

# MATH 470-3 Commutative Algebra

Chi Li

## Contents

<b>0 Syllabus</b>	<b>1</b>
<b>1</b>	<b>2</b>
<b>2</b>	<b>4</b>
<b>3</b>	<b>6</b>
<b>4</b>	<b>7</b>
<b>5</b>	<b>9</b>
<b>6 Spec</b>	<b>13</b>
<b>7</b>	<b>16</b>
<b>8</b>	<b>18</b>
<b>9 Integral Closure</b>	<b>20</b>
<b>10</b>	<b>23</b>
<b>11</b>	<b>25</b>
<b>12 Nullstellensatz</b>	<b>26</b>

If you see any typos, please email [chili2025@u.northwestern.edu](mailto:chili2025@u.northwestern.edu).

## 0 Syllabus

### Topics

1. Commutative algebra, linear algebra, tensor algebra.
2. Rings, ideals, modules, localization, Zariski topology/spec, tensor products.
3. Further topics include: Noether's normalization, going up and going down, completions of rings, dimension theory, Zariski's main theorem, Nullstellensatz.
4. Representation theory, noncommutative algebra.

## References

1. Atiyah and Macdonald (lots of problems here but pretty terse)
2. Milne's notes on commutative algebra

Both are available for free online.

## Grades

- Midterm: 20%
- Final: 20%
- Problemsets (fortnightly): 60%

Ask for hints on the problemsets only for the first 9 days. Office hours Saturday 1-2 on zoom. Further OH TBD.

## 1

### Notation

All rings are commutative, usually denoted  $R, A, B$  and have multiplicative identity 1.  $I, J, M, P$  denote ideals.  $M$  ideals are maximal and  $P$  ideals are prime. Modules are denoted by  $M, N$ .

#### Definition 1.1 (Prime Ideal)

An ideal  $P$  is prime if

$$xy \in P \implies x \in P \text{ or } y \in P.$$

#### Definition 1.2 (Maximal Ideal)

An ideal  $M$  is maximal if  $M \subset I \implies I = R$ .

#### Proposition 1.3

Maximal ideals are prime

*Proof.* We can show something stronger. We have equivalent definitions that

- An ideal  $I$  is prime iff  $R/I$  is an integral domain.
- An ideal  $I$  is maximal iff  $R/I$  is a field.

A field is an integral domain so we are done.



**Definition 1.4 (Special elements of ring)**


Let  $x \in R$ . Then  $x$  is

1. A unit, if there is  $y \in R$  such that  $xy = 1$ .
2. A zero divisor, if there is  $y \in R \setminus \{0\}$  such that  $xy = 0$ .
3. Nilpotent, if there is some  $n$  such that  $x^n = 0$ .

**Remark.** The set of units form a multiplicative set. The complement of units need not form an ideal, for instance  $\mathbb{Z}/6$ . Similarly, the set of zero divisors need not form an ideal.

**Proposition 1.5**


The set of nilpotent elements form an ideal. We call this the nilradical of  $R$  and denote it  $n(R)$ .

*Proof.* 0 is nilpotent,  $n(R)$  is nonempty. Let  $x^n = 0, y^m = 0$ . Then  $(x + y)^{n+m} = 0 = (rx)^n$  for any  $r \in R$ . So the nilradical is closed under addition and multiplication. 

**Proposition 1.6**

We have

$$n(R/n(R)) = \{0\}.$$

*Proof.* Let  $[a]$  be nilpotent in  $R/n(R)$ . Then there exists  $k$  such that  $a^k \in n(R)$ . But then this means  $a$  is nilpotent in  $R$  too. So  $[a] = 0$ . 

**Definition 1.7 (Reduced ring)**

$R$  is reduced if  $n(R)$  is trivial.

Similarly we can define nilradicals based on other ideals.

**Definition 1.8 (Nilradical)**

Let  $I \subseteq R$  be an ideal. Then the nilradical of  $I$  is

$$n(I) \stackrel{\text{def}}{=} \{r \in R : \exists n \text{ s.t. } r^n \in I\}.$$

**Proposition 1.9**

- $n(I)$  is an ideal.
- $n(R/n(I))$  is trivial.

*Proof.* The same as above. 

## 2

### Theorem 2.1


$$n(R) = \bigcap_{\text{prime ideals } P \subseteq R} P.$$

*Proof.* The inclusion  $\subseteq$  is easy. Let  $r \in R$  be nilpotent and  $P$  be a prime ideal. Then  $r^n = 0 \in P$ . Backwards induction on  $n$  gives that  $r \in P$ .

We now prove the opposite inclusion. Let  $r \in R$  be not nilpotent. Let  $S$  be the set of all ideals of  $R$  that do not contain any power of  $r$ . We give this a partial order by inclusion. This is non-empty as the trivial ideal satisfies this condition. Every ascending chain is bounded by the union of the ideals, and the union of the ideals in an ascending chain is an ideal that does not contain any power of  $r$ . So we apply Zorn's lemma to obtain a maximal element of the set  $P$ . We want to show that  $P$  is prime.

Suppose not, then there is  $xy \in P$  but  $x \notin P$  and  $y \notin P$ . But now we have ideals  $(P, x)$  and  $(P, y)$  that both contain some power of  $r$ , say  $r^n$  and  $r^m$  respectively. We have

$$r^n = p_1 + a_1x, r^m = p_2 + a_2y.$$


But now  $r^{n+m} = (p_1 + a_1x)(p_2 + a_2y) \in P$  giving a contradiction. 

### Definition 2.2

$S \subseteq R$  is multiplicatively closed  $s_1, s_2 \in S \implies s_1s_2 \in S$ .

### Theorem 2.3

Let  $S$  be multiplicatively closed. Then there is a prime ideal that is disjoint from  $S$ .

*Proof.* Same as above. But now set the set of ideals to be those that are disjoint from  $S$ , and find the maximal element. The previous example for the nilradical proof is for the multiplicatively closed set  $\{r, r^2, r^3 \dots\}$ . 

**Remark.** This ideal need not be maximal. For instance, take the ring of integers and  $S$  be  $\mathbb{Z} - \{0\}$ . The only prime ideal disjoint from this is the zero ideal. Another example would be  $\mathbb{C}[x, y]$ . By Hilbert's Nullstellensatz the only maximal ideals are in the form  $(x - a, y - b)$ . The set of polynomials

$$\{f \in \mathbb{C}[x, y] - \{0\} : f(x, y) = g_1(x)g_2(y), g_1, g_2 \in \mathbb{C}[t]\}$$

intersects every maximal ideal. A non trivial prime ideal that does not intersect  $S$  would be  $(x - y^2)$  which does not split into products of  $x$  and  $y$ .

We now consider the intersection of all maximal ideals.


### Definition 2.4 (Jacobson Radical)

The Jacobson radical of  $R$  is denoted  $J(R)$  and is the intersection of all maximal ideals in  $R$ .

**Theorem 2.5**

$J(R)$  consists of exactly the elements  $x \in R$  such that  $1 - xy$  is a unit for all  $y \in R$ .

*Proof.* For the  $\subseteq$  direction, let  $1 - xy$  be not a unit. Then there is a maximal ideal containing  $1 - xy$ . This ideal cannot contain  $x$ , as this would be the ideal would also contain  $(1 - xy) + x(y) = 1$ . Therefore  $x$  is not in the Jacobson radical.

For the other direction, suppose that  $x$  is not contained in a maximal ideal  $m$ . Then we would have  $(m, x) = R$ , so that  $m + xy = 1$  for some  $y$ , then  $1 - xy = m$  is not a unit. 

**Definition 2.6 (Local Ring)**

$R$  is called a local ring if it contains exactly one maximal ideal.


**Example 2.7**

- A field is a local ring.
- Let  $P$  be a prime ideal that does not contain 1. Take its complement  $S$ , which is a multiplicatively closed set. The localization  $S^{-1}R$  is a local ring. This is because set of non-units in this ring are in the form  $\frac{p}{s}$  for  $p \in P, s \in S$ , the others  $\frac{s_1}{s_2}$  are invertible.

**Lemma 2.8**


$R$  is a local ring iff there is an ideal  $M$  such that  $R \setminus M$  is the set of all units in  $R$ .

*Proof.* The backwards direction is obvious. This  $M$  is maximal, and contains all other ideals except for  $R$ .

For the forwards direct, suppose not, then consider a maximal ideal. Take an element from its complement that is not a unit and consider a maximal ideal containing it. 

**Lemma 2.9**

Let  $M \subset R$  be maximal. Then if  $1 + m$  is a unit for every  $m \in M$ ,  $R$  is local.

*Proof.* We have  $R/M$  is a field. Therefore, for every  $r \in M^c$ . We have  $y$  such that  $ry = 1 + m$  for some  $m \in M$ . Since  $ry$  is a unit,  $r$  is a unit. 

**Example 2.10**

The formal power series ring  $\mathbb{C}[[x_1, \dots, x_n]]$  is local. Take the ideal  $(x_1, \dots, x_n)$ . Then for every power series  $f$  in  $x_1, \dots, x_n$  with 0 constant term, we show that  $1 + f$  is a unit. This is apparent as we have the formal power series  $(1 + f)^{-1} = (1 - f + f^2 - f^3 + \dots)$ .

### 3


#### Theorem 3.1

Let  $R$  be a ring. Let  $P_1, \dots, P_n \subseteq R$  be prime ideals. Let  $I \subseteq \cup P_i$  be an ideal. Then  $I$  is contained in some  $P_i$ .

**Remark.** There is a counterexample. In  $\mathbb{F}_2[x, y]$  pick  $I = (x, y)$ . We can find three ideals in  $\mathbb{F}_2[x, y]$  whose union contains  $(x, y)$  but none contains  $(x, y)$ . (left as an “interesting” exercise) The same is not true for an infinite field.

*Proof.* We induct on  $n$ .  $n = 1$  is easy. We look at the case for  $n = 2$  as an example. Let  $n = 2$ . We suppose that  $I$  is not contained in either  $P_1$  or  $P_2$ . Suppose  $a_1, a_2 \in I$  such that  $a_1 \notin P_1, a_2 \notin P_2$  (so that  $a_1 \in P_2, a_2 \in P_1$ ). Then  $a_1 + a_2 \in I$  is not an element of  $P_1$  or  $P_2$ . This gives a contradiction.

The idea is to pick element in  $I \cap P_{k \neq i}$  for each  $i$  from  $1 - n$ .

Suppose the statement holds for  $n - 1$ , we want to show for  $n$ . Then by contradiction suppose  $I$  is not contained in either of the  $P_i$ 's. Then by the induction hypothesis we can assume that there are no inclusion among the  $P_i$ 's, since this will reduce to the case for  $n - 1$ . Choose elements  $a_i \in I$  but  $a_i \notin P_i$ . Then for each other  $P_{j \neq i}$  pick an element  $b_k$  distinct from  $P_i$  and multiply  $a_i$  by  $b_k$ . Then this product of  $b_k$ 's and  $a_i$  is not in  $P_i$ , as  $P_i$  is prime. However, it is in the intersection of  $I$  and the  $P_{k \neq i}$ 's. The sum of all the products  $b_{k \neq i} a_i$  is not in each of the ideals. 

#### Definition 3.2 (Coprime ideals)

Let  $I_1, I_2 \subseteq R$ . Then they are coprime  $I_1 + I_2 = R$ .

#### Proposition 3.3

Let  $I_1, I_2 \subseteq R$ . Let

$$I_1 \cdot I_2 \stackrel{\text{def}}{=} (ab : a \in I_1, b \in I_2).$$

We have


$$I_1 \cdot I_2 \subseteq I_1 \cup I_2,$$

with equality when the ideals are coprime.

**Remark.** The equality condition of coprime is not an if and only if in the first statement. For example the  $0$  ideal plus the  $0$  ideal does not have  $1$ . The algebraic completion  $\bar{\mathbb{Z}} \subseteq \bar{\mathbb{Q}}$  is a non-noetherian subring and contains  $p, p^{1/2}, p^{1/3}, \dots$ . The ideal generated by  $I = p^{a/b} : a/b \text{ is a positive real number}$  satisfies  $I^2 = I = I \cap I$ .

*Proof.* We prove the specific statement first. The first inclusion is obvious as  $ab \in I_1 \cap I_2$ . For the other inclusion, let  $I, J$  coprime ideals Pick  $i \in I, j \in J$  such that  $i + j = 1$ . Then for every  $a \in I \cap J$  we have

$$a = a \cdot 1 = ai + aj$$

is a sum of an element in  $I$  and an element in  $J$ . 

**Theorem 3.4 (Chinese Remainder)**

Let  $I, J$  be coprime ideals. Then

$$R/(I \cap J) \rightarrow R/I \oplus R/J$$

is an isomorphism.


In general, let  $I_1, \dots, I_n$  be ideals of  $R$  such that they are pairwise coprime. Then we have

$$R/\cap_i I_i \rightarrow \oplus R/I_i$$

is an isomorphism.

*Proof.* We prove the case for two ideals. The case for multiple ideals is an exercise. We have a natural ring morphism from  $R \rightarrow R/I \oplus R/J$ . So we want to show that this is surjective with kernel  $I \cap J$ .

The kernel is  $I \cap J$  by definition as  $x = 0 \pmod I$  and  $x = 0 \pmod J$  iff  $x \in I$  and  $x \in J$ .

For surjection, pick  $i \in I, j \in J$  such that  $i + j = 1$ . Then  $i = 1 \pmod J$  and  $j = 1 \pmod I$ . Then for every  $([a], [b]) \in R/I \oplus R/J$ ,  $aj + bi$  maps to this element by linearity. 

**Theorem 3.5 (Nakayama's Lemma)**


Let  $J \subseteq J(R)$  be an ideal. Let  $M$  be a finitely generated  $R$  module such that  $JM = M$ . Then  $M = 0$ .

*Proof.* Let  $(e_1, \dots, e_n)$  be a minimal set of generators for  $M$ . Then we have

$$m_1 = j_1 m_1 + j_2 m_2 + \dots + j_n m_n.$$

Such that  $j_i \in J \subseteq J(R)$ . But then

$$(1 - j_1)m_1 = j_2 m_2 + \dots + j_n m_n.$$

Because  $1 - j_1$  is a unit by the characterization of Jacobson radical, we are done. 

**Remark.** *The thing fails if  $M$  is not finitely generated. Let  $R$  be the set of fractions  $\{a/b : p \text{ does not divide } b\}$ . Then  $(p)$  is the unique maximal ideal. If we take  $M = \mathbb{Q}$ , we have  $(p)M = M$ .*

## 4

Let  $R$  be a local ring with maximal ideal  $m$ ,  $M$  a finitely generated  $R$ -module.

**Corollary 4.1:** If the  $m_1, \dots, m_n \in M$  generate  $M/m$  as a  $R/m$  vector space, then  $m_1, \dots, m_n$  generate  $M$  as an  $R$  module.


*Proof.* This is an application of Nakayama's Lemma.

Let  $N$  be the module generated by the  $m_i$ 's. We have

$$M = N \oplus mM.$$

Now we can mod everything by  $N$  to get

$$M/N = 0 \oplus mM/N.$$

Thus by Nakayama's lemma,  $N = M$ . 

#### Theorem 4.2

Let  $M$  be a non-zero Noetherian  $R$  module. Then  $\exists$  a filtration by submodules  $\{0\} = M_0 \subset M_1 \subset \dots \subset M_n = M$  such that  $M_{i+1}/M_i = R/p_i$  for some prime ideal  $p_i$ .


#### Definition 4.3 (Annihilator)

Let  $M$  be an  $R$  module. For  $m \in M$  we define the annihilator of  $m$

$$\text{Ann}(m) \stackrel{\text{def}}{=} \{r \in R : rm = 0\}.$$

This is an ideal.

*Proof.* Look at all  $\text{Ann}(m)$  for each  $0 \neq m \in M$ . There is a maximal element in this set by Zorn's lemma. (Exercise) The maximal element is a prime ideal.

Let  $M_1 = Rm_1$ , where  $m_1$  is picked such that annihilator is maximal. This is isomorphic to  $R/\text{Ann}(m_1)$ . Now we can repeat the process on  $M/M_1$  to pick the second prime ideal. This process terminates by Noetherian condition of module. 

#### Theorem 4.4 (Krull's Intersection)

Let  $R$  be a noetherian ring.  $I \subset R$  an ideal. Then

$$I \cap \bigcap_{n \geq 1} I^n = \bigcap_{n \geq 1} I^n.$$

**Remark.** *This is not in Atiyah Macdonald, but is in Milne.*

*It is tempting to move the  $I$  into the intersection, but it is not the same. Counterexample: exercise (smile)*

*Proof.* Let  $I = (a_1, \dots, a_r)$ . Then  $I^2 = (a_i a_j)$ , and so on  $I^n = (n - \text{products of the } a_i)$ . The trick now is to notice that this is related to the symmetric polynomials

$$I^n = \{g(a_1, \dots, a_r) : g \text{ is a } R\text{-homogeneous polynomial of degree } n.\}$$

Let  $S_m \stackrel{\text{def}}{=} \{g(x_1, \dots, x_r) \in R[x_1, \dots, x_r] : g(a_1, \dots, a_r) \in \bigcap_{n \geq 1} I^n\}$ . Then

$$\left( \bigcup_{m \geq 1} S_m \right) \subseteq R[x_1, \dots, x_r]$$

is a finitely generated (generated by  $(f_i)$ ) ideal by Hilbert Basis theorem.

Let  $d$  be such that  $f_i \in S_{m_i}$  satisfies  $d \geq m_i$ .


Let  $b \in \bigcap I^n$ . Then  $b \in I^{d+1}$ , and we write

$$b = f(a_1, \dots, a_r),$$



$f \in S_{d+1}$ , so can be written as

$$f = \sum_i g_i f_i.$$

We can pick  $g_i$  such that these are homogeneous with degree  $\deg f - \deg f_i > 0$ . If not, the different degrees have to cancel each other. So the  $g_i$  have no constant terms. Evaluate these at the  $a_i$ 's. Since  $g$  has no constant term,  $g(a_i) \in I$  and we have expressed  $f$  in the left hand side. 

## Localization

### Definition 4.5 (Multiplicatively Closed Set)

$S \subseteq R \setminus \{0\}$  is multiplicatively closed if it contains 1 and  $s, t \in S \implies st \in S$ .

We define localization

$$S^{-1}R \stackrel{\text{def}}{=} \left\{ \left[ \frac{r}{s} \right] : r \in R, s \in S \right\} / \sim,$$

where the equivalence relation is

$$\frac{r_1}{s_1} \sim \frac{r_2}{s_2} \text{ if } (r_1 s_2 - r_2 s_1) \cdot s = 0$$

for some  $s \in S$ .

### Proposition 4.6

$S^{-1}R$  is a ring by the standard definitions plus and minuses.

$$\begin{aligned} \frac{r_1}{s_1} + \frac{r_2}{s_2} &= \frac{r_1 s_2 + r_2 s_1}{s_1 s_2} \\ \frac{r_1}{s_1} \cdot \frac{r_2}{s_2} &= \frac{r_1 r_2}{s_1 s_2}. \end{aligned}$$

It has additive and multiplicative identity  $\frac{0}{1}, \frac{1}{1}$  respectively.

### Proposition 4.7

There is a canonical ring homomorphism  $R \rightarrow S^{-1}R$ . This sends  $r \rightarrow \frac{r}{1}$ .

### Theorem 4.8 (Universal property of localization)

Let  $S \subset R$  be multiplicatively closed. Let  $g : R \rightarrow R'$  be a ring homomorphism such that  $g(s)$  is a unit for every  $s \in S$ . Then there is a unique map  $g_s : S^{-1}R \rightarrow R'$  such that the composite  $R \rightarrow S^{-1}R \rightarrow R'$  is equal to  $g$ .

In other words,  $S^{-1}R$  is the smallest ring such that every element in  $S$  is a unit.

## 5

We now prove the Universal property of localization.

*Proof.* We need to define  $S^{-1}f(a/s)$ . Notice we must have  $S^{-1}f(a/s)S^{-1}f(s) = S^{-1}f(a)$ . So we must have

$$S^{-1}f(a/s) = f(a)f(s)^{-1}.$$


This is the uniqueness. We now need this to be well defined.

Suppose  $\frac{a}{s} = \frac{a'}{s'}$ . Then there is  $\tilde{s} \in S$  such that  $(as' - sa')\tilde{s} = 0$ . Then we have

$$(f(a)f(s') - f(s)f(a'))f(\tilde{s}) = 0$$

$f(\tilde{s})$  is a unit, so we have

$$f(a)f(s') - f(s)f(a') = 0 \implies f(a)f(s)^{-1} = f(a')f(s')^{-1}.$$

Now we can confirm that this indeed satisfy ring homomorphism properties (this is just tedious). 

### Proposition 5.1

It is useful to think of quotients  $A/I$  as surjective maps  $A \rightarrow B$  with kernel  $I$ .

In the same way, it is useful to think of localization  $S^{-1}R$  as


$$f : A \rightarrow B,$$

such that

- $f(s)$  is a unit for  $s \in S$
- Every element in  $B$  is in the form  $f(a)/f(s)$ .
- $f(a) = 0 \implies \exists s \in S$  such that  $as = 0$

*Proof.* By the universal property of quotients and the first property, we have  $S^{-1}A \rightarrow B$ . The second property guarantes this map is surjective. We now need this map to be injective.

$$S^{-1}f\left(\frac{a}{s}\right) = 0 \implies f(a)f(s)^{-1} = 0 \implies f(a) = 0$$

By the third property, we have  $s' \in S$  such that  $as' = 0$ . But this would mean  $\frac{a}{s} = \frac{as'}{ss'} = 0$  to begin with. 

Let  $M$  be an  $A$ -module. We define  $S^{-1}M$

$$S^{-1}M \stackrel{\text{def}}{=} \left\{ \frac{m}{s} : m \in M, s \in S \right\} / \sim,$$

with the equivalence

$$\frac{m}{s} \sim \frac{m'}{s'}$$


if  $\exists \tilde{s} \in S$  s.t.  $\tilde{s}(s'm - sm') = 0$ .

**Notation.** If  $S = A/p$  for some prime ideal  $p$ , we write  $A_p \stackrel{\text{def}}{=} S^{-1}A$ ,  $M_p \stackrel{\text{def}}{=} S^{-1}M$ . If  $S = \{1, f, f^2, \dots\}$ , we denote  $A_f, M_f$  respectively.

**Proposition 5.2**

$S^{-1}$  is an exact functor in  $\text{Mod}_R$ .

*Proof.* Let  $M' \xrightarrow{f} M \xrightarrow{g} M''$  exact. Consider exactness at  $S^{-1}M$ .

Let  $m \in M, s \in S$  such that  $g(m/s) = 0$ . Then  $g(m)/s = 0$ . Then  $\exists s' \in S$  such that  $s'g(m) = 0$ . So that  $g(s'm) = 0$ . Then we have  $s'm \in f(M')$ . So take this and divide by  $s's$  to get  $m/s$ . 

**Definition 5.3**

Let  $\phi : A \rightarrow B$ . Then we can consider  $B$  an  $A$ -module by

$$a \cdot b = \phi(a)b.$$

Let  $A \rightarrow B$ . If  $M$  is an  $A$ -module, we can look at

$$B \otimes_A M,$$

viewed as the tensor product of  $A$  modules. This is also a  $B$ -module. This is because we can define

$$b \cdot \left( \sum_i b_i \otimes m_i \right) = \sum_i b b_i \otimes m_i.$$

Therefore, we can build another  $S^{-1}A$  module by

$$S^{-1}A \otimes_A M.$$

**Proposition 5.4**

There is an isomorphism

$$S^{-1}A \otimes_A M \rightarrow S^{-1}M.$$

*Proof.* Consider the map  $S^{-1}A \times M \rightarrow S^{-1}M$  by

$$\left( \frac{a}{s}, m \right) \mapsto \frac{am}{s}.$$

This induces a map

$$S^{-1}A \times M \rightarrow S^{-1}A \otimes_A M \rightarrow S^{-1}M$$

where we have

$$f\left(\sum_i a_i/s_i \otimes m_i\right) = \sum_i \frac{a_i m_i}{s_i},$$

which is obviously surjective. For injectivity, we would expect that every element in  $S^{-1}A \otimes_A M$  to be a pure tensor element.

Now we have (let  $s = s_1 \dots s_n$ )

$$\sum_i \frac{a_i}{s_i} \otimes m_i = \sum_i \frac{1}{s_i} \otimes a_i m_i = \sum_i \frac{1}{s} \otimes a_i (s/s_i) m_i$$

is a pure tensor. So every element in  $S^{-1}A \otimes_A M$  can be written as a primitive tensor. This makes life easier. Let  $r = \frac{1}{s} \otimes m$  such that  $f(r) = 0$ . Then we have  $m/s = 0$ . So there is  $s' \in S$  such that  $s'm = 0$ . Then

$$r = \frac{s'}{ss'} \otimes m = 0.$$



#### Definition 5.5 (Local properties)

Let  $P$  be a property of some an  $A$ -module. We say that  $P$  is a **Local property** if

$$M \text{ has } P \iff M_p \text{ has } P$$

for all prime ideals  $p \subset A$ .

#### Proposition 5.6

The following are equivalent:

1.  $M = 0$
2.  $M_p = 0 \forall p \subset A$  prime
3.  $M_m = 0 \forall m \subset A$  maximal.

*Proof.* Trivially, 1 implies 2 implies 3. We now show  $3 \implies 1$ . Suppose  $M \neq 0$ . Then let  $x \in M \setminus 0$ . Consider the annihilator of  $x$ . Consider a maximal ideal  $m$  containing  $\text{Ann}(x)$ . Then  $s \cdot x \neq 0$  for all  $s \notin m$ . But then  $\frac{x}{1}$  is not 0 in  $M_m$ .



#### Proposition 5.7

Let  $\phi : M \rightarrow N$ . TFAE:

1.  $\phi$  injective
2.  $\phi_p : M_p \rightarrow N_p$  injective for all  $p \subset A$
3.  $\phi_m : M_m \rightarrow N_m$  injective for all  $m \subset A$

*Proof.* Similar as above.



#### Definition 5.8 (Flatness)

Let  $M$  be an  $A$ -module. Then  $M$  is flat if  $\otimes M$  is an exact functor.

#### Theorem 5.9

TFAE

1.  $M$  is flat.
2.  $M_p$  is a flat  $A_p$  module for all  $p$  prime.

3.  $M_m$  is a flat  $A_m$  module for all  $m$  maximal.

*Proof.* (3  $\implies$  1) Tensor products are right exact, so we need left exactness. Suppose  $M$  is not flat. Then there is  $N \rightarrow N''$  injective but  $M \otimes N \rightarrow M \otimes N''$  not injective.

Then by the previous proposition we have a maximal ideal such that

$$M_m \otimes N_m \rightarrow M_m \otimes N''_m$$

is not injective.



**Remark.** We have  $(S^{-1}A \otimes_A M) \otimes_{S^{-1}A} (S^{-1}A \otimes_A N) \simeq S^{-1}A \otimes (M \otimes_A N)$ .

## 6 Spec

### Definition 6.1 (Spec)

Let  $R$  be a ring. The Spec of  $R$  is the set of all prime ideals in  $R$ , denoted as  $\text{Spec } (R)$ .

**Notation.** Write  $x \in \text{Spec } (R)$ . This corresponds to prime ideal  $p_x \subseteq R$ .

### Definition 6.2

Let  $E \subset R$ . Define

$$V(E) \stackrel{\text{def}}{=} \{x \in \text{Spec } (R) : E \subseteq p_x\}.$$

### Proposition 6.3

Let  $a$  be the ideal generated by  $E$ .

$$V(E) = V(a) = V(r(a)).$$

*Proof.* The inclusions  $\supseteq$  are tautological.

Now we need if  $p \supseteq E$  then  $p \supseteq r(a)$ . Trivially  $p \supseteq a$ . Now if  $r \in r(a)$ , then for some  $n$ ,  $r^n \in a \subseteq p$ . Since  $p$  is prime we must have  $r \in p$ .



### Definition 6.4 (Topology on Spec)

We define the topology on Spec, such that the closed sets are exactly all the sets  $V(a)$ . This is known as the Zariski Topology.


### Proposition 6.5

This is a well defined topology.

We will complete the proof later.

Proposition 6.6

$$\bigcap_{i \in I} V(E_i) = V\left(\bigcup_{i \in I} E_i\right).$$


*Proof.* If  $x \in \bigcap_{i \in I} V(E_i)$ , then  $p_x \supseteq E_i$  for all  $i \in I$ . Then  $p_x \supseteq \bigcup_i E_i$ . On the other hand, if  $p_x \supseteq \bigcup_i E_i$  then  $p_x \supseteq E_i$ , so  $x \in V(E_i)$  for all  $i$ . 

Proposition 6.7

$$V(ab) = V(a) \cup V(b).$$


*Proof.* ( $\subseteq$ ) Supposed  $p \supseteq ab$ . We want  $p \supseteq a$  or  $p \supseteq b$ .

Suppose not, then pick  $r_1 \in a - p, r_2 \in b - p$ , but then  $ab \ni r_1 r_2 \notin p$ .

( $\supseteq$ ) On the other inclusion, if  $x \in V(a)$  then  $p_x \supseteq ab$ . 


*Proof of 6.5.* We need

1. Empty set and  $\text{Spec}$  to be closed. This is easy as  $\text{Spec } R = V(\{0\}), \{\} = V(R)$ .
2. Arbitrary intersections as closed.
3. Finite unions are closed.

The other two statements are from proposition 6.7 and 6.6. 

Proposition 6.8

$$V(ab) = V(a \cap b).$$

*Proof.* This is because  $r(a \cap b) = r(ab)$ . The inclusion  $\supseteq$  is trivial. For the other inclusion, if  $x^n \in a \cap b$ , then  $x^{2n} \in ab$ . 


**Remark.** This proof breaks down when we have infinite intersections. Therefore we cannot use it.

Example 6.9

- $\text{Spec}(K) = \{(0)\}$  for any field  $K$ .
- $\text{Spec}(\mathbb{Z}) = (0), (2), (3), (5), \dots$ . Since each ideal generated by a prime number is prime, we have  $V((p)) = (p)$ .

Proposition 6.10

$x \in \text{Spec } R$  is closed iff  $p_x \subseteq R$  is maximal.

*Proof.*  $\implies$  : Suppose not maximal, then there is a maximal ideal  $m$  containing it. Then for any  $p_x \in V(a)$ , we would have  $m \in V(a)$ . 


$\impliedby$  : Consider  $V(p_x) = \{x\}$ .

**Remark.** We have if  $p_y \supseteq p_x$ , then  $x \in V(a) \implies y \in V(a)$ .

Corollary 6.11: Let  $x \in \operatorname{Spec} R$ . Then the closure  $\bar{x} = \{y : p_y \supseteq p_x\}$ .

Proposition 6.12

The only closed subsets of  $\operatorname{Spec} \mathbb{Z}$  are  $V((l))$ , some positive integer  $l$ .

*Proof.* Since  $\mathbb{Z}$  is a pid, every closed set is of the form  $V((l))$ . If  $l = 0, 1$  then we are done. Else consider the prime factorization of  $l$ . This means we have the  $V((l)) = \cup(p_i)$ . This is also finite unions of closed points in  $\operatorname{Spec}$  . 

Example 6.13

Let  $R = \mathbb{C}[x, y]$ . Assume that a maximal chain of prime ideals in  $R$  has the form

$$(0) \subset (f) \subset m \subset \mathbb{C}[x, y],$$

where  $f$  is irreducible. We can reason through this by the nullstellensatz, i.e. all  $m = ((x - \alpha), (y - \beta))$ .

I.e. we can think of every closed point in  $\operatorname{Spec} R$  corresponds to a point in the 2D plane. Now every  $f$ , we have  $f \in m \iff f(\alpha, \beta) = 0$ , so we can think of  $f$  as the curve  $f = 0$  in the 2D plane (with a fuzzy point corresponding to the curve itself).

Definition 6.14 (Open sets of Zariski topology)

Define  $D(f) \stackrel{\text{def}}{=} \{p : f \notin p\} = \operatorname{Spec} R \setminus V(f)$ .

Proposition 6.15

- $D(f_i)$  forms a basis for the topology.
- $D(f) \cap D(g) = D(fg)$
- $D(f) = \{\}$   $\iff f$  if nilpotent
- $D(f) = \operatorname{Spec} R \iff f$  is a unit.
- $D(f) = D(g) \iff r(f^n) = r(g^n)$ .

Proposition 6.16

$$D(f) \simeq \operatorname{Spec} R_f,$$

and  $\operatorname{Spec} R$  is a quasi-compact topological space. I.e. every open cover has a finite subcover

*Proof.* Exercise. 

## 7


**Remark.** Atiyah Macdonald is so terse...

We continue the discussion of Open sets of Zarski topology.

### Proposition 7.1

Let  $\text{Spec } R = \cup_{i \in I} X_i$ , where each  $X_i$  open. Then there is a finite cover

$$\text{Spec } R = X_1 \cup \dots \cup X_n.$$

*Proof.* We assume that  $X_i = D(f_i)$  since  $D$  forms a basis. We claim that  $(f_i)_{i \in I} = R$ . Suppose not, then there is some prime (maximal) ideal  $p$  containing every  $f_i$ . But this is absurd because then we would not have a covering. Write  $1 = \sum_i a_i f_i$ . Then We would have a finite covering. 


### Definition 7.2

Let  $\phi : A \rightarrow B$  be a ring homomorphism. Since each prime ideal's preimage is prime, we can define a map induced by  $\phi$

$$\phi^* : \text{Spec } B \rightarrow \text{Spec } A.$$

### Proposition 7.3

$\phi^*$  is continuous.


*Proof.* Let  $V(I)$  be closed in  $\text{Spec } A$ . We want  $\phi^{*-1}(V(I))$  be closed. We just check that  $\phi^{*-1}(V(I)) = V(\phi(I))$  

### Example 7.4

Let  $f \in R$ . We have a ring homomorphism  $\phi_f : R \rightarrow R_f$ . Show that the map

$$\phi_f^* : \text{Spec } R_f \rightarrow \text{Spec } R$$

is a homeomorphism onto  $D_f$ .

*Proof.* In exercise 2. 

Let  $x \in \text{Spec } R$ . Consider the  $R_x \stackrel{\text{def}}{=} \text{Frac}(R/p_x)$ , the field of fractions of the integral domain. Given  $f \in R$  we can define a map that sends

$$x \mapsto f \pmod{p_x}.$$

### Example 7.5

In  $\mathbb{C}[x, y]$ , take a maximal ideal  $(x - a, y - b)$ . Take  $f$  a polynomial, then the map

$$(x - a, y - b) \mapsto f(a, b)$$

is the evaluation map.

Now take  $I \subseteq \mathbb{C}[x, y]$  a radical ideal i.e. if  $a^k \in I$  then  $a \in I$ . We now evaluate this on



$V(I)$ . a function  $f$  induces the identically zero map if and only if it is nilpotent. Similarly, the function  $f$  is identically zero on  $V(I)$  if and only if  $f \in r(I) = I$ . So  $f \in I$ . So if two functions are in the same coset  $\mathbb{C}[x, y]/I$ , they induce the same function on  $V(I)$ . So we can view functions on  $V(I)$  as functions onto  $R/I$ .

#### Example 7.6

Let  $I = r(I)$ . Let  $\phi : R \rightarrow R/I$ . Show that  $\phi^* : \text{Spec } (R/I) \rightarrow \text{Spec } R$  is a homeomorphism onto  $V(I)$ .

#### Definition 7.7 (Integral)

Let  $B$  be an  $A$ -algebra. We say that  $\alpha \in B$  is **integral** over  $A$  if  $\alpha$  satisfies

$$\alpha^n + a_{n-1}\alpha^{n-1} + \dots + a_1\alpha + a_0 = 0.$$

for some  $a_i \in A$ .

#### Example 7.8

$1/2 \in \mathbb{Q}$  is not integral in  $\mathbb{Z}$ . This is because the polynomial has to be a monic.  
 $i \in \mathbb{C}$  is integral over  $\mathbb{Z}$ .

We want to prove the following result:

#### Theorem 7.9

If two elements are integral then their sum and products are integral.

#### Proposition 7.10

The following are equivalent.

1.  $\alpha \in B$  is integral over  $A$ .
2. There is a faithful  $A[\alpha] \subseteq B$  submodule that is finitely generated as an  $A$  module.

**Remark.** An  $R$ -module  $M$  is faithful if  $r_1 m = r_2 m$  for all  $m \in M \implies r_1 = r_2$ .

*Proof.*  $1 \implies 2$ : Let  $\alpha \in B$  be integral. Such that  $\alpha^n + a_{n-1}\alpha^{n-1} \dots + a_0 = 0$ . Consider the submodule  $M = A[\alpha]$ . It contains  $1_M$  and we have  $r \in A[\alpha]$  satisfies  $r \cdot 1 = r_m$ . So this module is faithful.

Now notice that  $A[\alpha]$  is generated by  $\{1, \alpha, \dots, \alpha^{n-1}\}$  by the monic polynomial relation.

$2 \implies 1$ . Let  $e_1, \dots, e_n$  be a generating set (over  $A$ ). Then

$$\alpha e_i \in \text{Span}_A \{e_i\}.$$

Then there is some matrix transformation


$$(M - \alpha I_n) \begin{bmatrix} e_1 \\ e_2 \\ \vdots \\ e_n \end{bmatrix} = \vec{0}.$$

Multiply by the adjugate of  $(M - \alpha I_n)$  gives

$$\det(M - \alpha I_n) I_n \begin{bmatrix} e_1 \\ e_2 \\ \vdots \\ e_n \end{bmatrix} = \vec{0}$$

kills every element in  $B$ . By faithfulness this has to be the zero transformation, so that

$$\det(M - \alpha I_n) = 0 \in A[\alpha].$$

The characteristic polynomial is a monic (up to factor of  $-1$ ) polynomial in  $\alpha$ , so we are done. 

## 8

### Definition 8.1 (Integral module)

We say  $B/A$  is **integral** if every element in  $B$  is integral over  $A$ .

### Definition 8.2 (Finite algebra)


$B$  is a finite  $A$ -algebra if  $B$  is finitely generated as an  $A$ -module.

**Remark.** This is stronger than finitely generated algebra. For instance, take  $\mathbb{Q}[i]$  over  $\mathbb{Q}$ . This is finitely generated by  $(1, i)$  as a module. But  $\mathbb{Q}[x]$  is not finitely generated as a  $\mathbb{Q}$  module, but finitely generated as an algebra by  $(1, x)$ .

### Proposition 8.3


$B$  is a finite  $A$ -algebra iff  $B$  is a finitely generated  $A$ -algebra and generated by integral elements.

*Proof.* ( $\implies$ ). This follows from the previous proposition.  $B$  is finitely generated as an  $A$ -algebra by the same elements. Moreover, each generating element is integral as  $B$  is a  $A[\alpha]$ -module that is finitely generated as  $A$ -module. This is faithful because  $1 \in B$  is not killed by  $A[\alpha]$  except for 0.

( $\impliedby$ ). Let  $B = A[\alpha_1, \dots, \alpha_n]$  such that each  $\alpha_i$  is integral. Then  $(\alpha_1, \alpha_1^2, \dots, \alpha_2, \alpha_2^2, \dots, \alpha_n, \dots, \alpha_1 \alpha_2, \dots)$  is finitely generated by finite powers of  $\alpha_i$ , since each  $\alpha_i$  satisfies a monic polynomial, we can pick multi-index  $I$  such that it is of degree  $\sum$  order of monic polynomial. So  $B$  is finitely generated as an  $A$ -module by  $(\alpha_1, \dots, \alpha_1^{k_1}, \dots, \alpha_n, \dots, \alpha_n^{k_n}, \alpha_1 \alpha_2, \dots)$ . 

Proposition 8.4

$B$  is a finite  $A$ -algebra iff  $B$  is a finitely generated  $A$ -algebra and generated by integral elements **and every element in  $B$  is integral over  $A$ .**


*Proof.* Backward direction is the same. For the forward direction, we apply for  $b \in B$  the  $A[b]$ -module  $B$  which is finitely generated as an  $A$ -module and is faithful. 

Proposition 8.5

Let  $B$  be an  $A$ -algebra, and  $C$  be a  $B$ -algebra. Then if  $C$  integral over  $B$  and  $B$  integral over  $A$ , then  $C$  is integral over  $A$ .

*Proof.* Let  $c \in C$ . Then we have for some  $n$  and  $b_i \in B$ ,

$$c^n + b_{n-1}c^{n-1} + \dots + b_0 = 0.$$

So  $c$  is integral over  $B' = A[b_0, \dots, b_{n-1}]$ . Consider the algebra generated by  $C' = A[b_0, \dots, b_{n-1}, c]$ . This is a finite  $B'$  algebra by integral element  $c, c^2, \dots, c^{n-1}$ . But  $B'$  is also a finite  $A$ -algebra by previous proposition. So then  $C'$  is finite. By the previous proposition, every element in  $C'$  is integral over  $A$ , in particular,  $c$  is integral over  $A$ . 

Lemma 8.6

If  $C$  finite over  $B$  and  $B$  finite over  $A$  as algebras, then  $C$  is finite over  $A$ .

*Proof.* Let  $\{b_i\}$  generate  $B$  as  $A$  module and  $\{c_j\}$  generate  $C$  as  $B$  module. Then  $\{b_i c_j\}$  generate  $C$  as  $A$  module. As every  $c \in C$  is some


$$\sum_j r_j c_j = \sum_{i,j} a_{i,j} b_i c_j.$$



Theorem 8.7

Let  $B$  be an  $A$ -algebra. Then the set of elements of  $B$  that are integral over  $A$  is a subalgebra of  $B$ .

That is, sum, difference, products of integral elements are integral.

*Proof.* Let  $\alpha, \beta \in B$  integral over  $A$ . Consider  $A \subseteq A[\alpha, \beta]$ .  $A[\alpha, \beta]$  is a finite  $A$  algebra as it is finitely generated by integral elements. Therefore, we have the stronger statement that every element in  $A[\alpha, \beta]$  is integral over  $A$ . 

Corollary 8.8: The set of elements in  $\bar{\mathbb{Q}}$  that satisfy monic polynomials in  $\mathbb{Z}[x]$  is a subring.

Now let  $A$  be in integral domain, and  $F$  be its field of fractions.

**Definition 8.9 (Integrally closed/Normal)**

We say that  $A$  is integrally closed/normal if the only elements of  $F$  that are integral over  $A$  already lie in  $A$ .


**Remark.** For instance,  $\mathbb{Z}$  is integrally closed.

**Theorem 8.10**

Let  $A$  be a unique factorization domain. Then  $A$  is integrally closed. In particular, all PID's are integrally closed.

*Proof.* Let  $\frac{a}{b} \in F$ . Let  $p$  a prime element such that  $p|b$  (so that it does not divide  $a$  or else there will be cancellation). Suppose that  $\frac{a}{b}$  is integral. Then clearing out denominators gives

$$a^n = b \cdot (\tilde{a})$$

for some  $\tilde{a} \in A$ . Because  $A$  is a UFD, this is a contradiction as the LHS is not divisible by  $p$  but the right is. 


**Remark.**  $\mathbb{Z}[2i]$  is not integrally closed. The field of fractions is  $\mathbb{Q}[i]$ , and  $i^2 + 1 = 0$  gives an integral element  $i \in \mathbb{Q}[i]$  not in  $\mathbb{Z}[2i]$ .

Another non example:  $\mathbb{C}[t^2, t^3]$ . The fraction field is the fraction field of  $\mathbb{C}[t]$ , for which  $t$  is integral as it satisfies  $x^2 - t^2 = 0$ .

**Proposition 8.11**

Let  $A$  be normal integral domain, and  $F$  be its field of fractions. Let  $K/F$  be a finite extension. Then  $\alpha \in K$  is integral over  $A$  iff the minimal polynomial of  $\alpha$  is in  $A[x]$ .

**Remark.** The minimal polynomial is the unique monic polynomial.

*Proof.* The backwards direction is obvious. For the forward direction, suppose that  $\alpha \in K$  integral over  $A$ . Let  $f \in A[x]$  kill  $\alpha$ . Let  $g \in F[x]$  be the minimal polynomial. We have  $g|f$ . Let  $K'$  be an extension of  $F$  for which  $g$  splits. Then set  $\alpha_1, \dots, \alpha_n \in K'$  are the roots. So each  $f(\alpha_i) = 0$ . So each  $\alpha_i$  is integral over  $A$ . So by Vieta's formulae, we have each coefficient in  $g$  is a sum of products in the  $\alpha_i$ . So the coefficients are integral over  $A$ . Since  $A$  is integral, we have  $g \in A[x]$ . 

## 9 Integral Closure

For the following statements, let  $B$  be an integral algebra over  $A$ .

**Proposition 9.1**

If  $A$  and  $B$  are integral domains then  $A$  is a field iff  $B$  is a field.

*Proof.*  $\implies$  : Let  $A$  be a field. Let  $0 \neq b \in B$ . Then consider the monic polynomial

$$b^n + \dots + a_0 = 0.$$

WLOG we can assume  $a_0$  is non zero, as integral domain. Then subtract  $a_0$  on each side and divide by  $-a_0$ . We can factor  $b$  out to find an inverse.

$\Leftarrow$  : **We first prove it assuming that  $A$  is integrally closed.** Let  $B$  be a field. Then  $\text{Frac} A \subseteq B$ . So the field of fractions is integral over  $A$ . But  $A$  is integrally closed, i.e. the field of fractions of  $A$  lies in  $A$ .

Now we drop the integrally closed condition. Let  $a \in A$ . Consider  $a^{-1} \in B$ . There is a monic polynomial

$$a^{-n} + \dots + a_0 = 0.$$

Multiplying both sides by  $a^{n-1}$  gives

$$a_0 a^{n-1} + \dots + a^{-1} = 0.$$


Now we have expressed  $a^{-1}$  in  $A$ . 

#### Proposition 9.2

Let  $S \subset A$  be a multiplicatively closed set. Then  $S^{-1}B$  is integral over  $S^{-1}A$ .


*Proof.* Let  $\frac{b}{s} \in S^{-1}B$ . Then we have

$$b^n + \dots + a_0 = 0.$$

Dividing both sides by  $s^n$  will produce a polynomial with coefficients in  $S^{-1}A$ . 

#### Proposition 9.3

Let  $q \subset B$  a prime ideal. Then  $q$  is maximal iff  $p \stackrel{\text{def}}{=} q \cap A$  is maximal.


*Proof.* Consider  $B/q$  is integral over  $A/p$  (because quotients). Since  $q$  is prime, these two are both integral domains. By the previous proposition, one is a field if and only if the other is field. Translating back to ideals, one is maximal if and only if the other is maximal. 

#### Proposition 9.4

Let  $q_1 \subseteq q_2 \subset B$  both prime ideals, and

$$q_1 \cap A = p = q_2 \cap A.$$

Then  $q_1 = q_2$ .

*Proof.* If  $p$  is maximal then the statement follows directly from the previous proposition. Else consider the multiplicatively closed set  $S = A \setminus p$ . Then  $S^{-1}B$  integral over  $S^{-1}A$ . Now  $S^{-1}p$  is maximal. So  $S^{-1}q_1 = S^{-1}q_2$ . Since we have bijection between prime ideals that avoid  $S$  and prime ideals in  $S^{-1}B$ , they have to be the same before localization. 

#### Example 9.5

Let  $\mathbb{K}/\mathbb{Q}$  be a finite extension of fields.

$\mathbb{Z} \subset \mathbb{Q}$ . We would like to find something in  $\mathbb{K}$  that looks like an extension of  $\mathbb{Z}$ .


**Definition 9.6 (Integral closure)**

The closure  $\mathcal{O}_K \subseteq K$  is the ring of elements in  $K$  that satisfies a monic  $\mathbb{Z}$ -polynomial.

**Remark.** This is a ring because the sum and products of integral elements are integral.

**Proposition 9.7**

Every non-zero prime ideal in  $\mathcal{O}_K$  is maximal.


*Proof.* Let  $p$  be prime. If  $p \cap \mathbb{Z} = (0) = (0) \cap \mathbb{Z}$ , then we have  $p = (0)$ . Else consider the maximal ideal  $p \cap [\mathbb{Z}] = (p_0)$ . Take a maximal ideal  $q$  containing  $p$ , then  $q \cap \mathbb{Z} = p \cap \mathbb{Z}$ . So  $p = q$  is maximal. 

**Proposition 9.8**

The field of fractions of  $\mathcal{O}_K$  is  $K$ .


*Proof.* We will show that  $\alpha \in K$  there exists  $0 \neq n \in \mathbb{Z}$  such that  $n\alpha \in \mathcal{O}_K$ . Since  $K/\mathbb{Q}$  finite, write

$$\alpha^n + \dots + k_0 = 0.$$

Each  $k_i = a_i/b_i$ . So multiply each side by  $b = \prod_i b_i^n$ . Then  $b\alpha$  satisfies a monic polynomial with coefficients in  $\mathbb{Z}$ . 

**Proposition 9.9**

$\mathcal{O}_K$  is integrally closed.

*Proof.* Let  $\alpha \in K$  integral over  $\mathcal{O}_K$ . Then  $\mathcal{O}_K(\alpha)$  integral over  $\mathcal{O}_K$  integral over  $\mathbb{Z}$ , so that  $\alpha$  integral over  $\mathbb{Z}$ . 

**Calculation of integral closures****Example 9.10**

We find the integral closure of  $\mathbb{Q}[\sqrt{2}]$ . We know these are the set of elements that satisfy minimal polynomials in  $\mathbb{Z}[x]$ . Since this is a field of degree 2, we just compute

$$x^2 - (a + b\sqrt{2} + a - b\sqrt{2})x + (a + b\sqrt{2})(a - b\sqrt{2}) = 0$$

such that these coefficients are in  $\mathbb{Z}$ . This turns out to be  $a, b \in \mathbb{Z}$ , so the integral closure is just  $\mathbb{Z}[\sqrt{2}]$ . This is not the case with  $\mathbb{Q}[\sqrt{5}]$ , as we have  $a = 1/2, b = 1/2$ . The integral closure of  $\mathbb{Q}[\sqrt{5}]$  is  $\mathbb{Z}[(1 + \sqrt{5})/2]$ .

# 10

## Theorem 10.1

$\mathcal{O}_K$  is Noetherian.

*Proof.* We will show that **every ideal of  $\mathcal{O}_K$  is finitely generated over  $\mathbb{Z}$** , thus finitely generated over  $\mathcal{O}_K$ .

Suppose  $K/\mathbb{Q}$  is an extension of degree  $n$ . Let  $\beta_1, \beta_n \in \mathcal{O}_K$  that forms a  $\mathbb{Q}$ -basis for  $K$ . This is possible because  $\mathbb{Z}^{+ -1} \mathcal{O}_K = K$ . Then  $\exists \beta_1^*, \dots, \beta_n^* \in K$  such that  $\text{Tr}(\beta_i \beta_j^*) = \delta_{ij}$ .

We want to show


$$\oplus_i \mathbb{Z} B_i \subseteq \mathcal{O}_K \subseteq \oplus_i \mathbb{Z} B_i^*.$$

First notice (exercise)

$$\oplus_i \mathbb{Z} \beta_i^* = \{\beta \in K : B(\beta, \beta_i) \in \mathbb{Z} \forall i\}.$$

So we want to show that

$$\text{Tr}(\alpha \beta_i) \in \mathbb{Z} \forall \alpha \in \mathcal{O}_K.$$

This is true because trace is in the fixed field  $\mathbb{Q}$  and the trace is integral if  $\alpha \in \mathcal{O}_K$ . So that the trace is an integer. 

## Definition 10.2 (Trace)

Let  $\alpha \in K$ , then the trace

$$\text{Tr}_{K/\mathbb{Q}}(\alpha) = \alpha_1 + \dots + \alpha_n,$$

the sum of all conjugates of  $\alpha$ . I.e. take the galois extension of  $\mathbb{Q}$  containing  $K$ . Let  $\sigma_i : K \rightarrow N$  where  $\sigma_1$  is inclusion. Then the trace is the sum of  $\sigma_i(\alpha)$ .

## Proposition 10.3

1.  $\text{Tr}(\alpha + \beta) = \text{Tr}\alpha + \text{Tr}\beta$
2.  $\text{Tr}(a\alpha/b) = a/b \text{Tr}\alpha$

Let  $B_{K/\mathbb{Q}} : K \times K \rightarrow \mathbb{Q}$  that sends  $(\alpha, \beta) \mapsto \text{Tr}(\alpha\beta)$ . This is bilinear and nondegenerate.

**Remark.** In general,  $\text{Tr}_{L/F} \text{ not } \equiv 0 \iff L/F \text{ is separable.}$

## Definition 10.4 (Dedekind domain)

An integral domain  $R$  is a **Dedekind domain** if

1.  $R$  is Noetherian
2. All non-zero prime ideals are maximal
3.  $R$  is normal (integrally closed).


Corollary 10.5:  $\mathcal{O}_K$  is a Dedekind domain.

Corollary 10.6:  $A$  Dedekind domain,  $F$  field of fractions, and  $K/F$  separable extension, then the integral closure of  $A$  in  $K$  is a Dedekind domain.

**Theorem 10.7**


Let  $B/A$  integral. Let  $p \subseteq A$  prime ideal. Then there is a prime ideal in  $B$  that contracts to  $p$  in  $A$ . i.e.

$$q \cap A = p.$$

*Proof.* Localize  $p$ .  $A \rightarrow A_p$ . Then  $pA_p$  is (uniquely) maximal. Moreover, since  $A_p$  is not a field,  $B_p$  is not a field and has a nonzero maximal ideal  $m$ . Then  $m \cap A_p$  is maximal so it is  $pA_p$ . Now we have  $m \cap A = p$ . Then  $m \cap B$  contracts to  $p$ . 

**Theorem 10.8 (Going Up)**

Let  $B/A$  integral. Let  $q \subseteq B$  prime,  $p \subseteq p' \subseteq A$  prime. Also suppose that  $q \cap A = p$ . Then there exists  $q' \subseteq q' \subseteq B$  prime such that it contracts to  $p'$ .

*Proof.* Consider  $A/p$  and  $B/q$ . By the previous theorem, we have a prime ideal of  $\bar{q}' \subseteq B/q$  that contracts to  $p'/p \subseteq A/p$ . Now take the preimage of  $\bar{q}'$  in  $B$ . We can check that it contracts to  $p'$ . (exercise) 

Corollary 10.9 (Going Up): Let  $B/A$  integral. Let  $p_1 \subseteq p_2 \subseteq \dots \subseteq p_n \subseteq A$  be a chain of prime ideals, and  $q_1 \subseteq B$  prime that contracts to  $p_1$ . Then we can extend the chain in  $q$  to the full length  $n$  i.e.  $q_1 \subseteq q_2 \subseteq \dots \subseteq q_n$ , such that each  $q_i$  contracts to  $p_i$ .

We would like to work towards going down theorem. To extend the chain the other way, we need a few more statements and some additional assumptions.

**Definition 10.10**

Let  $a \subseteq A$ ,  $B/A$  integral. Then  $b \in B$  integral over  $a$  if  $B$  satisfies a monic polynomial with coefficients (except the first monic one...) lying in the ideal  $a$ .  
The set of elements that are integral over  $a$  is called the integral closure of  $a$  in  $B$ .

**Proposition 10.11**

Consider  $B/A$ . Then  $b \in B$  is integral over  $a \subseteq A$  iff there is a faithful  $A[b]$  section (module)  $M \subseteq B$  that is finitely generated as an  $A$  module and  $bM \subseteq aM$ .

*Proof.* Exercise. 

**Theorem 10.12**

The integral closure of  $a$  in  $B$  is  $r(aB)$ .




*Proof.*  $\supseteq$ : Let  $b \in r(aB)$ . Then write

$$b^n = \sum_i^m a_i x_i$$

for some  $x_i \in B$ ,  $a_i \in a$ . Then let  $M = A[x_i]$ . We thus have  $b^n M \subseteq aM$ . So that  $b^n$  integral over  $a$ . So  $b$  integral over  $a$ .

$\subseteq$ : For the other way, let  $b$  be integral over  $a$ . Write

$$b^n = \sum_{i < n} a_i b^i \in aB$$

so  $b \in r(aB)$ . 

## 11

### Proposition 11.1

Let  $I \subseteq A$  ideal,  $F = \text{Frac}(A)$ . Then if  $\alpha \in K/F$  is integral over  $I$  the minimal polynomial of  $\alpha$  has non-leading coefficients in  $r(I)$ .

### Proposition 11.2

Let  $B$  integral over  $A$ . Then  $\alpha \in B$  is integral over  $I \subseteq A$  iff  $\alpha \in r(aB)$ .

We want to prove the going down theorem.

### Theorem 11.3 (Going down)

Let  $B/A$  integral. **Further assume that  $A$  is an integral domain and is integrally closed.** Let  $q \subseteq B$  prime,  $p' \subseteq p \subseteq A$  prime. Also suppose that  $q \cap A = p$ . Then there exists  $q' \subseteq q \subseteq B$  prime such that it contracts to  $p'$ .

### Lemma 11.4

Let  $\phi : R_1 \rightarrow R_2$  ring homomorphism. Let  $p_1 \subset R_1$  prime. Then there is prime  $p_2 \subset R_2$  with  $\phi^{-1}(p_2) = p_1$  iff  $\phi^{-1}(\phi(p_1)R_2)$ .

*Proof.* We localize at  $q$ . We want to show  $p'B_q \cap A = p'$ . Then there is some prime ideal  $\tilde{q} \subseteq B_q$  such that  $\tilde{q} \cap A = p'$  (by the reverse direction of the previous lemma).  $B_q$  is local, so  $qB_q$  contains  $\tilde{q}$ . Take  $q' = \tilde{q} \cap B$ .

One inclusion is simple, so we show the  $\subseteq$  direction. Let  $b \in p'B_q$ . Then

$$b = \frac{y}{s}, y \in p'B, s \in B - q.$$

So  $y \in r(p'B)$ . So by proposition  $b$  is integral over  $p' \subset A$ . Then the minimal polynomial of  $y$  has non leading coefs in  $r(p') = p'$ . Now let we have  $b \in A \cap p'B_q$ . Then we must have  $b = y/s \implies s = y/b$ , as evaluated in  $b^{-1} \in \text{Frac}A$ .

So if  $y$  satisfies

$$y^n + \dots + a_1 y + a_0$$

then

$$s^n + a_{n-1}/bs^{n-1} + \dots + a_0/b^n = 0.$$

Now this is a minimal polynomial of  $s$  over  $\text{Frac} A$ , as the degree of extension of  $y$  and  $s$  have to be the same over the fraction field (they are the same extension). Therefore, we can now apply the fact that  $s \in B$  is integral over  $A$  to get each  $a_{n-i}/b^i$  is in  $A$ . But now we have

$$\frac{a_{n-i}}{b^i} \cdot b^i = a_{n-i} \in p'.$$

If  $b^i \in p'$  we are done as  $p'$  is prime. Else,

$$s^n = \sum_{i>0} -\frac{a_{n-i}}{b^i} s^{n-i} \in p'B \subseteq q,$$

this contradicts our assumption of  $b = \frac{y}{s} \in B_q$ . 

### Theorem 11.5 (Noetherian Normalization)

Let  $K$  be a field,  $R$  a finitely generated  $K$ -algebra. Then  $R$  is finite over a polynomial algebra.

*Proof.* We induct on the number of generators on  $R$ .

Let  $m$  be the minimal number of generators needed to generate  $R$ . If  $m = 1$  we are done as  $R = K[\alpha]$ . If  $\alpha$  is transcendental, this is a polynomial ring and we are good. If  $\alpha$  is integral, then  $R$  is finite over  $K$ .

Now we show for  $m$ -element generated algebras assuming the statement holds for  $m-1$  generators.

Let  $R = K[\alpha_1, \dots, \alpha_m]$ . If all of them are algebraically independent, then  $R$  is a polynomial ring generated by  $\alpha_I$  for each multiindex  $I$ .


WLOG assume that  $\alpha_m$  satisfies a polynomial in coefficients  $R_m \stackrel{\text{def}}{=} K[\alpha_1, \dots, \alpha_{m-1}]$ . If the polynomial is monic  $T^d + c_{d-1}T^{d-1} + \dots + c_1T + c_0$  and each  $c_i \in K[\alpha_1, \dots, \alpha_{m-1}]$ , then  $\alpha_m$  is integral over this ring. So this  $R$  is finite over  $R_{m-1}$ . Since  $R_{m-1}$  is finite, a finite extension is also finite.

If the polynomial is not monic, write

$$f(\alpha_1, \dots, \alpha_{m-1}, T) = \sum_{I,j} c_I \alpha_I T^j, c_I \in K$$

Now we make the change of variables  $\alpha'_i = \alpha_i - T^{N_i}$  for big  $N > 4 * (m + \deg f)$ . Then the power of  $T$  is uniquely determined by exactly one multiindex (i.e. there are no cancellations). Then the leading coefficient of

$$f(\alpha'_i - T^{N_i}, \dots, T)$$

is some  $c_I \in K$ , so is essentially a monic polynomial. Now  $\alpha_m$  is integral over  $K[\dots \alpha_i - \alpha_m^{N_i}, \dots]$ . This is a ring in  $m-1$  elements so is finite. The extension is finite so we are done. 

## 12 Nullstellensatz

### Theorem 12.1 (Zarski's Lemma)

Let  $K$  be a field. Let  $L/K$  a field which is a finitely generated  $K$ -algebra. Then  $L$  is a finite extension of  $K$ .

will fix this proof later. We induct on the number of generators of  $L$ .

Let  $L = K[\alpha]$ . If  $\alpha$  is algebraic, we are done. Else  $\alpha$  is transcendental and  $L \simeq K[x]$  which is not a field.

Suppose we have the statement for  $m$  generated  $L$ . We want to show for

$$L = K[\alpha_0, \alpha_1, \dots, \alpha_m].$$

Let  $K_0 = K(\alpha_0)$ ,  $R_0 = K[\alpha_0]$ .  $L = K_0[\alpha_1, \dots, \alpha_m]$ , where each is algebraic over  $K_0$  (induction).


Set  $g_i(\alpha_i) = 0, g_i \in K_0[t]$ .

Let  $s \in R_0 \setminus \{0\}$ , such that  $s \cdot g_i \in R_0[t] \forall i$ .


So  $g_i$ 's are monic with coefficients  $R_0[1/s]$ .  $L = R_0[1/s][\alpha_1, \dots, \alpha_m]$ .

So  $L$  is finitely generated  $R_0$ -algebra. Each generator is integral over  $R_0[1/s]$ . So  $L$  is integral over  $R_0[1/s]$ . In particular,  $K_0$  is integral over  $R_0[1/s]$ . If  $\alpha_0$  algebraic over  $K$ , we are done. Else, suppose that  $\alpha_0$  is transcendental over  $K$ . Then  $R_0 \simeq K[x]$ .

Then we have  $R_0[1/s] \simeq K[x][1/f(s)]$ .  $R_0$  is integrally closed (because it is PID so UFD), so that the integral closure of  $R_0[1/s] = K_0[1/s] = R_0[1/s]$ . Therefore  $R_0[1/s] = K_0$ .

This is not possible because  $K[t][1/f(t)]$  is never a field. Just find a prime ideal that avoids  $f(t)$  i.e. an irreducible polynomial that is not  $f(t)$ . As a concrete example, take maximal ideal containing  $f(t) + 1$ . 

**Corollary 12.2:** Let  $K$  be a field. Let  $R$  a finitely generated  $K$  algebra. Then for any maximal ideal  $m \subseteq R$ ,  $R/m$  is a finite extension of  $K$ .


*Proof.* Any quotient of  $R$  is finitely generated as a  $K$ -algebra. Apply Zariski's lemma. 

**Corollary 12.3:** Let  $K$  be algebraically closed,  $m \subset K[x_1, \dots, x_n]$ . Then  $m = (x_1 - a_1, x_2 - a_2, \dots, x_n - a_n)$  for some  $a_i \in K$ .

*Proof.* Mod  $K[x_1, \dots, x_n]$  by  $m$ . This is a finite extension of  $K$  which is  $K$  because it is algebraically closed.

Now the map  $K[x_1, \dots, x_n] \rightarrow K$  is determined uniquely by where  $x_i$  goes, so we have

$$(x_1 - f(x_1), \dots, x_n - f(x_n)) \subseteq \ker(f) = m.$$

But the left hand side is maximal, so we are done. 

**Remark.** If you relax the condition for algebraically closed, we map

$$K[x_1, \dots, x_n] \rightarrow \bar{K}.$$


Each  $x_i$  maps to the algebraic closure of  $K$ . Let  $g_i$  be the minimal polynomial of  $f(x_i)$ , then  $(g_i) \subseteq m$ . The left hand side is maximal because

$$K[x_1, \dots, x_n]/(f_1(x_1)) = K[\alpha_1, x_2, \dots, x_n]$$

repeat this to get  $K[x_1, \dots, x_n]/(f_i(x_i)) = K[\alpha_1, \dots, \alpha_n]$ . *This only works if the polynomials are disjoint.*

*Non-example:*  $\mathbb{Q}[x, y] \rightarrow \mathbb{C}$ , where both  $x, y \mapsto i$ . Then we have kernel  $(x^2 + 1, x - y) \supset (x^2 + 1, y^2 + 1)$ .

Corollary 12.4: Let  $I \subset K[x_1, \dots, x_n]$ . Then there is some point in  $\bar{K}$  such that there is some  $a_1, \dots, a_n \in K^{a.c.}$  such that  $f(a_i) = 0$  for all  $f \in I$ .

*Proof.* Take maximal ideal containing  $I$ . Mod by this ideal and embed the quotient into the algebraic closure of  $K^{a.c.}$ . Then the image of each  $x_i$  is the  $a_i$ 's. 

#### Lemma 12.5

Let  $R, S$  be finitely generated  $K$  algebras. Let  $f : R \rightarrow S$ . Then for maximal  $m \subset S$  we have  $f^{-1}(m)$  is maximal.

*Proof.* Let  $m$  maximal. Then consider

$$R \xrightarrow{f} S \xrightarrow{e} S/m.$$

Then  $R/f^{-1}(m) \simeq e \circ f(R)$ . By Zariski's lemma,  $S/m$  is a finite extension of  $K$ . But now the image of  $R$  is a subring of  $L$  containing  $K(*)$ , so the image is a field. Therefore the pullback is maximal.

(\*) each element is algebraic, so adjoining each element also adjoins the inverse. 