

# Commutative Algebra

October 18, 2020

## Contents

<b>0</b>	<b>Introduction</b>	<b>2</b>
<b>1</b>	<b>Noetherian Rings: Definitions and Examples</b>	<b>3</b>
1.1	Ideal Structure . . . . .	7
1.2	Minimal and Associated Primes . . . . .	11

## 0 Introduction

Commutative Algebra is the study of commutative rings and the spaces on which those rings act, namely modules. It was developed from two key sources: algebraic geometry, and algebraic number theory.

In algebraic geometry we are focused on polynomial rings over a field  $k$ , whilst in number theory we are focused on  $\mathbb{Z}$ , the ring of rational integers. Much of this work was done by Grothendieck, but the subject goes back much further, at least to Hilbert who wrote a series of papers on polynomial invariant theory in the late nineteenth century.

As an example, take  $\Sigma_n$ , the symmetric group on the set  $\{1, 2, \dots, n\}$ .  $\Sigma_n$  acts on  $k[x_1, \dots, x_n]$  by permuting the variables, so that  $(\sigma f)(x_1, \dots, x_n) = f(x_{\sigma^{-1}(1)}, \dots, x_{\sigma^{-1}(n)})$ .  $\sigma_n$  acts here via ring automorphisms, and it is then natural to consider the **ring of invariants**, given by  $\{f \in k[x] : \sigma f = f \ \forall \sigma \in \Sigma_n\} := S$ .  $S$  is a ring, **the ring of symmetric polynomials**. We can consider the elementary symmetric functions, which are:

$$\begin{aligned} e_1(x_1, \dots, x_n) &= x_1 + \dots + x_n \\ e_2(x_1, \dots, x_n) &= \sum_{i < j} x_i x_j \\ &\vdots \\ e_n(x_1, \dots, x_n) &= x_1 \dots x_n \end{aligned}$$

In fact,  $S$  is generated as a ring by these  $e_i$ , and there are canonical maps  $k[y_1, \dots, y_n] \rightarrow S$  such that  $Y_i \mapsto e_i$ , which is a ring isomorphism.

Hilbert showed that  $S$  is finitely generated, and moreover for many other groups, not just symmetric groups.

Along the way, he proved four very deep theorems:

- Basis theorem
- Nullstellensatz
- The polynomial nature of the Hilbert function (leading to the beginnings of dimension theory)
- The syzygy theorem (leading to the beginnings of homological theory of polynomial rings)

In 1921 Emmy Noether extracted the key property that made the basis theorem, namely that a commutative ring is **noetherian** if every ideal is finitely generated (there are several equivalent definitions).

**Theorem 0.1** (Hilbert's Basis Theorem). *If  $R$  is a commutative noetherian ring, then  $R[x]$  is also noetherian.*

**Corollary 0.2.** *If  $k$  is a field, then  $k[x_1, \dots, x_n]$  is noetherian.*

Noether developed a theory of ideals for noetherian rings, for example the existence of primary decomposition, which generalises factorisation into primes in noetherian rings.

## Link between Commutative Algebra and Algebraic Geometry

The starting point for this link is the ***fundamental theorem of algebra***, which says that  $f \in \mathbb{C}[x]$  is determined up to scalar multiples by its zeros up to multiplicity. Given  $f \in \mathbb{C}[x_1, \dots, x_n]$ , there is a polynomial function  $\mathbb{C}^n \rightarrow \mathbb{C}$  given by  $(a_1, \dots, a_n) \mapsto f(a_1, \dots, a_n)$ .

Different polynomials will yield different functions, and so  $\mathbb{C}[x_1, \dots, x_n]$  can be viewed as a ring of polynomial functions on complex affine  $n$ -space.

More specifically, given  $I \subseteq \mathbb{C}[x_1, \dots, x_n]$ , we can define the ***set of common zeros***,  $Z(I) = \{(a_1, \dots, a_n) \in \mathbb{C}^n : f(a_1, \dots, a_n) = 0 \ \forall f \in I\}$ , called an ***(affine) algebraic set***.

Remarks:

- One can replace  $I$  by the ideal generated by  $I$ , and you get the same algebraic set. Similarly, replacing an ideal by a generating set of the ideal leaves the algebraic set. The basis theorem asserts that any algebraic set is the set of common zeros of some ***finite*** set of polynomials.
- $\bigcap_j Z(I_j) = Z(\bigcup_j I_j)$ ,  $\bigcup_{j=1}^n Z(I_j) = Z(\prod_{j=1}^n I_j)$ , for ideal  $I_j$ . If we define a topology on  $\mathbb{C}^n$  by calling these algebraic sets the closed sets, we get the ***Zariski topology***, which is a rather coarser topology on  $\mathbb{C}^n$  than the usual topology.
- For  $S \subseteq \mathbb{C}^n$ , we can define  $I(S) = \{f \in \mathbb{C}[x_1, \dots, x_n] : f(a_1, \dots, a_n) = 0 \ \forall (a_1, \dots, a_n) \in S\}$ . This is an ***ideal*** of  $\mathbb{C}[x_1, \dots, x_n]$ , and it is ***radical***, i.e.  $f^r \in I(S) \implies f \in I(S)$ . The Nullstellensatz is a family of results asserting that the correspondence

$$\begin{aligned} I &\mapsto Z(I) \\ I(S) &\leftrightarrow S \end{aligned}$$

gives a bijection between the radical ideals in  $\mathbb{C}[x_1, \dots, x_n]$  and the algebraic subsets of  $\mathbb{C}^n$ . In particular, the maximal ideals of  $\mathbb{C}[x_1, \dots, x_n]$  correspond to points in  $\mathbb{C}^n$ .

## Dimension

A large portion of the course deals with the dimension of rings. We can define it in three main ways:

- The maximal length of a chain of prime ideals.
- In a geometric context in terms of growth rates.
- The transcendence degree of a field of fractions.

For commutative rings, all three give the same answer. There is in fact a fourth method, using homological algebra, which in the case of “nice” noetherian rings also gives the same answer.

Most of this theory dates back to 1920-1950. Rings of dimension 0 are called ***artinian*** rings, and in dimension 1 there are special properties which are important in number theory, particularly in the study of algebraic curves.

## 1 Noetherian Rings: Definitions and Examples

Throughout this section,  $R$  is a commutative ring with a 1.

**Lemma 1.1.** *Let  $M$  be a (left)  $R$ -module. The following are equivalent:*

1. All submodules of  $M$  (including  $M$  itself) are finitely generated.
2. The ascending chain condition (ACC) holds: there are no strictly increasing infinite chains of submodules.
3. The maximum condition of submodules holds: any nonempty set  $S$  of submodules of  $M$  has a maximal element  $L$ , i.e.  $L \subseteq L', L' \in S \implies L = L'$ .

*Proof.*

1.  $\implies$  2. Suppose there is a strictly increasing chain  $N_1 \subsetneq N_2 \subsetneq \dots$ , and let  $N = \bigcup_{i=1}^{\infty} N_i$ . By 1  $N$  is finitely generated, say by  $m_1, \dots, m_r$ . Each  $m_i$  lies in some  $N_{n_i}$ . Then let  $n = \max_i n_i$ , so that  $m_i \in N_n$ . Then  $N_n = M$ , contradicting strict ascent.

2.  $\implies$  3. Assume ACC. Pick  $M_1 \in S$ . If it is the maximal member then we're done. If not, there is  $M_2 \supsetneq M_1$ . If  $M_2$  is maximal, then we're done, otherwise there is some  $M_3 \supsetneq M_2$ , and so on. By ACC this process terminates, and we get a maximal element.

3.  $\implies$  1. Let  $N \triangleleft M$ , and let  $S$  be the collection of all finitely generated submodules of  $N$ . Then  $S \neq \emptyset$  since it contains the 0 submodule. So  $S$  contains a maximal member, say  $L$ . We then claim  $N = L$ . If  $x \in N$  then  $L + Rx \in S$ , and by maximality of  $L$ ,  $x \in L$ .  $\square$

**Definition 1.2.** An  $R$ -module satisfying 1, 2, 3 is **noetherian**.

**Lemma 1.3.** Let  $N \triangleleft M$ . Then  $M$  is noetherian if and only if  $N$  and  $M/N$  are noetherian.

*Proof.*

$\implies$  Let  $M$  be noetherian, so that all its submodules are finitely generated. This property is inherited by  $N$ . Also, the submodules of  $M/N$  are all of the form  $Q/N$  with  $Q \triangleleft M$  containing  $N$ . If  $M$  is noetherian, then  $Q$  is finitely generated, say by  $x_1, \dots, x_r$ . Then  $x_1 + N, \dots, x_r + N$  generates  $Q/N$ .

$\Leftarrow$  Let  $N, M/N$  be noetherian, and let  $L_1 \subset L_2 \subset L_3 \subset \dots$  be a strictly increasing chain of submodules of  $M$ . Set  $Q_i/N = (L_i + N)/N$ , and  $N_i = L_i \cap N$ . These give ascending chains of submodules of  $M/N$  and  $N$  respectively. By ACC there are  $r, s$  with  $Q_i/N = Q_r/N$  for  $i \geq r$ ,  $N_i = N_s$  for  $i \geq s$ . Let  $k = \max\{r, s\}$ . Then we claim  $L_i = L_k$  for  $i \geq k$ . Pick  $\ell \in L_i$ ,  $i \geq k$ . Then  $\ell + N \in Q_k/N$ , and so there is some  $\ell' \in L_k$  such that  $\ell - \ell' \in N \cap L_i = N \cap L_k$ . So  $\ell \in L_k$ , and the claim is proved. Hence our original ascending chain was not strictly increasing,  $\nmid$ .  $\square$

**Lemma 1.4.** 1. If  $M, N$  are  $R$ -modules, then  $M \oplus N$  is noetherian iff  $M$  and  $N$  are noetherian.

2. If  $M_1, \dots, M_n$  are  $R$ -modules then  $M_1 \oplus \dots \oplus M_n$  is noetherian iff each  $M_i$  is noetherian.
3. If  $M$  is noetherian then every homomorphic image of  $M$  is noetherian.
4. Suppose  $M$  can be expressed as a sum of finitely many submodules (not necessarily as a direct sum)  $M = M_1 + \dots + M_n$ . Then  $M$  is noetherian iff each  $M_i$  is.

*Proof.* 1.  $M \cong N/N$ , so this follows by 1.3.

2. Apply 1 and induction on  $n$ .

3. If  $\theta : M \rightarrow N$  then  $\text{im } \theta \cong M / \ker \theta$ , so apply 1.3.

4. The forwards direction follows as  $M_i \triangleleft M$ . For the reverse, there is a map from  $M_1 \oplus \dots \oplus M_n \rightarrow M$ ,  $(m_1, \dots, m_n) \mapsto m_1 + \dots + m_n$ , and then apply 2 and 3.

□

**Definition 1.5.** A ring  $R$  is **noetherian** if it is noetherian as a (left)  $R$ -module

Remark: Submodules of  $R$  as an  $R$ -module are the same as ideals of  $R$  as a ring, and so the ACC for modules gives us the ACC for ideals.

**Lemma 1.6.** Let  $R$  be a noetherian ring. Then any finitely generated  $R$ -module  $M$  is noetherian.

*Proof.* Suppose  $M = Rm_1 + \dots + Rm_n$ . There exist  $R$ -module epimorphisms:

$$\begin{aligned} R &\rightarrow Rm_i \\ r &\mapsto rm_i \end{aligned}$$

$R$  is noetherian, so  $Rm_i$  is the homomorphic image of  $R$ . Then, by 1.4 (4), so is  $M$ . □

**Theorem 1.7** (Hilbert Basis Theorem). Let  $R$  be a noetherian ring. Then the polynomial ring  $R[x]$  is noetherian.

*Proof.* We show that every ideal of  $R[x]$  is finitely generated. Let  $I$  be an ideal. We define  $I(n) = \{f \in I : \deg f \leq n\}$ . Then  $I(n) \neq \emptyset$  as  $0 \in I(n)$ , and  $I(0) \subseteq I(1) \subseteq I(2) \subseteq \dots$

Let  $R(n) = \{\text{Coefficient of } x^n \text{ in } f : f \in I(n)\} \subseteq R$ . We claim  $R(n) \triangleleft R$ , and  $R(n) \subseteq R(n+1)$ .

To see this, suppose  $a, b \in R(n)$ . Then there are polynomials  $f(x) = ax^n + \dots, g(x) = bx^n + \dots$  in  $I$ , where  $\dots$  indicates lower order terms. Since  $I \triangleleft R$ ,  $f \pm g \in I$ ,  $rf \in I$  for all  $r \in R$ , and  $xf \in I$ .

Hence  $a \pm b \in R(n)$ ,  $ra \in R(n)$ , and  $a \in R(n+1)$ , and the claim is proved.

So then we have a chain  $R(0) \subseteq R(1) \subseteq R(2) \subseteq \dots$  terminates, so we may say  $R(n) = R(N) \forall n \geq N$ . Each of  $R(0), \dots, R(N)$  is a finitely generated ideal of  $R$ , say  $R(j) = (a_{j,1}, \dots, a_{j,k_j})$ .

Then by definition of  $R(j)$ , we may take polynomials  $f_{j,1}, \dots, f_{j,k_j}$  in  $I(j)$  which have the  $a_{j,i}$  as their leading coefficients.

Clearly  $I \supseteq (f_{j,k} : 0 \leq j \leq N, 1 \leq k \leq k_j) =: J$  - it remains to show that equality holds, then we will have found a finite generating set of  $I$ . So pick  $f \in I$ , then we claim  $f \in J$ , and prove this by induction on the degree of  $f$ .

If  $\deg f = 0$ , then  $f(x) = a$ , say. But then  $a \in R(0)$ , and so  $a = \sum_i r_i a_{0,i}$  for some  $r_i \in R$ . Since  $f_{0,i}$  has  $a_{0,i}$  as its leading coefficient and has degree zero,  $f_{0,i}(x) = a_{0,i}$ , and  $f = \sum_i r_i f_{0,i} \in J$ .

If instead  $\deg f = n$ , with  $0 < n \leq N$ , and the claim holds for all  $g$  with  $\deg g < n$ , then write  $f(x) = ax^n + \dots$ .  $a \in R(n)$  then by definition, so  $a = \sum_i r_{n,i} a_{n,i}$  for some  $r_{n,i} \in R$ . Then define  $g(x) = f(x) - \sum_i r_{n,i} f_{n,i}(x)$ .  $g(x)$  has degree  $\leq n$ , and the coefficient of  $x^n$  is  $a - a = 0$ , hence  $\deg g < n$ . Since  $f_{n,i} \in I$ , we have  $g \in I$ , and hence by induction  $g \in J$ . But  $f_{n,i} \in J$  as well, so  $f \in J$ .

Finally if  $\deg f = n$ , with  $n > N$ , and the claim holds for all  $g$  with  $\deg g < n$ , again write  $f(x) = ax^n + \dots$ . Then  $a \in R(n) = R(N)$ , so  $a = \sum r_{N,j} a_{N,j}$  for  $r_{N,j} \in R$ . We may then define

$g(x) = f(x) - \sum_i x^{n-N} r_{N,j} f_{N,j}(x)$ , and use the same argument as in the previous paragraph to deduce that  $f \in J$ .

Hence  $I \subseteq J$ , and so  $I = J$  and  $I$  is finitely generated. But  $I$  was an arbitrary ideal of  $R[x]$ , so  $R[x]$  is noetherian.  $\square$

In practice, one uses **Gröbner bases** for ideals - these are generating sets with extra properties that make algorithms more efficient.

Examples:

- Fields are noetherian.
- Principle Ideal Domains (PIDs) are noetherian.
- $\{q \in Q : q = \frac{m}{n}, m, n \in \mathbb{Z}, p \nmid n \text{ for some fixed prime } p\}$ , an example of a *localisation* of  $\mathbb{Z}$ . All localisations of noetherian rings are noetherian - we will see this later.
- $k[x_1, x_2, \dots]$  is not noetherian:  $(x_1) \subsetneq (x_1, x_2) \subsetneq \dots$  is an infinite strictly increasing chain.
- $k[x_1, x_2, \dots, x_n]$  is noetherian - this follows by induction using the Hilbert basis theorem.
- $\mathbb{Z}[x_1, x_2, \dots, x_n]$  is noetherian, so any finitely generated commutative ring is noetherian: if  $R$  is generated by  $r_1, \dots, r_n$ , then there is an epimorphism  $\mathbb{Z}[x_1, \dots, x_n] \rightarrow R$  given by  $x_i \mapsto r_i$ , and  $R$  is the homomorphic image of a noetherian ring.
- If  $A$  is a free abelian group, write  $\mathbb{Z}A$  for its group algebra, which is the set of formal linear combinations of elements of  $A$ , i.e. terms of the form  $\sum_{\alpha \in A} \lambda_\alpha \alpha$  where  $\lambda_\alpha \in \mathbb{Z}$  and only finitely many of the  $\lambda_\alpha$  are nonzero.  
If  $A$  is generated as a group by  $g_1, \dots, g_n$ , then its group algebra is generated as a ring by  $g_1, g_1^{-1}, \dots, g_n, g_n^{-1}$ .
- $k[[x]]$ , the ring of formal power series with coefficients in  $k$ , is noetherian.

There are also some non-commutative examples that are both left and right noetherian:

- Enveloping algebras of a finite dimensional Lie algebra.
- Iwasawa algebras of compact  $p$ -adic groups.

**Theorem 1.8.** *If  $R$  is noetherian, then  $R[[x]]$  is noetherian.*

*Proof 1.* As in 1.7, consider  $R(n)$  = the set of trailing coefficients  $a_n$ , for elements  $a_n x^n +$  higher order terms, and mimic the proof. This is on example sheet 1.  $\square$

We will give a second proof, which uses

**Theorem 1.9** (Cohen's Theorem). *If every prime ideal in a ring  $R$  is finitely generated, then  $R$  is noetherian.*

*Proof.* If  $R$  is not noetherian, then there is a family of non-finitely generated ideals. Call it  $\mathcal{S}$ . By assumption,  $\mathcal{S} \neq \emptyset$ . Partially order  $\mathcal{S}$  by inclusion.

Suppose  $I_1 \subseteq I_2 \subseteq \dots$  is a chain of non-finitely generated ideals. Then we claim  $\bigcup_i I_i$  is also non-finitely generated.

If it were, say by  $(a_1, \dots, a_k)$ , then  $a_i \in I_{n(i)}$  for some finite integer  $n(i)$ , and so, if  $N = \max\{n(i) : 1 \leq i \leq k\}$ ,  $N$  is also finite and  $a_i \in I_N$  for all  $i$ . But then  $I_N = I_n$  for all  $n \geq N$ , and in particular  $I_N$  is finitely generated  $\nmid$ .

So  $\mathcal{S}$  has upper bounds to its chains, and so we may apply Zorn's lemma to get a maximal element of  $\mathcal{S}$ , say  $I$ , so that  $I$  is not finitely generated but any ideal containing  $I$  is finitely generated.

We now claim  $I$  must be prime. Suppose  $aI, bI$ , but  $ab \in I$ . Then  $I + (a) \supsetneq I$ , so  $I + (a)$  is finitely generated, say by  $i_1 + r_1a, \dots, i_n + r_na$ . Define  $J = \{s \in R : sa \in I\} \supseteq I + (b) \supsetneq I$ . Again,  $J$  is finitely generated.

Take  $t \in I \subset I + (a)$ , so  $t = u_1(i_1 + r_1a) + \dots + u_n(i_n + r_na)$  for some  $u_i \in R$ . So  $t = u_1i_1 + \dots + u_ni_n + (u_1r_1 + \dots + u_nr_n)a \in (i_1) + (i_2) + \dots + (i_n) + Ja$ .

Hence  $I \subseteq (i_1) + \dots + (i_n) + Ja$ , so  $I = (i_1) + \dots + (i_n) + Ja$ , so  $I$  is finitely generated  $\nmid$ .

So  $I$  must be prime, but then by our hypothesis  $I$  is still finitely generated  $\nmid$ . So  $R$  must be noetherian.  $\square$

We will also use the following lemma:

**Lemma 1.10.** *Let  $P$  be a prime ideal of  $R[[x]]$  and  $\theta : R[[x]] \rightarrow R, x \mapsto 0$ . Then  $P$  is finitely generated if and only if  $\theta(P)$  is a finitely generated ideal of  $R$ .*

*Proof.* Clearly if  $P$  is finitely generated then  $\theta(P)$  is.

Conversely, suppose  $\theta(P) = Ra_1 + \dots + Ra_n$ .

If  $x \in P$ , then  $P = (a_1, \dots, a_n, x)$ .

This is immediate - if  $g \in P$ ,  $g = a +$  higher order terms. Now  $a \in (a_1, \dots, a_n)$ , so  $g = \sum_i r_i a_i + xg'$  as required.

If  $xP$ , then let  $f_1, \dots, f_n$  be power series with constant terms  $a_1, \dots, a_n$  respectively. Then  $P = (f_1, \dots, f_n)$ .

Take  $g \in p$ , say  $g = b +$  higher terms, with  $b$  the constant term. Then  $b = \sum b_i a_i$ , so  $g - \sum b_i f_i = g_1 x$  for some  $g_1$ . Note that  $g_1 x \in P$ ,  $P$  is prime, and  $xP$ , so  $g_1 \in P$ . Similarly,  $g_1 = \sum c_i f_i + g_2 x$ , and  $g_2 \in P$ . Continuing, we get  $h_1, \dots, h_n \in R[[x]]$ , where  $h_i = b_i + c_i x + \dots$  with  $g = h_1 f_1 + \dots + h_n f_n$ .  $\square$

We are now ready to give the second proof the  $R$  noetherian implies  $R[[x]]$  noetherian:

*Proof 2.* Suppose  $P$  is a prime ideal of  $R[[x]]$ . Then  $P$  is finitely generated iff  $\theta(P)$  is. But  $R$  is noetherian, so  $\theta(P)$  is finitely generated, so  $P$  was finitely generated. Then we apply Cohen's theorem to get  $R[[x]]$  noetherian.  $\square$

## 1.1 Ideal Structure

Here, we assume  $R$  is a commutative ring with a 1, not necessarily noetherian.

**Lemma 1.11.** *The set  $N(R)$  of all nilpotent<sup>1</sup> elements of  $R$  is an ideal, and  $R/N(R)$  has no nonzero nilpotent elements.*

<sup>1</sup>An element  $x$  of a ring is called nilpotent if there is some integer  $m$  such that  $x^m = 0$ .

*Proof.* If  $x \in N(R)$ , then  $x^m = 0$  for some  $m$ . Hence  $(rx)^m = 0$  for all  $r \in R$ , and so  $rx \in N(R)$ .

If  $x, y \in N(R)$ , then  $x^n = 0, y^m = 0$  for some  $n, m$ . Then  $(x + y)^{n+m-1}$  expands to give terms  $\lambda x^s y^t$  where  $s + t = n + m - 1$ . So either  $s \geq n$  or  $t \geq m$ , so all the terms are zero, and  $x + y \in N(R)$ .

So  $N(R) \triangleleft R$ .

Finally, if  $s \in R/N(R)$  then  $s = x + N(R)$ . Note that  $s^n = x^n + N(R)$  for all  $n$ . If  $x + N(R)$  is nilpotent then  $(x + N(R))^m = N(R)$  for some  $m$ , and hence  $x^m \in N(R)$ . So  $x^m$  is nilpotent, and  $(x^m)^n = x^{mn} = 0$  for some  $n$ . But then  $x$  is nilpotent, so  $x + N(R) = 0 + N(R)$ .  $\square$

**Definition 1.12.**  $N(R)$  is called the **nilradical** of  $R$ .

**Theorem 1.13** (Krull).  $N(R)$  is the intersection of all prime ideals of  $R$ .

*Proof.* Let  $I = \bigcap_{P \text{ prime}} P$ . If  $x \in R$  is nilpotent then  $x^n = 0 \in P \forall P$ . So  $x \in P \forall P \implies x \in I$ , so  $N(R) \subseteq I$ .

Suppose  $x$  is not nilpotent. Let  $\mathcal{S}$  be the family of ideals  $J$  such that for  $n > 0$ ,  $x^n \notin J$ . Then  $(0) \in \mathcal{S}$ , so  $\mathcal{S} \neq \emptyset$ , and a union of a chain of ideals in  $\mathcal{S}$  is also in  $\mathcal{S}$ . We apply Zorn's lemma to get a maximal element  $J_1$ .

We claim  $J_1$  is prime - suppose  $yz \in J_1$ , but  $y, z \notin J_1$ . So the ideals  $J_1 + Ry, J_1 + Rz$  strictly contain  $J_1$ , and so  $x^m \in J_1 + Ry$  and  $x^n \in J_1 + Rz$ . But then  $x^{m+n} \in J_1 + Ry = J_1 \nsubseteq$ .

So  $J_1$  is prime, so contains  $I$ , and hence  $x \notin I$ , so  $I \supseteq N(R)$ . Thus  $I = N(R)$ .  $\square$

**Definition 1.14.** The **radical**  $\sqrt{I}$  of an ideal  $I$  is defined by  $\{r \in R : \exists k \in \mathbb{N} \text{ s.t. } r^k \in I\}$ .

Note that  $\sqrt{I}/I = N(R/I)$ , and  $\sqrt{I} = \bigcap_{\text{prime } P \supset I} P$ . We say an ideal  $I$  is radical if  $I = \sqrt{I}$ .

**Definition 1.15.** The **Jacobson radical**  $J(R)$  of  $R$  is the intersection of all the maximal ideals of  $R$  (so  $N(R) \subseteq J(R)$ ).

**Theorem 1.16** (Nakayama's Lemma). If  $M$  is a finitely generated  $R$ -module with  $MJ = M$ , where  $J = J(R)$ , then  $M = 0$ .

*Proof.* <sup>2</sup> If  $M \neq 0$  and is a finitely generated  $R$ -module, then by Zorn's lemma there are maximal proper submodules.

Take  $M_1$  maximal in  $M$ . Then  $M/M_1$  is irreducible (or simple), hence generated by  $m + M_1$  say.

Then, considering the map  $R \rightarrow M/M_1; r \mapsto rm + M_1$ , which is an  $R$ -module homomorphism with kernel a maximal ideal, we see that  $M/M_1 \cong R/I$ , where  $I$  is a maximal ideal of  $R$ , so  $MI \leq M_1$ .

Finally,  $J \leq I$ , then  $MJ \leq MI \leq M_1 \subsetneq M$ , so if  $M \neq 0, MJ \subsetneq M$ .  $\square$

For a commutative ring  $R$ ,  $N(R) \leq J(R)$ . These need not be equal - for example, take  $R = \{\frac{m}{n} \in \mathbb{Q} : p \nmid n\} = \mathbb{Z}_{(p)}$ . This has unique maximal ideal  $P = \{\frac{m}{n} \in \mathbb{Q} : p|m, p \nmid n\}$ . It is an integral domain, so has no nonzero nilpotent elements, so  $N(R) = (0)$ , and  $J(R) = P$ .

<sup>2</sup>Note - this is not the usual Atiyah-Macdonald proof, but this one can be adapted to the case of non-commutative rings.



For rings  $R = k[x_1, \dots, x_n]/I$  with  $k$  algebraically closed and  $I$  any ideal, we do have  $N(R) = J(R)$  - this is the Nullstellensatz - see later on.

Example: A commutative ring is **artinian** if it doesn't contain an infinite strictly descending chain of ideals (or equivalently if every nonempty set of ideals has a minimal member). An  $R$ -module is **artinian** if it satisfies the analogous properties for submodules. As an exercise (on the first example sheet), prove that artinian rings are noetherian.

For example,  $\mathbb{Z}/p\mathbb{Z}, k[x]/(f)$ .  $k[x]$  is not artinian ( $(x) > (x^2) > \dots$ ).

Recall that  $I$  is prime if and only if one following three equivalent properties holds:

$$\begin{aligned} ab \in I &\implies a \in I \text{ or } b \in I \\ R/I &\text{ is an integral domain} \\ I_1 I_2 \subseteq I &\implies I_1 \subseteq I \text{ or } I_2 \subseteq I \end{aligned}$$

Claim:  $J(R) = N(R)$  for artinian rings  $R$

This follows if we can show that  $R$  artinian  $\implies$  every prime ideal is maximal.

*Proof.* Let  $P$  be prime,  $x \notin P$ . By the descending chain condition,  $(x) \supseteq (x^2) \subseteq \dots$  is not strict, so  $(x^n) = (x^{n+1}) = \dots$  for some  $n$ . Hence  $x^n = yx^{n+1}$  for some  $y$ . Then  $x^n(1 - xy) = 0 \in P$ . But  $x^n \notin P$ , and  $P$  is prime, so  $1 - xy \in P$ . Thus  $y + P$  is the inverse of  $x + P$  in  $R/P$ , and so  $R/P$  is a field, and  $P$  is maximal.  $\square$

**Lemma 1.17** (Artin-Tate). *Suppose we have commutative rings  $R \leq S \leq T$ . Suppose  $R$  is noetherian and  $T$  is generated as a ring by  $R$  and finitely many elements  $t_1, \dots, t_n$ . Suppose that  $T$  is a finitely generated  $S$ -module. Then  $S$  is generated by  $R$  and finitely many elements as an  $R$ -algebra.*

*Proof.*  $T$  is generated by  $x_1, \dots, x_m \in T$  as an  $S$ -module, so  $T = Sx_1 + \dots + Sx_m$ . Then:

$$t_i = \sum_j s_{ij} x_j, \quad s_{ij} \in S \tag{1}$$

$$x_i x_j = \sum_k s_{ijk} x_k, \quad s_{ijk} \in S \tag{2}$$

Let  $S_0$  be the ring generated by  $R$ , the  $s_{ij}$  and the  $s_{ijk}$ , so that  $R \leq S_0 \leq S$ .

Any element of  $T$  is polynomial in the  $t_i$  with coefficients in  $R$ . In (1), (2), each element is a linear combination of the  $x_j$  with coefficients in  $S_0$ . Thus  $T$  is a finitely generated  $S_0$ -module. But  $S_0$  is noetherian, being generated as a ring by  $R$  and finitely many elements.  $T$  is noetherian as an  $S_0$ -module, and  $S$  is an  $S_0$ -submodule of  $T$ , hence is finitely generated as an  $S_0$ -module.

But  $S_0$  is generated by  $R$  and finitely many elements, so  $S$  is generated by  $R$  and finitely many elements.  $\square$

**Lemma 1.18** (Zariski). *Let  $k$  be a field, and  $R$  a finitely generated  $k$ -algebra. If  $R$  itself is a field, then it is a finite algebraic extension of  $k$ , i.e. a finitely generated  $k$ -space.*

*Proof.* Suppose  $R$  is generated by  $k$  and  $x_1, \dots, x_n$ , and is a field. If  $R$  is not a finite algebraic extension over  $k$ , then we can reorder the  $x_1, \dots, x_n$  so that  $x_1, \dots, x_m$  are algebraically independent, i.e. the ring generated by  $k$  and  $x_1, \dots, x_m$  is a polynomial algebra  $k[x_1, \dots, x_m]$ , and

$x_{m+1}, \dots, x_n$  are algebraic over the field of fractions  $F = k(x_1, \dots, x_m)$ . Because  $R$  is not finite algebraic over  $k$ ,  $m \geq 1$ .

Hence  $R$  is a finite algebraic extension over  $F$ , and  $R$  is a finitely generated  $F$ -module, (i.e. vector space). Apply Artin-Tate (1.17) for  $k \leq F \leq R$ , it follows that  $F$  is a finitely generated  $k$ -algebra by  $k$  and  $q_1, \dots, q_t$  say, with each  $q_i = f_i/g_i$ , where  $f_i, g_i \in k[x_1, \dots, x_m]$ ,  $g_i \neq 0$ .

Now there is a polynomial  $h$  which is prime to each of the  $g_i$ s, e.g.  $g_1 \dots g_m + 1$ , and the element  $1/h$  cannot be in the ring generated by  $k$  and  $q_1, \dots, q_t$ . This a contradiction, and hence  $m = 0$ , and  $R$  was indeed algebraic over  $k$ .  $\square$

**Theorem 1.19** (Weak Nullstellensatz). *Let  $k$  be a field,  $T$  a finitely generated  $k$ -algebra. Let  $P$  be a maximal ideal of  $T$ . Then  $T/P$  is a finite algebraic extension of  $k$ . In particular, if  $k$  is algebraically closed and  $T$  is the polynomial algebra, then the maximal ideals are of the form  $(x_1 - a_1, \dots, x_n - a_n)$ .*

*Proof.* See later.  $\square$

**Theorem 1.20** (Strong Nullstellensatz). *Let  $k$  be an algebraically closed field, and  $R$  a finitely generated  $k$ -algebra. Then  $N(R) = J(R)$ . Thus, if  $I$  is a radical ideal of  $k[x_1, \dots, x_n]$  and  $R = k[x_1, \dots, x_n]/I$ , then the intersection of the maximal ideals of  $R$  is 0.*

*Furthermore, any radical ideal is the intersection of the maximal ideals containing it.*

*Proof.* Deferred until chapter 2.  $\square$

*Proof of 1.19.* Let  $P$  be the maximal ideal of the finitely generated  $k$ -algebra  $T$ . Put  $R = T/P$ . By Zariski's lemma,  $T/P$  over  $k$  is a finite algebraic extension. If  $k$  is closed, then  $k = T/P$ . Set  $\pi : T \rightarrow k$  with kernel  $P$ .

We then claim that  $\ker \pi = (x_1 - \pi(x_1), \dots, x_n - \pi(x_n))$ .

Now  $\pi$  fixes elements of  $k$ , so the RHS is in the kernel. Conversely,  $T/(x_1 - \pi(x_1), \dots, x_n - \pi(x_n))$  is a 1-dimensional  $k$ -space, so the kernel is contained in the RHS, and so they are equal.

Recall the bijection proposed earlier between radical ideals in  $\mathbb{C}[\mathbf{x}]$  and affine algebraic sets in  $\mathbb{C}^n$ .

Rephrase this by defining  $Q_{(a_1, \dots, a_n)} = (x_1 - a_1, \dots, x_n - a_n)$ . We claim there is a bijection:

$$\begin{aligned} \{\text{radical ideals}\} &\leftrightarrow \{\text{algebraic subsets}\} \\ I &\mapsto \{(a_1, \dots, a_n) : I \subseteq Q_{(a_1, \dots, a_n)}\} \\ \bigcap_{(a_1, \dots, a_n) \in S} Q_{(a_1, \dots, a_n)} &\leftrightarrow S \end{aligned}$$

$\square$

## 1.2 Minimal and Associated Primes

**Lemma 1.21.** *If  $R$  is noetherian, then any ideal  $I$  contains a power of its radical  $\sqrt{I}$ . In particular,  $N(R)$  is nilpotent, i.e.  $N(R)^m = (0)$  for some  $m$ , as  $N(R) = \sqrt{(0)}$ .*

*Proof.* Suppose  $x_1, \dots, x_m \in \sqrt{I}$  generate  $\sqrt{I}$  as an ideal. Then  $x_i^{n_i} \in I$  for some  $n_i$ . Then, if  $n$  is sufficiently large (e.g.  $n \geq \sum (n_i - 1) + 1$ ). Then  $\sqrt{I}^n$  is generated by  $x_1^{r_1}, \dots, x_m^{r_m}$  with  $\sum r_i = n$ . We must thus have some  $r_i \geq n_i$ , and so  $\sqrt{I}^n \subseteq I$ .  $\square$

**Lemma 1.22.** *If  $R$  is noetherian, then a radical ideal is the intersection of finitely many prime ideals.*

*Proof.* Suppose not for contradiction, and take a maximal element  $I$  from the set of radical ideals not of this form (using Zorn's lemma). We then claim that  $I$  is prime, yielding a contradiction.

If not, there is  $J_1, J_2 \not\subseteq I$  with  $J_1 J_2 \subseteq I$ . If necessary, replace  $J_i$  by  $J_i + I$ , we can assume  $I \subsetneq J_1, J_2$ .

Then by the maximality of  $I$ ,  $\sqrt{J_1} = Q_1 \cap \dots \cap Q_m$ ;  $\sqrt{J_2} = Q'_1 \cap \dots \cap Q'_n$  as prime intersections.

Set  $J = \sqrt{J_1} \cap \sqrt{J_2} = Q_1 \cap \dots \cap Q_m \cap Q'_1 \cap \dots \cap Q'_n$ . So  $J^{n_1} \subseteq J_1, J^{n_2} \subseteq J_2$  for some  $n_1, n_2$ . Hence  $J^{n_1+n_2} \subseteq J_1 J_2 \subseteq I$ . But  $I$  is radical, so  $J \subseteq I$ . Now all  $Q_i, Q'_j$  contain  $I$ , so  $J \supseteq I$ . Thus  $J = I$ .  $\square$

Now suppose by the previous lemma that any radical ideal  $\sqrt{I} = P_1 \cap \dots \cap P_m$  is an intersection of finitely many primes. We can remove  $P_i$  from the list if it contains any of the others, so WLOG we may assume that  $P_i \not\subseteq P_j$  for any  $i \neq j$ . If  $P$  is prime with  $\sqrt{I} \subseteq P$ , then  $P_1 \dots P_m \subseteq \bigcap_i P_i = \sqrt{I} \subseteq P$ , and so some  $P_i \subseteq P$ .

**Definition 1.23.** *The minimal primes  $\mathbf{P}$  over an ideal  $\mathbf{I}$  of a noetherian ring are those such that, if  $P'$  is prime with  $I \subseteq P' \subseteq P$ , then  $P' = P$ .*

Clearly the  $P_i$  mentioned above are minimal primes over  $I$ . In fact:

**Lemma 1.24.** *Let  $I$  be an ideal in a noetherian ring. Then  $\sqrt{I}$  is the intersection of the minimal primes over  $I$ , and  $I$  contains a finite product of the minimal primes over  $I$ .*

*Proof.* Each minimal prime over  $I$  contains  $\sqrt{I}$ . So the primes minimal over  $I$  are precisely the minimal ones over  $\sqrt{I}$ . We know  $\sqrt{I}$  is the intersection of these, and thus their product lies in  $\sqrt{I}$ , and 1.21 gives the last part.  $\square$