Commutative Algebra Notes

Notes By: Aryaman Maithani

Last Updated: November 21, 2022

Contents

1 Artinian and Noetherian rings **2**
1.1 Primary decompositions . . . 2
1.2 Artinian rings . . . 2

2 Valuation rings **5**
2.1 Definitions . . . 5
2.2 Discrete Valuation Rings . . . 9

3 Graded rings and modules **12**
3.1 Graded rings and modules . . . 12
3.2 Filtrations and Topology . . . 19
3.3 The Artin-Rees Lemma . . . 22
3.4 Krull's intersection theorems . . . 24

4 Dimension Theory **26**
4.1 Integer valued polynomials . . . 26
4.2 Embedding dimension . . . 28
4.3 Dimension à la Hilbert polynomials . . . 28
4.4 Properties of dimension . . . 31
4.5 Characterisation of dimension . . . 37
4.6 Krull dimension . . . 38

§1. Artinian and Noetherian rings

We assume basic results about Artinian and Noetherian rings. We prove some others.

§§1.1. Primary decompositions

§§1.2. Artinian rings

Proposition 1.2.1. Let R be a ring, and $I \subseteq R$ an ideal. Let M be an R-module such that $IM = 0$. Equivalently, M is an R/I-module.

Then, M is Artinian (resp. Noetherian) as an R-module if it is so as an R/I-module.

Proof. Check that the family of submodules is the same in both cases. □

Proposition 1.2.2. Let $0 \to N \to M \to L \to 0$ be an exact sequence of R-modules. The following are equivalent:

1. M is Artinian (resp. Noetherian).
2. N and L are Artinian (resp. Noetherian).

Corollary 1.2.3. Any quotient of an Artinian ring is Artinian (as a ring).

Corollary 1.2.4. Every prime ideal in an Artinian ring is maximal. In other words, the (Krull) dimension of an Artinian ring is zero.

Since it is convenient to refer to this, we make a special definition of dimension now. We have an elaborate discussion of dimension later.

Definition 1.2.5. A ring R is said to be of dimension zero, denoted $\dim(R) = 0$, if every prime ideal of R is maximal.

Proposition 1.2.6. An Artinian ring has finitely many prime (maximal) ideals.

Proof. Suppose not. Let $\mathfrak{m}_1, \mathfrak{m}_2, \ldots$ be a sequence of distinct prime (and hence, maximal) ideals. Note that the chain

$$\mathfrak{m}_1 \supseteq \mathfrak{m}_1 \cap \mathfrak{m}_2 \supseteq \cdots$$

must stabilise. Thus, there exists n such that

$$\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_n = \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_n \cap \mathfrak{m}_{n+1}.$$

Note that the ideal on the right is contained in $\mathfrak{m}_{n+1}$. Thus, $\mathfrak{m}_{n+1}$ contains the intersection on the left. But then, since $\mathfrak{m}_{n+1}$ is prime, it must contain some $\mathfrak{m}_i$ with $i \leqslant n$. This contradicts that $\mathfrak{m}_i$ and $\mathfrak{m}_{n+1}$ are distinct maximal ideals. □

Proposition 1.2.7. Let R be a field, and M an R-module, i.e., an R-vector space. Then, M is Noetherian iff M is Artinian (iff $\dim_R(M) < \infty$).

Proposition 1.2.8. Let M be an R-module. Suppose there exists a filtration of submodules

$$0 = M_0 \subseteq M_1 \subseteq M_2 \subseteq \cdots \subseteq M_n = M$$

such that each M_{i+1}/M_i is Artinian (resp. Noetherian). Then, M is Artinian (resp. Noetherian).

Conversely, if M is an Artinian (resp. Noetherian) module and we have a filtration as above, then each M_{i+1}/M_i is Artinian (resp. Noetherian).

Proof. By hypothesis, $M_1 \cong M_1/M_0$ is Artinian (resp. Noetherian). The exact sequence

$$0 \to M_1 \to M_2 \to M_2/M_1$$

shows the same for M_2. Induct.

The converse is again an easy consequence of Proposition 1.2.2. □

Corollary 1.2.9. Let R be any ring, and M an R-module. Let $\mathfrak{m}_1, \ldots, \mathfrak{m}_n$ be maximal ideals of R (not necessarily distinct) such that $\mathfrak{m}_1 \cdots \mathfrak{m}_n M = 0$.

Then, M is Noetherian iff M is Artinian.

Proof. Consider the filtration

$$0 = \mathfrak{m}_1 \cdots \mathfrak{m}_n M \subseteq \mathfrak{m}_1 \cdots \mathfrak{m}_{n-1} M \subseteq \cdots \subseteq \mathfrak{m}_1 M \subseteq M.$$

Note that $\mathfrak{m}_1 \cdots \mathfrak{m}_i M / \mathfrak{m}_1 \cdots \mathfrak{m}_{i+1} M$ is an $R/\mathfrak{m}_{i+1}$-module.

Now use the previous two propositions. □

Proposition 1.2.10. Let R be an Artinian ring. The nilradical $\mathcal{N}$ is nilpotent, i.e., $\mathcal{N}^k = 0$ for some $k \geqslant 0$.

Proof. The descending chain of powers of $\mathcal{N}$ must stabilise to some $\mathcal{N}^k$. We claim $\mathcal{N}^k = 0$.

Suppose not. Let $I := \mathcal{N}^k$. By hypothesis, $II = I \neq 0$. Thus, by the Artinian condition, we may pick J minimal with respect to the property that $IJ \neq 0$.

Thus, there exists $z \in J$ with $Iz \neq 0$. But also, $I(Iz) = Iz \neq 0$.
Since $Iz \subseteq (z) \subseteq J$, minimality forces $Iz = (z)$. Thus, we can write $z = xz$ for some $x \in I$.
Thus, we have $z = xz = x^2z = x^3z = \cdots$.
But x is nilpotent, since $I \subseteq \mathcal{N}$. Thus, $z = 0$, contradicting that $Iz \neq 0$. □

Corollary 1.2.11. Any Artinian ring is Noetherian.

Proof. Let R an an Artinian ring. Note that $\mathcal{N} = \bigcap_{\mathfrak{p} \in \operatorname{Spec} R} \mathfrak{p}$. Since R is Artinian, $\mathcal{N}$ is the intersection of all the finitely many maximal ideals of R.
But this is just the product $\prod \mathfrak{m}_i$ since the ideals are comaximal. In turn, $\mathcal{N}^k$ is a product of maximal ideals. Now use Corollary 1.2.9. □

Corollary 1.2.12. Let R be a ring. The following are equivalent:

(i) R is Artinian.

(ii) R is Noetherian and $\dim(R) = 0$.

Proof. (i) $\Rightarrow$ (ii) follows from earlier.

(ii) $\Rightarrow$ (iii): Since R is Noetherian, R has finitely many minimal primes. Since $\dim(R) = 0$, all of these are maximal as well. Since every prime contains a minimal prime, it follows that there are only finitely many primes. Then, we have $\mathcal{N} = \bigcap_i \mathfrak{p}_i = \prod_i \mathfrak{p}_i$. But in a Noetherian ring, the nilradical is nilpotent and thus, $\mathcal{N}^k = 0$ for some k. Using Corollary 1.2.9, we get that R is Artinian. □

§2. Valuation rings

§§2.1. Definitions

Definition 2.1.1. A valuation ring is an integral domain R such that for all $a, b \in R$: either a divides b or b divides a.

Equivalently, the set of principal ideals is totally ordered by inclusion.

Equivalently, if $K = \mathrm{Frac}(R)$, then for every $x \in K^\times$, either $x \in R$ or $x^{-1} \in R$.

Recall that a totally ordered abelian group is an abelian group $(A, +)$ with a total order $\leqslant$ such that $x \leqslant y \Rightarrow x + z \leqslant y + z$ for all $x, y, z \in A$.
We often consider the ordered set $A_\infty := A \sqcup \{\infty\}$, this extends the order from A by defining $a < \infty$ for all $a \in A$.

Definition 2.1.2. Let K be a field, and A a totally ordered abelian group. A valuation is a map

$$v : K \to A \sqcup \{\infty\}$$

such that

- $v(0) = \infty$,
- $v(K^\times) \subseteq A$,
- $v(xy) = v(x) + v(y)$ for all $x, y \in K^\times$,
- $v(x + y) \geqslant \min(v(x), v(y))$ for all $x, y \in K$.

Note that the third point is simply stating that v is a group homomorphism when restricted to $K^\times \to A$. We often just specify valuations by defining them on $K^\times$.

Observation 2.1.3. Since v is a group homomorphism, we have $v(1) = 0$ and $v(x^{-1}) = -v(x)$ for $x \in K^\times$.

Proposition 2.1.4. Let R be an integral domain, and $K = \mathrm{Frac}(R)$. The following are equivalent:

(i) R is a valuation ring.

(ii) There exists a totally ordered abelian group A and a valuation $v : K \to A_\infty$ such that $R = \{x \in K : v(x) \geqslant 0\}$.

Proof. We prove the nontrivial direction, namely (i) $\Rightarrow$ (ii).

Assume that R is a valuation ring. Define a preorder on $K^\times$ as follows: $x \leqslant y$ iff $y/x \in R$. By hypothesis, any two elements are comparable.
Define the equivalence relation $\sim$ on $K^\times$ as $x \sim y$ iff $x \leqslant y$ and $y \leqslant x$.
Let $A := K^\times/\sim$. Note that we can define multiplication on A by $[x] \cdot [y] = [xy]$. (Check that this is well-defined.)
The map $\nu : K^\times \twoheadrightarrow A$ defined by $x \mapsto [x]$ does the job. □

In view of the above proposition, whenever we talk about a valuation ring R, we always have an associated valuation with it. Proceeding forward, K will denote the fraction field of R. We have the relation $R = \{x \in K : \nu(x) \geqslant 0\}$.
For $x, y \in R$, we see that $x \mid y$ is equivalent to $\nu(x) \leqslant \nu(y)$.

Proposition 2.1.5. Any valuation ring R is normal.

Proof. Let $x \in K$ be integral over R. We wish to show $\nu(x) \geqslant 0$. Write

$$x^n = a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

for $a_i \in R$. Applying ν, we get

$$n\nu(x) \geqslant \min(\nu(a_{n-1}) + (n-1)\nu(x), \ldots, \nu(a_0)).$$

Thus, there exists some $i \in \{0, \ldots, n-1\}$ such that $n\nu(x) \geqslant \nu(a_i) + i\nu(x)$. Thus, $(n-i)\nu(x) \geqslant \nu(a_i) \geqslant 0$. This proves the result. □

Proposition 2.1.6. Any valuation ring R is normal. The unique maximal ideal is given by $\{x \in R : \nu(x) > 0\} = \{x \in K : \nu(x) > 0\}$.

Proof. Let $\mathfrak{m} := \{x \in R : \nu(x) > 0\}$. The properties of valuation imply that $\mathfrak{m}$ is indeed an ideal. $\mathfrak{m}$ is proper since $\nu(1) = 0$ and thus, $1 \notin \mathfrak{m}$.

On the other hand, if $x \in R \setminus \mathfrak{m}$, then $\nu(x) = 0$. This means that $x^{-1} \in K$ also satisfies $\nu(x^{-1}) = -\nu(x) = 0$ and thus, $x^{-1} \in R$, i.e., x is a unit. □

Theorem 2.1.7. Let R be a domain, not necessarily a valuation ring.
Let $\mathfrak{p} \in \operatorname{Spec} R$, and $K = \operatorname{Frac}(R)$.
Then, there exists a valuation ring V such that

- $R \subseteq V \subseteq K$,
- the maximal ideal of V contracts to $\mathfrak{p}$.

In particular, if ν is the associated valuation to V, we have $\mathfrak{p} = \{x \in R : \nu(x) > 0\}$.

Proof. Throughout this proof, localisations of R (and of other subrings of K) will be considered as subrings of K in the natural way.

Let Σ denote the collection of intermediate subrings R': $R_{\mathfrak{p}} \subseteq R' \subseteq K$ such that $\mathfrak{p}R' \neq R'$.

Σ is nonempty since $R_{\mathfrak{p}} \in \Sigma$. Ordering Σ by inclusion, we note that Σ satisfies the hypothesis of Zorn's Lemma[1] and thus, there exists a maximal V. We show that V has the desired properties.

Claim 1. V is local.

Proof. By construction, $\mathfrak{p}V \neq V$. Thus, $\mathfrak{p}V$ is contained in some maximal ideal $\mathfrak{m} \subseteq V$. In turn, $\mathfrak{p}V_{\mathfrak{m}}$ is a proper subset of $V_{\mathfrak{m}}$ and hence, $V_{\mathfrak{m}} \in \Sigma$. By maximality, we must have $V = V_{\mathfrak{m}}$, proving that V is a local ring. □

Going forth, let $\mathfrak{m}$ denote the maximal ideal of V. Note that $\mathfrak{p}V \subseteq \mathfrak{m}$. In particular, intersecting with $R_{\mathfrak{p}}$ shows that

$$\mathfrak{p}V \cap R_{\mathfrak{p}} = \mathfrak{m} \cap R_{\mathfrak{p}}.$$

But $\mathfrak{p}R_{\mathfrak{p}}$ is clearly contained in the left ideal. Thus, we have

$$\mathfrak{p}R_{\mathfrak{p}} = \mathfrak{m} \cap R_{\mathfrak{p}}.$$

Further contracting to R gives us

$$\mathfrak{p} = \mathfrak{m} \cap R.$$

Thus, we now only need to prove that V is a valuation ring.

Claim 2. V is normal.

Proof. Let $x \in K$ be integral over V. Showing $x \in V$ is equivalent to saying $V = V[x]$. Using maximality of V in Σ, it suffices to prove that $V[x] \in \Sigma$.

Note that $V \hookrightarrow V[x]$ is an integral extension. Thus, there is a prime $\mathfrak{m}' \subseteq V[x]$ lying over V. In particular, $\mathfrak{p} \subseteq \mathfrak{m}'$ showing that $\mathfrak{p}V[x] \neq V[x]$. □

We are now ready to show that V is a valuation ring. Let $x \in K^{\times}$ with $x \notin V$. We need to show that $x^{-1} \in V$.

Consider the subring $V[x]$. This is strictly larger than V. By maximality, we must have that $V[x] \notin \Sigma$ and thus, $1 \in \mathfrak{p}V[x]$. We can then write

$$1 = p_0 + p_1 x + \cdots + p_t x^t$$

for some $p_i \in \mathfrak{p}V$.

[1]Note that $1 \in \mathfrak{p}R'$ is a "finite condition".

Rearrange the above to get

$$1 - p_0 = p_1 x + \cdots + p_t x^t.$$

Note that $p_0 \in \mathfrak{p}V \subseteq \mathfrak{m}$ and thus, $1 - p_0$ is a unit in V. Thus, we can write

$$\frac{1}{x^t} = \frac{1}{1 - p_0}\left(\frac{p_1}{x^{t-1}} + \cdots + p_t\right).$$

The above shows that x^{-1} is integral over V. By Claim 2, it follows that $x^{-1} \in V$, as desired. □

Corollary 2.1.8. Let R be an integral domain, and let $\mathfrak{q} \subseteq \mathfrak{p}$ be primes. There exists a valuation ring V and a ring homomorphism $f : R \to V$ such that $f^{-1}(\mathfrak{m}_V) = \mathfrak{p}$ and $f^{-1}(0) = \mathfrak{q}$.
($\mathfrak{m}_V$ denotes the maximal ideal of V.)

Proof. Applying the previous proposition to $R/\mathfrak{q}$, there exists a valuation ring V and an injection $g : R/\mathfrak{q} \hookrightarrow V$ such that $g^{-1}(\mathfrak{m}_V) = \mathfrak{p}/\mathfrak{q}$ (and necessarily $g^{-1}(0) = 0$).
Compose this with the projection $R \twoheadrightarrow R/\mathfrak{q}$. □

Corollary 2.1.9. If R is a normal domain, then

$$R = \bigcap_{\substack{R \subseteq V \subseteq K \\ V \text{ is a valuation ring}}} V.$$

More generally, if R is any integral domain, and $\overline{R}$ is its integral closure in K, then

$$\overline{R} = \bigcap_{\substack{R \subseteq V \subseteq K \\ V \text{ is a valuation ring}}} V.$$

Proof. Note that since valuation rings are integrally closed, it follows that $\overline{R}$ is contained the intersection.

Conversely, suppose x belongs to the intersection. This means that $\nu(x) \geqslant 0$ for every valuation ν on K. We must show that x is integral over R.

Let $R' = R\left[\frac{1}{x}\right]$ and $I = \left(\frac{1}{x}\right) R'$.

Claim. $I = R'$.

Proof. If not, then $I \subseteq \mathfrak{m}$ for some maximal ideal $\mathfrak{m} \subseteq R'$. By the previous proposition, there exists a valuation ring $V \supseteq R'$ such that $x^{-1} \in \mathfrak{m}_V$. This implies that $\nu(x) = -\nu(x^{-1}) > 0$. A contradiction. □

Thus, $I = R'$. In other words, $1/x$ is a unit in R' and hence, $x \in R'$. This means we can write

$$x = r_0 + \frac{r_1}{x} + \cdots + \frac{r_n}{x^n}$$

for some $r_i \in R$. Multiplying with x^n shows that x satisfies a monic polynomial over R, as desired. □

Proposition 2.1.10. Let R be an integral domain. The following are equivalent:

(i) R is a valuation ring.

(ii) R is a local Bézout domain. (That is, R is a local ring, where every finitely generated ideal is principal.)

Proof. (i) $\Rightarrow$ (ii): Suppose R is a valuation ring. We have already seen that R is local. Let $I = (f_1, \ldots, f_n)$ be a finitely generated ideal. By definition of a valuation ring, we may pick a maximal ideal among the principal ideals $(f_1), \ldots, (f_n)$. Then, I is equal to that principal ideal.

(ii) $\Rightarrow$ (i): Let $x, y \in R$ be nonzero. We wish to show that either $x \mid y$ or $y \mid x$.
By hypothesis, we can write $(x, y) = (d)$ for some $d \in R$. In turn, we have the relations

$$x = dx',\ y = dy',\ d = ax + by,$$

for some $a, b, x', y' \in R$.

Plugging the first two relations in the last gives us

$$d = (ax' + by')d.$$

We may cancel d to see that $(x', y') = (1)$. Since R is a local ring, this implies that one of x' or y' is a unit. Without loss of generality, x' is a unit (in R).

Then, we have

$$y = dy' = \frac{y'}{x'}x.$$ □

§§2.2. Discrete Valuation Rings

Definition 2.2.1. A valuation $\nu : K \to A_\infty$ is said to be a discrete valuation if $\nu(K^\times)$ is isomorphic to $\mathbb{Z}$.

A discrete valuation ring (DVR) is a ring that is of the form $\{x \in K : \nu(x) \geqslant 0\}$ for some discrete valuation $\nu : K \to A_\infty$.

Note that the trivial valuation is not a discrete valuation. Equivalently, a field is not a discrete valuation ring.

Note that given a discrete valuation, we may always assume that $A = \mathbb{Z}$ and that $\nu(x) \neq 0$ for some $x \in K$.

Proposition 2.2.2. Let R be a valuation ring. The following are equivalent.

(i) R is Noetherian.

(ii) R is a DVR or a field.

(iii) R is a local PID.

((ii) and (iii) are equivalent even without the a priori assumption that R is a valuation ring. See Corollary 2.2.4)

Proof. Let $\nu : K \to A_\infty$ and $\mathfrak{m} \subseteq R$ be as usual

(i) $\Leftrightarrow$ (iii) is clear by Proposition 2.1.10.

(iii) $\Rightarrow$ (ii): Assume R is a local PID and not a field.
By hypothesis, we have $\mathfrak{m} = (x)$ with $0 < \nu(x) < \infty$. In turn,

$$\nu(x) = \min\{\nu(r) : r \in K, \nu(r) > 0\}.$$

(The above follows since $\nu(r) > 0 \Rightarrow r \in \mathfrak{m} = (x) \Rightarrow x \mid r$.)
In other words, $\nu(x)$ is the smallest positive valuation.

We show that $\nu(K^\times)$ is generated by $\nu(x)$. Let $y \in K^\times$ be arbitrary. We may assume y is not a unit. By replacing y with y^{-1}, we may assume that $\nu(y) > 0$ and hence, $y \in R$.

Consider the following subsets of K:

$$yR \subsetneq \frac{y}{x}R \subsetneq \frac{y}{x^2}R \subsetneq \cdots .$$

Note that as long as $y/x^n \in R$, the set $(y/x^n)R$ is an ideal of R. Since R is Noetherian, the chain must eventually escape R, i.e., there exists $n \geqslant 0$ such that $y/x^{n+1} \notin R$. Choose the smallest such n. Then, we have

$$\nu(y/x^n) \geqslant 0 > \nu(y/x^{n+1}).$$

If $\nu(y/x^n) = 0$, then we are done since we have $\nu(y) = n\nu(x)$. If this is not the case, then we have strict inequalities above, which gives

$$\nu(y/x^n) > 0 > \nu(y/x^{n+1}).$$

Rearranging gives

$$\nu(x) > \nu(x^{n+1}/y) > 0.$$

But this contradicts that x had smallest positive valuation.

(ii) $\Rightarrow$ (i): Clearly we may assume that R is a DVR. Let $\nu : K \to \mathbb{Z}_\infty$ be the associated valuation. Consider the ideals I_n defined as

$$I_n := \{x \in R : \nu(x) \geqslant n\},$$

for $n \geqslant 0$. (I_n is an ideal by properties of valuation.)

We claim that any nonzero ideal in R is of the form. Indeed, given a nonzero ideal J, let $n \geqslant 0$ and $x \in J$ be such that $\nu(x) = n$ is the smallest valuation among elements of J.
In particular, $J \subseteq I_n$. Conversely, if $y \in I_n$, then $\nu(x) \leqslant \nu(y)$ shows that $x \mid y$ in R and hence, $y \in (x) \subseteq J$.

Thus, the ideals of R all appear in the following chain:

$$I_0 \supseteq I_1 \supseteq I_2 \supseteq \cdots \supseteq 0.$$

It follows that R is Noetherian. □

Note that if $\nu : K \to \mathbb{Z}_\infty$ is a valuation, then $\nu(K^\times)$ is a nonzero subgroup of $\mathbb{Z}$ and thus, of the form $n\mathbb{Z}$ for some $n > 0$. This gives us a new valuation $\nu' : K \to \mathbb{Z}_\infty$ defined by $\nu'(x) = \nu(x)/n$.
Both of these define the same valuation ring. Thus, we may always assume that a discrete valuation surjects onto $\mathbb{Z}_\infty$.

From the last part of the above proof, we extract the following.

Porism 2.2.3 (Description of ideals in DVRs)**.** Let R be a DVR, and $\nu : K \twoheadrightarrow \mathbb{Z}_\infty$ the associated valuation.
Pick any $t \in K$ with $\nu(t) = 1$. Then, the ideals

$$(1), (t), (t^2), (t^3), \ldots, (0)$$

are all the distinct ideals of R.

In particular, R is a local PID.

Corollary 2.2.4. Let R be a ring which is not a field. The following are equivalent:

(i) R is a local PID.

(ii) R is a DVR.

Proof. In either case, we need to show that R is a valuation ring and then we can appeal to Proposition 2.2.2. If we assume (ii), then this follows tautologically. If we assume (i), then this follows from Proposition 2.1.10. □

§3. Graded rings and modules

Going forth, we make the convention that $0 \in \mathbb{N}$.

§§3.1. Graded rings and modules

Definition 3.1.1. A ($\mathbb{N}$-)graded ring is a ring R with a sequence of additive subgroups $\langle R_n \rangle_{n \geqslant 0}$ such that

$$R = \bigoplus_{n \geqslant 0} R_n \quad \text{and} \quad R_m R_n \subseteq R_{m+n}$$

for all $n, m \geqslant 0$.

Elements of $R_0 \cup R_1 \cup \cdots$ are called homogeneous elements. A nonzero homogeneous element x belongs to R_n for some unique n, this is called the degree of x.

$R_+ := \bigoplus_{n \geqslant 1} R_n$ is an ideal of R, called the irrelevant ideal.

Note that $0 \in R_n$ for all n. There is some care that must be taken when defining the degree of 0. We do not bother about it and leave the edge cases to the reader.

Note that being graded is not a property of a ring. Rather, it consists of additional data given to a ring. (In contrast to something like how being a field is a property of a ring.) However, we still often say "R is a graded ring" and tacitly assume that we are given a *grading* $\langle R_n \rangle_{n \in \mathbb{N}}$.

Definition 3.1.2. Let R be a graded ring. A graded R-module is an R-module M with a sequence of additive subgroups $\langle M_n \rangle_{n \in \mathbb{Z}}$ such that

$$M = \bigoplus_{n \in \mathbb{Z}} M_n \quad \text{and} \quad R_m M_n \subseteq M_{m+n}$$

for all $n, m \geqslant 0$.

A homogeneous element and its degree is defined as before.

Proposition 3.1.3. Let R be a graded ring, and M a graded R-module.
Then, R_0 is a subring of R. In particular, $1 \in R$.
Moreover, each M_n is an R_0-module.

Note that M_n will typically *not* be an R-module.

Proof. The only nontrivial thing to check is that $1 \in R$. By hypothesis, we can write

$$1 = r_0 + r_1 + \cdots, \tag{3.1}$$

where $r_i \in R_i$ and $r_n = 0$ for $n \gg 0$.

We show that $r_i = 0$ for all $i > 0$ and hence, $1 = r_0 \in R_0$.
Multiplying (3.1) with r_0 shows

$$r_0 = r_0^2 + r_0 r_1 + \cdots .$$

Comparing the homogeneous components on each side shows that $r_0 r_i = 0$ for $i > 0$.

Now, fix $i > 0$ and multiply (3.1) with r_i to get

$$r_i = r_0 r_i + r_1 r_i + \cdots .$$

Again, comparing the homogeneous components gives

$$r_i = r_0 r_i.$$

But by the earlier calculation, the element on the right is 0. □

Example 3.1.4. 1. If k is a field, and $R = k[x_1, \ldots, x_d]$, then R has a natural grading with R_n consisting of the k-vector space generated by monomials of degree n.

2. Let R be a graded ring, and $f \in R$ be a nonzero homogeneous element. Then, $R_f = R[f^{-1}]$ has a natural R-module structure. (Note that unless f is nilpotent (in which case, $R_f = 0$) or $\deg(f) = 0$, R_f will have graded pieces in the negative component. Thus, R_f is not an $\mathbb{N}$-graded ring.)

3. More generally, let $S \subseteq R$ be a multiplicative subset consisting of homogeneous elements. Then, $S^{-1}R$ is a graded R-module: $(S^{-1}R)_n$ consists of elements of the form r/s where $r \in R$ and $s \in S$ are homogeneous with $\deg(r) - \deg(s) = n$. (If $r/s = r'/s'$ with r' and s' also homogeneous, it will follow that $\deg(r') - \deg(s') = n$.)

   By the above definition, it follows that $R_n (S^{-1}R)_m \subseteq (S^{-1}R)_{m+n}$. In fact, it even follows that $S^{-1}R$ is a $\mathbb{Z}$-graded ring (the definition is the obvious one).

   Even in this case, the homogeneous elements of degree 0 form a subring of $S^{-1}R$.

   If $\mathfrak{p} \subseteq R$ is a graded homogeneous prime ideal (defined just below), then one can consider S to be the set of homogeneous elements not contained in $\mathfrak{p}$. This is a multiplicative subset. The 0-degree subring of $S^{-1}R$ is sometimes denoted $R_{(\mathfrak{p})}$.

Example 3.1.5 (Rees algebra)**.** Given a ring R and an ideal I, we can construct the Rees algebra as follows:
Let $S_0 := R$, $S_n := I^n$ for $n \geqslant 1$. Then,

$$\bigoplus_{n \geqslant 0} S_n$$

has a natural ring structure.

There is a notational issue as to how one would write an element of S. One way is to write them as tuples, this is unwieldy. We would like to write them as sums, but then there's the issue of whether one interprets an element $x \in I$ as sitting in S_1 or S_0.

To combat this, we attach a dummy variable and define

$$R[It] := \bigoplus_{n \geqslant 0} I^n t^n \cong \bigoplus_{n \geqslant 0} S_n.$$

The upshot is that the variable t now succinctly acts as a bookkeeping device. Given a ring R and an ideal I, we can construct the Rees algebra as follows:
Let $S_0 := R$, $S_n := I^n$ for $n \geqslant 1$. Then,

$$\bigoplus_{n \geqslant 0} S_n$$

has a natural ring structure.

There is a notational issue as to how one would write an element of S. One way is to write them as tuples, this is unwieldy. We would like to write them as sums, but then there's the issue of whether one interprets an element $x \in I$ as sitting in S_1 or S_0.

To combat this, we attach a dummy variable and define

$$R[It] := \bigoplus_{n \geqslant 0} I^n t^n \cong \bigoplus_{n \geqslant 0} S_n.$$

The upshot is that the variable t now succinctly acts as a bookkeeping device.

Definition 3.1.6. Let M, N be graded R-modules. A graded module homomorphism $f : M \to N$ is a module homomorphism f such that $f(M_n) \subseteq N_n$.

A sequence of graded modules is defined similarly.

Definition 3.1.7. Given a graded R-module M, and an integer d, we defined the shift $M(d)$ to be the graded R-module M with new grading

$$(M(d))_n = M_{d+n}.$$

Observation 3.1.8. Let M be a graded R-module, and $x \in R$ a homogeneous element of degree d. Note that

$$M \xrightarrow{x} M$$

is a map of R-modules, but not a graded map (barring some trivial cases).

However, by shifting the domain, we do get a graded map as

$$M(-d) \xrightarrow{x} M.$$

Indeed, note that if $m \in (M(-d))_n$, then

$$xm \in R_d M_{-d+n} \subseteq M_n,$$

as desired.

Definition 3.1.9. Let M be a graded R-module. A submodule $N \subseteq M$ is said to be a graded (or homogeneous) R-submodule if N satisfies any of the following equivalent properties:

1. N is generated by homogeneous elements.
2. $N = \bigoplus_{n \in \mathbb{Z}} (N \cap M_n)$.
3. Whenever $x \in N$, every homogeneous component (in M) of x is an element of N.

Observation 3.1.10. If $N \leqslant M$ is a graded submodule, then M/N has a natural grading given by

$$(M/N)_n := M_n/(N \cap M_n).$$

Note that by definition, we have $N = \bigoplus_{n \in \mathbb{Z}} (N \cap M_n)$, where this is an internal direct sum. Thus, one has the natural isomorphism $M/N \cong \bigoplus_{n \in \mathbb{Z}} (M/N)_n$.

Under this grading, we have an exact sequence of graded R-modules given as

$$0 \to N \to M \to M/N \to 0.$$

For homogeneous ideals, primality can be checked on homogeneous elements:

Proposition 3.1.11. Let $I \subseteq R$ be a graded ideal with the property that if x, y are homogeneous elements with $xy \in I$, then either $x \in I$ or $y \in I$. Then, I is prime.

Proposition 3.1.12. Let R be a graded ring. Let $S \subseteq R_+$ be any subset. The following are equivalent:

(i) S generates R_+ as an R-ideal.

(ii) S generates R as an R_0-algebra.

Proof. Only (i) $\Rightarrow$ (ii) is nontrivial. Let $T := R_0[S]$. We show that $R = T$ by proving $R_n \subseteq R$ for all $n \geqslant 0$.

We prove this by induction. $n = 0$ is clear. Let $n > 0$. By hypothesis, we have $R_n \subseteq R_+ = RS$. Thus,

$$\begin{aligned} R_n &= (R \cdot S) \cap R_n \\ &= (R_0 + \cdots + R_{n-1})S \cap R_n && \textit{If } m \geqslant n, \textit{ then } R_m S \cap R_n = 0 \\ &\subseteq TS \cap R_n && \textit{by induction} \\ &\subseteq T, \end{aligned}$$

as desired. □

Corollary 3.1.13. Let R be a graded ring.
R is a Noetherian ring iff R_0 is a Noetherian ring and R is a finitely generated R_0-algebra.

Proof. ($\Leftarrow$) Follows from Hilbert's Basis Theorem since we can write R as a quotient of $R[x_1, \ldots, x_d]$.

($\Rightarrow$) R_+ is a finitely generated as an ideal and thus, R is finitely generated as an R_0-algebra. R_0 is Noetherian since $R_0 = R/R_+$. □

Definition 3.1.14. Let R be a graded ring with grading $\langle R_n \rangle_{n \geqslant 0}$. Let $d > 0$.
We define the twisted graded ring $R^{(d)}$ to be the graded ring with

$$\left(R^{(d)}\right)_n = R_{dn}.$$

This is also called the d-th Veronese subalgebra.

$R^{(d)}$ can be visualised as follows: We have the additive subgroups $R_0, R_d, R_{2d}, \ldots$ of R such that their *internal* sum is direct. This realises $R^{(d)}$ as a subset (subgroup even) of R. We now just scale the grading by d.

Example 3.1.15. Consider $R = k[x, y]$ with the standard grading. Then, $R^{(2)}$, when considered as a subring of R consists of those polynomials such that each monomial has even degree.

This can be written as $k[x^2, xy, y^2]$, as a set. However, x^2 now has degree 1 in $R^{(2)}$.

Similarly, $R^{(3)} = k[x^3, x^2y, xy^2, y^3]$.

Definition 3.1.16. Let M be a graded R-module, and $d > 0$. Let $\ell \in \{0, \ldots, d-1\}$. Then, we define

$$M^{(d,\ell)} := \bigoplus_{k : k \equiv \ell (d)} M_k.$$

The above has the structure of a graded $R^{(d)}$-module.

A slightly more precise way of writing the above would be to specify that the n-th graded component of $M^{(d,\ell)}$ is $nd + \ell$. Note that

$$R^{(d)}_m M^{(d,\ell)}_n = R_{md} M_{nd+\ell} \subseteq M_{(m+n)d+\ell} = M^{(d,\ell)}_{m+n}$$

and thus, $M^{(d,\ell)}$ is indeed a graded $R^{(d)}$-module.

Definition 3.1.17. Given a graded ring R, $\operatorname{Proj}(R)$ denotes the set of homogeneous primes of R not containing R_+.

Fact: $\operatorname{Proj}(R)$ is in bijection with $\operatorname{Proj}(R^{(d)})$ for all $d > 0$.

Proposition 3.1.18. Let R be a graded ring such that R is a finitely generated R_0-algebra. Let M be a finitely generated graded R-module. (For example, if R and M are both Noetherian.) Let $d > 0$.
Then,

(i) M_i is a finitely generated R_0-module for all i. Moreover, $M_i = 0$ for $i \ll 0$.

(ii) $M^{(d,\ell)}$ is a finitely generated $R^{(d)}$-module for all ℓ and thus,

$$M \cong \bigoplus_{\ell=0}^{d-1} M^{(d,\ell)}$$

is so.

(iii) In particular, R is a finitely generated $R^{(d)}$-module.

(iv) $R^{(d)}$ is a finitely generated R_0-algebra.

Note that in the above, M (and similarly R) is an ordinary $R^{(d)}$-module, not a graded one. (The module structure is the one inherited by virtue of $R^{(d)}$ being a subring of R, ignoring grading.)

Proof. We may assume that $m_1, \ldots, m_t$ are nonzero homogeneous and generate M. Let $d = \min_i \deg(m_i)$. Then, M_n must be zero for $i < d$ since any R-linear combination of the m_i has degree at least d.[2]

[2]It was crucial here that R is $\mathbb{N}$-graded.

Now, let $r_1, \ldots, r_p \in R_+ \setminus \{0\}$ be homogeneous elements that generate R as an R_0-algebra. Let $d_i := \deg(r_i)$.

Now, note that elements of M_i can be written as R_0-linear combination of elements of the form

$$r_1^{a_1} \cdots r_p^{a_p} m_s,$$

where $s \in \{1, \ldots, t\}$ and $a_1, \ldots, a_p \geqslant 0$ satisfy

$$\deg(m_s) + \sum_j a_j d_j = i.$$

But there are only finitely many such ways to pick s and $a_1, \ldots, a_p$ (once we fix i). Thus, each M_i is a finite R_0-module. This proves (i).

Note that each $M^{(d,\ell)}$ is a quotient of M and hence it suffices to prove that M is finitely generated. M can be generated *over* R_0 by elements of the form

$$r_1^{a_1} \cdots r_p^{a_p} m_s$$

where $a_1, \ldots, a_p \geqslant 0$ and $s \in \{1, \ldots, t\}$.

Since all powers of the form r_i^{kd} are in $R^{(d)}$, we see that we have a finite generating set by restricting the a_i to be in $[0, d-1]$. This proves (ii) and (iii).

Since R is a finitely generated R_0-algebra, R_+ is a finitely generated R-module (Proposition 3.1.12). By (ii), we see that R_+ is a finitely generated $R^{(d)}$-module. But $(R^{(d)})_+ = (R_+)^{(d,0)}$ and thus, part (ii) tells us that this is a finitely generated $R^{(d)}$-module. Using Proposition 3.1.12 again, we see that $R^{(d)}$ is a finitely generated R_0-algebra. (Note that $(R^{(d)})_0 = R_0$.)
This proves (iv). □

Corollary 3.1.19. If R is a Noetherian graded ring, then so is $R^{(d)}$ for all $d > 0$.

Proof. Use Corollary 3.1.13 and part (iv) of the previous proposition. □

Proposition 3.1.20. Let R be a graded ring, finitely generated as an R_0-algebra. Let M be a finitely generated graded R-module.
Then, there exist integers $n_0, d \geqslant 0$ such that

$$R_d M_n = M_{d+n}$$

for all $n \geqslant n_0$.

Note that we always have $R_d M_n \subseteq M_{d+n}$.

Proof. Let notation be as in the earlier proof: $m_1, \ldots, m_t$ are nonzero homogeneous and generate M over R; $r_1, \ldots, r_p \in R_+ \setminus \{0\}$ are homogeneous elements that generate R as an R_0-algebra, with $d_i := \deg(r_i)$.

Set $d := \operatorname{lcm}_i d_i$ and $n_0 := 1 + pd + \max_i \deg(m_i)$. For $1 \leqslant i \leqslant p$, define $s_i := r_i^{d/d_i} \in R_d$. We show that d and n_0 have the properties as desired. To this end, let $n \geqslant n_0$. Pick $m \in M_n$. As seen earlier, we can write m as an R_0-linear combination of elements of the form

$$r_1^{a_1} \cdots r_p^{a_p} m_s \tag{3.2}$$

such that $a_1 d_1 + \cdots + a_p d_p + \deg(m_s) = n$. Note that

$$a_1 d_1 + \cdots + a_p d_p = n - \deg(m_s) > pd.$$

Thus, there is some $i \in \{1, \ldots, p\}$ such that $a_i d_i > d$ and thus, $a_i > d/d_i$. Thus, we may write

$$r_i^{a_i} = r_i^{d/d_i} r_i^{a_i - d/d_i} = s_i r_i^{a_i - d/d_i}.$$

Thus, each term of the form in (3.2) can be written as an element of $R_d M_{n-d}$. □

Looking at the above proof, we may in fact extract a special result.

Porism 3.1.21. With the same hypothesis as earlier, assume further that $R = R_0[r_1, \ldots, r_p]$ with $\deg(r_i) = 1$ for all i.
Then, we may take $d = 1$ above, i.e., $R_1 M_n = M_{n+1}$ for $n \gg 0$.

Corollary 3.1.22. Suppose R is a graded ring and a finitely generated R_0-algebra. Then, there exists $d > 0$ such that $R^{(d)}$ is generated over R_0 by $(R^{(d)})_1 = R_d$.

In other words, by taking a high enough Veronese subalgebra, we can ensure that it is generated in degree 1.

Proof. By Proposition 3.1.20, there exist $d', n_0 > 0$ such that $R_{d'} R_n = R_{n+d'}$ for all $n \geqslant n_0$. Let d be a multiply of d' which is greater than n_0. Then, for $n \geqslant d$, we have

$$R_{d+n} = R_{d'} R_{d-d_0+n} = \cdots = R_d R_n.$$

In particular, we have $R_{kd} = (R_d)^k$ for all $k \geqslant 1$, as desired. □

§§3.2. Filtrations and Topology

Definition 3.2.1. Let R be a ring. A filtration on R is a sequence of ideals $\langle I_n \rangle_{n \in \mathbb{N}}$ satisfying

$$R = I_0 \supseteq I_1 \supseteq I_2 \supseteq \cdots \quad \text{and} \quad I_n I_m \subseteq I_{n+m}$$

for all $n, m \geqslant 0$.
We say that $(R, \langle I_n \rangle_{n \in \mathbb{N}})$ is a filtered ring.

Given such a filtered ring, and an R-module M, a filtration on M is a sequence of R-submodules $\langle M_n \rangle_{n \in \mathbb{N}}$ satisfying

$$M = M_0 \supseteq M_1 \supseteq M_2 \supseteq \cdots \quad \text{and} \quad I_n M_m \subseteq M_{n+m}$$

for all $n, m \geqslant 0$.

Example 3.2.2. Let R be any ring, $I \subseteq R$ an ideal, and M an R-module. The I-adic filtration on R is the sequence $\langle I^n \rangle_{n \geqslant 0}$. Corresponding to this filtration, we have the filtration on M given by $\langle I^n M \rangle_{n \geqslant 0}$.

Example 3.2.3. Let R be a graded ring with grading $\langle R_n \rangle_{n \geqslant 0}$. Set $I_n := R_{\geqslant n} = \bigoplus_{i \geqslant n} R_i$. Then, $\langle I_n \rangle_{n \geqslant 0}$ is a filtration on R.

Definition 3.2.4. Let $(R, \langle I_n \rangle_{n \geqslant 0})$ be a filtered ring. The associated graded ring $\operatorname{gr}(R)$ is defined by

$$\operatorname{gr}(R) := R/I_1 \oplus I_1/I_2 \oplus I_2/I_3 \oplus \cdots .$$

This has the natural structure of a graded ring.

Correspondingly, if we have a filtered module $(M, \langle M_n \rangle_{n \geqslant 0})$, then we define

$$\operatorname{gr}(M) := M/M_1 \oplus M_1/M_2 \oplus M_2/M_3 \oplus \cdots .$$

$\operatorname{gr}(M)$ is a graded $\operatorname{gr}(R)$-module.

Definition 3.2.5. A topological ring R is a ring with a topology such that the following three maps are continuous:

- $+ : R \times R \to R$, $(x, y) \mapsto x + y$;
- $\cdot : R \times R \to R$, $(x, y) \mapsto xy$;
- $- : R \to R$, $x \mapsto -x$.

R is said to have a linear topology if 0 has a neighbourhood basis of ideals (that is, there is a collection of ideals $\mathcal{I}$ such that any neighbourhood of 0 contains an ideal $I \in \mathcal{I}$).

Note for any fixed $x \in R$, the translation map $T_x : R \to R$ defined by $y \mapsto x + y$ is a homeomorphism which takes 0 to x. Thus, studying neighbourhoods of 0 is sufficient.

Note that if $\langle I_n \rangle_{n \geqslant 0}$ is a filtration on a ring R, then the collection of all cosets $\{x + I_n : x \in R, n \geqslant 0\}$ is a basis for a topology on R. Indeed, it is clear that the union is all of R. Suppose that $z \in (x + I_n) \cap (y + I_m)$. Then, check that

$$z \in (z + I_{n+m}) \subseteq (x + I_n) \cap (y + I_m).$$

Definition 3.2.6. Given a filtration $\langle I_n \rangle_{n \geqslant 0}$ on R, the topology generated by the basis $\{x + I_n : x \in R, n \geqslant 0\}$ is called the topology induced by $\langle I_n \rangle_{n \geqslant 0}$.

Similarly, given a filtration $\langle M_n \rangle_{n \geqslant 0}$ on an R-module M, one gives M a topology.

This is the topology that we will be focusing on now.

Proposition 3.2.7. Let $\langle I_n \rangle_{n \geqslant 0}$ be a filtration on R. Then, R is a topological ring under the induced topology. (Similarly, M is a topological R-module.)

Proof. For $x, y \in R$ and $n \geqslant 0$, note that

$$\begin{aligned} (x + I_n) + (y + I_n) &\subseteq x + y + I_n, \\ (x + I_n) \cdot (y + I_n) &\subseteq xy + I_n, \\ -(x + I_n) &= -x + I_n. \end{aligned}$$

The continuity of the three operations now follows. The reader may formulate the definition of a topological module and prove the result similarly. □

Observation 3.2.8. Note that the I_n are clopen subsets of R. Indeed, each I_n by virtue of being a basis element. On the other hand, we can write the complement as a union of open sets as well: $R \setminus I_n = \bigcup_{x \notin I_n} (x + I_n)$.

Similarly, each $x + I_n$ is a clopen subset.

Example 3.2.9. We consider the $\mathfrak{m}$-adic topology on R for the following cases.

1. $R = \mathbb{Z}$, $\mathfrak{m} = (p)$ for some prime p.
   In this topology, x and y are "close" if $x - y$ is divisible by a "large" power of p.

2. $R = k[x, y]$, $\mathfrak{m} = (x, y)$.
   Here, f and g are "close" if $f - g \in \mathfrak{m}^i$ for "large" i (i.e., all monomials appearing in $f - g$ have degree $\geqslant i$).

Proposition 3.2.10. $\langle I_n \rangle_{n \geqslant 0}$ induces a Hausdorff topology iff $\bigcap_{n \geqslant 0} I_n = 0$.
Similarly, a filtered R-module M is Hausdorff iff $\bigcap_{n \geqslant 0} M_n$.

Proof. We prove the statement about rings and leave the other one to the reader.

($\Rightarrow$) Suppose $\bigcap_{n \neq 0} I_n \neq 0$. Pick a nonzero y in the intersection. Then, y and 0 cannot be separated.

($\Leftarrow$) As noted, each I_n is closed. Thus, the intersection being 0 implies that $\{0\}$ is closed. By continuity of multiplication, the diagonal is then closed in $R \times R$, which is equivalent to R being Hausdorff. □

An alternate proof for ($\Leftarrow$) direction: Let $x, y \in R$ be distinct. Pick N large such that $x - y \notin I_N$. Then, $x + I_N$ and $y + I_N$ are disjoint neighbourhoods.

Proposition 3.2.11. Let M be a filtered R-module, and $N \leqslant M$ a submodule. Then,

$$\overline{N} = \bigcap_{n \geqslant 0} (N + M_n).$$

Proof. Let $x \in M$. $x \in \overline{N}$ iff every basic neighbourhood of x intersects N iff $(x + M_n) \cap N \neq \varnothing$ for all n. This happens iff $x \in N + M_n$ for all n. □

§§3.3. The Artin-Rees Lemma

We wish to prove the Artin-Rees Lemma. Loosely speaking, it tells us the following (under Noetherian hypotheses): Suppose $N \subseteq M$ is a submodule, and $I \subseteq R$ an ideal. Give M the I-adic topology. Now, we can give N a topology in two ways: either the subspace topology, or the I-adic topology. The Artin-Rees lemma gives us that the two are the same.

We will assume the following setup for this subsection.

Setup. R is a Noetherian ring. $I \subseteq R$ is an ideal, and R is given the I-adic filtration. M is a finitely generated R-module with some filtration $\langle M_n \rangle_{n \geqslant 0}$. $N \subseteq M$ is an R-submodule.
$S := R[It]$ is the Rees algebra (as defined in Example 3.1.5).

Definition 3.3.1. The filtration $\langle M_n \rangle_{n \geqslant 0}$ is said to be I-good if $IM_n = M_{n+1}$ for $n \gg 0$.

Lemma 3.3.2. $\langle M_n \rangle_{n \geqslant 0}$ is I-good iff $F = \bigoplus_{n \geqslant 0} M_n t^n$ is a finitely generated S-module.

As before, the variable t^n in the direct sum above is for bookkeeping. This definition makes F a graded S-module. (Indeed, the definition of filtration implies that $I_n t^n M_m t^m \subseteq M_{n+m} t^{n+m}$.)

Proof. ($\Leftarrow$) Suppose F is a finitely generated S-module. Note that S is finitely generated in degree 1. Thus, Porism 3.1.21 tells us that $S_1 M_n = M_{n+1}$ for $n \gg 0$. This translates to $IM_n = M_{n+1}$ for $n \gg 0$, which is precisely being I-good.

($\Rightarrow$) Let n_0 be such that $IM_n = M_{n+1}$ holds for all $n \geqslant n_0$.
Now, each of $M_0, \ldots, M_{n_0}$ is finitely generated (over $R = S_0$) and the above equation shows that using generators for these is enough to generate everything. □

Lemma 3.3.3. S is Noetherian.

Proof. Note that $S_0 = R$ is Noetherian, and S is a finitely generated R-algebra. (Indeed, if $x_1, \ldots, x_n$ generate I as an R-ideal, then $x_1 t, \ldots, x_n t$ generate S as an R_0-algebra.) □

Theorem 3.3.4 (Artin-Rees Lemma)**.** Let R be a Noetherian ring, $I \subseteq R$ an ideal, M a finitely generated R-module, and $N \subseteq M$ a submodule.
Then,

(i) there exists $c \geqslant 1$ such that $I^{n+c} M \cap N = I^n (I^c M \cap N)$ for all $n \geqslant 1$;

(ii) there exists $c \geqslant 1$ such that $I^{n+c} M \cap N \subseteq I^n N$ for all $n \geqslant 1$;

(iii) the subspace topology on N (when M is given the I-adic topology) agrees with the I-adic topology on N.

In the statement of (ii), we can add some more obvious inclusions:

$$I^{n+c} M \subseteq I^{n+c} M \cap N \subseteq I^n N \subseteq I^n M.$$

This shows how (ii) implies (iii). It is also clear that (i) implies (ii). So we shall only prove (i).

Proof. Note that (i) is equivalent to proving the filtration $\langle I^n M \cap N \rangle_{n \geqslant 0}$ on N is I-good. Clearly, the I-adic filtration on M is I-good. Thus, $\bigoplus_{n \geqslant 0} I^n M$ is a finitely generated S-module (Lemma 3.3.2).

Since S is Noetherian (Lemma 3.3.3), it follows that the submodule $\bigoplus_{n \geqslant 0}(I^n M \cap N)$ is finitely generated.
Now, using Lemma 3.3.2 again shows that $\langle I^n M \cap N \rangle_{n \geqslant 0}$ is I-good, as desired. □

§§3.4. Krull's intersection theorems

We now use the Artin-Rees lemma to deduce that certain infinite intersections are zero. In view of Proposition 3.2.10, it is saying that a certain module is Hausdorff.

Theorem 3.4.1. Let $(R, \mathfrak{m})$ be a local Noetherian ring, and $I \subsetneq R$ a proper ideal. If M is a finitely generated R-module, then

$$\bigcap_{n \geqslant 0} I^n M = 0.$$

That is, the I-adic topology on M is Hausdorff.

In particular, $\bigcap_{n \geqslant 0} I^n = 0$.

A special case is $I = \mathfrak{m}$.

Proof. Let $N := \bigcap_{n \geqslant 0} \mathfrak{m}^n M$. We wish to show that $N = 0$. Let c be as given by the Artin-Rees Lemma 3.3.4. Note that $N \subseteq \mathfrak{m}^{1+c} M$, by definition of N. Thus, we have

$$N \subseteq \mathfrak{m}^{1+c} M \cap N \subseteq \mathfrak{m} N.$$

Now, using NAK, we see that $N = 0$, as desired. □

Aliter. We use topological language in this proof. As before, let N be the intersection.
Artin-Rees Lemma 3.3.4 tells us that the $\mathfrak{m}$-adic topology on N is the restriction of the $\mathfrak{m}$-adic topology on M. Note that N is contained in every $\mathfrak{m}$-adic neighbourhood of 0 in M. Thus, only neighbourhood of 0 in N is N itself.
It follows that N has the indiscrete topology. But $\mathfrak{m}N$ is a nonempty open subset in the $\mathfrak{m}$-adic topology. Thus, $N = \mathfrak{m}N$ and hence, $N = 0$ by NAK. □

Porism 3.4.2. If R is a commutative ring, M a finitely generated R-module, and I is contained in the Jacobson radical of R, then $\bigcap_{n \geqslant 0} I^n M = 0$.

Corollary 3.4.3. Let R be a Noetherian ring, M a finitely generated R-module, and I be an ideal contained in the Jacobson radical. Then, every submodule $N \leqslant M$ is closed in the I-adic topology. In particular, every ideal of R is closed in the I-adic topology.

Proof. M/N is a Hausdorff space in the I-adic topology. In particular, $\{0\}$ is closed. The map $\pi : M \to M/N$ is continuous (both have the I-adic topology). Thus, $N = \pi^{-1}(0)$ is closed. $\square$

Theorem 3.4.4. Let R be a Noetherian integral domain (not necessarily local).
Let $I \subsetneq R$ be a proper ideal. Then,

$$\bigcap_{n \geqslant 0} I^n = 0.$$

Proof. Let $\mathfrak{m} \supseteq I$ be maximal. Since R is a domain, have the inclusion $R \hookrightarrow R_{\mathfrak{m}}$. Thinking of R and $R_{\mathfrak{m}}$ as subrings of the fraction field, we note the containments

$$\begin{aligned} \bigcap_{n \geqslant 0} I^n &\subseteq \left(\bigcap_{n \geqslant 0} I^n \right) R_{\mathfrak{m}} \\ &\subseteq \bigcap_{n \geqslant 0} (IR_{\mathfrak{m}})^n = 0, \end{aligned}$$

where the last equality follows from Theorem 3.4.1, since $R_{\mathfrak{m}}$ is local. $\square$

Example 3.4.5. The theorems breaks down if drop both the hypotheses of being local and integral domain.
Indeed, take any ring R with a nontrivial idempotent e. Then, the ideal (e) is an idempotent ideal and hence $\bigcap_{n \geqslant 0} (e)^n = (e) \neq 0$. (Note that this is possible when R is Noetherian, finite even.)

If R is not assumed Noetherian, then one cannot conclude even with the integral domain and local hypothesis. Consider $R = \mathbb{Z}_{(p)}[p^{1/p}, p^{1/p^2}, \ldots]$.
Then, R is a local domain with maximal ideal $\mathfrak{m} = (p^{1/p}, p^{1/p^2}, \ldots)$. But $\mathfrak{m}$ is idempotent.

§4. Dimension Theory

We may tacitly be assuming that $M \neq 0$ in many places, when we talk about dimension. It may be safe to assume that we are defining $\dim(M) = -1$ when $M = 0$.

§§4.1. Integer valued polynomials

As before, we continue with the notation that $0 \in \mathbb{N}$. We use $\mathbb{N}_{\geqslant 1}$ to denote the set of positive integers.

Definition 4.1.1. A function $f : \mathbb{Z} \to \mathbb{Z}$ is an eventual polynomial if there exists a polynomial $P(t) \in \mathbb{Q}[t]$ such that

$$f(n) = P(n) \quad \text{for all } n \gg 0.$$

The degree of f is defined to be the degree of P.

Note that the polynomial P is uniquely determined. For if Q is another such polynomial, then $P - Q$ vanishes at infinitely many points. Thus, the degree is well-defined.

Definition 4.1.2. For a function $f : \mathbb{Z} \to \mathbb{Z}$, we define the difference function $\Delta f : \mathbb{N}_{\geqslant 1} \to \mathbb{Z}$ by

$$(\Delta f)(n) := f(n) - f(n-1).$$

Proposition 4.1.3. Let $f : \mathbb{Z} \to \mathbb{Z}$ be any function. The following are equivalent:

1. f is eventually polynomial.
2. Δf is eventually polynomial.

In this case, we have $\deg(f) = \deg(\Delta f) + 1$.

We are not worrying about degree of the zero polynomial. The reader can take care of that.

Proof. If f agrees with P eventually, then Δf agrees with ΔP eventually. In this case, we clearly have $\deg(f) = \deg(\Delta f)$.

Now suppose that Δf is eventually a polynomial. Assume $Q(t) \in \mathbb{Q}[t]$ and $N > 1$ are such that

$$\Delta f(n) = Q(n)$$

for $n \geqslant N$.

For $n > N$, note that we have $f(n) = f(n-1) + \Delta f(n)$. Adding such equalities gives us

$$f(n) = f(N) + \sum_{k=N}^{n-1} \Delta f(k) = f(N) + \sum_{k=N}^{n-1} Q(k).$$

Thus, for a constant $C \in \mathbb{Z}$, we can write

$$f(n) = C + \sum_{k=0}^{n-1} Q(k).$$

But now note that the sum is itself a polynomial of degree $\deg(Q) + 1$. This finishes the proof. $\square$

Definition 4.1.4. For $n \geqslant 0$, define the rational polynomial $\binom{t}{n} \in \mathbb{Q}[t]$ as

$$\binom{t}{n} := \frac{t(t-1)\cdots(t-(n-1))}{n!}.$$

Note that $\binom{t}{n}$ is a polynomial with (non-integer) rational coefficients, but takes integer values at all integers. We show that these polynomials are essentially all.

Proposition 4.1.5. Let $P(t) \in \mathbb{Q}[t]$. The following are equivalent:

(i) $P(t) = \sum_n c_n \binom{t}{n}$ for some sequence of integers $\langle c_n \rangle_{n \geqslant 0}$ eventually zero.

(ii) $P(n) \in \mathbb{Z}$ for all $n \in \mathbb{Z}$.

(iii) $P(n) \in \mathbb{Z}$ for all $n \gg 0$.

Proof. (i) $\Rightarrow$ (ii) $\Rightarrow$ (iii) is clear.

(iii) $\Rightarrow$ (ii): Write $P(x) = Q(x)/M$ for $Q(x) \in \mathbb{Z}[x]$ and $M \in \mathbb{N}_{\geqslant 1}$.
If there exists $n \in \mathbb{Z}$ such that M does not divide $Q(n)$, then M does not divide $Q(n+M)$ either.
In other words, if $P(n) \notin \mathbb{Z}$, then $P(n+M), P(n+2M), \ldots$ are also not in $\mathbb{Z}$.

(ii) $\Rightarrow$ (i): Let $d := \deg(P)$. By linear algebra, we can write

$$P(t) = \sum_{k=0}^{d} a_k \binom{t}{k},$$

for some choice of rationals $a_k \in \mathbb{Q}$.

Now, evaluating the above sequentially at $t = 0, \ldots, d$ shows that each a_k is an integer. (Note that for such t, $\binom{t}{k}$ vanishes when $k > t$ and equals 1 when $k = t$.) $\square$

Remark 4.1.6. The above holds even if we started with $P(t) \in \mathbb{R}[t]$ or $\mathbb{C}[t]$. Lagrange interpolation immediately tells us that such a P must have rational coefficients.

§§4.2. Embedding dimension

Definition 4.2.1. Let $(R, \mathfrak{m}, k)$ be a local Noetherian ring. The embedding dimension of R is defined as

$$\operatorname{emb.dim}(R) := \dim_k(\mathfrak{m}/\mathfrak{m}^2).$$

By Nakayama's lemma, the above is equal to the minimum number of generators needed to generate $\mathfrak{m}$ (as an R-ideal). This is not a very good notion. We try capture information by looking at all quotients of the form $\mathfrak{m}^k/\mathfrak{m}^{k+1}$.

§§4.3. Dimension à la Hilbert polynomials

We now define some functions, which we show are eventually polynomial. Then we define dimension using the degree.

Definition 4.3.1. Let $(R, \mathfrak{m}, k)$ be a local Noetherian ring. The function

$$n \mapsto \ell(R/\mathfrak{m}^n)$$

is eventually polynomial. This function is called the Hilbert-Samuel function.
The corresponding polynomial is called the Hilbert-Samuel polynomial. Its degree is defined to be the dimension of R, denoted $\dim(R)$.

More generally, if $M \neq 0$ is a finitely generated R-module, then

$$n \mapsto \ell(M/\mathfrak{m}^n M)$$

is eventually polynomial, whose degree defines $\dim(M)$. We define the Hilbert-Samuel polynomial $H_M(t) \in \mathbb{Q}[t]$ to be the polynomial such that $H_M(n) = \ell(M/\mathfrak{m}^n M)$ for $n \gg 0$.

Moreover, $\dim(M) \leqslant \operatorname{emb.dim}(R)$. (In particular, $\dim(R) \leqslant \operatorname{emb.dim}(R)$.)

These assertions are Proposition 4.3.7.

In the above, ℓ denotes the length of the R-module. Note that $M/\mathfrak{m}^n M$ is annihilated by $\mathfrak{m}^n$ and is hence, Artinian (Corollary 1.2.9) and therefore has finite length. We also have

$$\ell(M/\mathfrak{m}^n) = \sum_{i=0}^{n-1} \dim_k(\mathfrak{m}^i M/\mathfrak{m}^{i+1} M).$$

Definition 4.3.2. Let k be a field, and $M \neq 0$ be a finitely generated graded module over the polynomial ring $k[x_1, \ldots, x_r]$. Then, the Hilbert function, defined by

$$n \mapsto \sum_{i \leqslant n} \dim_k(M_i)$$

is eventually a polynomial of degree $\leqslant r$ (Proposition 4.3.5).

The corresponding polynomial is denoted by $f_M^+(t) \in \mathbb{Q}[t]$, and is called the Hilbert polynomial. We also define $f_M := \Delta f_M^+$.

Note that in the above, it makes sense to talk about $\dim_k(M_i)$ since k is in fact a subring of the polynomial ring. (As opposed to earlier, when we cannot talk about $\dim_k(R/\mathfrak{m}^n)$.) Moreover, these dimensions are finite, by Proposition 3.1.18.

Example 4.3.3 (Dimension of a field)**.** Let k be a field (and hence, a local ring), and $M \neq 0$ be a finitely generated k-module. Then, $\dim(M) = 0$. In particular, $\dim(k) = 0$. (Note the contrast from the usual vector space dimension.)

To see this, note that the maximal ideal here is 0. Thus, $\ell(M/\mathfrak{m}^n M) = \ell(M)$ for all n. Thus, the Hilbert-Samuel polynomial is constant, i.e., its degree is zero.

Example 4.3.4 (Dimension of a polynomial ring)**.** Let k be a field, and $R = k[x_1, \ldots, x_d]_{(x_1, \ldots, x_d)}$.
Note that R is a local ring with maximal ideal $\mathfrak{m} = (x_1, \ldots, x_d)$. We claim that $\dim(R) = d$.

To see this, note that $\mathfrak{m}^n/\mathfrak{m}^{n+1}$ has a k-basis given by (the images of) the monomials of degree n. (Here we are looking at k as the quotient $R/\mathfrak{m}$ and not the subring $k \subseteq R$.) Thus,

$$\dim_k(\mathfrak{m}^n/\mathfrak{m}^{n+1}) = \binom{d+n-1}{d-1}.$$

Thus, the above is a polynomial (in n) of degree $d-1$. In turn, $\ell(M/\mathfrak{m}^n)$ is a polynomial of degree d.

Proposition 4.3.5. The assertions made in Definition 4.3.2 hold.

Proof. Define $g_M : \mathbb{Z} \to \mathbb{Z}$ to be $g_M(n) = \dim_k(M_n)$. Note that this is the difference function of the one given in the definition. Thus, by Proposition 4.1.3, it suffices to show that that g_M is eventually polynomial.

We repeatedly use the following fact: If

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

is an exact sequence of *graded* R-modules, then $g_M = g_{M'} + g_{M''}$.

Note that as a consequence, we get that if we there is a filtration

$$0 = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_t,$$

then

$$g_{M_t} = g_{M_t/M_{t-1}} + \cdots + g_{M_1/M_0}.$$

In particular, if all the functions on the right are eventually polynomials of degree d, then the same is true for g_{M_t}. (t here is fixed.)

Another trick that we will use is that we will consider modules annihilated by x_r, so that we can view them as modules over a smaller polynomial ring. Note that the function g_M does not change.

We prove the statement by induction on r.

If $r = 0$, then the statement is clear since g_M is eventually zero. Thus, f_M^+ is a constant polynomial.

Since x_r is homogeneous, we have a chain of graded submodules of M given by

$$0 \subseteq \operatorname{ann}_M(x_r) \subseteq \operatorname{ann}_M(x_r^2) \subseteq \cdots.$$

Since M is Noetherian, then above stabilises to some M'.

Note that each $\operatorname{ann}_M(x_r^i)/\operatorname{ann}_M(x_r^{i+1})$ is a finitely generated module over the polynomial ring in $r-1$ variables. By induction, each of these modules have a Hilbert polynomial[3] of degree $\leqslant r-1$. Thus, by our observation about filtrations, the same is true for M'.

Thus, we have shown that $g_{M'}$ is a eventually a polynomial of degree $\leqslant r-1$. Since we have the graded exact sequence

$$0 \to M' \to M \to M/M' \to 0,$$

it suffices to prove that $g_{M/M'}$ is eventually a polynomial of degree $\leqslant r$. Thus, we may replace M with M/M'. The gain is that x_r is a nonzerodivisor on M/M'.

Now, note that we have a graded exact sequence

$$0 \to M(-1) \xrightarrow{x_r} M \to M/(x_r) \to 0.$$

Thus, we have

$$g_M - g_{M(-1)} = g_{M/(x_r)}.$$

Again, by induction, the right function is eventually polynomial of degree $\leqslant r-1$. Moreover the left function is exactly Δg_M. Thus, Proposition 4.1.3 tells us that g_M is eventually a polynomial of degree $\leqslant r$. □

[3] By this, we mean that the corresponding function is eventually polynomial for them.

Remark 4.3.6. Note that in the above proof, we did not really use that $k[x_1, \ldots, x_r]$ is a polynomial ring. Rather, all we needed was a finitely generated graded k-algebra, with generators in degree 1. (The proof would have to be slightly modified if the generators are homogeneous of different degrees.)

Proposition 4.3.7. The assertions made in Definition 4.3.1 hold.

Proof. We prove the result for modules. Consider the associated graded ring $\mathrm{gr}(R) = \bigoplus_{n \geqslant 0} \mathfrak{m}^n/\mathfrak{m}^{n+1}$ and the associated graded module $\mathrm{gr}(M) = \bigoplus_{n \geqslant 0} \mathfrak{m}^n M/\mathfrak{m}^{n+1}M$.

Let $r = \mathrm{emb.dim}(R)$. Then, we can generate $\mathfrak{m}$ by some $t_1, \ldots, t_r \in \mathfrak{m}$. Note that $\mathrm{gr}(R)_0 = R/\mathfrak{m} = k$. We have a surjective map of graded k-algebras

$$k[x_1, \ldots, x_r] \to \mathrm{gr}(R)$$

given by

$$x_i \mapsto \overline{t_i}.$$

(Note that x_i and $\overline{t}_i \in \mathfrak{m}/\mathfrak{m}^2$ both do have degree 1.)

Thus, $\mathrm{gr}(M)$ is a finitely generated graded $k[x_1, \ldots, x_r]$-module. Now, by Proposition 4.3.5, the function

$$n \mapsto \dim_k(\mathfrak{m}^n M/\mathfrak{m}^{n+1}M)$$

is eventually polynomial, of degree $\leqslant r - 1$.

In turn, the Hilbert-Samuel function

$$n \mapsto \sum_{i=0}^{n-1} \dim_k(\mathfrak{m}^i M/\mathfrak{m}^{i+1}M)$$

is eventually a polynomial of degree $\leqslant r$. $\square$

§§4.4. Properties of dimension

To summarise, we have shown the following:

- If M is a finitely generated module over $(R, \mathfrak{m})$, then we have a polynomial H_M such that $H_M(n) = \ell(M/\mathfrak{m}^n M)$ for large n.
- If M is a finitely generated graded module over $k[x_1, \ldots, x_r]$, then there are polynomials f_M, f_M^+ such that

  $$f_M(n) = \dim_k(M_n) \quad \text{and} \quad f_M^+(n) = \sum_{i \leqslant n} \dim_k(M_i)$$

  for large n.

We now wish to see how the degrees of these polynomials interact with exact sequences. It is direct for the graded case. The local case requires more work.

Proposition 4.4.1. Suppose we have an exact sequence

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

of graded modules over $k[x_1, \ldots, x_r]$. Then,

$$f_M = f_{M'} + f_{M''} \quad \text{and} \quad f_M^+ = f_{M'}^+ + f_{M''}^+.$$

Consequently, $\deg(f_M) = \max(\deg(f_{M'}), \deg(f_{M''}))$.

Proof. The first result about the sum is clear since the exact sequence is graded, giving an exact sequence of k-vector space.
The statement about degree follows since the leading coefficients of the concerned polynomials are positive. $\square$

Proposition 4.4.2. Let $(R, \mathfrak{m})$ be a Noetherian local ring. Let

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

be an exact sequence of finite R-modules. Then, $\dim(M) = \max(\dim(M'), \dim(M''))$.

Proof. Note that since $\otimes_R R/\mathfrak{m}^n$ is a right-exact functor, we have the exact sequence

$$M'/\mathfrak{m}^n M' \to M/\mathfrak{m}^n M \to M''/\mathfrak{m}^n M'' \to 0.$$

We show that the genuine kernel is a "good approximation" for the leftmost term there. To this end, let $M'_n := M'/\mathfrak{m}^n M'$, and let K_n be the genuine kernel, i.e., the sequence

$$0 \to K_n \to M/\mathfrak{m}^n M \to M''/\mathfrak{m}^n M'' \to 0 \tag{4.1}$$

is exact.

Note that $K_n \cong (M' + \mathfrak{m}^n M)/\mathfrak{m}^n M \cong M'/(N' \cap \mathfrak{m}^n N)$. In particular, we have a surjection $M'_n \twoheadrightarrow K_n$ and thus, $\ell(K_n) \leqslant \ell(M'_n)$.

On the other hand, Artin-Rees Lemma 3.3.4 implies the existence of $c \geqslant 1$ such that

$$M' \cap \mathfrak{m}^n M \subseteq \mathfrak{m}^{n-c} M'$$

for all $n \geqslant c$.

Thus, for $n \geqslant c$, we have

$$\ell(M'_{n-c}) \leqslant \ell(K_n) \leqslant \ell(M'_n). \tag{4.2}$$

Note that (4.1) tells us that the Hilbert polynomials satisfy

$$H_M(n) = H_{M''}(n) + \ell(K_n) \tag{4.3}$$

for all n.

This implies that $n \mapsto \ell(K_n)$ is eventually a polynomial. (4.2) shows that $H_{M'}$ has the same degree as this. The result now follows from (4.3) since the leading coefficients of the polynomials in questions are positive. □

Corollary 4.4.3. If M is a Noetherian module over a Noetherian local ring, then $\dim(M^{\oplus n}) = \dim(M)$ for all $n \geqslant 1$.

Theorem 4.4.4. Let R be a local Noetherian ring. Then, $\dim(R) = \dim(R/\operatorname{nil}(R))$.

$\operatorname{nil}(R)$ above denotes the ideal of nilpotents.

Proof. Let $I = \operatorname{nil}(R)$. Since R is Noetherian, we have $I^n = 0$ for $n \gg 0$. Thus, it suffices to prove that

$$\dim(R/I^k) = \dim(R/I^{k+1})$$

for all $k \geqslant 1$.

Note that we have an exact sequence

$$0 \to I^k/I^{k+1} \to R/I^{k+1} \to R/I^k \to 0$$

of R-modules.

In view of Proposition 4.4.2, it suffices to show that $\dim(I^k/I^{k+1}) \leqslant \dim(R/I^{k+1})$.

Note that I^k/I^{k+1} is a (finitely generated) R/I^k-module. Thus, we have a surjection of the form

$$\bigoplus_{i=1}^{N} R/I^k \to I^k/I^{k+1} \to 0.$$

Corollary 4.4.3 and Proposition 4.4.2 now imply that $\dim(R/I^k) \geqslant \dim(I^k/I^{k+1})$. □

Theorem 4.4.5. [Dimension only depends on support] Let $(R, \mathfrak{m})$ be a local Noetherian, and $M \neq 0$ a finitely generated R-module. Then,

$$\dim(M) = \max_{\substack{\mathfrak{p} \in \operatorname{Supp}(M) \\ \mathfrak{p} \text{ minimal}}} \dim(R/\mathfrak{p}).$$

In particular, $\dim(R) = \max_{\mathfrak{p}} \dim(R/\mathfrak{p})$, where $\mathfrak{p}$ runs over all minimal primes.

Proof. There exists a filtration of M of the form

$$0 = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_m = M$$

such that each M_{i+1}/M_i is isomorphic to some $R/\mathfrak{p}_i$, with $\mathfrak{p}_i \in \operatorname{Supp}(M)$.

Using Proposition 4.4.2 successively on exact sequences of the form $0 \to M_i \to M_{i+1} \to M_{i+1}/M_i \to 0$, we see that

$$\dim(M) = \max_i \dim(R/\mathfrak{p}_i) \leqslant \sup_{\mathfrak{p} \in \operatorname{Supp} M} \dim(R/\mathfrak{p}).$$

To prove the reverse inequality, we fix $\mathfrak{p} \in \operatorname{Supp}(M)$ and show that $\dim(R/\mathfrak{p}) \leqslant \dim(M)$.

Since $M_\mathfrak{p} \neq 0$ and localisation is exact, we must have that $(R/\mathfrak{p}_i)_\mathfrak{p} \neq 0$ for some i[4] and hence, $\mathfrak{p}_i \subseteq \mathfrak{p}$. This gives us $\dim(R/\mathfrak{p}) \leqslant \dim(R/\mathfrak{p}_i)$.
This also shows that the supremum is indeed a maximum.

To see that the maximum can be taken over minimal primes, first note that we clearly have

$$\max_{\mathfrak{p} \in \operatorname{Supp} M} \dim(R/\mathfrak{p}) \geqslant \max_{\substack{\mathfrak{p} \in \operatorname{Supp}(M) \\ \mathfrak{p} \text{ minimal}}} \dim(R/\mathfrak{p}).$$

For the other direction, note that if $\mathfrak{p} \in \operatorname{Supp} M$, then $\mathfrak{p} \supseteq \mathfrak{q}$ for some minimal $\mathfrak{q} \in \operatorname{Supp} M$ and $\dim(R/\mathfrak{p}) \leqslant \dim(R/\mathfrak{q})$. $\square$

Corollary 4.4.6. With the same hypothesis, $\dim(M) = \dim(R/\operatorname{ann}(M))$.
In particular, $\dim(M) \leqslant \dim(R)$.

Proof. It suffices to show that $\operatorname{Supp}(M) = \operatorname{Supp}(R/\operatorname{ann}(M))$. But note that $\operatorname{Supp}(M) = V(\operatorname{ann}(M))$, since M is finitely generated. But $V(\operatorname{ann}(M)) = \operatorname{Supp}(R/\operatorname{ann}(M))$. $\square$

Theorem 4.4.7. Let $(R, \mathfrak{m})$ be local, and $M \neq 0$ be a finitely generated R-module.
Let $x \in \mathfrak{m}$ be a nonzerodivisor on M. Then,

$$\dim(M/xM) = \dim(M) - 1.$$

Proof. We have the exact sequence

$$0 \to xM \to M \to M/xM \to 0.$$

Thus,

$$0 \to xM/(xM \cap \mathfrak{m}^n M) \to M/\mathfrak{m}^n M \to M/(xM + \mathfrak{m}^n M) \to 0$$

[4]Indeed, localise the filtration $M_0 \subseteq \cdots \subseteq M_m$ at $\mathfrak{p}$. Since $(M_m)_\mathfrak{p} \neq 0$, there is some i with $(M_i)_\mathfrak{p} \neq (M_{i+1})_\mathfrak{p}$.

is an exact sequence for all n. In terms of the Hilbert polynomials, we see that

$$H_M(n) = H_{M/xM}(n) + \ell(xM/(xM \cap \mathfrak{m}^n M)) \tag{4.4}$$

for $n \gg 0$. In particular, the rightmost term is eventually polynomial.

Note that since x is a nonzerodivisor, we have $xM \cong M$ and hence,

$$xM/(xM \cap \mathfrak{m}^n M) \cong M/N_n,$$

where $N_n = (\mathfrak{m}^n M :_M x) = \{a \in M : xa \in \mathfrak{m}^n M\}$. Indeed, N_n is the preimage of $xM \cap \mathfrak{m}^n M$ under the isomorphism $M \xrightarrow{x} xM$.

Note that since $x \in \mathfrak{m}$, we have $\mathfrak{m}^{n-1}M \subseteq N_n$ and hence,

$$\ell(M/N_n) \leqslant \ell(M/\mathfrak{m}^{n-1}M) \leqslant H_M(n-1)$$

for $n \gg 0$. Combining this with (4.4) gives

$$H_M(n) \leqslant H_{M/xM}(n) + H_M(n-1)$$

for $n \gg 0$. Thus, $H_{M/xM} \geqslant \Delta H_M$ eventually and hence, $\dim(M/xM) \geqslant \dim(M) - 1$.

We now need to prove the other direction of the inequality.

The Artin-Rees Lemma 3.3.4 tells us that there exists c such that $N_{n+c} \subseteq \mathfrak{m}^n M$ for all n.[5] Thus,

$$\ell(M/N_n) \geqslant \ell(M/\mathfrak{m}^{n-c}M) = H_M(n-c)$$

for $n \gg 0$. Since $M/N_n \cong xM/(xM \cap \mathfrak{m}^n M)$, (4.4) now tells us that

$$H_M(n) \geqslant H_{M/xM}(n) + H_M(n-c)$$

for $n \gg 0$.

Thus, $H_{M/xM}(n) \leqslant H_M(n) - H_M(n-c)$ and thus, the degree drops in the desired way giving us $\dim(M/xM) \leqslant \dim(M) - 1$. □

Using the above, we can prove a weaker inequality when x is possibly a zerodivisor.

Corollary 4.4.8. Let M be a finitely generated module over the local Noetherian ring $(R, \mathfrak{m})$.
If $x \in \mathfrak{m}$, then

$$\dim(M) - 1 \leqslant \dim(M/xM) \leqslant \dim(M).$$

In words, the dimension can drop by at most 1.

[5]Indeed, it tells us that there exists c such that $\mathfrak{m}^{n+c}M \cap xM \subseteq \mathfrak{m}^n(xM)$ for all n. Now, take preimages under the isomorphism $M \xrightarrow{x} xM$.

Proof. $\dim(M/xM) \leqslant \dim(M)$ is clear since M surjects onto M/xM.

Let N denote the x-torsion submodule of M, i.e., $N = \{a \in M : x^n a = 0 \text{ for some } n \geqslant 1\}$. Let $M'' = M/N$. Then, we have an exact sequence

$$0 \to N \to M \to M'' \to 0.$$

Tensoring with R/x gives us an exact sequence

$$0 \to N/xN \to M/xM \to M''/xM'' \to 0.$$

We only need to check that $N/xN \to M/xM$ is indeed an inclusion. This is equivalent to showing $N \cap (xM) \subseteq xN$. But this is is clear.[6]

Now, note that $\dim(M''/xM'') = \dim(M'') - 1$ since x is a nonzerodivisor on M'', by construction.
On the other hand, $\dim(N/xN) = \dim(N)$ since dimension only depends on the support (Theorem 4.4.5), and $\operatorname{Supp}(N/xN) = \operatorname{Supp}(N)$ since N is x-torsion.[7] We now apply Proposition 4.4.2 twice. We have

$$\begin{aligned}
\dim(M/xM) &= \max(\dim(M''/xM''), \dim(N/xN)) \\
&= \max(\dim(M'') - 1, \dim(N)) \\
&\geqslant \max(\dim(M'') - 1, \dim(N) - 1) \\
&= \max(\dim(M''), \dim(N)) - 1 = \dim(M).
\end{aligned}$$

□

Corollary 4.4.9. Let $(R, \mathfrak{m})$ be a (nonzero) local Noetherian ring of dimension zero. Then, every element of $\mathfrak{m}$ is a zerodivisor. In particular, if R is a domain, then R is a field.

Proof. Let $x \in \mathfrak{m}$ be arbitrary. If x is a nonzerodivisor, then

$$\dim(R) = \dim(R/xR) + 1 \geqslant 1,$$

a contradiction. □

Note that the above is a converse of sorts to Example 4.3.3. However, note that there do exist rings of dimension zero which are not fields. Indeed, Artinian local rings are precisely these zero dimensional Noetherian local rings.
We have already shown most of this in Corollary 1.2.12; we only need to show that the notion of $\dim(R)$ is the same.

[6] If $a \in M$ and $xa \in N$, then $x^n(xa) = 0$ for some n and hence, $a \in N$.

[7] In general, $\operatorname{Supp}(N/xN) = \operatorname{Supp}(N) \cap V(x)$. Now, since N is x-torsion, if $N_{\mathfrak{p}} \neq 0$, we must have $x \in \mathfrak{p}$. Thus, $\operatorname{Supp}(N) \subseteq V(x)$.

§§4.5. Characterisation of dimension

For this discussion, assume that $(R, \mathfrak{m}, k)$ is local Noetherian. We showed that the function $n \mapsto \ell(R/\mathfrak{m}^n)$ is eventually polynomial, and defined $\dim(R)$ to be the degree of this (unique) polynomial.

We also showed the following properties.

(P1) $\dim(R) = \max_{\mathfrak{p} \text{ a minimal prime}} \dim(R/\mathfrak{p})$.
(Note that R has only finitely many minimal primes.)

(P2) $\dim(R) = 0$ if R is a field (Example 4.3.3).

(P3) If R is a domain, and $x \in \mathfrak{m} \setminus \{0\}$, then $\dim(R/(x)) = \dim(R) - 1$.

Note that (P3) above implies the following.

(P3') If R is a domain which is not a field, then $\dim(R) = \sup_{x \in \mathfrak{m} \setminus \{0\}} \dim(R/xR) + 1$.

Theorem 4.5.1. (P1)-(P3) uniquely characterise the dimension function. In other words, if we are given a function

$$d : \{\text{local Noetherian rings}\} \to \mathbb{Z}_{\geqslant 0}$$

satisfying (P1)-(P3), then $d = \dim$.

The statement is true even if we replace (P3) with (P3').

(We are ignoring any set-theoretic issues and using the term "function".)

Proof. Note that if d satisfies (P3), then it satisfies (P3'). Thus, we may assume that d satisfies (P1), (P2), (P3'), and show that $d = \dim$.

It suffices to show $d(R) = \dim(R)$ whenever R is a domain. It then follows for a general ring by using (P1).

We prove this by induction on $\dim(R)$.

$\dim(R) = 0$: In this case, R is a field, by Corollary 4.4.9. But then $d(R) = 0$, by (P2).

$\dim(R) > 0$: Then, R is not a field (by (P2)). By (P3'), there exists $x \in \mathfrak{m} \setminus \{0\}$ such that $d(R) = d(R/xR) + 1$.
Note that the ring $R' = R/xR$ has dimension equal to $\dim(R) - 1$.[8] We wish to use the inductive hypothesis, but R' need not be a domain. But note that $R'/\mathfrak{p}$ is, for every $\mathfrak{p} \in \operatorname{Spec}(R')$.
Moreover, $\dim(R'/\mathfrak{p}) \leqslant \dim(R') < \dim(R)$ due to (P1). Thus, the induction hypothesis applies to all such quotients. Now using (P1) again, we see

$$d(R') = \max_{\mathfrak{p} \text{ minimal}} d(R'/\mathfrak{p}) = \max_{\mathfrak{p} \text{ minimal}} \dim(R'/\mathfrak{p}) = \dim(R').$$

[8] We are allowed to use (P3) for dim!

Thus, $d(R) = d(R') + 1 = \dim(R') + 1 = \dim(R)$. □

§§4.6. Krull dimension

We now define a new notion of dimension that makes sense for any commutative ring (with the additional possibility of it being ∞ in some cases). We will then show that when restricted to local Noetherian rings, this dimension function is finite and satisfies (P1), (P2), (P3'). This will show that the newly defined dimension agrees with the earlier definition.

Definition 4.6.1. Let R be any commutative ring. A chain of prime ideals in R is a finite sequence of prime ideals

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n.$$

The above chain is said to have length n.

The Krull dimension of R is defined as

$$\operatorname{krdim}(R) := \sup\{n : \text{there exists a chain of prime ideals of length } n\}.$$

Example 4.6.2. Corollary 1.2.12 told us that Artinian rings are precisely Noetherian rings with Krull dimension zero.

Theorem 4.6.3. If $(R, \mathfrak{m})$ is a Noetherian local ring, then $\operatorname{krdim}(R) = \dim(R)$.

Proof. We refer to (P1), (P2), (P3') from the previous section.

(P1): Any chain in $R/\mathfrak{p}$ can lifted back to R showing that $\dim(R/\mathfrak{p}) \leqslant \dim(R)$ for all $\mathfrak{p} \in \operatorname{Spec}(R)$.
Conversely, any chain of primes in R contains a minimal prime and then continues to be a chain in the quotient by that prime.

(P2): Obvious.

(P3'): Let R be a domain and not a field.
Let $x \in \mathfrak{m} \setminus \{0\}$ be arbitrary. A chain of length n in R/xR can be lifted to a chain of length n in R. Moreover, (0) is a prime strictly contained in this chain. Thus, we have a chain of length $n + 1$ in R. This shows

$$\operatorname{krdim}(R) \geqslant \sup_{x \in \mathfrak{m} \setminus \{0\}} \operatorname{krdim}(R/xR) + 1. \tag{4.5}$$

Conversely, if

$$0 = \mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_{m+1} = \mathfrak{m}$$

is a chain of length $m+1$ in R, then pick any nonzero $x \in \mathfrak{p}_1$. Then,

$$\mathfrak{p}_1/(x) \subsetneq \cdots \subsetneq \mathfrak{p}_{m+1}/(x)$$

is a chain of length m in R/xR, proving equality in (4.5).

To finish concluding, we must show that $\operatorname{krdim}(R) < \infty$ for all local Noetherian rings R. We do this by showing that $\operatorname{krdim}(R) \leqslant \dim(R)$ for all Noetherian local *domains* R. (The general case then follows by (P1).)

We prove this by induction on $\dim(R)$.

$\dim(R) = 0$: In this case, R must be a field, for which the statement is known.

Now, assume that $d := \dim(R) \geqslant 1$ and that the statement is known whenever $\dim < R$. For the sake of contradiction, assume that $\operatorname{krdim}(R) > d$. Thus, there exists a chain

$$0 = \mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_{d+1} = \mathfrak{m}.$$

Pick $x \in \mathfrak{p}_1 \setminus \{0\}$. Then, $\dim(R/xR) = \dim(R) - 1$. Since we have a surjection $R/x \twoheadrightarrow R/\mathfrak{p}_1$, we get $\dim(R/\mathfrak{p}_1) \leqslant d - 1$ as well.
But $R/\mathfrak{p}_1$ is a domain in which we have the chain

$$0 \subseteq \mathfrak{p}_2/\mathfrak{p}_1 \subseteq \cdots \subseteq \mathfrak{p}_{d+1}/\mathfrak{p}_1,$$

of length d, contradicting the inductive hypothesis. □

A related concept is the height of a prime.

Definition 4.6.4. Let R be a commutative ring. The height of a prime $\mathfrak{p} \in R$ is defined to be

$$\operatorname{ht}(\mathfrak{p}) := \sup\{n : \text{there exists a chain of prime ideals of length } n \text{ ending at } \mathfrak{p}\}.$$

Equivalently, $\operatorname{ht}(\mathfrak{p}) = \operatorname{krdim}(R_{\mathfrak{p}})$.

Note that under this definition, we have

$$\operatorname{krdim}(R) = \sup_{\mathfrak{p} \in \operatorname{Spec}(R)} \operatorname{ht}(\mathfrak{p}).$$

Note that $\operatorname{ht}(\mathfrak{p})$ is always finite if R is Noetherian, since then $\operatorname{ht}(\mathfrak{p}) = \operatorname{krdim}(R_{\mathfrak{p}}) = \dim(R_{\mathfrak{p}}) < \infty$.
Moreover, for a local ring $(R, \mathfrak{m})$, we have $\dim(R) = \operatorname{ht}(\mathfrak{m})$.

4.6.1 Whacky behaviour of Krull dimension

To begin with, $\operatorname{krdim}(R)$ can be infinite even when R is Noetherian (and necessarily not local).

Note that in the local case, the (Krull) dimension being finite tells us that there exists a maximal chain of primes (i.e., a chain of primes which cannot be extended to a strictly larger chain of primes) with length equal to the dimension. (Thus, this chain is maximal in terms of inclusion and in terms of length.)
But even in the local case, there can exist maximal chains of different length.

Maximal chains of different lengths.
Consider the local (!) Noetherian ring $R = k[x,y,z]_{(x,y,z)}/(xy,xz)$.

R has two minimal primes: $(\bar{x})$, $(\bar{y},\bar{z})$. Computing dimension using (P1) shows that $\dim(R) = 2$. (Example 4.3.4 tells us that the dimensions of $k[x]_x$ and $k[y,z]_{(y,z)}$ are 1 and 2 respectively.)
R has the following two maximal chains, of different lengths:

$$(\bar{y},\bar{z}) \subsetneq (\bar{x},\bar{y},\bar{z}),$$
$$(\bar{x}) \subsetneq (\bar{x},\bar{y}) \subsetneq (\bar{x},\bar{y},\bar{z}).$$

Note that here the chains did start at different minimal primes. However, there are more complicated examples of local Noetherian domains with maximal chains of different lengths (these maximal chains are necessarily between the zero ideal and the maximal ideal).

Maximal ideals of different heights.
Let $R = \mathbb{Q}[\![t]\!]$ be the power series ring over $\mathbb{Q}$ in one variable, and $\mathfrak{p} = (t)$ the maximal ideal.
Let $S = R[x]$.
Consider the ideals $\mathfrak{m}_1 := (tx-1)$ and $\mathfrak{m}_2 = (t,x)$.
Note that $S/\mathfrak{m}_1 = R[x]/(tx-1) \cong R[t^{-1}]$ is the field of Laurent series. In particular, $\mathfrak{m}_1$ is maximal. Moreover, since $tx-1$ is prime, it follows that $\operatorname{ht}(\mathfrak{m}_1) = 1$.[9]
On the other hand, note that we have the chain $0 \subsetneq (x) \subsetneq (t,x)$ of primes showing that $\operatorname{ht}(\mathfrak{m}_2) \geqslant 2$. Thus, $\operatorname{ht}(\mathfrak{m}_1) \neq \operatorname{ht}(\mathfrak{m}_2)$.

More generally, one can replace R with a DVR. In that case, $\mathfrak{p}$ will again be principally generated (Corollary 2.2.4). Moreover, $R[t^{-1}] \cong \operatorname{Frac}(R)$, showing that $\mathfrak{m}_1$ is still maximal. As we shall later see, $\dim(R[x]) = \dim(R) + 1 = 2$ and so we can in fact conclude $\operatorname{ht}(\mathfrak{m}_2) = 2$ and not just $\geqslant 2$.

4.6.2 Dimension theory for k-algebras

We will show that the above behaviour does not happen for (finite type) k-algebras that are integral domains. We will prove the following theorem.

[9] Note that $R[x]$ is a unique factorisation domain since R is a PID. Consequently, if $0 \subsetneq \mathfrak{p} \subseteq (tx-1)$, then we can pick a nonzero element $f \in \mathfrak{p}$. By factoring and using the fact that $\mathfrak{p}$ is prime, we may assume that f is irreducible. But $f \in (tx-1)$ implies that $tx-1 \mid f$. Thus, $(tx-1) = (f)$.

Theorem 4.6.5. Let k be a field, and R be an integral domain which is a finite type k-algebra.
Then, every maximal ideal $\mathfrak{m}$ has the same height d, where $d = \operatorname{trdeg}_k(\operatorname{Frac}(R))$.

In particular, $\dim(R) = d = \operatorname{trdeg}_k(\operatorname{Frac}(R))$.

We now look at some more theory to deduce the above result.

Definition 4.6.6. Let R be a ring. An R-module is said to be flat if $- \otimes_R M$ is exact.
A flat module is said to be faithfully flat (fflat) if $- \otimes_R M$ is a faithful functor, i.e., the map

$$\operatorname{Hom}_R(N, N') \to \operatorname{Hom}_R(N \otimes_R M, N' \otimes_R M)$$

is an injection for all R-modules N, N'.

We leave the following proposition as an exercise.

Proposition 4.6.7. The following are equivalent for an R-module M.

1. M is fflat.
2. $N' \to N \to N''$ is exact iff $N' \otimes M \to N \otimes M \to N'' \otimes M$ is exact (for all sequences $N' \to N \to N''$).
3. M is flat. For all R-modules N, $N \neq 0$ iff $N \otimes M \neq 0$.
4. M is flat. For all $\mathfrak{p} \in \operatorname{Spec}(R)$, $M \otimes k(\mathfrak{p}) \neq 0$. (Here, $k(\mathfrak{p}) = R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p}$.)
5. M is flat. For all maximal ideals $\mathfrak{m} \subseteq R$, $M \otimes k(\mathfrak{m}) \neq 0$.

Example 4.6.8. 0 is flat but not fflat (unless $R = 0$).

$\mathbb{Q}$ is a flat $\mathbb{Z}$-module, but not fflat. (Flatness follows since $\mathbb{Q}$ is a localisation. On the other hand, the nonzero map $\mathbb{Z} \twoheadrightarrow \mathbb{Z}/2$ becomes the zero map after tensoring.)

$R^{\oplus n}$ is fflat.

Lemma 4.6.9. Suppose $f : (R, \mathfrak{m}) \to (S, \mathfrak{n})$ is a ring homomorphism of local rings such that $f^{-1}(\mathfrak{n}) = \mathfrak{m}$.
If S is a flat R-module (via f), then S is fflat.

Proof. We use Item 5 of Proposition 4.6.7. We only need to show that $S \otimes_R k(\mathfrak{m})$ is nonzero.

Note that

$$\begin{aligned} S \otimes_R k(\mathfrak{m}) &\cong S \otimes_R R/\mathfrak{m} \\ &\cong S/\mathfrak{m}S. \end{aligned}$$

By hypothesis, $\mathfrak{m}S \subseteq \mathfrak{n} \neq S$. Thus, the quotient $S/\mathfrak{m}S$ is nonzero. $\square$