

# Introduction to Commutative Algebra:

and affine algebraic varieties

Amal M

January 4, 2021

## Abstract

The motivation for the study of algebraic geometry is how algebraic objects (rings of rational functions) are associated with varieties (zeros of polynomials). This subject flourished during the second half of the twentieth century. Algebraic geometry allows us to study the geometry arising from algebraic objects. Core to the deeper understanding of this subject is an understanding of the subject of commutative algebra which studies commutative rings and their ideals and modules. The purpose of the present project is to gain an understanding of commutative algebra through solving exercises from Atiyah-MacDonald's book, *Introduction to Commutative Algebra*. The reading project comprised of the study of the theory of rings and modules, their tensor product and exact sequences of rings and modules. The project concluded with a proof of the Going-Up Theorem.

# Contents

<b>1</b>	<b>Introduction</b>	<b>2</b>
<b>2</b>	<b>The Zariski Topology</b>	<b>5</b>
2.1	Prime Spectrum . . . . .	6
2.2	Maximal Spectrum . . . . .	7
2.3	Affine Algebraic Varieties . . . . .	8
2.3.1	Polynomial Functions . . . . .	8
<b>3</b>	<b>Tensor Product and Direct Limits</b>	<b>9</b>
3.1	Tensor Product . . . . .	10
3.2	Flatness . . . . .	11
3.3	Tensor Product of Algebras . . . . .	11
3.4	Direct Limit . . . . .	11
<b>4</b>	<b>Sheaf and Presheaf</b>	<b>12</b>
4.1	Support . . . . .	12
4.2	Presheaf . . . . .	12
4.3	Sheaf . . . . .	12
4.4	Constructible Topology . . . . .	12
4.5	Absolute Flatness . . . . .	12
<b>5</b>	<b>The Going-Up Theorem</b>	<b>13</b>

# Chapter 1

## Introduction

The purpose of the current project is to give an understanding to the reader of how commutative algebra is used to define the basic objects of algebraic geometry. Algebraic Geometry is the study of the geometric properties of the solution set of polynomial equations in arbitrary variables. For this purpose it is useful to confine the discussion to algebraically closed fields  $k$  and the polynomial ring  $k[x_1, \dots, x_n]$ . We define *affine  $n$ -space* over the algebraically closed field  $k$  as  $k^n$  and denote it by  $\mathbb{A}_k^n$ .

**Definition 1.0.1.** *The algebraic variety [1] in the affine space  $\mathbb{A}_k^n$  of a set  $S$  of polynomials  $f \in k[x_1, \dots, x_n]$ , is a subset  $V(S) \subseteq \mathbb{A}_k^n$  cut out by the set of mutual zeros of all the polynomials in the set  $S$ .*

$$V(S) = \{x = (x_1, \dots, x_n) \in \mathbb{A}_k^n : f(x) = 0 \text{ for all } f \in S\}.$$

The affine variety is not the only example of a variety. The projective variety defined over projective spaces  $\mathbb{P}_k^n$  is another example of an algebraic variety.

The solution set or *locus* of solutions of polynomials of degree one are discrete points in  $k$ . But over  $k^2$  the *locus* are curves. For example, the solution of the elliptic curve given by the polynomial equation in  $\mathbb{R}[x, y]$  in  $\mathbb{R}^2$

$$y^2 = x^3 - 3x + 5$$

is a curve (Fig 1.). The question then arises: *what does the solution set of a set of polynomials in  $k^3$  look like? What about  $k^n$ ?* This is same asking the question: *what does an affine algebraic variety in  $\mathbb{A}_k^n$  look like?* We may go further by demanding: *what is the topology of the affine algebraic variety?* (The answer is called the *Zariski Topology*, which we shall get to in due time.)

Once we have an affine algebraic variety we may define functions on them and we may define functions from one algebraic variety to another. Thus we start to do the usual mathematical *sh\*tick* on affine varieties.

To answer the proposed questions we need to know the properties of an affine algebraic varieties. For example: *what is so algebraic about an affine algebraic variety?* The answer is that we may consider every *affine algebraic variety* to be some *finitely generated nilpotent-free  $k$ -algebra*  $A$ . To know what each of these terms means we first need some commutative algebra. The purpose of this article is to explain these terms and give a brief introduction to Algebraic Geometry focusing only on affine algebraic varieties.

The exposition is based on the knowledge gained after spending many hours working out the exercises contained in [2]. I would advise anyone thinking about learning algebraic geometry to start there and work out those exercises themselves.

We divide the article into four sections. In the first section we introduce the *prime spectrum* of a ring  $A$ ,  $X = \text{Spec}(A)$  by which we denote the set of all prime ideals of  $A$ . We endow this space  $X$  with a topology called *the Zariski Topology*.

In the next section, we introduce *modules*, which are a sort of generalised vector spaces and *algebras*, which are modules on rings, and we define the tensor product on a collection of such *modules*. Then we discuss a particular sort of structure that can be given to a collection of modules called *the direct limit* – a term loaned from Category Theory.

In the third section we introduce the *rings of fractions* of modules and the concept of *localization* which we use in the formulation of a sort of structure called *presheaf* and *sheaf*. We also introduce the *constructible topology* and the precise condition under which this topology is equivalent to the *Zariski Topology* on  $\text{Spec}(A)$ .

In the final section we introduce integral dependence, that is elements of rings that are integral over a subring and discuss the proof of the Going-Up Theorem, one of the two well known theorems of Cohen-Seidenberg.

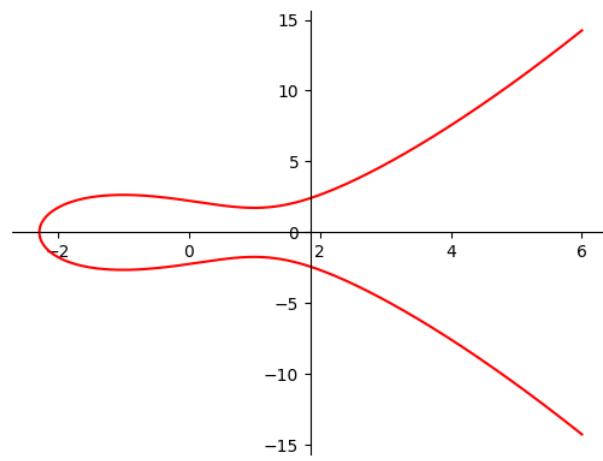


Figure 1.1: Fig 1.

## Chapter 2

# The Zariski Topology

In commutative algebra what we generally call a *ring* is a ring with unity, i.e,  $1 \in A$ . So from now on, when we say ring we mean a set  $A$  with two binary operations on its elements  $a + b$  and  $ab$ , for all  $a, b \in A$  such that  $A$  is an abelian group with respect to addition and multiplication is associative and distributive over addition and  $1 \in A$  is the unique identity element.

A *unit* in a ring  $A$  is an element  $x \in A$  such that there is another element  $y \in A$  so that  $xy = 1$ . A ring in which every element is a *unit* is called a *field*.

An element  $x \in A$  is a *nilpotent* element if  $x^n = 0$  for some  $n > 0$ . An element  $x$  is an *idempotent* element if  $x^2 = x$ .

If we are given a group we know that if we quotient it by a normal subgroup we obtain another group and that the kernel of a group homomorphism is always a normal subgroup. Similarly rings have *ideals*. Using *ideals* can form a quotient ring and we have the fact that the kernel of every ring homomorphism is an ideal.

**Definition 2.0.1.** A subset  $\mathfrak{a} \subseteq A$  is called an *ideal* of  $A$  if  $\mathfrak{a}$  is an additive subgroup and it has the property,  $y \in \mathfrak{a}$  and  $x \in A$  implies  $xy \in \mathfrak{a}$ .

Once we understand what an ideal is we can define a *prime ideal* of  $A$  which is an ideal  $\mathfrak{p}$  of  $A$  with the property that  $xy \in \mathfrak{p} \implies x \in \mathfrak{p}$  or  $y \in \mathfrak{p}$ . Similarly an ideal  $\mathfrak{m}$  in  $A$  is *maximal* if  $\mathfrak{m} \neq (1)$  and if there is no ideal  $\mathfrak{a}$  such that  $\mathfrak{m} \subset \mathfrak{a} \subset (1)$ . If we understand that given an ideal  $\mathfrak{a}$  of a ring  $A$  we can form the quotient ring  $A/\mathfrak{a}$ , we can look at the following proposition given without proof

**Proposition 2.0.2.**

$$\mathfrak{p} \text{ is prime} \iff A/\mathfrak{p} \text{ is an integral domain}$$

$$\mathfrak{m} \text{ is maximal} \iff A/\mathfrak{m} \text{ is a field}$$

Therefore every *maximal ideal* is a *prime ideal* but the converse is not true in general. The reason prime ideals and maximal ideals are

so important is because they have "nice" properties when we transport them across ring homomorphisms. For example given a ring homomorphism  $f : A \rightarrow B$  and a prime ideal  $\mathfrak{q} \subset B$  the set  $f^{-1}(\mathfrak{q})$  is a prime ideal  $\mathfrak{p} \subset A$ . This result will be useful later on. Meanwhile we move onto the other members of *ring theory*.

A ring with just one *maximal* ideal  $\mathfrak{m}$  is called a *local ring*. The quotient ring  $k = A/\mathfrak{m}$  which is a field, is called the *residue field* of  $A$ .

**Definition 2.0.3.** *The radical of an ideal  $\mathfrak{a} \subset A$  is another ideal*

$$r(\mathfrak{a}) = \{x \in A : x^n \in \mathfrak{a} \text{ for some } n > 0\}$$

We can show that the *radical* of an ideal is the intersection of all prime ideals that contain that ideal. If  $x$  is an element of  $\mathfrak{a}$  and if  $x$  is any power of an element then that element belongs to the *radical*. So the *radical* is a way to associate elements related to  $\mathfrak{a}$  by its power. That is, if  $f^n \in \mathfrak{a}$  then by definition of an ideal all the powers of  $f$  higher than  $n$  also belongs to  $\mathfrak{a}$ , the *radical* ideal includes *lower powers* of  $f$  such as  $f^{n-2}, f^{n-5}$  and so on. So we can have all powers of  $f$  in  $r(\mathfrak{a})$ .

We just need to define one more concept before we can move on to define the *prime spectrum* of a ring.

**Proposition 2.0.4.** *The set  $\mathfrak{N}$  of all nilpotent elements in a ring  $A$  is an ideal and  $A/\mathfrak{N}$  has no nilpotent element  $\neq 0$ . [2]*

The *nilradical* of a ring  $A$  has the property that it is equal to the intersection of all the prime ideals of  $A$ . It's worth asking the question: *What is the intersection of all maximal ideals of  $A$ ?* The answer is precisely the *Jacobson ideal* of  $A$  denoted by  $\mathfrak{R}$ . It has the following property

**Proposition 2.0.5.**  $x \in \mathfrak{R} \Leftrightarrow 1 - xy$  is a unit in  $A$  for all  $y \in A$ . [2]

## 2.1 Prime Spectrum

The *prime spectrum* of a ring is the set of all *prime* ideals of the ring  $A$  and we denote it by  $X = \text{Spec}(A)$ . We consider this set to be a space in the following way. Each *prime ideal*  $\mathfrak{p}_x \in \text{Spec}(A)$  is a point which we denote by  $x$ .

A topology on a space can be axiomatically defined using just the closed sets. We claim that for each subset  $E$  of  $A$

$$V(E) = \{\mathfrak{p} \in \text{Spec}(A) : E \subseteq \mathfrak{p}\}$$

satisfies the axioms for closed sets. To see this by Ex 15.ii  $V(0) = X$  and  $V(1) = \emptyset$ . By 15.iii arbitrary intersection of closed sets are seen to be closed. By 15.iv along with 15.i we can see that union of finitely many closed sets is closed. So the sets  $V(E)$  do indeed form a topology on  $\text{Spec}(A)$ . This topology is called *the Zariski Topology*.



This is not the only topology on  $\text{Spec}(A)$  we will discuss another such topology, the *constructible topology*, later on. But for now we focus on the properties of the *Zariski Topology*.

The sets  $X_f = X - V(f)$  are open sets in  $X$  for each  $f \in A$  since each  $V(f)$  is closed. The family of such sets,  $\{X_f\}_{f \in A}$  is the basis (Ex 17) of the *Zariski Topology* and we call them the *basic open sets* of  $X$ .

$X$  is *quasi-compact*. Which is exactly the same as *compactness* in regular topology. For some reason Algebraic Geometers do not use the term *compactness* to mean just the condition *every open cover has a finite subcover*. But instead a space is *compact* if it is also Hausdorff as well as *quasi-compact*. This is because every  $\text{Spec}(A)$  has the usual property of having a finite subcover for an open covering. So just calling it *compact* is a waste of a perfectly good word that can be used for something more significant.

We find that every open set  $X_f$  is quasi-compact as well every finite union of sets  $X_f$ . Indeed we have that a subset of  $X$  is quasi-compact if and only if it is a union of finitely many open sets  $X_f$  (Ex 17.vii).

A singleton set  $\{x\}$  in the Zariski Topology is closed if and only if  $\mathfrak{p}_x$  is maximal (Ex 18.i).  $X$  is also  $T_0$ -space.

Now would be a good time to see some examples of the *prime spectrum* of some well known rings such as  $\mathbb{Z}, \mathbb{R}, \mathbb{C}[x]$  and  $\mathbb{Z}[x]$  (Ex 16).

## 2.2 Maximal Spectrum

The *maximal spectrum* of a ring is the set of all *maximal* ideals of the ring. It is denoted by  $\text{Max}(A)$ . The *maximal spectrum* is a subset of the *prime spectrum*  $\text{Spec}(A)$ . We can quickly give a concrete example for a *maximal spectrum*.

Let  $X$  be a compact Hausdorff space and let  $C(X)$  be the ring of all real valued continuous functions on  $X$ . Define

$$\mathfrak{m}_x = \{f \in C(X) : f(x) = 0\}$$

Then  $\mathfrak{m}_x$  is an ideal and furthermore it is a maximal ideal since if we define a function  $\phi_x : C(X) \rightarrow \mathbb{R}$  as the mapping  $f \mapsto f(x)$  then the kernel of the map is  $\mathfrak{m}_x$ .

Let  $\hat{X} = \text{Max}(A)$  we can define a mapping  $\mu : X \rightarrow \hat{X}$  by  $x \mapsto \mathfrak{m}_x$ . By Ex 26.i  $\mu$  is surjective and by Ex 26.ii it is injective. Let  $f \in C(X)$  and define

$$U_f = \{x \in X : f(x) \neq 0\}$$

$$\hat{U}_f = \{\mathfrak{m} \in \hat{X} : f \notin \mathfrak{m}\}$$

We can show that  $\mu(U_f) = \hat{U}_f$  (Ex 27.iii). So  $\mu$  sends the basis of  $X$  the basis of  $\hat{X}$  and so  $\mu$  is a homeomorphism.

We have just show that given only the functions on a compact Hausdorff space  $X$  we can reconstruct the underlying space.

## 2.3 Affine Algebraic Varieties

Given a set  $S$  of polynomial in  $k[x_1, \dots, x_n]$  we have defined the *affine algebraic variety* on  $S$  as the subset  $V(S)$  of the affine space  $\mathbb{A}_k^n$ .

$$V(S) = \{x = (x_1, \dots, x_n) \in \mathbb{A}_k^n : f(x) = 0 \text{ for all } f \in S\}.$$

Now we consider the opposite behavior?

Given a subset  $X$  of the affine space we define the *ideal of the variety*  $X$  to be the set of polynomials  $g \in k[x_1, \dots, x_n]$  that vanish on  $X$ . It is denoted by  $I(X)$ .

$$I(X) = \{g \in k[x_1, \dots, x_n] : g(x) = 0, \forall x \in X\}$$

This set is an ideal since if two polynomials  $f, g \in I(X)$  then  $f + g \in I(X)$  as the sum of the polynomials vanish if they each individually vanish and for any polynomial  $f \in k[x_1, \dots, x_n]$  and  $g \in I(X)$ ,  $fg = 0$  so  $fg \in I(X)$  as well.

The quotient ring

$$P(X) = k[x_1, \dots, x_n]/I(X)$$

is called the ring of polynomial functions on  $X$ . If two polynomials  $f$  and  $g$  belong to the same coset, then  $f - g \in I(X)$  that means over  $X$ ,  $(f - g)(x) = 0$ , i.e., the two polynomials agree in value over  $X$ . So the polynomial ring contains only distinct polynomials over  $X$ .

Let  $\xi_i$  be the image in  $P(X)$  of  $x_i$ . Then the  $\xi_i (1 \leq i \leq n)$  are called the *coordinate functions* on  $X$ .  $P(X)$  is generated as a  $k$ -algebra by the *coordinate functions* and it is called the *coordinate ring* or *affine algebra* on  $X$ .

For each  $x \in X$  the ideal  $\mathfrak{m}_x$  consisting of  $f \in P(X)$  such that  $f(x) = 0$  is a maximal ideal. Let  $\hat{X} = \text{Max}(P(X))$ . We can use Hilbert's Nullstellensatz to show that the mapping  $\mu : X \rightarrow \hat{X}$  given by  $x \mapsto \mathfrak{m}_x$  is a bijection.

### 2.3.1 Polynomial Functions

Let  $f_1, \dots, f_m$  be  $m$  polynomials in  $k[x_1, \dots, x_n]$ . We can define a mapping  $\phi : k^n \rightarrow k^m$  by  $\phi(x) = (f_1(x), \dots, f_m(x))$ . Such a mapping is called a *polynomial mapping*.

Let  $X, Y$  be affine algebraic varieties in  $k^n$  and  $k^m$  respectively. A mapping  $\phi : Y \rightarrow X$  is a *regular mapping* if  $\phi$  is a restriction of a polynomial mapping from  $k^n$  to  $k^m$ .

$\phi$  induces a  $k$ -algebra homomorphism  $P(Y) \rightarrow P(X)$  given by sending polynomial functions on  $Y$  to their composition with  $\phi$ . Therefore there is a one-to-one correspondence between the regular mappings  $X \rightarrow Y$  and the  $k$ -algebra homomorphism  $P(Y) \rightarrow P(X)$ .

## Chapter 3

# Tensor Product and Direct Limits

Let  $A$  be a ring. An  $A$ -module is an abelian group  $M$  along with a mapping  $\mu : A \times M \rightarrow M$ ,  $\mu(a, x)$  denoted by  $ax$ ,  $a \in A$ ,  $x \in M$  which satisfies the following

1.  $a(x + y) = ax + ay$
2.  $(a + b)x = ax + bx$
3.  $(ab)x = a(bx)$
4.  $1x = x$ , ( $\forall a, b \in A, \forall x, y \in M$ .)

A module homomorphism between two modules  $M$  and  $N$  is an  $A$ -linear mapping between two abelian groups  $f : M \rightarrow N$ , such that the following two properties are satisfied

1.  $f(x + y) = f(x) + f(y)$
2.  $f(ax) = a.f(x)$

A *submodule*  $M'$  of  $M$  is a subgroup that is closed under multiplication by elements of  $A$ . The quotient  $M/M'$  is also an  $A$ -module as it is the action of  $A$  on the quotient is  $a(x + M') = ax + M'$ .

Given two modules  $M$  and  $N$ , their direct product is given as the module  $M \oplus N$  which is the set of all elements  $(x, y)$ ,  $x \in M, y \in N$  with two operations defined on it

$$(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$$

$$a(x, y) = (ax, ay)$$

Given an arbitrary family of  $A$ -modules,  $(M_i)_{i \in I}$  the direct sum of the family is the sum  $\bigoplus_{i \in I} M_i$  is the set of all families  $(x_i)_{i \in I}$ ,  $x_i \in M_i$  such that all but finitely many  $x_i$  are nonzero. It is a module by the same operation as above.

A sequence of  $A$ -modules and  $A$ -homomorphisms,

$$\cdots \rightarrow M_{i-1} \xrightarrow{f_i} M_i \xrightarrow{f_{i+1}} M_{i+1} \rightarrow \cdots$$

is said to be *exact* at  $M_i$  if,  $\text{Ker}(f_{i+1}) = \text{Im} f_i$ . The sequence is exact if it is exact at each  $M_i$ .

1.  $0 \rightarrow M' \xrightarrow{f} M$  is exact  $\Leftrightarrow f$  is injective.
2.  $M \xrightarrow{g} M'' \rightarrow 0$  is exact  $\Leftrightarrow g$  is surjective.
3.  $0 \rightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \rightarrow 0$  is exact  $\Leftrightarrow f$  is injective and  $g$  is surjective. But also  $\text{Coker}(f) = M/f(M')$  is isomorphic to  $M''$ . This type of exact sequence is also called a short exact sequence.

A sequence of type (3) is called a *short exact sequence*.

### 3.1 Tensor Product

The *tensor product* of two  $A$ -modules  $M$  and  $N$  is the  $A$ -module  $M \otimes N$  of all linear combination of the pair  $x \otimes y$  with coefficients in  $A$  along with the following properties,

1.  $(x + x') \otimes y = x \otimes y + x' \otimes y$
2.  $x \otimes (y + y') = x \otimes y + x \otimes y'$
3.  $a \cdot x \otimes y = x \otimes a \cdot y = a(x \otimes y)$

We see that  $0 \otimes x = x \otimes 0 = 0$  as  $0 \cdot (a \otimes x) = 0$ . If  $x_i$  generates  $M$  and  $y_i$  generates  $N$  then  $x_i \otimes y_i$  generates  $M \otimes N$ .

Let  $x \in M$  and  $y \in N$  if  $M' \subseteq M$  and  $N' \subseteq N$  are submodules then  $x \otimes y \in M \otimes N$  is not the same as  $x \otimes y \in M' \otimes N'$

To be specific the tensor product of  $A$ -modules is denoted by  $M \otimes_A N$  but if the context is clear we can write  $M \otimes N$ .

**Proposition 3.1.1.** [2] Let  $M, N, P$  be  $A$ -modules. Then there exists unique isomorphisms called the canonical isomorphisms

1.  $M \otimes N \rightarrow N \otimes M$ , (given by  $x \otimes y \mapsto y \otimes x$ )
2.  $(M \otimes N) \otimes P \rightarrow M \otimes (N \otimes P) \rightarrow M \otimes N \otimes P$ , (given by  $(x \otimes y) \otimes z \mapsto x \otimes (y \otimes z) \mapsto x \otimes y \otimes z$ )
3.  $(M \oplus N) \otimes P \rightarrow (M \otimes P) \oplus (N \otimes P)$ , given by  $(x, y) \otimes z \mapsto (x \otimes z, y \otimes z)$
4.  $A \otimes M \rightarrow M$ , given by  $a \otimes x \mapsto ax$ .

### 3.2 Flatness

A  $A$ -module  $N$  is called a *flat* module if for every exact sequence

$$\cdots \rightarrow M_{i-1} \xrightarrow{f_i} M_i \xrightarrow{f_{i+1}} M_{i+1} \rightarrow \cdots$$

when *tensor*ed (multiplied) by  $N$  gives another sequence

$$\cdots \rightarrow M_{i-1} \otimes N \xrightarrow{f_i} M_i \otimes N \xrightarrow{f_{i+1}} M_{i+1} \otimes N \rightarrow \cdots$$

which is *exact*.

### 3.3 Tensor Product of Algebras

We now define multiplication on the tensor product in the following way so that it turns into a commutative ring with identity element  $1 \otimes 1$ :

Let  $B, C$  be two  $A$ -algebras with associated homomorphisms  $f : A \rightarrow B$  and  $g : A \rightarrow C$ . As algebras are themselves modules we take their tensor product  $D = B \otimes_A C$ .

Define the multiplication  $D \otimes D \rightarrow D$  by the  $A$ -bilinear mapping  $\mu : D \times D \rightarrow D$  so that,

$$\mu(b \otimes c, b' \otimes c') = b b' \otimes c c'.$$

That is,  $(b \otimes c)(b' \otimes c') = b b' \otimes c c'$  and more generally,  $(\sum_i (b_i \otimes c_i))(\sum_j (b'_j \otimes c'_j)) = \sum_{i,j} (b_i b'_j \otimes c_i c'_j)$

1. The mapping  $a \mapsto f(a) \otimes g(a)$  is a ring homomorphism  $A \rightarrow D$ .
2. There is a commutative diagram of ring homomorphisms,

$$\begin{array}{ccc} & B & \\ f \nearrow & & \searrow u \\ A & & D \\ g \searrow & & \nearrow v \\ & C & \end{array}$$

### 3.4 Direct Limit

## Chapter 4

# Sheaf and Presheaf

4.1 Support

4.2 Presheaf

4.3 Sheaf

4.4 Constructible Topology

4.5 Absolute Flatness

## Chapter 5

# The Going-Up Theorem

# Bibliography

- [1] Ravi Vakil, *Math 145: Algebraic Geometry*
- [2] Atiyah-Macdonald, *Introduction to Commutative Algebra*
- [3] Mumford's Treasure Map, *Mumford's Treasure Map*