The Minimal Number of Generators for Ideals in Commutative Rings

Erika Pirnes

Matematiikan pro gradu

Jyväskylän yliopisto
Matematiikan ja tilastotieteen laitos
Kevät 2018

Tiivistelmä

Pirnes, Erika: *The Minimal Number of Generators for Ideals in Commutative Rings (Kommutatiivisten renkaiden ideaalien minimaalinen virittäjämäärä)*, Matematiikan Pro Gradu -tutkielma, Jyväskylän yliopisto, Matematiikan ja tilastotieteen laitos, Toukokuu 2018. 58 sivua, 1 liite (1 sivu).

Olkoon R kommutatiivinen rengas. Tämän tutkielman tarkoituksena on etsiä ylä- ja alarajat äärellisviritteisen ideaalin $I = (a_1, \ldots, a_n) \subset R$ minimaaliselle virittäjämäärälle. Tärkeänä työkaluna toimii moduliteoria; modulit yleistävät sekä ideaalit että vektoriavaruudet.

Jos joukko $\{a_1, \ldots, a_n\}$ on vektoriavaruuden V virittäjäjoukko, jossa mikään alkioista a_i ei kuulu toisten virittäjien lineaariseen verhoon, on kyseinen joukko lineaarisesti riippumaton virittäjäjoukko eli kanta. Tällöin kaikissa vektoriavaruuden V virittäjäjoukoissa on vähintään n alkiota, ja kaikissa kannoissa niitä on tasan n kappaletta. Tarpeettomien virittäjien poistaminen ei ideaalin ollessa kyseessä kuitenkaan riitä. Vaikka mitään ideaalin virittäjistä a_i ei voitaisi poistaa, pienempi virittäjäjoukko saattaa silti olla olemassa.

Erityinen kokoelma renkaita, joissa ideaalin minimaalisen virittäjämäärän selvittäminen on verrattain helppoa, on lokaalit renkaat. Hieman yleisemmin: kun R on lokaali rengas, niin äärellisviritteisen R-modulin minimaalinen virittäjämäärä on sama kuin tietyn renkaaseen ja moduliin liittyvän vektoriavaruuden dimensio. Todistus pohjautuu moduliteorian tulokseen, joka tunnetaan nimellä Nakayaman lemma. Lokaalien renkaiden tapauksessa kysymys voidaan siten palauttaa vektoriavaruuden dimension selvittämiseen.

Renkaan lokalisaatio syntyy samantapaisella (vaikkakin hieman yleisemmällä) konstruktiolla kuin rationaaliluvut. Sen avulla voidaan löytää alaraja ideaalin minimaaliselle virittäjämäärälle renkaassa, joka ei ole lokaali. Jokaisella ideaalilla on lokalisaatiossa sitä vastaava ideaali, jota kutsutaan sen laajennukseksi, ja laajennuksen minimaalinen virittäjämäärä on pienempi tai yhtä suuri kuin alkuperäisen ideaalin minimaalinen virittäjämäärä. Alkuideaalin suhteen tehty lokalisaatio on lokaali rengas, joten yllä esitetty tulos antaa halutun alarajan. Jos tämän suuruinen virittäjäjoukko on löydetty, voidaan näin todistaa että se on minimaalinen siinä mielessä, että pienempiä virittäjäjoukkoja ei ole olemassa.

Mikäli R on Noetherin rengas, voidaan sen ideaalien minimaaliselle virittäjämäärälle löytää myös yläraja. Tässä tekstissä esitellään Otto Forsterin tulos. Jokaiselle äärellisviritteiselle R-modulille E määritellään luku $b(E)$ siten, että E voidaan virittää joukolla alkioita, joita on $b(E)$ kappaletta. Myös tämä tulos hyödyntää lokalisaatiota, ja sen lisäksi Krullin dimensiokäsitettä ja Zariski-topologiaa.

Käsitteiden selventämiseksi käytetyistä esimerkeistä suurin osa käsittelee polynomirenkaita.

Asiasanat: kommutatiivinen rengas, ideaali, lokalisaatio, virittäjä, moduli, polynomi

Abstract

Pirnes, Erika: *The Minimal Number of Generators for Ideals in Commutative Rings*, Master's Thesis in Mathematics, University of Jyväskylä, Department of Mathematics and Statistics, May 2018. 58 pages, 1 appendix (1 page).

Let R be a commutative ring. The goal of this work is to find upper and lower bounds for the minimal number of generators for a given finitely generated ideal $I = (a_1, \ldots, a_n) \subset R$. The way towards the solution passes through some module theory; modules generalize both ideals and vector spaces.

If $\{a_1, \ldots, a_n\}$ is a generating set for a vector space V, and none of the generators a_i belongs to the linear span of the others, the set in question is a linearly independent generating set and thus a basis. Then all generating sets of V have at least n elements, with bases having exactly n. However, in the case of an ideal, it is not enough to remove unnecessary generators. Even if none of the elements a_i can be removed, a smaller generating set might still exist.

Local rings are a special type of rings where it is easier to determine the minimal number of generators for an ideal. More generally, the minimal number of generators for a finitely generated module over a local ring is the same as the dimension of a specific vector space related to the ring and the module. The proof is based on a module theory result, which is known as Nakayama's lemma. In the case of local rings, the problem thus simplifies to finding the dimension of a vector space.

Localization of a ring is constructed in a similar way to rational numbers, although the process is more general. Using localization, it is possible to obtain a lower bound for the minimal number of generators for an ideal in a ring that is not local itself. For any ideal, there is a corresponding ideal, called extension, in the localization, and the minimal number of generators for the extension is smaller than or equal to the minimal number of generators for the original ideal. If the localization is done at a prime ideal, it is a local ring; therefore the result described above gives the lower bound. In the case when a generating set of this cardinality has been found, this approach can be used to prove that the generating set in question is "minimal" in the sense that there cannot exist any smaller generating sets.

For Noetherian rings, also an upper bound for the number of generators can be obtained. This text presents a result by Otto Forster. For any finitely generated module E over a Noetherian ring, it assigns a number $b(E)$ so that E can be generated by $b(E)$ elements. Also this result makes use of localization, in addition to Krull dimension concept and Zariski topology.

Polynomial rings are used as an example throughout the text to illustrate the concepts.

Keywords: commutative ring, ideal, localization, generator, module, polynomial

Contents

Preface

The idea for this master's thesis dates back to roughly a year ago, when I spent two months in Ann Arbor, Michigan. I participated in a program called Research Experience for Undergraduates (REU) at the University of Michigan, with Karen Smith as my mentor. The main goal of my stay was to learn about algebraic geometry, but I also took several small algebraic (and not so geometric) side steps. I had been working with ideals in $\mathbb{C}[x, y]$, and one day I asked Karen (without having thought much about it, I have to admit), whether every ideal in that ring can be generated by two elements. This would have seemed reasonable, as two is also the number of variables, but of course it was not true.

As a part of her answer, Karen presented a theorem (Corollary 3.7 in this text) that characterizes the minimal number of generators for an ideal in a local ring, but there were many things in her explanation that I did not understand. For example, the theorem was about *local* rings, which means rings that have a unique maximal ideal, and it was not clear why or how the result could be applied to the non-local polynomial ring $\mathbb{C}[x, y]$. The following autumn, after considering other options, I decided to write my master's thesis on this subject, as I wanted to understand the theory behind these ideas.

The topic gradually evolved to include other types of rings besides polynomial rings, as the results can be applied to a more general situation. And when I started looking for proofs, it soon became obvious that they required module theory: even to such extent that most of the results of this work are for modules, which are a more general concept than ideals. Despite this, I have decided to hold on to ideals and the "original" title (which actually changed twice during the process). The main reason behind my decision is that the most natural examples seem to come from polynomial rings.

Finally, I want to thank two people without whom this text would be completely different. One of them is of course Karen, who gave me the idea for this work. Last but not least, I want to thank my advisor Jouni Parkkonen, who has used a tremendous amount of time and effort in reading the unfinished text over and over again. His valuable support and sharp observations have allowed me to reach much higher than I could ever have been able to on my own.

Erika Pirnes

Jyväskylä, May 24th, 2018

Introduction

Let R be a commutative ring, and let $I = (a_1, \ldots, a_k) \subset R$ be an ideal. The ideal I has a generating set of k elements, but some set of fewer elements might also generate it. The set of those numbers so that I has a generating set of that many elements is a nonempty subset of the natural numbers, so it has a minimal element. Therefore there exists a number μ so that I can be generated by μ elements, but no set of less than μ elements generates I. Now the problem is how this number can be found: it is obviously not sensible to try to go through all the possible generating sets, unless the ring R happens to be finite.

In some cases it is easy to see that some of the given elements are not necessary in defining the ideal. For example, the elements a_1 and a_2 generate the ideal $(a_1, a_2, a_1a_2) \subset R$, and depending on these elements, the ideal might be generated by just one of them. However, generally it is not obvious whether some of the generators of an ideal $(a_1, \ldots, a_k) \subset R$ can be removed.

For a vector space X, if there is a set of vectors S which spans X and the span of any subset of S is a proper subspace of X, then S is a basis. Furthermore, all bases have the same cardinality. So in the case of a vector space, a basis can be found by removing unnecessary elements. Both ideals and vector spaces are examples of a more general concept, modules, but the situation with ideals is not as fortunate as with vector spaces. As an example, consider $I = (2) = (4, 6) \subset \mathbb{Z}$. As 2 belongs to neither (4) nor (6), one might think that both of the two elements are required for generators, which is not the case.

The example given above is a bit trivial, as $\mathbb{Z}$ is a principal ideal domain (i.e. all its ideals can be generated by a single element), but a similar example for a ring which is not a principal ideal domain would be $(x) = (x^2+x, x^2) \subset \mathbb{Z}[x]$, discussed in Example 2.1. So it is not sufficient to look at the given generators and decide whether all of them are necessary, which makes the problem more complex.

The goal of this work is to present some existing results regarding upper and lower bounds for the minimal number of generators, and thus also the structure of this work breaks naturally into two parts. The first part consists of Chapters 1 to 5; it treats the special case of local rings and establishes a lower bound for non-local rings. The purpose of the second part, Chapters 6 and 7, is to find an upper bound for Noetherian rings.

It is assumed that the reader is somewhat familiar with rings, ring homomorphisms and quotient rings, as well as groups and quotient groups, polynomial rings in one variable, and vector spaces. However, few results are assumed to be known, and the majority of elementary resulsts in this work include a detailed proof. A reader

wanting to refresh their memory or learn about the basic concepts may benefit from reading the comprehensive textbook *Abstract Algebra* by David Dummit and Richard Foote [**Dummit**].[1]

Chapter 1 is a preparation for the theory needed in the other chapters. It introduces ideals, ideals generated by subsets, Noetherian rings, products of ideals, maximal and prime ideals and some of their properties. It also discusses the basic concepts of module theory and gives examples of maximal and prime ideals in polynomial rings.

Chapter 2 presents the problem of finding the minimal number of generators for an ideal, and compares it with finding the dimension for an vector space. It also gives examples, one of which shows that the minimal number of generators for the ideal $(x, 2) \subset \mathbb{Z}[x]$ is two. This example can be done by elementary methods, but more general examples need more tools.

In Chapter 3, the minimal number of generators is established for ideals in local rings, which are rings that have a unique maximal ideal. In the case of local rings, the minimal number of generators for an ideal is the same as the dimension of a specific vector space related to the ring and the ideal. However, not every ring is local: for an example, the familiar rings $\mathbb{Z}$ and $\mathbb{Z}[x]$ are not, together with other polynomial rings. Therefore, the result only applies to a narrow collection of rings.

Chapter 4 introduces a process of localizing a ring: from a given ring it produces another, which is called the localization of the ring. This process is a generalization of the construction of rational numbers. In the case of rational numbers, all nonzero integers become invertible, but the more general process makes a possibly smaller subset of the ring invertible. When this subset is the complement of a prime ideal, the resulting ring is a local ring.

In Chapter 5, localization is used to obtain a lower bound for the minimal number of generators for ideals in non-local rings. For any ideal, there is a corresponding ideal, called extension, in the localization, and the minimal number of generators for the extension is smaller than or equal to the minimal number of generators for the original ideal. Localizing at a prime ideal and using the results of Chapter 3 gives thus a lower bound.

The purpose of Chapter 6 is to build up the background needed for the last chapter. Its topics include radical ideals, Krull dimension concept, tensor products and localization of modules.

Chapter 7 presents a result by Otto Forster. This result gives an upper bound for the minimal number of generators for an ideal in a Noetherian ring: it assigns a number $b(E)$ for any finitely generated module E so that E can be generated by $b(E)$ elements. The chapter ends with an example which shows that the result does not hold for a module that is not finitely generated. In this case the number $b(E)$ might be finite, even though no finite set generates the module.

Throughout this whole text, the capital letter R is used to denote a commutative ring with a multiplicative identity $1_R \neq 0_R$. When the ring R is clear from context,

[1]Referring to this book by the name of only one of the authors is not done in order to ignore the other author, but it is an attempt to create labels that are easy to remember and not too long.

the subscripts are dropped and less cumbersome notation $1 = 1_R$ and $0 = 0_R$ is used. When R and S are rings and $\varphi\colon R \to S$ a ring homomorphism, it is required that $\varphi(1_R) = 1_S$. For (additive) quotient groups, quotient rings and quotient modules, the notation $x + D$ is used to denote the class of the element x, when D is the subgroup, ideal or submodule with respect to which the quotient is taken.

The symbol $\mathbb{Z}_+$ is used to denote the positive integers $\{1, 2, 3, \dots\}$, and the symbol $\mathbb{N}$ for the natural numbers $\{0, 1, 2, \dots\}$. For inclusion of sets, the notations $A \subset B$ and $A \subsetneq B$ are used, where the first allows the sets to be equal, and the second does not. The difference of two sets is denoted by $A - B$. A list of used notation is in Appendix A.

CHAPTER 1

Preparation: Ideals and Beyond

The goal of this chapter is to provide sufficient background for the subsequent chapters. It concentrates on generators of ideals, Noetherian rings, maximal ideals, polynomials and modules.

1.1. Generators

The beginning of this section up to Corollary 1.9 deals with ideals generated by subsets of a ring, and it uses [**Dummit**, section 7.4]. Proposition 1.13, which characterizes a Noetherian ring, is a modified version of the well-known result presented in [**Dummit**, section 15.1]. The section ends with Lemma 1.16 taken from [**Dummit**, exercise 12, section 7.4], which helps to find generators for the product of two ideals.

DEFINITION 1.1. A nonempty subset I of a commutative ring R is an *ideal*, if it is a subgroup of the abelian additive group $(R, +)$, and closed under multiplication by elements of R.

The following two conditions can be used to check whether a subset is an ideal:

(i) for every $a, b \in I$ also $a - b \in I$ (the subgroup criterion)
(ii) for every $a \in I$ and $r \in R$, $ra \in I$.

The second condition implies that if an ideal $I \subset R$ contains a unit (an invertible element) or the multiplicative identity, then $I = R$.

REMARK 1.2. The intersection of arbitrarily many ideals can be easily shown to be an ideal. In general, unions of ideals may not be ideals, which the next example shows.

EXAMPLE 1.3. Let $R = \mathbb{Z}$. The union of the ideals $(2), (3) \subset \mathbb{Z}$ is not an ideal: The union consists of integers which are divisible by either 2 or 3. Therefore $5 = 2 + 3$ is not an element of the union, so the union is not an additive subgroup, and thus not an ideal.

DEFINITION 1.4. Let $S \subset R$ be a subset. The *ideal generated by* S is the ideal

$$(S) = \bigcap \{I \subset R \colon I \text{ is an ideal}, I \supset S\}.$$

The set S is called the *generating set* of (S). An ideal $I \subset R$ is said to be *finitely generated* if it has a finite generating set, i.e. $I = (S)$ for some finite set S.

REMARK 1.5. Every ideal has a generating set, as an ideal always generates itself. The ideal generated by a set S is the smallest ideal that contains S, as it is the intersection of all such ideals.

LEMMA 1.6. *Let $S \subset R$ be a subset. Let S^* be the set of all finite R-linear combinations of elements of S:*

$$S^* = \left\{ \sum_{i=1}^{k} r_i s_i \colon s_i \in S, r_i \in R, k \in \mathbb{Z}_+ \right\}.$$

Then S^* is an ideal of R which contains S. Moreover, if $I \subset R$ is an ideal, then $S^* \subset I$ if and only if $S \subset I$.

PROOF.
It is straightforward to verify that S^* is an ideal, as all the elements of S^* consist of sums. As any $s \in S$ can be expressed as $s = 1_R \cdot s \in S^*$, it follows that $S \subset S^*$. This proves the first claim.

Let $I \subset R$ be an ideal, and assume first that $S^* \subset I$. Then $S \subset S^* \subset I$. Assume then that $S \subset I$. Let $t \in S^*$, so there exists $k \in \mathbb{Z}_+$ so that $t = \sum_{i=1}^{k} r_i s_i$ for some $r_i \in R$ and $s_i \in S$. As I is an ideal and each $s_i \in S \subset I$, also each $r_i s_i \in I$, and as I is a subgroup of $(R, +)$, also $t \in I$. Therefore $S^* \subset I$. □

PROPOSITION 1.7. *Let $S \subset R$ be a subset, and S^* as in the previous lemma. Then $(S) = S^*$.*

PROOF.
By the previous lemma, for $S^* \subset (S)$ it is enough to show $S \subset (S)$, but this is obvious. Again by the lemma, S^* is an ideal which contains S, so as (S) is the intersection of all ideals of this kind, the inclusion $(S) \subset S^*$ follows. □

The preceding proposition thus gives a convenient form for the ideal generated by a subset: all its elements can be expressed as finite sums. In the case of a finite set $S = \{a_1, \ldots, a_n\}$, it may be assumed that this sum has n terms for each element of (S); this might be convenient in some proofs. (Gather terms with same s_i to get $k \leq n$, and if this results in $k < n$, take $r_i = 0$ for the remaining indices.)

COROLLARY 1.8. *Let $S \subset R$ be a subset and $I \subset R$ an ideal. Then $S \subset I$ if and only if $(S) \subset I$.*

The preceding corollary transforms the problem of deciding whether two ideals are the same, into determining if the generators of each ideal belong to the other ideal. More precisely:

COROLLARY 1.9. *Let $I, J \subset R$ be ideals with generating sets $S_I, S_J \subset R$, respectively. Then $I = J$ if and only if $S_I \subset J$ and $S_J \subset I$.*

DEFINITION 1.10. A ring R is *Noetherian* if each of its ideals is finitely generated.

DEFINITION 1.11. An integral domain R is a *principal ideal domain*, if its every ideal can be generated by one element.

EXAMPLE 1.12. All fields are Noetherian rings, as any field F has only two ideals: the zero ideal generated by 0_F and the field itself, generated by 1_F. All principal ideal domains are also Noetherian rings. Some examples of principal ideal domains are $\mathbb{Z}$ and $R[x]$ when R is a field, and they are thus also Noetherian rings.

Hilbert's basis theorem (which is proved in section 1.3) states that polynomial rings over Noetherian rings are also Noetherian, but these are not always principal ideal domains. Examples 2.3 and 5.3 present ideals of $\mathbb{Z}[x]$ and $\mathbb{Z}[x, y]$[1] where the minimal numbers of generators are 2 and 3. When the number of variables is more than 1, not even R being a field improves the situation: Remark 5.5 gives for each $n \in \mathbb{Z}_+$ an ideal in $R[x, y]$ which cannot be generated by less than $n + 1$ elements.

For many proofs, it is convenient to use a property called the ascending chain condition on ideals, which states that there are no infinite strictly increasing chains of ideals. This is equivalent to the ring being Noetherian:

PROPOSITION 1.13. *A ring R is Noetherian if and only if it satisfies the ascending chain condition: whenever $I_1 \subset I_2 \subset \ldots$ is an increasing chain of ideals of R, then there exists $m \in \mathbb{N}$ such that $I_k = I_m$ for all $k \geq m$.*

PROOF.
Assume first that R satisfies the ascending chain condition. Assume on the contrary, that R is not Noetherian. Therefore there exists an ideal $I \subset R$ which cannot be generated by finitely many elements. Let $a_1 \in I$. Then a_1 does not generate I, so there is $a_2 \in I$ such that $(a_1) \subsetneq (a_1, a_2)$. The set $\{a_1, a_2\}$ does not generate I, so there is $a_3 \in I$ so that $(a_1, a_2) \subsetneq (a_1, a_2, a_3)$. By continuing like this, an infinite strictly increasing chain of ideals can be constructed. This contradicts the ascending chain condition. Therefore R is Noetherian.

Assume then that R is Noetherian. Let $I_1 \subset I_2 \subset \ldots$ be an increasing chain of ideals. Their union $U = \cup_{k \in \mathbb{Z}_+} I_i$ is an ideal as the ideals I_k are nested. As R is Noetherian, U has a finite set of generators $\{a_1, \ldots, a_n\}$. Each $a_i \in I_{k_i}$ for some k_i. Let $m = \max\{k_1, \ldots, k_n\}$. As the ideals I_k are nested, $I_{k_i} \subset I_m$ for all k_i. Therefore $\{a_1, \ldots, a_n\} \subset I_m$, which implies that $U \subset I_m$ by Corollary 1.8. As also $I_m \subset U$, the equality $I_m = U$ holds. Let $k \geq m$, so $I_m \subset I_k$. Also

$$I_k \subset U = I_m,$$

so $I_k = I_m$, and the ascending chain condition is satisfied. □

DEFINITION 1.14. The *product* IJ of two ideals $I, J \subset R$ is the set of all finite sums of terms of the form ij, where $i \in I$ and $j \in J$.

It is straightforward to verify that the product of two ideals is an ideal. However, in the definition of the product, it is necessary to take the sums of the elements ij, because the set of these elements might not be an ideal:

EXAMPLE 1.15. Consider the ideal $I = (x, 2) \subset \mathbb{Z}[x]$, which is a proper ideal consisting of all polynomials with an even constant term. The polynomials x^2 and 4 are both of the form fg, where $f, g \in (x, 2)$. Their sum $x^2 + 4$ is an irreducible polynomial in $\mathbb{Z}[x]$, so if $x^2 + 4 = fg$ for some $f, g \in (x, 2)$, either f or g has to be a constant polynomial. But only 1 and -1 are possible, and these are not elements of $(x, 2)$. Therefore the set of elements fg, where $f, g \in (x, 2)$, is not an ideal, as it is not closed under addition.

[1] see Definition 1.29 for polynomials in several variables

This kind of an example cannot be constructed with two ideals when one or both of them are generated by one element, which follows from the next lemma.

LEMMA 1.16. *Let $I, J \in R$ be ideals, and assume that $I = (a_1, \ldots, a_n)$ and $J = (b_1, \ldots, b_m)$. Then IJ is generated by the elements $a_i b_j$ where $i \in \{1, \ldots, n\}$ and $j \in \{1, \ldots, m\}$.*

PROOF.
It is obvious that the ideal generated by the elements $a_i b_j$ is contained in IJ. For the other inclusion, it needs to be shown that any element of IJ can be expressed as an R-linear combination of the elements $a_i b_j$.

Assume that $c = ab$ for some $a \in I$ and $b \in J$. The elements a and b can be expressed as R-linear combinations of the generators: there exist $r_1, \ldots, r_n, s_1, \ldots, s_m \in R$ such that

$$c = (r_1 a_1 + \ldots r_n a_n)(s_1 b_1 + \ldots s_m b_m) = \sum_{\substack{1 \leq i \leq n, \\ 1 \leq j \leq m}} r_i s_j a_i b_j.$$

As any element of IJ can be expressed as a finite sum of elements of the above type, IJ is generated by the elements $a_i b_j$. □

As both I and J are ideals, $IJ \subset I \cap J$. The next example shows that both equality and a strict inclusion are possible.

EXAMPLE 1.17. Let $R = \mathbb{Z}$, $I = (2)$ and $J = (3)$. Then $IJ = (6)$ by the previous lemma. Also $I \cap J = (6)$, because the elements of the intersection have to be divisible by both 2 and 3. Therefore, in this case $IJ = I \cap J$.

However, the inclusion might be strict. If $I = (2)$ and $J = (6)$, again $I \cap J = (6)$, but the lemma gives that $IJ = (12)$. Therefore $IJ \subsetneq I \cap J$.

1.2. Maximal Ideals

In this section the goal is to prove a few known results regarding properties and existence of maximal ideals. The presentation follows [**Dummit**, sections 7.4 and 8.2].

DEFINITION 1.18. An ideal $M \subsetneq R$ is a *maximal ideal*, if for any ideal I satisfying $M \subset I \subset R$ either $I = M$ or $I = R$.

DEFINITION 1.19. An ideal $P \subsetneq R$ is a *prime ideal*, if $ab \in P$ always implies $a \in P$ or $b \in P$.

LEMMA 1.20. *Maximal ideals are prime.*

PROOF.
Let $M \subset R$ be a maximal ideal: then $M \subsetneq R$ by definition. Assume $ab \in M$. If $a \notin M$, then the ideal $(M \cup \{a\})$ generated by M and a is the whole ring R, because M is maximal. Thus $1_R = m + ra$ for some $m \in M$ and $r \in R$. It follows that

$$b = (m + ra)b = mb + rab \in M,$$

as M is an ideal and $m, ab \in M$. Therefore either $a \in M$ or $b \in M$, so M is a prime ideal. □

In principal ideal domains, the converse of the result holds for all nonzero prime ideals:

LEMMA 1.21. *If R is a principal ideal domain, all its nonzero prime ideals are maximal ideals.*

PROOF.
Assume that $(p) \subset R$ is a nonzero prime ideal, so $p \neq 0$. Let (q) be an ideal for which $(p) \subset (q)$. Then $p \in (q)$, so $p = rq$ for some $r \in R$. As (p) is prime ideal, either $r \in (p)$ or $q \in (p)$. If $q \in (p)$, then $(p) = (q)$. On the other hand, if $r \in (p)$, then $r = ps$ for some $s \in R$. In this case

$$p = rq = psq,$$

which implies that $p(1_R - sq) = 0$. As $p \neq 0$, it follows that $sq = 1_R$. Therefore the generator q is invertible, so $(q) = R$. This shows that (p) is a maximal ideal. □

PROPOSITION 1.22. *An ideal $I \subset R$ is a maximal ideal if and only if the ring quotient R/I is a field.*

PROOF.
Assume first that the ideal I is maximal. Let $r + I \in R/I$, and assume $r + I \neq 0_R + I$. Then $r \notin I$. As I is maximal, $(I \cup \{r\}) = R$, so $1_R = m + br$ for some $m \in I$ and $b \in R$. It follows that $br - 1_R \in I$, so

$$(b + I)(r + I) = br + I = 1_R + I.$$

Therefore $r + I$ is invertible and $(r + I)^{-1} = b + I$. As every nonzero element has an inverse, R/I is a field.

Assume then that the quotient R/I is a field. Let J be an ideal for which $I \subset J \subset R$. If $J \neq I$, then there exists an element $x \in J - I$, and therefore $x + I \neq 0 + I$. As R/I is a field, $x + I$ has an inverse $y + I$, and

$$xy + I = (x + I)(y + I) = 1_R + I.$$

Therefore $xy - 1_R = a \in I$, and $1_R = xy - a \in (I \cup \{x\}) \subset J$. It follows that $J = R$, so I is a maximal ideal. □

The next goal is to prove that every proper ideal is contained in some maximal ideal. The general version, Theorem 1.23, uses Zorn's lemma: Assume that S is a partially ordered set and every chain (totally ordered subset) in S has an upper bound in S. Then S contains a maximal element. Zorn's lemma is equivalent to the Axiom of Choice, and can be found in e.g. [**Ciesielski**]. However, the version for Noetherian rings, Theorem 1.24, does not need Zorn's lemma.

THEOREM 1.23. *Let $I \subset R$ be a proper ideal. Then there exists a maximal ideal $M \subset R$ that contains I.*

PROOF.
Define S to be the set of all proper ideals of R which contain I. The set S is nonempty, as $I \in S$, and partially ordered by inclusion. Let C be a chain in S and

$$J_0 = \bigcup_{J \in C} J.$$

The set $J_0 \subset R$ is an ideal: Firstly it is nonempty, because 0 belongs to each ideal in the union and thus $0 \in J_0$. Assume that $a, b \in J_0$. Then there exist ideals $A, B \in C$ so that $a \in A$ and $b \in B$. As C is a chain, either $A \subset B$ or $B \subset A$. Thus the element $a - b$ belongs to either A or B, and therefore also to J_0. Furthermore, if $r \in R$, then $ra \in A \subset J_0$, because A is an ideal. Therefore J_0 is an ideal.

The ideal J_0 is a proper ideal: if it is not, then $1 \in J_0$, so $1 \in J$ for some $J \in C$. However, this is not possible, as all the elements of S were assumed to be proper ideals. As also $I \subset J_0$ (all ideals of the union contain I), it can be concluded that $J_0 \in S$. Clearly J_0 is an upper bound for the chain C.

Now each chain in S has an upper bound in S. By Zorn's lemma, S has a maximal element. This is thus a maximal ideal which contains I. □

THEOREM 1.24. *Let R be a Noetherian ring and $I \subset R$ a proper ideal. Then there exists a maximal ideal $M \subset R$ that contains I.*

PROOF.
Assume on the contrary that such an ideal does not exist. Then I itself is not a maximal ideal, so there is an ideal I_1 with $I \subsetneq I_1 \subsetneq R$. Because I_1 is not a maximal ideal either, there exists I_2 with $I_1 \subsetneq I_2 \subsetneq R$. Continuing inductively, an infinite strictly increasing chain of ideals can be obtained, and this contradicts with R being Noetherian. □

1.3. Polynomials

In this section, the first goal is to prove Hilbert's basis theorem (Theorem 1.28), which states that the polynomial ring in one variable over a Noetherian ring is itself Noetherian. The proof is rearranged from [**Dummit**, section 9.6] and part of the proof is separated into a lemma. In the end of the section there are some examples of maximal ideals in polynomial rings in n variables.

DEFINITION 1.25. Let $f = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in R[x]$. If $a_n \neq 0$, then f has *degree* n ($\deg f = n$), *leading term* $a_n x_n$ and *leading coefficient* a_n. The degree of the zero polynomial is not defined, and its leading term and leading coefficient are both 0. The term a_0 is called the *constant term*, and the constant term of a polynomial f is denoted by f_0.

REMARK 1.26. Assume that R is an integral domain. If $f, g \in R[x]$ are nonzero polynomials, then $\deg fg = \deg f + \deg g$.

LEMMA 1.27. *Let $I \subset R[x]$ be an ideal. Define $C(I)$ to be the set of all leading coefficients of elements in I, and $C_d(I) \subset C(I)$ the set of leading coefficients of elements in I with degree d, together with 0. Then $C(I)$ and $C_d(I)$ are ideals of R.*

PROOF.
As 0 is the leading coefficient of $0 \in I$, it follows that $0 \in C(I)$ and thus $C(I) \neq \emptyset$. Let $a, b \in C(I)$. Then there exist $f, g \in I$ with leading terms ax^j, bx^k for some $j, k \in \mathbb{N}$. Let $r \in R$. Then

(i) $a - b \in C(I)$, because it is either 0 or the leading coefficient of $x^k f - x^j g \in I$
(ii) $ra \in C(I)$, because it is the leading coefficient of rf.

Therefore $C(I)$ is an ideal.

The smaller set $C_d(I)$ can be proven to be an ideal by modifying the proof above; note that it is nonempty by definition. Now $j = k = d$. The element $a - b \in C_d(I)$, because it is either 0 or if it is nonzero, it is the leading coefficient of $f - g$, which has degree k. The polynomial rf is either 0 or has degree k, so $ra \in C_d(I)$. Therefore $C_d(I)$ is an ideal as well. □

THEOREM 1.28 (Hilbert's Basis Theorem). *Assume that R is a Noetherian ring. Then the polynomial ring $R[x]$ is also Noetherian.*

PROOF.
Let I be an ideal in $R[x]$. Then $C(I) \subset R$ is an ideal by Lemma 1.27, so as R is Noetherian, $C(I) = (a_1, \ldots, a_n)$ for some $a_i \in R$, $i \in \{1, \ldots, n\}$. For each i, choose $f_i \in I$ with leading coefficient a_i. Denote the degree of f_i by d_i, and let $D = \max\{d_1, \ldots, d_n\}$.

For each $d \in \{0, 1, \ldots, D\}$, $C_d(I) \in R$ is an ideal by Lemma 1.27. For each nonzero ideal $C_d(I)$, let $b_{d,1}, b_{d,2}, \ldots, b_{d,n_d} \in R$ be a set of generators, and choose $f_{d,i} \in I$ of degree d with leading coefficient $b_{d,i}$. Let

$$I' = \left(\{f_1, \ldots, f_n\} \cup \{f_{d,i} \colon 0 \leq d \leq D, 1 \leq i \leq n_d\}\right).$$

The next step is to prove that $I = I'$. As all the generators for the new ideal I' were chosen from I, clearly $I' \subset I$. It thus remains to show that $I \subset I'$. Assume on the contrary that this does not hold; then there exists a nonzero $f \in I$ with $f \notin I'$ of minimum degree. Denote the degree of f by δ, and the leading coefficient of f by α.

Suppose first that $\delta > D$. As $\alpha \in C(I)$, there exist elements $r_1, \ldots, r_n \in R$ such that $\alpha = r_1 a_1 + \cdots + r_n a_n$. Then $g = r_1 x^{\delta - d_1} f_1 + \ldots r_n x^{\delta - d_n} f_n \in I'$ has the same degree δ and the same leading coefficient α as f. Therefore $f - g \in I$ has a degree strictly smaller than f. Now either

(i) $f - g \neq 0$, in which case $f - g \in I'$ by the minimality of f, and thus $f = (f - g) + g \in I'$, or
(ii) $f - g = 0$, so $f = g \in I'$,

which gives a contradiction in both cases, because it was assumed that $f \notin I'$.

Suppose then that $\delta \leq D$. In this case $\alpha \in C_\delta(I)$, so $\alpha = r_1 b_{\delta,1} + \cdots + r_{n_\delta} b_{\delta,n_\delta}$ for some $r_1, \ldots, r_{n_\delta} \in R$. Then $g = r_1 f_{\delta,1} + \cdots + r_{n_\delta} f_{\delta,n_\delta} \in I'$ has the same degree δ and the same leading coefficient α as f, so this gives a contradiction as above.

Beginning with an arbitrary ideal $I \in R[x]$, it was possible to find a finite generating set. It follows that any ideal of $R[x]$ is finitely generated, so $R[x]$ is Noetherian. □

DEFINITION 1.29. The *polynomial ring over R in n variables $x_1, \ldots, x_n$* is defined inductively by

$$R[x_1, \ldots, x_n] = R[x_1, \ldots, x_{n-1}][x_n].$$

Polynomials in n variables consist of finite sums of *monomials*: terms of the form $r x_1^{d_1} \ldots x_n^{d_n}$, where $r \in R$ and $d_i \in \mathbb{N}$. The *degree* of the monomial $r x_1^{d_1} \ldots x_n^{d_n}$ is $d_1 + \cdots + d_n$. The monomials of degree 0 (with $d_i = 0$ for all i) are called *constant terms*. The constant term of a polynomial f is denoted by f_0.

COROLLARY 1.30. *Let R be a Noetherian ring. Then every polynomial ring $R[x_1, \ldots, x_n]$ in finitely many variables is Noetherian.*

PROOF.
The claim follows from Hilbert's Basis Theorem (Theorem 1.28) and induction. □

The rest of this section gives examples of prime and maximal ideals in polynomial rings in n variables over different types of rings. Note that by Lemma 1.20, all maximal ideals are prime.

PROPOSITION 1.31. *If R is an integral domain, the ideal $(x_1, \ldots, x_n) \subset R[x_1, \ldots, x_n]$, which consists of all polynomials with constant term 0, is a prime ideal.*

PROOF.
The constant term of the product of two polynomials is the product of their constant terms. If it is zero, one of the polynomials has to belong to $(x_1, \ldots, x_n)$, as R is an integral domain. □

PROPOSITION 1.32. *The ideal $I = (x_1, \ldots, x_n) \subset R[x_1, \ldots, x_n]$ is maximal if and only if R is a field.*

PROOF.
Assume first that R is a field. Note that I is a proper ideal, as it does not contain the constant polynomial 1_R. Let J be an ideal for which $I \subset J \subset R[x_1, \ldots, x_n]$. If $I \neq J$, there is $f \in J - I$. Therefore $f = f_1 + f_0$, where $f_0 \in R$, $f_0 \neq 0$, and $f_1 \in I \subset J$. As J is an ideal, it follows that $f_0 = f - f_1 \in J$. Because R is a field, f_0 has an inverse and therefore $1_R = f_0 f_0^{-1} \in J$, which implies that $J = R[x_1, \ldots, x_n]$. This proves the maximality of the ideal $(x_1, \ldots, x_n)$.

Assume then that I is maximal. Let $a \in R$, $a \neq 0$. Consider the ideals

$$I \subset (x_1, \ldots, x_n, a) \subset R[x_1, \ldots, x_n].$$

Clearly $a \in (x_1, \ldots, x_n, a)$, and as a is a nonzero constant, $a \notin I$, so $I \subsetneq (x_1, \ldots, x_n, a)$. As I was assumed to be maximal, it follows that

$$(x_1, \ldots, x_n, a) = R[x_1, \ldots, x_n].$$

In particular, there exist some polynomials r and q_i, with $i \in \{1, \ldots, n\}$, so that

$$1_R = ar + \sum_{i=1}^{n} x_i q_i.$$

As the constant term of the rightmost sum is 0, it follows that the constant term $r_0 \in R$ of the polynomial r has to satisfy $ar_0 = 1_R$. Therefore a has an inverse. This holds for all nonzero elements $a \in R$, so R is a field. □

PROPOSITION 1.33. *Let R be a Noetherian ring. If $m_1, \ldots m_k$ are generators for any maximal ideal in R, the ideal*

$$I = (x_1, \ldots, x_n, m_1, \ldots, m_k) \subset R[x_1, \ldots, x_n]$$

is a maximal ideal.

PROOF.
First note that I is a proper ideal: if there exist polynomials q_i, p_j such that

$$1_R = \sum_{i=1}^{n} q_i x_i + \sum_{j=1}^{k} p_j m_j,$$

then the constant terms c_j of p_j satisfy $\sum_{j=1}^{k} c_j m_j = 1_R$, which is not possible as $M \subset R$ is a maximal ideal.

Assume that J is an ideal for which $I \subset J \subset R[x_1, \ldots, x_n]$ holds. If $J \neq I$, there exists $f \in J$ such that $f \notin I$. This polynomial can be written as $f = f_1 + f_0$, where $f_1 \in (x_1, \ldots, x_n) \subset I \subset J$ and $f_0 \in R$ is the constant term. As all the elements of $(m_1, \ldots, m_k) \subset R$ belong to I, it follows that the constant term $f_0 \notin (m_1, \ldots, m_k)$: otherwise f would be in I.

As $(m_1, \ldots, m_k) \subset R$ is maximal, it can be concluded that $(m_1, \ldots, m_k, f_0) = R$. Therefore there exist elements $r_1, \ldots, r_k, r \in R$ such that

$$1_R = r_1 m_1 + \cdots + r_k m_k + r f_0. \tag{1}$$

Because $f, f_1 \in J$, also $f_0 = f - f_1 \in J$. As additionally all $m_i \in J$, it follows from (1) that $1_R \in J$. Therefore $J = R[x_1, \ldots, x_n]$, and thus the ideal I is maximal. □

COROLLARY 1.34. *If R is a principal ideal domain and m is a generator for any maximal ideal in R, then the ideal $(x_1, \ldots, x_n, m) \subset R[x_1, \ldots, x_n]$ is maximal.*

EXAMPLE 1.35. The ideal $(x_1, \ldots, x_n, p) \in \mathbb{Z}[x_1, \ldots, x_n]$ is maximal for any prime number p.

REMARK 1.36. The variables x_i can be replaced by new "variables" $x_i - r_i$, where each $r_i \in R$. Any polynomial can be written in these variables: each x_i can be replaced by $(x_i - r_i) + r_i$ and the expression of the polynomial can then be expanded. Therefore the propositions 1.31, 1.32 and 1.33 can be generalized for ideals $(x_1 - r_1, \ldots, x_n - r_n)$ and $(x_1 - r_1, \ldots, x_n - r_n, m_1, \ldots, m_k)$.

REMARK 1.37. When the coefficient field F is algebraically closed, all maximal ideals of $F[x_1, \ldots, x_n]$ are of the type $(x_1 - r_1, \ldots, x_n - r_n)$ for some $r_i \in F$; this follows from a classical result called Hilbert's Nullstellensatz, and is proven in [**Arrondo**]. However, with a field that is not algebraically closed, there exist also other types of maximal ideals, which the next example shows. The classification of maximal ideals of e.g. $\mathbb{Z}[x_1, \ldots, x_n]$ would be an interesting problem, but it is not within the scope of this text.

EXAMPLE 1.38. This example shows that the ideal $I = (x^2 + 1) \subset \mathbb{R}[x]$ is a maximal ideal. As this ideal consists of the zero polynomial and polynomials of degree at least two, no polynomial of degree 1 can generate the ideal. Therefore I is not of the type given above.

The goal is to prove that $\mathbb{R}[x]/I \cong \mathbb{C}$. Then, as the quotient is a field, the ideal has to be maximal by Proposition 1.22. Note that all classes of elements in the quotient have representatives of degree 1. This follows from the fact that $\mathbb{R}[x]$ has division algorithm: each $f \in \mathbb{R}[x]$ can be written as $f = g(x^2 + 1) + h$, where $g, h \in \mathbb{R}[x]$ are

unique and either $h = 0$ or $\deg h < 2$. (Division algorithm can be found in [**Dummit**, section 9.2].) Therefore

$$\mathbb{R}[x]/I = \{(ax + b) + I \colon a, b \in \mathbb{R}\}.$$

So define $\varphi \colon \mathbb{R}[x]/I \cong \mathbb{C}$ by

$$\varphi\left((ax + b) + I\right) = ai + b.$$

Firstly, φ is well defined: assume that $(ax + b) + I = (cx + d) + I$. Then

$$(a - c)x + (b - d) = (ax + b) - (cx + d) \in I,$$

so $a = c$ and $b = d$ (I does not have any polynomials of degree 0 or 1). Secondly, φ is a homomorphism, as

$$\begin{aligned}\varphi(((ax + b) + I) + ((cx + d) + I)) =& \varphi(((a + c)x + (b + d)) + I)\\ =&(a + c)i + (b + d) = ai + b + ci + d\\ =&\varphi((ax + b) + I) + \varphi((cx + d) + I),\end{aligned}$$

and

$$\begin{aligned}\varphi(((ax + b) + I) \cdot ((cx + d) + I)) =& \varphi((acx^2 + (ad + bc)x + bd) + I)\\ =&\varphi((acx^2 + (ad + bc)x + bd - ac(x^2 + 1)) + I)\\ =&\varphi(((ad + bc)x + bd - ac) + I\\ =&(ad + bc)i + (bd - ac)\\ =&(ai + b)(ci + d)\\ =&\varphi((ax + b) + I) \cdot \varphi((cx + d) + I).\end{aligned}$$

Thirdly, φ is injective: Assume that

$$\varphi((ax + b) + I) = ai + b = ci + d = \varphi((cx + d) + I).$$

Then $a = c$ and $b = d$, so $(ax + b) + I = (cx + d) + I$. Finally, surjectivity of φ is trivial. This verifies the isomorphism.

1.4. Modules

This section introduces the basic concepts of module theory, which will be used in Chapter 3 to prove a characterization for the minimal number of generators for an ideal in a local ring, and in Chapters 6 and 7 to find an upper bound for the minimal number of generators for an ideal in a Noetherian ring. It follows [**Dummit**, sections 10.1 and 10.2].

Definition 1.39. A *(left) R-module* or a *(left) module over R* is an abelian group $(E, +)$ together with an action of R on E: a map $R \times E \to E$, $(r, e) \mapsto re$, which satisfies the following conditions whenever $r, s \in R$ and $e, e' \in E$:

(i) $(r + s)e = re + se$
(ii) $(rs)e = r(se)$
(iii) $r(e + e') = re + re'$
(iv) $1_R e = e$.

REMARK 1.40. If the ring R is clear from context, it is common to use the word module instead of R-module. An R-module for a field R is the same as an R-vector space, as the above requirements are exactly the same ones as for vector spaces. A ring is a module over itself, and also an ideal $I \subset R$ is an R-module (or a submodule of R; see the definition below). Thus the concept of modules generalizes both vector spaces and ideals.

EXAMPLE 1.41. When $\varphi\colon R \to S$ is a ring homomorphism, S becomes an R-module via the action $R \times S \to S$, $(r, s) \mapsto \varphi(r)s$. More generally, if E is an S-module, then the action $(r, e) \mapsto \varphi(r)e$ makes it an R-module. The properties of the ring homomorphism φ guarantee the properties of the module action.

DEFINITION 1.42. Let E be an R-module. A subgroup $F \subset E$ is a *submodule of* E, if it becomes an R-module when the action of R on E is restricted to $R \times F$.

REMARK 1.43. If $F \subset E$ is a subset of an R-module E, the four conditions required of an action in the definition of a module are automatically satisfied for any $r, s \in R$ and $f_1, f_2 \in F \subset E$. For proving that a subgroup F is a submodule, it thus suffices to show that the action indeed can be restricted to a map $R \times F \to F$: that $rf \in F$ when $r \in R$ and $f \in F$.

Whenever $F \subset E$ is a submodule, it is possible to form the quotient module E/F which inherits the R-module structure of E:

PROPOSITION 1.44. *Let E be an R-module and $F \subset E$ a submodule. The quotient group E/F is an R-module with the action*

$$r(e + F) = re + F,$$

where $r \in R$ and $e + F \in E/F$.

PROOF.
Since E is an additive abelian group and $F \subset E$ its subgroup, the quotient group E/F is defined and also an additive abelian group. The action given above is well defined, because if $e_1 + F = e_2 + F$, then $e_1 - e_2 \in F$ and, as F is a submodule, $re_1 - re_2 = r(e_1 - e_2) \in F$ whenever $r \in R$. This implies that

$$r(e_1 + F) = re_1 + F = re_2 + F = r(e_2 + F).$$

Therefore the action does not depend on the representatives. It is straightforward to check that the properties for the action hold. Therefore E/F is an R-module. □

DEFINITION 1.45. Let E and F be R-modules. A map $\varphi\colon E \to F$ is an *R-module homomorphism*, if

(i) $\varphi(e_1 + e_2) = \varphi(e_1) + \varphi(e_2)$ for all $e_1, e_2 \in E$, and
(ii) $\varphi(re) = r\varphi(e)$ for all $r \in R$, $e \in E$.

The *kernel* of an R-module homomorphism φ is the set $\ker \varphi = \{e \in E\colon \varphi(e) = 0_F\}$. A bijective R-module homomorphism is an *(R-module) isomorphism*, and if such an isomorphism exists, the modules E and F are *isomorphic*, denoted by $E \cong F$.

REMARK 1.46. From the first condition of Definition 1.45, it can be seen that any R-module homomorphism φ can also be thought as a group homomorphism. The kernel of φ as a group homomorphism is the same set as the kernel of φ as an R-module homomorphism. If R is a field, an R-module homomorphism is a linear map.

PROPOSITION 1.47. *Let E and G be R-modules, $\varphi\colon E \to G$ an R-module homomorphism and $F \subset E$ a submodule. If $F \subset \ker\varphi$, then the map $\Phi\colon E/F \to G$, $\Phi(e+F) = \varphi(e)$, is an R-module homomorphism.*

PROOF.
Firstly, Φ is well defined: If $e_1 + F = e_2 + F$, then $e_1 - e_2 \in F \subset \ker\varphi$ by the assumption. Therefore

$$\Phi(e_1+F) - \Phi(e_2+F) = \varphi(e_1) - \varphi(e_2) = \varphi(e_1 - e_2) = 0,$$

so $\Phi(e_1+F) = \Phi(e_2+F)$. Secondly, Φ is a homomorphism, because for $e, e_1, e_2 \in E$ and $r \in R$,

$$\begin{aligned}\Phi((e_1+F)+(e_2+F)) =& \Phi((e_1+e_2)+F) = \varphi(e_1+e_2) = \varphi(e_1)+\varphi(e_2)\\ =& \Phi(e_1+F)+\Phi(e_2+F),\end{aligned}$$

and

$$\Phi(r(e+F)) = \Phi(re+F) = \varphi(re) = r\varphi(e) = r\Phi(e+F).$$

Therefore Φ is an R-module homomorphism. □

The next proposition is often called the first isomorphism theorem.

PROPOSITION 1.48. *Let E and F be R-modules and $\varphi\colon E \to F$ an R-module homomorphism. Then $\ker\varphi \subset E$ and $\varphi(E) \subset F$ are submodules and*

$$E/\ker\varphi \cong \varphi(E).$$

PROOF.
The kernel and the image are both nonempty, as $\varphi(0_E) = 0_F$. Let $a, b \in \ker\varphi$ and $r \in R$. Then

$$\varphi(a-b) = \varphi(a) - \varphi(b) = 0 \text{ and } \varphi(ra) = r\varphi(a) = 0,$$

so $a - b \in \ker\varphi$ and $ra \in \ker\varphi$. Therefore $\ker\varphi$ is a submodule, and the quotient module $E/\ker\varphi$ exists.

Let $y_1, y_2 \in \varphi(E)$. Then there exist $x_1, x_2 \in E$ such that $\varphi(x_1) = y_1$ and $\varphi(x_2) = y_2$. Now

$$y_1 - y_2 = \varphi(x_1) - \varphi(x_2) = \varphi(x_1 - x_2) \in \varphi(E),$$

and $ry_1 = r\varphi(x_1) = \varphi(rx_1) \in \varphi(E)$ for any $r \in R$, so $\varphi(E)$ is a submodule.

Define $\Phi\colon E/\ker\varphi \to \varphi(E)$ by $\Phi(e+\ker\varphi) = \varphi(e)$. Note that φ remains an R-module homomorphism, when the codomain F is replaced by $\varphi(E)$. Therefore Φ is an R-module homomorphism by Proposition 1.47. The map Φ is clearly surjective. It is also injective, as $\Phi(e_1+\ker\varphi) = \Phi(e_2+\ker\varphi)$ implies $\varphi(e_1-e_2) = \varphi(e_1) - \varphi(e_2) = 0$, so $e_1 - e_2 \in \ker\varphi$, and thus $e_1 + \ker\varphi = e_2 + \ker\varphi$. Therefore Φ is a bijection, which verifies the isomorphism. □

DEFINITION 1.49. Let E be an R-module and $F_1, \dots, F_n \subset E$ submodules. The *sum of the submodules* F_i is the R-module

$$F_1 + \cdots + F_n = \{f_1 + \cdots + f_n \colon f_i \in F_i \text{ for all } i = 1, \dots, n\}.$$

The sum of the submodules $F_1, \dots, F_n$ is the smallest submodule that contains each F_i.

DEFINITION 1.50. Let E be an R-module, $e \in E$ and $A \subset E$ a subset. The *submodule generated by* e is $Re = \{re \colon r \in R\}$, and *the submodule generated by* A is

$$RA = \left\{ \sum_{i=1}^{n} r_i a_i \colon r_i \in R, a_i \in A, n \in \mathbb{Z}_+ \right\}.$$

The submodule generated by a finite set $B = \{e_1, \dots, e_n\} \subset E$ can also be written as $RB = Re_1 + \cdots + Re_n$, which coincides with the above definition. A submodule $F \subset E$ is finitely generated if $F = RB$ for some finite set $B \subset E$. By convention, the empty set generates the zero module.

LEMMA 1.51. *Let $I \subset R$ be an ideal, and E an R-module. Then the set*

$$IE = \left\{ \sum_{i=1}^{k} a_i e_i \colon a_i \in I, e_i \in E, k \in \mathbb{Z}_+ \right\}$$

is a submodule of E.

PROOF.
Clearly $IE \subset E$, and $IE \neq \emptyset$, as both I and E are nonempty. Let $x = \sum_{i=1}^{n} a_i e_i$ and $y = \sum_{i=1}^{m} b_i e_i'$ be elements of IE. Then

$$x - y = \sum_{i=1}^{n} a_i e_i - \sum_{i=1}^{m} b_i e_i' = \sum_{i=1}^{n} a_i e_i + \sum_{i=1}^{m} (-b_i) e_i',$$

and as I is an ideal, the elements $-b_i \in I$ and thus $x - y \in IE$. By the subgroup criterion,[2] IE is a subgroup. Furthermore, if $r \in R$, then

$$rx = r \sum_{i=1}^{n} a_i e_i = \sum_{i=1}^{n} r a_i e_i,$$

and because I is an ideal, the elements $ra_i \in I$, and thus $rx \in IE$. Therefore IE is also closed under the action of elements of R. This shows that IE is a submodule. □

REMARK 1.52. In the case when also E is an ideal of R, the product IE is exactly the same as the product of two ideals.

LEMMA 1.53. *Let $I \subset R$ be an ideal and E an R-module. Then E/IE is an R/I-module.*

PROOF.
By Lemma 1.51, $IE \subset E$ is a submodule, so the quotient E/IE is an additive abelian group. Define an action of R/I on E/IE by

$$(r + I)(e + IE) = re + IE,$$

[2] see Definition 1.1

when $r + I \in R/I$ and $e + IE \in E/IE$. This action is well defined: Assume that $r_1, r_2 \in R$ and $e_1, e_2 \in E$ so that $r_1 + I = r_2 + I$ and $e_1 + IE = e_2 + IE$. Then $r_1 - r_2 \in I$ and $e_1 - e_2 \in IE$. Thus

$$r_1e_1 - r_2e_2 = r_1e_1 - r_1e_2 + r_1e_2 - r_2e_2 = r_1(e_1 - e_2) + (r_1 - r_2)e_2 \in IE,$$

which implies that

$$(r_1 + I)(e_1 + IE) = r_1e_1 + IE = r_2e_2 + IE = (r_2 + I)(e_2 + IE).$$

Therefore the action does not depend on the representatives. It is straightforward to verify that the action also satisfies the requirements for a module action. Thus E/IE is an R/I-module. □

Definition 1.54. Let E be an R-module. The set

$$\mathrm{Ann}(E) = \{r \in R \colon re = 0 \text{ for all } e \in E\}$$

is called the *annihilator of* E.

Lemma 1.55. *The annihilator of E is an ideal of R.*

Proof.
Firstly, $0 \in \mathrm{Ann}(E)$, so $\mathrm{Ann}(E)$ is a nonempty subset of R. Let $a, b \in \mathrm{Ann}(E)$, $e \in E$ and $r \in R$. Then $(a - b)e = ae - be = 0$ and $(ra)e = r(ae) = 0$, so $\mathrm{Ann}(E)$ is an ideal. □

CHAPTER 2

The Problem: Minimal Number of Generators

For some rings, there exists a number k so that every ideal of that ring can be generated by k elements. In principal ideal domains, this number is 1; every ideal can be generated by one element. In *Dedekind domains*, any ideal can be generated by two elements; this is proven in [**Dummit**, section 16.3].

In the general situation, a global upper bound for the minimal number of generators might not exist. Example 5.4 shows that when R is an integral domain, for every $n \in \mathbb{Z}_+$ there exists an ideal $I_n \subset R[x, y]$ that cannot be generated by less than $n+1$ elements. Therefore no $k \in \mathbb{Z}_+$ can serve as an upper bound for the minimal number of generators for all ideals in $R[x, y]$. It can still be asked what is the minimal number of generators needed to generate a given ideal $I \subset R$. This number always exists if I is finitely generated, as in that case the set

$$\{k \in \mathbb{N} \colon \text{the ideal } I \text{ can be generated by } k \text{ elements}\}$$

is a nonempty subset of the natural numbers and hence has a minimal element.

If $I = (a_1, \ldots, a_n)$, the first idea might be to check whether any of the generators a_i could be removed so that the others would still generate I. The problem is unfortunately not so simple, which the following example points out.

Example 2.1. Consider the ideal $I = (x^2 + x, x^2) \subset \mathbb{Z}[x]$. As $x = (x^2 + x) - x^2 \in I$, $(x) \subset I$. Because both generators of I belong to (x), actually $I = (x)$. On the other hand, the ideal $(x^2 + x)$ is a proper subset of I: If $f \in (x^2 + x)$, $f = (x^2 + x)g$ for some $g \in \mathbb{Z}[x]$. Then either $g = 0$, which implies that also $f = 0$, or $g \neq 0$, in which case $\deg f = \deg(x^2 + x) + \deg g \geq 2$. Therefore $x \notin (x^2 + x)$. Similarly, $(x^2) \subsetneq I$.

The original generating set for I had two elements, neither of which suffices to generate I. However, there exists a third element, which generates I by itself. In a vector space, this kind of a situation is not possible: the two-element set would be a basis so it would not be possible for a single element to span the vector space. This example shows that the problem of finding the minimal number of generators for an ideal is more complicated than finding a basis for a vector space, as it is not sufficient to remove unnecessary generators.

Another way in which ideals and vector spaces differ, is the number of elements needed to generate a subset. The basis for a proper subspace always has less elements than the basis for the whole vector space. However, a proper ideal might require several generators whereas the ring itself is always generated by the identity element.

Example 2.2. The given generating set might also have infinitely many excessive elements. An infinite ring R generates itself, but also $R = (1_R)$. For a less obvious example, consider $I = (x, x^2, x^3, \ldots) \subset \mathbb{Z}[x]$. The elements of I consist of finite sums

where each term is divisible by some power of x. Therefore $I \subset (x)$. As clearly also $(x) \subset I$, in this case just one element, x, generates the whole ideal.

Even though $\mathbb{Z}$ is a principal ideal domain, the polynomial ring $\mathbb{Z}[x]$ is not. In some cases, the minimal number of generators can be verified using elementary methods, as in the next example. More general version of this example is given in Example 5.6.

EXAMPLE 2.3. The minimal number of generators for the ideal $(x, 2) \subset \mathbb{Z}[x]$ is two. This ideal consists of polynomials with even constant terms. Assume on the contrary, that there exists some $f \in \mathbb{Z}[x]$ so that $(f) = (x, 2)$. Then either $f_0 = 0$ of $f_0 \neq 0$. If $f_0 = 0$, then $g_0 = 0$ for all $g \in (f)$, which is not possible, as $2 \in (f)$. Therefore $f_0 \neq 0$.

As $x \in (f)$, $x = fg$ for some $g \in \mathbb{Z}[x]$. Then $\deg f + \deg g = 1$ by Remark 1.26. Therefore one of the polynomials f and g has degree 0 and the other degree 1, and thus there exist some $a, b, c \in \mathbb{Z}$, $a, c \neq 0$ for which

$$x = (ax + b)c = acx + bc.$$

Therefore $ac = 1$ and $bc = 0$, so $a = c = \pm 1$ and $b = 0$. As $f_0 \neq 0$, it follows that $f = c = \pm 1$, but this is a contradiction, as $(x, 2) \neq \mathbb{Z}[x]$.

CHAPTER 3

A Special Case: Local Rings

The goal of this chapter is to prove that the minimal number of generators for an ideal in a local ring is the same as the dimension of a specific vector space related to the ring and the ideal. This will be a corollary of a result for modules: Theorem 3.6, which is found in [**Matsumura**, chapter 2]. The proof of this theorem relies on Proposition 3.4 and Corollary 3.5, the formulation of which follows the one in [**Lang**, chapter X, section 4].

Definition 3.1. A commutative ring R is a *local ring*, if it has a unique maximal ideal M. The local ring is denoted by (R, M).

Example 3.2. All fields are local rings, as $\{0\}$ is the only proper ideal. More examples of local rings are given in the next chapter in the context of localization at a prime ideal.

The ring $\mathbb{Z}$ is not local, as $(p) \subset \mathbb{Z}$ is a maximal ideal whenever p is a prime number. The polynomial ring $\mathbb{Z}[x_1, \ldots, x_n]$ is not local either, as the ideal $(x_1, \ldots, x_n, p)$ is maximal for any prime p (look at Example 1.35).

In fact, polynomial rings $R[x_1, \ldots, x_n]$, where $R \neq \{0\}$ is a Noetherian ring, are never local. If $\{m_1, \ldots, m_k\} \subset R$ is some generating set for a maximal ideal in R, the maximal ideals $(x_1, \ldots, x_n, m_1, \ldots, m_k)$ and $(x_1 - 1_R, \ldots, x_n - 1_R, m_1, \ldots, m_k)$ from Remark 1.36 are not the same ideal: if they were, then $1_R = x_1 - (x_1 - 1_R)$ would be in this ideal. For fields the same conclusion holds for ideals $(x_1, \ldots, x_n)$ and $(x_1 - 1_R, \ldots, x_n - 1_R)$. So polynomial rings over fields are not local rings either, regardless of the fact that fields themselves are local rings.

Definition 3.3. The *Jacobson radical* of R is the intersection of all maximal ideals of R, and it is denoted by $\mathrm{rad}(R)$.

As the intersection of a (possibly infinite) collection of ideals, the Jacobson radical $\mathrm{rad}(R) \subset R$ is an ideal.

Proposition 3.4 (Nakayama's lemma). *Let $I \subset \mathrm{rad}(R)$ be an ideal of R, and let E be a finitely generated R-module. If $IE = E$, then $E = \{0\}$.*

Proof.
The statement can be proven by induction on the number of generators of E. First assume that E is generated by one element $e_1 \in E$, so $E = Re_1$. As $IE = E$, there exist $k \in \mathbb{Z}_+$, $a_1, \ldots, a_k \in I$ and $r_1, \ldots, r_k \in R$ such that

$$e_1 = a_1(r_1 e_1) + \cdots + a_k(r_k e_1) = \alpha e_1,$$

where $\alpha = \sum_{i=1}^{k} a_i r_i \in I$. Therefore

$$(1_R - \alpha)e_1 = 0_R. \tag{2}$$

Now $1_R - \alpha$ is a unit: if it is not, it generates a proper ideal which is contained in some maximal ideal $M \subset R$. As $\alpha \in I \subset \mathrm{rad}(R) \subset M$, also $1_R = (1_R - \alpha) + \alpha \in M$, which is not possible for a maximal ideal. By multiplying both sides of the equation (2) by $(1-\alpha)^{-1}$, it can be concluded that $e_1 = 0$, so $E = \{0\}$.

Assume then that the claim holds for any module with $n-1$ generators. Let E be a module generated by $\{e_1, \ldots, e_n\} \subset E$, so $E = \sum_{i=1}^{n} Re_i$. As $IE = E$, there exist $k \in \mathbb{Z}_+$, $a_1, \ldots, a_k \in I$ and $r_{i,1}, \ldots, r_{i,n}$, $i \in \{1, \ldots, k\}$ for which

$$e_n = \sum_{i=1}^{k} a_i(r_{i,1}e_1 + \cdots + r_{i,n}e_n) = \alpha_1 e_1 + \ldots \alpha_n e_n,$$

where each $\alpha_j = \sum_{i=1}^{k} a_i r_{i,j} \in I$. This means that

$$(1_R - \alpha_n)e_n = \alpha_1 e_1 + \cdots + \alpha_{n-1}e_{n-1}.$$

The same reasoning as above shows that $1_R - \alpha_n$ is a unit, so it can be concluded that e_n belongs to the module generated by the remaining elements. Therefore E is, in fact, generated by $n-1$ elements, and by the induction hypothesis $E = \{0\}$. □

Corollary 3.5. *Let E be an R-module, $F \subset E$ a submodule and $I \subset \mathrm{rad}(R)$ an ideal of R. Assume that E/F is finitely generated and $E = F + IE$. Then $E = F$.*

Proof.
Let $f \in F$ and $\sum_{i=1}^{n} a_i e_i \in IE$, so $a_i \in I$ and $e_i \in E$. As elementwise

$$\left(f + \sum_{i=1}^{n} a_i e_i\right) + F = \left(\sum_{i=1}^{n} a_i e_i\right) + F = \sum_{i=1}^{n} a_i \left(e_i + F\right),$$

it follows that

$$\frac{E}{F} = \frac{F + IE}{F} = I\frac{E}{F}.$$

As E/F is a finitely generated module by assumption, Nakayama's lemma implies that $E/F = \{0\}$, so $E = F$. □

Theorem 3.6. *Let (R, M) be a local ring, and E a finitely generated R-module. Then E is generated by $\{e_1, \ldots, e_n\}$ if and only if the set $\{e_1 + ME, \ldots, e_n + ME\}$ spans E/ME as an R/M -vector space.*

Proof.
As $M \subset R$ is a maximal ideal, the quotient R/M is a field by Proposition 1.22. By Lemma 1.53, E/ME is an R/M-module, which is the same as an R/M-vector space. Thus the claim of the theorem makes sense.

Assume first that E is generated by the elements e_i, which means that $E = \sum_{i=1}^{n} Re_i$. Let $v \in E/ME$. Then $v = b + ME$ for some $b \in E$, so there exist elements $r_i \in R$ such that $b = r_1e_1 + \cdots + r_ne_n$. Thus

$$\begin{aligned} v &= (r_1e_1 + \cdots + r_ne_n) + ME \\ &= (r_1e_1 + ME) + \cdots + (r_ne_n + ME) \\ &= (r_1 + M)(e_1 + ME) + \cdots + (r_n + M)(e_n + ME). \end{aligned}$$

Therefore the elements $e_i + ME$ span the vector space E/ME.

Assume then that E/ME is spanned by the elements $e_i + ME$. Let $x \in E$. Then there exist elements $r_i + M \in R/M$ such that

$$x + ME = \sum_{i=1}^{k} (r_i + M)(e_i + ME) = \sum_{i=1}^{k} r_i e_i + ME,$$

so $x - \sum_{i=1}^{k} r_i e_i = s \in ME$. Therefore

$$x = \sum_{i=1}^{k} r_i e_i + s \in \sum_{i=1}^{k} Re_i + ME,$$

and this implies that $E \subset \sum_{i=1}^{k} Re_i + ME$. Clearly also $\sum_{i=1}^{k} Re_i + ME \subset E$, so $E = \sum_{i=1}^{k} Re_i + ME$. Now $M = \mathrm{rad}(R)$ as the unique maximal ideal, $\sum_{i=1}^{k} Re_i \subset E$ is a submodule, and $E/(\sum_{i=1}^{k} Re_i)$ is finitely generated as E is. By Corollary 3.5, $E = \sum_{i=1}^{k} Re_i$. □

Corollary 3.7. *The minimal number of generators for a finitely generated ideal $I \subset R$ in a local ring (R, M) is the same as the R/M -vector space dimension of I/MI.*

Proof.
As the finitely generated ideal I is also a finitely generated R-module, the result of the previous theorem can be applied. Firstly, as I is finitely generated, there is some generating set $\{a_1, \ldots, a_n\}$. By the theorem, the set $\{a_1 + MI, \ldots, a_n + MI\}$ spans I/MI as a R/M -vector space. Therefore the vector space I/MI is finite-dimensional, with dimension $k \in \mathbb{N}$, where $k \leq n$. Fix a basis $\{b_1 + MI, \ldots, b_k + MI\}$ of I/MI. Then, by the theorem, I is generated by $\{b_1, \ldots, b_k\}$. This is the minimal number of generators: if there was a smaller set of generators, their images in I/MI would span I/MI, which is not possible. □

CHAPTER 4

A Useful Tool: Localization

The purpose of this chapter is to introduce the process of localization of a commutative ring. This process is similar to the one of constructing rational numbers from integers; that is actually an example of localization. Generally, localization does not make all nonzero elements of the ring invertible, as in the rational case. A special case, localization at a prime ideal, gives a local ring as the result. The chapter follows [**Dummit**, section 15.4].

Let $S \subset R$ be a multiplicatively closed subset and assume that $1_R \in S$. Define a relation $\sim$ on $R \times S$ by

$$(r_1, s_1) \sim (r_2, s_2) \iff (r_1 s_2 - r_2 s_1)t = 0 \quad \text{for some } t \in S. \tag{3}$$

LEMMA 4.1. *The relation* (3) *is an equivalence relation.*

PROOF.
Let $(r_1, s_1), (r_2, s_2), (r_3, s_3) \in R \times S$. The relation is reflexive: $(r_1, s_1) \sim (r_1, s_1)$ because $1 \in S$ and $(r_1 s_1 - r_1 s_1) \cdot 1 = 0$. It is also symmetric: if $(r_1, s_1) \sim (r_2, s_2)$, then there exists $t \in S$ for which $(r_1 s_2 - r_2 s_1)t = 0$. Then also

$$(r_2 s_1 - r_1 s_2)t = -(r_1 s_2 - r_2 s_1)t = 0,$$

so $(r_2, s_2) \sim (r_1, s_1)$.

Transitivity: Assume that $(r_1, s_1) \sim (r_2, s_2)$ and $(r_2, s_2) \sim (r_3, s_3)$. Then there exist $a, b \in S$ such that $(r_1 s_2 - r_2 s_1)a = 0$ and $(r_2 s_3 - r_3 s_2)b = 0$. Therefore $r_1 s_2 a = r_2 s_1 a$ and $r_2 s_3 b = r_3 s_2 b$, so

$$(r_1 s_3 - r_3 s_1)s_2 ab = (r_1 s_2 a)bs_3 - (r_3 s_2 b)s_1 a = (r_2 s_1 a)bs_3 - (r_2 s_3 b)s_1 a = 0.$$

As $s_2, a, b \in S$ and S is multiplicatively closed, also $s_2 ab \in S$ and thus the above calculation implies that $(r_1, s_1) \sim (r_3, s_3)$. □

REMARK 4.2. If the ring R is an integral domain and it is assumed that $0 \notin S$, the condition $(r_1 s_2 - r_2 s_1)t = 0$ for some $t \in S$ simplifies to $r_1 s_2 = r_2 s_1$. Note that $(r_1 s_2 - r_2 s_1) \cdot 0 = 0$, so if $0 \in S$, all pairs of elements in $R \times S$ are equivalent; in this case there is only one equivalence class.

DEFINITION 4.3. The set of equivalence classes under relation (3), denoted by $S^{-1}R$, is called the *localization of R at S*. The equivalence class of $(r, s) \in R \times S$ is denoted by $\frac{r}{s}$.

LEMMA 4.4. *Let $S \subset R$ be a multiplicatively closed subset with $1 \in S$. Then the operations*

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \quad \textit{and} \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

are well defined operations in $S^{-1}R$.

PROOF.
Note first that as R is a ring and S multiplicatively closed, the elements resulting from these operations are in $S^{-1}R$.

Assume that $\frac{a_1}{b_1} = \frac{a_2}{b_2}$ and $\frac{c_1}{d_1} = \frac{c_2}{d_2}$. Then there exist elements $s, t \in S$ such that $(a_1b_2 - a_2b_1)s = 0$ and $(c_1d_2 - c_2d_1)t = 0$. Also $st \in S$, because S is multiplicatively closed. Then

$$\begin{aligned}&((a_1d_1 + b_1c_1)b_2d_2 - (a_2d_2 + b_2c_2)b_1d_1)st\\ =&(a_1b_2d_1d_2 + c_1d_2b_1b_2 - a_2b_1d_1d_2 - c_2d_1b_1b_2)st\\ =&(a_1b_2 - a_2b_1)sd_1d_2t + (c_1d_2 - c_2d_1)tb_1b_2s = 0,\end{aligned}$$

so

$$\frac{a_1}{b_1} + \frac{c_1}{d_1} = \frac{a_1d_1 + b_1c_1}{b_1d_1} = \frac{a_2d_2 + b_2c_2}{b_2d_2} = \frac{a_2}{b_2} + \frac{c_2}{d_2}.$$

Therefore the addition is well defined. The multiplication does not depend on the representatives either:

$$\begin{aligned}&(a_1c_1b_2d_2 - a_2c_2b_1d_1)st\\ =&(a_1c_1b_2d_2 - a_2b_1c_1d_2 + a_2b_1c_1d_2 - a_2c_2b_1d_1)st\\ =&(a_1b_2 - a_2b_1)sc_1d_2t + (c_1d_2 - c_2d_1)ta_2b_1s = 0,\end{aligned}$$

so

$$\frac{a_1}{b_1} \cdot \frac{c_1}{d_1} = \frac{a_1c_1}{b_1d_1} = \frac{a_2c_2}{b_2d_2} = \frac{a_2}{b_2} \cdot \frac{c_2}{d_2}.$$

□

THEOREM 4.5. *$(S^{-1}R, +, \cdot)$ is a commutative ring.*

PROOF.
Let $\frac{r}{s}, \frac{r_1}{s_1}, \frac{r_2}{s_2}, \frac{r_3}{s_3} \in S^{-1}R$. Firstly, $(S^{-1}R, +)$ is an abelian group: It has a neutral element $0_{S^{-1}R} = \frac{0}{1}$, as

$$\frac{r}{s} + \frac{0}{1} = \frac{r + 0}{s} = \frac{r}{s}.$$

Note that $\frac{0}{1} = \frac{0}{t}$ for any $t \in S$. The addition is commutative, as both operations of R are commutative. Every element has an additive inverse, as

$$\frac{r}{s} + \frac{-r}{s} = \frac{rs - rs}{s^2} = \frac{0}{s^2} = 0_{S^{-1}R},$$

and the associativity of the addition follows from

$$\begin{aligned}\left(\frac{r_1}{s_1} + \frac{r_2}{s_2}\right) + \frac{r_3}{s_3} =& \frac{r_1s_2 + r_2s_1}{s_1s_2} + \frac{r_3}{s_3} = \frac{(r_1s_2 + r_2s_1)s_3 + r_3s_1s_2}{s_1s_2s_3}\\ =& \frac{r_1s_2s_3 + s_1(r_2s_3 + r_3s_2)}{s_1s_2s_3} = \frac{r_1}{s_1} + \frac{r_2s_3 + r_3s_2}{s_2s_3}\\ =& \frac{r_1}{s_1} + \left(\frac{r_2}{s_2} + \frac{r_3}{s_3}\right).\end{aligned}$$

Secondly, the multiplication satisfies the properties required of ring multiplication. The multiplicative identity is $\frac{1}{1}$, as

$$\frac{r}{s} \cdot \frac{1}{1} = \frac{r}{s}.$$

Note that for any $t \in S$, $\frac{t}{t} = \frac{1}{1}$, because $(t-t) \cdot 1 = 0$. Both associativity and commutativity of the multiplication are straightforward consequences of R being a commutative ring. For the distributivity

$$\begin{aligned}\frac{r_1}{s_1} \cdot \left(\frac{r_2}{s_2} + \frac{r_3}{s_3}\right) &= \frac{r_1}{s_1} \cdot \frac{r_2 s_3 + r_3 s_2}{s_2 s_3} = \frac{r_1(r_2 s_3 + r_3 s_2)}{s_1 s_2 s_3} \cdot \frac{1}{1} \\ &= \frac{r_1(r_2 s_3 + r_3 s_2)}{s_1 s_2 s_3} \cdot \frac{s_1}{s_1} = \frac{r_1 r_2 s_1 s_3 + r_1 r_3 s_1 s_2}{s_1 s_2 s_1 s_3} \\ &= \frac{r_1 r_2}{s_1 s_2} + \frac{r_1 r_3}{s_1 s_3} = \frac{r_1}{s_1} \cdot \frac{r_2}{s_2} + \frac{r_1}{s_1} \cdot \frac{r_3}{s_3},\end{aligned}$$

and by the above case and the commutativity of both addition and multiplication also

$$\left(\frac{r_1}{s_1} + \frac{r_2}{s_2}\right) \cdot \frac{r_3}{s_3} = \frac{r_3}{s_3} \cdot \left(\frac{r_1}{s_1} + \frac{r_2}{s_2}\right) = \frac{r_1}{s_1} \cdot \frac{r_3}{s_3} + \frac{r_2}{s_2} \cdot \frac{r_3}{s_3}.$$

Therefore $S^{-1}R$ is a commutative ring. □

Example 4.6. Let $R = \mathbb{Z}$ and $S = \mathbb{Z} - \{0\}$. As $\mathbb{Z}$ is an integral domain, the simpler version (look at Remark 4.2) of the equivalence relation (3) determines whether two elements of the localization are the same. This is the familiar cross-multiplication of rational numbers, and actually $S^{-1}R = \mathbb{Q}$: this is exactly the way to construct rational numbers from integers.

Proposition 4.7. *The map $\pi\colon R \to S^{-1}R$ given by $\pi(r) = \frac{r}{1}$, is a ring homomorphism.*

Proof.
Let $r, s \in R$. Then

$$\pi(r+s) = \frac{r+s}{1} = \frac{r}{1} + \frac{s}{1} = \pi(r) + \pi(s), \quad \text{and}$$

$$\pi(rs) = \frac{rs}{1} = \frac{r}{1} \cdot \frac{s}{1} = \pi(r) \cdot \pi(s).$$

Also $\pi(1_R) = \frac{1}{1} = 1_{S^{-1}R}$, so π is a ring homomorphism. □

Remark 4.8. The homomorphism π is injective in the case when S contains neither 0 nor zero divisors: if $\frac{r}{1} = \pi(r) = \frac{0}{1}$, then $rt = 0$ for some $t \in S$. But as $t \neq 0$ and t is not a zero divisor, the only possibility is that $r = 0$. Therefore $\ker(\pi) = \{0\}$, and thus π is injective. In this case, the localization $S^{-1}R$ thus contains a copy of the ring R.

Definition 4.9. Let $\varphi\colon R_1 \to R_2$ be a homomorphism of commutative rings. If $I \subset R_1$ is an ideal, then the *extension of I to R_2* is the ideal $I^e = (\varphi(I)) \subset R_2$, that is, the ideal generated by the image of I.

The notation for the extension is a bit vague, as it does not carry information about the homomorphism in question. However, in this text, the extension is used only in the context of localization. This means that $I^e = (\pi(I)) \subset S^{-1}R$, where π is the homomorphism from the ring R to its localization $S^{-1}R$ given in Proposition 4.7.

LEMMA 4.10. *Let $I \subset R$ be an ideal. The extension of I to a localization $S^{-1}R$ has the form*

$$I^e = \left\{ \frac{a}{s} \colon a \in I, s \in S \right\}.$$

PROOF.
By definition, I^e is generated by $\pi(I)$, thus by elements of the form $\frac{a}{1}$, $a \in I$. Let $s \in S$. Then $\frac{a}{s} = \frac{1}{s} \cdot \frac{a}{1} \in I^e$, so all the elements of this type are in I^e. Let now $y \in I^e$, so $y = \sum_{i=1}^k \frac{a_i}{1} \cdot \frac{r_i}{s_i}$, where $a_i \in I$, $r_i \in R$ and $s_i \in S$. Then

$$y = \sum_{i=1}^k \frac{a_i r_i}{s_i} = \frac{\sum_{i=1}^k \left(\prod_{j \neq i} s_j \right) a_i r_i}{\prod_{i=1}^k s_i} = \frac{b}{t},$$

where $b \in I$ and $t \in S$, because I is an ideal and S is multiplicatively closed. Therefore all elements of I^e are of this form. □

REMARK 4.11. Images of elements of S are invertible, as $\frac{s}{1} \cdot \frac{1}{s} = \frac{1}{1} = 1_{S^{-1}R}$ for any $s \in S$. (Remember the case of rational numbers, where each $k \in \mathbb{Z} - \{0\}$ becomes invertible.)

PROPOSITION 4.12. *Let $I \subset R$ be an ideal. Then $I^e = S^{-1}R$ if and only if $I \cap S$ is nonempty.*

PROOF.
Assume first that $I \cap S \neq \emptyset$, so there exists $s \in I \cap S$. Then $1_{S^{-1}R} = \frac{s}{1} \cdot \frac{1}{s} \in I^e$, so $I^e = S^{-1}R$.

Assume then that $I^e = S^{-1}R$, so $1_{S^{-1}R} \in I^e$. By Lemma 4.10, there exist elements $a \in I$, $b \in S$ for which $1_{S^{-1}R} = \frac{1}{1} = \frac{a}{b}$, which implies that $(b-a)t = 0$ for some $t \in S$. As S is multiplicatively closed, $at = bt \in S$. Because $a \in I$ and I is an ideal, also $at \in I$, so $at \in I \cap S$ and thus $I \cap S \neq \emptyset$. □

PROPOSITION 4.13. *Let $I \subset R$ be an ideal and A an index set. If I is generated by the set $\{a_i\}_{i \in A}$, then I^e is generated by $\{\frac{a_i}{1}\}_{i \in A}$.*

PROOF.
By Lemma 4.10, the extension I^e consists of all elements of the form $\frac{a}{s}$, where $a \in I$, $s \in S$. As $1_R \in S$, it follows that the elements $\frac{a_i}{1}$ are of this form, and thus the ideal generated by $\{\frac{a_i}{1}\}_{i \in A}$ is a subset of I^e. On the other hand, if $a \in I$, there exists a finite subset $B \subset A$, $r_i \in R$ and $a_i \in I$ for which $a = \sum_{i \in B} r_i a_i$. Thus for $s \in S$,

$$\frac{a}{s} = \frac{\sum_{i \in B} r_i a_i}{s} = \sum_{i \in B} \frac{r_i}{s} \cdot \frac{a_i}{1},$$

so $\frac{a}{s}$ belongs to the ideal generated by $\{\frac{a_i}{1}\}_{i \in A}$. Therefore I^e is a subset of this ideal. □

REMARK 4.14. In the case of a finite index set, the above proposition has the following form: If $I = (a_1, \ldots, a_n) \subset R$, then $I^e = \left(\frac{a_1}{1}, \ldots, \frac{a_n}{1}\right) = (\pi(a_1), \ldots, \pi(a_n))$. The reversed implication does not hold: even if $I^e = (\pi(a_1), \ldots, \pi(a_n))$, it is possible that the elements a_i do not generate I (look at Example 4.20).

DEFINITION 4.15. Let $P \subset R$ be a prime ideal. The localization $R_P = (R - P)^{-1}R$ is called the *localization of R at (the prime ideal) P*.

PROPOSITION 4.16. *Let $P \subset R$ be a prime ideal. Then the localization R_P is a local ring, with the unique maximal ideal P^e.*

PROOF.
As P is a prime and thus a proper ideal, $1_R \in R - P$, and particularly $R - P \neq \emptyset$. If $a, b \in R - P$, then $ab \in R - P$: $ab \in P$ would imply either $a \in P$ or $b \in P$, because P is a prime ideal. Therefore the set $R - P$ is closed under multiplication, and it is possible to construct the localization $R_P = (R - P)^{-1}R$.

The goal is to prove that the set of nonunits of R_P, here denoted by N, is an ideal. As every proper ideal is a subset of N (consists of nonunits), this will then be the unique maximal ideal. The first step is to prove that $\frac{a}{b} \in R_P$ is a unit if and only if $a \in R - P$, which will then imply that

$$N = \left\{ \frac{p}{u} : p \in P, u \in R - P \right\} \subset R_P. \tag{4}$$

Assume first that $\frac{a}{b}$ is a unit. Then there exists $\frac{c}{d} \in R_P$ such that $\frac{a}{b} \cdot \frac{c}{d} = \frac{1}{1}$, and thus $(ac - bd)f = 0$ for some $f \in R - P$. As P is prime, $0 \in P$ and $f \notin P$, this implies $ac - bd \in P$. Now if $a \in P$, also $ac \in P$. Then $bd = ac - (ac - bd) \in P$, as P is an ideal. This is a contradiction because both b and d are elements of the multiplicatively closed set $R - P$. Therefore $a \in R - P$.

Assume then that $a \in R - P$. Then $\frac{b}{a} \in R_P$, and $\frac{a}{b} \cdot \frac{b}{a} = \frac{1}{1}$, so $\frac{a}{b}$ is a unit.

The expression (4) is exactly the same as Lemma 4.10 gives for the ideal P^e, so N is an ideal. Therefore R_P is a local ring and $N = P^e$ is its unique maximal ideal. □

REMARK 4.17. The above proof used the expression for the extension of an ideal $I \subset R$ to R_P given by Lemma 4.10:

$$I^e = \left\{ \frac{a}{u} : a \in I, u \in R - P \right\}.$$

EXAMPLE 4.18. Let $R = \mathbb{Z}$. The ideal $P = (0)$ is a prime ideal, as $\mathbb{Z}$ is an integral domain. The localization $Z_{(0)} = \mathbb{Q}$; this was already discussed in Example 4.6. A similar construction exists also in other integral domains:

DEFINITION 4.19. If R is an integral domain, the localization $R_{(0)}$ is called its *quotient field* or *field of fractions*.

EXAMPLE 4.20. This example shows that the statement in Proposition 4.13 cannot be reversed: even if the images of some set of elements generate the extension of an ideal, the elements might not generate the original ideal. Let $R = \mathbb{Z}$ and $I = (4)$. The ideal (2) is a prime ideal, so the localization $\mathbb{Z}_{(2)}$ can be formed. The ring $\mathbb{Z}_{(2)}$ consists of those rational numbers the denominator of which is not divisible by 2.

By Proposition 4.13, $I^e = \left(\frac{4}{1}\right) \in \mathbb{Z}_{(2)}$. Also $\frac{12}{1}$ is a generator for I^e: $\frac{4}{1} = \frac{12}{1} \cdot \frac{1}{3}$, so $\left(\frac{4}{1}\right) \subset \left(\frac{12}{1}\right)$, and $\frac{12}{1} = \frac{4}{1} \cdot \frac{3}{1}$, so $\left(\frac{12}{1}\right) \subset \left(\frac{4}{1}\right)$. However, 12 does not generate I.

EXAMPLE 4.21. By Proposition 4.16, the localization $\mathbb{Z}_{(2)}$ is a local ring with the unique maximal ideal $M = (2)^e$, and $M = \left(\frac{2}{1}\right)$ by Proposition 4.13. Consider the product of M with itself: the ideal M^2. By Lemma 1.16, $M^2 = \left(\frac{4}{1}\right)$, and Proposition 4.13 gives that also $(4)^e = \left(\frac{4}{1}\right)$, so $M^2 = (4)^e$. By Remark 4.17,

$$M^2 = (4)^e = \left\{ \frac{a}{u} \colon a \in (4), u \notin (2) \right\},$$

so the generator $\frac{2}{1}$ of M is not an element of M^2, as it is not of this form. Therefore $M^2 \subsetneq M$. This is another example for the strict inclusion $IJ \subsetneq I \cap J$ when I and J are ideals, which was treated in Example 1.17.

In the previous example, the ideal $(2) \in \mathbb{Z}$ had the property

$$((2)(2))^e = (4)^e = M^2 = (2)^e(2)^e.$$

This is true in a more general setting:

PROPOSITION 4.22. *Let $I, J \subset R$ be ideals, and $S^{-1}R$ a localization of the ring R. Then $I^e J^e = (IJ)^e$.*

PROOF.
By Lemma 4.10, all elements of $I^e J^e$ consist of finite sums of terms of the form $\frac{a}{s} \cdot \frac{b}{t}$, where $a \in I$, $b \in J$, and $s, t \in S$. By the same lemma, all elements of $(IJ)^e$ are of the form $\frac{c}{u}$ where $c \in IJ$ and $u \in S$.

Elements of $I^e J^e$ can thus be written as follows:

$$\frac{a_1 b_1}{s_1 t_1} + \cdots + \frac{a_k b_k}{s_k t_k} = \frac{\sum_{i=1}^k \left(\prod_{j \neq i} s_j t_j \right) a_i b_i}{\prod_{i=1}^k s_i t_i} = \frac{\sum_{i=1}^k a_i' b_i}{\prod_{i=1}^k s_i t_i} = \frac{c}{u},$$

where $c \in IJ$ and $u \in S$, because each $a_i' = \left(\prod_{j \neq i} s_j t_j \right) a_i \in I$ and S is multiplicatively closed. Therefore $I^e J^e \subset (IJ)^e$.

Conversely, elements of $(IJ)^e$ can be written as

$$\frac{a_1 b_1 + \cdots + a_k b_k}{u} = \frac{1}{u} \left(\frac{a_1 b_1}{1} + \cdots + \frac{a_k b_k}{1} \right) = \frac{a_1 b_1}{u} + \cdots + \frac{a_k b_k}{u} = \frac{a_1}{1} \cdot \frac{b_1}{u} + \cdots + \frac{a_k}{1} \cdot \frac{b_k}{u},$$

so also $(IJ)^e \subset I^e J^e$. □

CHAPTER 5

Generalization: A Lower Bound for Non-Local Rings

In this chapter, the goal is to use the results of Chapter 3 to obtain a lower bound for the minimal number of generators for an ideal in a ring which is not local.

PROPOSITION 5.1. *Assume that R is not a local ring. Let $P \subset R$ be a prime ideal and $I \subset R$ a finitely generated ideal. Then the minimal number of generators for I is greater than or equal to the minimal number of generators for $I^e \subset R_P$.*

PROOF.
As I is finitely generated, $I = (a_1, \ldots, a_k)$ for some $a_i \in R$. Proposition 4.13 implies that $I^e = (\frac{a_1}{1}, \ldots, \frac{a_k}{1})$, so the ideal $I^e \subset R_P$ is also finitely generated. Let μ denote the minimal number of generators for I^e. If $\{b_1, \ldots, b_j\}$ is some other generating set for I, then $I^e = (\frac{b_1}{1}, \ldots, \frac{b_j}{1})$, which forces j to be greater than or equal to μ. Therefore the minimal number of generators for I is at least μ. □

REMARK 5.2. As R_P is a local ring by Proposition 4.16, it follows from Corollary 3.7 that $\mu = \dim_{R_P/P^e} I^e/P^eI^e$. In the case where a generating set for I of μ elements has already been found, the above proposition can be used to prove that there does not exist a smaller generating set.

If $I \not\subset P$, then $I^e = R_P$ by Proposition 4.12, and thus merely the trivial lower bound 1 is obtained. However, by Theorem 1.23 (or 1.24, if R is Noetherian), there exists a maximal ideal $M \supset I$, which is prime by Lemma 1.20. By Proposition 4.12, the ideal $I^e \subset R_M$ is then proper. So by using this ideal M as the prime ideal, it may be possible to obtain a nontrivial lower bound.

EXAMPLE 5.3. Let $I = (x, y)^2 \subset \mathbb{Z}[x, y]$. Then $I = (x^2, xy, y^2)$ by Lemma 1.16. In fact, all generating sets for I have at least three elements:

Let $M = (x, y, 2) \subset \mathbb{Z}[x, y]$. The ideal M is maximal (Example 1.35) and thus prime. As $I \subset M$, by the remark above it is possible to obtain a nontrivial lower bound by localizing at this ideal. The localization $L = \mathbb{Z}[x, y]_M$ consists of equivalence classes of elements of the form $\frac{f}{g}$, where $f, g \in \mathbb{Z}[x, y]$ and $g \notin M$, and L is a local ring with the unique maximal ideal M^e (Proposition 4.16). Proposition 4.13 gives generators for the extensions of the ideals I and M to L:

$$I^e = \left(\frac{x^2}{1}, \frac{xy}{1}, \frac{y^2}{1}\right) \quad \text{and} \quad M^e = \left(\frac{x}{1}, \frac{y}{1}, \frac{2}{1}\right).$$

By Proposition 5.1, the minimal number of generators for I is at least the minimal number of generators for $I^e \subset L$, which in turn is the L/M^e-vector space dimension of I^e/M^eI^e by Corollary 3.7. The elements

$$\frac{x^2}{1} + M^eI^e, \quad \frac{xy}{1} + M^eI^e, \quad \frac{y^2}{1} + M^eI^e$$

generate I^e/M^eI^e by Theorem 3.6, because the finitely generated ideal $I^e \subset L$ is also an L-module, and the localization L is a local ring. In order to verify that the dimension of I^e/M^eI^e is 3, it suffices to show that these three generators are linearly independent.

Fortunately the structure of the quotient field L/M^e is quite simple: it turns out that it is isomorphic to the field $\mathbb{F}_2$ of two elements. This can be seen in two steps:

Firstly, $\frac{f}{g} + M^e = 0 + M^e$ if and only if $\frac{f}{g} \in M^e$. This is equivalent to $f \in M$, as by Remark 4.17, $M^e = \{\frac{f}{g} \colon f \in M, g \notin M\}$. Note that $f \in M$ if and only if the constant term f_0 of f belongs to $(2) \subset \mathbb{Z}$: the ideal M consists of all polynomials with an even constant term. Therefore $f \notin M$ if and only if f_0 is an odd integer.

Secondly, if $a, b \in L$ with $a+M^e \neq 0+M^e$ and $b+M^e \neq 0+M^e$, then $a+M^e = b+M^e$, so there exist only two equivalence classes, which verifies the isomorphism. Indeed, assume that $\frac{f_1}{g_1}, \frac{f_2}{g_2} \in L$ so that the classes of these element are nonzero, so $f_1, f_2 \notin M$. Then

$$\frac{f_1}{g_1} - \frac{f_2}{g_2} = \frac{f_1g_2 - f_2g_1}{g_1g_2} \in M^e,$$

because the constant term of $f_1g_2 - f_2g_1$ belongs to the ideal $(2) \subset \mathbb{Z}$ as the difference of the constant terms of f_1g_2 and f_2g_1 which are both odd. Thus

$$\frac{f_1}{g_1} + M^e = \frac{f_2}{g_2} + M^e.$$

The isomorphism $L/M^e \simeq \mathbb{F}_2$ significantly simplifies the verification of linear independence, as it suffices to show that if $a_i \in \{0, 1\}$, the equation

$$(a_1+M^e)\left(\tfrac{x^2}{1} + M^eI^e\right) + (a_2+M^e)\left(\tfrac{xy}{1} + M^eI^e\right) + (a_3+M^e)\left(\tfrac{y^2}{1} + M^eI^e\right) = 0+M^eI^e$$

implies that $a_i = 0$ for all i. This is true, as none of the elements

$$\frac{x^2}{1}, \frac{xy}{1}, \frac{y^2}{1}, \frac{x^2+xy}{1}, \frac{x^2+y^2}{1}, \frac{xy+y^2}{1}, \frac{x^2+xy+y^2}{1}$$

belongs to M^eI^e. This can be justified as follows:

By Proposition 4.22, $M^eI^e = (MI)^e$, and by Lemma 1.16,

$$MI = (x^3, x^2y, 2x^2, xy^2, 2xy, y^3, 2y^2).$$

If $\frac{x^2}{1} \in M^eI^e = (MI)^e$, then $x^2 \in MI$, as Remark 4.17 gives the expression

$$(MI)^e = \left\{ \frac{f}{g} \colon f \in MI, g \notin M \right\}.$$

Assume that $x^2 \in MI$, so x^2 can be expressed by using the generators of MI. By gathering all generators with y, there exist some $a, b, c \in \mathbb{Z}[x, y]$ for which

$$x^2 = ax^3 + b(2x^2) + cy.$$

On the right-hand side, the only term that could produce the term x^2 is $b_0 \cdot 2x^2$, but this has an even coefficient. Therefore $x^2 \notin MI$ and thus $\frac{x^2}{1} \notin M^eI^e$. Similar reasoning holds for the other elements. (In somewhat imprecise terms, the elements of the ideal MI are of degree at least 3 in "variables" $\{x, y, 2\}$.)

EXAMPLE 5.4. Assume that R is an integral domain, and let $I_n = (x, y)^n \subset R[x, y]$ for each $n \in \mathbb{Z}_+$. Then the minimal number of generators for I_n is $n + 1$.

Firstly, I_n can be generated by the set $\{x^n, x^{n-1}y, \ldots, xy^{n-1}, y^n\}$, which has $n + 1$ elements. This follows from Lemma 1.16 and induction. As R is an integral domain, the ideal $P = I_1 = (x, y)$ is a prime ideal by Proposition 1.31. The ideal P consists of polynomials with constant term 0, and $I_n \subset P$. The goal is to prove that the minimal number of generators for $I_n^e \subset R[x, y]_P$ is $n + 1$, and then Proposition 5.1 gives the lower bound for minimal number of generators for I. By Corollary 3.7, this number is the same as the dimension of $I_n^e/P^eI_n^e$ as an $R[x, y]_P/P^e$-vector space. Note that by Proposition 4.22,

$$I_n^e/P^eI_n^e = I_n^e/(PI_n)^e = I_n^e/I_{n+1}^e.$$

By Proposition 4.13, the ideal I_n^e is generated by the set $\{\frac{x^n}{1}, \frac{x^{n-1}y}{1}, \ldots, \frac{xy^{n-1}}{1}, \frac{y^n}{1}\}$, and the images of these generate I_n^e/I_{n+1}^e. It remains to show that the set of the images,

$$\left\{ \frac{x^{n-i}y^i}{1} + I_{n+1}^e \colon i = 0, \ldots, n \right\},$$

is linearly independent. This verification can be simplified, as for any $\frac{f}{g} \in R[x, y]_P$, $\frac{f}{g} + P^e = \frac{f_0}{g_0} + P^e$: the constant term of the polynomial $g_0f - f_0g$ is $g_0f_0 - f_0g_0 = 0$, so this polynomial is in P, and thus by Remark 4.17

$$\frac{f}{g} - \frac{f_0}{g_0} = \frac{g_0f - f_0g}{g_0g} \in P^e.$$

Actually $R[x, y]_P/P^e \cong R_{(0)}$, where $R_{(0)}$ is the quotient field of R, but this isomorphism is not needed for the argument. By the observation above, it suffices to verify that when $r_i \in R$, $t_i \in R - \{0\}$, the relation

$$\sum_{i=0}^{n} \left(\frac{r_i}{t_i} + P^e \right) \left(\frac{x^{n-i}y^i}{1} + I_{n+1}^e \right) = \frac{0}{1} + I_{n+1}^e$$

implies $\frac{r_i}{t_i} + P^e = \frac{0}{1} + P^e$ for all i. The relation can be written as

$$\frac{\sum_{i=0}^{n} \left[\left(\prod_{j \neq i} t_j \right) r_i x^{n-i} y^i \right]}{\prod_{i=0}^{n} t_i} = \sum_{i=0}^{n} \frac{r_i x^{n-i} y^i}{t_i} \in I_{n+1}^e,$$

which is equivalent to

$$\sum_{i=0}^{n} \left[\left(\prod_{j \neq i} t_j \right) r_i x^{n-i} y^i \right] \in I_{n+1}.$$

As the ideal I_{n+1} is generated by monomials of degree $n + 1$, the monomials of any nonzero polynomial in I_{n+1} have at least this degree. As every $t_j \neq 0$ and R does not have any zero divisors, it follows that every $r_i = 0$; otherwise the above polynomial would have monomial terms with degree n. Therefore also $\frac{r_i}{t_i} + P^e = \frac{0}{1} + P^e$ for all $i = 0, \ldots, n$. Now every generating set of I_n has at least $n + 1$ elements, and a generating set with this number of elements was already found, which proves that the minimal number of generators for I_n is $n + 1$.

REMARK 5.5. As fields are integral domains, the above example shows that the minimal number of generators for $(x,y)^n \subset R[x,y]$ is $n+1$, when R is a field. This shows that polynomial rings in several variables over fields are not principal ideal domains, even though those in one variable are.

The next example is a generalization of Example 2.3. It follows the structure of Example 5.4, and therefore not all the details are repeated.

EXAMPLE 5.6. Let $I_n = (x,2)^n \in \mathbb{Z}[x]$. Then the minimal number of generators for I_n is $n+1$.

The ideal I_n can be generated by the set $\{x^n, 2x^{n-1}, \ldots, 2^{n-1}x, 2^n\}$, which has $n+1$ elements. The ideal $P = I_1 = (x,2)$, which consists of polynomials with even constant terms, is a maximal ideal by Example 1.35, and thus prime. Also, $I_n \subset P$ for all n. The minimal number of generators for $I_n^e \subset \mathbb{Z}[x]_P$ is the same as the dimension of $I_n^e/P^eI_n^e$ as $R[x]_P/P^e$-vector space. Also in this case $I_n^e/P^eI_n^e = I_n^e/I_{n+1}^e$, elements of the form $\frac{2^{n-i}x^i}{1}$ generate I_n^e, and the goal is to prove that the set of their images,

$$\left\{ \frac{2^{n-i}x^i}{1} + I_{n+1}^e \colon i = 0, \ldots, n \right\},$$

is linearly independent. The verification can be simplified with the observation that $\frac{f}{g} + P^e = \frac{f_0}{g_0} + P^e$ for any $\frac{f}{g} \in R[x,y]_P$: the constant term of the polynomial $g_0 f - f_0 g$ is $g_0 f_0 - f_0 g_0 = 0$, therefore even, so this polynomial is in P, and thus

$$\frac{f}{g} - \frac{f_0}{g_0} = \frac{g_0 f - f_0 g}{g_0 g} \in P^e.$$

Note that when $g \notin P$, g_0 is odd. It is now enough to show that for $a_i \in \mathbb{Z}$, $b_i \in \mathbb{Z} - 2\mathbb{Z}$ (odd integers), the relation

$$\sum_{i=0}^{n} \left(\frac{a_i}{b_i} + P^e \right) \left(\frac{2^{n-i}x^i}{1} + I_{n+1}^e \right) = \frac{0}{1} + I_{n+1}^e$$

implies $\frac{a_i}{b_i} + P^e = \frac{0}{1} + P^e$ for all i. The relation can be written as

$$\frac{\sum_{i=0}^{n} \left[\left(\prod_{j \neq i} b_j \right) a_i 2^{n-i} x^i \right]}{\prod_{i=0}^{n} b_i} = \sum_{i=0}^{n} \frac{a_i 2^{n-i} x^i}{b_i} \in I_{n+1}^e,$$

which is equivalent to

$$\sum_{i=0}^{n} \left[\left(\prod_{j \neq i} b_j \right) a_i 2^{n-i} x^i \right] \in I_{n+1}.$$

As the ideal I_{n+1} is generated by the set $\{x^{n+1}, 2x^n, \ldots, 2^n x, 2^{n+1}\}$, it is clear that all the terms of its polynomials have to be divisible by $2^k x^j$ with $k + j \geq n+1$. As all b_j are odd, it follows that numbers a_i have to be divisible by 2. Therefore $\frac{a_i}{b_i} + P^e = \frac{0}{1} + P^e$ for all i. This completes the proof.

CHAPTER 6

More Tools: Ring and Module Constructions

This chapter builds more background for the result of [**Forster**] in the next chapter.

6.1. Radical Ideals

Radical ideals are a special subtype of ideals. The beginning of the section lists some basic properties, and it uses [**Dummit**, section 15.2]. Proposition 6.7 in the end of this section states that in Noetherian rings, every proper radical ideal is a finite intersection of prime ideals. The proof, together with Lemma 6.5 and its corollary on which it relies, are based on a question and its answer [**Radical Ideal**] on math.stackexchange.com, with the missing details filled in.

DEFINITION 6.1. Let $I \subset R$ be an ideal.

(i) The *radical of* I is
$$\sqrt{I} = \{r \in R \colon r^k \in I \text{ for some } k \in \mathbb{Z}_+\}.$$
(ii) The ideal I is a *radical ideal* if $I = \sqrt{I}$.

LEMMA 6.2. *Let $I \subset R$ be an ideal. Then $\sqrt{I}$ is a radical ideal of R that contains I.*

PROOF.
The inclusion $I \subset \sqrt{I}$ is clear by definition, and especially $\sqrt{I}$ is nonempty. Let $r \in R$ and $a, b \in \sqrt{I}$, so there exist $m, n \in \mathbb{Z}_+$ for which $a^m \in I$ and $b^n \in I$. Then $(ra)^m = r^m a^m \in I$, so $ra \in \sqrt{I}$. It remains to show that $a - b \in \sqrt{I}$. Now
$$(a-b)^{m+n} = \sum_{\substack{j,k \in \mathbb{N}, \\ j+k=m+n}} r_{jk} a^j b^k$$
for some $r_{jk} \in R$, and in each term either $j \geq m$ or $k \geq n$: otherwise $j + k < m + n$. Therefore each term $r_{jk} a^j b^k \in I$, so $(a-b)^{m+n} \in I$. This shows that $\sqrt{I}$ is an ideal.

To prove that $\sqrt{I}$ is a radical ideal, the equality $\sqrt{\sqrt{I}} = \sqrt{I}$ is needed. Again, $\sqrt{I} \subset \sqrt{\sqrt{I}}$ is clear. If $c \in \sqrt{\sqrt{I}}$, then there exists $s \in \mathbb{Z}_+$ for which $a^s \in \sqrt{I}$. Then there also exists $t \in \mathbb{Z}_+$ for which
$$a^{st} = (a^s)^t \in I.$$
It follows that $a \in \sqrt{I}$; this verifies the inclusion $\sqrt{\sqrt{I}} \subset \sqrt{I}$. Therefore $\sqrt{I}$ is a radical ideal. □

LEMMA 6.3. *Let $I \subset R$ be an ideal and $P \subset R$ a prime ideal. Then*
$$I \subset P \iff \sqrt{I} \subset P.$$

PROOF.
Assume first that $\sqrt{I} \subset P$. As $I \subset \sqrt{I}$ by Lemma 6.2, then $I \subset P$. Assume then that $I \subset P$. Let $a \in \sqrt{I}$, so there is $k \in \mathbb{Z}_+$ for which $a^k \in I \subset P$. As P is prime, either $a \in P$ or $a^{k-1} \in P$. Both options eventually imply that $a \in P$. Therefore $\sqrt{I} \subset P$. □

EXAMPLE 6.4. Prime ideals are radical ideals. This can be seen from Lemma 6.3 by setting $I = P$, and using the fact given by Lemma 6.2: every ideal is contained in its radical. However, not every radical ideal is a prime ideal: as an example, $(6) \subset \mathbb{Z}$ is radical but not prime. Indeed, if $a \in \sqrt{(6)}$, then there exists $k \in \mathbb{Z}_+$ and $b \in \mathbb{Z}$ for which $a^k = 6b$. Now either $b = 0$, from which follows $a = 0 \in (6)$, or $b \neq 0$, which implies that a has both 2 and 3 in its prime factorization, and thus $a \in (6)$. This shows that (6) is a radical ideal.

Even though the radical ideal $(6) \subset \mathbb{Z}$ is not a prime ideal (prime ideals in $\mathbb{Z}$ are generated by prime numbers), it is the intersection of two prime ideals: $(6) = (2) \cap (3)$. This is true in a more general setting: in Noetherian rings, all radical ideals are finite intersections of prime ideals: this will be proven in Proposition 6.7, after the following preparatory lemma and its corollary. It is also easy to verify that every finite intersection of prime ideals is a radical ideal.

LEMMA 6.5. *Let $I \subset R$ be a radical ideal, and $ab \in I$. Then*

$$I = \sqrt{I + (a)} \cap \sqrt{I + (b)}.$$

PROOF.
By Lemma 6.2, an ideal is contained in its radical. Therefore $I \subset I + (a) \subset \sqrt{I + (a)}$ and $I \subset I + (b) \subset \sqrt{I + (b)}$, so

$$I \subset \sqrt{I + (a)} \cap \sqrt{I + (b)}.$$

Let $r \in \sqrt{I + (a)} \cap \sqrt{I + (b)}$. Then $r^m \in I + (a)$ for some $m \in \mathbb{Z}_+$, and $r^n \in I + (b)$ for some $n \in \mathbb{Z}_+$. This means that there exist $c_1, c_2 \in I$, $s_1, s_2 \in R$ for which $r^m = c_1 + s_1 a$ and $r^n = c_2 + s_2 b$. It follows that

$$r^{m+n} = r^m r^n = (c_1 + s_1 a)(c_2 + s_2 b) = c_1 c_2 + c_1 s_2 b + s_1 a c_2 + s_1 s_2 ab \in I,$$

as $ab \in I$. Therefore $r \in \sqrt{I} = I$, so $\sqrt{I + (a)} \cap \sqrt{I + (b)} \subset I$. □

COROLLARY 6.6. *Let $I \subset R$ be a proper nonprime radical ideal. Then there exist proper radical ideals I_1 and I_2 with $I \subsetneq I_1$ and $I \subsetneq I_2$, so that $I = I_1 \cap I_2$.*

PROOF.
As I is not a prime ideal, there exists $ab \in I$ with neither a nor b being an element of I. By Lemma 6.5,

$$I = \sqrt{I + (a)} \cap \sqrt{I + (b)}.$$

It remains to prove that these two ideals satisfy the given conditions. Firstly, they are radical ideals by Lemma 6.2. Secondly, as $a \notin I$,

$$I \subsetneq I + (a) \subset \sqrt{I + (a)},$$

and similarly $I \subsetneq \sqrt{I + (b)}$. Lastly, if $\sqrt{I + (a)} = R$, then

$$I = \sqrt{I + (a)} \cap \sqrt{I + (b)} = R \cap \sqrt{I + (b)} = \sqrt{I + (b)},$$

which is a contradiction, and $\sqrt{I+(b)} = R$ leads to a similar contradiction. Therefore both $\sqrt{I+(a)}$ and $\sqrt{I+(b)}$ are proper ideals. □

PROPOSITION 6.7. *Every proper radical ideal in a Noetherian ring is a finite intersection of prime ideals.*

PROOF.
Let R be a Noetherian ring and $I \subset R$ a proper radical ideal. If I is a prime ideal, there is nothing to prove, so it can be assumed that I is not a prime ideal. By Corollary 6.6, there exist proper radical ideals I_1 and I_2 with $I \subsetneq I_1$ and $I \subsetneq I_2$, and $I = I_1 \cap I_2$. If both I_1 and I_2 are prime, then I is a finite intersection of prime ideals. Otherwise, the process can be repeated to the nonprime ideal(s). For example, if I_1 is not prime, then Corollary 6.6 gives proper radical ideals I_{11} and I_{12} with $I_1 = I_{11} \cap I_{12}$, and then

$$I = I_1 \cap I_2 = I_{11} \cap I_{12} \cap I_2.$$

At stage n, there are at most 2^n proper radical ideals as intersection of which I can be expressed. It remains to show that after a finite number of steps, prime ideals are reached. If this does not hold, then at each stage at least one of the ideals is not prime, and there is a strictly increasing chain, consisting of $n+1$ ideals, that ends with that nonprime ideal. Therefore the process creates an infinite strictly increasing chain of ideals, which is a contradiction with R being Noetherian. Therefore I can be expressed as a finite intersection of prime ideals. □

6.2. Zariski Topology

The set of all prime ideals of R can be equipped with a topology called the Zariski topology. This section uses [**Dummit**, section 15.5].

DEFINITION 6.8. The *prime spectrum of* R is the set of all prime ideals of R, and it is denoted by $\operatorname{Spec} R$. The *maximal spectrum of* R is correspondingly the set of all maximal ideals of R, and it is denoted by $\operatorname{mSpec} R \subset \operatorname{Spec} R$.

DEFINITION 6.9. Let $A \subset R$ be a subset and define

$$V(A) = \{P \in \operatorname{Spec} R \colon A \subset P\}.$$

The *Zariski topology* on $\operatorname{Spec} R$ is the topology τ where the collection of closed sets is $\{V(I) \colon I \subset R \text{ is an ideal}\}$.

REMARK 6.10. When defining $V(A)$, the subset A can be replaced by the ideal it generates. This follows from the fact given by Corollary 1.8: if I is any ideal, $A \subset I$ if and only if $(A) \subset I$.

LEMMA 6.11. *Let $I \subset R$ be an ideal. Then $V(I) = V(\sqrt{I})$.*

PROOF.
This follows from Lemma 6.3, which states that when $P \subset R$ is a prime ideal , $I \subset P$ if and only if $\sqrt{I} \subset P$. □

PROPOSITION 6.12. *The Zariski topology is a topology:* $(\operatorname{Spec} R, \tau)$ *is a topological space.*

PROOF.
Note that the ideals 0 and R give $V(0) = \operatorname{Spec} R$ and $V(R) = \emptyset$, so $\operatorname{Spec} R$ and $\emptyset$ are closed. It remains to prove that finite unions and arbitrary intersections of sets $V(I_j)$ are closed (of the form $V(I)$ for some ideal I).

Finite unions: When I and J are ideals, $V(I) \cup V(J) = V(IJ)$. Firstly, if a prime ideal $P \in V(I) \cup V(J)$, then $I \subset P$ or $J \subset P$. As IJ is contained in both I and J, it follows that $IJ \subset P$, and thus $P \in V(IJ)$. Secondly, if $P \in V(IJ)$, then $IJ \subset P$. If $I \not\subset P$, then there is $i \in I$ such that $i \notin P$. But as $IJ \subset P$, also $iJ \subset P$, so as P is prime, it follows that $J \subset P$. Therefore $P \in V(I) \cup V(J)$. By induction, when I_j, $j \in \{1, \ldots, k\}$ are ideals, $\cup_{j=1}^{k} V(I_j)$ is closed.

Arbitrary intersections: Let A be an index set and $\{I_j \colon j \in A\}$ a collection of ideals. For a prime ideal $P \subset R$,

$$P \in \bigcap_{j \in A} V(I_j) \iff I_j \subset P \ \forall j \in A \iff \bigcup_{j \in A} I_j \subset P \iff P \in V\left(\bigcup_{j \in A} I_j\right),$$

it follows that

$$\bigcap_{j \in A} V(I_j) = V\left(\bigcup_{j \in A} I_j\right).$$

The union of the ideals I_j is not an ideal in general (look at Example 1.3). However, by Remark 6.10, it can be replaced by the ideal it generates. Therefore arbitrary intersections are closed. □

DEFINITION 6.13. A prime ideal $P \subset R$ is said to have *(Krull) dimension k*, denoted by $\dim P = k$, when there exists a chain $P \subsetneq P_1 \subsetneq \cdots \subsetneq P_k \subsetneq R$ of prime ideals, but no longer chains exist. The *(Krull) dimension of R* is defined to be

$$\dim R = \sup_{P \in \operatorname{Spec} R} \dim P.$$

REMARK 6.14. For a maximal ideal $M \subset R$, $\dim M = 0$. The only prime ideal of a field F is the zero ideal, which is also a maximal ideal. Therefore $\dim F = 0$.

EXAMPLE 6.15. The Krull dimension of $\mathbb{Z}$ is 1. The integers is a principal ideal domain, so its every nonzero prime ideal is maximal by Lemma 1.21. If P_1 and P_2 are prime ideals, the inclusion $P_1 \subsetneq P_2 \subsetneq \mathbb{Z}$ is therefore possible only for $P_1 = (0)$, so the only prime ideal having nonzero dimension is the zero ideal, which has dimension 1.

REMARK 6.16. In Noetherian rings, these kinds of strictly increasing chains of ideals cannot be infinite. However, the supremum of the lengths, and therefore the Krull dimension of a Noetherian ring, might be infinite. An example of this is discussed in [**Eisenbud**, exercise 9.6], and the original example is in [**Nagata**, appendix A1, example 1].

6.3. Tensor Product of Modules

This section introduces the construction of the tensor product of two modules, and it follows [**Lang**, chapter 16, section 1]. The construction needs the following concepts: direct products of groups [**Lang**, chapter 1, section 2], direct products and sums of

modules [**Dummit**, exercise 20, section 10.3], and free modules [**Lang**, chapter 3, section 4]. Existence and universal property of free modules (Propositions 6.23 and 6.24) follow [**Dummit**, section 10.3], and Propositions 6.28 and 6.29 use [**Dummit**, section 10.4].

DEFINITION 6.17. Let A be an index set and G_i an additive group for all $i \in A$. Let $G = \prod_{i\in A} G_i$ be the Cartesian product of the sets G_i; elements of G are thus of the form $(g_i)_{i\in A}$ where each $g_i \in G_i$. The set G together with componentwise addition is called the *direct product of the groups* G_i.

PROPOSITION 6.18. *The direct product of groups G_i, $i \in A$, is a group, and it is abelian if each G_i is abelian.*

PROOF.
The addition $(g_i)_{i\in A} + (h_i)_{i\in A} = (g_i + h_i)_{i\in A}$ is associative, as the addition in each G_i is. The zero element of G is $(0_{G_i})_{i\in A}$. Also every element $(g_i)_{i\in A}$ has an inverse $(-g_i)_{i\in A}$. Therefore G is a group. The commutativity of addition in each G_i implies commutativity for addition in G, from which the second claim follows. □

DEFINITION 6.19. Let A be an index set and E_i an R-module for each $i \in A$. The *direct product of the modules* E_i, denoted by $\prod_{i\in A} E_i$, is their direct product as abelian groups with componentwise multiplication by elements of R. The *direct sum of the modules* E_i is the subset of the direct product consisting of all elements $(e_i)_{i\in A}$ for which only finitely many of the components e_i are nonzero, and it is denoted by $\bigoplus_{i\in A} E_i$.

REMARK 6.20. The case of a finite index set A is simple: the direct product of modules $E_1, \ldots, E_k$ is the same as their direct sum.

PROPOSITION 6.21. *The direct product of any collection of R-modules E_i is an R-module, and the direct sum of the modules E_i is its submodule.*

PROOF.
Denote the direct product and the direct sum by $E = \prod_{i\in A} E_i$ and $E_+ = \bigoplus_{i\in A} E_i$. The direct product is nonempty as $(0_{E_i})_{i\in A} \in E$, and it is an abelian group by Proposition 6.18. As each E_i is an R-module, it is straightforward to verify that the ring action $r(e_i)_{i\in A} = (re_i)_{i\in A}$ satisfies the required properties, so E is an R-module.

The direct sum is a nonempty subset of the direct product, because $(0_{E_i})_{i\in A} \in E_+$. If $(a_i)_{i\in A}, (b_i)_{i\in A} \in E_+$, then

$$(a_i)_{i\in A} - (b_i)_{i\in A} = (a_i - b_i)_{i\in A} \in E_+,$$

as the set of indices for which $a_i - b_i \neq 0$ is finite. By the subgroup criterion, E_+ is a subgroup. As also $r(a_i)_{i\in A} = (ra_i)_{i\in A} \in E_+$ for any $r \in R$, E_+ is a submodule. □

DEFINITION 6.22. Let E be an R-module. A nonempty subset $T \subset E$ is a *basis of* E, if every element $a \in E$ has a unique expression $a = \sum_{e\in U} r_e e$ where $U \subset T$ is finite and each $r_e \in R$. If a basis T exists, the module E is called a *free R-module (on the set T)*, and in this case $E = \bigoplus_{e\in T} Re$.

PROPOSITION 6.23. *For any nonempty set T, there exists a free R-module $E(T)$ on the set T.*

PROOF.
Let $E(T)$ be the collection of all functions $f\colon T \to R$ that take on nonzero values at finitely many points, that is, for which the set $\{t \in T\colon f(t) \neq 0\}$ is finite. The set $E(T)$ becomes an R-module, when addition of functions and multiplication by ring elements are defined pointwise:

$$(f+g)(t) = f(t) + g(t) \text{ and } (rf)(t) = rf(t).$$

For example, for $f, g \in E(T)$ and $r \in R$,

$$\begin{aligned}(r(f+g))(t) &= r(f+g)(t) = r(f(t)+g(t)) \\ &= rf(t) + rg(t) = (rf)(t) + (rg)(t)\end{aligned}$$

for all $t \in T$, so $r(f+g) = rf + rg$. The other R-module properties can be checked similarly.

Elements $t \in T$ can be identified with functions $f_t \in E(T)$, where

$$f_t(x) = \begin{cases} 1, & x = t \\ 0, & x \neq t. \end{cases}$$

In this way, T can be interpreted as a subset of $E(T)$. Now every function $f \in E(T)$ is a sum of functions f_t: If f gets nonzero values at n different points $\{t_1, \ldots, t_n\}$ and the values at these points are $f(t_i) = r_i \in R$, then

$$f = \sum_{i=1}^{n} r_i f_{t_i}.$$

These sums are unique, because each f_{t_i} only contributes to the value at t_i. Also, this sum can be identified with $\sum_{i=1}^{n} r_i t_i$. This proves that $E(T)$ is a free R-module on the set T. □

The next proposition shows that free modules have the following property: any map from the basis to some R-module can be uniquely extended into an R-module homomorphism from the free module. This is known as the *universal property of free modules*.

PROPOSITION 6.24. *Let E be a free R-module with basis T, and F an R-module. For every function $\varphi\colon T \to F$, there exists a unique R-module homomorphism $\Phi\colon E \to F$ for which $\Phi|_T = \varphi$.*

PROOF.
Define $\Phi\colon E \to F$ by setting

$$\Phi\left(\sum_{i=1}^{n} r_i t_i\right) = \sum_{i=1}^{n} r_i \varphi(t_i).$$

As E is a free module, its elements have unique sum representations, which ensures that Φ is well defined. It is also an R-module homomorphism, which can be checked using straightforward calculations, and $\Phi|_T = \varphi$ follows from the definition.

If $\Psi\colon E \to F$ is some other R-module homomorphism for which $\Psi|_T = \varphi$, then

$$\Psi\left(\sum_{i=1}^{n} r_i t_i\right) = \sum_{i=1}^{n} r_i \Psi(t_i) = \sum_{i=1}^{n} r_i \varphi(t_i) = \Phi\left(\sum_{i=1}^{n} r_i t_i\right),$$

which verifies the uniqueness. □

Definition 6.25. Let A and B be R-modules. Denote the free R-module on $A \times B$ (which exists by Proposition 6.23) by E, so

$$E = \bigoplus_{\substack{(a,b)\\ \in A\times B}} R(a,b).$$

Let F be the submodule of E which is generated by all the elements of the following types:

$$\begin{gathered}(a_1 + a_2, b) - (a_1, b) - (a_2, b),\\ (a, b_1 + b_2) - (a, b_1) - (a, b_2),\\ r(a,b) - (ra, b),\\ r(a,b) - (a, rb),\end{gathered}$$

where $r \in R$, $a, a_1, a_2 \in A$ and $b, b_1, b_2 \in B$. The quotient module E/F is called the *tensor product of the modules A and B*, and it is denoted by $A \otimes_R B$. The classes of elements (a,b) in the quotient are called *simple tensors* and they are denoted by $a \otimes b$.

Remark 6.26. The tensor product is an R-module by construction. As the free R-module on $A \times B$ consists of finite sums of terms $r(a,b)$, and taking the quotient forces the relation $r(a \otimes b) = ra \otimes b$, any element of $A \otimes_R B$ can be expressed as a finite sum of simple tensors. This expression might not be unique, which can be seen from the relation $(a_1 + a_2) \otimes b = a_1 \otimes b + a_2 \otimes b$. This property makes it difficult to show that maps defined on the tensor product are well defined; however, the next proposition provides a useful tool for this purpose.

Definition 6.27. Let A, B and E be R-modules. The map $\varphi\colon A \times B \to E$ is called *R-bilinear*, if it is R-linear in both components, that is,

$$\varphi(r_1 a_1 + r_2 a_2, b) = r_1 \varphi(a_1, b) + r_2 \varphi(a_2, b)$$

and

$$\varphi(a, r_1 b_1 + r_2 b_2) = r_1 \varphi(a, b_1) + r_2 \varphi(a, b_2)$$

for all $a, a_1, a_2 \in A$, $b, b_1, b_2 \in B$ and $r_1, r_2 \in R$.

Proposition 6.28. *Let A, B and E be R-modules. If $\varphi\colon A \times B \to E$ is R-bilinear, then the map $\Psi\colon A \otimes_R B \to E$ given by*

$$\Psi\left(\sum_{i=1}^{n} a_i \otimes b_i\right) = \sum_{i=1}^{n} \varphi(a_i, b_i),$$

is an R-module homomorphism.

PROOF.
Firstly, by Proposition 6.24, the map φ defines an R-module homomorphism Φ from the free module on $A \times B$ to E, and

$$\Phi\left(\sum_{i=1}^{n} r_i(a_i, b_i)\right) = \sum_{i=1}^{n} r_i \varphi(a_i, b_i),$$

especially $\Phi(a, b) = \varphi(a, b)$ for each $(a, b) \in A \times B$. Let F denote the submodule in the construction of the tensor product, so $A \otimes_R B$ is the quotient of the free module by F. Now the R-bilinearity of φ ensures that the generators of F belong to $\ker \Phi$, as

$$\Phi((a_1 + a_2, b) - (a_1, b) - (a_2, b)) = \varphi(a_1 + a_2, b) - \varphi(a_1, b) - \varphi(a_2, b) = 0$$

and

$$\Phi(r(a, b) - (ra, b)) = r\varphi(a, b) - \varphi(ra, b)$$

for all $a, a_1, a_2 \in A$, $b \in B$ and $r \in R$ (other generators similarly). As Φ is an R-module homomorphism, it follows that $F \subset \ker \Phi$. By Proposition 1.47, the map Φ induces an R-module homomorphism $\Psi\colon A \otimes_R B \to E$, where $\Psi(a \otimes b) = \Phi(a, b)$; note that simple tensors are classes of elements (a, b). As then

$$\Psi\left(\sum_{i=1}^{n} a_i \otimes b_i\right) = \sum_{i=1}^{n} \Phi(a_i, b_i) = \sum_{i=1}^{n} \varphi(a_i, b_i),$$

this map is the one in the claim. □

PROPOSITION 6.29 (Extension of scalars). *Let T be a commutative ring, $\varphi\colon R \to T$ a ring homomorphism and E an R-module. Then the tensor product $E \otimes_R T$ is a T-module.*

PROOF.
The homomorphism φ makes T into an R-module (look at example 1.41), so the tensor product $E \otimes_R T$ can be constructed and it is an R-module, particularly an abelian group. Let $t \in T$ and define an action of T on $E \otimes_R T$ by setting

$$t \cdot \left(\sum_{i \in A} e_i \otimes s_i\right) = \sum_{i \in A} e_i \otimes ts_i,$$

note that all the sums in this proof are finite. It needs to be shown that the action is well defined: that it does not depend on the representation of the element as simple tensors, which is not unique. It also needs to be shown that the action satisfies the properties required of a ring action; this, however, can be done using straightforward calculations which are left out of this proof.

Let F be the submodule of the free R-module on $E \times T$ in the construction of the tensor product (as in Definition 6.25). If $\sum_{i \in A} e_i \otimes s_i$ and $\sum_{j \in B} e_j \otimes s_j$ are two representations for the same element in $E \otimes_R T$, then $\sum_{i \in A}(e_i, s_i) - \sum_{j \in B}(e_j, s_j) \in F$. For the ring action to be well defined, it needs to be shown that

$$\sum_{i \in A} e_i \otimes ts_i = \sum_{j \in B} e_j \otimes ts_j$$

for every $t \in T$. This follows if $\sum_{i\in A}(e_i, ts_i) - \sum_{j\in B}(e_j, ts_j) \in F$. The elements of the free module, and thus the elements of F, are unique sums $\sum_{k\in D} r_k(e_k, s_k)$, where $r_k \in R$, $e_k \in E$ and $s_k \in T$. Therefore it is enough to prove the following:

Claim: If $\sum_{k\in D} r_k(e_k, s_k) \in F$ and $t \in T$, then $\sum_{k\in D} r_k(e_k, ts_k) \in F$. Firstly, this holds for all the generators, which are of the form

$$\begin{gathered}(e_1 + e_2, s) - (e_1, s) - (e_2, s),\\ (e, s_1 + s_2) - (e, s_1) - (e, s_2),\\ r(e, s) - (re, s),\\ r(e, s) - (e, rs),\end{gathered}$$

where $r \in R$, $e, e_1, e_2 \in E$ and $s, s_1, s_2 \in T$. If the second entries of any of these elements are multiplied by t, another generator is achieved; this follows from the distributivity and commutativity properties of the ring T. Now a general element of F can be expressed in terms of the generators, denoted by f_l:

$$\sum_{k\in D} r_k(e_k, s_k) = \sum_{l\in C} r_l f_l.$$

As the sum on the left-hand side is unique, the same pairs (e_k, s_k) appear also in the generators f_l. (On the right-hand side, there might be other pairs that cancel each other, but it does not make any difference.) Therefore multiplying the second entries by t gives a new set of generators, and thus $\sum_{k\in D} r_k(e_k, ts_k) \in F$. This completes the proof. □

6.4. Localization of Modules

The process of localizing modules is very similar to localization of rings that was discussed in Chapter 4. Localization of modules has also a connection with tensor products. This section follows [**Dummit**, section 15.4].

Let $S \subset R$ be a multiplicatively closed subset that contains 1_R. The relation on $E \times S$ given by

$$(e_1, s_1) \sim (e_2, s_2) \iff t(s_2e_1 - s_1e_2) = 0 \text{ for some } t \in S$$

is an equivalence relation. The equivalence class of (e, s) is denoted by $\frac{e}{s}$. Let $S^{-1}E$ denote the set of equivalence classes. The operation

$$\frac{e_1}{s_1} + \frac{e_2}{s_2} = \frac{s_2e_1 + s_1e_2}{s_1s_2}$$

is well defined and makes $S^{-1}E$ into an additive abelian group, and the ring action of $S^{-1}R$ given by

$$\frac{r}{t} \cdot \frac{e}{s} = \frac{re}{ts}$$

is also well defined and gives $S^{-1}E$ an $S^{-1}R$-module structure. The proofs for the above claims follow the same pattern as the proofs of the corresponding results for $S^{-1}R$ in Chapter 4. (The only major difference is that module elements must always be kept on the right-hand side in the calculations.)

DEFINITION 6.30. The $S^{-1}R$-module $S^{-1}E$ is called the *localization of E at S*. If $P \subset R$ is a prime ideal, the R_P-module $(R-P)^{-1}E$ is called the *localization of E at P*, and denoted by E_P.

REMARK 6.31. The ring homomorphisms $R \to S^{-1}R$ and $R \to R_P$ from Proposition 4.7 make $S^{-1}E$ and E_P also into R-modules; look at Example 1.41.

LEMMA 6.32. *Let E be a finitely generated R-module, and $P \subset R$ a prime ideal. Then $E_P = 0$ if and only if there exists an element $s \in R - P$ for which $sE = 0$.*

PROOF.
Assume that there exists $s \in R - P$ with $sE = 0$. Let $\frac{e}{t} \in E_P$. As the image of s is invertible in R_P,

$$\frac{e}{t} = \frac{se}{st} = \frac{0}{st} = 0_{E_P},$$

which implies that $E_P = \{0\}$.

Assume then that $E_P = 0$. As E is finitely generated, there exist generators $e_1, \ldots, e_k$. For any generator e_i, $\frac{e_i}{1} = \frac{0}{1}$, so there exists some $s_i \in R - P$ for which $s_i e_i = 0$. Now the element $s = \prod_{i=1}^{k} s_i \in R - P$ satisfies $sE = 0$:

Every element $e \in E$ can be written in terms of the generators: there exist $r_i \in R$ so that $e = r_1 e_1 + \cdots + r_k e_k$. Therefore

$$se = \left(\prod_{i=1}^{k} s_i \right) (r_1 e_1 + \cdots + r_k e_k) = 0.$$

□

REMARK 6.33. The annihilator of E is exactly $\operatorname{Ann}(E) = \{r \in R \colon rE = 0\}$ (and it is an ideal by Lemma 1.55). Therefore, the previous lemma implies that $E_P \neq 0$ if and only if $\operatorname{Ann}(E) \subset P$.

LEMMA 6.34. *Let $P \subset R$ be a prime ideal, E an R-module and A an index set. If E is generated by $\{e_i\}_{i \in A}$, then the R_P-module E_P is generated by $\{\frac{e_i}{1_R}\}_{i \in A}$. Especially, if E is finitely generated, then E_P is finitely generated.*

PROOF.
The proof is straightforward and very similar to the proof of the corresponding result for ideals, Proposition 4.13. □

PROPOSITION 6.35. *Let $P \subset R$ be a prime ideal, E an R-module and $F \subset E$ a submodule. Then $(E/F)_P \cong E_P/F_P$ as R_P-modules.*

PROOF.
Define $\varphi \colon (E/F)_P \to E_P/F_P$ by $\varphi\left(\frac{e+F}{q}\right) = \frac{e}{q} + F_P$. It first needs to be shown that φ is well defined. If $\frac{e_1+F}{q_1} = \frac{e_2+F}{q_2}$, then there exists $s \in R - P$ for which

$$s(q_2 e_1 - q_1 e_2) + F = s\left(q_2(e_1 + F) - q_1(e_2 + F)\right) = 0 + F,$$

so $s(q_2 e_1 - q_1 e_2) \in F$. Therefore

$$\frac{e_1}{q_1} - \frac{e_2}{q_2} = \frac{q_2 e_1 - q_1 e_2}{q_1 q_2} = \frac{s(q_2 e_1 - q_1 e_2)}{s q_1 q_2} \in F_P,$$

so

$$\varphi\left(\frac{e_1+F}{q_1}\right) = \frac{e_1}{q_1} + F_P = \frac{e_2}{q_2} + F_P = \varphi\left(\frac{e_2+F}{q_2}\right).$$

This shows that the value of φ does not depend of the module and ring elements chosen to represent the class.

The map is an R_P-module homomorphism, because for any $\frac{e_1+F}{q_1}, \frac{e_2+F}{q_2} \in (E/F)_P$,

$$\begin{aligned}\varphi\left(\frac{e_1+F}{q_1} + \frac{e_2+F}{q_2}\right) &= \varphi\left(\frac{q_2e_1+q_1e_2+F}{q_1q_2}\right)\\ &= \frac{q_2e_1+q_1e_2}{q_1q_2} + F_P\\ &= \left(\frac{e_1}{q_1}+F_P\right) + \left(\frac{e_2}{q_2}+F_P\right) = \varphi\left(\frac{e_1+F}{q_1}\right) + \varphi\left(\frac{e_2+F}{q_2}\right),\end{aligned}$$

and for any $\frac{r}{t} \in R_P$, $\frac{e+F}{q} \in (E/F)_P$,

$$\varphi\left(\frac{r}{t}\cdot\frac{e+F}{q}\right) = \varphi\left(\frac{re+F}{tq}\right) = \frac{re}{tq} + F_P = \frac{r}{t}\left(\frac{e}{q}+F_p\right) = \frac{r}{t}\cdot\varphi\left(\frac{e+F}{q}\right).$$

Surjectivity of φ is trivial. For the injectivity, if $\varphi\left(\frac{e_1+F}{q_1}\right) = \varphi\left(\frac{e_2+F}{q_2}\right)$, then

$$\frac{q_2e_1 - q_1e_2}{q_1q_2} \in F_P.$$

This means that $1_R(q_2e_1 - q_1e_2) \in F$, and as $1_R \in R - P$, it follows that $\frac{e_1+F}{q_1} = \frac{e_2+F}{q_2}$. Therefore φ is an R_P-module isomorphism. □

LEMMA 6.36. *Let E be an R-module and $P \subset R$ a prime ideal. Then $P^eE_P = (PE)_P$.*

PROOF.
It is a simple matter to check that both of these modules consist of finite sums of elements of the type

$$\frac{pe}{s},$$

where $p \in P$, $e \in E$ and $s \in R - P$. This verifies the equality. □

The last goal of this chapter is to establish a relation between the tensor product and localization of modules.

PROPOSITION 6.37. *Let E be an R-module and $S \subset R$ a multiplicatively closed subset with $1_R \in S$. Then $S^{-1}E \cong E \otimes_R S^{-1}R$ as $S^{-1}R$-modules.*

PROOF.
By Proposition 4.7, there exists a ring homomorphism $\pi\colon R \to S^{-1}R$, and thus by Proposition 6.29, the tensor product $E \otimes_R S^{-1}R$ is an $S^{-1}R$-module. Define $\varphi\colon S^{-1}E \to E \otimes_R S^{-1}R$ by setting

$$\varphi\left(\frac{e}{s}\right) = e \otimes \frac{1}{s}.$$

Firstly, the map φ is well defined. Assume that $\frac{e_1}{s_1} = \frac{e_2}{s_2}$. Then there exists $s \in S$ for which $s(s_2e_1 - s_1e_2) = 0$, so $ss_2e_1 = ss_1e_2$. Therefore

$$\varphi\left(\frac{e_1}{s_1}\right) = e_1 \otimes \frac{1}{s_1} = ss_2e_1 \otimes \frac{1}{ss_2s_1} = ss_1e_2 \otimes \frac{1}{ss_1s_2} = e_2 \otimes \frac{1}{s_2} = \varphi\left(\frac{e_2}{s_2}\right).$$

Secondly, φ is a homomorphism of $S^{-1}R$-modules, as

$$\begin{aligned}\varphi\left(\frac{e_1}{s_1} + \frac{e_2}{s_2}\right) &= \varphi\left(\frac{s_2e_1 + s_1e_2}{s_1s_2}\right) = (s_2e_1 + s_1e_2) \otimes \frac{1}{s_1s_2} \\ &= s_2e_1 \otimes \frac{1}{s_1s_2} + s_1e_2 \otimes \frac{1}{s_1s_2} = e_1 \otimes \frac{1}{s_1} + e_2 \otimes \frac{1}{s_2} \\ &= \varphi\left(\frac{e_1}{s_1}\right) + \varphi\left(\frac{e_2}{s_2}\right)\end{aligned}$$

for any $\frac{e_1}{s_1}, \frac{e_2}{s_2} \in S^{-1}E$, and

$$\varphi\left(\frac{r}{t} \cdot \frac{e}{s}\right) = re \otimes \frac{1}{ts} = \frac{r}{t}\left(e \otimes \frac{1}{s}\right) = \frac{r}{t} \cdot \varphi\left(\frac{e}{s}\right)$$

for any $\frac{r}{t} \in S^{-1}R$ and $\frac{e}{s} \in S^{-1}E$.

Thirdly, φ is surjective; as every element of $E \otimes_R S^{-1}R$ is a finite sum of simple tensors, and as φ is a homomorphism, it is enough to show that every simple tensor lies in the image of φ. So let $e \otimes \frac{r}{s} \in E \otimes_R S^{-1}R$. Then

$$\varphi\left(\frac{re}{s}\right) = re \otimes \frac{1}{s} = e \otimes \frac{r}{s}.$$

Lastly, the injectivity of φ follows, if the map can be proven to possess a well-defined inverse. If an inverse exists, it has to be $e \otimes \frac{r}{s} \mapsto \frac{re}{s}$ on simple tensors, as $e \otimes \frac{r}{s} = re \otimes \frac{1}{s}$. It remains to show that this map is well defined: this is done by showing that it is induced by an R-bilinear map on $E \times S^{-1}R$.

Define $\psi\colon E \times S^{-1}R \to S^{-1}E$ by setting $\psi(e, \frac{r}{s}) = \frac{re}{s}$. The map ψ is well defined: Assume that $(e_1, \frac{r_1}{s_1}) = (e_2, \frac{r_2}{s_2})$. Then $e_1 = e_2 = e$ and there exists $s \in S$ so that $s(s_2r_1 - s_1r_2) = 0$. It follows that

$$s(s_2r_1e - s_1r_2e) = s(s_2r_1 - s_1r_2)e = 0,$$

which implies that

$$\psi\left(e_1, \frac{r_1}{s_1}\right) = \frac{r_1e}{s_1} = \frac{r_2e}{s_2} = \psi\left(e_2, \frac{r_2}{s_2}\right).$$

The map ψ is also R-bilinear, as

$$\psi\left(t_1e_1 + t_2e_2, \frac{r}{s}\right) = \frac{r(t_1e_1 + t_2e_2)}{s} = t_1\frac{re_1}{s} + t_2\frac{re_2}{s} = t_1 \cdot \psi\left(e_1, \frac{r}{s}\right) + t_2 \cdot \psi\left(e_2, \frac{r}{s}\right)$$

and

$$\psi\left(e, t_1\frac{r_1}{s_1} + t_2\frac{r_2}{s_2}\right) = \psi\left(e, \frac{s_2t_1r_1 + s_1t_2r_2}{s_1s_2}\right) = \frac{(s_2t_1r_1 + s_1t_2r_2)e}{s_1s_2}$$
$$= t_1\frac{r_1e}{s_1} + t_2\frac{r_2e}{s_2} = t_1 \cdot \psi\left(e_1, \frac{r_1}{s_1}\right) + t_2 \cdot \psi\left(e_2, \frac{r_2}{s_2}\right).$$

As both $S^{-1}R$ and $S^{-1}E$ are R-modules, the map $\Psi\colon E \otimes_R S^{-1}R \to S^{-1}E$,

$$\Psi\left(\sum_{i=1}^{n} e_i \otimes \frac{r_i}{s_i}\right) = \sum_{i=1}^{n} \psi\left(e_i, \frac{r_i}{s_i}\right),$$

is an R-module homomorphism by Proposition 6.28, and $\Psi = \varphi^{-1}$, as these maps agree on simple tensors. Hence the inverse is well defined, which completes the proof. □

COROLLARY 6.38. *Let E be an R-module and $P \subset R$ a prime ideal. Then $E_P \cong E \otimes_R R_P$ as R_P-modules.*

CHAPTER 7

Upper Bound: A Result for Noetherian Rings

This chapter provides an upper bound for the minimal number of generators for a module, and thus for an ideal. It is based on the article of [**Forster**]. The results use the localization E_P for a prime ideal P, as in Definition 6.30. In the original article, the tensor product $E \otimes_R R_P$ is used instead of the localization E_P. These are isomorphic as R_P-modules by Corollary 6.38.

Let E be an R-module, and $P \subset R$ a prime ideal. Consider the ideal $P^e \subset R_P$ and the R_P-module E_P. Their product $P^e E_P$ is an R_P-submodule of E_P by Lemma 1.51, and $E_P/P^e E_P$ is an R_P/P^e-module by Lemma 1.53. As P^e is a maximal ideal by Proposition 4.16, R_P/P^e is a field by Proposition 1.22. Thus the module is actually a vector space. In the remainder of this chapter, denote

$$L_P(E) = E_P/P^e E_P \text{ and } K_P(R) = R_P/P^e,$$

so $L_P(E)$ is a $K_P(R)$-vector space. Let $\beta_P \colon R \to K_P(R)$ and $\lambda_P \colon E \to L_P(E)$ be the natural maps given by $\beta_P(r) = \frac{r}{1} + P^e$, $\lambda_P(e) = \frac{e}{1} + P^e E_P$. The map β_P is a ring homomorphism, as it is the composition of the map $\pi \colon R \to R_P$ and the map from R_P to the quotient $K_P(R)$, which are both homomorphisms. The following lemma states some other properties:

LEMMA 7.1. *For the maps β_P and λ_P defined above, the following properties hold:*

(i) $\beta_P(r) = 0$ *if and only if* $r \in P$
(ii) $\lambda_P(e_1 + e_2) = \lambda_P(e_1) + \lambda_P(e_2)$ *for all* $e_1, e_2 \in E$
(iii) $\lambda_P(re) = \beta_P(r)\lambda_P(e)$ *for all* $r \in R$, $e \in E$.

PROOF.

(i) The condition $\beta_P(r) = 0$ is equivalent to $\frac{r}{1} \in P^e$, which is equivalent to $r \in P$ (look at Lemma 4.10)
(ii) $\lambda_P(e_1 + e_2) = \frac{e_1+e_2}{1} + P^e E_P = \frac{e_1}{1} + P^e E_P + \frac{e_2}{1} + P^e E_P = \lambda_P(e_1) + \lambda_P(e_2)$
(iii) $\lambda_P(re) = \frac{re}{1} + P^e E_P = \left(\frac{r}{1} + P^e\right)\left(\frac{e}{1} + P^e E_P\right) = \beta_P(r)\lambda_P(e)$. □

REMARK 7.2. The parts (ii) and (iii) of Lemma 7.1 may resemble the properties required of a homomorphism, and indeed, λ_P is an R-module homomorphism. By Remark 6.31, E_P is an R-module, so PE_P is its submodule. It can be easily verified that $PE_P = P^e E_P$, and therefore $L_P(E) = E_P/PE_P$ is also an R-module.

LEMMA 7.3. *Let E be an R-module and $P_1, \ldots, P_k \in \operatorname{Spec} R$ with $L_{P_i}(E) \neq 0$ for all $i = 1, \ldots, k$. Then there exists $e \in E$ for which $\lambda_{P_i}(e) \neq 0$ for all $i = 1, \ldots, k$.*

PROOF.
Assuming that the ideals P_i are distinct does not change the situation. After a possible

relabeling of the ideals, it can thus be assumed that $P_i \not\subset P_j$ when $i < j$. The proof is an induction on the number k of prime ideals.

Case $k = 1$: let $P \in \operatorname{Spec} R$ with $L_P(E) \neq 0$. Assume on the contrary that $\lambda_P(e) = 0$ for all $e \in E$, so $\frac{e}{1} \in P^e E_P$ for all $e \in E$. Let $\frac{e}{s} \in E_P$. Now

$$\frac{e}{s} = \frac{1}{s} \cdot \frac{e}{1} \in P^e E_P,$$

because $P^e E_P$ is an R_P-submodule of E_P. Therefore $E_P = P^e E_P$, which implies that $L_P(E) = 0$, but this is a contradiction. Thus $\lambda_P(e) \neq 0$ for some $e \in E$.

Assume then that the claim holds for $k-1$ prime ideals. Therefore an element $e_1 \in E$ can be found so that $\lambda_{P_i}(e_1) \neq 0$ for all $i = 1, \ldots, k-1$. If also $\lambda_{P_k}(e_1) \neq 0$, then the choice $e = e_1$ gives the desired element, so it can be assumed that $\lambda_{P_k}(e_1) = 0$. Then it is enough to find $e_2 \in E$ for which $\lambda_{P_k}(e_2) \neq 0$ and $\lambda_{P_i}(e_2) = 0$ for all $i < k$, and then choose $e = e_1 + e_2$. This follows from the fact given by Lemma 7.1 (ii): $\lambda_{P_i}(e) = \lambda_{P_i}(e_1) + \lambda_{P_i}(e_2)$. In this sum exactly one of the terms will be nonzero for any $i = 1, \ldots, k$.

As $P_i \not\subset P_k$ when $i < k$, there exist elements $a_i \in P_i - P_k$ for each $i = 1, \ldots, k-1$. By Lemma 7.1 (i), $\beta_{P_k}(a_i) \neq 0$ and $\beta_{P_i}(a_i) = 0$ for all $i = 1, \ldots, k-1$. Let $a = \prod_{i=1}^{k-1} a_i$. As P_k is a prime ideal, $a \notin P_k$. Therefore $a \in \left(\bigcup_{i=1}^{k-1} P_i\right) - P_k$, so $\beta_{P_k}(a) \neq 0$, and $\beta_{P_i}(a) = 0$ for all $i = 1, \ldots, k-1$. As $L_{P_k}(E) \neq 0$, by case $k = 1$ there exists $e' \in E$ for which $\lambda_{P_k}(e') \neq 0$. It remains to prove that the element $e_2 = ae'$ has the desired properties. For all $i = 1, \ldots, k-1$,

$$\lambda_{P_i}(e_2) = \beta_{P_i}(a)\lambda_{P_i}(e') = 0 \cdot \lambda_{P_i}(e') = 0$$

by Lemma 7.1 (iii). Furthermore, if $\lambda_{P_k}(e_2) = 0$, then the element $\frac{ae'}{1}$ belongs to $P_k^e E_{P_k}$, which is an R_P-submodule of E_{P_k}. As a is an invertible element in R_P, it follows that

$$\frac{e'}{1} = \frac{1}{a} \cdot \frac{ae'}{1} \in P_k^e E_{P_k},$$

and therefore $\lambda_{P_k}(e') = 0$, which is a contradiction. Thus $\lambda_{P_k}(e_2) \neq 0$, and the proof is complete. □

PROPOSITION 7.4. *Let E be a finitely generated R-module. Then $L_P(E) = 0$ if and only if $E_P = 0$.*

PROOF.
As E is finitely generated, E_P is a finitely generated R_P-module by Lemma 6.34. Assume that $L_P(E) = 0$. As $L_P(E) = E_P/P^e E_P$, this implies that $E_P = P^e E_P$. As P^e is the unique maximal ideal of the local ring R_P by Proposition 4.16, $P^e = \operatorname{rad}(R_P)$. Therefore Nakayama's lemma (Proposition 3.4) implies that $E_P = 0$. The other direction is trivial. □

LEMMA 7.5. *Let $P \subset R$ be a prime ideal, and E a finitely generated R-module, which has a generating set of k elements. Denote the minimal number of generators for the R_P-module E_P by μ. Then*

$$\dim L_P(E) = \mu \leq k.$$

PROOF.
By Lemma 6.34, also E_P can be generated by k elements. This gives $\mu \leq k$. Now E_P is a finitely generated module over the local ring (R_P, P^e), so $\dim L_P(E) = \mu$ by Theorem 3.6, when $\mu \geq 1$. The case $\mu = 0$ follows from Proposition 7.4. □

PROPOSITION 7.6. *Let E be a finitely generated R-module. Then the sets*

$$X_k(E) = \{P \in \operatorname{Spec} R \colon \dim L_P(E) \geq k\}$$

are closed subsets of $\operatorname{Spec} R$ *for all* $k \in \mathbb{N}$.

PROOF.
As $X_0(E) = \operatorname{Spec} R$, it is closed. Now $\dim L_P(E) \geq 1$ if and only if $L_P(E) \neq 0$, which is equivalent to $E_P \neq 0$ by Proposition 7.4. This is equivalent to $\operatorname{Ann}(E) \subset P$ by Remark 6.33. Therefore

$$\begin{aligned} X_1(E) =& \{P \in \operatorname{Spec} R \colon \dim L_P(E) \geq 1\} \\ =& \{P \in \operatorname{Spec} R \colon P \supset \operatorname{Ann}(E)\} \\ =& V(\operatorname{Ann}(E)). \end{aligned}$$

As the annihilator $\operatorname{Ann}(E)$ is an ideal by Lemma 1.55, this proves that also $X_1(E)$ is closed.

Let $k > 1$. The goal is to find a collection of finitely generated R-modules E_i so that $X_k(E) = \bigcap_i X_1(E_i)$. The rest of this proof makes use of the following notation: when $A_j \subset E$ is a subset of $k-1$ elements, set $F_j = RA_j$, which is a submodule of E. Now Proposition 6.35 gives

$$(E/F_j)_P \cong E_P/(F_j)_P. \tag{5}$$

By Lemma 7.5, the minimal number of generators for the R_P-module E_P is the same as $\dim L_P(E)$. If $\dim L_P(E) < k$, then E_P can be generated by $k-1$ elements $\frac{a_i}{q_i} \in E_P$, so

$$E_P = \sum_{i=1}^{k-1} R_P \frac{a_i}{q_i} = \left(\sum_{i=1}^{k-1} Ra_i \right)_P,$$

where the equality of the two sets is given by straightforward comparison of elements. For the subset $A_0 = \{a_1, \ldots, a_{k-1}\} \subset E$ and the corresponding submodule

$$F_0 = RA_0 = \sum_{i=1}^{k-1} Ra_i,$$

the isomorphism (5) gives $(E/F_0)_P = 0$, as in this case $E_P = (F_0)_P$. By Proposition 7.4, it then follows that $L_P(E/F_0) = 0$, so $P \notin X_1(E/F_0)$.

On the other hand, if $\dim L_P(E) \geq k$, no subset of $k-1$ elements generates E_P, so for any subset A_j of $k-1$ elements and the corresponding submodule F_j, the submodule $(F_j)_P \subset E_P$ is proper. Therefore the isomorphism (5) implies that $(E/F_j)_P \neq 0$, so $L_P(E/F_j) \neq 0$, and thus $P \in X_1(E/F_j)$. From these two cases it follows that

$$X_k(E) = \bigcap X_1(E/F_j),$$

where the intersection is taken over all possible subsets A_j and the corresponding submodules F_j. The sets $X_1(E/F_j)$ are closed by the first part of the proof, as the modules E/F_j are finitely generated; this follows from the fact that E is finitely generated. As an intersection of (possibly infinitely many) closed sets, $X_k(E)$ is therefore closed. □

COROLLARY 7.7. *Let E be a finitely generated R-module and $P, Q \in \operatorname{Spec} R$. If $P \subset Q$, then $\dim L_P(E) \leq \dim L_Q(E)$.*

PROOF.
Denote $k = \dim L_P(E)$, so $P \in X_k(E)$. As $X_k(E)$ is closed, there exists an ideal $I \subset R$ so that $X_k(E) = V(I)$. Therefore $I \subset P \subset Q$, so also $Q \in X_k(E)$. It follows that $\dim L_Q(E) \geq k = \dim L_P(E)$. □

LEMMA 7.8. *Let $P \subset R$ be a prime ideal, E an R-module and $e \in E$. Then*

$$L_P(E/Re) \cong L_P(E)/K_P(R)\lambda_P(e)$$

as $K_P(R)$-vector spaces.

PROOF.
By definition, $L_P(E/Re) = (E/Re)_P/P^e(E/Re)_P$, and $L_P(E) = E_P/P^eE_P$. Both of these are R_P-modules as well as $K_P(R)$-vector spaces. The set $K_P(R)\lambda_P(e)$, which is a subspace of the vector space $L_P(E)$, has the form

$$\begin{aligned} K_P(R)\lambda_P(e) &= \left\{ \left(\frac{r}{t} + P^e\right)\left(\frac{e}{1} + P^eE_P\right) : r \in R, t \in R - P \right\} \\ &= \left\{ \frac{re}{t} + P^eE_P \colon r \in R, t \in R - P \right\}. \end{aligned}$$

This proof makes frequent use of Lemma 6.36, which states that $P^eE_P = (PE)_P$ whenever E is an R-module and $P \subset R$ a prime ideal.

The goal is to find a surjective R_P-module homomorphism the kernel of which is $P^e(E/Re)_P$, and then use the first isomorphism theorem to establish the isomorphism. Define $\varphi \colon (E/Re)_P \to L_P(E)/K_P(R)\lambda_P(e)$,

$$\varphi\left(\frac{a + Re}{s}\right) = \left(\frac{a}{s} + P^eE_P\right) + K_P(R)\lambda_P(e).$$

Firstly, φ is well defined: if

$$\frac{a_1 + Re}{s_1} = \frac{a_2 + Re}{s_2},$$

then there exists $t \in R - P$ for which

$$t(s_2a_1 - s_1a_2) + Re = t[s_2(a_1 + Re) - s_1(a_2 + Re)] = 0 + Re.$$

Then $t(s_2a_1 - s_1a_2) \in Re$, so $t(s_2a_1 - s_1a_2) = re$ for some $r \in R$. Therefore

$$\frac{a_1}{s_1} - \frac{a_2}{s_2} = \frac{s_2a_1 - s_1a_2}{s_1s_2} = \frac{t(s_2a_1 - s_1a_2)}{ts_1s_2} = \frac{re}{ts_1s_2},$$

so

$$\left(\frac{a_1}{s_1} + P^eE_P\right) - \left(\frac{a_2}{s_2} + P^eE_P\right) = \left(\frac{a_1}{s_1} - \frac{a_2}{s_2}\right) + P^eE_P = \frac{re}{ts_1s_2} + P^eE_P \in K_P(R)\lambda_P(e).$$

It thus follows that

$$\begin{aligned}\varphi\left(\frac{a_1+Re}{s_1}\right) &= \left(\frac{a_1}{s_1}+P^eE_P\right)+K_P(R)\lambda_P(e)\\ &= \left(\frac{a_2}{s_2}+P^eE_P\right)+K_P(R)\lambda_P(e) = \varphi\left(\frac{a_2+Re}{s_2}\right).\end{aligned}$$

Secondly, φ is an R_P-module homomorphism, as

$$\begin{aligned}\varphi\left(\frac{a_1+Re}{s_1}+\frac{a_2+Re}{s_2}\right) =& \varphi\left(\frac{(s_2a_1+s_1a_2)+Re}{s_1s_2}\right)\\ =& \left(\frac{s_2a_1+s_1a_2}{s_1s_2}+P^eE_P\right)+K_P(R)\lambda_P(e)\\ =& \left(\left(\frac{a_1}{s_1}+P^eE_P\right)+\left(\frac{a_2}{s_2}+P^eE_P\right)\right)+K_P(R)\lambda_P(e)\\ =& \varphi\left(\frac{a_1+Re}{s_1}\right)+\varphi\left(\frac{a_2+Re}{s_2}\right)\end{aligned}$$

for $\frac{a_1+Re}{s_1}, \frac{a_2+Re}{s_2} \in (E/Re)_P$, and

$$\begin{aligned}\varphi\left(\frac{r}{t}\cdot\frac{a+Re}{s}\right) =& \varphi\left(\frac{ra+Re}{ts}\right)\\ =& \left(\frac{ra}{ts}+P^eE_P\right)+K_P(R)\lambda_P(e)\\ =& \left(\frac{r}{t}\cdot\left(\frac{a}{s}+P^eE_P\right)\right)+K_P(R)\lambda_P(e)\\ =& \frac{r}{t}\cdot\left(\left(\frac{a}{s}+P^eE_P\right)+K_P(R)\lambda_P(e)\right)\\ =& \frac{r}{t}\cdot\varphi\left(\frac{a+Re}{s}\right)\end{aligned}$$

for $\frac{r}{t} \in R_P$ and $\frac{a+Re}{s} \in (E/Re)_P$.

Thirdly, $\ker\varphi = P^e(E/Re)_P$: Let first $\frac{a+Re}{s} \in P^e(E/Re)_P$. The equality

$$P^e(E/Re)_P = (P(E/Re))_P$$

then implies that $a+Re \in P(E/Re)$. The elements of $P(E/Re)$ have the form

$$\sum_{i=1}^{n} p_i(e_i+Re) = \left(\sum_{i=1}^{n} p_ie_i\right)+Re,$$

where $p_i \in P$ and $e_i \in E$. Thus it follows that $a \in PE$, so $\frac{a}{s} \in (PE)_P = P^eE_P$. Therefore

$$\varphi\left(\frac{a+Re}{s}\right) = \left(\frac{a}{s}+P^eE_P\right)+K_P(R)\lambda_P(e) = \left(\frac{0}{1}+P^eE_P\right)+K_P(R)\lambda_P(e),$$

so $P^e(E/Re)_P \subset \ker\varphi$.

Let then $\frac{a+Re}{s} \in \ker\varphi$. Then $\frac{a}{s}+P^eE_P \in K_P(R)\lambda_P(e)$, so

$$\frac{a}{s}+P^eE_P = \frac{re}{t}++P^eE_P$$

for some $r \in R$, $t \in R - P$. Then

$$\frac{ta - sre}{st} = \frac{a}{s} - \frac{re}{t} \in P^e E_P = (PE)_P,$$

so $ta - sre \in PE$. This implies that $ta - sre = \sum_{i=1}^{n} p_i e_i$ for some $p_i \in P$, $e_i \in E$ and $n \in \mathbb{Z}_+$. Thus

$$ta + Re = \left(\sum_{i=1}^{n} p_i e_i \right) + Re = \sum_{i=1}^{n} p_i (e_i + Re) \in P(E/Re).$$

Now

$$\frac{a + Re}{s} = \frac{ta + Re}{ts} \in (P(E/Re))_P = P^e (E/Re)_P,$$

from which the other inclusion $\ker \varphi \subset P^e (E/Re)_P$ follows.

Lastly, surjectivity of φ is trivial, so it has been shown that φ is a surjective R_P-module homomorphism and its kernel is $P^e (E/Re)_P$. Thus the R_P-module isomorphism

$$L_P(E/Re) \cong L_P(E)/K_P(R)\lambda_P(e)$$

follows from the first isomorphism theorem (Proposition 1.48). Now this isomorphism is given by the map $\psi \colon L_P(E/Re) \to L_P(E)/K_P(R)\lambda_P(e)$,

$$\psi \left(\frac{a + Re}{s} + P^e (E/Re)_P \right) = \left(\frac{a}{s} + P^e E_P \right) + K_P(R)\lambda_P(e),$$

so for this to be an isomorphism of $K_P(R)$-vector spaces, it only needs to be shown that ψ is $K_P(R)$-linear. This is indeed true: for any $\frac{r}{t} \in R_P$ and $\frac{a+Re}{s} \in (E/Re)_P$

$$\begin{aligned}
&\psi \left(\left(\frac{r}{t} + P^e \right) \cdot \left(\frac{a + Re}{s} + P^e (E/Re)_P \right) \right) \\
=&\psi \left(\frac{ra + Re}{ts} + P^e (E/Re)_P \right) \\
=&\left(\frac{ra}{ts} + P^e E_P \right) + K_P(R)\lambda_P(e) \\
=&\left(\left(\frac{r}{t} + P^e \right) \left(\frac{a}{s} + P^e E_P \right) \right) + K_P(R)\lambda_P(e) \\
=&\left(\frac{r}{t} + P^e \right) \left(\left(\frac{a}{s} + P^e E_P \right) + K_P(R)\lambda_P(e) \right) \\
=&\left(\frac{r}{t} + P^e \right) \cdot \psi \left(\frac{a + Re}{s} + P^e (E/Re)_P \right).
\end{aligned}$$

This completes the proof. □

THEOREM 7.9. *Assume that R is a Noetherian ring and let E be a finitely generated R-module. Define for each $P \in \operatorname{Spec} R$*

$$b_P(E) = \begin{cases} \dim P + \dim L_P(E), \text{ if } L_P(E) \neq 0, \\ 0, \text{ if } L_P(E) = 0. \end{cases}$$

Let

$$b(E) = \sup_{P \in \operatorname{Spec} R} b_P(E).$$

Then E can be generated by a set of at most $b(E)$ elements.

PROOF.
The proof is an induction on $b(E)$. If $b(E) = 0$, then $L_P(E) = 0$ for every $P \in \operatorname{Spec} R$: otherwise some prime ideal P would give $b_P(E) \geq 1$. Therefore $X_1(E) = \emptyset$, and $X_1(E) = V(\operatorname{Ann}(E))$ by the proof of Proposition 7.6. The annihilator $\operatorname{Ann}(E)$ is an ideal of R by Lemma 1.55. If it is a proper ideal, Theorem 1.24 implies that it is contained in some maximal and thus prime ideal M. But in this case $M \in V(\operatorname{Ann}(E))$, which is not possible, as this set was proven to be empty. Therefore $\operatorname{Ann}(E) = R$, so $e = 1_R \cdot e = 0$ for every $e \in E$. It follows that E is the zero module, which is generated by zero elements.

Assume then that $b(E) > 0$, and that the claim has been proven for all finitely generated R-modules F with $b(F) \leq b(E) - 1$. As E is finitely generated, it has a generating set with m elements for some $m \in \mathbb{N}$. By Lemma 7.5, $\dim L_P(E) \leq m$ for each $P \in \operatorname{Spec} R$, so $X_t(E) = \emptyset$ for all $t > m$. On the other hand, $X_1(E) \neq \emptyset$: if this does not hold, then $L_P(E) = 0$ for each $P \in \operatorname{Spec} R$, and thus $b(E) = 0$. Therefore there exists index $j \leq m$ for which $X_j(E) \neq \emptyset$ and $X_t(E) = \emptyset$ for all $t > j$.

Let now $k \in \{1, \ldots, j\}$. Then the inclusion $X_k(E) \supset X_j(E)$ implies that $X_k(E)$ is nonempty. As $X_k(E)$ is closed by Proposition 7.6, there exists an ideal $I_k \subset R$ so that $X_k(E) = V(I_k)$. As $V(I_k) = V(\sqrt{I_k})$ by Lemma 6.11, and the radical of an ideal is a radical ideal by Lemma 6.2, it can be assumed that I_k is a radical ideal. If $I_k = R$, then $X_k(E) = \emptyset$, so the ideal I_k is a proper ideal, and thus a finite intersection of prime ideals by Proposition 6.7. Therefore there exist prime ideals P_{ki}, $i = 1, \ldots, l_k$, for which $I_k = P_{k1} \cap \cdots \cap P_{kl_k}$, and thus

$$X_k(E) = V(I_k) = V(P_{k1} \cap \cdots \cap P_{kl_k}).$$

Lemma 7.3 gives $e \in E$ for which $\lambda_{P_{ki}}(e) \neq 0$ for all k and i. The next step is to prove that $b(E/Re) < b(E)$. By Lemma 7.8,

$$L_P(E/Re) \cong L_P(E)/K_P(R)\lambda_P(e), \tag{6}$$

so $\dim L_P(E/Re) \leq \dim L_P(E)$. The isomorphism (6) also implies that if $L_P(E) = 0$, also $L_P(E/Re) = 0$, so it is enough to show that $b_P(E/Re) < b(E)$ for all P for which $L_P(E) \neq 0$.

Let $P \in \operatorname{Spec} R$ with $\dim L_P(E) = k > 0$, so $k \in \{1, \ldots, j\}$. Then $P \in X_k(E)$, so $P \supset P_{k1} \cap \cdots \cap P_{kl_k}$. Now $P_{ki} \subset P$ for some i: if this does not hold, then for each i there exist elements $a_{ki} \in P_{ki}$ with $a_{ki} \notin P$. Then the element $\prod_{i=1}^{l_k} a_{ki}$ belongs to each P_{ki}, and therefore also to the intersection and thus to P. As P is a prime ideal, $a_{ki} \in P$ for some i, which is a contradiction. Therefore $P_{ki} \subset P$ for some i, and it can be seen from the definition of Krull dimension that $\dim P \leq \dim P_{ki}$.

If $P_{ki} = P$, then $\lambda_P(e) \neq 0$ and thus $K_P(R)\lambda_P(e)$ is a nonzero subspace of $L_P(E)$. In this case the isomorphism (6) implies that $\dim L_P(E/Re) = \dim L_P(E) - 1$. If instead $P_{ki} \subsetneq P$, then $\dim P < \dim P_{ki}$ by definition of Krull dimension. The obvious inclusion $P_{ki} \supset P_{k1} \cap \cdots \cap P_{kl_k} = I_k$ implies that $P_{ki} \in V(I_k) = X_k(E)$. Therefore $\dim L_{P_{ki}}(E) \geq k$, so

$$\dim L_P(E/Re) \leq \dim L_P(E) = k \leq \dim L_{P_{ki}}(E).$$

Both alternatives thus lead to

$$\dim P + \dim L_P(E/Re) < \dim P_{ki} + \dim L_{P_{ki}}(E) \leq b(E).$$

Therefore $b(E/Re) < b(E)$, so $b(E/Re) \leq b(E) - 1$. As E/Re is a finitely generated R-module, it has a generating set of at most $b(E)-1$ elements by induction hypothesis. Therefore there exist elements $a_i \in E$, $i = 1, \ldots, n \leq b(E) - 1$ so that for any $a \in E$

$$a + Re = \sum_{i=1}^{n}(a_i + Re) = \left(\sum_{i=1}^{n} a_i\right) + Re.$$

This implies that $a = (\sum_{i=1}^{n} a_i) + re$ for some $r \in R$, so especially E can be generated by a set of at most $b(E)$ elements. □

The result of Theorem 7.9 can be applied to an ideal $E = I$ of a Noetherian ring R, as ideals are also modules. In this case, $L_P(I) = I^e/P^eI^e$ is an R_P/P^e-vector space, the dimension of which needs to be found for each prime ideal $P \subset R$ in order to find $b(I)$.

Remark 7.10. If $b(E) = \infty$, the theorem does not offer any information. However, if R has finite Krull dimension, then $b(E) < \infty$: Let k be the minimal number of generators for E. By Lemma 7.5, $\dim L_p(E)$ is bounded from above by k. Therefore

$$\begin{aligned} b(E) &= \sup_{P \in \operatorname{Spec} R} b_P(E) \\ &\leq \sup_{P \in \operatorname{Spec} R} (\dim P + \dim L_p(E)) \\ &\leq \sup_{P \in \operatorname{Spec} R} \dim P + \sup_{P \in \operatorname{Spec} R} \dim L_p(E) \\ &\leq \dim R + k < \infty. \end{aligned}$$

Example 7.11. This example shows that the assumption "finitely generated" is crucial in Proposition 7.6 and Theorem 7.9. It shows that if a module E is not finitely generated, it is possible that some sets $X_k(E)$ are not closed, and that the number $b(E)$ can be finite even though E does not have a finite generating set. Let $R = \mathbb{C}[x]$ be the polynomial ring in one variable over the complex numbers. The prime ideals of R are

$$P_z = (x - z) \text{ for } z \in \mathbb{C} \text{ and } P_\infty = (0).$$

Firstly, the ideals of the first type are prime ideals by the results in Chapter 1 (see Proposition 1.31 and Corollary 1.36), and the zero ideal is a prime ideal because R is an integral domain. Assume then that $P \subset R$ is a prime ideal. As R is a principal ideal domain (look at Example 1.12), $P = (p)$ for some $p \in R$. The case $p = 0$ is the only one when the degree of p is not defined, and it gives the ideal P_∞. Now if $\deg p = 0$, then $p \in \mathbb{C} - \{0\}$, so p is a unit and thus $P = R$, which is not possible. On the other hand, if $\deg p \geq 2$, then p can be factored into linear factors, but P does not have any elements of degree 1: this implies that P cannot be a prime ideal. Therefore the only prime ideals are the ones mentioned above, and thus $\operatorname{Spec} R$ can be identified with $\mathbb{C} \cup \{\infty\}$.

The closed sets of $\operatorname{Spec} R$ are finite subsets and $\operatorname{Spec} R$ itself: Assume that $D \subset \operatorname{Spec} R$ is a closed set, so $D = V(I)$ for some ideal $I \subset R$. If $I = (0)$, then $D = \operatorname{Spec} R$,

and if $I = R$, then $D = \emptyset$. Assume then that I is a proper nonzero ideal. As R is a principal ideal domain, $I = (f)$ for some nonzero polynomial $f \in R$. Now $\deg f = k \geq 1$, otherwise $I = (0)$ or $I = R$. The polynomial f can be factored: there exist $a, z_i \in \mathbb{C}$, $a \neq 0$, for which $f = \prod_{i=1}^{k} a(x - z_i)$. If $P \in D$, then $P \supset I$ so especially $f \in P$. As P is a prime ideal, $x - z_i \in P$ for some i, and therefore $(x - z_i) \subset P$. As R is a principal ideal domain, all nonzero P_z are maximal ideals by Lemma 1.21, so it follows that $P = (x - z_i)$. In this case $D = \{P_z \colon f(z) = 0\}$ is a finite set.

For each $n \in \mathbb{Z}$, let $E_n = (\mathbb{C}, +)$ with the R-module structure given by the ring action $f \cdot c = f(n)c$: the evaluation homomorphism $R \to \mathbb{C}$, $f \mapsto f(n)$ makes (the $\mathbb{C}$-module) $\mathbb{C}$ into an R-module (see Example 1.41). Let then $E = \bigoplus_{n\in\mathbb{Z}} E_n$. All modules E_n are nonzero, so as a countably infinite direct sum, E is not finitely generated. The elements of E are sequences $(c_n)_{n\in\mathbb{Z}}$, where each $c_n \in E_n$, and only finitely many terms are nonzero. For each $n \in \mathbb{Z}$, let $\varepsilon(n)$ denote the sequence where

$$\varepsilon(n)_i = \begin{cases} 1, \text{ if } i = n, \\ 0, \text{ if } i \neq n. \end{cases}$$

Then E is generated by $\{\varepsilon(n) \colon n \in \mathbb{Z}\}$, because for constant polynomials c_n,

$$(c_n)_{n\in\mathbb{Z}} = \sum_{n\in\mathbb{Z}} c_n \cdot \varepsilon(n).$$

First claim: Let E_{P_z} be the localization of E at the prime ideal P_z. Then $E_{P_z} = 0$ for $z \notin \mathbb{Z}$, and $E_{P_z} \cong E_z$ for $z \in \mathbb{Z}$.

Verification of the first claim needs the following lemma: Let $n \in \mathbb{Z}$. If the polynomial $h_n = x - n \in R - P_z$, then in E_{P_z}

$$\frac{\varepsilon(n)}{1} = \frac{(0)_{n\in\mathbb{Z}}}{1}.$$

Proof of the lemma: as

$$\big(h_n \cdot \big(\varepsilon(n) - (0)_{n\in\mathbb{Z}}\big)\big)_n = (h_n \cdot \varepsilon(n))_n = h_n(n) = 0,$$

the sequence $(h_n \cdot \varepsilon(n))_{n\in\mathbb{Z}}$ is the zero sequence $(0)_{n\in\mathbb{Z}}$. The claim of the lemma thus follows from the definition of localization.

Let first $z \notin \mathbb{Z}$. Then the prime ideal P_z is either $(x - z)$ for some $z \in \mathbb{C} - \mathbb{Z}$, or the zero ideal. In either case, $h_n \in R - P_z$ for all $n \in \mathbb{Z}$: note that as P_z is a prime ideal, it cannot contain polynomials $x - z_1$ and $x - z_2$ where $z_1 \neq z_2$. By the lemma above, $\frac{\varepsilon(n)}{1} = \frac{(0)_{n\in\mathbb{Z}}}{1}$ for all n. By Lemma 6.34, the elements $\frac{\varepsilon(n)}{1}$ generate E_{P_z}, so the localization is the zero module.

Let then $z \in \mathbb{Z}$. Define $\varphi \colon E_{P_z} \to E_z$ by

$$\varphi\left(\frac{(c_n)_{n\in\mathbb{Z}}}{g}\right) = \frac{c_z}{g(z)},$$

so the value of φ depends only on the element indexed by z. (The division on the right-hand side is the customary division of $\mathbb{C}$.) Firstly, φ is well defined: if

$$\frac{(c_n)_{n\in\mathbb{Z}}}{g} = \frac{(d_n)_{n\in\mathbb{Z}}}{f},$$

then there exists $h \in R - P_z$ for which

$$(h(n)\,[f(n)c_n - g(n)d_n])_{n\in\mathbb{Z}} = h \cdot (f \cdot (c_n)_{n\in\mathbb{Z}} - g \cdot (d_n)_{n\in\mathbb{Z}}) = (0)_{n\in\mathbb{Z}}.$$

Especially $h(z)\,(f(z)c_z - g(z)d_z) = 0$. Now $h \in R - P_z$, so $h(z) \neq 0$. Therefore $f(z)c_z - g(z)d_z = 0$, so it follows that

$$\varphi\left(\frac{(c_n)_{n\in\mathbb{Z}}}{g}\right) = \frac{c_z}{g(z)} = \frac{d_z}{f(z)} = \varphi\left(\frac{(d_n)_{n\in\mathbb{Z}}}{f}\right).$$

The map φ is surjective, as $\varphi\left(\frac{(c)_{n\in\mathbb{Z}}}{1}\right) = c$ for any $c \in E_z$. Injectivity can be verified by looking at the kernel: Assume that $\varphi\left(\frac{(c_n)_{n\in\mathbb{Z}}}{g}\right) = 0$. Then $\frac{c_z}{g(z)} = 0$, so $c_z = 0$. As $h_n \in R - P_z$ for all $n \neq z$, the above lemma implies that $\frac{\varepsilon(n)}{1} = \frac{(0)_{n\in\mathbb{Z}}}{1}$ for all $n \neq z$, and therefore

$$\frac{(c_n)_{n\in\mathbb{Z}}}{g} = \frac{\sum_{n\in\mathbb{Z}} c_n \cdot \varepsilon(n)}{g} = \frac{1}{g}\left(\sum_{n\in\mathbb{Z}} c_n \cdot \frac{\varepsilon(n)}{1}\right) = \frac{(0)_{n\in\mathbb{Z}}}{1}.$$

It remains to show that φ is a homomorphism of R-modules. This holds, as

$$\begin{aligned}\varphi\left(\frac{(c_n)_{n\in\mathbb{Z}}}{g} + \frac{(d_n)_{n\in\mathbb{Z}}}{f}\right) =& \varphi\left(\frac{(f(n)c_n + g(n)d_n)_{n\in\mathbb{Z}}}{gf}\right)\\ =& \frac{f(z)c_z + g(z)d_z}{g(z)f(z)} = \frac{c_z}{g(z)} + \frac{d_z}{f(z)}\\ =& \varphi\left(\frac{(c_n)_{n\in\mathbb{Z}}}{g}\right) + \varphi\left(\frac{(d_n)_{n\in\mathbb{Z}}}{f}\right),\end{aligned}$$

and

$$\begin{aligned}\varphi\left(f \cdot \frac{(c_n)_{n\in\mathbb{Z}}}{g}\right) =& \varphi\left(\frac{(f(n)c_n)_{n\in\mathbb{Z}}}{g}\right)\\ =& \frac{f(z)c_z}{g(z)} = f \cdot \varphi\left(\frac{(c_n)_{n\in\mathbb{Z}}}{g}\right).\end{aligned}$$

This proves the first claim. By Proposition 7.4, $L_{P_z}(E) \neq 0$ if and only if $E_{P_z} \neq 0$, which happens with $z \in \mathbb{Z}$. Thus the first claim implies that $X_1(E) = \mathbb{Z}$, which is not a closed set. Therefore the result of Proposition 7.6 does not hold for this module.

Second claim: $b(E) = 1$.

As $b(E)$ is defined to be the supremum of all numbers $b_{P_z}(E)$, it is enough to show that each of these is bounded above by 1. By the definition of $b_{P_z}(E)$, it suffices to show that

$$\dim P_z + \dim L_{P_z}(E) \leq 1 \tag{7}$$

for each P_z for which $L_{P_z}(E) \neq 0$. As $L_{P_z}(E) \neq 0$ is equivalent to $E_{P_z} \neq 0$ by Proposition 7.4, the equation (7) thus needs to be shown for each $z \in \mathbb{Z}$.

As noted above, all nonzero P_z are maximal ideals, so $\dim P_z = 0$ for all $z \in \mathbb{Z}$. Each E_z is a nonzero module and generated by $1_{\mathbb{C}}$, so the isomorphism $E_{P_z} \cong E_z$ implies that the minimal number of generators for E_{P_z} is also 1. By Lemma 7.5, $\dim L_{P_z}(E) = 1$. Therefore $\dim P_z + \dim L_{P_z}(E) = 1$ for all $z \in \mathbb{Z}$. This proves the second claim. As the module E is not finitely generated, it is not possible to find a single generator: this shows that the result of Theorem 7.9 does not hold for this ideal.

Afterword

This text presents results that give the minimal number of generators for an ideal in local rings, a lower bound for this number in non-local rings, and an upper bound in Noetherian rings. It is not a complete treatment of the subject, but in my opinion, the most important goal was to gain more confidence in commutative algebra, in which I think I succeeded. Despite a few moments of despair, on the whole the writing process was a positive experience, and I learned a lot.

The last chapter is based on an article by Otto Forster. As this article is not quite recent, it should be no surprise that also other people have brought up the subject after the publication of the article, and improvements to the result have been introduced. However, I decided to concentrate on this one article, as I felt that it (or actually just the first 5 pages of it) offered enough challenges.

Gröbner bases are one topic which I originally planned to include but later left out. A Gröbner basis of an ideal I in a polynomial ring is a generating set of I so that the leading terms of its polynomials generate the same ideal as the leading terms of all polynomials in I. A Gröbner basis is minimal, when none of its subsets is a Gröbner basis, and all minimal Gröbner bases are of the same size. My question, to which I did not yet find an answer, was whether it is possible to find a generating set that is smaller than the minimal Gröbner basis. If a generating set like this can be found, it means that finding the Gröbner basis, for which there exist algorithms, does not help in the search for the minimal number of generators.

APPENDIX A

Index of Notation

Notation	*Explanation*
$\mathbb{N}$	Natural numbers $\{0, 1, 2, 3, \dots\}$
$\mathbb{Z}$	Integers
$\mathbb{Z}_+$	Positive integers $\{1, 2, 3, \dots\}$
$\mathbb{R}$	Real numbers
$\mathbb{C}$	Complex numbers
$\mathbb{F}_p$	Field with p elements, where p is a prime number
R	A commutative ring with multiplicative identity 1_R
(a)	Ideal generated by one element a
$(a_1, \dots, a_n)$	Ideal generated by elements $a_1, \dots, a_n$
(S)	Ideal generated by a subset $S \subset R$
$S^{-1}R \quad (S^{-1}E)$	Localization of a ring R (module E) at S
$R_P \quad (E_P)$	Localization of a ring R (module E) at a prime ideal $P \subset R$
I^e	Extension of an ideal $I \subset R$ (to the localization $S^{-1}R$)
$R[x]$	Polynomial ring over R in one variable x
$R[x_1, \dots, x_n]$	Polynomial ring over R in n variables
$\deg f$	Degree of a polynomial $f \in R[x]$
f_0	Constant term of a polynomial $f \in R[x_1, \dots, x_n]$
$\dim R$	Krull dimension of a ring R
$\dim P$	Krull dimension of a prime ideal $P \subset R$
$\sqrt{I}$	Radical of an ideal $I \subset R$
$\operatorname{rad} R$	Jacobson radical of R (intersection of maximal ideals)
$\operatorname{Spec} R$	Prime spectrum of R
$\operatorname{mSpec} R$	Maximal spectrum of R
$V(I)$	Closed set in Zariski topology, $\{P \in \operatorname{Spec} R\colon P \supset I\}$
Re	R-module generated by one element e in R-module E
$\operatorname{Ann}(E)$	Annihilator of a module E
$\prod_{i \in A} E_i$	Direct product of modules E_i
$\bigoplus_{i \in A} E_i$	Direct sum of modules E_i
$A \otimes_R B$	Tensor product of R-modules A and B
$a \otimes b$	Simple tensor in $A \otimes_R B$
$\Phi\vert_T$	Restriction of Φ to set T
$\ker \varphi$	Kernel of a ring/module homomorphism φ
$\cong$	Symbol for (ring/module) isomorphism

Bibliography

[Arrondo] Arrondo, Enrique: *A geometric introduction to commutative algebra*, retrieved from http://www.mat.ucm.es/∼arrondo/commalg.pdf, 2006.

[Ciesielski] Ciesielski, Krzysztof: *Set theory for the working mathematician*, Cambridge University Press, 1997.

[Dummit] David S. Dummit, Richard M. Foote: *Abstract Algebra*, Third Edition, John Wiley and Sons, Inc., 2004.

[Eisenbud] David Eisenbud: *Commutative Algebra with a View Toward Algebraic Geometry*, Springer, 1995.

[Forster] Otto Forster: *Über die Anzahl der Erzeugenden eines Ideals in einem Noetherschen Ring*, Mathematische Zeitschrift 84, 80-87, 1964.

[Lang] Serge Lang: *Algebra*, Revised Third Edition, Springer, 2002.

[Matsumura] Hideyuki Matsumura: *Commutative Ring Theory*, Cambridge University Press, 1986.

[Nagata] Masayoshi Nagata: *Local Rings*, Interscience Publishers, John Wiley and Sons, 1962.

[Radical Ideal] *Every radical ideal in a Noetherian ring is a finite intersection of primes*, question on math.stackexchange.com, retrieved from https://math.stackexchange.com/questions/767455/every-radical-ideal-in-a-noetherian-ring-is-a-finite-intersection-of-primes?answertab=active#tab-top, 2014.