *Let R be a Dedekind ring. Then the following statements are true:*

i) *Two finitely generated torsion R-modules T and T' are isomorphic if and only if $T[\mathfrak{p}_i] \cong T'[\mathfrak{p}_i]$ for all i.*

ii) *Every finitely generated $\mathfrak{p}$-primary R-module T is a direct sum of cyclic R-modules, and the number of summands of each type is an invariant of T.*

Proof:

i) The result follows from the observation that if $f : T \longrightarrow T'$ is an isomorphism, then $\operatorname{ann}(t) = \operatorname{ann}\big(f(t)\big)$ for all $t \in T$. The other direction is the same as Proposition 2.2.9.

ii) The Primary Decomposition shows that T is the direct sum of its primary components $T[\mathfrak{p}_i]$. By Proposition 4.1.7, $T[\mathfrak{p}_i]$ is an $R_{\mathfrak{p}_i}$-module, but $R_{\mathfrak{p}_i}$ is a PID and so the Basis Theorem and the Fundamental Theorem hold (Theorem 2.3.8 and 2.3.14). We can conclude that each $T[\mathfrak{p}_i]$ is a direct sum of cyclic modules. The number and isomorphic types of cyclic summands are unique determined. □

Now we reached the full decomposition of a finitely generated module over a Dedekind domain. Moreover we have seen that the decomposition of the torsion part is unique. Unfortunately the the decomposition of the free-torsion is not unique. It can be described in a way that is unique under isomorphism. We will see that the invariant of these decompositions is the class of the product of the ideals on the ideal class group.

The next proposition is sometimes surprising because in general the Dedekind domains are not PID but all the ideals are generated by at most two elements. The next example points this property and the fact that not all ideals are principal.

Example 4.2.2 The ring of integers $\mathbb{Z}\big[\sqrt{-5})\big]$ is not principal because the ideal $I = (2, \sqrt{-5})$ can not be generated by one element. If we suppose that this ideal is principal, $I = (a + b\sqrt{-5})$ where $a, b \in \mathbb{Z}$ then $a + b\sqrt{-5}$ divides 2. This implies that the norm of this element divides 4, hence $a^2 - 5b^2$ has to divide 4 in the ring of integers. Then it is immediate to see that $b = 0$ and $a = 1$ and $b = 0$ and $a = 2$ are the only solution to this. The first one is a contradiction because I is a proper ideal and the second one also conducts to a contradiction. Because 2 does not divide $\sqrt{-5}$ since 4 does not divide -5.

Proposition 4.2.3 *Let R be a Dedekind ring*

i) *If $I \subseteq R$ is a nonzero ideal, then every ideal in R/I is principal.*

ii) *Every fractional ideal J can be generated by two elements. More generally for any nonzero $a \in J$ there exists $b \in J$ with $J = (a, b)$.*

Proof:

i) First note that for every prime ideal $\mathfrak{p}$ we have that $R/\mathfrak{p}^n \cong R_{\mathfrak{p}}/(\mathfrak{p}^n)_{\mathfrak{p}}$ since $R/\mathfrak{p}^n$ is a local ring that has $\mathfrak{p}$ as a maximal ideal. Then $R/\mathfrak{p}^n$ is a principal ideal ring (because $R_{\mathfrak{p}}$ is principal). Let $I = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_n^{e_n}$, since the ideals $\mathfrak{p}_i^{e_i}$ are pairwise coprimes we have by the Chinese Remainder Theorem that
$$R/I = R/(\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_n^{e_n}) \cong R/\mathfrak{p}_1^{e_1} \times \cdots \times R/\mathfrak{p}_n^{e_n}$$
hence is a PID.

ii) First we prove the statement for an ideal $J \subseteq R$. Choose a nonzero element $a \in J$. By i) we have that the ideal J/aR in R/aR is principal. Then there exists a $b \in R$ such that J/aR is generated by $b + aR$ hence $J = (a, b)$.
For the general case where J is a fractional ideal, there is a nonzero $c \in R$ with $cJ \subseteq R$. Since $cJ \subseteq R$ is an ideal we have that $cJ = (a', b')$ for $a', b' \in cJ$ thus there are $a, b \in J$ such that $a' = ca$ and $b' = cb$. Therefore $cJ = (ca, cb)$ then it follows that $J = (a, b)$. □

Corollary 4.2.4 *If I and J are fractional ideals over a Dedekind ring R, then there are $a, b \in \mathrm{Frac}(R)$ such that*
$$aI + bJ = R$$

Proof: First choose a nonzero $a \in I^{-1}$. Now $aI \subseteq I^{-1}I = R$ so that $aIJ^{-1} \subseteq J^{-1}$. By the previous proposition there is an element $b \in J^{-1}$ such that $J^{-1} = aIJ^{-1} + bR$.
Since $b \in J^{-1} \Rightarrow bJ \subseteq R$ and we can multiply the previous expression by J, so
$$R = JJ^{-1} = J(aIJ^{-1} + bR) = aI + bRJ = aI + bJ$$
□

With the previous corollary we can decompose the torsion-free modules over a Dedekind domain in another way. This decomposition together with the cancellation property will allow us to prove the uniqueness of these direct sums.

Proposition 4.2.5 *Let R be a Dedekind domain with $Q = \mathrm{Frac}(R)$. Then two fractional I, J ideals of R are isomorphic if and only if there exist some $c \in Q$ such that $I = cJ$.*

Proof: If $I = cJ$ for some $c \in Q$ then $I \cong J$ with the morphism $\varphi : J \longrightarrow I$ defined by $\varphi(x) = cx$. Now suppose that $f : J \longrightarrow I$ is an isomorphism. Then we can consider the morphism $f : J \longrightarrow Q$ that is obtained composing f with the inclusion $I \longrightarrow Q$. Then $f : J \longrightarrow Q$ is a monomorphism and since Q is

an injective R-module (Example A.4.17), there is an R-morphism $g : Q \longrightarrow Q$ extending f. Now we will see that $g(x) = cx$ for some $c \in Q$.
First note that $g_{|_R} : R \longrightarrow Q$ is an R-morphism and for every $a, b \in R$ then

$$ag_{|_R}(b) = g_{|_R}(ab) = bg_{|_R}(a) \quad \Rightarrow \quad g_{|_R}(a)/a = g_{|_R}(b)/b = c \in Q \quad \Rightarrow \quad g_{|_R}(a) = ca$$

for every $a \in R$. Let $x \in Q$, then $x = r/s$ where $r, s \in R$. This implies that $r = sx$ and $g(sx) = g(r)$. But $g(sx) = sg(x)$ and $g(r) = g_{|_R}(r) = cr$. Therefore $g(x) = g(r)/s = c(r/s)$. □

Observe that the previous proposition characterizes the isomorphisms between ideals of a Dedekind domain. With that in mind we can prove the next result that simplifies the decomposition of a torsion-free module.

Lemma 4.2.6 *Let M be a finitely generated torsion-free R-module, where R is a Dedekind ring, so that $M \cong I_1 \oplus \cdots \oplus I_n$ where the I_i are ideals. Then $M \cong R^{n-1} \oplus J$ where $J = I_1 \cdots I_n$.*

Proof: It suffices to prove that $I \oplus J \cong R \oplus IJ$ and then do induction. By the previous corollary there are nonzero $a, b \in \mathrm{Frac}(R)$ with $aI + bJ = R$ and since $aI \cong I$ and $bJ \cong J$ (by the previous proposition) we can assume that I and J are coprime ideals of R. There is an exact sequence

$$0 \longrightarrow I \cap J \xrightarrow{\delta} I \oplus J \xrightarrow{\alpha} I + J \longrightarrow 0$$

where $\delta(x) = (x, x)$ and $\alpha(u, v) = u - v$. Since I and J are coprime, we have $I \cap J = IJ$ and $I + J = R$. Since R is projective this sequence splits, that is $I \oplus J \cong R \oplus IJ$. □

The next proposition states a very important property that a module can have, the cancellation one. An R-module M is said to be *cancellative* if $R^n \oplus M \cong R^n N$ implies that $M \cong N$. For example if R is a PID we saw that every R-module has this property. In this case, if R is a Dedekind Domain then every module is cancellative too. It is a powerfull result, and here we will prove it with the exterior power construction (done in section A.2).

Proposition 4.2.7 *Let R be a Dedekind ring. If $R \oplus G \cong R \oplus H$ where G and H are R-modules then $G \cong H$.*

Proof: First we can assume that there is a module $E = A \oplus G = B \oplus H$ where $A \cong R \cong B$. Our objective is to reduce this problem for the case where G and H are ideals. Let $p : E \longrightarrow B$ the projection $p(b, h) \mapsto b$ and consider $p_{|_G}$. Now

$$\ker(p_{|_G}) = G \cap H \quad \text{and} \quad \mathrm{im}(p_{|_G}) \subseteq B \cong R$$

If $\mathrm{im}(p_{|_G}) = 0$ (the degenerated case) then $G \subseteq \ker(p) = H$. Now we can consider an other projection morphism $p' : E \longrightarrow G$ where $p'(a, g) \mapsto g$ and the restriction to H is also a retraction (that is $p'_{|_H} \circ j = \mathrm{Id}_G$ where $j : G \longrightarrow H$ is the inclusion morphism). Then the following exact sequence splits

$$0 \longrightarrow \ker(p'_{|_H}) \xrightarrow{i} H \xrightarrow{p'_{|_H}} G \longrightarrow 0$$

Thus $H \cong G \oplus \ker(p'_{|_H}) = G \oplus (A \cap H)$. Now we have $E/G = (A \oplus G)/G \cong A \cong R$ but since $G \subseteq H$ we have also that $E/G = (B \oplus H)/G \cong B \oplus (H/G) \cong R \oplus (H/G)$ because the following exact sequence and the First Isomorphism Theorem

$$0 \longrightarrow G \longrightarrow E \longrightarrow B \oplus (H/G) \longrightarrow 0$$

Thus $R \cong R \oplus (H/G)$. This isomorphism is an R-module isomorphism, then the submodules $R \oplus 0$ and $0 \oplus (H/G)$ can be thought as an ideals I and J of R. Then if $a \in I$ and $b \in J$ we have $a \cdot b \in I \cap J$ but throught the isomorphism this corresponds to $\big(R \oplus 0\big) \cap \big(0 \oplus (H/G)\big) = 0$. Hence $H/G = 0$ because R is a domain, this implies that $G = H$.

If $L = \operatorname{im}(p_{|_G})$ is a nonzero ideal then with the First Isomorphism Theorem we have that $G/(G \cap H) \cong L$. Since R is a Dedekind ring, L is a projective module and so the following exact sequence splits

$$0 \longrightarrow G \cap H \longrightarrow G \longrightarrow L \longrightarrow 0$$

Then $G \cong L \oplus (G \cap H)$ that is $G = I \oplus (G \cap H)$ where $I \cong L$.

With the same arguments we get that $H = J \oplus (G \cap H)$ where J is isomorphic to an ideal of R. Therefore

$$E = A \oplus G = A \oplus I \oplus (G \cap H)$$
$$E = B \oplus H = B \oplus J \oplus (G \cap H)$$

It follows that

$$A \oplus I \cong E/(G \cap H) \cong B \oplus H$$

If we prove that $I \cong J$ we will get that

$$G = I \oplus (G \cap H) \cong J \oplus (G \cap H) = H$$

Therefore, we have reduced the theorem to the special case where G and H are nonzero ideals. For this, we will use the exterior powers and some properties.

Suppose that $R \oplus I \cong R \oplus J$. First note that by the Theorem A.2.17 we have

$$\bigwedge^2 (R \oplus I) \cong \Big(R \otimes \bigwedge^2 I\Big) \oplus \Big(\bigwedge^1 R \otimes \bigwedge^1 I\Big) \oplus \Big(\bigwedge^2 R \otimes I\Big)$$

But $\bigwedge^2 R = \{0\}$ by the Corollary A.2.14 and $\bigwedge^1 R \otimes \bigwedge^1 I \cong R \otimes I \cong I$. We now show, for every maximal ideal $\mathfrak{m}$, that $\big(\bigwedge^2 I\big)_{\mathfrak{m}} = \{0\}$. By the Proposition A.2.15 we have

$$\Big(\bigwedge^p I\Big)_{\mathfrak{m}} \cong \bigwedge^p I_{\mathfrak{m}}$$

since R_m is an R-algebra. We know that $R_{\mathfrak{m}}$ is a PID, so $I_{\mathfrak{m}}$ is a principal ideal and hence

$$\Big(\bigwedge^2 I\Big)_{\mathfrak{m}} \cong \bigwedge^2 I_{\mathfrak{m}} = \{0\}$$

Finally we have that $\bigwedge^2 (R \oplus I) \cong I$ and then

$$R \oplus I \cong R \oplus J \quad \Rightarrow \quad \bigwedge^2 (R \oplus I) \cong \bigwedge^2 (R \oplus J) \quad \Rightarrow \quad I \cong J$$

□

All these results lead to the Steinitz theorem that characterizes the direct sum decomposition of the finitely generated torsion-free modules over a Dedekind domain. Also giving the uniqueness of this decomposition.

Theorem 4.2.8 (Steinitz) *Let R be a Dedekind ring, and let $M \cong I_1 \oplus \cdots \oplus I_n$ and $M' \cong I'_1 \oplus \cdots \oplus I'_l$ be finitely generated torsion-free R-modules where I_i and I'_i are fractional ideals of R. Then $M \cong M'$ if and only if $n = l$ and $I_1 \cdots I_n \cong I'_1 \cdots I'_n$.*

Proof: First of all by the Proposition A.2.6 iii) we have that every R-submodule I of $Q = \mathrm{Frac}(R)$ has $\mathrm{rank}(I) = 1$. Then the same proposition part i) shows that

$$\mathrm{rank}(M) = \sum_{i=1}^{n} \mathrm{rank}(I_i) = n$$

Since $M \cong M'$ we have that $Q \otimes_R M \cong Q \otimes_R M'$ so that $\mathrm{rank}(M) = \mathrm{rank}(M')$ and $n = l$. By Lemma 4.2.6 it suffices to prove that if $R^n \oplus I \cong R^n \oplus J$ then $I \cong J$. But this is the previous proposition that we proved with the exterior power. □

This chapter can be concluded with the following theorem which gives the full decomposition of finitely generated modules over a Dedekind ring. Observe that the unicity is given by the equivalence class of the ideal class group. This is due to Observation 3.3.4 and Proposition 4.2.5.

Theorem 4.2.9 *Let R be a Dedekind ring, and let M be a finitely generated R-module. Then M is of the form $M \cong T \oplus R^n \oplus I$ where T is the finite sum of cyclic primary modules and I is a fractional ideal of R.*
This decomposition is unique up to the equivalence class of I on the ideal class group of R.

Chapter 5

Decomposition of Modules with Cyclic Summands

In this chapter the main goal is to prove that if every R-module can be decomposed into a direct sum of cyclic modules, then this ring R is an Artinian principal ideal ring. For proving this, we choose a demonstration that uses injective modules. Therfore we have to introduce this theory before the Theorem. All these results will not be proven for lack of space. All the proofs can be found in [12].

5.1 Essential Extensions

First of all we will see that every module can be embedded in an injective module, that is, every module is a submodule of an injective module. This, as we will see, it is not trivial.

Lemma 5.1.1 *Every $\mathbb{Z}$-module can be embedded in a injective $\mathbb{Z}$-module.*

Lemma 5.1.2 *Let G be an injective $\mathbb{Z}$-module. Then $\mathrm{Hom}_{\mathbb{Z}}(R, G)$ is an injective R-module.*

Lemma 5.1.3 *Let M be an R-module. Then M can be embedded in the R-module $\mathrm{Hom}_{\mathbb{Z}}(R, M)$*

Theorem 5.1.4 *Every module has an injective extension, with other words that can be embedded in an injective module.*

Definition 5.1.5 Let E be an extension of the R-module M (that is E is a submodule of M). Then E is said to be an essential extension of M is, for every nonzero submodule E' of E then $E' \cap M \neq \{0\}$.

Example 5.1.6 Let R be a domain. Then its field K of fractions is an essential extension of R (when are considered as an R-modules). It is very immediate to prove this: Let I be a nonzero R-submodule of K, then it has a nonzero element, say $a \in I$. In particular $a \in K$, therefore there exist an $r \in R$ such that $ra \in R$. By the definition of a submodule we have that $ra \in I$, that is $ra \in I \cap R$ and we supposed that R was a domain. Hence ra is a nonzero element of R.

Definition 5.1.7 Let M be an R-module and E an extension of M. Then R is said to be a maximal essential extension of M if satisfies that

i) E is an essential extension of M.

ii) Whenever E' is a proper extension of E, then E' us not an essential extension of M.

Definition 5.1.8 Let M be an R-module and E an extension of N. Then N is said to be a minimal injective extension of M if satisfies

i) N is injective.

ii) Whenever N' is a proper submodule of N which contains M, then N' is not injective.

Proposition 5.1.9 *Let M be an R-module and let N be an injective extension of M. Then N has a submodule E which is a maximal essential extension of M.*

Proposition 5.1.10 *Let M be an R-module and let E be an extension of M. Then the following statements are equivalent:*

i) *E is an essential injective extension of M.*

ii) *E is a maximal essential extension of M.*

iii) *E is a minimal injective extension of M.*

Theorem 5.1.11 *Let M be an R-module. Then theer exists an R-module E satisfying the following equivalent conditions:*

i) *E is an essential injective extension of M.*

ii) *E is a maximal essential extension of M.*

iii) *E is a minimal injective extension of M.*

Moreover, if E_1 and E_2 are both essential injective extensions of A, then there is an isomorphism $\theta : E_1 \longrightarrow E_2$ such that the following diagram is commutative.

$$\begin{tikzcd}
A \arrow[d, "inc"'] \arrow[dr, "inc"] & \\
E_1 \arrow[r, "\theta"] & E_2
\end{tikzcd}$$

Definition 5.1.12 Let M be an R-module. An R-module E satisfying the conditions of the previous Theorem is called an injective envelope of M. We use the notation $E(M)$ to denote the injective envelope of M.

Observation 5.1.13 An R-module M is injective if and only if $M = E(M)$. Also if M is an R-module and N is a submodule of $E(A)$ which contains M then $E(M)$ is also an injective envelope of N.

Example 5.1.14 Let R be a commutative domain. Then the field of fractions of R, when is considered as an R-module, is an injective envelope. First of all we knew that the field of fractions is an injective R-module (we saw it on the Observation 2.1.17). Then by the Example 5.1.6 we know that is an injective essential extension and hence, an injective envelope of R.

Proposition 5.1.15 *Let M be an R-module. Then the following statements are equivalent:*

i) *M is injective.*

ii) *M is a direct summand of every extension of itself.*

Definition 5.1.16 An R-module M is said to be finitely embedded if there exist finitely many simple module $S_1, \ldots, S_n$ such that

$$E(M) \cong E(S_1) \oplus \cdots \oplus E(S_n)$$

Proposition 5.1.17 *Let M be a finitely embedded R-module. Then every submodule of M is finitely embedded.*

Theorem 5.1.18 *Let M be an R-module. Then the following statements are equivalent:*

i) *M is Artinian.*

ii) *Every factor module of M is finitely embedded.*

Theorem 5.1.19 *Let R be a Noetherian ring and M and R-module. Then the following statements are equivalent:*

i) *M is Artinian.*

ii) *M is finitely embedded.*

5.2 Indecomposable Injective Modules

Definition 5.2.1 Let M be an R-module and let N be a submodule of M. Then N is said to be an irreducible submodule if $N \neq M$ and there do not exist submodule N_1, N_2 of M such that $N \subsetneq N_1$, $N \subsetneq N_2$ and $N_1 \cap N_2 = N$.

Proposition 5.2.2 *Let M be an injective R-module. Then the following statements are equivalent:*

i) *M is indecomposable.*

ii) *$M \neq \{0\}$ and is an injective envelope of every nonzero submodule of itself.*

iii) *The zero submodule of M is irreducible*

Corollary 5.2.3 *Let M be an indecomposable injective R-module and suppose that either M or R is Artinian. Then $M = E(S)$ for some simple R-module S.*

Proposition 5.2.4 *Let M be an injective R-module. Then the following statements are equivalent:*

i) *M is indecomposable.*

ii) *The ring of endomorphisms of M is local.*

Proposition 5.2.5 *Let R be a Noetherian ring and M an R-module. Then the following statemnets are equivalent:*

i) *M is an indecomposable injective R-module.*

ii) *$M \cong E(R/P)$ for some prime ideal P of R.*

Proposition 5.2.6 *Let R be a Noetherian ring, then every direct sum of injective R-modules is injective.*

Lemma 5.2.7 *Let M be a nonzero Noetherian R-module. Then M has a submodule K such that $E(K)$ is indecomposable.*

Corollary 5.2.8 *Let R be a Noetherian ring and let M be a nonzero R-module. Then M has a submodule K such that $E(K)$ is indecomposable.*

Now we will use the definition done in Section 2.2 Definition 1.2.9. It says that $c(M) = |I|$ where M is an R-module and I is the set of indexes of the following direct sum:

$$S(M) = \bigoplus_{i \in I} S_i$$

where each S_i is a simple module. For definition $S(M)$ is the sum of all the simple submodules of M and is called the socle of the module M.

Theorem 5.2.9 *The following statements are equivalent:*

i) *R is a Noetherian ring.*

ii) *Every injective R-module is a direct sum of indecomposable (injective) R-modules.*

iii) *There is a cardinal number κ such that every injective R-module is of the form $\bigoplus_{i \in I} M_i$, where $c(M_i) \leq \kappa$ for all $i \in I$.*

Observation 5.2.10 We know that for every R-module M we have

$$c(M) \leq |S(M)| \leq |M|$$

where $||$ denotes the cardinal number of a set. In particular, it follows form the previous Theorem, that a ring R is Noetherian if every injective R-module is the direct sum of a family of finitely generated submodules. Because we have to observe that if M is a finitely generated R-module, then $M = \langle m_1 \rangle + \cdots + \langle m_n \rangle$. Hence

$$|M| \leq |R \oplus \cdots \oplus R| = n|R|$$

and $n|R|$ either is finite or $|R|$. Therefore $c(M) \leq |M| \leq \max \{\aleph_0, |R|\} = \kappa$.

Theorem 5.2.11 *The following statements are equivalent:*

i) *R is an Artinian ring.*

ii) *Every injective R-module is a direct sum of a family of injective envelopes of simple modules.*

Corollary 5.2.12 *Let R be a Noetherian ring. Then the following statements are equivalent:*

i) *R is Artinian.*

ii) *Every prime ideal of R is maximal.*

5.3 Characterization of Cyclic Decomposition

Proposition 5.3.1 *Let R be a Noetherian ring. Then the following statements are equivalent*

i) *R is Artinian.*

ii) *Every indecomposable injective R-module is Noetherian.*

Lemma 5.3.2 *Let R be a quasi local ring with a maximal ideal M and let U be an R-module with the property that every finitely generated submodule of U is cyclic. Then the submodules of U are totally ordered.*

Corollary 5.3.3 *Let R be a quasi local ring with maximal ideals M and let $E = (E/M$- Suppose taht every finitely generated submodule of E is cyclic. Then the ideals of R are totally ordered.*

Lemma 5.3.4 *Let R be a quasi local ring. Then the following statements are equivalent:*

i) *R is a principal ideal ring.*

ii) *There is an element p of R such that every nonzero ideal of R is of the form p^nR, wherer $n \geq 0$.*

iii) *The ideals of R are totally ordered.*

Lemma 5.3.5 *Let R be a local Artinian principal ring. Then R/I is self-injective for every ideal I of R.*

Definition 5.3.6 A ring is said to be self-injective if it is injective as a module over itslef.

Lemma 5.3.7 *Let R be a local ring such that every ring R/I is self-injective for every ideal I of R. Then the ideals of R are totally ordered.*

Lemma 5.3.8 *Let R be a local Artinian ring. Then the following statements are equivalent:*

i) *R is a principal ideal ring.*

ii) *There is an element $p \in R$ and $n \geq 1$ such that the ideals of R are precisely R, pR, $p^2R, \ldots, p^nR$, being all distinct.*

iii) *The ideals of R are totally ordered.*

iv) *For every ideal I of R, the ring R/I is self-injective.*

Theorem 5.3.9 *Let R be a ring. Then the following statements are equivalent:*

i) *Every R-module is a direct sum of cyclic submodules.*

ii) *R is an Artinian principal ideal ring.*

iii) *R is Noetherian and, for every ideal I of R, the ring R/I is self-injective.*

Proof: Our first goal is to reduce the proof for local Artinian rings. To achieve this first part we have to deduce for each statement that the ring R is Artinian. Assume i), then the Observation 5.2.10 gives that R is Noetherian. Also i) gives that every indecomposable injective R-module if cyclic, and so Noetherian. Then by the Proposition 5.3.1 R is Artinian. It is immediate that ii) implies that R is Artinian. Now assume iii) and consider a prime ideal P of R. We know that the domain R/P as a module over itself has its field of fraction as an injective envelope (as we saw in Example 5.1.14). By hypothesis R/P is a self-injective ring, therefore R/P is a field and P is a maximal ideal. Hence, by the Corollary 5.2.12 we have that R is Artinian. Thus, to prove the equivalence of i), ii), iii), we can take R to be Artinian, so a direct sum of local Artinian rings (Theorem A.3.15). Say

$$R = R_1 \oplus R_2 \oplus \cdots \oplus R_n$$

We must next see that it is sufficient to prove the equivalence of i), ii), iii) when R is a local Artinian ring. We will do this by proving that R satisfies i) if and only if each R_i satisfies i); and similary of ii) and iii). Observe that

$$1_R = e_1 + e_2 + \cdots + e_n$$

where $e_i \in R_i$. Then, for each i, e_i is the identity element of R_i (because they are in direct sum). Note that $e_i \cdot e_j = 0$ when $i \neq j$ and $e_i^2 = e_i$. Let L be an R-module. Then

$$L = e_1L \oplus e_2L \oplus \cdots \oplus e_nL.$$

This sum is direct because if $x \in e_iL \cap e_jL$ when $i \neq j$ then $x = e_im = e_jn$ and multiplying by e_i we have that $x = 0$. Also, e_iL can be regarded as an R_i-module as well as an R-module and its submodules are the same in both cases, because

$$(r_1 + \cdots + r_n)e_ix = r_ie_ix$$

wherer $r_j \in R_j$ and $x \in L$. Thus $e_ixR = e_ixR_i$ and hence, the cyclic submodules of e_iL are the same whether it is regarded as an R module or as an R_i-module. It follows that if, for $1 \leq i \leq n$, every R_i-module is a direct sum of cyclic submodules, then every R-module is a direct sum of submodules. Conversely, let $1 \leq i \leq n$ and consider an R_i-module L_i. We can regard L_i as an R-module:

$$rx_i = (r_1 + r_2 + \cdots + r_n)x_i = r_ix_i = (re_i)x_i$$

where $r_j \in R_j$ and $x_i \in L_i$. Further $Rx_i = R_ix_i$, so the cyclic submodules of L_i are the same whether it is regarded as an R_i-module or as an R-module. Therefore the converse is also true.
Now we prove the same thing but for ii). Let I be an ideal of R, we can write

$$I = e_1I \oplus e_2I \oplus \cdots \oplus e_nI$$

and e_jI can be regarded as an ideal of the ring R_j for every $1 \leq j \leq n$. Suppose that, for $1 \leq j \leq n$ every ideal of R_j is principal. Then $e_jI = a_jR_j$ where $a_j \in R_j$, so

$$I = R(a_1 + a_2 + \cdots + a_n).$$

Thus evert ideal of R is principal. Conversely, every ideal of R_j can be regarded as an ideal of R, for $1 \leq j \leq n$. And an ideal of R_j is principal as an R_j-ideal if and only if it is principal as an R-ideal. Thus, the converse is true.

Now it only remains to consider iii). let I_j an ideal of R_j. Let $\varphi_j : R \longrightarrow R_j$ be the projection mapping. Put $I = \varphi_j^{-1}(I_j)$. Then I is an ideal of R and $R/I \cong R_j/I_j$ (First Isomorphism Theorem of rings). If we suppose that R/I is a self-injective ring, then R_j/I_j is a self-injective ring. Conversely, consider an ieal I of R. Now

$$R/I = \big(R_1 \oplus \cdots \oplus R_n\big)/I = (R_1 + I)/I \oplus \cdots \oplus (R_n + I)/I.$$

This express the ring R/I as a direct sum of rings. By the Second Isomorphism Theorem we have $(R_j + I)/I \cong R_j/(I \cap R_j)$. Thus, if we assume that R_j/I_j is a self-injective ring for every ideal I_j then we have expressed R/I as a direct sum of self-injective rings. Thus, to deduce that R/I is self-injective ring, we need to show that a direct sum of self-injectives rigns is self-injective. To do this, we shall simplify the notation. Suppose that we have a direct sum

$$R = R_1 \oplus \cdots \oplus R_n$$

where the rings R_j are self-injective. Consider an R-module L which has R as a submodule. We have

$$L = e_1 L \oplus \cdots \oplus e_n L.$$

Then each $e_j L$ can be considered as an R_j-module, with R_j as a submodule. It follows from Proposition 5.1.10 that R_j is a direct summand of $e_j L$ as an R_j-module. Since the R-submodules and R_j-submodules of $e_j L$ are the same, R_j is a direct summand of $e_j L$ as an R-module. Thus R is a direct summand of L. This shows that R is a self-injective ring because we considered any module L which has R as a submodule (Proposition 5.1.10).

Now we have to prove the equivalence of i), ii) and iii), but we can add the assuption that R is a local Artinian ring, with a maximal ideal M. The equivalence of ii) and iii) follows form Lemma 5.3.8 and Proposition A.3.9. Now assume i) and consider a submodule of N of $E(R/M)$ (note that R/M is a simple module). Then N is a direct sum of cyclic submodules, but the zero submodule of $E(R/M)$ is irreducible (Proposition 5.2.2). So N must actually be cyclic. It follows form the Corollary 5.3.3 that the ideals of R are totally ordered. Therefore by Lemma 5.3.8, R is a principal ideal ring. This proves i)⇒ii).

It only remains ro assume ii) and iii) and deduce i). We are also assuming that R is a local Artinian ring, so from Lemma 5.3.8 we have that the ideals of R can be written as follows:

$$R,\ Rp,\ Rp^2,\ \ldots,\ Rp^{s-1},\ Rp^s = 0$$

these being all distincts. Consider an R-module N. Let A be a maximal family of submodules of N of the form Rx where $(0 : x) = 0$, whose sum is direct. If N has an element x such that $(0 : x) = 0$ then this family exists because we can apply Zorn's Lemma. Let F_0 be the sum of the members of A (or be 0 if there no exists any A). Then we may write

$$F_0 \cong \bigoplus_{i \in I_0} R.$$

Since R is a self-injective ring and is also Noetherian, F_0 is injective by the Proposition 5.2.6. Hence we can write

$$N = F_0 + N_1$$

where N_1 is a submodule of N. Consider an element $x_1 \in N_1$. Now $(0 : x) \neq 0$ for the maximality of A. Let $r \in R$ such that $rx_1 = 0$ and $r \neq 0$. We can write $r = up^l$ where u is a unit of R and $l < s$, so that $p^{s-1}x_1 = 0$. This is true for all $x \in N_1$, so that $Rp^{s-1} \subseteq \operatorname{ann}_R(N_1)$. If $s = 1$, this means that $N_1 = 0$.

Suppose that $s > 1$. Let $\overline{R} = R/Rp^{s-1}$ and denote the natural image of p in $\overline{R}$ by $\overline{p}$. Now $\overline{R}$ as well as R is a local Artinian principal ideal ring, and its ideals are

$$\overline{R},\ \overline{R}\overline{p},\ \overline{R}\overline{p}^2,\ \ldots,\ \overline{R}\overline{p}^{s-1} = \overline{0}.$$

Moreover, N_1 may be regarded as an $\overline{R}$-module. It follows from above that we can write

$$N_1 = F_1 \oplus N_2$$

where F_1 and N_2 are $\overline{R}$-submodules of N_1

$$F_1 \cong \bigoplus_{i \in I_1} \overline{R}, \qquad \overline{R}\overline{p}^{s-2} \subseteq \operatorname{ann}_{\overline{R}}(N_2).$$

If $s = 2$ then $N_2 = 0$. If $s > 2$ we now regard N_2 as a module over the ring R/Rp^{s-2} and continue as before. In this way, we obtain

$$N = F_0 \oplus F_1 \oplus \cdots \oplus F_{s-1}$$

where $\quad F_k \cong \bigoplus_{i \in I_k} R/Rp^{s-k} \quad$ for $0 \leq k \leq s-1$. This establishes i). □

Conclusions

On this work we achieved the goals that the tutor has initially propose. That is the study of the structure of finitely generated modules over a PID and over a Dedekind domain. Also we have gone further in this topic with the last chapter characterizing the rings whose modules are the direct sum of cyclic modules.

One could summarize this work by saying that it only proves existence theorems of direct sum decomposition of modules and the unicity of these. I think that this reduction is not fair. For me it goes beyond that, it also proves some characterizations of the rings that satisfies that every module is the direct sum of some module type. This point of view starts at the beginning characterizing the rings that every module is semisimple. On the modules over PID this question is recovered concluding that a Noetherian Domain is a PID if and only if every finitely generated module is the direct sum of cyclic modules. This characterization lead to the last chapter where the Noetherianity, domain and finitely generated is removed from the statement.

Throughout this work I learned a lot of things. I delved into the commutative module theory and commutative ring theory, in particular on Dedekind domains and Injective modules. I also have learned some methods related to Category Theory for example for proving some results about the exterior power.

This work also improved my LaTeX writing skills. I have to admit that for me, the most difficult thing (besides from the mathematical part) it was the language. I am used to read and listen English, but I do not write often in this idiom. It has supposed for me an extra effort to taker care that everything was well wrote.

Along this semester I realized how much I like search, think, prove and read mathematics. In particular I discover the book Injective Modules of Sharpe and Vamos ([12]) which I really enjoyed reading. This book has encouraged me to do the final chapter and do it through injective modules.

Bibliography

[1] Anderson, Frank W.; Fuller, Kent R. *Rings and categories of modules.* Second edition. Graduate Texts in Mathematics, **13**. Springer-Verlag, New York, 1992.

[2] Atiyah, M. F.; Macdonald, I. G. *Introduction to commutative algebra.* Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont. 1969

[3] Cohen, I. S.; Kaplansky, I. *Rings for which every module is a direct sum of cyclic modules.* Math. Z. **54** (1951), 97–101.

[4] Cohn, P. M. *Algebra. Vol. 2.* Second edition. John Wiley & Sons, Ltd., Chichester, 1989.

[5] Facchini, Alberto *Module theory. Endomorphism rings and direct sum decompositions in some classes of modules.* Progress in Mathematics, **167**. Birkhäuser Verlag, Basel, 1998.

[6] Gopalakrishnan, N. S. *Commutative algebra.* Oxonian Press Pvt. Ltd., New Delhi, 1984.

[7] Jacobson, Nathan, *Basic algebra. I. Second edition.* W. H. Freeman and Company, New York, 1985.

[8] Kaplansky, Irving *Commutative rings.* Revised edition. The University of Chicago Press, Chicago, Ill.-London, 1974.

[9] Kaplansky, Irving *Modules over Dedekind rings and valuation rings.* Trans. Amer. Math. Soc. **72** (1952), 327–340.

[10] Larsen, Max. D.; McCarthy, Paul J. *Multiplicative theory of ideals.* Pure and Applied Mathematics, Vol. 43. Academic Press, New York-London, 1971.

[11] Rotman, Joseph J. *Advanced modern algebra.* Second edition. Graduate Studies in Mathematics, **114**. American Mathematical Society, Providence, RI, 2010.

[12] Sharpe, D. W.; Vámos, P. *Injective modules.* Cambridge Tracts in Mathematics and Mathematical Physics, No. 62. Cambridge University Press, London-New York, 1972.

[13] Steinitz, Ernst *Rechteckige Systeme und Moduln in algebraischen Zahlköppern.* I. Math. Ann. **71** (1911), no. 3, 328–354.

[14] Uzkov, A. I. *On the decomposition of modules over a commutative ring into direct sums of cyclic submodules.* Mat. Sb. **62** (1963), 469–475.

[15] Warfield, R. B., Jr. *Decomposability of finitely presented modules.* Proc. Amer. Math. Soc. **25** (1970), 167–172.

[16] Zariski, Oscar; Samuel, Pierre *Commutative algebra.* Vol. II. Reprint of the 1960 edition. Graduate Texts in Mathematics, Vol. 29. Springer-Verlag, New York-Heidelberg, 1975.

Appendix: Basic Concepts

This appendix is a survey of all the results that we will use and are done in the optional subject: Introduction to Commutative Algebra. The proof of all the statements can be found in [2].

A.1 Rings and Modules

Definition A.1.1 Let R be a ring, an R-module M is an (additive) abelian group M with a scalar multiplication $R \times M \longrightarrow M$ that for all $m, m' \in M$ and $r, r', 1 \in R$ satisfies:

i) $r(m + m') = rm + rm'$.

ii) $(r + r')m = rm + r'm$.

iii) $(rr')m = r(r'm)$.

iv) $1m = m$.

Proposition A.1.2 *Let R be a ring and $I \subseteq R$ a proper ideal. Then there exists a maximal ideal $\mathfrak{m} \subseteq R$ such that $I \subseteq \mathfrak{m}$.*

Definition A.1.3 Let R be a ring, we say that R is local when it has only one maximal ideal.

Lemma A.1.4 (intersection prime avoidance) *Let $I_1, \ldots, I_n \subseteq A$ be ideals, $\mathfrak{p}$ a prime ideal such that $\bigcap_{j=1}^{n} I_j \subseteq \mathfrak{p}$, then $I_i \subseteq \mathfrak{p}$ for some i (if the equality holds then there exists an i such that $I_i = \mathfrak{p}$).*

Proposition A.1.5 *Let I and J be ideals in a domain R. If $I_\mathfrak{m} = J_\mathfrak{m}$ for every maximal ideal $\mathfrak{m}$, then $I = J$.*

Proposition A.1.6 *If R is a domain, then*

$$\bigcap_{\mathfrak{m}} R_\mathfrak{m} = R$$

where the intersection is over all the maximal ideals $\mathfrak{m}$ in R.

Definition A.1.7 Let M, M', M'' R-modules and $f : M' \longrightarrow M$, $g : M \longrightarrow M''$ two morphisms. We call this an exact sequence

$$0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$$

when f is an homomorphism, g an epimorphism and $\operatorname{im}(f) = \ker(g)$.

Definition A.1.8 A short exact sequence

$$0 \longrightarrow A \xrightarrow{i} B \xrightarrow{p} C \longrightarrow 0$$

is split if there exists an R-homomorphism $j : C \longrightarrow B$ such that $p \circ j = 1_C$. We call such a morphism j a section.

Proposition A.1.9 *Let* $0 \longrightarrow A \xrightarrow{i} B \xrightarrow{p} C \longrightarrow 0$ *be an exact sequence. Then following statements are equivalent:*

i) *This sequence is split.*

ii) *There exists a morphism* $f : B \longrightarrow A$ *such that* $f \circ i = \mathrm{Id}_A$*.*

iii) *There is an isomorphism* $h : B \longrightarrow A \oplus C$ *such that* $h \circ i$ *is the injection of* A *into the direct sum, and* $p \circ h^{-1}$ *is the projection of the direct sum onto* C*.*

A.2 Tensor product and exterior power

For this section we give another reference: For the tensor product [4] section 4.7 and for the exterior power [11] section 8.6.2.

Definition A.2.1 Let M, N, S be R-modules, then $f : M \times N \longrightarrow S$ is a bilinear morphism if it satisfies

$$\begin{aligned} f(m+m',n) &= f(m,n) + f(m',n) \\ f(m,n+n') &= f(m,n) + f(m,n') \\ f(rm,n) &= rf(m,n) = f(m,rn) \end{aligned}$$

in other words that the maps $f(m,\cdot)$ and $f(\cdot,n)$ are R-morphisms.

Definition A.2.2 Let A, B be an R-modules, then their tensor porduct is an R-module E with a bilinear form $h : A \times B \longrightarrow E$ such that for every R-module G and bilinear morphism $f : A \times B \longrightarrow G$ there exist a unique morphism $\tilde{f} : E \longrightarrow G$ making the following diagram commute:

$$\begin{tikzcd} A \times B \arrow[rr, "f"] \arrow[dr, "h"'] & & G \\ & E \arrow[ur, "\tilde{f}"'] & \end{tikzcd}$$

Observation A.2.3 If a tensor product exists then is unique up to isomorphism, because it is defined with a universal property. We denote the tensor product of A and B by $A \otimes_R B$.

Proposition A.2.4 *If* A *and* B *are* R*-modules, then their tensor product exists.*

The next proposition is an example of an application of the tensor product. In general this construction is called scalar extension.

Definition A.2.5 Let R be a domain and $Q = \mathrm{Frac}(R)$. If M is an R-module, define

$$\mathrm{rank}(M) = \dim_Q \big(Q \otimes_R M\big)$$

Proposition A.2.6 *Let* R *be a domain with* $Q = \mathrm{Frac}(R)$ *and let* M *be an* R*-module.*

i) *If* $0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$ *is a short exact sequence of* R*-modules then*

$$\operatorname{rank}(M) = \operatorname{rank}(M') + \operatorname{rank}(M'')$$

ii) *An* R*-module is torsion if and only if* $\operatorname{rank}(M) = 0$.

iii) *Let* M *be torsion-free, then* M *has rank* 1 *if and only if it is isomorphic to a nonzero* R*-submodule of* Q.

Definition A.2.7 Let $A_1, \ldots, A_n, B$ be R-modules, then $f : A_1 \times \cdots \times A_n \longrightarrow B$ is a multilinear morphism if it is an R-morphism for each variable when we fix the other ones.

Observation A.2.8 With this definition we can generalize the universal property of tensor product for more than two modules. Then this construction is the same as if we iterate the tensor product of two modules and it is associative. This last fact is not trivial and it should be proved, here we do not have too much space and is not the goal of this work.

Notation: If we have an R-module M, we denote $M \overbrace{\otimes \cdots \otimes}^{n} M$ by $\bigotimes^n M$ and similary with the product $M \overbrace{\times \cdots \times}^{n} M$ by $\times^n M$.

Definition A.2.9 Let M, N be R-modules, then an R-multilinear morphism $f : \times^n M \longrightarrow N$ is alternating if

$$f(m_1, \ldots, m_n) = 0$$

whenever $m_i = m_j$ for some $i \neq j$.

Now we can do the same construction as we did with the tensor product.

Definition A.2.10 Let M be an R-module, then his nth exterior power is an R-module E with an alternating multilinear morphism $h : \times^n M \longrightarrow E$ such that for every alternating multilinear morphism $f : \times^n M \longrightarrow G$ there exists a unique morphism $\tilde{f} : E \longrightarrow G$ making the following diagram commute:

$$\begin{tikzcd}
\times^n M \arrow[rr, "f"] \arrow[dr, "h"'] & & G \\
& E \arrow[ur, "\tilde{f}"'] &
\end{tikzcd}$$

Observation A.2.11 If an nth exterior power exists then is unique up to isomorphism, because it is defined with a universal property (like in tensor product). We denote the nth exterior power of M by $\bigwedge^n M$.

Proposition A.2.12 *If* M *is an* R*-module then the* n*th exterior power exists.*

Proposition A.2.13 *Let* M *be an* R*-module.*

i) *If* $m, m' \in M$ *then* $m \wedge m' = -m' \wedge m$ *in* $\bigwedge^2 M$.

ii) *If* $p \geq 2$ *and* $m_i = m_j$ *for some* $i \neq j$ *then* $m_1 \wedge \cdots \wedge m_p = 0$ *in* $\bigwedge^n M$.

Corollary A.2.14 *If* M *can be generated by* n *elements then* $\bigwedge^p M = \{0\}$ *for all* $p > n$.

Proposition A.2.15 *Let M be an R-module and A an R-algebra, then for all $n \geq 0$*

$$A \otimes_R \bigwedge^n M \cong \bigwedge^n (A \otimes_R M)$$

We can construct a graded algebra from the exterior powers.

Proposition A.2.16 *Let M be an R-module, then the follow R-module*

$$\bigwedge M = \bigoplus_{n \geq 0} \bigwedge^n M$$

is a graded R-algebra with the action of $r \in R$ on $\bigwedge^n M$ by

$$r(x_1 \wedge \cdots \wedge x_p) = (rx_1) \wedge x_2 \wedge \cdots \wedge x_n$$

and the multiplication $\bigwedge^p M \times \bigwedge^q M \longrightarrow \bigwedge^{p+q} M$ for $p, q \geq 1$ given by

$$\big(x_1 \wedge \cdots \wedge x_p,\, y_1 \wedge \cdots \wedge y_q\big) \longmapsto x_1 \wedge \cdots \wedge x_p \wedge y_1 \wedge \cdots \wedge y_q.$$

Theorem A.2.17 *For all $p \geq 0$ and all R-modules M and N then*

$$\bigwedge^n (M \oplus N) \cong \bigoplus_{i=0}^{n} \Big(\bigwedge^i M \otimes_R \bigwedge^{n-i} N \Big)$$

A.3 Noetherian and Artinian Rings and Modules

Definition A.3.1 An R-module M is Noetherian if every ascending chain of submodules of M is finite, by ascending chain of M we mean the following increasing sequence of submodules:

$$N_1 \subsetneq N_2 \subsetneq N_3 \subsetneq \cdots$$

Proposition A.3.2 *Let M be an R-module, then the following conditions are equivalent*

i) *M is Noetherian.*

ii) *Every submodule of M is finitely generated.*

iii) *Every nonempty set of submodules of M has a maximal element with respect to set inclusion.*

Corollary A.3.3 *A ring R is noetherian if and only if all its ideals are finitely generated*

Proof: We just have to apply the previous proposition to the R-module R that is finitely generated (generated by 1). □

Definition A.3.4 An R-module M is Artinian if every descending chain of submodules of M is finite, by descending chain of M we mean the following decreasing sequence of submodules:

$$N_1 \supsetneq N_2 \supsetneq N_3 \supsetneq \cdots$$

Proposition A.3.5 *Let M be an R-module, then the following conditions are equivalent*

i) *M is Artinian.*

ii) *Every nonempty set of submodules of M has a minimal element with respect to set inclusion.*

Proposition A.3.6 *Let M_1, M_2, M be R-modules such that*

$$0 \longrightarrow M_1 \longrightarrow M \longrightarrow M_2 \longrightarrow 0$$

is an exact sequence. Then M is Noetherian (resp. Artinian) if and only if M_1 and M_2 are Noetherian (resp. Artinian).

Corollary A.3.7 *Let $M_1, \dots, M_n$ be R-modules. Then $M_1 \oplus \cdots \oplus M_n$ is Noetherian (resp. Artinian) if and only if each M_i is Noetherian (resp. Artinian).*

Proof: We have to do induction over the number of summands and apply the previous proposition since the following is an exact sequence:

$$0 \longrightarrow M_1 \oplus \cdots \oplus M_{n-1} \longrightarrow M_1 \oplus \cdots \oplus M_n \longrightarrow M_n \longrightarrow 0$$

□

Proposition A.3.8 *The following statements are equivalent:*

i) *R is a Noetherian (resp. Artinian) ring.*

ii) *All finitely generated R-module are Noetherian (resp. Artinian).*

Proposition A.3.9 *Let R be an Artinian ring, then it is also Noetherian. Moreover it has finite length.*

Proposition A.3.10 *Let R be an Artinian ring and M an R-module. Then the following statements are equivalent:*

i) *M is Noetherian.*

ii) *M is Artinian.*

Proposition A.3.11 *Let R be an Artinian ring. Then every prime ideal of R is maximal. Also R has only finitely many prime ideals.*

Definition A.3.12 Let R be a ring, its Jacobson radical denoted by $J(R)$ is the intersection of all the maximal ideals of R.

Proposition A.3.13 *Let R be a ring. Then its Jacobson radical $J(R)$ is the set of elements $r \in R$ such that $rS = 0$ for every simple module S.*

Proposition A.3.14 *Let R an Artinian ring. Then the Jacobson radical of R is a nilpotent ideal, that is, there exists $n \geq 1$ such that $J(R)^n = \{0\}$.*

Theorem A.3.15 *Let R be an Artinian ring. Then $R = R_1 \oplus \cdots \oplus R_n$ where R_i are local Artinian rings.*

A.4 Projective and Injective Modules

Definition A.4.1 An R-module F is projective if, where $p : A \longrightarrow A'$ is surjective and $h : F \longrightarrow A'$ is any morphism, there exists a lifting $g : F \longrightarrow A$, that is, there exists a map g making the following diagram commute:

$$\begin{tikzcd}
 & F \arrow[dl, "g"'] \arrow[d, "h"] & \\
A \arrow[r, "p"'] & A' \arrow[r] & 0
\end{tikzcd}$$

equivalently $h = p \circ g$.

Proposition A.4.2 *An R-module F is projective if and only if for every exact sequence*

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

then the following sequence is exact

$$0 \longrightarrow \mathrm{Hom}_R(F, M_3) \longrightarrow \mathrm{Hom}_R(F, M_2) \longrightarrow \mathrm{Hom}_R(F, M_1) \longrightarrow 0$$

Proposition A.4.3 *Let P be an R-module. Then P is projective if and only if every short exact sequence $0 \longrightarrow A \longrightarrow B \longrightarrow P \longrightarrow 0$ is split.*

Corollary A.4.4 *Let A be a submodule of a module B. If B/A is projective then A has a complement: there is a submodule C of B with $C = B/A$ and $B = A \oplus C$.*

Theorem A.4.5 *Let F be a free R-module, then F is projective.*

Theorem A.4.6 *An R-module P is projective if and only if it is a direct summand of a free R-module.*

Theorem A.4.7 (Dual basis lemma) *Let R be a ring, M an R-module and $\{u_i\}$ a generating system for M. Then M is projective if and only if there exist $\alpha_i \in \mathrm{Hom}_R(M, R)$ such that for any $m \in M$ there are only a finite number of i such that $\alpha_i(m)$ is nonzero and*

$$m = \sum_i \alpha_i(m) \cdot u_i$$

Definition A.4.8 An R-module E is injective if, where $i : A \longrightarrow B$ is injective and $h : A \longrightarrow E$ is any morphism then there exists a morphism $g : B \longrightarrow E$ making the following diagram commute

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r, "i"] \arrow[d, "h"'] & B \arrow[dl, "g"] \\
 & E &
\end{tikzcd}$$

equivalently $g \circ i = h$.

Proposition A.4.9 *Let E be an R-module. Then the following conditions are equivalent:*

i) *E is an injective module.*

ii) *For every ideal $I \subseteq R$ and R-morphism $h : I \longrightarrow E$ there exist an R-morphsim $g : R \longrightarrow E$ making the following diagram commutative:*

$$\begin{tikzcd}
0 \arrow[r] & I \arrow[r, "inc"] \arrow[d, "h"'] & R \arrow[dl, "g"] \\
& E &
\end{tikzcd}$$

iii) *For every exact sequence*

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

then the following sequence is exact

$$0 \longrightarrow \mathrm{Hom}_R(M_1, E) \longrightarrow \mathrm{Hom}_R(M_2, E) \longrightarrow \mathrm{Hom}_R(M_3, E) \longrightarrow 0$$

Proposition A.4.10 *Let E be an R-module. Then E is injective if and only if every short exact sequence $0 \longrightarrow E \longrightarrow A \longrightarrow B \longrightarrow 0$ is split.*

Proposition A.4.11 *Let $\{E_i\}_{i\in I}$ be a family of R-modules. Then $\prod_{i\in I} E_i$ is injective if and only if each E_i is injective.*

Corollary A.4.12 *Let $\{E_i\}_{i\in I}$ be a finite family of R-modules. Then $\bigoplus_{i\in I} E_i$ is injective if and only if each E_i is injective.*

Proof: We have to note that $\prod_{i\in I} E_i \cong \bigoplus_{i\in I} E_i$ when I is a finite set. Hence it is just the previous proposition. □

Definition A.4.13 Let M be an R-module. An element m of M is said to be divisible if, for every $r \in R$ which is not a zero divisor, there exists $m' \in M$ such that $m = rm'$.
If every element of M is divisible, then M is said to be a divisible module. Alternatively M is divisible if $M = rM$ for every $r \in R$ that is not a zero divisor.

Proposition A.4.14 *Every injective module is divisble.*

Definition A.4.15 Let M be an R module. An element $m \in M$ is said to be a torsion element if there exists a nonzero $r \in R$ such that $rm = 0$. If the only torsion element of M is the zero element, then E is said to be a torsion free module.

This definition is developed at the section 2.1 where we define the torsion module and its properties. The next proposition gives a sufficient condition to a divisible module to be injective.

Proposition A.4.16 *Let R be an integral domain and let M be a torsion free divisible R-module. Then M is injective.*

Example A.4.17 It follows from the previous proposition that the field of fractions of a domain is an injective module over that domain. This will be relevant at the last chapter when we will deal with injective essential extensions (the injective envelope).