

**Part B**  
**Commutative Algebra**

**MATH 101B: ALGEBRA II**  
**PART B: COMMUTATIVE ALGEBRA**

I want to cover Chapters VIII, IX, X, XII. But it is a lot of material. Here is a list of some of the particular topics that I will try to cover. Maybe I won't get to all of it.

- (1) integrality (VII.1)
- (2) transcendental field extensions (VIII.1)
- (3) Noether normalization (VIII.2)
- (4) Nullstellensatz (IX.1)
- (5) ideal-variety correspondence (IX.2)
- (6) primary decomposition (X.3) [if we have time]
- (7) completion (XII.2)
- (8) valuations (VII.3, XII.4)

There are some basic facts that I will assume because they are much earlier in the book. You may want to review the definitions and theorems:

- Localization (II.4): Invert a multiplicative subset, form the quotient field of an integral domain (=entire ring), localize at a prime ideal.
- PIDs (III.7):  $k[X]$  is a PID. All f.g. modules over PID's are direct sums of cyclic modules. And we proved in class that all submodules of free modules are free over a PID.
- Hilbert basis theorem (IV.4): If  $A$  is Noetherian then so is  $A[X]$ .
- Algebraic field extensions (V). Every field has an algebraic closure. If you adjoin all the roots of an equation you get a normal (Galois) extension.

An excellent book in this area is Atiyah-Macdonald "Introduction to Commutative Algebra."

## CONTENTS

1. Integrality	2
1.1. Integral closure	3
1.2. Integral elements as lattice points	4
1.3. Proof of Lemma 1.3	7
2. Transcendental extensions	8
2.0. Purely transcendental extensions	8
2.1. Transcendence basis	9
2.2. Noether Normalization Theorem	11
3. Outline of rest of Part B	15
3.1. Valuation rings	15
3.2. Noetherian rings	17
4. Algebraic spaces	18
4.0. Preliminaries	18
4.1. Hilbert's Nullstellensatz	19
4.2. Algebraic sets and varieties	22
5. Noetherian rings	26
5.1. Hilbert basis theorem	26
5.2. Noetherian modules	27
5.3. Associated primes	29
5.4. Primary decomposition	35
5.5. $\text{Spec}(R)$	39
6. Local rings	40
6.1. Basic definitions and examples	40
6.2. Nakayama's Lemma	41
6.3. Complete local rings	43
6.4. Discrete valuation rings	44

## 1. INTEGRALITY

I just want to go over briefly the basic properties of integral extensions. All rings are commutative with 1.

**Definition 1.1.** *Suppose that  $R$  is a subring of  $S$  and  $\alpha \in S$ . Then  $\alpha$  is integral over  $R$  if any of the following equivalent conditions is satisfied.*

- (1)  $\alpha$  is the root of a monic polynomial with coefficients in  $R$ . I.e.,

$$f(\alpha) = \alpha^n + r_1\alpha^{n-1} + \cdots + r_n = 0$$

for some  $r_i \in R$ .

- (2) The subring  $R[\alpha] \subseteq S$  is a finitely generated (f.g.)  $R$ -module.  
 (3) There exists a faithful  $R[\alpha]$ -module which is a f.g.  $R$ -module.

Each condition makes some aspect of integrality most apparent. The first condition implies:

**Lemma 1.2.** *If  $\alpha$  is integral over  $R$  then  $\alpha$  is integral over any subring of  $S$  which contains  $R$ .*

The second (and third) condition implies:

**Lemma 1.3.** *If  $R \subset T$  are subrings of  $S$ ,  $\alpha \in S$  is integral over  $T$  and  $T$  is finitely generated as an  $R$ -module then  $\alpha$  is integral over  $R$ .*

This follows from the following lemma.

**Lemma 1.4.** *If  $R$  is a subring of  $T$  and  $T$  is finitely generated as an  $R$ -module then any f.g.  $T$ -module is also f.g. as an  $R$ -module.*

*Proof.* Let  $x_1, \dots, x_n$  be generators of  $T$  as an  $R$ -module. Then any  $t \in T$  can be written as  $t = \sum r_j x_j$ . If  $M$  is a f.g.  $T$  module with generators  $y_1, \dots, y_m$  then any element of  $M$  can be written as

$$\sum t_i y_i = \sum r_{ij} x_j y_i$$

So, the products  $x_j y_i$  generate  $M$  as an  $R$ -module.  $\square$

The last condition looks strange. A *faithful* module  $M$  is one where the only element of the ring which annihilates  $M$  is 0. (Show that any nonzero free module over any ring is faithful.) In other words,  $M$  is faithful  $R[\alpha]$ -module if the action of  $R[\alpha]$  on  $M$  gives a ring monomorphism:

$$R[\alpha] \hookrightarrow \text{End}_{\mathbb{Z}}(M)$$

One immediate consequence of the third definition is the following:

**Lemma 1.5.** *Any  $\beta \in R[\alpha]$  is also integral over  $R$ .*

*Proof.*

$$R[\beta] \subset R[\alpha] \hookrightarrow \text{End}(M)$$

and  $M$  is f.g. as an  $R$ -module. □

*Proof of equivalence of three definitions.* (1)  $\Rightarrow$  (2) since  $1, \alpha, \dots, \alpha^{n-1}$  generate  $R[\alpha]$  as an  $R$ -module.

(2)  $\Rightarrow$  (3)  $M = R[\alpha]$  is a faithful f.g.  $R[\alpha]$ -module.

(3)  $\Rightarrow$  (1). Suppose that  $M$  is a faithful  $R[\alpha]$ -module which is generated by  $w_1, w_2, \dots, w_n$  as an  $R$ -module. Then, for each  $w_j$ ,

$$(1.1) \quad \alpha w_j = \sum_{i=1}^n a_{ij} w_i$$

for some  $a_{ij} \in R$ . Then I claim that  $\alpha$  is a root of the characteristic polynomial of the  $n \times n$  matrix  $A = (a_{ij})$

$$f(t) = \det(tI_n - A) = t^n - \text{Tr } At^{n-1} + \dots + (-1)^n \det A$$

The reason is that Equation (1.1) can be written in matrix form as:

$$(w_1, w_2, \dots, w_n)\alpha I_n = (w_1, w_2, \dots, w_n)A$$

or

$$(w_1, w_2, \dots, w_n)(\alpha I_n - A) = (0, 0, \dots, 0)$$

If we multiply by the *adjoint matrix*  $(\alpha I_n - A)^{ad}$  and use the fact that

$$(\alpha I_n - A)(\alpha I_n - A)^{ad} = \det(\alpha I_n - A)I_n = f(\alpha)I_n$$

we get:

$$(w_1, \dots, w_n)f(\alpha)I_n = (f(\alpha)w_1, f(\alpha)w_2, \dots, f(\alpha)w_n) = (0, 0, \dots, 0)$$

Since  $f(\alpha)w_j = 0$  for all generators  $w_j$  of  $M$  we get  $f(\alpha)M = 0$ . This implies that  $f(\alpha) = 0$  since  $M$  is a faithful  $R[\alpha]$ -module. □

### 1.1. Integral closure.

**Proposition 1.6.** *If  $R$  is a subring of  $S$  then the set of all  $\alpha \in S$  which are integral over  $R$  forms a ring (which contains  $R$ ). This is called the integral closure of  $R$  in  $S$ .*

*Proof.* Suppose that  $\alpha, \beta \in S$  are integral over  $R$ . Then  $\alpha$  is integral over  $R[\beta]$  by Lemma 1.2. Any element of  $R[\alpha, \beta]$  is integral over  $R[\beta]$  by Lemma 1.5. So every element of  $R[\alpha, \beta]$  (e.g.,  $\alpha + \beta, \alpha\beta$ ) is also integral over  $R$  by Lemma 1.3. Therefore,  $\alpha + \beta$  and  $\alpha\beta$  are integral over  $R$  and the integral elements form a ring. □

Here is an example.

**Theorem 1.7.**  $\mathbb{Z}$  is the integral closure of  $\mathbb{Z}$  in  $\mathbb{Q}$ .

*Proof.* Suppose that  $x = a/b \in \mathbb{Q}$  is integral over  $\mathbb{Z}$  where  $a, b \in \mathbb{Z}$  are relatively prime. Then there are integers  $n, c_1, \dots, c_n$  so that

$$x^n + c_1x^{n-1} + c_2x^{n-2} + \dots + c_n = 0$$

multiplying by  $b^n$  we get the integer equation

$$a^n + c_1a^{n-1}b + c_2a^{n-2}b^2 + \dots + b^n = 0$$

This implies that  $b$  divides  $a^n$ . Since  $a, b$  are relatively prime this means  $b = \pm 1$  and  $x = a/b \in \mathbb{Z}$ .  $\square$

**Definition 1.8.** A domain (= entire ring) is called integrally closed if it is integrally closed in its fraction field.

The last theorem shows that  $\mathbb{Z}$  is integrally closed.

Here is another example. The domain  $R = \mathbb{Z} + \mathbb{Z}\sqrt{5}$  is not integrally closed since its fraction field contains the “golden ratio”

$$\alpha = \frac{1 + \sqrt{5}}{2}$$

which is a root of the monic polynomial

$$x^2 - x - 1 = 0$$

**1.2. Integral elements as lattice points.** Suppose  $V$  is a vector space over a field  $k$  of characteristic 0 and  $B = \{b_1, \dots, b_n\}$  is a basis for  $V$ . Then the additive subgroup  $\mathbb{Z}B$  generated by  $B$  forms a lattice  $L$  in  $V$ . (A *lattice* in  $V$  is defined to be an additive free subgroup whose free basis elements form a basis for  $V$  as a vector space over  $k$ .)

**Theorem 1.9.** Suppose that  $K$  is an algebraic number field, i.e., a finite extension of  $\mathbb{Q}$ . Let  $\mathcal{O}_K$  be the integral closure of  $\mathbb{Z}$  in  $K$ . Then

- (1)  $\mathcal{O}_K$  is a lattice in  $K$  as a vector space over  $\mathbb{Q}$ . (So,  $\mathcal{O}_K$  is the free additive group generated by some  $\mathbb{Q}$ -basis for  $K$ .)
- (2)  $\mathcal{O}_K$  contains any other subring of  $K$  which is finitely generated as an additive group. (So,  $\mathcal{O}_K$  contains any subring of  $K$  which is a lattice.)

To prove this theorem we need to review the properties of the *trace*.

1.2.1. *example.* Take  $K = \mathbb{Q}(i)$  where  $i = \sqrt{-1}$ . Then  $\mathbb{Q}(i)$  has an automorphism  $\sigma$  given by complex conjugation

$$\sigma(a + bi) = a - bi$$

$\mathbb{Q}(i)$  is a Galois extension of  $\mathbb{Q}$  with Galois group

$$\text{Gal}(\mathbb{Q}(i)/\mathbb{Q}) = \{1, \sigma\}$$

**Proposition 1.10.** *The ring of integers in  $\mathbb{Q}(i)$  (= the integral closure of  $\mathbb{Z}$  in  $\mathbb{Q}(i)$ ) is*

$$\mathcal{O}_{\mathbb{Q}(i)} = \mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$$

*Proof.* Certainly,  $\mathbb{Z}[i] \subseteq \mathcal{O}_{\mathbb{Q}(i)}$  since 1 and  $i$  are integral elements of  $\mathbb{Q}(i)$ . Conversely, suppose that  $\alpha = a + bi$  is integral. Then  $\sigma(\alpha) = a - bi$  is also integral. So, the sum and product of  $\alpha, \sigma(\alpha)$  which are called the *trace* and norm of  $\alpha$  are also elements of the ring  $\mathcal{O}_{\mathbb{Q}(i)}$ . Since  $\mathcal{O}_{\mathbb{Q}(i)} \cap \mathbb{Q} = \mathbb{Z}$  (Theorem 1.7), these are rational integers:

$$\text{Tr}_{K/\mathbb{Q}}(\alpha) := \alpha + \sigma(\alpha) = 2a \in \mathbb{Z}$$

$$N_{K/\mathbb{Q}}(\alpha) := \alpha\sigma(\alpha) = a^2 + b^2 \in \mathbb{Z}$$

Also,  $\text{Tr}(i\alpha) = -2b \in \mathbb{Z}$ . These imply that  $a, b \in \mathbb{Z}$  as claimed.  $\square$

1.2.2. *properties of trace.* Suppose that  $E$  is a finite separable field extension of  $K$ . This means that

$$[E : K] = [E : K]_s$$

where  $[E : K] = \dim_K(E)$  is the *degree* of the extension and  $[E : K]_s$  is the number of distinct embeddings

$$\sigma_i : E \hookrightarrow \overline{K}$$

over  $K$ . Here  $\overline{K}$  is the algebraic closure of  $K$  and an *embedding over  $K$*  means that  $\sigma_i$  is the inclusion map on  $K$  for each  $i = 1, \dots, n$ .

Recall that, if  $K$  has characteristic zero then all algebraic extensions of  $K$  are separable.

The *trace*  $\text{Tr}_{E/K} : E \rightarrow K$  is defined by

$$\text{Tr}_{E/K}(x) = \sum \sigma_i(x)$$

This is an element of  $K$  since any element  $\phi \in \text{Gal}(\overline{K}/K)$  will permute the  $\sigma_i$  and therefore fix  $\sum \sigma_i(x)$ . It is clear that this mapping is  $K$ -linear since it is a sum of  $K$ -linear maps.

**Lemma 1.11.** *If  $R$  is an integrally closed subring of  $K$  and  $S$  is the integral closure of  $R$  in  $E$  then  $\text{Tr}_{E/K}(\alpha) \in R$  for all  $\alpha \in S$*

*Proof.* If  $\alpha$  is integral over  $R$  then so is each  $\sigma_i(\alpha)$ . Thus their sum,  $\text{Tr}_{E/K}(\alpha)$  is also integral over  $R$ . But this trace is an element of  $K$ . Since  $R$  is integrally closed in  $K$ ,  $\text{Tr}_{E/K}(\alpha) \in R$ .  $\square$

**Lemma 1.12.** *If  $E$  is a finite separable extension of  $K$  the mapping*

$$E \times E \rightarrow K$$

*sending  $(a, b)$  to  $\text{Tr}_{E/K}(ab)$  is a nondegenerate symmetric  $K$ -bilinear pairing which induces an isomorphism of  $E$  with its  $K$ -dual:*

$$E \cong E^\wedge = \text{Hom}_K(E, K)$$

*Proof.* (char 0 case) The bilinear map  $\text{Tr}(ab)$  gives a linear map

$$E \otimes_K E \rightarrow K$$

whose adjoint is the map  $E \rightarrow E^\wedge$ . Since  $E, E^\wedge$  have the same dimension, the map  $E \rightarrow E^\wedge$  is an isomorphism if and only if it is a monomorphism. In other words we need to show that, for any  $a \in E$  there exists a  $b \in E$  so that  $\text{Tr}_{E/K}(ab) \neq 0$ . This is easy: just take  $b = a^{-1}$ . Then  $\text{Tr}(ab) = \text{Tr}(1) = n \neq 0$  since  $\text{char } K = 0$ .  $\square$

1.2.3. *proof of the theorem.* Now we can prove Theorem 1.9. First choose a basis  $x_1, \dots, x_n$  for  $K$  over  $\mathbb{Q}$ .

Claim: There are positive integers  $m_i$  so that  $y_i = m_i x_i \in \mathcal{O}_K$ . To see this suppose that  $x_i$  is a root of the polynomial  $f(X) \in \mathbb{Q}[X]$ . By multiplying by all the denominators we may assume that  $f(X) \in \mathbb{Z}[X]$ . So, there are integers  $m_j$  so that

$$m_0 x_i^d + m_1 x_i^{d-1} + \dots + m_d = 0$$

Multiply by  $m_0^{d-1}$  and you get:

$$(m_0 x_i)^d + m_1 (m_0 x_i)^{d-1} + m_2 m_0 (m_0 x_i)^{d-2} + \dots = 0$$

So,  $y_i = m_0 x_i \in \mathcal{O}_K$ .

Thus  $\mathcal{O}_K$  contains the  $n$  linearly independent elements  $y_i$ . So, the rank of this additive group is at least  $n$ .

By Lemma 1.12, there is a dual basis  $z_1, \dots, z_n \in E$  so that

$$\text{Tr}_{K/\mathbb{Q}}(y_i z_j) = \delta_{ij}$$

Take any  $\alpha \in \mathcal{O}_K$ . Then  $\alpha = \sum a_j z_j$  for some  $a_i \in \mathbb{Q}$ . But then

$$\text{Tr}_{K/\mathbb{Q}}(y_i \alpha) = a_j \in \mathcal{O}_K \cap \mathbb{Q} = \mathbb{Z}$$

So,  $\mathcal{O}_K$  is a subgroup of the additive free group generated by the  $z_i$ . This implies that it is free of rank  $\leq n$ . But we already know that its rank is at least  $n$ . So,  $\mathcal{O}_K \cong \mathbb{Z}^n$  and it spans  $K$ .

**1.3. Proof of Lemma 1.3.** I explained this in class but I didn't write it yet. You need properties (2) and (3) to show that if  $\alpha \in S$  is integral over  $T$  and  $T$  is a f.g.  $R$ -module then  $\alpha$  is integral over  $R$ .

Property (2) implies that  $T[\alpha]$  is a f.g.  $T$ -module. Lemma 1.4 tells us that  $T[\alpha]$  is a f.g.  $R$ -module. But  $T[\alpha]$  contains  $R[\alpha]$  so it is a faithful  $R[\alpha]$ -module. Condition (3) then tells us that  $\alpha$  is integral over  $R$ .

## 2. TRANSCENDENTAL EXTENSIONS

*Transcendental* means “not algebraic.” We want to look at finitely generated field extensions

$$k(x_1, x_2, \dots, x_n)$$

where not all the  $x_i$  are algebraic over  $k$ . Transcendental extensions are also called *function fields*. The simplest cases are:

**2.0. Purely transcendental extensions.** These are field extensions of  $k$  which are isomorphic to a fraction field of a polynomial ring:

$$k(X_1, \dots, X_n) = Qk[X_1, \dots, X_n]$$

Here the capital letters  $X_i$  are formal variables. So,  $k[X_1, \dots, X_n]$  is the ring of polynomials in the generators  $X_1, \dots, X_n$  with coefficients in the field  $k$  and  $Q$  is the functor which inverts all the nonzero elements. I.e.,  $QR$  is the quotient field of an integral domain  $R$ . Elements of  $k(X_1, \dots, X_n)$  are fractions  $f(X)/g(X)$  where  $g(X) \neq 0$ . These are called *rational functions* in  $n$  variables.

When is  $k(x_1, \dots, x_n) \cong k(X_1, \dots, X_n)$ ?

**Definition 2.1.** Suppose that  $R$  is a  $k$ -algebra, i.e., a (commutative) ring which contains the field  $k$ . We say that  $y_1, \dots, y_n \in R$  are algebraically independent over  $k$  if the  $k$ -algebra homomorphism (a homomorphism of rings containing  $k$  which is the identity on  $k$ )

$$\phi : k[X_1, \dots, X_n] \rightarrow R$$

which sends  $X_i$  to  $y_i$  is a monomorphism. Equivalently,

$$f(y_1, \dots, y_n) \neq 0$$

for every nonzero polynomial  $f$  over  $k$  in  $n$  variables.

For example,  $y \in E$  is algebraically independent (as a set) if and only if it is transcendental over  $k$ .

**Proposition 2.2.** Suppose that  $E$  is a field extension of  $k$  and  $y_1, \dots, y_n \in E$  are algebraically independent over  $k$ . Then we get an isomorphism

$$k(X_1, \dots, X_n) \cong k(y_1, \dots, y_n)$$

sending  $X_i$  to  $y_i$ .

Because of this we can define a *purely transcendental* field extension to be an extension  $k(y_1, \dots, y_n)$  generated by a set of algebraically independent elements.

## 2.1. Transcendence basis.

**Definition 2.3.** If  $E$  is a transcendental extension of  $k$  then a transcendence basis for  $E$  over  $k$  is defined to be a maximal algebraically independent subset  $\{x_1, \dots, x_n\}$ .

If  $\{x_1, \dots, x_n\}$  is a transcendence basis then, if we add one more element, it will become algebraically dependent.

2.1.1. *algebraic dependence.* Suppose that  $y_1, \dots, y_m$  is algebraically dependent and  $k$  minimal. In other words, any if we delete any element it becomes algebraically independent. Then there exists a nonzero polynomial  $f(X) \in k[X]$  so that

$$f(y_1, \dots, y_m) = 0$$

Furthermore, by minimality of  $m$ , every variable  $y_i$  appears in the polynomial. The polynomial  $f(X)$  can be written as a polynomial in one variable  $X_1$  with coefficients in  $k[X_2, \dots, X_m]$ . Plugging in the elements  $y_i$  for  $X_i$  we get:

$$f(y_1, \dots, y_m) = \sum_j g_j(y_2, \dots, y_m) y_1^j$$

This means that  $y_1$  is algebraic over the purely transcendental extension  $k(y_2, \dots, y_m)$ . Similarly, each  $y_i$  is algebraic over the purely transcendental extension  $k(y_1, \dots, \widehat{y}_i, \dots, y_m)$ .

2.1.2. *transcendence degree.* We say that  $E$  has transcendence degree  $m$  over  $k$  if it has a transcendence basis with  $m$  elements. The following theorem shows that this is a well defined number.

**Theorem 2.4.** Every transcendence basis for  $E$  over  $k$  has the same number of elements.

I'll use the following lemmas which are supposed to be obvious.

**Lemma 2.5.** If  $\{x_1, \dots, x_m\}$  is a transcendence basis for  $E$  over  $k$  then  $\{x_2, \dots, x_m\}$  is a transcendence basis for  $E$  over  $k(x_1)$ .

*Proof.* Suppose not. Then there is a nonzero polynomial  $f$  in  $n - 1$  variables with coefficients in  $k(x_1) \cong k[X_1]$ , so that  $f(x_2, \dots, x_m) = 0$ . We can multiply by all the denominators to get another polynomial  $g$  with coefficients in  $k[x_1] \cong k[X_1]$ . But then  $g$  is a polynomial in  $m$  variables so  $g(x_1, \dots, x_m) = 0$  which is a contradiction.  $\square$

**Lemma 2.6.** *Suppose that  $\mathcal{Y}$  is a subset of  $E$  so that  $E$  is algebraic over  $k(\mathcal{Y})$ . Then any maximal algebraically independent subset of  $\mathcal{Y}$  is a transcendence basis for  $E$ .*

*Proof of the theorem.* Suppose that  $\{x_1, \dots, x_m\}$  is any transcendence basis for  $E$  over  $k$ . Suppose that  $\mathcal{Y}$  is a subset of  $E$  so that  $E$  is algebraic over  $k(\mathcal{Y})$ . Then we want to show that  $\mathcal{Y}$  has at least  $m$  elements because this will imply in particular that every transcendence basis has at least  $m$  elements. I will show this by induction on  $m$ .

Suppose that  $m = 0$ . Then the statement is that  $\mathcal{Y}$  has at least 0 elements which is true. Now suppose that  $m > 0$  and  $\mathcal{Y} = \{w_1, \dots, w_n\}$ . Suppose first that  $w_1 = x_1$ . Then  $\{x_2, \dots, x_m\}$  will be transcendence bases for  $E$  over  $k(x_1)$  and  $E$  will be algebraic over  $k(x_1)(w_2, \dots, w_n) = k(x_1, w_2, \dots, w_n)$ . So,  $n - 1 \geq m - 1$  by induction on  $m$  and this implies  $n \geq m$ . So, all we have to do is replace one of the  $w_i$  with  $x_1$ .

By the previous lemma,  $\mathcal{Y}$  contains a transcendence basis which, by rearranging the elements, can be taken to be  $\{w_1, \dots, w_r\}$ . If we add  $x_1$  it will be algebraically independent. So, there will be some polynomial in  $x_1$  and some of the  $w_i$  which will be zero. Rearrange the  $w_i$  so that only  $w_1, \dots, w_s$  are involved in the polynomial and  $s$  is minimal. So,

$$f(x_1, w_1, \dots, w_s) = 0$$

Since  $x_1$  is transcendental, we must have  $s \geq 1$ . So we can write this as a polynomial in  $w_1$ :

$$f(x_1, w_1, \dots, w_s) = \sum_{j=0}^N g_j(x_1, w_2, \dots, w_s) w_1^j = 0$$

where  $N$  is the highest power of  $w_1$  which appears in  $f$ . Then

$$g_N(x_1, w_2, \dots, w_s) \neq 0$$

by minimality of  $s$ . Therefore,  $w_1$  is algebraic over  $k(x_1, w_2, \dots, w_s)$  which implies that  $E$  is algebraic over  $k(x_1, w_2, \dots, w_n)$ . By the previous paragraph, this implies by induction on  $m$  that  $n \geq m$  and we are done.  $\square$

2.1.3. *example.* Let  $k = \mathbb{C}$  and let  $E = \mathbb{C}(X)[Y]/(f(X, Y))$  where

$$f(X, Y) = Y^2 - (X - a)(X - b)(X - c)$$

Since  $f$  is irreducible,  $E$  is a quadratic extension of  $\mathbb{C}(X)$ .  $E$  is also a cubic extension of  $\mathbb{C}(Y)$  since  $f$  is a cubic polynomial in  $X$  with coefficients in  $\mathbb{C}(Y)$ . Therefore,  $\{X\}$  and  $\{Y\}$  are transcendence bases for  $E$  and the transcendence degree is 1.

**2.2. Noether Normalization Theorem.** The statement is:

**Theorem 2.7** (Noether Normalization). *Suppose that  $R$  is a finitely generated domain over a field  $K$ . Then there exists an algebraically independent subset  $\mathcal{Y} = \{y_1, y_2, \dots, y_r\}$  of  $R$  so that  $R$  is integral over  $K[\mathcal{Y}]$ .*

I pointed out that  $r$  (the maximal number of algebraically independent elements of  $R$  over  $K$ ) must be equal to the transcendence degree of the quotient field  $Q(R)$  of  $R$  over  $K$ . Recall that a transcendence basis is a maximal algebraically independent subset. If  $\mathcal{Y}$  is not a transcendence basis for  $Q(R)$  then we can add at least one more element  $x = a/b \in Q(R)$  where  $a, b \in R$ . But then  $y_1, \dots, y_r$  and  $a$  are algebraically independent elements of  $R$  which is a contradiction. So,  $\{y_1, \dots, y_r\}$  is a transcendence basis for  $Q(R)$  over  $K$ .

**2.2.1. motivation.** Before I proved the theorem, I explained why this is important using general language and the specific example of the elliptic curve (2.1.3).

The basic idea is that the inclusion map

$$K[\mathcal{Y}] = K[y_1, y_2, \dots, y_r] \hookrightarrow R$$

corresponds to a mapping of spaces going the other way:

$$K^r \leftarrow X$$

The correspondence is that  $K[\mathcal{Y}]$  is the ring of polynomial functions on  $K^r$  and  $R$  is supposed to be the ring of polynomial functions on some space  $X$ . The fact that  $R$  is integrally closed over  $K[\mathcal{Y}]$  means that  $R$  is finitely generated as a  $K[\mathcal{Y}]$ -module. This correspond to the fact that the mapping of spaces is  $n$ -to-one where  $n$  is the minimal number of generators of  $R$  over  $K[\mathcal{Y}]$  provided that  $K$  is algebraically closed.

The specific example made this a lot clearer.

Suppose that  $K = \mathbb{C}$ . Then the equation

$$f(X, Y) = Y^2 - (X - a)(X - b)(X - c) = 0$$

defines a subset of  $E_f \subset \mathbb{C}^2$ . Projection to the first coordinate gives a mapping

$$p_1 : E_f \rightarrow \mathbb{C}$$

Because the polynomial  $f$  is monic in  $Y$ , this mapping has exactly 2 inverse image points for every  $x \in \mathbb{C}$  except for the three points  $a, b, c$  (which I am assuming are distinct) and, even at these three point, the inverse image is  $Y = 0$  which is a double root of the equation  $Y^2 = 0$ . If the polynomial  $f$  were not monic, e.g., if the equation were:

$$(X - d)Y^2 - (X - a)(X - b)(X - c) = 0$$

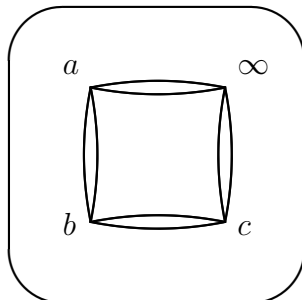
then the polynomial would have a different degree in  $Y$  for different values of  $X$ . For example, when  $X = d$ , this polynomial has no roots at all. Therefore,  $d \in \mathbb{C}$  would not be in the image of the projection map  $X \rightarrow \mathbb{C}$ .

At this point I decided to do some topology to determine that the elliptic curve  $E_f \cup \infty$  is topologically a torus. We need to add the point at infinity to make it compact. The projection map  $p_1 : E_f \rightarrow \mathbb{C}$  extends to a continuous mapping to the Riemann sphere

$$E_f \cup \infty \rightarrow \mathbb{C} \cup \infty = S^2$$

This mapping has four branch points:  $a, b, c, \infty$ . (When  $X$  is very large, the constants  $a, b, c$  are like 0 and the equation looks like  $Y^2 = X^3$ . As  $X$  rotates a full  $2\pi$ ,  $Y$  goes  $3\pi$ , i.e., changes sign. So  $\infty$  is a branch point.)

Now, comes the Euler characteristic calculation: Cut up the Riemann sphere  $S^2$  into two squares along edges connecting  $a$  to  $b$  to  $c$  to  $\infty$  and back to  $a$ . This decomposes  $E_f \cup \infty$  into



- (1) four squares (since each square in  $S^2$  has two squares lying over it)
- (2) eight edges (each of the 4 edges in  $S^2$  has two edges over it)
- (3) four vertices (each of the four vertices in  $S^2$  is a branch point and has only one point lying over it)

So, the Euler characteristic of  $E_f \cup \infty$  is

$$\chi(E_f \cup \infty) = 4 - 8 + 4 = 0 = 1 - 2g$$

making the genus  $g = 1$ . So, it is a torus.

2.2.2. *proof of the theorem.* The proof was by induction on  $n$ , the number of generators of  $R$  over  $K$ . Thus

$$R = K[x_1, \dots, x_n]$$

If  $n = 0$  then  $R = K$  and there is nothing to prove.

If  $n = 1$  then  $R = [x_1]$ . There are two cases: either  $x_1$  is algebraic or it is transcendental. If  $x_1$  is algebraic then  $r = 0$  and  $x_1$  is integral over  $K$ . So, the theorem holds. If  $x_1$  is transcendental then let  $y_1 = x_1$ . We get  $R = K[x_1]$  which is integral over  $K[x_1]$ .

Now suppose that  $n \geq 2$ . If  $x_1, \dots, x_n$  are algebraically independent then we let  $\mathcal{Y} = \{x_1, \dots, x_n\}$  and we are done. If they are not algebraically independent then there is a nonzero polynomial  $f(X) \in K[X_1, \dots, X_n]$  so that  $f(x_1, \dots, x_n) = 0$ . The polynomial  $f(X)$  can be written as

$$f(X) = \sum_{\alpha} c_{\alpha} X^{\alpha}$$

where we use the notation  $X^{\alpha} = X_1^{a_1} X_2^{a_2} \dots X_n^{a_n}$  for  $\alpha = (a_1, \dots, a_n)$ . We can write this as a polynomial in  $X_1$  with coefficients in  $K[X_2, \dots, X_n]$ :

$$f(X) = \sum_{j=0}^N f_j(X_2, \dots, X_n) X_1^j$$

(Since  $f$  is nonzero, it involves at least one of the  $X_i$  and we can assume it is  $X_1$ .) We want to somehow arrange to have  $f_N = 1$ . Then  $x_1$  would be integral over  $K[x_2, \dots, x_n]$  which by induction on  $n$  would be integral over  $K[\mathcal{Y}]$  for some algebraically independent subset  $\mathcal{Y}$ . Since integral extensions of integral extensions are integral, the theorem follows.

To make  $f$  monic in  $X_1$  we change coordinates as follows. Let  $Y_2, \dots, Y_n$  and  $y_2, \dots, y_n \in R$  be given by

$$Y_i = X_i - X_1^{m_i} \quad y_i = x_i - x_1^{m_i}$$

or:  $X_i = Y_i + X_1^{m_i}$  and  $x_i = y_i + x_1^{m_i}$  where the positive integers  $m_i$  will be chosen later. We get the new polynomial

$$g(X_1, Y_2, \dots, Y_n) = f(X_1, \dots, X_n) \in K[X_1, Y_2, \dots, Y_n]$$

so that  $g(x_1, y_2, \dots, y_n) = 0$ . Also, it is clear that  $R = K[x_1, y_2, \dots, y_n]$ .

Now take  $m_i = d^{i-1}$  where  $d$  is an integer greater than any of the exponents  $a_i$  which occur in the polynomial  $f(X)$ . For example, let

$$f(X) = x_1^9 x_2^5 x_3^2 + x_1^2 x_2^2 x_3^3 + x_2^8 x_3$$

Then  $d = 10$  will do. The three multi-indices which occur are  $\alpha = (9, 5, 2), (2, 2, 3), (0, 8, 1)$ . Reverse the orders of these and write them in

descending lexicographic order:  $(3, 2, 2), (2, 5, 9), (1, 8, 0)$ . Saying that these numbers are in lexicographic order is the same as saying that

$$322 > 259 > 180$$

More generally, the value of  $\sum a_i d^{i-1}$  is different for every multi-index  $\alpha$  and is the largest for the multi-index  $\alpha$  which is maximal in this lexicographic order. Look at

$$g(X_1, Y_2, \dots, Y_n) = \sum_{\alpha} c_{\alpha} X_1^{a_1} (X_1^d + X_2)^{a_2} (X_1^{d^2} + X_3)^{a_3} \dots (X_1^{d^{n-1}} + X_n)^{a_n}$$

The highest power of  $X_1$  which occurs is  $N = \sum a_i d^{i-1}$  where  $\alpha$  is maximal in lexicographic order. The coefficient of  $X_1^N$  is  $c_{\alpha}$ . We can divide  $g$  by this nonzero constant and make  $g$  monic in  $X_1$  and we are done by induction on  $n$  as discussed earlier.

## 3. OUTLINE OF REST OF PART B

For the next three weeks we will discuss

- (1) Algebraic spaces (for motivation)
- (2) Noetherian rings
- (3) Valuation rings (local rings)

This is in motivational rather than logical order.

The main idea is that somehow “Algebraic spaces are the same as Noetherian rings which are the same as transcendental extensions.” This is based on the correspondence

$$\text{points} \leftrightarrow \text{local rings}$$

**3.1. Valuation rings.** The definition of places and valuation rings given in most books seems complicated and artificial. I like the old definition which is very simple.

**Definition 3.1.** *Suppose that  $E$  is a field extension of  $K$ . Then a place in  $E$  (over  $K$ ) is a subring  $K \subseteq V \subseteq E$  so that for any  $x \in E$  either  $x \in V$  or  $x^{-1} \in V$  or both.*

3.1.1. *example.*  $E = K(X)$ ,  $V = K[X]_{(X-a)}$ . This is  $K[X]$  localized at the prime ideal  $(X - a)$ .

Recall that if  $p$  is a prime ideal in  $R$  then the complement  $S$  of  $p$  in  $R$  is a multiplicative set and

$$R_p = \text{“}R \text{ localized at } p\text{”} := S^{-1}R = \{a/b \mid a, b \in R, b \notin p\}$$

$R_p$  is a *local ring*, i.e., it has a unique maximal ideal  $S^{-1}p$ . By the following lemma this is equivalent to saying that all elements in the complement of  $S^{-1}p$  are invertible.

**Lemma 3.2.** *The union of all maximal ideals in a ring  $R$  is equal to the complement of the set of all units.*

*Proof.* ( $\subseteq$ ) Ideals cannot contain invertible elements, otherwise they would contain 1.

( $\supseteq$ ) Conversely, any nonunit  $a$  generates an ideal  $(a) = Ra \neq R$ . This is contained in a maximal ideal by Zorn’s lemma.  $\square$

Back to the example:  $p = (X - a)$  is a maximal ideal and is thus prime since it is the kernel of the homomorphism  $\phi : K[X] \rightarrow K$  given by  $\phi(f) = f(a)$ . Since  $K$  is a field,  $\ker \phi = p$  is maximal.

$$V = K[X]_{(X-a)} = \left\{ \frac{f(X)}{g(X)} \in K(X) \mid g(a) \neq 0 \right\}$$

To show that  $V$  is a place suppose that  $x = f(X)/g(X) \in E = K(X)$ . We can assume that  $f, g$  are relatively prime. This implies that either  $f(a) \neq 0$  or  $g(a) \neq 0$  (otherwise both  $f(X)$  and  $g(X)$  would be divisible by  $X - a$ ). If  $g(a) \neq 0$  then  $x = f/g \in V$ . If  $f(a) \neq 0$  then  $x^{-1} = g/f \in V$ . So,  $V$  is an example of a place.

This means that every point  $a \in K$  corresponds to a place in  $K(X)$ . But there are other places such as “ $\infty$ ” which is given by

$$V = \left\{ \frac{f(X)}{g(X)} \in K(X) \mid \deg f \leq \deg g \right\}$$

This is a local ring with unique maximal ideal

$$m = \left\{ \frac{f(X)}{g(X)} \in K(X) \mid \deg f < \deg g \right\}$$

### 3.1.2. *properties of places.*

**Proposition 3.3.** *Suppose that  $V$  is any place in  $E$  over  $K$ . Then*

- (1)  $V$  is a local ring
- (2)  $V$  is integrally closed in  $E$ .

*Proof.* First I showed (2):  $V$  is integrally closed in  $E$ . Suppose that  $x \in E$  is integral over  $V$ . Then

$$x^n = \sum_{k=0}^{n-1} a_k x^k$$

where  $a_k \in V$ . Suppose that  $x \notin V$ . Then  $x^{-1} \in V$  and

$$x = \frac{x^n}{x^{n-1}} = \sum_{k=0}^{n-1} a_k x^{k-n+1}$$

But this is an element of  $V$  since  $k - n + 1 \leq 0$  for all  $k \leq n - 1$ .

To prove (1) it suffices to show that the set  $W$  of nonunits of  $V$  is closed under subtraction and under multiplication by elements of  $V$ . So, suppose that  $r \in V$  and  $y \in W$ , i.e.,  $y^{-1} \notin V$ . Then  $ry$  is not a unit (otherwise  $(ry)^{-1} = z \in V$  gives  $y^{-1} = rz \in V$ ). So,  $VW \subseteq W$ .

Finally, I have to show that, if  $x, y \in W$  then  $x - y \in W$ . If  $x = 0$  or  $y = 0$  then we are done since  $x - y = -y$  or  $x$ . So, suppose that  $x, y$  are nonzero. Then either  $x/y \in V$  or  $y/x \in V$ . Suppose by symmetry that  $x/y \in V$ . Then  $x/y - 1 \in V$  and  $x - y = (x/y - 1)y \in VW \subseteq W$ . So, the nonunits form the unique maximal ideal and  $V$  is a local ring.  $\square$

### 3.2. Noetherian rings.

**Definition 3.4.** *The ascending chain condition (ACC) for ideals in a ring  $R$  says that every increasing sequence of ideals is eventually stationary. I.e., if*

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$$

*is an increasing sequence of ideals in  $R$  then, for some  $N$ , we have  $I_N = I_{N+1} = \cdots$ .*

**Definition 3.5.** *A ring is called Noetherian if it has the ACC for ideals.*

There are two other well known equivalent characterizations of Noetherian rings.

**Theorem 3.6.** *A ring  $R$  is Noetherian if and only if every ideal is finitely generated.*

So, e.g., PID's are Noetherian.

*Proof.* ( $\Leftarrow$ ) Suppose that every ideal is finitely generated. Then we have to show that every ascending chain of ideals  $I_1 \subseteq I_2 \subseteq \cdots$  stops. Let  $I = \cup I_i$ . This is an ideal so it is generated by a finite set  $\{x_1, \dots, x_n\}$ . Each  $x_i$  lies in some  $I_j$ . So, taking  $N$  to be the largest  $j$ , we see that  $I_N$  which contains all of the  $x_i$ . But then  $I = I_N = I_{N+1} = \cdots$ .

( $\Rightarrow$ ) Suppose that  $I$  is an ideal which is not finitely generated. Let  $x_1 \in I$ . Then  $I \neq (x_1)$  so there is an element  $x_2 \in I$  which is not in  $(x_1)$  and there is an element  $x_3 \in I$  which is not in  $(x_1, x_2)$ , etc. This gives a strictly increasing sequence of ideals in  $R$ :

$$(x_1) \subset (x_1, x_2) \subset (x_1, x_2, x_3) \subset \cdots$$

So,  $R$  is not Noetherian. □

The last characterization I only proved in one direction.

**Theorem 3.7.**  *$R$  is Noetherian if and only if every submodule of a finitely generated  $R$ -module is finitely generated.*

**Corollary 3.8.** *The category  $R\text{-Mod}$  of finitely generated  $R$ -modules is an abelian category if  $R$  is Noetherian.*

*Proof of the theorem in one direction.* ( $\Leftarrow$ ) Suppose that every submodule of a finitely generated  $R$ -module is finitely generated. Then this applies to the free module  $R = {}_R R$  which is generated by one element. The submodules of  $R$  are the ideal of  $R$ . So, ideals are all finitely generated making  $R$  Noetherian. □

## 4. ALGEBRAIC SPACES

We want to study zero sets of polynomial equations. The basic theorem is the *Nullstellensatz*. But first we need some preliminaries.

**4.0. Preliminaries.** First we need to know that any finitely generated ring over a field  $K$  can be mapped to the algebraic closure  $\overline{K}$ . This is not true for finitely generated field extensions. For example, there is no homomorphism of  $K(X)$  into  $\overline{K}$  over  $K$ . I used Noether normalization which makes the proofs shorter.

**Lemma 4.1.** *If  $R$  is integral over  $S$  and  $R$  is a field then  $S$  is a field.*

*Proof.* We just need to show that if  $x \neq 0 \in S$  then  $x^{-1} \in S$ . Since  $R$  is a field,  $x^{-1} \in R$ . Since  $R$  is integral over  $S$ ,  $x^{-1}$  satisfies a monic polynomial:

$$x^{-n} = \sum_{i=0}^{n-1} a_i x^{-i}$$

where  $a_i \in S$ . Multiply by  $x^{n-1}$  to get

$$x^{-1} = \frac{x^{n-1}}{x^n} = \sum_{i=0}^{n-1} a_i x^{n-i-1}$$

Since  $n - i - 1 \geq 0$  for all  $i \leq n - 1$ , this is an element of  $S$  and we are done.  $\square$

**Theorem 4.2.** *If  $R = K[x_1, \dots, x_n]$  is a field then  $x_1, \dots, x_n$  are algebraic over  $K$ .*

*Proof.* By Noether normalization there is an algebraically independent set  $\mathcal{Y} = \{y_1, \dots, y_r\}$  in  $R$  so that  $R$  is integral over  $K[\mathcal{Y}]$ . Since  $R$  is a field, the lemma says that  $K[\mathcal{Y}]$  must be a field. This is only possible if  $r = 0$ . So,  $R$  is integral and thus algebraic over  $K$ .  $\square$

**Corollary 4.3.** *Suppose that  $K$  is a field and  $R = K[x_1, \dots, x_n]$  is a finitely generated ring over  $K$ . Then there is a homomorphism*

$$\varphi : R \rightarrow \overline{K}$$

*of rings over  $K$ , i.e., so that  $\varphi$  is the identity on  $K$ .*

*Proof.*  $R$  f.g. implies  $R \cong K[X_1, \dots, X_n]/I$  for some ideal  $I$ . ( $I = \{f(X) \mid f(x) = 0\}$ ). Let  $M$  be a maximal ideal containing  $I$ . Then we have an epimorphism of rings over  $K$ :

$$R \twoheadrightarrow K[X]/M = L$$

Since  $M$  is maximal,  $L$  is field. Since  $L$  is an extension of  $K$  which is finitely generated as a ring, the theorem says that  $L$  is algebraic over  $K$ . Therefore  $L \subseteq \overline{K}$  and the homomorphism what we want is the composition:

$$\varphi : R \twoheadrightarrow L \hookrightarrow \overline{K}$$

□

**Corollary 4.4.** *Suppose that  $R = K[x_1, \dots, x_n]$  is a f.g. domain over  $K$ . Suppose that  $y_1, \dots, y_m$  are nonzero elements of  $R$ . Then there is a homomorphism*

$$\psi : R \rightarrow \overline{K}$$

*of rings over  $K$  so that  $\psi(y_i) \neq 0$  for all  $i$ .*

*Proof.* In the quotient field  $Q(R)$  we have  $y_1^{-1}, \dots, y_m^{-1}$ . Let

$$S = K[x_1, \dots, x_n, y_1^{-1}, \dots, y_m^{-1}] \subseteq Q(R)$$

Then  $R \subseteq S$  and by the previous corollary there is a homomorphism

$$\varphi : S \rightarrow \overline{K}$$

of rings over  $K$ .  $\psi = \varphi|_R$  is the homomorphism that we want. □

**4.1. Hilbert's Nullstellensatz.** Now we can prove the theorem about zero sets of polynomials. First, I gave the definition and some examples.

**Definition 4.5.** *Suppose that  $S$  is a subset of  $K[X] = K[X_1, \dots, X_n]$  and  $L$  is a field extension of  $K$ . Then let  $\mathcal{Z}_S(L)$  denote the set of all common zeroes of  $f_i \in S$  in  $L^n$ :*

$$\mathcal{Z}_S(L) = \{(a) = (a_1, \dots, a_n) \in L^n \mid f_i(a) = 0 \forall f_i \in S\}$$

One of the key features of the zero set is the duality between points and polynomials, namely, the equation

$$f(a) = 0$$

can be interpreted in two ways:  $(a) \in L^n$  is a zero of  $f$  or  $f \in K[X]$  lies in the kernel of the evaluation at  $(a)$  mapping

$$ev_{(a)} : K[X] \rightarrow L$$

The equivalence of these two statements gives the following lemma.

**Lemma 4.6.**  $(a) \in \mathcal{Z}_S(L) \iff S \subseteq \ker(\text{ev}_{(a)} : K[X] \rightarrow L)$ .

Since  $S \subseteq \ker(\text{ev}_{(a)})$  iff the ideal  $(S)$  of  $K[X]$  generated by  $S$  is contained in the ideal  $\ker(\text{ev}_{(a)})$ , we get:

**Proposition 4.7.**  $\mathcal{Z}_S(L) = \mathcal{Z}_{(S)}(L)$ .

We are assuming the Hilbert basis theorem which implies that  $K[X]$  is Noetherian. Therefore, every ideal of  $K[X]$  is finitely generated. So, we may assume that  $S$  is a finite set of polynomials.

Now comes the first version of the Nullstellensatz:

**Theorem 4.8.** *Let  $S = \{f_1, \dots, f_m\} \subseteq K[X_1, \dots, X_n]$  and suppose that  $L \supset K$  is algebraically closed. Then either*

- (1)  $1 = \sum f_i \cdot g_i$  for some  $g_i \in K[X]$  or
- (2)  $\mathcal{Z}_S(L) \neq \emptyset$ .

*Proof.*  $(S) = \{\sum f_i \cdot g_i\}$  is either equal to  $K[X]$  or it is an ideal in  $K[X]$ . In the first case we get  $1 \in (S)$ . So,  $1 = \sum f_i \cdot g_i$ . In the second case,  $R = K[X]/(S)$  is a finitely generated ring over  $K$ . So, there is a homomorphism of rings over  $K$ :

$$\varphi : K[X]/(S) \rightarrow \overline{K} \hookrightarrow L$$

Let  $a_i = \varphi(X_i)$ . Then  $\varphi(f) = f(a)$ . Since each  $f_i \in S$  is in the kernel of  $\varphi$  we have  $f_i(a) = 0$  for all  $i$ . I.e.,  $(a) \in \mathcal{Z}_S(L)$ .  $\square$

**Theorem 4.9** (weak Nullstellensatz). *The maximal ideals of  $\overline{K}[X]$  are*

$$(X_1 - a_1, X_2 - a_2, \dots, X_n - a_n)$$

*where  $a_i \in \overline{K}$ . (So, the maximal ideals of  $\overline{K}[X]$  are in 1-1 correspondence with the points in  $\overline{K}^n$ .)*

*Proof.* Take any ideal  $I$  in  $K[X]$ . By the previous theorem,  $\exists(a_1, \dots, a_n) \in \mathcal{Z}_I(\overline{K})$ . By the lemma, this is equivalent to:

$$I \subseteq (X_1 - a_1, \dots, X_n - a_n)$$

If  $I$  is maximal, these must be equal.  $\square$

**Theorem 4.10** (Hilbert's Nullstellensatz). *If  $f \in K[X]$  so that  $f(a) = 0$  for all  $(a) \in \mathcal{Z}_S(\overline{K})$  then  $f^m \in (S)$  for some  $m \geq 1$ .*

*Proof.* Let  $S = \{h_1, \dots, h_r\}$ . Introduce a new variable  $Y$  and one more polynomial:

$$h_0 = 1 - Yf(X_1, \dots, X_n)$$

Then

$$\mathcal{Z}_{h_0, h_1, \dots, h_r} = \emptyset$$

since, for any common zero  $(a_1, \dots, a_n, b)$ , we have  $f(a) = 0$  by assumption and

$$0 = h_0(a, b) = 1 - bf(a) = 1$$

which is a contradiction. Therefore, there exist  $g_0, \dots, g_n \in K[X, Y]$  so that

$$1 = \sum_{i=0}^n g_i h_i$$

Plugging in  $Y = 1/f(X)$  makes  $h_0 = 0$  and we get

$$1 = \sum_{i=1}^n g_i(1/f(X), X_1, \dots, X_n) h_i(X)$$

If  $m$  is sufficiently large then

$$f(X)^m g_i(1/f(X), X) \in K[X]$$

for all  $i$  and  $f^m \in (S)$ . □

**4.2. Algebraic sets and varieties.** Now I just want to talk about the consequences of the Nullstellensatz. One formulation of the statement is that there is a 1-1 correspondence between algebraic sets and reduced ideals.

**Definition 4.11.** An algebraic set is a subset  $A \subseteq L^n$  (where  $L = \bar{L}$  is algebraically closed) which is defined by polynomial equations with coefficients in  $K \subseteq L$ . In other words,

$$A = \mathcal{Z}_S(L)$$

where  $S \subseteq K[X_1, \dots, X_n], K \subseteq L$ . We say that  $A$  is defined over  $K$ .

4.2.1. associated ideal.

**Definition 4.12.** If  $A \subseteq L^n$  is an algebraic set defined over  $K$  then the associated ideal  $\mathfrak{a}$  is defined by

$$\mathfrak{a} = \{f \in K[X] \mid f(a) = 0 \forall (a) \in A\}$$

Hilbert's Nullstellensatz says that if  $L = \bar{L}$  and  $\mathfrak{a} \subseteq K[X]$  is an ideal then the ideal associated to the algebraic set  $\mathcal{Z}_{\mathfrak{a}}(L)$  is the radical

$$\text{rad}(\mathfrak{a}) = \{f \in K[X] \mid f^n \in \mathfrak{a} \text{ for some } n \geq 1\}$$

**Definition 4.13.** The radical of an ideal  $I$  in a ring  $R$  is defined to be the set of all  $f \in R$  so that some positive power of  $f$  lies in  $I$ . The radical of  $I$  is written  $\text{rad}(I)$ .

Some people write the radical of  $I$  as  $\sqrt{I}$ . (But then we get silly things like:  $\sqrt{(8)} = (2)$ .)

**Definition 4.14.** The radical of the ring  $R$  is defined to be the radical of the ideal  $0$ :

$$\text{rad}(R) := \text{rad}(0) = \{r \in R \mid r^n = 0 \text{ for some } n \geq 1\}$$

**Proposition 4.15.**  $\text{rad}(I) = \pi^{-1} \text{rad}(R/I)$  where  $\pi : R \rightarrow R/I$  is the quotient map.

*Proof.*  $x^n \in I \iff (x + I)^n = I$ . □

Now we can restate the Nullstellensatz again: It says that there is a 1-1 correspondence between algebraic subsets of  $L^n$  defined over  $K$  and ideals  $\mathfrak{a}$  in  $K[X_1, \dots, X_n]$  so that  $\text{rad}(\mathfrak{a}) = \mathfrak{a}$  (we call such ideals *reduced*).

$$\{\text{algebraic sets}\} \cong \{\text{reduced ideals}\}$$

$$A \subseteq L^n \text{ defined over } K \quad \mathfrak{a} \subseteq K[X_1, \dots, X_n]$$

Note that

a) This bijection is *inclusion reversing*:

$$\mathfrak{a} \subseteq \mathfrak{b} \iff \mathcal{Z}_{\mathfrak{a}} \supseteq \mathcal{Z}_{\mathfrak{b}}$$

Assuming the Hilbert basis theorem ( $K[X]$  is Noetherian), this has the following immediate consequence.

**Proposition 4.16.** *Algebraic sets satisfy the DCC.*

*Proof.* Suppose that  $A_1 \supseteq A_2 \supseteq A_3 \supseteq \dots$  is a descending sequence of algebraic subsets of  $L^n$ . Then the associated ideals form an ascending sequence:  $\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \mathfrak{a}_3 \subseteq \dots$ . So, it eventually stops:  $\mathfrak{a}_N = \mathfrak{a}_{N+1} = \dots$ . And the corresponding algebraic sets must be equal:  $A_N = A_{N+1} = \dots$ .  $\square$

One consequence of this is that every algebraic set decomposes as a finite union of irreducible sets.

#### 4.2.2. irreducible sets.

**Definition 4.17.** *An algebraic set defined over  $K$  is called  $K$ -irreducible if it is not the union of two proper algebraic subsets. An irreducible algebraic set is called an (affine) variety over  $K$ .*

When people talk about varieties they often view  $L$  as being variable. Lang formalizes this by saying calling the function  $L \mapsto \mathcal{Z}_{\mathfrak{a}}(L)$  an *algebraic space* and defining a variety as an algebraic space rather than an irreducible algebraic set.

The field of definition is very important. For example, the two point set  $A = \{i, -i\} \subset \mathbb{C}$  is  $\mathbb{R}$ -irreducible but not  $\mathbb{C}$ -irreducible. This has many explanations. It is because the polynomial  $f(X) = X^2 + 1$  which defines this set is irreducible over  $\mathbb{R}$  but not over  $\mathbb{C}$ . Another way to say it is that the Galois group of  $\mathbb{C}/\mathbb{R}$  acts transitively on the set.

**Corollary 4.18.** *Every algebraic set is a finite union of irreducible sets.*

*Proof.* Suppose that  $A$  is not a finite union of irreducible sets. Then it is not irreducible. So  $A = A_0 \cup A_1$ . Either  $A_0$  or  $A_1$  is not a finite union of irreducible sets (otherwise we get a contradiction). Suppose it is  $A_0$ . Then  $A_0 = A_{00} \cup A_{01}$  where one of the pieces is not a finite union of irreducibles, etc. This contradicts the DCC. So, the corollary holds.  $\square$

Another feature of the algebraic set–reduced ideal correspondence:  
 b) It converts products into unions, e.g.

$$\mathcal{Z}_{fg} = \mathcal{Z}_f \cup \mathcal{Z}_g$$

if  $f, g \in K[X]$ . We will discuss products of ideals later.

This has the following important consequence.

**Theorem 4.19.** *A is  $K$ -irreducible iff the associated ideal  $\mathfrak{a} \subset K[X]$  is prime.*

The proof is easy if you realize that the Nullstellensatz can be formulated in the following way:

**Lemma 4.20.** *Suppose  $\mathfrak{a} \subseteq K[X]$  is a reduced ideal,  $f \in K[X]$  and  $K \subseteq L = \bar{L}$ . Then  $f \in \mathfrak{a}$  iff  $\mathcal{Z}_{\mathfrak{a}}(L) \subseteq \mathcal{Z}_f(L)$ .*

4.2.3. *coordinate ring.* For the next subtopic I need to assume that  $K = \bar{K} = L$  and  $A \subseteq K^n$  is an irreducible algebraic set with associated (prime) ideal  $\mathfrak{p} \subseteq K[X]$ . In that case the *coordinate ring* of  $A$  is defined by

$$R := K[X]/\mathfrak{p}$$

This can be interpreted as the ring of all polynomial functions

$$A \rightarrow K$$

since two polynomials  $f, g \in K[X]$  give the same function  $A \rightarrow K$  iff  $f - g = 0$  on  $A$ . By the Nullstellensatz this is equivalent to saying that  $f - g \in \text{rad } \mathfrak{p} = \mathfrak{p}$ .

**Lemma 4.21.** *Suppose that  $I$  is an ideal in a ring  $R$ . Then the maximal ideals of  $R/I$  are  $\mathfrak{m}/I$  where  $\mathfrak{m}$  is a maximal ideal of  $R$  containing  $I$ .*

*Proof.* What I said in class was that  $\mathfrak{m}$  is a maximal ideal in  $R$  iff  $R/\mathfrak{m}$  is a field. But

$$\frac{R}{\mathfrak{m}} \cong \frac{R/I}{\mathfrak{m}/I}$$

which is a field iff  $\mathfrak{m}/I$  is a maximal ideal in  $R/I$ . This proof assumes that  $\mathfrak{m} \subseteq R$  is an ideal containing  $I$ .

Suppose that  $M$  is a maximal ideal in  $R/I$ . Then  $M$  is the kernel of an epimorphism  $\phi : R/I \rightarrow K$  where  $K$  is a field. Let  $\mathfrak{m} = \pi^{-1}(M)$  be the inverse image of  $M$  under  $\pi : R \rightarrow R/I$ . Then  $\mathfrak{m} \subseteq R$  is an ideal containing the kernel  $I$  of  $\pi$ . So the previous paragraph applies.  $\square$

To apply this lemma to the coordinate ring  $R = K[X]/\mathfrak{p}$  we need to recall the weak Nullstellensatz which says that the maximal ideals of  $K[X]$  are  $(X_1 - a_1, \dots, X_n - a_n)$  where  $(a) = (a_1, \dots, a_n) \in K^n$ . This ideal is the kernel of the evaluation map:

$$ev_{(a)} : K[X] \rightarrow K$$

And you need to remember that  $S$  is contained in this kernel iff  $(a) \in \mathcal{Z}_S(K)$ . Putting  $S = \mathfrak{p}$  we see that  $\mathfrak{p}$  is contained in  $(X_1 - a_1, \dots, X_n - a_n)$  iff  $(a) \in A = \mathcal{Z}_{\mathfrak{p}}(K)$ . This proves the following.

**Theorem 4.22.** *There is a 1-1 correspondence between the points of  $A$  and the maximal ideals of the coordinate ring  $R$  of  $A$ .  $\square$*

## 5. NOETHERIAN RINGS

Since I have an extra day, I decided to go back and prove some of the basic properties of Noetherian rings that I haven't already proven.

**5.1. Hilbert basis theorem.** Recall that  $R$  is called a *Noetherian ring* iff the ideal of  $R$  satisfy the ACC. We saw that this was equivalent to saying that every ideal  $\alpha \subseteq R$  has a finite set of generators  $a_1, \dots, a_n$  which means that  $\mathfrak{a}$  is the set of all  $R$ -linear combinations of the  $a_i$ .

**Theorem 5.1** (Hilbert Basis Theorem). *If  $R$  is Noetherian then so is  $R[X]$ .*

*Proof.* Suppose that  $I$  is an ideal in  $R[X]$ . For each  $n \geq 0$  let  $\mathfrak{a}_n$  be the set consisting of 0 and all leading coefficients of polynomials in  $I$  of degree  $n$ . This can also be described as the set of all  $a \in R$  so that  $I$  contains an element of the form

$$aX^n + a_1X^{n-1} + a_2X^{n-2} + \dots + a_n$$

Claim 1.  $\mathfrak{a}_n$  is an ideal of  $R$  or is equal to  $R$ .

*Proof:* To show that  $\mathfrak{a}_n$  is an ideal, choose two elements  $a, b \in \mathfrak{a}_n$ . This is equivalent to saying that  $I$  contains two polynomials of the form

$$f(X) = aX^n + \text{lower terms}$$

$$g(X) = bX^n + \text{lower terms}$$

Suppose that  $r, s \in R$ . Then  $rf + sg \in I$ . But

$$rf + sg = (ra + sb)X^n + \text{lower terms}$$

Therefore,  $ra + sb \in \mathfrak{a}_n$ . So,  $\mathfrak{a}_n$  is an ideal in  $R$  (or  $\mathfrak{a}_n = R$ ).

Claim 2.  $\mathfrak{a}_m \subseteq \mathfrak{a}_{m+1}$ .

This statement is obvious: If  $a \in \mathfrak{a}_m$  then  $I$  contains a polynomial  $f(X) = aX^m + \dots$ . Since  $X \in R[X]$ ,  $I$  also contains  $Xf(X) = aX^{m+1} + \dots$ . So,  $a \in \mathfrak{a}_{m+1}$ .

Since  $R$  is Noetherian, the ascending sequence

$$\mathfrak{a}_0 \subseteq \mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \dots$$

stops at some point  $N$  and we get  $\mathfrak{a}_N = \mathfrak{a}_{N+1} = \dots$ .

For  $i = 0, \dots, N$  let  $a_{ij} \in R$  be a finite set of generators for the ideal  $\mathfrak{a}_i$ . Let  $f_{ij} \in I$  be a polynomial of degree  $i$  with leading coefficient  $a_{ij}$ .

Claim 3. The polynomials  $f_{ij}$  for  $i = 0, \dots, N$  generate  $I$  as an ideal over  $R[X]$ .

I proved this by induction on  $n$ : If  $f(X)$  is a polynomial in  $I$  of degree  $n$  then  $f(X)$  is equal to a polynomial of degree less than  $n$  plus

some  $R[X]$ -linear combination of the polynomials  $f_{ij}$ . To prove this I considered two cases.

Case 1. Suppose first that  $n > N$ . In that case  $f(X) = aX^n + \cdots$ . Since  $a \in \mathfrak{a}_n = \mathfrak{a}_N$  there are elements  $r_j \in R$  so that  $a = \sum r_j a_{Nj}$ . This means that  $\sum r_j f_{Nj}(X) = aX^N + \cdots$ . So,

$$f(X) - \sum r_j X^{n-N} f_{Nj}(X)$$

is an element of  $I$  of degree  $< n$ .

Case 2. Suppose that  $n \leq N$  then the same argument applies to show that there exist  $r_j \in R$  so that

$$f(X) - \sum r_j f_{nj}(X)$$

is an element of  $I$  of degree  $< n$ .

This proves Claim 3 which proved the theorem.  $\square$

There are some immediate consequences of this theorem which I hope I mentioned. First, we have the following immediate consequence of the definition of Noetherian ring.

**Lemma 5.2.** *Any quotient of a Noetherian ring is Noetherian.*

And then we have the following consequence of this lemma and the Hilbert basis theorem.

**Corollary 5.3.** *If  $R$  is Noetherian, then any finitely generated ring over  $R$  is also finitely generated.*

For example, any finitely generated ring over a field is Noetherian.

**5.2. Noetherian modules.** The next basic property was the third equivalent definition of a Noetherian ring:

**Theorem 5.4.** *A ring  $R$  is Noetherian if and only if every submodule of a finitely generated  $R$  module is finitely generated.*

I pointed out that one direction ( $\Leftarrow$ ) is obvious since  $R$  is a finitely generated module over itself and the proper submodules of  $R$  are the ideals. To prove the converse I needed some definitions.

**Definition 5.5.** *Suppose that  $R$  is any ring. Then an  $R$ -module  $M$  is called Noetherian if the submodules of  $M$  satisfy the ACC. This is clearly equivalent to saying that every submodule of  $M$  is finitely generated.*

Using this definition, a ring  $R$  is Noetherian if and only if  $R$  is a Noetherian  $R$ -module. From this we want to conclude that every f.g.  $R$ -module is Noetherian. But every f.g.  $R$ -module is the quotient of a

f.g. free module  $R^n$ . Therefore, the theorem follows from the following two lemmas.

**Lemma 5.6.** *If  $M$  is a Noetherian  $R$ -module then so is every quotient module of  $M$ .*

This is obvious because the submodules of any quotient  $M/N$  correspond to the submodules of  $M$  containing  $N$ .

**Lemma 5.7.** *If  $M, N$  are Noetherian  $R$ -modules then so is  $M \oplus N$ .*

I proved the following generalization of this lemma. And I pointed out that since the proposition proves the lemma and the lemma proves the theorem we will be done.

**Proposition 5.8.** *Suppose that  $0 \rightarrow K \rightarrow M \xrightarrow{\pi} N \rightarrow 0$  is a short exact sequence of  $R$ -modules. Then tfae.*

- (1)  $M$  is Noetherian.
- (2)  $K$  and  $N$  are both Noetherian.

*Proof.* It is clear that the first statement implies the second. So, suppose that the second statement is true. Let  $L_1 \subseteq L_2 \subseteq \dots$  be an ascending sequence of submodules of  $M$ . Then we want to show that the sequence stops.

Let  $A_i = L_i \cap K$ . This is an increasing sequence of submodules of  $K$ . So, for large enough  $N$ , we have  $A_N = A_{N+1} = \dots$ .

Let  $B_i = \pi(L_i)$  be the image of  $L_i$  in  $N$ . Then, because  $N$  is Noetherian, there is a large number  $N'$  which we can take to be equal to  $N$  so that  $B_{N'} = B_{N'+1} = \dots$ .

Now we claim that  $L_N = L_{N+1} = \dots$ . This is a special case of the 5-lemma applied to the following diagram.

$$\begin{array}{ccccccccc}
 0 & \longrightarrow & A_N & \longrightarrow & L_N & \longrightarrow & B_N & \longrightarrow & 0 \\
 & & \downarrow = & & \downarrow & & \downarrow = & & \\
 0 & \longrightarrow & A_{N+1} & \longrightarrow & L_{N+1} & \longrightarrow & B_{N+1} & \longrightarrow & 0
 \end{array}$$

Since the rows are exact and the diagram commutes, the mapping  $L_N \hookrightarrow L_{N+1}$  is an isomorphism. I.e.,  $L_N = L_{N+1}$ .  $\square$

**5.3. Associated primes.** The idea is to obtain something similar to the unique factorization theorem for integers:  $n = \prod p_i^{e_i}$  where we replace  $p_i$  with prime ideals in a Noetherian ring  $R$  and we replace  $n$  with a f.g.  $R$ -module  $M$ . For example,  $12 = 2^2 3$  corresponds to the statement that the prime ideals  $(2), (3) \subseteq \mathbb{Z}$  are associated to the  $\mathbb{Z}$ -module  $M = \mathbb{Z}/(12)$ .

There are three ways to associate prime ideals to modules. Two are easy and we also use a third method which has better properties. The first way is to look at the cyclic submodules. For example,  $M = \mathbb{Z}/(12)$  contains submodules isomorphic to  $\mathbb{Z}/(2)$  and  $\mathbb{Z}/(3)$ . The other simple method is to look at the quotient modules. There is an epimorphism  $\mathbb{Z}/(12) \rightarrow \mathbb{Z}/(p)$  only for the primes  $p = 2, 3$ . However, there tend to be more quotients than submodules. For example,  $\mathbb{Z}/(p)$  is a quotient of  $M = \mathbb{Z}$  for every prime  $p$ . But the only prime ideal  $\mathfrak{p} \subset \mathbb{Z}$  so that  $\mathbb{Z}/\mathfrak{p}$  is embedded in  $\mathbb{Z}$  is  $\mathfrak{p} = 0$ .

5.3.1. *annihilators and associated primes.* I will always assume that  $R$  and  $M$  are both Noetherian.

**Definition 5.9.** *If  $x \neq 0 \in M$  then the annihilator  $\text{ann}(x)$  is the set of all  $a \in R$  so that  $ax = 0$ . It is easy to see that this is an ideal in  $R$ .*

**Definition 5.10.** *For any  $R$ -module  $M$ , the associated primes are the prime ideals  $\mathfrak{p}$  which occur as annihilators of nonzero elements of  $M$ . This is equivalent to the statement that there is a monomorphism*

$$R/\mathfrak{p} \hookrightarrow M$$

The set of associated ideals is denoted  $\text{ass}(M)$ . So,

$$\text{ass}(M) = \{\mathfrak{p} \subset R \text{ prime} \mid \mathfrak{p} = \text{ann}(x) \text{ for some } x \in M\}$$

**Example 5.11.** *If  $\mathfrak{p} \subset R$  is prime then  $\text{ass}(R/\mathfrak{p}) = \{\mathfrak{p}\}$ .*

*Proof.* Clearly,  $\mathfrak{p}$  is a prime associated to  $R/\mathfrak{p}$ . Suppose that  $\mathfrak{q}$  is another associated prime. Then  $\mathfrak{q} = \text{ann}(x)$  for some  $x = y + \mathfrak{p}$  in  $R/\mathfrak{p}$ . But then

$$\begin{aligned} \mathfrak{q} = \text{ann}(x) &= \{a \in R \mid ax = 0 \in R/\mathfrak{p}\} \\ &= \{a \in R \mid ay \in \mathfrak{p}\} = \mathfrak{p} \end{aligned}$$

□

The next theorem is that the union of the associated primes is the set of zero divisors.

**Definition 5.12.**  $a \in R$  is called a zero divisor of  $M$  if  $ax = 0$  for some nonzero  $x \in M$ . In other words, the set of zero divisors of  $M$  is equal to the union of all  $\text{ann}(x)$  for all nonzero  $x \in M$ .

I pointed out that  $a \in R$  is not a zero divisor of  $M$  if and only if multiplication by  $a$  does not kill any nonzero element of  $M$ . I.e.,

$$a \cdot = a_M : M \rightarrow M$$

is a monomorphism. In that case  $a$  is called  $M$ -regular.

**Theorem 5.13.** The union of the associated primes of  $M$  is equal to the set of zero divisors of  $M$ :

$$\bigcup_{\mathfrak{p} \in \text{ann}(M)} \mathfrak{p} = \{\text{zero divisors of } M\}$$

First we need a lemma:

**Lemma 5.14.** Consider the set of all ideals  $I \subset R$  so that  $I = \text{ann}(x)$  for some  $x \in R$ . Then the maximal elements of this set are prime.

*Proof.* Suppose that  $I = \text{ann}(x)$  is maximal but not prime. Then there exist  $a, b \in R$  so that  $ab \in I$  but  $a, b \notin I$ . Since  $b \notin I$ ,  $bx \neq 0$ . But  $abx = 0$ . So,  $a \in \text{ann}(bx)$  and  $a \notin I = \text{ann}(x)$ . This implies that  $\text{ann}(bx)$  is strictly larger than  $\text{ann}(x)$  which is a contradiction.  $\square$

5.3.2. *localization and support.* There are two other methods to associate primes to  $R$ -modules. The easy way is to take the set of all  $\mathfrak{p}$  so that  $M/\mathfrak{p}M \neq 0$ . However, localization is a better method even though it is more complicated.

Recall that, for any multiplicative subset  $S$  of  $R$ ,  $S^{-1}M$  is the  $R$  module given by:

$$S^{-1}M = \{x/s \mid x \in M, s \in S\} / \sim$$

where  $x/s \sim y/t$  iff  $rtx = rsy$  for some  $r \in S$ . If  $\mathfrak{p}$  is a prime ideal then the *localization*  $M_{\mathfrak{p}}$  of  $M$  at  $\mathfrak{p}$  is defined to be  $M_{\mathfrak{p}} = S^{-1}M$  where  $S$  is the complement of  $\mathfrak{p}$  in  $R$ .

**Definition 5.15.** The support of  $M$  is defined to be the set of all primes  $\mathfrak{p}$  so that  $M_{\mathfrak{p}} \neq 0$ :

$$\text{supp}(M) := \{\mathfrak{p} \subset R \text{ prime} \mid M_{\mathfrak{p}} \neq 0\}$$

**Example 5.16.**  $\text{supp}(R/I) = \{\mathfrak{p} \subset R \text{ prime} \mid I \subseteq \mathfrak{p}\}$ .

This follows from the elementary fact that

$$S^{-1}(R/I) = 0 \iff S \cap I \neq \emptyset$$

The advantage of the localization functor  $M \mapsto M_{\mathfrak{p}}$  is that it is exact while  $M \mapsto M/\mathfrak{p}M$  is not exact.

**Proposition 5.17.** *Suppose that  $S \subset R$  is a multiplicative set. Then the functor  $M \mapsto S^{-1}M$  is exact.*

*Proof.* Suppose that  $N \xrightarrow{\psi} M \xrightarrow{\phi} L$  is exact, i.e.,  $\ker \phi = \text{im } \psi$ . Then we want to show that

$$S^{-1}N \xrightarrow{\bar{\psi}} S^{-1}M \xrightarrow{\bar{\phi}} S^{-1}L$$

is exact. The composition is certainly 0. So, suppose that  $x/s \in S^{-1}M$  is in the kernel of  $\bar{\phi}$ . Then  $\phi(x)/s = 0$ . So,  $\exists t \in S$  s.t.  $t\phi(x) = 0 = \phi(tx)$ . This implies that  $tx = \psi(y)$  for some  $y \in N$ . Then  $x/s = tx/ts = \bar{\psi}(y/ts)$ . So,  $\ker \bar{\phi} = \text{im } \bar{\psi}$ .  $\square$

An immediate consequence of the exactness of localization is the following.

**Corollary 5.18.** *If  $0 \rightarrow N \rightarrow M \rightarrow M/N \rightarrow 0$  is a short exact sequence of  $R$ -modules then*

$$\text{supp}(M) = \text{supp}(N) \cup \text{supp}(M/N)$$

*Proof.* For any prime  $\mathfrak{p}$  we get a short exact sequence

$$0 \rightarrow N_{\mathfrak{p}} \rightarrow M_{\mathfrak{p}} \rightarrow (M/N)_{\mathfrak{p}} \rightarrow 0$$

$\mathfrak{p} \in \text{supp}(M) \iff M_{\mathfrak{p}} \neq 0 \iff \text{either } N_{\mathfrak{p}} \neq 0 \text{ or } (M/N)_{\mathfrak{p}} \neq 0 \iff \mathfrak{p} \in \text{supp}(N) \cup \text{supp}(M/N)$ .  $\square$

The main result relating associated primes and the support is the following.

**Theorem 5.19.** *Suppose that  $R$  and  $M$  are Noetherian. Then*

$$\text{ass}(M) \subseteq \text{supp}(M)$$

*Furthermore, the minimal elements of  $\text{supp}(M)$  are associated primes.*

The minimal elements of  $\text{supp}(M)$  are called the *minimal* (or *isolated*) *associated primes*.

*Proof.* Suppose that  $\mathfrak{p}$  is an associated prime. Then we have a short exact sequence

$$0 \rightarrow R/\mathfrak{p} \rightarrow M \rightarrow X \rightarrow 0$$

By exactness of localization, we get an exact sequence

$$0 \rightarrow (R/\mathfrak{p})_{\mathfrak{p}} \rightarrow M_{\mathfrak{p}} \rightarrow X_{\mathfrak{p}} \rightarrow 0$$

But  $(R/\mathfrak{p})_{\mathfrak{p}} \neq 0$  by Example 5.16. So,  $M_{\mathfrak{p}} \neq 0$ . So  $\mathfrak{p}$  is in the support of  $M$ .

Now suppose that  $\mathfrak{p} \in \text{supp}(M)$  is minimal. Then  $M_{\mathfrak{p}} \neq 0$ . So it has a nonzero element  $x/s$ . This being nonzero means that  $tx \neq 0$  for all  $t \in S$  (where  $S$  is the complement of  $\mathfrak{p}$  in  $R$ ). Consequently, the annihilator of  $x/s$  is disjoint from  $S$ . So

$$\text{ann}(x) \subseteq \text{ann}(x/s) \subseteq \mathfrak{p}$$

Let  $\mathfrak{q} = \text{ann}(x/s)$  be maximal. Then  $\mathfrak{q} \in \text{ass}(M_{\mathfrak{p}})$  by Lemma 5.14. Since  $R$  is Noetherian,  $\mathfrak{q} = (a_1, \dots, a_n)$ . This means that there are elements  $t_1, \dots, t_n \in S$  so that  $t_i a_i x = 0$ . This implies that

$$\mathfrak{q} \subseteq \text{ann}(\prod t_i x) \subseteq \text{ann}(\prod t_i x/s)$$

But  $\text{ann}(\prod t_i x/s) = \mathfrak{q}$  by maximality of  $\mathfrak{q}$ . So,

$$\mathfrak{q} = \text{ann}(\prod t_i x) \in \text{ass}(M) \subseteq \text{supp}(M)$$

which implies that  $\mathfrak{q} = \mathfrak{p} \in \text{ass}(M)$ . □

5.3.3. *intersection of associated primes.* One consequence of the theorem is that the intersection of the associated primes is the same as the intersection of the primes in the support.

**Corollary 5.20.**

$$\bigcap_{\mathfrak{p} \in \text{ass}(M)} \mathfrak{p} = \bigcap_{\mathfrak{p} \in \text{supp}(M)} \mathfrak{p} = \text{rad}(\text{ann}(M))$$

To prove this we need the following lemma.

**Lemma 5.21.** *The radical of any ideal  $I$  is the intersection of all prime ideals containing it:*

$$\text{rad } I = \bigcap_{I \subseteq \mathfrak{p} \text{ prime}} \mathfrak{p}$$

For this we need a description of the embedding

$$\text{Spec}(S^{-1}R) \hookrightarrow \text{Spec}(R)$$

where  $\text{Spec}(R)$  is the set of prime ideals in  $R$ . This embedding sends any ideal  $\mathfrak{a}$  in  $S^{-1}R$  to the ideal

$$I = \mathfrak{a}|R := \{a \in R \mid a/1 \in \mathfrak{a}\}$$

This is clearly an ideal in  $R$  which is disjoint from  $S$  (otherwise  $\mathfrak{a}$  contains a unit  $s/1$ ). Also  $\mathfrak{a}$  prime implies  $S^{-1}R/\mathfrak{a}$  is a domain which implies that  $\mathfrak{a}|R$  is prime since it is the kernel of the composition

$$R \rightarrow S^{-1}R \rightarrow S^{-1}R/\mathfrak{a}.$$

( $\mathfrak{a} \mapsto I = \mathfrak{a}|R$  describes an embedding since  $\mathfrak{a} = S^{-1}I$ .)

*Proof of the lemma.* ( $\subseteq$ ) is clear since  $I \subseteq \mathfrak{p} \Rightarrow \text{rad } I \subseteq \mathfrak{p}$ .

( $\supseteq$ ) If  $a \notin \text{rad}(I)$  then the multiplicative set  $S = \{1, a, a^2, \dots\}$  is disjoint from  $I$ . This implies that the ring  $T^{-1}(R/I)$  is nonzero ( $T$  is the image of  $S$  in  $R/I$ ). So, it has a maximal (and thus prime) ideal  $\mathfrak{m}$ . Then  $P = \mathfrak{m}|R/I$  is a prime in  $R/I$  disjoint from  $T$ . Then  $P = \mathfrak{p}/I$  for some prime ideal  $\mathfrak{p}$  containing  $I$  and disjoint from  $S$ . This implies that  $a \notin \mathfrak{p}$ . So,  $a \notin \bigcap \mathfrak{p}$ .  $\square$

*Proof of corollary.* Since the minimal associated primes are the same as the minimal supporting primes, the two intersections are equal.

( $\supseteq$ )  $\text{ann}(M) \subseteq \text{ann}(x)$  for all  $x \in M$ . In particular,  $\text{ann}(M)$  is contained in every associated prime  $\mathfrak{p}$ . But then  $\text{rad}(\text{ann}(M))$  is also contained in each  $\mathfrak{p}$ .

( $\subseteq$ ) Suppose that  $a \notin \text{rad}(\text{ann}(M))$ . Then, by the lemma, there is a prime ideal  $\mathfrak{p}$  containing  $\text{ann}(M)$  so that  $a \notin \mathfrak{p}$ . But  $\mathfrak{p} \subseteq \text{ann}(M) \Rightarrow M_{\mathfrak{p}} \neq 0$ . So,  $\mathfrak{p}$  is a supporting prime. So,  $a \notin \bigcap \mathfrak{p}$ .  $\square$

#### 5.3.4. primes associated to extensions.

**Theorem 5.22.** *Suppose that  $0 \rightarrow N \rightarrow M \rightarrow M/N \rightarrow 0$  is a short exact sequence of  $R$ -modules. Then*

$$\text{ass}(N) \subseteq \text{ass}(M) \subseteq \text{ass}(N) \cup \text{ass}(M/N)$$

*Proof.* The first inclusion is obvious: If  $R/\mathfrak{p}$  embeds in  $N$  then it embeds in  $M$ . So, suppose that  $\mathfrak{p}$  is associated to  $M$ . Then  $\mathfrak{p} = \text{ann}(x)$  for some  $x \in M$ . There are two cases. Either  $Rx \cap N = 0$  or  $Rx \cap N \neq 0$ .

If  $Rx \cap N = 0$  then  $R/\mathfrak{p} \cong Rx$  embeds in  $M/N$  making  $\mathfrak{p}$  an associated prime of  $M/N$ .

If  $Rx \cap N$  contains  $y = ax \neq 0$  in particular,  $a \notin \text{ann}(x) = \mathfrak{p}$ . The annihilator of  $y$  is the set of all  $b \in R$  so that  $bay = 0$ . But this implies  $ba \in \mathfrak{p}$ . Since  $a \notin \mathfrak{p}$  we must have  $b \in \mathfrak{p}$ . So,  $\text{ann}(y) = \mathfrak{p} \in \text{ass}(N)$ .

The theorem holds in both cases.  $\square$

When the short exact sequence splits, this theorem implies that

$$\text{ass}(M) = \text{ass}(N) \cup \text{ass}(M/N)$$

By induction this implies the following.

**Corollary 5.23.**  $\text{ass}(\bigoplus M_i) = \bigcup \text{ass}(M_i)$ .

**5.4. Primary decomposition.** In a Noetherian ring, the radical of any ideal  $\mathfrak{a}$  is the intersection of a finite number of prime ideals

$$(5.1) \quad \text{rad } \mathfrak{a} = \bigcap \mathfrak{p}_i$$

where  $\mathfrak{p}_i$  are the primes associated with the module  $R/\mathfrak{a}$ . When  $R = K[X_1, \dots, X_n]$  this corresponds, by the Nullstellensatz, to the decomposition of the corresponding algebraic set  $A = \mathcal{Z}_{\mathfrak{a}}(L) \subset L^n$  as a finite union of irreducible sets:

$$(5.2) \quad A = \bigcup V_i$$

The ideal itself is the intersection of corresponding “primary” ideals  $\mathfrak{q}_i$ :

$$(5.3) \quad \mathfrak{a} = \bigcap \mathfrak{q}_i$$

The correspondence is that  $\text{rad } \mathfrak{q}_i = \mathfrak{p}_i$ . Thus every term in the expression (5.1) is the radical of the corresponding term in (5.3). It is interesting that only the minimal primes are needed in (5.1) but all of the primary ideals in (5.3) are needed.

The zero sets for the ideals in (5.3) corresponding to the nonminimal “embedded” associated primes are contained in the union of the others.

5.4.1. *primary submodule.*

**Definition 5.24.** A submodule  $Q$  of an  $R$ -module  $M$  is called primary if any zero divisor of  $M/Q$  is also nilpotent on  $M/Q$ .

- (1)  $a \in R$  is a zero divisor of  $M/Q$  iff there is some  $x \in M, x \notin Q$  so that  $ax \in Q$ .
- (2)  $a \in R$  is nilpotent on  $M/Q$  iff some power of  $a$  annihilates  $M/Q$ , i.e.,  $a^n M \subseteq Q$  for some  $n \geq 1$ . In other words,  $a \in \text{rad}(\text{ann}(M/Q))$ .

Since the set of zero divisors of  $M/Q$  is the union of the associated ideals and  $\text{rad } \text{ann}(M/Q)$  is the intersection of the associated ideals, we have:

$$\bigcap_{\mathfrak{p} \in \text{ass}(M/Q)} \mathfrak{p} = \bigcap_{\mathfrak{p} \in \text{ass}(M/Q)} \mathfrak{p} = \text{rad}(\text{ann}(M/Q))$$

So,

**Proposition 5.25.**  $Q \subseteq M$  is primary if and only if  $M/Q$  has a unique associated prime  $\mathfrak{p} = \text{rad}(\text{ann}(M/Q))$ .

We call  $\mathfrak{p}$  the prime *belonging to*  $Q$  and we say that  $Q$  is  $\mathfrak{p}$ -primary. In the special case when  $M = R, Q = \mathfrak{q}$  is an ideal in  $R$  and  $\text{ann}(R/\mathfrak{q}) = \mathfrak{q}$ . So,  $\mathfrak{p} = \text{rad } \mathfrak{q}$ . The definition of a primary module translates to the following.

**Definition 5.26.** An ideal  $\mathfrak{q} \subset R$  is called primary if whenever  $a, b \in R$ ,  $ab \in \mathfrak{q}, b \notin \mathfrak{q} \Rightarrow a \in \text{rad } \mathfrak{q}$ .

**Proposition 5.27.** The intersection of finitely many  $\mathfrak{p}$ -primary submodules of  $M$  is  $\mathfrak{p}$ -primary.

*Proof.* Suppose that  $Q_1, \dots, Q_n$  are  $\mathfrak{p}$ -primary submodules of  $M$ . Then  $\text{ass}(M/Q_i) = \{\mathfrak{p}\}$ . This implies that

$$\text{ass}\left(\bigoplus M/Q_i\right) = \bigcup \text{ass}(M/Q_i) = \{\mathfrak{p}\}$$

Since  $M/\bigcap Q_i$  embeds in  $\bigoplus M/Q_i$  it also has  $\mathfrak{p}$  as its unique associated prime. So,  $\bigcap Q_i$  is  $\mathfrak{p}$ -primary.  $\square$

5.4.2. *existence of primary decomposition.* Suppose that  $N \subseteq M$ . Then a primary decomposition of  $N$  is defined to be a minimal expression of the form

$$N = Q_1 \cap Q_2 \cap \dots \cap Q_n$$

where  $Q_i$  are primary submodules of  $M$ . By the proposition, the prime ideals  $\mathfrak{p}_i$  belonging to the  $Q_i$  will be distinct.

**Theorem 5.28.** Every submodule  $N \subseteq M$  admits a primary decomposition.

*Proof.* If not, there exists a maximal  $N$  with no primary decomposition. The plan of the proof is to express  $N$  as the intersection of two larger submodules  $N = K \cap I$ . By maximality of  $N$ , both  $K$  and  $I$  are intersections of primary submodules. This makes  $N$  an intersection of primary submodules and we will be done.

Since  $N$  is a counterexample, it is in particular not primary. So there is an  $a \in R$  which is a zero divisor for  $M/N$  but is not nilpotent on  $M/N$ . This gives a sequence of submodules of  $L = M/N$ :

$$\ker a_L \subseteq \ker a_L^2 \subseteq \ker a_L^3 \subseteq \dots$$

By the ACC, this sequence stops. So,  $\ker a_L^m = \ker a_L^{m+1} = \dots$ . Let  $\bar{K} = \ker a_L^m \subseteq M/N$ . Since  $a$  is a zero divisor,  $\bar{K} \neq 0$ . Let  $\bar{I} = \text{im } a_L^m$ . Since  $a$  is not nilpotent on  $L$ ,  $\bar{I} \neq 0$ . But  $\bar{K} \cap \bar{I} = 0$  since any element of the intersection has the form  $a^m x$  and satisfies  $a^m(a^m x) = 0$  which implies that  $x \in \ker a_L^{2m} = \ker a_L^m$ . So,  $a^m x = 0$ .

But  $\bar{K} = K/N$  and  $\bar{I} = I/N$  for some  $K, I \subseteq M$ . And  $\bar{K} \cap \bar{I} = 0 \Rightarrow K \cap I = N$ . So we are done.  $\square$

5.4.3. *partial uniqueness of primary decomposition.*

**Lemma 5.29.** *There is a primary decomposition  $N = Q_1 \cap \cdots \cap Q_n$  which is reduced in the sense that*

- (1) *the primes  $\mathfrak{p}_i$  belonging to  $Q_i$  are all distinct and*
- (2) *each of the  $Q_i$  is necessary, i.e.,  $N \neq Q_1 \cap \cdots \cap \widehat{Q}_i \cap \cdots \cap Q_n$  for all  $i$ .*

In the following theorem I used  $N = 0$  in class. But that seemed to be confusing so I put an arbitrary  $N$ . This also explains where “ $L$ ” came from.

**Theorem 5.30.** *Suppose  $N = Q_1 \cap \cdots \cap Q_n$  is a (reduced) primary decomposition of  $N \subseteq M$ . Let  $\mathfrak{p}_i$  be the prime belonging to  $Q_i$ . Then*

$$\text{ass}(M/N) = \{\mathfrak{p}_1, \dots, \mathfrak{p}_n\}$$

*Proof.* ( $\subseteq$ ) Since  $N = Q_1 \cap \cdots \cap Q_n$ , we have a monomorphism

$$M/N \hookrightarrow \bigoplus M/Q_i$$

So,

$$\text{ass}(M/N) \subseteq \text{ass}\left(\bigoplus M/Q_i\right) = \bigcup \text{ass}(M/Q_i) = \{\mathfrak{p}_1, \dots, \mathfrak{p}_n\}$$

( $\supseteq$ ) We want to show that  $\mathfrak{p}_1 \in \text{ass}(M/N)$ . Let

$$L = Q_2 \cap \cdots \cap Q_n$$

Then,  $L \cap Q_1 = N$ . So, we have a monomorphism  $L/N \hookrightarrow M/Q_1$ . So,

$$\text{ass}(L/N) \subseteq \text{ass}(M/Q_1) = \{\mathfrak{p}_1\}$$

Since  $L \neq N$ ,  $L/N$  has at least one associated prime (a maximal  $\text{ann}(x)$  where  $x \neq 0 \in L/N$ ). Therefore,  $\text{ass}(L/N) = \{\mathfrak{p}_1\}$ . Since  $L/N \subseteq M/N$  this implies that  $\mathfrak{p}_1 \in \text{ann}(M/N)$ .  $\square$

**Theorem 5.31.** *Suppose that  $\text{ann}(M/N) = \{\mathfrak{p}_1, \dots, \mathfrak{p}_n\}$  and  $N = Q_1 \cap \cdots \cap Q_n$ ,  $N = Q'_1 \cap \cdots \cap Q'_n$  are two primary decompositions of  $N \subseteq M$  where  $Q_i, Q'_i$  are  $\mathfrak{p}_i$ -primary. Then for every minimal (=isolated)  $\mathfrak{p}_i$ ,  $Q_i = Q'_i$ .*

*Proof.* Suppose that  $\mathfrak{p}_1$  is minimal. This means that it does not contain any of the other associated primes. So, for  $i \geq 2$ , there exists  $a_i \in \mathfrak{p}_i$  so that  $a_i \notin \mathfrak{p}_1$ . This implies that  $a = a_2 a_3 \cdots a_n \in \mathfrak{p}_i$  for  $i \geq 2$  but  $a \notin \mathfrak{p}_1$ .

Claim:  $Q_1 = \{x \in M \mid a^m x \in N \text{ for some } m > 0\}$ . This will prove that  $Q_1 = Q'_1$  since the expression on the right is independent of the primary decomposition.

Pf: ( $\subseteq$ ) Let  $x \in Q_1$ . Then we want to show that  $a^m x$  lies in each  $Q_i$  for sufficiently large  $m$ . This will show that  $a^m x \in \cap Q_i = N$ .  $x \in Q_1 \Rightarrow a^m x \in Q_1$ . For  $i \geq 2$ ,  $a \in \mathfrak{p}_i = \text{rad ann}(M/Q_i) \Rightarrow a^m x \in Q_i$ .

( $\supseteq$ ) Suppose that  $a^m x \in N$ . Then  $x \in Q_1$ . Otherwise,  $a$  is a zero divisor for  $M/Q_1$  which implies that  $a \in \mathfrak{p}_1$  which is a contradiction. This proves the claim and the theorem follows.  $\square$

5.4.4. *example.* (from Atiyah-Macdonald) In this example,  $\mathfrak{p}$  is a prime whose square  $\mathfrak{p}^2$  is not primary. However,  $\text{rad } \mathfrak{p}^2 = \mathfrak{p}$ .

Let  $R = K[X, Y, Z]/(XY - Z^2)$  and let  $x, y, z$  denote the image of  $X, Y, Z$  in  $R$ . Let  $\mathfrak{p} = (x, z)$ . This is a prime ideal in  $R$  since

$$R/\mathfrak{p} \cong K[X, Y, Z]/(X, Z) \cong K[Z]$$

But  $\mathfrak{p}^2 = (x^2, xz, z^2)$  is not primary since  $xy = z^2 \in \mathfrak{p}^2$  but  $x \notin \mathfrak{p}^2$  and no power of  $y$  lies in  $\mathfrak{p}^2$ . Finally, it is clear that  $\text{rad } \mathfrak{p}^2 = \mathfrak{p}$ . (For any  $w \in \mathfrak{p}, w^2 \in \mathfrak{p}^2$ . Conversely,  $\mathfrak{p}^2 \subseteq \mathfrak{p} \Rightarrow \text{rad } \mathfrak{p}^2 \subseteq \mathfrak{p}$ .)

The ideal  $\mathfrak{p}^2$  has two associated primes:  $\mathfrak{p}$  and the maximal ideal  $\mathfrak{m} = (x, y, z)$  which contains  $\mathfrak{p}$ . It is easy to verify that these are associated primes since  $\mathfrak{p}$  is the annihilator of  $z$  module  $\mathfrak{p}^2$  and  $\mathfrak{m}$  is the annihilator of  $x$  module  $\mathfrak{p}^2$ . There are no other associated primes because the primary decomposition of  $\mathfrak{p}^2$  has only two terms:

$$\mathfrak{p}^2 = \mathfrak{q}_1 \cap \mathfrak{q}_2$$

where

$$\mathfrak{q}_1 = (x) = (x, z^2)$$

This is  $\mathfrak{p}$ -primary since  $\mathfrak{p}/\mathfrak{q}_1$  is generated by  $z$  with annihilator  $\mathfrak{p}$ . So there is a short exact sequence

$$0 \rightarrow R/\mathfrak{p} \rightarrow R/\mathfrak{q}_1 \rightarrow R/\mathfrak{p} \rightarrow 0$$

which implies that  $\mathfrak{p}$  is the only prime associated to  $R/\mathfrak{q}_1$  and, therefore,  $\mathfrak{q}_1$  is  $\mathfrak{p}$ -primary. The other primary ideal is

$$\mathfrak{q}_2 = \mathfrak{m}^2 = (x^2, xz, z^2, y^2, yz)$$

This is  $\mathfrak{m}$ -primary since  $\text{rad } \mathfrak{m}^2 = \mathfrak{m} = \cap \{\mathfrak{p}_2 \in \text{ass}(M/\mathfrak{m}^2)\}$ . Since  $\mathfrak{m}$  is maximal,  $\mathfrak{p}_2 = \mathfrak{m}$  is the only associated prime.

There is a modified version of the powers of a prime ideal  $\mathfrak{p}$  called the *symbolic power* of  $\mathfrak{p}$  which always gives a  $\mathfrak{p}$ -primary ideal. As a special case of HW6, problem 2, this is given by

$$\mathfrak{p}^{(2)} = \mathfrak{p}^2 R_{\mathfrak{p}} | R$$

5.5.  $\text{Spec}(R)$ . For any ideal  $I \subset R$  let  $C(I)$  ( $= \mathcal{Z}_I$ ) be the set of all prime ideals  $\mathfrak{p}$  of  $R$  which contain  $I$ .

**Definition 5.32.** *If  $R$  is a Noetherian ring then  $\text{Spec}(R)$  is the set of all prime ideals in  $R$  with the topology given by taking  $C(I)$  (for all ideals  $I$ ), the empty set  $\emptyset$  and the whole space  $\text{Spec}(R)$  to be the closed subsets.*

Since  $R$  is Noetherian,  $\text{Spec}(R)$  satisfies the DCC for closed subsets. In particular, any collection of closed subsets has a minimal element. To verify that this is a topology we need to show that any intersection or finite union of closed sets is closed. The DCC implies that any intersection is a finite intersection.

The first problem on HW6 was to show that, given any ideal  $I$ , the set  $C(I)$  contains a finite number of minimal elements. The fancy proof of this is the following. First, define a closed subset of  $\text{Spec}(R)$  to be *indecomposable* if it is not the union of two proper subsets.

**Lemma 5.33.**  $C(I) = C(\text{rad}(I))$ .

**Lemma 5.34.**  $C(I)$  is indecomposable iff  $\text{rad}(I)$  is prime.

**Lemma 5.35.** *In any topological space satisfying the DCC for closed subsets, every closed subset is a finite union of indecomposable closed subsets.*

**Theorem 5.36.** *For every ideal  $I$ , there are finitely many primes  $\mathfrak{p}_1, \dots, \mathfrak{p}_n$  containing  $I$  so that any other prime which contains  $I$  will contain one of the  $\mathfrak{p}_i$ .*

*Proof.* Let  $C(I) = C_1 \cup \dots \cup C_n$  be a decomposition of  $C(I)$  into indecomposables. Then  $C_i = C(\mathfrak{p}_i)$  for some prime  $\mathfrak{p}_i$  containing  $I$  and, for any other primes  $P$  containing  $I$  we have that  $C(P) \subseteq C(I)$  and therefore,

$$C(P) = (C(P) \cap C_1) \cup \dots \cup (C(P) \cap C_n)$$

Since  $C(P)$  is indecomposable, this implies that  $C(P) \subseteq C_i = C(\mathfrak{p}_i)$  and this implies that  $P$  contains  $\mathfrak{p}_i$ .  $\square$

## 6. LOCAL RINGS

Our last topic in commutative algebra is local rings. I first went over the basic definitions, talked about Nakayama's Lemma and I plan to do discrete valuation rings and then more general valuation rings and then return to places in fields. All rings are commutative with 1. They might not be Noetherian.

## 6.1. Basic definitions and examples.

**Definition 6.1.** A local ring is a ring  $R$  with a unique maximal ideal  $\mathfrak{m}$ .

**Proposition 6.2.** A ring is local iff the nonunits form an ideal.

*Proof.* Suppose first that  $R$  is local with maximal ideal  $\mathfrak{m}$ . Let  $x$  be any element not in  $\mathfrak{m}$ . Then  $x$  must be a unit. Otherwise,  $x$  generates an ideal  $(x)$  which is contained in a maximal ideal other than  $\mathfrak{m}$ .

Conversely, suppose that  $R$  is a ring in which the nonunits form an ideal  $I$ . Then every ideal in  $R$  must be contained in  $I$  since ideals cannot contain units.  $\square$

**Example 6.3.** An example is  $\mathbb{Z}/(p)$ , the integers localized at the prime ideal  $(p)$ . Recall that  $R_{\mathfrak{p}} = S^{-1}R$  is the set of all equivalence classes of fractions  $a/b$  where  $a \in R$  and  $b \in S$  where  $S$  is the complement of  $\mathfrak{p}$ . When  $R$  is an integral domain,  $R_{\mathfrak{p}}$  is contained in the quotient field  $QR$ . So, it is easier to think about:

$$\mathbb{Z}_{(p)} = \left\{ \frac{a}{b} \in \mathbb{Q} \text{ s.t. } p \nmid b \right\}$$

This is a local ring with unique maximal ideal

$$\mathfrak{m} = \left\{ \frac{a}{b} \in \mathbb{Q} \text{ s.t. } p|a, p \nmid b \right\}$$

This is the unique maximal ideal since all of the other elements are clearly units. The quotient  $\mathbb{Z}_{(p)}/\mathfrak{m}$  is isomorphic to  $\mathbb{Z}/p$  although this is not completely trivial.

More generally we have:

**Proposition 6.4.** If  $R$  is a ring and  $\mathfrak{p}$  is a prime ideal then  $R_{\mathfrak{p}} = S^{-1}R$  is a local ring with maximal ideal  $S^{-1}\mathfrak{p}$ .

**6.2. Nakayama's Lemma.** You probably already know this but it is an very useful result which is also very easy to prove. There are two equivalent versions.

**Lemma 6.5** (Nakayama's Lemma, version 1). *Suppose that  $R$  is a local ring and  $M$  is a f.g.  $R$ -module. If  $\mathfrak{m}M = 0$  then  $M = 0$ .*

**Lemma 6.6** (Nakayama's Lemma, version 2). *Suppose that  $R$  is a local ring and  $E$  is a f.g.  $R$ -module and  $F \subseteq E$  is a submodule. If  $E = F + \mathfrak{m}E = 0$  then  $E = F$ .*

First I showed that these are equivalent. The first version is obviously a special case of the second version: just let  $F = 0$ . To prove the second given the first let  $M = E/F$ . Then  $E = F + \mathfrak{m}E$  implies that  $M = \mathfrak{m}M$  which implies  $M = E/F = 0$  which is the same as  $E = F$ .

*Proof of Nakayama, 1st version.* This will be by induction on the number of generators. If this number is zero, then  $M = 0$  so the lemma is true. So, suppose that  $x_1, \dots, x_s$  is a minimal set of generators for  $M$  and  $s \geq 1$ . Since  $x_s \in M = \mathfrak{m}M$ , there exist  $a_1, \dots, a_s \in \mathfrak{m}$  so that

$$x_s = a_1x_1 + \dots + a_sx_s$$

This gives:

$$(1 - a_s)x_s = a_1x_1 + \dots + a_{s-1}x_{s-1}$$

But  $1 - a_s$  is invertible since it is not an element of  $\mathfrak{m}$  (if  $1 - a_s \in \mathfrak{m}$  then we would get  $1 - a_s + a_s = 1 \in \mathfrak{m}$  which is not possible). Therefore,

$$x_s = (1 - a_s)^{-1}(a_1x_1 + \dots + a_{s-1}x_{s-1})$$

which implies that  $x_1, \dots, x_{s-1}$  generate  $M$ . So,  $M = 0$  by induction on  $s$ .  $\square$

**Remark 6.7.** *Note that  $M/\mathfrak{m}M$  is an  $R/\mathfrak{m}$ -module. Since  $R/\mathfrak{m}$  is a field (called the residue field of  $R$ ),  $M/\mathfrak{m}M$  is a vector space over the residue field. If  $f : M \rightarrow N$  is a homomorphism of  $R$ -modules then we get an induced linear mapping*

$$f_* : M/\mathfrak{m}M \rightarrow N/\mathfrak{m}N$$

*given by  $f_*(x + \mathfrak{m}M) = f(x) + \mathfrak{m}N$  (or  $f_*(\bar{x}) = \overline{f(x)}$  if  $\bar{x}$  denotes  $x + \mathfrak{m}M$ ). This defines a functor from the category of  $R$ -modules to the category of vector spaces over  $R/\mathfrak{m}$ .*

**Definition 6.8.** *One definition of the dimension of a local ring  $R$  is the vector space dimension of  $\mathfrak{m}/\mathfrak{m}^2$ :*

$$\dim R = \dim_{R/\mathfrak{m}} \mathfrak{m}/\mathfrak{m}^2$$

**Proposition 6.9.**  $x_1, \dots, x_n$  are generators for the  $R$ -module  $M$  if and only if their images  $\bar{x}_1, \dots, \bar{x}_n$  span the vector space  $M/\mathfrak{m}M$ .

*Proof.* ( $\Rightarrow$ ) This direction is clear. Every element  $x \in M$  can be written as  $x = \sum a_i x_i$ . So, any element  $\bar{x} = x + \mathfrak{m}M$  of  $M/\mathfrak{m}M$  can be written as  $\bar{x} = \sum \bar{a}_i \bar{x}_i$ .

(*neht*) Let  $N$  be the submodule of  $M$  generated by  $x_1, \dots, x_n$ . If  $\bar{x}_1, \dots, \bar{x}_n$  span  $M/\mathfrak{m}M$  then  $N + \mathfrak{m}M = M$ . Then  $N = M$  by Nakayama.  $\square$

**Corollary 6.10.**  $x_1, \dots, x_n$  is a minimal set of generators for  $M$  iff  $\bar{x}_1, \dots, \bar{x}_n$  form a basis for the vector space  $M/\mathfrak{m}M$ .

**Theorem 6.11.** Any finitely generated  $R$ -module  $M$  is projective if and only if it is free (isomorphic to  $R^n$ ).

*Proof.* It is clear that every free module is projective. So, suppose that  $M$  is projective. Let  $x_1, \dots, x_n$  be a minimal set of generators for  $M$ . Then we get an epimorphism  $\phi : R^n \rightarrow M$  sending the  $i$ -th generator of  $R^n$  to  $x_i$ . Since  $M$  is projective by assumption, there is a section  $s : M \rightarrow R^n$  of this homomorphism. I.e.,  $\phi \circ s = id_M$ . This gives the following diagram:

$$\begin{array}{ccccc} M & \xrightarrow{s} & R^n & \xrightarrow{\phi} & M \\ \downarrow & & \downarrow & & \downarrow \\ M/\mathfrak{m}M & \xrightarrow{\bar{s}} & R^n/\mathfrak{m}^n & \xrightarrow{\bar{\phi}} & M/\mathfrak{m}M \end{array}$$

Since  $\phi \circ s$  is the identity on  $M$ ,  $\bar{\phi}/\bar{s}$  is the identity on  $M/\mathfrak{m}M$ . Therefore,  $\bar{s} : M/\mathfrak{m}M \rightarrow R^n/\mathfrak{m}^n$  is a monomorphism. But  $M/\mathfrak{m}M$  and  $R^n/\mathfrak{m}^n$  have the same finite dimension over  $R/\mathfrak{m}$ . Therefore,  $\bar{s}$  is an isomorphism. This implies that  $s(M) + \mathfrak{m}^n = R^n$ . By Nakayama this shows that  $s(M) = R^n$ . So,  $M \cong R^n$  as we wanted to show.  $\square$

**6.3. Complete local rings.** If  $R$  is a local ring we get a sequence of ring homomorphisms:

$$\dots \rightarrow R/\mathfrak{m}^{n+1} \rightarrow R/\mathfrak{m}^n \rightarrow R/\mathfrak{m}^{n-1} \rightarrow \dots \rightarrow R/\mathfrak{m}$$

The inverse limit  $\lim_{\leftarrow} R/\mathfrak{m}^n$  is the set of all sequences  $(a_n \in R/\mathfrak{m}^n)$  which are *compatible* in the sense that  $a_n$  maps to  $a_{n-1}$  under the homomorphism  $R/\mathfrak{m}^n \rightarrow R/\mathfrak{m}^{n-1}$ , i.e.,  $a_{n-1} = a_n + \mathfrak{m}^{n-1}$ .

The inverse limit is defined by a universal condition. It is the universal object  $L$  with ring homomorphisms  $f_n : L \rightarrow R/\mathfrak{m}^n$  so that the composition  $L \rightarrow R/\mathfrak{m}^n \rightarrow R/\mathfrak{m}^{n-1}$  is  $f_{n-1}$ . In other words, given any other  $L'$  with homomorphisms  $f'_n : L' \rightarrow R/\mathfrak{m}^n$ , there exists a unique ring homomorphism  $g : L' \rightarrow L$  so that  $f_n \circ g = f'_n$  for all  $n$ . It is easy to see that the set of all compatible sequences  $(a_n)$  satisfies this universal property since  $g(x) = (f'_n(x))$

**Definition 6.12.**  $R$  is a complete local ring if  $R \cong \lim_{\leftarrow} R/\mathfrak{m}^n$ .

**Example 6.13.** The  $p$ -adic integers  $\mathbb{Z}_p$  form a complete local ring by definition. They are defined to be  $\mathbb{Z}_p = \lim_{\leftarrow} \mathbb{Z}/p^n\mathbb{Z}$ . I.e., it is the inverse limit of the sequence

$$\dots \rightarrow \mathbb{Z}/p^n \rightarrow \mathbb{Z}/p^{n-1} \rightarrow \dots \rightarrow \mathbb{Z}/p$$

In other words,  $\mathbb{Z}_p$  is the set of all sequences  $(a_n)$  of integers  $a_n$  defined modulo  $p^n$  so that  $a_n + p^{n-1}\mathbb{Z} = a_{n-1}$ . There is a natural ring monomorphism  $\mathbb{Z} \hookrightarrow \mathbb{Z}_p$  sending  $m$  to the sequence  $(a_n = m)$  for all  $n$ . The unique maximal ideal is given by  $a_1 = 0$ , i.e.,  $\mathfrak{m}$  is the kernel of the epimorphism  $\mathbb{Z}_p \twoheadrightarrow \mathbb{Z}/p$  given by  $(a_n) \mapsto a_1$ .

A typical element of  $\mathbb{Z}_3$  has an infinite 3-ary expansion with digits 0, 1, 2 to the left of the decimal place:

$$\dots 2110220112.$$

$p$ -adic integers do not have signs. They are all positive since, e.g.,

$$-1 = \dots 2222222.$$

The maximal ideal is the set of all numbers with last digit equal to 0.

Problem: Show that there is a monomorphism of rings  $\mathbb{Z}_{(p)} \hookrightarrow \mathbb{Z}_p$  which is not an epimorphism (since  $\mathbb{Z}_p$  is a Cantor set and therefore uncountable whereas  $\mathbb{Z}_{(p)}$  is countable, being a subset of  $\mathbb{Q}$ ).

**6.4. Discrete valuation rings.** This is the last topic in commutative algebra.

6.4.1. *definition.* I gave two of the elementary definitions.

**Definition 6.14** (1st definition). A discrete valuation ring (DVR) is an integral domain  $R$  together with a mapping

$$v : QR^* \rightarrow \mathbb{Z}$$

called a valuation from the group of nonzero elements  $QR^*$  of the quotient field  $QR$  of  $R$  onto  $\mathbb{Z}$  so that

- (1)  $v(ab) = v(a) + v(b)$  for all  $a, b \in QR^*$
- (2)  $v(a + b) \geq \min(v(a), v(b))$  for all  $a, b \in QR^*$
- (3)  $R^* = \{a \in QR^* \mid v(a) \geq 0\}$

I pointed out that the first condition implies  $v(1) = 0$  (since  $v(1) = v(1) + v(1)$ ) and  $v(a/b) = v(a) - v(b)$  (since  $a = (a/b)b \Rightarrow v(a) = v(a/b) + v(b)$ ).

**Example 6.15.** Take  $R = \mathbb{Z}_{(p)}$ . Then  $Q\mathbb{Z}_{(p)} = \mathbb{Q}$  and we can define

$$v_p : \mathbb{Q}^* \rightarrow \mathbb{Z}$$

by  $v_p\left(\frac{a}{b}\right) = n$  where  $n$  is the number of times that  $p$  divides  $a/b$ . I.e.,

$$\frac{a}{b} = p^n \frac{c}{d}$$

where  $p \nmid c$  and  $p \nmid d$ . It is easy to verify that the conditions are satisfied. We figured out in class that equality holds in (2) when  $v(a) \neq v(b)$ .

There is one thing I don't like about the first definition. The valuation is assumed to be defined outside of the original set  $R$ . The second definition restricts the valuation just to  $R^*$ .

**Definition 6.16** (2nd definition). A DVR is a domain  $R$  together with a mapping

$$v : R^* \rightarrow \{0, 1, 2, \dots\}$$

so that

- (1)  $v(ab) = v(a) + v(b)$  for all  $a, b \in R^*$
- (2)  $v(a + b) \geq \min(v(a), v(b))$  for all  $a, b \in R^*$
- (3')  $b|a \iff v(b) \leq v(a)$

**Proposition 6.17.** These two definitions are equivalent.

*Proof.* ( $\Rightarrow$ ) If  $v$  is defined on  $QR^*$  we can just take the restriction of  $v$  to  $R^*$ . Then the only condition we need to check is (3'). If  $b|a$  then  $a = bc$  for some  $c \in R^*$ . So,  $v(a) = v(b) + v(c) \geq v(b)$ . Conversely, if  $v(b) \leq v(a)$  then  $v(a/b) = v(a) - v(b) \geq 0$ .

( $\Leftarrow$ ) Suppose we have  $v$  defined on  $R^*$ . Then we can extend it to  $QR^*$  by the equation

$$v\left(\frac{a}{b}\right) = v(a) - v(b)$$

This is well defined since  $a/b = c/d$  implies  $ad = bc$  which implies that

$$v(ad) = v(a) + v(d) = v(b) + v(c) = v(bc)$$

$$v(a) - v(b) = v(c) - v(d)$$

Conditions (1) is obvious. For condition (2):

$$\begin{aligned} v\left(\frac{a}{c} + \frac{b}{c}\right) &= v\left(\frac{a+b}{c}\right) = v(a+b) - v(c) \\ &\geq \min(v(a), v(b)) - v(c) \\ &= \min(v(a) - v(c), v(b) - v(c)) \\ &= \min(v(a/c), v(b/c)) \end{aligned}$$

For the last condition:

$$v(a/b) \geq 0 \iff v(a) \geq v(b) \iff b|a \iff a/b \in R$$

□

### 6.4.2. properties.

**Proposition 6.18.** *Suppose that  $R$  is a DVR with valuation  $v$ . Then*

- (1)  $a \in R$  is a unit iff  $v(a) = 0$ .
- (2)  $R$  is a local ring
- (3)  $\mathfrak{m} = \{a \in R \mid v(a) \geq 1 \text{ and } a \neq 0\}$
- (4)  $\mathfrak{m} = (\pi)$  for any  $\pi \in R$  so that  $v(\pi) = 1$ .
- (5)  $\mathfrak{m}^n = (\pi^n)$ .

$\pi$  is called the *uniformizer* of  $R$ .

*Proof.* For (1),  $a$  is a unit iff  $a|1$  iff  $v(a) \leq v(1) = 0$  iff  $v(a) = 0$ . This implies that the set of nonunits is  $I = \{a \in R \mid v(a) \geq 0 \text{ or } a = 0\}$ .  $R$  is a local ring iff  $I$  is an ideal. But this is easy:  $I$  is closed under addition since

$$v(a+b) \geq \min(v(a), v(b)) \geq 1$$

and it is an ideal since, for any  $a \in I, r \in R$  which are nonzero,

$$v(ra) = v(r) + v(a) \geq v(a) \geq 1$$

which implies  $ra \in I$ . Therefore,  $I = \mathfrak{m}$  is the unique maximal ideal.

Now choose any  $\pi \in R$  so that  $v(\pi) = 1$ . Then,  $\pi$  divides any element  $a \in \mathfrak{m}$  since  $v(\pi) \leq v(a)$ . So,  $\mathfrak{m} = (\pi)$ .

Finally, it is clear that if  $\pi$  generates  $\mathfrak{m}$  then  $\pi^n$  generates  $\mathfrak{m}^n$ .  $\square$

The converse to this is also true giving a 3rd definition of DVR:

**Proposition 6.19.** *If  $R$  is a local domain whose unique maximal ideal is principal, then  $R$  is a DVR.*

*Proof.* If  $\pi$  is a generator for  $\mathfrak{m}$  then any nonzero element of  $R$  can be written uniquely as  $\pi^n u$  where  $u$  is a unit. Then the valuation is given by  $v(\pi^n u) = n$ .  $\square$

6.4.3. *DVRs and Riemann surfaces.* The theorem is that there is a 1-1 correspondence between isomorphism classes of field extensions  $E$  of  $\mathbb{C}$  of transcendence degree 1 and isomorphism classes of (compact) Riemann surfaces (complex curves). The points of the Riemann surface are given by the discrete valuations  $v : E^* \rightarrow \mathbb{Z}$  associated to places in  $E$  which are DVRs.

I didn't prove this but I gave an example, the simplest possible example, which is  $E = \mathbb{C}(X)$ . This field corresponds to the Riemann sphere  $S^2 = \mathbb{C} \cup \infty$ . Any point  $x_0 \in \mathbb{C}$  corresponds to the valuation  $v_{x_0} : E^* \rightarrow \mathbb{Z}$  given by

$$v_{x_0} \left( \frac{f(X)}{g(X)} \right) = n$$

where  $n$  is the number of times that  $X - x_0$  divides  $f(X)/g(X)$ . In other words,

$$\frac{f(X)}{g(X)} = (X - x_0)^n \frac{\phi(X)}{\psi(X)}$$

where  $\phi(X), \psi(X)$  are not divisible by  $X - x_0$ . The condition that these are not divisible by  $X - x_0$  is equivalent to the condition that  $\phi(x_0) \neq 0$  and  $\psi(x_0) \neq 0$ . In other words, the function  $f(X)/g(X)$  has a zero of order  $n$  at  $x_0$ . When  $n < 0$ ,  $f(X)/g(X)$  has a *pole* at  $x_0$ , i.e.,  $f(x_0)/g(x_0) = \infty$ . The DVR is the set of all  $f(X)/g(X)$  which does not have a pole at  $x_0$ . The maximal ideal is the set of all rational functions which are zero at  $x_0$ .

There is one other valuation on  $E = \mathbb{C}(X)$  corresponding to the point at infinity. This should be the set of all rational functions  $f(X)/g(X)$  which do not have a pole at  $\infty$ . This is equivalent to saying that  $\deg(f) \leq \deg(g)$ . So, the valuation at infinity is:

$$v_\infty(f(X)/g(X)) = \deg(g) - \deg(f).$$