Algebraic Geometry

Jubayer Ibn Hamid

Contents

Algebraic geometry is about solutions of polynomial equations and the geometric structures on the space of those solutions. We use the language and techniques from abstract algebra on these geometric objects.

1 Terminology

A field k is algebraically closed if any non-constant polynomial $f \in k[x]$ has at least one root/zero in k i.e if $f \in k[x]$, then $f(x) = \mu \prod(x - \lambda_i)^{e_i}$ where $\lambda_i \in k$ are the roots. The field $\mathbb{R}$ is not algebraically closed as $f(x)x^{+}1$ has no root in $\mathbb{R}$, whereas $\mathbb{C}$ is algebraically closed.

The affine space of field k is denoted by $\mathbb{A}_k^n$ which is the Cartesian n-product of k.

The true coordinate ring $O(\mathbb{A}^n)$ of functions on $\mathbb{A}^n$ is the commutative ring $k[x_1, ..., x_n]$ of polynomials with n variables.

Let $f \in k[x_1, ..., x_n]$ be a polynomial. Then, $V(f)$ is the set of zeros of f and is called the hypersurface defined by f. If S is a set of polynomials from $k[x_1, .., x_n]$, then $V(S) := \{p \in \mathbb{A}_k^n \mid f(p) = 0, \forall f \in S\}$. One can check that $V(S) = \cap_{f \in S} V(f)$. When $S = \{f_1, ..., f_r\}$, we write $V(S)$ as $V(f_1, ..., f_r)$.

A subset $X \subseteq \mathbb{A}_k^n$ is called an affine algebraic set if $X = V(S)$ for some set S of polynomials in $k[x_1, ..., x_n]$. Throughout these notes, we will use the term affine variety to mean the same thing as affine algebraic sets (although some texts refer to only *irreducible* algebraic sets as affine varieties). One can easily show that if I is the ideal in $k[x_1, ..., x_n]$ generated by polynomials in S, then $V(S) = V(I)$. Suppose, $I = (f_1, ..., f_n)$, then, $V(I) = \cap_{i=1}^n V(f_i)$. Some more properties:

(1) If $\{I_\alpha\}$ is a collection of ideals, then $V(\cup_\alpha I_\alpha) = \cap_\alpha V(I_\alpha)$. (2) $I \subset J \implies V(J) \subset V(I)$ (3) $V(fg) = V(f) \cup V(g)$ (4) Any finite subset of $\mathbb{A}_k^n$ is an algebraic set (5) $V(A) = V((A))$ where (A) is the ideal generated by A.

The ideal generated by a set of functions $f_1, ..., f_m \in k[x_1, ..., x_n]$ is the set $(f_1, ..., f_m) := \{\sum_{i=1}^m g_i f_i : g_i \in k[x_1, ..., x_n]\}$. For a subset $X \subseteq \mathbb{A}_k^n$, consider the ideal in $k[x_1, ..., x_n]$ generated by polynomials that vanish on X. This ideal is called the vanishing ideal of X, denoted by $I(X)$. So,
$I(X) = \{f \in k[x_1, ..., x_n] : f(a) = 0, \forall a \in X\}$. So, if $f, g \in I$, then $f + g \in I$ and for any $h \in k[x_1, ..., x_n]$, $hf \in I$. Some more properties:

(1) $X \subset Y \implies I(Y) \subset I(X)$ (2) $I(\emptyset) = k[x_1, ..., x_n], I(\mathbb{A}^n) = \emptyset, I(\{a\}) = (x_1 - a_1, ..., x_n - a_n)$.

We say $f_1, ..., f_m$ scheme-theoretically define the affine variety $X \subset \mathbb{A}^n$ if $I(X) = (f_1, ..., f_m)$ i.e the ideal generated by $f_1, ..., f_m$. Furthermore, the ideal I is said to set-theoretically define variety X if $X = V(I)$ if It can be easily shown that $V(I)(X)) = X$. $V(-)$ and $I(-)$ allow us to switch betwen the geometric world and the algebraic world which is a key tool used in algebraic geometry. In particular, later on, we will see that using Hilbert's Nullstellensatz, there is no information lost after we make this switch.

We also define fractional fields. Let R be an integral domain. Its fractional field $K = Frac(R)$ is defined as the ring

$$K := \{\frac{f}{g} : f, g \in R, g \neq 0\}$$

.

A polynomial mapping/morphism $p : V \to W$, where $V \subset \mathbb{A}^n$, $W \subset \mathbb{A}^m$ are varieties, is a mapping such that $(x_1, ..., x_n) \to f(x_1, ..., x_n) := (f_1(x_1, ..., x_n), ..., f_m(x_1, ..., x_n))$, $f_i \in k[x_1, ..., x_n]$ and the image of the algebraic set V lies inside the algebraic set W. The mapping set $Map(V, W)$ is the set of all polynomial maps from V to W and in our case this is the set of all polynomial maps from V to W. We need polynomial mappings in order to investigate the relationships between varieties. Given X is an affine variety, an **automorphism** of X is a polynomial map $f : X \to X$ which is an isomorphism. $Aux(X)$ denotes the group of all automorphisms of X.

2 Hilbert Basis Theorem

First, we note that for $a := (a_1, ..., a_n) \in \mathbb{A}^n_k$, $I(\{a\}) = (x_1 - a_1, ..., x_n - a_n) \subset k[x_1, ..., x_n]$. To see this, note that $(x_1 - a_1, ..., x_n - a_n) \subset I(\{a\})$ which is straightforward. To see the other direction, suppose $f \in I(\{a\})$. Since $f \in k[x_1, .., x_n]$, we can write it as $f = \sum_{i_1,...i_n \geq 0} a_{i_1 \cdots i_n} x_1^{i_1} \cdots x_n^{i_n}$. Since $f(a) = 0$, we can write this as $f(x) = \sum_{i_1,...i_n \geq 0} b_{i_1 \cdots i_n} (x_1 - a_1)^{i_1} \cdots (x_n - a_n)^{i_n}$ and so $f(x) \in (x_1 - a_1, ..., x_n - a_n)$.

Definition 1. *A ring* R *is called Noetherian if every ideal in* R *is finitely generated.*

Fields and Principal Ideal Domains (PIDs) are Noetherian rings.

One can easily verify the following:

R is Noetherian if and only if every sequence of ideals $I_1 \subset I_2 \subset \cdots$ stabilizes i.e there exists N such that $I_N = I_{N+1} = \cdots$.

Proof. Forward direction: If every ideal is finitely generated then the ideal $\cup_i I_i$ is finitely generated and so the generating set of $\cup_i I_i$ must lie in some I_N. Conversely, suppose the sequence stabilizes but there exists an I that is not finitely generated. Then take a sequence of $f_i \in I$ such that $f_i \notin (f_1, ..., f_{i-1})$ yields an increasing sequence of ideals i.e $(f_1) \subset (f_1, f_2) \subset (f_1, f_2, f_3) \subset \cdots$ that does not stabilize - contradiction. □

Theorem 1. *(Hilbert Basis Theorem) If* R *is a Noetherian ring, then* $R[x_1, ..., x_n]$ *is a Noetherian Ring.*

Proof. We know $R[x_1, ..., x_n] \cong R[x_1, ..., x_{n-1}][x_n]$. So, if we can prove that R Noetherian implies R[x] is Noetherian, by induction we will have proven that $R[x_1, ..., x_n]$ is also Noetherian.

Suppose R is Noetherian. Let I be an ideal in R[x]. Let J denote the set of leading coefficients of polynomials in I. Then, given I is an ideal, J is an ideal in R. Since R is Noetherian, we can write that J is generated by the leading coefficients of $f_1, ..., f_r \in I$. Suppose $N \in \mathbb{Z}$ such that N is greater than the degrees of all polynomials $f_1, ..., f_r$. Then, for any $m \leq N$, we define J_m to be the ideal in R generated by the leading coefficients of all polynomials f in I such that $\deg(f) \leq m$. Once again, since J_m is an ideal in R, we can say that J_m is generated by the finite set of polynomials, $\{f_{mj}\}$, such that each polynomial's degree is less than or equal to m. Finally, define I' be the ideal generated by polynomials $\{f_{mj}\}$ and f_i.

We claim $I' = I$. Suppose not i.e suppose there exists elements in I that are not in I'. Let g be the minimal element such that $g \in I$, $g \notin I'$.

Case 1: $\deg(g) > N$. Then, there exists polynomials Q_i such that $\sum_i Q_i f_i$ has the same leading term as g. Therefore, $\deg(g - \sum_i Q_i f_i) < \deg(g)$. Clearly, $g - \sum_i Q_i f_i$ is in I'. But since g is the minimal element and $\deg(g - \sum_i Q_i f_i) < \deg(g)$, therefore $g - \sum_i Q_i f_i \in I'$, which implies $g \in I'$.

Case 2: $m := \deg(g) \leq N$. Then, there exists polynomials Q_j such that $\sum_j Q_j f_{mj}$ and g have the same leading term. Using a similar argument, we get that $g \in I'$. □

This has the following interesting implication:

Theorem 2. *An algebraic set is the intersection of a finite number of hypersurfaces.*

Proof. Let $V(I)$ be an algebraic set. We prove that I is finitely generated since that implies $V(I) = V(f_1, ..., f_r) = \cap_{i=1}^r V(f_i)$. Given k is a field, k is a Noetherian ring and by the Hilbert Basis Theorem, $k[x]$ is also Noetherian. Therefore, the ideal I in $k[x]$ is finitely generated. □

Corollary 3. $k[x_1, ..., x_n]$ *is a Noetherian ring for any field* k.

Proof. Follows from the Hilbert Basis Theorem. □

We have some other useful corollaries:

- Any descending chain of subvarieties of $\mathbb{A}^n$ must stabilize i.e if $V_1 \supset V_2 \supset V_3 \cdots$, then there exists N such that $V_N = V_{N+1} = \cdots$.

- There exists a finite subset $B \subset A$ such that $V(A) = V(B)$.

3 Modules Revision

Definition 2. R-*Module.*

Let R *be a ring. Let* M *be an abelian group* $(M,+)$*. Then, an* R*-module is* M *with multiplication* $R\times M \to M$ *such that for any* $a, b \in R$, $m \in M$, $(a+b)m = am+bm$, $a(m+n) = am+an$, $(ab)m = a(bm)$, $1_R m = m$.

Definition 3. *Submodule.*

A submodule N *is a subgroup of* R*-module,* M*, such that* $an \in N$ *for any* $a \in R, n \in N$.

One can check that for any $m \in M$, $0_R m = 0_M$ by noting that $0_R m = (x-x)m = xm-xm = 0_M$ for any $x \in R, m \in M$. Also, the submodule N of an R-module is an R-module itself.

Definition 4. *Submodule generated by* S.

Let $S := \{s_1, s_2, ...\}$ *be a set of elements of the* R*-module* M*. Then the submodule generated by* S *is* $\{\sum_i r_i s_i \mid r_i \in R, s_i \in S\}$.

When S *is finite, we denote the submodule generated by* S *as* $\sum_i Rs_i$.

Definition 5. *Finiteness conditions of subrings of a ring.*

Let S *be a ring and let* R *be a subring of* S.

(1) S *is module-finite over* R *if* S *is finitely-generated as an* R*-module i.e* $S = \sum_{i=1}^n Rv_i$ *where* $v_1, ..., v_n \in S$*. More explicitly,* $S = \{\sum_{i=1}^n r_i v_i : r_i \in R\}$*, for* $v_1, ..., v_n \in S$ *fixed.*

(2) S *is ring-finite over* R *if* $S = R[v_1, ..., v_n] = \{\sum_i a_i v_1^{i_1} \cdots v_n^{i_n} \mid a_i \in R\}$ *where* $v_1, ..., v_n \in S$.

(3) S *is a finitely-generated field extension of* R *if* S *and* R *are fields and* $S = R(v_1, ..., v_n)$ *(the quotient field of* $R[v_1, ..., v_n]$*) where* $v_1, ..., v_n \in S$.

(Recall: the definition of field extension. Firstly, given A *is a field, then a subset* $B \subseteq A$ *is a subfield if it contains 1 and it is closed under addition and multiplication and taking the inverse of non-zero elements of* B*. Given* B *is a subfield of* A*, we call* A *a field extension of* B*.)*

Properties:

1. If S is module-finite over R, then S is ring-finite over R. (This is straightforwardly seen from the definitions)

2. If L = K(x), then L is a finitely-generated field extension of K but L is not ring-finite over K.

Proof. Using the definition, L is a finitely generated field extension of K and so K(X) is a finitely-generated field extension of K. Now, suppose L is ring-finite over K. Then, $L = K[v_1, ..., v_n]$ and so $K(x) = K[v_1, ..., v_n]$, where $v_1, ..., v_n \in k(x)$.

Then, there exists $\frac{s_i}{t_i} \in K(X)$ that generate L where $i = 1, ..., n$. Define $p := 1/q$ where q is an irreducible polynomial that has a higher degree than all t_i's. Then, as $p \in K(X)$, $p = \frac{h}{t_1^{e_1} \cdots t_n^{e_n}}$. Since q has a higher degree than all the t_i's, we see that p cannot be equal to $\frac{1}{q}$. □

Definition 6. *Integral elements*

Let R *be a subring of the ring* S*. Then,* $v \in S$ *is* integral over R *if there exists a monic polynomial* $f = x^n + a_1 x^{n-1} + \cdots + a_n \in R[x]$ *such that* $f(v) = 0$ *and* $a_i \in R$*. If* R *and* S *are fields, we say* v *is algebraic over* R.

When all elements of S *is integral over* R*, we say* S *is integral over* R*. When* S *and* R *are fields and* S *is integral over* R*, we call* S *an* algebraic extension of R.

Theorem 4. *Let* R *be a subring over an integral domain* S *and let* $v \in S$*. Then, the following are equivalent:*

(1) v *is integral over* R.

(2) R[v] *is module-finite over* R.

(3) There exists a subring R' *of* S *such that* R' *contains* R[v] *and it is module-finite over* R.

Proof. We see (2) implies (3) readily. Now, (1) implies (2): Suppose v is integral over R with the monic polynomial $f(x) = x^n + a_1 x^{n-1} + ... + a_n$. Then, $f(x) = 0 \implies v^n \in \sum_{i=0}^{n-1} Rv^i$. Therefore, for any integer m, $v^m \in \sum_{i=0}^{n-1} Rv^i$. This implies R[v]. Lastly, (3) implies (1) as follows: Suppose R' is module-finite over R. Then, $R' = \sum Rw_i$, where $w_i \in R'$. Then, $vw_i \in R[v] \subset R'$, so $vw_i \sum_j a_{ij} w_j$ where $a_{ij} \in R$.

Now, $vw_i - vw_i = 0$ implies $\sum_{j=1}^n \delta_i j v w_j - vw_i = 0$ which then implies $\sum_{j=1}^n (\delta_{ij} v - a_{ij}) w_j = 0$ (here $\delta_{ij} = 1\{i = j\}$. Write this in matrix notation and consider these equations in the quotient field of S and note than $(w_1, ..., w_n)$ is a non-trivial solution to these equations (as we see, they give 0). Therefore, $\det(\delta_{ij} v - a_{ij}) = 0$ from which we get $v^n + a_1 v^{n-1} + ... + a_n = 0$. Therefore, v is integral over R. □

Corollary 5. *The set of elements of* S *that are integral over* R *is a subring of* R *that contains* R.

Proof. Suppose a, b are elements in S that are integral over R. Now. b is integral over R implies b is integral over R[a] as $R \subset R[a]$. Therefore, by the previous theorem, R[a, b] is module-finite over R. Then by the previous theorem $a+b, a-b, ab \in R[a,b]$ and so they are all integral over R. $\square$

We will require the following results:

Theorem 6. *Suppose an integral domain* S *is ring-finite over* R*. Then,* S *is module-finite over* R *if and only if* S *is integral over* R*.*

Proof. For the forward direction, write $S = \sum Rv_i$. Then consider any $s \in S$. So, $s = \sum Rv_i$. Consider the monic polynomial $f(x) = x - s$. Conversely, suppose S is integral over R. Then consider any $s \in S$ for which we have, using the monic polynomial, $s + a_1 s^{n-1} + \cdots + a_n = 0$. From this, we write $s = -a_1 s^{n-1} + ... - a_n$. $\square$

Theorem 7. *Let* L *be a field and let* k *be an algebraically closed subfield of* L*. Then an element of* L *that is algebraic over* k *is in* k*. Furthermore, an algebraically closed field has no module-finite field extension except itself.*

Proof. Proof of the first part - suppose $p \in L$ that is algebraic over k. Therefore, $p^n + a_1 p^{n-1} + \cdots + a_n = 0$ with $a_i \in k$. This is a polynomial in k[x] with a root p in k, so $p \in k$.

Now, we prove the second part. Suppose L is module-finite over k. Then, by the previous theorem, L is integral over k. Then, by the first part $L = k$. $\square$

Lastly,

Theorem 8. *Let* k *be a field. Let* $L = k(x)$ *be the field of rational functions over* k*. Then, (a) any element of* L *that is integral over* k[x] *is also in* k[x]*. (b) There is no non-zero element* $f \in k[x]$ *such that* $\forall z \in L$, $f^n z$ *is integral over* k[x] *for some* $n > 0$*.*

Proof. (a) p is integral over k[x] implies there exists the following polynomial $p^n + a_1 p^{n-1} + ... = 0$. Now, since $p \in k(x)$, we may write it as $p = \frac{s}{t}$ where $s, t \in k[x], t \neq 0$. Then, we get $s^n + a_1 s^{n-1} t + \cdots + a_n t^n = 0$. Rearranging, we get $s^n = -a_1 s^{n-1} t - \cdots - a_n t^n$. Since t divides the right hand side, t divides s. This means, s/t is a polynomial in k[x]. Therefore, $p \in k[x]$.

(b) Suppose, not. Let f be such a function. Let $p(x) \in k[x]$ such that p(x) does not divide f^m for any m. Set $z = \frac{1}{p}$, so $z \in L = k(x)$. Then, $f^n z = \frac{f^n}{p}$ is integral over k[x]. This means, there exists $a_i \in k[x]$ such that $(\frac{f^n}{p})^d + \sum_{i=1}^{d-1} a_i (\frac{f^n}{p})^i = 0$. From this, we get $f^{nd} = \sum_{i=1}^{d-1} a_i p^{d-i} f^{in}$. Since p divides the right hand side, we get that p divides f^{nd} which contradicts our definition of p. $\square$

4 Hilbert's Nullstellensatz

First, we prove the following:

Theorem 9. *(Zariski) If a field* L *is ring-finite over a subfield* k*, then* L *is module finite (and, hence, algebraic) over* k*.*

Note that L is module finite over k if and only if L is integral over k which means L is algebraic over k.

Proof. Suppose L is ring-finite over k. Then, $L = k[v_1, ..., v_n]$ where $v_i \in L$. We proceed by induction.

Suppose $n = 1$. We have that k is a subfield of L and $L = k[v]$. Let $\psi : k[x] \to L$ be a homomorphism that takes x to v. Now $\ker(\psi) = (f)$ for some f since k[x] is a principal ideal domain. Then, $k[x]/(f) \cong k[v]$ by the first isomorphism theorem. This implies (f) is prime (since k[v] is an integral domain).

Now, if $f = 0$. Then $k[x] \cong k[v]$, so $L \cong k[x]$. However, by the second property following definition 5, this cannot be true. Therefore, $f \neq 0$.

Given $f \neq 0$, we can assume f is monic. Then, (f) prime implies f is irreducible and (f) is a maximal ideal (check Dummit and Foote). This means, $k[v] \cong k[x]/(f)$ is a field (check Dummit and Foote). Therefore, $k[v] = k(v)$. Since $f(v) = 0$, so v is algebraic over k and so, by theorem 4, $L = k[v]$ is module-finite over k. This concludes the proof for $n = 1$.

Now, for the inductive step, assume true for $n-1$ i.e $k[v_1, ..., v_{n-1}]$ is module-finite over k. Let $L = k_1[v_2, ..., v_n]$ where $k_1 = k(v_1)$. Then, by the inductive hypothesis, $k_1[v_2, \cdots, v_n]$ is module-finite over k_1.

We show that v_1 is algebraic over k which would say $k[v_1]$ is module-finite over k concluding the proof. Suppose, v_1 is not algebraic over k. Then, using the inductive hypothesis, for each $i = 2, ..., n$, we have an equation $v_i^{n_i} + a_{i1}v_i^{n_i-1} + \cdots = 0$ where $a_{ij} \in k_1$.

Let $a \in k[v_1]$ such that a is a multiple of all the denominators of $a_{ij} \in k(v_1)$. We get $av_i^{n_i} + aa_{i1}(av_1)^{n_i-1} + \cdots = 0$. Then, by corollary 5, for any $z \in L = k[v_1, \cdots, v_n]$, there exists N such that $a^N z$ is integral over $k[v_1]$ (since the set of integral elements forms a subring). Since this holds for any $z \in L$, this also holds for any $z \in k(v_1)$. But by theorem 8, this is impossible. This gives us the contradiction. □

Assume k is algebraically closed.

Theorem 10. *(Nullstellensatz Version I) If* I *is a proper ideal in* $k[x_1, ..., x_n]$*, then* $V(I) \neq \emptyset$.

Proof. For any ideal I, there exists a maximal ideal J containing I (since we are assuming our ring has an identity $1 \neq 0$, see Dummit and Foote). So, for simplicity, we assume I is the maximal ideal itself since $V(J) \subset V(I)$. Then, $L = k[x_1, \cdots, x_n]/I$ is a field (since I is maximal, see Dummit and Foote) and k is an algebraically closed subfield of L. Note that there is a ring-homomorphism from $k[x_1, ..., x_n]$ onto L, which is the identity. This means, L is ring-finite over k. Then, by theorem 9, L is module-finite over k. Then, by theorem 7, $L = k$ i.e $k = k[x_1, ..., x_n]/I$.

Now, since $k = L$, in particular this means $k \cong k[x_1, ..., x_n]/I$. Suppose $x_i \in k[x_1, ..., x_n]$ is mapped to a_i by the homormorphism ψ whose kernel is I. Then, $x_i - a_i$ is mapped to 0, so $x_i - a_i \in I$. Now, note that $(x_1 - a_1, ..., x_n - a_n)$ is a maximal ideal as one can easily verify and it contains I, so $I = (x_1 - a_1, ..., x_n - a_n)$. So, $(a_1, ..., a_n) \in V(I)$. Therefore, $V(I) \neq \emptyset$. □

The fact that every maximal ideal in the polynomial ring over n **variables is of the form** $(x_1 - a_1, ..., x_n - a_n)$ **is a very important thing to remember.**

We recall some definitions before moving to Hilbert's Nullstellensatz. The radical of an ideal I in R is $\sqrt{I} := \{a \in R : a^n \in I, \text{for some} n \in \mathbb{Z}, n > 0\}$. It can be easily shown that $\sqrt{I}$ is an ideal itself and $I \subseteq \sqrt{I}$. I is called a radical ideal if $I = \sqrt{I}$.

For any ideal I in $k[x_1...x_n]$, $V(I) = V(\sqrt{I})$. To see this, note that $I \subseteq \sqrt{I}$ implies $V(\sqrt{I}) \subseteq V(I)$. Conversely, let $v \in V(I)$ and let $f \in \sqrt{I}$. Then, $f^n \in I$ for some $n > 0$. This implies $f^n(v) = 0$ which implies $f(v) = 0$ as k has no zero divisor. Therefore, $v \in V(\sqrt{I})$.

Lastly, $\sqrt{I} \subset I(V(I))$. To see this, suppose $s \in \sqrt{I}$. Then, $s^n \in I$ for some n. Now, let $v \in V(I)$. Then, $s^n(v) = 0$ implies $s(v) = 0$, so $s \in I(V(I))$.

Now, we prove Hilbert's Nullstellensatz:

Theorem 11. *(Hilbert's Nullstellensatz) Let* I *be an ideal in* $k[x_1, ..., x_n]$ *where* k *is algebraically closed. Then,* $I(V(I)) = \sqrt{I}$.

Proof. We already know $\sqrt{I} \subset I(V(I))$. So, we only need to prove the other direction. Let $I = (f_1, ..., f_r)$ where $f_i \in k[x_1, ..., x_n]$. Suppose, $G \in I(V(f_1, ..., f_r))$. Define $J := (f_1, ..., f_r, x_{n+1}G - 1) \subset k[x_1, ..., x_n, x_{n+1}]$. Then, $V(J) \subset \mathbb{A}^n_k$ is $\emptyset$ since G is 0 whenever all f_i are 0 and therefore, $x_{n+1}G - 1 \neq 0$ at those points.

Since $V(J) = \emptyset$, J is not a proper ideal by the previous theorem. Therefore, $J = k[x_1, \cdots, x_{n+1}]$. So, $1 \in J$ (check Dummit and Foote; an ideal in R is all of R iff it contains a unit). So $1 = \sum_i a_i(x_1, ..., x_{n+1})f_i + b(x_1, .., x_{n+1})(x_{n+1}G - 1)$.

In particular, if $x_{n+1} = \frac{1}{G}$, then, $1 = \sum_i a_i f_i + b(1-1) = \sum_i a_i f_i$. Therefore, $G^N = G^N \sum_i a_i f_i$, so $G^N \in (I)$. Therefore, $G \in \sqrt{I}$. Therefore, $I(V(I)) \subseteq \sqrt{I}$. □

This has a series of interesting applications.

Corollary 12. *If* I *is a radical ideal in* $k[x_1, ..., x_n]$*, then* $I(V(I)) = I$*. Therefore, there is a one-to-one correspondence between radical ideals and algebraic sets.*

Corollary 13. *If* I *is a prime ideal, then* $V(I)$ *is irreducible. There is a one-to-one correspondence between prime ideals and irreducible algebraic sets. The maximal ideals correspond to points.*

Corollary 14. *Let* F *be a non-constant polynomial in* $k[x_1, \cdots, x_n]$ *with the irreducible decomposition of* F *being* $F = F_1^{n_1} F_2^{n_2} \cdots F_r^{n_r}$*. Then,* $V(F) = V(F_1) \cup \cdots \cup V(F_r)$ *is the decomposition of* $V(F)$ *into irreducible components and* $I(V(F)) = (F_1 \cdots F_r)$*. Therefore, there is a one-to-one correspondence between irreducible polynomials* $F \in k[x_1, \cdots, x_n]$ *(up to multiplication by a non-zero element of* k*) and irreducible hypersurfaces in* $\mathbb{A}_k^n$*.*

Corollary 15. *Let* I *be an ideal in* $k[x_1, \cdots, x_n]$*. Then,* $V(I)$ *is a finite set if and only if* $k[x_1, \cdots, x_n]/I$ *is a finite dimensional vector space over* k*. If this occurs, then, the number of points in* $V(I)$ *is at most* $\dim_k(k[x_1, \cdots, x_n]/I)$*.*

Proof. Let $p_1, \cdots, p_r \in V(I)$. Choose $f_1, \cdots, f_r \in k[x_1, \cdots, x_n]$ such that $f_i(p_j) = 0$ if $i \neq j$ and $f_i(p_i) = 1$ and let $\bar{f_i}$ be the residue class of f_i. Now, if $\sum_i \lambda_i \bar{f_i} = 0$ with $\lambda_i \in k$, then, $\sum_i \lambda_i f_i \in I$. Therefore, $\lambda_j = (\sum_i \lambda_i f_i)(p_j) = 0$. Therefore, $\bar{f_i}$ are linearly independent over k. So $r \leq \dim_k(k[x_1, \cdots, x_n]/I)$.

Conversely, suppose $V(I) = (p_1, \cdots, p_r)$ and so is finite. Let $p_i = (a_{1i}, \cdots, a_{1n})$ and define $f_j := \prod_{i=1}^r (x_j - a_{ij}), j = 1, \cdots, n$. Then, $f_j \in I(V(I))$, so for all j, $f_j^N \in I$ for some large enough $N > 0$. Now, taking I-residues, $\bar{f_j}^N = 0$. By expanding f_j^N, we get that $\bar{x_j}^{rN}$ is a k-linear combination of $\bar{1}, \bar{x_j}, \cdots, \bar{x_j}^{rN-1}$. So, for all s, $\bar{x_j}^s$ is a k-linear combination of $\bar{1}, \bar{x_j}, \cdots, \bar{x_j}^{rN-1}$. Therefore, the set $\{\bar{x_1}^{m_1}, \cdots, \bar{x_n}^{m_n} : m_i < rN\}$ generates $k[x_1, \cdots, x_n]/I$ as a vector space over k. □

Definition 7. *Reduced Rings. A ring* R *is called reduced if* $f^N = 0 \in R$ *implies* $f = 0$*.*

Next, we find irreducible decompositions of algebraic sets of an affine space.

5 Irreducible Components of Algebraic Sets

So far, we have seen polynomials and the varieties defined over them. Now, we bring in topological invariants.

Definition 8. *Irreducible decomposition of a set. Let* $V \in \mathbb{A}^n_k$ *be an algebraic set. Then,* V *is reducible if* $V = V_1 \cup V_2$ *where* V_1, V_2 *are non-empty, algebraic sets in* $\mathbb{A}^n_k$ *i.e* $V_i \neq V$ *for* $i = 1, 2$. *If* V *is not irreducible, we call it reducible.*

Theorem 16. *The algebraic set* V *is irreducible if and only if* $I(V)$ *is prime.*

Proof. Suppose, V is irreducible. Now, suppose for contradiction, $I(V)$ is not prime. Therefore, by definition of prime, there exists $f_1 f_2 \in I(V)$ such that $f_1 \notin I(V)$ and $f_2 \notin I(V)$. Now, $V = (V \cap V(f_1)) \cup (V \cap V(f_2))$ and $V \cap V(f_i) \subset V, V \cap V(f_i) \neq V$- to see this, note that for any $p \in V$ such that p is a zero of $f_1 f_2$, p has to be a root of either f_1 or f_2 since f_i belong to an integral domain, therefore, $p \in (V \cap V(f_1)) \cup (V \cap V(f_2))$ (the other direction is obvious). Then, $V = (V \cap V(f_1)) \cup (V \cap V(f_2))$ is decomposition of V which means V is not irreducible - contradiction.

Conversely, suppose $I(V)$ is prime. For contradiction, suppose V is reducible with $V = V_1 \cup V_2$, V_i non-empty. Then, consider $f_i \in I(V_i)$ such that $f_i \notin V$. Clearly, $f_1 f_2 \in I(V)$, so $I(V)$ is not prime - contradiction. □

Corollary 17. *The affine space* $\mathbb{A}^n_k$ *is irreducible if* k *is infinite.*

Theorem 18. *Let* A *be a non-empty collection of ideals in a Noetherian ring* R. *Then,* A *has a maximal ideal i.e an ideal* I *such that* $I \in A$ *and no other ideal in* A *contains* I.

Proof. Given our collection of ideals, A, choose an ideal $I_0 \in A$. Then, define $A_1 = \{I \in A : I_0 \subsetneq I\}$ and $I_1 \in A_1$, $A_2 = \{I \in A : I_1 \subsetneq I\}$ and $I_2 \in A_2$ and so on. Then, the statement in the theorem is equivalent to saying that there exists positive integer n such that A_n is empty since that would mean there exists no ideal containing I_{n-1}. Suppose this is not true. Then, with $I := \cup_{n=0}^{\infty} I_n$, since R is Noetherian, therefore there exists $f_1, ..., f_m$ that generates the ideal I where each $f_i \in I_n$ for n sufficiently large. But since the generates are all in I_n, $I = I_n$ and so $I_{n'} = I_n$ for any $n' > n$ (since $I = \cup_{n=0}^{\infty} I_n$ by definition) - contradiction. □

We finally prove the main result. Note that this is pretty closely tied to the Hilbert Basis Theorem which says that every algebraic set is the intersection of a finite number of algebraic sets/hypersurfaces:

Theorem 19. *Let* V *be an algebraic set in* $\mathbb{A}^n_k$. *Then, there exists unique, irreducible algebraic sets* $V_1, ..., V_r$ *such that* $V = V_1 \cup V_2 \cdots \cup V_r$ *and* $V_i \subsetneq V_i$ *for any* $i \neq j$.

Proof. Proving this statement is equivalent to disproving that $\mathcal{F}$ is non-empty where $\mathcal{F} :=$ {algebraic set$V \in \mathbb{A}^n_k$: $V$is not the union of finitely many irreducible algebraic sets}.

Suppose, $\mathcal{F}$ is not empty. Let $V \in \mathcal{F}$ such that V is the minimal member of $\mathcal{F}$ i.e V cannot be written as the union of sets in $\mathcal{F}$.

Now, since $V \in \mathcal{F}$, V is reducible (if V is irreducible, then it is trivially the union of 1 irreducible subsets). Since V is reducible, $V = V_1 \cup V_2$ where $V_i \neq \emptyset$. Since V is the minimal member of $\mathcal{F}$, $V_i \notin \mathcal{F}$. Since $V_i \notin \mathcal{F}$, it is the union of finitely many irreducible algebraic sets, so let $V_i = V_{i1} \cup V_{i2} \cdots \cup V_{im_i}$. Then, $V = \cup_{i,j} V_{ij}$, so $V \notin \mathcal{F}$. So, we have shown that V can be written as $V = V_1 \cup \cdots \cup V_m$ where each V_i is irreducible. First, remove any V_i such that $V_i \subset V_j$. Now we prove uniqueness. Suppose $V = W_1 \cup \cdots W_m$ be another such decomposition. Then, $V_i = \cup_j (W_j \cap V_i)$. Now, $W_j \cap V_i = V_i$ since otherwise we will have found a decomposition of the irreducible set V_i. Therefore, $V_i \subset W_{j(i)}$ for some j(i). Similarly, by symmetry, $W_{j(i)} \subset V_k$ for some k. But then, $V_i \subset V_k$ implies $i = k$ and so $V_i = W_{j(i)}$. Continuing this for each $i \in \{1, ..., m\}$, we get that the two decompositions are equal. □

Furthermore, we use the following terms:

Definition 9. *An ideal* $I \subset k[x_1, ..., x_n]$ *set-theoretically defines a variety* V *if* $V = V(I)$. *An ideal* $J \subset \mathbb{A}^n$ *scheme-theoretically defines a variety* V *if* $J = I(V)$.

Here's a pretty straightforward result:

Theorem 20. *For an affine variety* X, *if* $f_1, ..., f_m$ *scheme-theoretically define* X, *then* $V(I(X)) = X$

Two affine-varities can be isomorphic in the usual sense using the language of polynomial maps:

Definition 10. *Isomorphic affine varieties. Two affine varieties* $V \subset \mathbb{A}^n$ *and* $W \subset \mathbb{A}^m$ *are isomorphic if there exists polynomial maps* $f : V \to W$ *and* $g : W \to V$ *such that* $f \circ g = g \circ f = i_d$.

Theorem 21. *Let* f *and* g *be two polynomials in* $k[x, y]$ *with no common factors. Then,* $V(f, g)$ *is a finite set of points.*

Proof. Check [1]. □

6 Zariski Topology

We will require this following result:

Theorem 22. *Let* $Z \subset \mathbb{A}^n$ *be an affine variety and let* $x \in \mathbb{A}^n - Z$*. Then, there exists* $f \in k[x_1, ..., x_n]$ *such that* $f(Z) = 0$ *and* $f(x) \neq 0$*.*

Proof. Suppose this is not true. Then, $f \in I(Z) \implies f \in I(Z \cup \{x\})$. Then, $I(Z) = I(Z \cup \{x\})$. Therefore, $Z = Z \cup \{x\}$ since $V(I(X)) = X$. This is contradiction since this implies $x \in Z$. $\square$

Now, we move on to define a topology on $\mathbb{A}^n$.

Definition 11. *Let* $X \subseteq \mathbb{A}^n$ *be an affine variety. Then,* $Z \subseteq X$ *is closed if* $Z \subseteq X \subseteq \mathbb{A}^n$ *is an affine variety i.e there exists* $f_1, ..., f_m \in k[x_1, ..., x_n]$ *such that* $Z = V(f_1, ..., f_m) \subset X$*.*

This forms a topology. $\emptyset$ is closed as $\emptyset = V(1)$. X itself is closed since $X = V(g_1, ..., g_m)$ by definition (since it's an affine variety). Now, suppose $\{Z_i\}_{i \in A}$ are affine varieties. Then, $\cap_{i \in A} Z_i = V(\sum_i I(Z_i))$. Lastly, $V(f_1, ..., f_m) \cup V(h_1, ..., h_r) = V(\sum_{i,j} f_i h_j)$.

Given any affine variety has a unique irreducible, this gives us topological invariants. This allows us to move between worlds:

$$\{\text{Polynomials}\} \leftrightarrow \{\text{Varieties}\} \rightarrow \{\text{Topological Invariants}\}$$

Theorem 23. *The pre-image of an affine variety under a polynomial map* $p : V \rightarrow W$ *is a variety. Therefore, in Zariski topology, polynomial maps/morphisms between varieties are continuous.*

Proof. Let $V \subseteq \mathbb{A}_k^n, W \subseteq \mathbb{A}_k^m$ be affine varieties. Write p as $p = (p_1, ..., p_m)$ where the image of each p_i is in k. Now, suppose $Z := V(g_1, ..., g_m) \subseteq W$ is closed. We show $f^{-1}(Z)$ is closed. $f^{-1}(Z) = \{x = (x_1, ..., x_n) \in V : (p_1(x), ..., p_m(x) \in Z\} = \{x \in V : g_j(f(x)) = 0, \forall j\} \implies f^{-1}(Z)$ is closed. $\square$

For an example, consider the Zariski topology on $\mathbb{A}_k^1$ and let $V(f_1, ..., f_m) \subset \mathbb{A}_k^1$. Now, given K is a field, k[x] is a principal ideal domain so $(f_1, ..., f_m) = (g)$ for some $g \in k[x]$. Then, the closed subset i.e variety of $\mathbb{A}_k^1$ is of the form $V(g) = \{x \in k : g(x) = 0\}$ which is finite since g is a polynomial of some degree. This means that the closed subsets of $\mathbb{A}_k^1$ are of the form $\emptyset, \mathbb{A}_k^1$ and finite subsets of $\mathbb{A}_k^1$.

Definition 12. *Coordinate Ring. Let* $X \subset \mathbb{A}^n$ *be an affine variety. The coordinate ring of functions on* V *is*

$$O(X) := k[x_1, .., x_n]/I(X)$$

is the quotient ring of polynomials in n*-variables.*

Note that, for a point $a = (a_1, ..., a_n) \in X$ and $f \in O(X)$, the value of $f(a) \in k$ is well-defined. This is because for any $f' \in I(X), f'(a) = 0$, so the value $f(a)$ is independent of our choice of function from $I(V)$.

The coordinate ring $O(X)$ can be thought of as a ring of polynomials such that we only care about their values on X since we identify two polynomials that are equal on X to be the same.

We can always write, using first isomorphism theorem, $O(X) = k[x_1, .., x_n]/I(X) \cong k$ by sending each $f \in I(X)$ to 0 which means $(x_1, ..., x_n) \in X$ (by properties of homomorphisms).

Definition 13. *First, we define* $\underline{V(f)_X := V(f) \cap X}$ *where* $X \subset \mathbb{A}^n$ *is an affine variety. Now, we define* <u>*basic closed sets of* X</u> *be sets of the form* $V(f)_X$*. Note that* $V(\{f_i\}_{i \in I}) = \cap_i V(f_i)$*. Any closed set in* <u>*the Zariski topology*</u> *is a union of basic closed sets for some set of functions. On the other hand, the* <u>*basic open sets of* X</u> *are of the form* $D(f)_X := \{x \in X : f(x) \neq 0\}$ *i.e* $D(f)_X = X - V(f)$*. Any open set in* <u>*Zariski topology*</u> *is the union of some basic open sets.*

Note that, by Hilbert Basis Theorem, every closed subset of X *is a finite intersection of basic closed sets. Similarly, every open set is a finite union of basic open sets.*

There is a particularly **local nature of algebraic geometry** as evident by the following:

Corollary 24. *Let* $U \subseteq X$ *be a basic open subset of an affine variety* X*. Then, for any* $x \in U$*, there exists a basic open subset* $D(f) \subset X$ *and* $f \in k[x_1, ..., x_n]$ *such that* $x \in D(f) \subseteq U$*.*

Proof. Let $Z = X - U$ be the closed subset of X i.e an affine variety. Then, Theorem 15 allows us to conclude the statement. □

Some more useful corollaries:

Corollary 25. *(Hausdorff property of Zariski topology) Let* $x, y \in X$ *such that* $x \neq y$*. There exists an open subset* U_x *containing* x *but not* y*.*

This can be proven using the theorem at the start of this section.

Corollary 26. $D(1) = V, D(0) = \emptyset, D(fg) = D(f) \cap D(g)$.

Definition 14. *For a subset* X *of* V*, the Zariski closure of* X *in* V *is the minimal closed subset of* V *that contains* X *which we denote by* $\bar{X} \subseteq V$*.*

Note: S is irreducible if and only if $\bar{S} \subseteq V$ is irreducible.

7 Coordinate Rings

First, we recall that given $V \subset \mathbb{A}^n$, $W \subset \mathbb{A}^m$ are varieties, $f : V \to W$ is a polynomial map if $f(x_1, ..., x_n) = (f_1(x_1, ..., x_n), \cdots, f_m(x_1, ..., x_n))$, $f_i \in k[x_1, ..., x_n]$ and $f(V) \subset W$.

Furthermore, given the definition of coordinate ring and $I(\mathbb{A}^n_k) = 0$, $O(\mathbb{A}^n_k = k[x_1, \cdots, x_n]$ is the true coordinate ring of $\mathbb{A}^n_k$.

Definition 15. k*-algebra. Let* k *be a field (i.e a commutative division ring). A ring* R *is a* k*-algebra if* $k \subseteq Z(R) := \{x \in R : xy = yx, \forall y \in R\}$ *and the identity of* k *is the same as the identity of* R*.*

Note, $Z(R)$ *is the center of the ring* R*.*

Definition 16. *Finitely generated* k*-algebra. A finitely generated* k*-algebra is a ring that is isomorphic to a quotient of a polynomial ring* $k[x_1, ..., x_n]/I$*.*

Equivalently, a ring R *is a finitely-generated* k*-algebra if* R *is generated as a ring by* k *with some finite set* $r_1, ..., r_n$ *of elements of* R *i.e* $k[r_1, ..., r_n]$*.*

These definitions are equivalent. Suppose, R is a finitely generated k-algebra i.e $R = k[r_1, ..., r_n]$. Then, by the first isomorphism theorem, $R \cong k[r_1, ..., r_n]/I$. Conversely, suppose $R \cong k[r_1, .., r_n]/I$ i.e $\varphi : k[r_1, .., r_n]/I \to R$. Then, with $\pi : k[r_1, ..., r_n] \to k[r_1, ..., r_n]/I$, $f := \varphi \circ \pi : k[x_1, ..., x_n] \to R$ is a surjective homomorphism. Since f is a homomorphism, $f(p(x_1, ..., x_n)) = p(f(x_1), f(x_2), ..., f(x_n))$ and so all elements of R is a polynomial in $f(x_1), ..., f(x_n)$ with coefficients in R so they are generated by these n elements as a k-algebra.

Definition 17. $Mor_k(R, S)$*. Let* R *and* S *be* k*-algebras. Then,* $\psi : R \to S$ *is a* k*-algebra homomorphism,* $\psi \in Mor_k(R, S)$ *if* ψ *is a ring homomorphism that is identity on* k*.*

Note that if $\phi : R \to k$ is a k-algebra homomorphism, then ϕ is surjective.

Theorem 27. $O(X) \cong Map(X, \mathbb{A}^1)$*. Here,* $Map(X, \mathbb{A}^1)$ *is a commutative* k*-algebra under addition and multiplication on* $\mathbb{A}^1$*. Furthermore,* $O(X)^m \cong Map(X, \mathbb{A}^m)$

Proof. Let $\varphi : O(X) \to \mathrm{Map}(X, \mathbb{A}^1)$. Then, define $\varphi(f)(a) = f(a)$ for any $a \in X$. This is a homomorphism by design. To show surjectivity, by definition of $\mathrm{Map}(X, \mathbb{A}^1)$, $f \in \mathrm{Map}(X, \mathbb{A}^1)$ implies $f(x) \in k[x_1, ..., x_n]$ so $\bar{f} \in O(X)$ is mapped to f. To show injectivity, suppose $f \in O(X)$ is mapped to 0. Then, $f(x) = 0$ for all $x \in X$. This means, $f \in I(X)$ implying $f = 0$ in $O(X)$. □

Corollary 28. *Given* X *and* Y *are affine varieties,* $X \cong Y$ *implies* $O(X) \cong O(Y)$*.*

With these results in mind, we note that a key idea in algebraic geometry is to characterize an affine variety X by the ring of functions $O(X) \cong Map(X, \mathbb{A}^1)$.

Let $Mor_k(R_1, R_2)$ be th set of morphisms between 2 k-algebras R_1 and R_2. More strictly:

With this, we can define the pullback function:

Definition 18. *Given* $X \in \mathbb{A}^n$, $Y \in \mathbb{A}^m$ *are affine varieties,* $p \in Map(X, Y)$*, define* p^* *to be the map* $p^* : Mor_k(O(Y), O(X))$*,* $p^*(f) = f \circ p$.

Note that p is a map from X to Y whereas p^* is a morphism from O(Y) to O(X). In light of the previous theorem, we can also say $p^* : Map(Y, \mathbb{A}^1 \to Map(X, \mathbb{A}^1)$.

Next, we prove that there is a one-to-one correspondence between p and p^*:

Theorem 29. *Let* $V \subset \mathbb{A}^n$ *and* $W \subset \mathbb{A}^m$ *be affine varieties. There exists a natural 1-1 correspondence between* $Map(V, W)$ *and* $Mor_k(O(W), O(V))$.

Proof. Define p and p^* as in the definition of pullbacks. We claim that the map $p \to p^*$ is injective.

Let $s, s' \in Map(V, W)$ with $s = (f_1, ..., f_m)$ and $s' = (f'_1, ..., f'_m)$. We want to show that if $s^* = s'^*$ i.e $s^*(f) = s'^*(f)$ for all $f \in O(W)$, then $s = s'$. To see this, note that $f_i = x_i \circ s = s^*(x_1) = s'^*(x_i) = x_i \circ s' = f'_i$. Given $f_i = f'_i$ for all $i = 1, ..., m$, therefore $s = s'$.

Now we claim that the map $p \to p^*$ is surjective. Let $\lambda \in Mor_k(O(W), O(V))$. We construct a map $s \in Map(V, W)$ such that $\lambda = s^*$.

Let $f_i \in k[x_1, ..., x_n]$ such that $\lambda(y_i) = f_i$ for $i = 1, ..., m$. Deine $s : \mathbb{A}^n \to \mathbb{A}^m$ such that $s(a_1, ..., a_n) = (f_1(a_1, ..., a_n), ..., f_m(a_1, ..., a_n))$. Now, if $g \in I(W)$, then $g(f_1, ..., f_m) = g(\lambda(y_1), ..., \lambda(y_m)) = \lambda g(y_1, ..., y_m) = 0$, where we got the last inequality by noting that $g \in I(W)$ so it is 0 in O(W) and λ is a homomorphism so it must send 0s to 0s. Note that for any $g \in k[y_1, ..., y_m]$, $\lambda(g) = g(f_1, ..., f_m)$; to see this, write $g(y_1, ..., y_m) = \sum_i c_i y_1^{i_1} \cdots y_m^{i_m}$, so $\lambda(g(y_1, ..., y_m)) = \lambda(\sum_i c_i y_1^{i_1} \cdots y_m^{i_m}) = \sum_i \lambda(c_i y_1^{i_1} \cdots y_m^{i_m}) = \lambda(c_i)\lambda(y_1^{i_1} \cdots y_m^{i_m}) =$
$\sum_i c_i \lambda(y_1^{i_1} \cdots y_m^{i_m}) = g(f_1, ..., f_m)$

This means, for any $a = (a_1, ..., a_n) \in V$, $g(s(a)) = g(f_1(a), ..., f_m(a)) = 0$. Therefore, all $g \in I(W)$ vanish on $s(a), a \in V$. So, $s(a) \in W, \forall a \in V$. This means s restricted to V is a polynomial map i.e $s|_V \in Map(V, W)$.

Note that $\lambda = s^*$ on $y_1, ..., y_m$ because if $s = (f_1, ..., f_m)$, then $s^*(y_i) = y_i \circ s = y_i \circ (f_1, ..., f_m) = y_i \circ (\lambda(y_1), ..., \lambda(y_m)) = \lambda(y_i)$. Since they agree on $y_1, ..., y_m$, they agree on all of O(W). $\square$

Now, we can naturally discover the notion of tensor products by considering the product of varieties:

Theorem 30. *Let* k *be any field. Let* X, Y *be two affine varieties. Then, the coordinate ring of* $X \times Y$ *is* $O(X \times Y) = O(X) \otimes_k O(Y)$*.*

Proof. Let $X \subset \mathbb{A}^n$. Let $Y \subset \mathbb{A}^m$. Let $X = V(I_1), Y = V(I_2)$. Let $I_1 = I(X)$ and $I_2 = I(X)$ (ignoring the radicals for ease of notation). We claim $I(X \times Y) = I(X) \otimes_k k[y_1, ..., y_m] + k[x_1, ..., x_n] \otimes I(Y)$. We prove this as follows:

Let $f \in I(X \times Y), f = \sum_{i=1}^t f_i \otimes g_i$, where $f_i \in k[x_1, ..., x_n], g_i \in k[y_1, ..., y_m]$. Then, for any $(x, y) \in X \times Y$, $\sum_{i=1}^t f_i \otimes g_i(x, y) = \sum_{i=1}^t f_i(x)g_i(y) = 0$. We do induction on t. If $t = 1$, then, $f(x)g(y) = 0$ so either $f_1 \in I(X)$ or $g_1 \in I(Y)$. Now for general t, if $g_j(y) = 0$ for all $y \in Y$ and j, then, $f \in k[x_1, ..., x_n] \otimes_k I(Y)$. Otherwise, we may fine $y_0 \in Y$ and j such that $g_j(y_0) \neq 0$. Then, $f_j(x) = \frac{-\sum_{i \neq j} f_i(x)g_i(y_0)}{g_j(y_0)}, \forall x \in X$. Therefore, $f_j - \frac{-\sum_{i \neq j} f_i g_i(y_0)}{g_j(y_0)} \in I(X) \otimes_k k[y_1, ..., y_m]$ (by inductive hypothesis) and so $f = \sum_{i \neq j} f_i g_i' + I(X) \otimes_k k[y_1, ..., y_m]$. By inducive hypothesis, $\sum_{i \neq j} f_i g_j' \in I(X) \otimes_k k[y_1, .., y_m] + k[x_1, .., x_n] \otimes_k I(Y)$, so $f \in I(X) \otimes_k k[y_1, .., y_m] + k[x_1, .., x_n] \otimes_k I(Y)$. This completes the proof of the claim.

Now, we have $O(X \times Y) = k[x_1, ..., x_n] \times_k k[y_1, ..., y_m]/(I(X) \otimes_k k[y_1, .., y_m] + k[x_1, .., x_n] \otimes_k I(Y)) = O(X) \otimes_k O(Y)$. □

Definition 19. *Kernel ideal. For a* k*-algebra homomorphism* $\phi : R \to S$*, the ideal* $\ker(\phi) = \{x \in R : phi(x) = 0\}$ *is called the kernel ideal.*

Definition 20. m_a*. Given* $a = (a_1, ..., a_n)$*,*

$$m_a = (x_1 - a_1, ..., x_n - a_n)$$

.

One can check that m_a *is the kernel of the* k*-algebra homomorphism* $\psi : k[x_1, ..., x_n] \to k$ *such that* $\psi(x_i) = a_i$*.*

Therefore, $m_a = I(\{a_1, ..., a_n\})$*.*

Theorem 31. *For* $I \subset k[x_1, \cdots, x_n]$*, the vanishing ideal* $I(V(I))$ *is given by the intersection of all kernels of* k*-algebra homorphisms* $k[x_1, \cdots, x_n] \to k$ *such that* I *is mapped to 0 i.e*

$$I(V(I)) = \cap_{a \in V(I)} m_a$$

Proof. This is pretty straightforward. Suppose $f \in I(V(I))$. Then, $f(a) = 0, \forall a \in V(I)$. Therefore, $f \in m_a, \forall a \in V(I)$. Therefore, $f \in \cap_{a \in V(I)} m_a$. On the other hand, suppose $f \in \cap_{a \in V(I)} m_a$. Then, $f(a) = 0$ for all $a \in V(I)$. So, $f \in I(V(I))$. □

Corollary 32. *A finitely generated* k*-algebra* R *is the coordinate ring of an affine variety if and only if for all* $f \neq 0$, $f \in R$, *there exists a* k*-algebra homomorphism* $\phi : R \to k$ *such that* $\phi(f) \neq 0$.

Proof. Suppose R is the coordinate ring of an affine variety, i.e $R = O(X)$. Let $X := V(I)$. Then, $I(X) = I(V(I)) = \cap_{a \in V(I)} m_a$. Now, if $f \neq 0$ in $R = O(X)$, then $f \notin I(V(I))$ implying $f \notin m_a$ for some $a \in V(I)$. Therefore, there exists some k-algebra homomorphism $\psi : k[x_1, ..., x_n] \to k$ such that $\psi(x_i) = a_i$ and $\psi(f) \neq 0$.

Conversely, suppose for any $f \neq 0$, $f \in R$, there exists a k-algebra homomorphism $\psi : R \to k$ such that $\psi(f) \neq 0$.

Now, suppose $f \neq 0$. Then, $f \notin m_a$ for some $a \in V := V(I)$. So, $f \in m_a$ for all $a \in V = V(I)$ implies $f = 0$. So, $f \in I(V(I))$ implies $f = 0$. Therefore, $I(V(I)) = \{0\}$ and we can write $R = O(V)$ i.e a coordinate ring of the affine variety V. □

With these results, we can redefine coordinate ring: a finitely generated k-algebra R is a coordinate ring if for any $f \neq 0$, $f \in R$, there exists a k-algebra homomorphism $\psi : R \to k$ such that $\psi(f) \neq 0$.

Theorem 33. *Let* $p : V \to W$ *be a morphism between 2 varieties where* $p = (p_1, ..., p_m)$. *Let* $w \in W$ *be a point with the vanishing ideal* $m_w = (x - w_1, ..., x - w_m) \subset I(W)$, *then the fiber* $p^{-1}(w) \subset V$ *is defined by* $p^*(m_w) = (p_1(x) - w_1, ..., p_m(x) - w_m) \subset O(V)$.

We can now define three abstract structures that are ubiquitous in algebraic geometry:

Definition 21. *Maximal space MSpec*(R). *For* R *a coordinate ring, the maximal space MSpec*(R) *of* R *is the set of* k*-algebra homomorphisms* $p : R \to k$ *which we call points. For* $f \in R$, *we say* f *vanishes at point* p *if* $p(f) = 0$.

Let's make this more clear. Let $R = k[x_1, ..., x_n]/I(X)$. Let $\varphi : R \to k$ be a k-algebra homomorphism where I is the kernel. Then, we can visualize φ as:

$$\begin{tikzcd}
k[x_1, \ldots, x_n] \arrow[r] \arrow[dr] & k[x_1, \ldots, x_n]/I \arrow[d, "\varphi \in \mathrm{MSpec}(k[x_1, .., x_n]/I)"] \\
& k
\end{tikzcd}$$

With this in mind, we note that we can associate an element of $\mathrm{MSpec}(k[x_1, ..., x_n]/I)$ with a point in $(a_1, \cdots, a_n) \in X$ in k. This is because $\varphi(f_i) = 0, \forall f_i \in I$, so $x_i \to a_i \in k$ and since x_i generate all of the quotient ring, therefore, we can send all polynomials to k.

Therefore, we will often write:

$$\text{MSpec}(k[x_1, ..., x_n]/(f_1, .., f_m)) = \{(a_1, ..., a_n) \in \mathbb{A}^n : f_i(a_1, .., a_n) = 0, \forall i = 1, .., r\}$$

We can turn MSpec(R) into a topological space by letting the basic closed sets be $V_{\text{MSpec}(R)}(f) = \{p \in \text{Mspec}(R) : p(f) = 0\}$.

Definition 22. *Abstract affine variety and ring of functions. A pair* (V, R) *is an abstract affine variety if* R *is a coordinate ring and* V *is identified with the topological space MSpec*(R).

We often just write V *instead of* (V, R). *We call* R *the ring of functions on* V.

Here's an intuition for why abstract affine varieties are required. We want to study polynomials in $R = O(X) = k[x_1, \cdots, x_n]$. We can move to the geometric world by studying the affine variety of a polynomial in R. Given a polynomial, we can fully determine the set of zeros and therefore attain the variety. But given a just variety in the geometric world which is just a set of elements in $\mathbb{A}^n$, we cannot hope to recover $R = O(X)$. Therefore, in an almost silly manner, we remember the data by just letting the abstract affine variety be (V, R).

Definition 23. *Morphism of abstract varieties. For* (V, R) *and* (W, S) *abstract varieties, the morphism of* (V, R) *and* (W, S) *is a* k*-algebra homomorphism* $\psi^* : W \to V$ *with the induced map* $\psi : V = \mathit{MSpec}(R) \to W = \mathit{MSpec}(S)$.

Theorem 34. *(Rabinowitch Trick) The solutions* $(a_1, ..., a_n)$ *to* $f_1 = f_2 = \cdots = f_n = 0$ *and* $f \neq 0$ *are in bijection with the solutions* $(a_1, \cdots, a_n, a_{n+1})$ *to* $f_1 = f_2 = \cdots = f_n = 0$ *and* $x_{n+1}f(x_1, \cdots, x_n) - 1 = 0$.

Proof. The bijections take $a_1, \cdots, a_n$ to $a_1, ...a_n, \frac{1}{f(a_1,...,a_n)}$ and (reverse) $a_1, ...a_n, a_{n+1}$ to $a_1, ...a_n$. □

Now, we define something central to a lot of the techniques.

Definition 24. *Localization of ring* R *at element* $g \in R$. *We define*

$$R_g := R[x]/(xg - 1).$$

Because $xg - 1 = 0$ *in* R_g, *we refer to* x *as* g^{-1} *(here* g *is a unit).*

Since $x = g^{-1}$ in R_g, therefore, we will often write R_g as $R[g^{-1}]$. Localization is very useful; for example, one can notice that we had used localization in the proof of Hilbert's

Nullstellensatz (although we used it as an arbitrary "trick" without really looking deep into the construction).

Here are some immediate properties of the localization of a ring at an element.

Lemma 35. *For any ring* R*, we have:*
(a) Every element of R_g *can be written as* rg^{-i} *for some* $r \in R$ *and* $i \geq 0$*.*
(b) $rg^{-i} = sg^{-i} \in R_g$ *if and only if* $g^N(r - s) = 0 \in R_g$ *for some* N*.*
(c) A ring map $R_g \to S$ *is the same as a ring map* $R \to S$ *such that* $\mathrm{Im}(g) \in S^\times$ *i.e* g *is mapped to a unit in* S*. In other words,*

$$\mathrm{Mor}(R_g, S) = \{\varphi \in \mathrm{Mor}(R, S) : \varphi(g) \in S^\times\}$$

(d) The map $R \to R_g$ *is an isomorphism exactly when* $g \in R^\times$*.*

Proof. (a) Suppose $s \in R_g$. Then, $s = f(x)$. Given f is a polynomial, for i large enough, sg^i not have any x (since $x = g^{-1}$), so $sg^i = r \in R$. This implies the result.
(b) Suppose $g^N(r - s) = 0$. Then, since g is a unit, this implies $r - s = 0$, so $r = s$ and $rg^{-i} = sg^{-i}$. Conversely, suppose $rg^{-i} = sg^{-i}$. Then, $(r - s)g^{-i} = 0$. Since we are operating in R_g, this implies $(r - s)g^{-i} = (1 - xg)(a_0 + a_1x + \cdots + a_nx^n)$. Expanding the right hand side and comparing the coefficients of $x^0, x^1, \cdots, x^n$, we see that $a_0 = r-s$, $a_1 = (r-s)g$ and $a_n = (r - s)g^n$. Now, comparing the coefficient of x^{n+1}, we get that $a_ng = 0 \implies (r - s)g^{n+1} = 0$. // (c) A ring map $\psi : R_g \to S$ is the same as a map $\phi : R \to S$ such that ϕ sends $(xg - 1)$ to 0. But then, $\phi(x)\phi(g) - \phi(1) = 0$, so $\phi(x) = \phi(g)^{-1} = \phi(g^{-1})$. Therefore, g has to be a unit. If g is not a unit, these maps cannot be equivalent.
(d) If g is a unit, then $R[x]/(xg - 1) = R[x](x - g^{-1}) = R$. Conversely, if g is not a unit, then R is not isomorphic to R_g. □

Now, we get the following result:

Theorem 36. *If* $V \subset \mathbb{A}^n$ *is a variety with cooridnate ring* R*, then,* $\{(v, f(v)^{-1}) : v \in V, f(v) \neq 0\} \subset \mathbb{A}_k^{n+1}$ *is a variety with coordiante ring* R_f *and isomorphic to* $D(f) \subseteq \mathbb{A}^n$*.*

Proof. First, we prove that for $R = O(V)$, R_f is a coordinate ring. Given R is the quotient of a polynomial ring, it is a finitely generated algebra. Now, using corollary 22, R_f is a coordinate ring if and only if for all $g \in R_f$, $g \neq 0$, there exists a k-algebra homomorphism $q : R_f \to k$ such that $q(g) \neq 0$. Let $g = hf^{-i}$ for $i \geq 0$, $h \in R$, $g \neq 0$ in R_f. Then, $hf \neq 0$, since otherwise $g = 0$. Now, we know there exists a k-algebra homomorphism $p : R := O(v) \to k$ such that $p(hf) = p(h)p(f) \neq 0$. As $p(f) \neq 0$, therefore, we get a map from $R_f \to k$ such that $p(g) \neq 0$. Therefore, R_f is a coordinate ring.

Furthermore, $\mathrm{MSpec}(R_f) = D(f)$. To see this, suppose $V = (f_1, ..., f_m)$, so $R_f = (k[x_1, ..., x_n]/(f_1, ..., f_m))_f = (k[x_1, ..., x_n]/(f_1, ..., f_m))[f^{-1}]$. Therefore, $\mathrm{MSpec}(R_f)$ is associated with points such that $(f_1, ..., f_m)$ are 0 but $1/f(x_1, ..., x_n)$ is not 0. This is the same as $D(f)_V$. Furthermore, $D(f)$ can be considered an affine variety too by considering it as $V(f_1, ..., f_m, xf - 1)$. □

Using the language of localization, we can also determine what ideals are radical which is important in light of Hilbert's Nullstellensatz:

Theorem 37. $I \subset R$ *is radical if and only if* R/I *is reduced if and only if* $(R/I)_f = 0$ *implies* $f = 0$

We define a few more important objects.

Definition 25. R *is a Jacobson ring, if every radical ideal* I *is the intersection of these maximal ideals containing it.*

Definition 26. *A quasi-affine variety is an open subset of an affine variety.*

As we close this section, we note that we now have a better understanding of what closed and open subsets are in Zariski topology:
Suppose k is an algebraically closed field and $V \subset \mathbb{A}^n$ is an irreducible affine variety. Then, let $R := O(V)$ be our coordinate ring. Given $I \subset R$ is an ideal, $V(I)$ is a variety, $V(I) \cap V$ is a closed subset and with $V(I)$, we can associate the coordinate ring $R/I(V(I))$.
On the other hand, let $g \in R$, then $D(g) \subset V$ is a basic open set and with it, we can associate the coordinate ring R_g in $k[x_1, ..., x_n][1/g] = k[x_1, ..., x_n, x_{n+1}]/(x_{n+1} - \frac{1}{f(x_1,...,x_n)}) = O(V(x_{n+1} - \frac{1}{f(x_1,...,x_n)}))$. Later on, we will see that we can study algebraic geometry of open subsets too using sheaves.

8 Dimensions

We need a notion of dimension on topological spaces which we can hope to use on Zariski topology. We have some expectations. We would want $\mathbb{A}^n$ to be of dimension n. If X_1 and X_2 are closed, then $\dim(X_1) \cap \dim(X_2) = \dim(X_1) + \dim(X_2)$. Dimension should be such that it can be understood locally through local rings or fractional fields. Given Y_1, Y_2 are closed subvarieties of X, we expect $\dim(Y_1 \cap Y_2) = \dim(Y_1) + \dim(Y_2) - \dim(X)$. For $f \in O(X)$, then $\dim(V(f)) = \dim(X) - 1$ for general f.

For motivation, we look at linear algebra. For a vector space V, we can define $\dim(V) = \max\{k : \exists V_0 \subsetneq V_1 \subsetneq \cdots \subsetneq V_k,$ linear subspaces of $V\}$.

We can use the same idea to define dimension for topological spaces.

Definition 27. *Krull dimension. Given* X *is a topological space. Then,*

$$dim(X) = \max\{k : \exists X_0 \subsetneq X_1 \subsetneq \cdots \subsetneq X_k \subsetneq X, X_i \textit{ irreducible closed subsets in } X\}.$$

We set $dim(\emptyset) = 0$.

With this, we notice that $\dim(\mathbb{A}^1) = 1$ since the irreducible closed subsets are $\emptyset$, finite subsets, $\mathbb{A}^1$.

Definition 28. *Equi-dimensional. A topological space* X *is equidimensional of dimension* n*, if any irreducible component of* X *has the same dimension* n*.*

With this definition of dimension, we get the following:

Proposition 38. *If* $X \subseteq Y$ *are closed, then* $dim(X) \leq dim(Y)$*.*

Proposition 39. *If* X *is an affine variety, then* $dim(X) = 0$ *if and only if* X *is finite.*

Proof. Write X as the union of irreducible components : $X = \cup_{i=1}^n X_i$. Then suppose $\dim(X) = 0$. Then, choose $x \in X_i$. Now, given $\dim(X) = 0$, $X_i = \{x_i\}$ and so X is the union of finitely many points. Conversely, if X is finite, then the topology is discrete and so any subset is closed. The irreducible closed subsets are points so $\dim(X) = 0$. □

We call 1 dimensional varieties algebraic curves. We call 2 dimensional varieties algebraic surfaces.

Definition 29. *Krull dimension of a ring* R*. Let* R *be any ring. The Krull dimension* $dim(R)$ *is the maximal length of strict chains of prime ideals of* R*.*

Definition 30. *Catenary Rings. A ring* R *is catenary if for any prime ideals* $p \subseteq q$ *of* R*, any maximal chain* $p = p_0 \subseteq p_1 \subseteq \cdots \subseteq p_e = q$ *has the same length* $e = e(p, q)$.

Theorem 40. *Let* k *be a field. Any finitely generated* k*-algebra* R *is catenary.*

Corollary 41. *For an irreducible algebraic variety* X*, the dimension of* X *can be computed by the length of any maximal strictly increasing chain of irreducible closed subsets.*

Example: $\dim \mathbb{A}^n = n$ since we have a strictly increasing chain $0 \subsetneq \mathbb{A}^1 \subsetneq \cdots \subsetneq \mathbb{A}^n$.

Corollary 42. *If* $V_i \subset \cdots \subset V_j$ *is a maximal chain of irreducible subvarieties of* X*, then* $dim V_{i+k} = dim V_i + k$.

Now, we define the following:

Definition 31. *Algebraically independent and algebraic over. Let* L/k *be a field extension (i.e* k *is a subfield of* L*). Then,* $\alpha \in L$ *is algebraically independent over* k *if* $f \in k[x]$ *such that* $f(a) = 0$ *implies* $f = 0$*. Otherwise,* a *is algebraic over* k.

Definition 32. *Transcendental degree.*

$$\mathrm{trdeg}(L/k) := \max\{r : \exists a_1, ..., a_r \textit{ algebraically independent over } k\}$$

With this, we have the following:

Theorem 43. *Let* X *be an irreducible affine variety over* k*. Then,*

$$\dim(X) = \mathrm{trdeg}(k(x)/k).$$

In other words, the dimension of an affine variety is the largest dimension of any irreducible component.

Corollary 44.

$$\dim(\mathbb{A}^n) = \mathrm{trdeg}(k(x_1, ..., x_n)/k) = n.$$

Corollary 45. $f : X \to Y$ *is a finite and surjective morphism between two affine varieties, then* $\dim(X) = \dim(Y)$.

Recall: $f : X \to Y$ and $y \in Y$. Then, $f^{-1}(y)$ is the fiber of y.

Definition 33. *Quasi-finite. Let* $f : X \to Y$ *be a polynomial map between two affine varieties. Then,* f *is quasi-finite if the number of elements in the fiber over* $y \in Y$ *is finite for any* $y \in Y$.

Theorem 46. *Krull's Principle Ideal Theorem. If the affine variety* V *is irreducible and* $0 \neq f \in O(V)$ *is not a unit, then all irreducible components* V_i *of* $V(f)$ *have dimension* $\dim(V) - 1$.

9 Sheaves

(Most of this section is from Ravi Vakil's "Rising Sea: Foundations of Algebraic Geometry".

So far, we have studied morphisms from an affine variety X to another affine variety Y. Now consider any *open* subset U of X. Now, given a polynomial map $f \in \mathrm{Map}(X, Y)$, we would like to localize f i.e $f|_U \in \mathrm{Map}(X, Y)$ where U is an open subset of the affine variety X. The problem is that U is not affine. However, we know that U is locally covered by affine varieties, by the local nature of algebraic geometry introduced in the section on Zariski topology. With this, we can define $\mathrm{Map}(U, \mathbb{A}^1)$ as:

$$\{p_{D(f)} \in \bigcup_{D(f)\subseteq U, f\in O(X)} \mathrm{Map}(D(f), \mathbb{A}^1) : \forall D(f), D(g) \subseteq U, p_{D(f)}|_{D(f)\cap D(g)} = p_{D(g)}|_{D(f)\cap D(g)}.\}$$

Recall that D(f) is isomorphic to $\{(v, f(v)^{-1} : v \in X, f(v) \neq 0\}$ and has the coordinate ring $R_f = k[x_1, ..., x_n][1/f]$. Note that if $U = D(f)$ is an affine variety, then our definition agrees with what we already know. We saw in the section on coordinate rings that $O(X) \cong \mathrm{Map}(X, \mathbb{A}^1)$, so $O(U) \cong \mathrm{Map}(U, \mathbb{A}^1)$.

We define sheaves in a similar way. While this is abstract, there are a few examples to keep in mind. In differential topology, for any manifold X, we define an atlas and then we define smooth functions on X using the atlas. Considering $X = \mathbb{R}^n$, here is a more straightforward example - consider smooth functions on $\mathbb{R}^n$. Then, the sheaf of smooth functions on X is the data of all smooth functions on open subsets of X. Let U be an open subset of X - then the ring of smooth functions on U is denoted by $\mathscr{O}(U)$. Given $V \subset U$, we can restrict smooth functions on U to V by $\mathrm{res}_{U,V} : \mathscr{O}(U) \to \mathscr{O}(V)$. These restrictions commute i.e if we have $W \subset V \subset U$, we could first restrict a function in $\mathscr{O}(U)$ to V and then restrict that to W but this would be equivalent to directly restriction the function in $\mathscr{O}(U)$ to W.

Now, if we want to do algebraic geometry on a general (possibly open subset) U, we need to remember all the coordinate rings $\mathrm{Map}(D(f), \mathbb{A}^1)$.

Although sheaves can defined using any category, we will define it using sets or rings.

First, we define the germ of a smooth function:

Definition 34. ***Germ of a smooth function at*** $p \in X$. *Germs are objects of the form* (f, *open set* U) *such that* $p \in U, f \in \mathscr{O}(U)$ *with the equivalence* $(f, U) \sim (g, V)$ *if there exists an open set* $W \subset U$, $W \subset V$ *and* $p \in W$ *such that* $f|_W = g|_W$ *i.e* $\mathrm{res}_{U,W} f = \mathrm{res}_{V,W} g$. *Therefore, two germs are* *equivalent as long as they agree on some open neighbourhood of* p *(even though they might disagree elsewhere).*

The set of germs is called the ***stalk*** *at* p*, denoted by* $\mathscr{O}_p$*.*

The stalk is a ring. One can add two germs and get another germ in the stalk: if f is defined on U and g is defined on V, then $f+g$ is defined on $U \cap V$. Also, $f+g$ is well-defined: if $\tilde{f}$ has the same germ as f (i.e f and $\tilde{f}$ agree on some open neighbourhood W of p) and $\tilde{g}$ has the same germ as g (i.e g and $\tilde{g}$ agree on some open neighbourhood W' of p), then $\tilde{f}+\tilde{g}$ agrees with $f+g$ on $U \cap V \cap W \cap W'$.

Furthermore, for $p \in U$, there is a natural map $\mathscr{O}(U) \to \mathscr{O}_p$.

Lastly, $\mathscr{O}_p$ is a ring itself. Let $m_p \subset \mathscr{O}_p$ be the set of germs that vanish at p. These germs form an ideal since m_p is closed under addition and multiplying any element in m_p by any function, the rest is also in m_p. This is also a maximal ideal since the quotient ring is a field.

Definition 35. ***Presheaf****. A presheaf of sets,* $\mathscr{F}$*, on a topological space* X *is the following data:*

(1) For each open set U *in* X*, we have* $\mathscr{F}(U)$ *(alternative notations include* $\mathscr{F}(U) = H^0(U, \mathscr{F}) = \Gamma(U, \mathscr{F})$ *where* $\mathscr{F}(U)$ *is called the* ***sections or functions over*** U*. When* U *is ommitted, we assume we are talking about* X *i.e* $\mathscr{F}$ *contains sections/functions over* X *which are often called the global sections.*

(2) For each inclusion $U \subseteq V$*, we have the* ***restriction*** *map:*

$$\mathrm{res}_{V,U} : \mathscr{F}(V) \to \mathscr{F}(U).$$

Given $f \in \mathscr{F}(V)$*, we write* $f|_U = \mathrm{res}_{V,U}(f)$*.*

We also require two more conditions:
(3) The map $\mathrm{res}_{U,U}$ *is the identity (as one would expect)* $\mathrm{res}_{U,U} = \mathrm{id}_{\mathscr{F}(U)}$

(4) If $U \subseteq V \subseteq W$ *are inclusions of open sets, then restrictions commute as the following diagram shows:*

$$\begin{tikzcd}
\mathcal{F}(U) \arrow[r, "\mathrm{res}_{U,V}"] \arrow[dr, "\mathrm{res}_{U,W}"'] & \mathcal{F}(V) \arrow[d, "\mathrm{res}_{V,W}"] \\
 & \mathcal{F}(W)
\end{tikzcd}$$

With the notion of a presheaf, we can now generalize our notion of germs and stalks:

Germs and stalks of presheaf: Let $\mathscr{F}$ be our presheaf. Then, each germ at p is a section over some open set containing p such that two sections are equivalent if they agree on some smaller open neighbourhood of p. Then, the stalk of a presheaf $\mathscr{F}$ at a point p is the set of germs at p and is denoted by $\mathscr{F}_p$ i.e

$$\mathscr{F}_p := \{(f, \text{ open set } U) : p \in U, f \in \mathscr{F}(U)\}$$

with the relation $(f, U) \sim (g, V)$ if $\exists W \subset U, W \subset V, p \in W$ such that $res_{U,W} f = res_{V,W} g$.

Now we finally define sheaf:

Definition 36. ***Sheaf.*** *A presheaf $\mathscr{F}$ is a sheaf if it satisfies two more axioms:*

Identity/injectivity axiom. *For any open set U, if $\{U_i\}_{i \in I}$ is an open cover of U and $f_1, f_2 \in \mathscr{F}(U)$ with $f_1 |_{U_i} = f_2 |_{U_i}$ for all $i \in I$, then $f_1 = f_2$.*

Gluability axiom. *If $\{U_i\}_{i \in I}$ is an open cover of U, then given $f_i \in \mathscr{F}(U_i)$ for all i such that $f_i |_{U_i \cap U_j} = f_j |_{U_i \cap U_j}$ for all $i, j \in I$, then there exists some $f \in \mathscr{F}(U)$ such that $res_{U,U_i} f = f_i$ for all i.*

We first look at a few important sheaves.

Sheaf of functions $\mathscr{O}$ on $X = \mathrm{MSpec}(R)$. (Recall: given R is an k-algebra (and integral domain), $X = \mathrm{MSpec}(R)$ is the set of all homomorphisms from R to k.) The sheaf of functions $\mathscr{O}$ on $X = \mathrm{MSpec}(R)$ has sections $\mathscr{O}(U) \subset \mathrm{Frac}(R)$ where $f \in \mathscr{O}(U)$ if for any $p \in U$, we can write $f = \frac{g}{h}, g, h \in R$ and $h(p) \neq 0$.

Proposition 47. *If R is an integral domain, then $\mathscr{O}(X = \mathrm{MSpec}(R)) = R$.*

Proof. If $f \in R$, then $f = f/1 \in \mathscr{O}(X)$ and we know $1 \in R$ does not vanish on any point of X. So $R \subset \mathscr{O}(X)$. Now, conversely, suppose $f \in \mathscr{O}(X) \subset \mathrm{Frac}(R)$. We want to show $f \in R$. Define the ideal of denominators of f to be $I := \{r \in R : rh \in R\} \subset R$. Now given $f \in \mathscr{O}(X)$, near any p, there exists some $h \in I$ where $h(p) \neq 0$ and $f = \frac{g}{h}$. This implies $V(I) = \emptyset$. By Hilbert's Nullstellensatz, this means $I = R$ and so $I = (1)$, implying $f = f/1 \in R$. □

Proposition 48. *Let $S = k[x_1, ..., x_n]/I(V)$. Recall that we can write $\mathrm{MSpec}(S)$ as $V \subset \mathbb{A}^n$. Then, consider any open set $U \subset \mathrm{MSpec}(S)$ (or $U \subset V$) where $U = D(f_1, ..., f_n)$. Then, $U = \cup_i D(f_i)$. Furthermore, $D(f) \cup D(g) = D(fg)$.*

The proof of this is straightforward.

Proposition 49. *Let* R *be an integral domain with* $z \in R$*. Then,*

$$\mathscr{O}(D(z)) = R_z = \{\frac{1}{z^n} f : n \in \mathbb{Z}_{\geq 0}, f \in R\}$$

Proof. Suppose $f \in \mathrm{Frac}(R)$ with $f \in \mathscr{O}(D(z))$. We want to show that $f \in R_z$. Let $I \subset R$ be the ideal of denominators of f i.e elements $r \in R$ with $rh \in R$. Then, near any point $p \notin V(z)$, we can write $f = \frac{g}{h}, h(p) \neq 0$. Therefore, $p \notin V(I)$. Thus, $V(I) \subset V(z)$. We know $z \in I(V(I)) \implies z \in \sqrt{I}$ (by Nullstellensatz) $\implies z^k \in I, k \in \mathbb{Z}^+$. □

Now, we go back to the question of studying algebraic geometry on not just closed subsets (i.e affine varieties) but also open subsets. We come to an important sheaf:

Proposition 50. *Let* k *be an algebraically closed field and let* R *be a finitely generated* k*-algebra with* $f \in R$*. Then, the sheaf over* D(f) *is given by*

$$\mathscr{O}(D(f)) = R_f = R[x]/(xf - 1) = \{\frac{a}{f^n} : n \in \mathbb{Z}^{\geq 0}, a \in R\}.$$

Proof. Given $a/f^N \in R_f$, we get a global section over D(f) i.e for
$m \in D(f)$, $m \to (a \bmod m)/(f^N \bmod m) \in R/m$. This is k-valued: R/m is finitely-generated k-algebra that is a field, it is therefore a field extension of k and since k is algebraically closed, $R/m = k$. Conversely, suppose $t \in \mathscr{O}(D(f))$ is a global section. This function can be locally written as $f = g/h$ where $h \neq 0$. Then, for any $p \in D(f)$, we first fix a local neighbourhood V on which t can be written in this form. Since we can form an open cover of $D(f) = \mathrm{MSpec}(R_f)$ using basic open sets, let the basic open sets be of the form $D(h_i) =: V_i$ i.e $D(f) = \cup_i D(h_i)$. Then, $t|_{V_i} = \frac{g_i}{h_i^{n_i}}$ where $h_i \neq 0, n_i \geq 0$.

We also require gluability (which we will show in reverse i.e we will find a that ensures this property) i.e if $t|_{V_i} = t|_{V_j}$, then for large enough N, $(g_i h_j^{n_j} - g_j h_i^{n_i})(h_i h_j)^N = 0$ on $D(h_i) \cap D(h_j) = D(h_i h_j)$. Replace g_i with $g_i h_i^N$ and h_i with h_i^{N+1}. Then, we get $g_i h_j - g_j h_i = 0$ for all i, j. Now, we know $f \in \sqrt{(f)} = \sqrt{(h_1, ..., h_n)}$ (by Nullstellensatz) so $f^N = c_1 h_1 + \cdots + c_n h_n$ for some $N \geq 0$ and $c_i \in R$. Let

$$a = c_1 g_1 + \cdots + c_n g_n.$$

Then, $a h_i = \sum_j c_j g_j h_i = \sum_j c_j g_i h_j = f^N g_i$. Therefore, $a/f^N = g_i/h_i$ on $D(h_i) \subset D(f)$ □

10 References

1. William Fulton. *Algebraic Curves. An Introduction to Algebraic Geometry*. 2008.

2. Dummit and Foote. *Abstract Algebra, 3rd Ed.*

3. Ravi Vakil. *Math 216 Lectures at Stanford University.*

4. Zhiyu Zhang. *Math 145 Lectures at Stanford University.*

5. Ravi Vakil. *The Rising Sea: Foundations of Algebraic Geometry*

6. Ravi Vakil. *Math 145 Lectures at Stanford University.*

A Category Theory

These introductory category theory notes are all taken, almost verbatim, from Ravi Vakil's textbook [5] - which I find to be arguably one of the best texts in any field of mathematics today.

A.1 Basic terminology

These notes are directly taken from (5).

Definition: Category. A **category** consists of a collection of **objects** and for each pair of objects, a set of **morphisms** or **arrows** between them (which are often called **maps**). The collection of objects of a category, $\mathscr{C}$, is denoted as obj($\mathscr{C}$) but we will often denote this also by $\mathscr{C}$. If $A, B \in \mathscr{C}$, the set of morphisms from A to B are denoted by **Mor**(A, B) where a morphism is often written as $f : A \to B$. A is the **source** of f whereas B is the **target** of f.

Morphisms compose as expected; $\mathrm{Mor}(B, C) \times \mathrm{Mor}(A, B) \to \mathrm{Mor}(A, C)$. Composition is associative, i.e $(f \circ g) \circ h = f \circ (g \circ h)$.

For each object $A \in \mathscr{C}$, there exists an **identity morphism** $\mathrm{id}_A : A \to A$ such that $f \circ \mathrm{id}_A = f$ and $\mathrm{id}_A \circ f = f$. Identity morphism is unique.

Definition: Isomorphism. An isomorphism between two objects is a morphism $f : A \to B$ such that there exists a unique morphism $g : B \to A$ such that $f \circ g = \mathrm{id}_B$ and $g \circ f = \mathrm{id}_A$

Definition: Automorphism. The set of invertible elements of $\mathrm{Mor}(A, A)$ forms a group called the **automorphism group of** A.

Examples:
(1) Category of sets. The objects are sets and the morphisms are maps of sets.

(2) Another good example is the category Vec_k of vector spaces over a given field k. The objects are k-vector spaces, and the morphisms are linear transformations.

(3) Category of Abelian groups. The objects are Abelian groups and the morphisms are the group homomorphisms. This category is denoted as Ab.

(4) Category of modules over a ring. If A is a ring, then the A-modules form a category Mod(A)

(5) Category of rings. Objects are rings and morphisms are ring homomorphisms.

Defintion: Subcategory. A subcategory $\mathscr{A}$ of a category $\mathscr{C}$ includes some of the objects and morphisms of $\mathscr{C}$ such that the objects of $\mathscr{A}$ include the sources and targets of morphisms of $\mathscr{A}$ and the morphisms of $\mathscr{A}$ include the identity morphisms of the objects in $\mathscr{A}$ and are preserved by composition.

Now, we define functors.

Definition: Covariant functor from category $\mathscr{A}$ to category $\mathscr{B}$, denoted by $F : \mathscr{A} \to \mathscr{B}$. This is a map of objects $F : \mathrm{obj}(\mathscr{A}) \to \mathrm{obj}(\mathscr{B})$ and for each $A_1, A_2 \in \mathscr{A}$ and morphism $m : A_1 \to A_2$, a morphism $F(m) : F(A_1) \to F(A_2)$. We require F preserves identity morphisms i.e $F(id)_A = id_{F(A)}, \forall A \in \mathscr{A}$. F must also preserve composition i.e $F(m_1 \circ m_2) = F(m_1) \circ F(m_2)$.

To emphasize, a covariant functor has two "functions". One is mapping objects in one category to objects in another one i.e $F : \mathrm{obj}(\mathscr{A}) \to \mathrm{obj}(\mathscr{B})$. The other is mapping morphisms in one category to morphisms in another one by taking the "shadow" of the morphism i.e $F(\cdot) : \mathrm{Mor}(\mathrm{obj}(\mathscr{A}), \mathrm{obj}(\mathscr{A})) \to \mathrm{Mor}(\mathrm{obj}(\mathscr{B}), \mathrm{obj}(\mathscr{B}))$

Example of covariant functor: Trivial example is the identity cofunctor id $: \mathcal{A} \to B$

Forgetful Functor: Consider the functor from the category of vectors space over k i.e Vec_k to the category of sets by sending each vector space to its underlying set. Furthermore, F sends each morphism m in Vec_k to the underlying map of sets. This is a forgetful functor because it forgets additional structure.

Definition: Faithfull and full covariant functors. A covariant functor F from category $\mathscr{A}$ to $\mathscr{B}$ is faithful if for any $A, A' \in \mathscr{A}$, the map $\mathrm{Mor}_{\mathscr{A}}(A, A') \to \mathrm{Mor}_{\mathscr{B}}(F(A), F(A'))$ is injective. It is full if it is surjective. A functor that is both full and faithful is called **fully faithful**.

Defintion: Contravariant functor from category $\mathscr{A}$ to category $\mathscr{B}$, denoted by $F : \mathscr{A} \to \mathscr{B}$. This is a map of objects $F : \mathrm{obj}(\mathscr{A}) \to \mathrm{obj}(\mathscr{B})$ and for each $A_1, A_2 \in \mathscr{A}$ and morphism $m : A_1 \to A_2$, a morphism $F(m) : F(A_2) \to F(A_1)$. We require F preserves identity morphisms i.e $F(\mathrm{id})_A = \mathrm{id}_{F(A)}, \forall A \in \mathscr{A}$. Therefore, $F(m_1 \circ m_2) = F(m_2) \circ F(m_1)$.

Example: Consider the category Vec_k of vector spaces over field k. Then, we can take the duals to define a contravariant functor. Let $f : V \to W$ be a linear transformation. Then, the dual transformation is $f^* : W^* \to V^*$.

Example: Here is a pretty straightforward example of covariant and contravariant functors. Consider a category $\mathscr{C}$ and the category of morphisms between sets $\mathscr{S}$ (note that in this category, each object is a morphism and we have morphisms between morphisms. Then, let $A \in \mathrm{obj}(\mathscr{C})$. We first define a covariant functor :
$h^A : \mathrm{obj}\mathscr{C} \to$ (some morphism between sets in S) and in particular $h^A(B \in \mathrm{obj}(\mathscr{C}) \in \mathrm{Mor}(A, B)$. Furthermore, given $f \in \mathrm{Mor}(B_1, B_2)$ in category $\mathscr{C}$, h^A will send f to a morphism from $\mathrm{Mor}(A, B_1)$ to $\mathrm{Mor}(A, B_2)$ and in particular $h^A(f \in \mathrm{Mor}(B_1, B_2)(g \in \mathrm{Mor}(A, B_1)) = (f \circ g) \in \mathrm{Mor}(A, B_2)$.

Now, we define a contravariant functor. With the same set up i.e $A \in \mathrm{obj}((C))$. Let $B \in \mathrm{obj}(\mathscr{C})$, we have $h_A(B) \in \mathrm{Mor}(B, A)$ (note that the direction has been reversed). Then, $h_A : \mathrm{Mor}(B_1, B_2) \to (\mathrm{Mor}(B_2, A) \to \mathrm{Mor}(B_1, A))$ by the following: $h_A(f \in \mathrm{Mor}(B_1, B_2))(g \in \mathrm{Mor}(B_2, A)) = g \circ f \in \mathrm{Mor}(B_1, A)$

Now, we introduce the concept of a **natural transformation** of covariant functors. Let F be a covariant functor. Then, we consider the transformation $F \to G$ as follows: consider the morphism $m_A : F(A) \to G(A)$ for each $A \in \mathscr{A}$ such that $f : A \to A'$ in $\mathscr{A}$. This has the following diagram:

$$\begin{tikzcd}
F(A) \arrow[r, "F(f)"] \arrow[d, "m_A"'] & F(A') \arrow[d, "m_{A'}"] \\
G(A) \arrow[r, "G(f)"'] & G(A')
\end{tikzcd}$$

A **natural isomorphism** of functors is a natural transformation such that each m_A is an isomorphism. One can analogously define natural transformation of contravariant functors.

Next, we introduce the notion of equivalnce of functors. The data of functors $F : \mathscr{A} \to \mathscr{B}$ and $F' : \mathscr{B} \to \mathscr{A}$ such that $F \circ F'$ is naturally isomorphic to $\mathrm{id}_{\mathscr{B}}$ and $F' \circ F$ is naturally isomorphic to $\mathrm{id}_{\mathscr{A}}$ is the **equivalence of categories**. Two categories are "essentially the same" when there is an equivalence of categories between them.

A.2 Universal properties

Definition: Initial, final and zero objects. An object of a category $\mathscr{C}$ is initial if it has only one map to every object. An object is final if has only one map from every object. An object iz zero if it is both initial and final.

Lemma 51. *Any two initial objects are uniquely isomorphic. Any two final objects are uniquely isomorphic.*

The proof follows from the definition. This also shows that initial and final objects are unique up to isomorphism. The fact an object is an initial or final or zero object is a universal property.

Here are some more examples:

Localization of rings and modules. First, recall: a **multiplicative subset** S of a ring A is a subse that is closed under multiplication and contains 1. Then, define the ring $S^{-1}A$ whose elements are of the form a/s such that $a \in A, s \in S, s \neq 0$ and $a_1/s_1 = a_2/s_2$ if and only if $\exists s \in S, s(s_2a_1 - s_1a_2) = 0$. Lastly, $a_1/s_1 + a_2/s_2 := (s_2a_1 + s_1a_2)/(s_1s_2)$ and $a_1/s_1 \times a_2/s_2 = (a_1a_2)/(s_1s_2)$. Note, if $0 \in S$, then $S^{-1}A$ is the 0-ring. Also, we have the map $A \to S^{-1}A$ by sending each $a \to a/1$.

Now, we look at a few important multiplicative subsets.

The first is $S = \{1, f, f^2, \cdots\}$ where $f \in A$. This is denoted by $A_f := S^{-1}A$. One can prove that this is isomorphic to $A_f \cong A[t]/(tf - 1)$. To prove this, we showed in the section on coordinate rings that all elements in $A[t]/(tf - 1)$ are of the form af^{-i} for some $a \in A, i \geq 0$. On the other hand, all elements in A_f can be trivially sent to the same element in $A[t]/(tf - 1)$.

The second important multiplicative subset is $S = A \backslash p$ where p is a prime ideal. We denote this by $A_p := S^{-1}A$ i.e we divide by elements that are *not* in p.

The third is constructed as follows: given A is an integral domain, $S := A \backslash \{0\}$. Then, $k(A) := S^{-1}(A)$ is called the fractional field of A.

B Ring Theory Revision

All the material here is from Dummit and Foote's "Abstract Algebra". Detailed proofs of the theorems can be found in the text.

Definition: Rings. A ring R is a set with binary operations $\times$ and + such that
(1) $(R, +)$ is an abelian group (i.e has identity, inverses and associativity).
(2) $\times$ is associatve i.e $(a \times b) \times c = a \times (b \times c)$
(3) distributive laws hold in R i.e $\forall a, b, c \in R$, we have $(a + b) \cdot c = a \cdot c + b \cdot c$ and $a \cdot (b + c) = a \cdot b + a \cdot c$.

Note: Rings that are commutative under multiplication are called **commutative rings**.

Example: Ring without identity The set of even integers $2\mathbb{Z}$ since 1 is not even.

Example: Ring of functions. For X a non-empty set and A any ring, the set of functions $f : X \to A$ forms a ring R with operations $(f + g)(x) = f(x) + g(x), (fg)(x) = f(x)g(x)$. R is commutative if and only if A is commutative. R has identity 1 if and only if A has 1.

Example: Some other easy rings. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are all commutative rings. $\mathbb{Z}/n\mathbb{Z}$ is a commutative ring with identity 1.

Example: Trivial and Zero ring. Any abelian group is a trivial ring with the operation $x \cdot y = 0$ for any $x, y \in R$.

Definition: Division Ring. A ring R with identity $1 \neq 0$ such that every $x \in R$ has a multiplicative inverse $x^{-1} \in R$ with $xx^{-1} = x^{-1}x = 1$ is a division ring.

Definition: Field. A field is a commutative division ring.

Proposition: Immediate properties of rings For any ring R:
(1) $0x = x0 = 0, \forall x \in R$
(2) $(-x)y = x(-y) = -(xy), \forall x, y \in R$
(3) $(-x)(-y) = xy, \forall x, y \in R$
(4) if $\exists 1 \in R$, then 1 is unique and $-x = (-1)x, \forall x \in R$.

Definition: Zero divisor. Let R be a ring. Let $x \neq 0$. Then, x is a zero vicisor if $\exists y \in R, y \neq 0$ such that $xy = 0$ or $yx = 0$.

Definition: Unit. Let R be a ring with identity 1. Then, $x \in R$ is called a unit if there exists $y \in R$ such that $xy = yx = 1$. $R^{\times}$ is the set of units in ring R. $(R^{\times}, \times)$ is a group under multiplication called the group of units.

Lemma: If $x \in R$ is a zero divisor then x is not a unit. If $x \in R$ is a unit, then x is not a zero divisor.

Corollary: Fields have no zero divisors.

Example: zero divisor. Let $x \neq 0, x \in \mathbb{Z}$ and suppose x is relatively prime to $n \in \mathbb{Z}$. Then, $\bar{x}$ is a zero divisor in $\mathbb{Z}/n\mathbb{Z}$.

Definition: Integral Domain. A commutative ring with identity $1 \neq 0$ such that it has no zero divisor.

Proposition: Cancellation laws hold in integral domains. Let $a, b, c \in R$ such that a is not a zero divisor. If $ab = ac$, then either $a = 0$ or $b = c$. In other words, if a, b, c are elements in an integral domain, then, $ab = ac \implies a = 0$ or $b = c$.

Proposition: Any finite integral domain is a field.

Definition: Subring. A subring of the ring R is a subgroup of R that is closed under multiplication i.e $S \neq \emptyset$ is closed under addition, for each $x \in S$, there exists an additive inverse in S, $0 \in S$ and S is closed under multiplication.

Definition: Polynomial Rings. Let R be a commutative ring with identity 1. Let x be an indeterminate. Then, R[x] is the ring of polynomials $\sum_{i=1}^{n} a_i x^i, n \geq 0, a_i \in R$. If $a_n \neq 0$, degree of the polynomial is n. Monic polynomials are those with $a_n = 1$. $R \subset R[x]$ is the set of constant polynomials. R[x] is itself a commutative ring with identity (where 1 is the same identity as in R).

- note: if S is a subring of R, then S[x] is a subring of R[x].

Proposition: immediate properties of polynomial rings. Let R be an integral domain. Let $p(x), q(x)$ be non-zero elements of R[x]. Then,
(1) degree $p(x)q(x)$ = degree $p(x)$+ degree $q(x)$.
(2) the units of R[x] are the same as the units of R
(3) R[x] is an integral domain.

Definition: Ring homomorphisms. Let R and S be rings. A ring homomorphism $f : R \to S$ is a map such that $f(x + y) = f(x) + f(y), f(xy) = f(x)f(y), \forall x, y \in R$. A bijective ring homomorphism is called an **isomorphism** and we say $R \cong S$.

Definition: Ideals. Let R be a ring, let $r \in R$ and let I be a subset of R. Then, $rI := \{rx : x \in I\}$. $Ir := \{xr : x \in I\}$. A subset I of R is a left ideal of R is I is a subring of R and $rI \subseteq I, \forall r \in R$. A subset I of R is a right ideal of R is I is a subring of R and $Ir \subseteq I, \forall r \in R$. If I is both a left and right ideal, it is called an ideal of R.

Proposition: Quotient ring is a ring. Let R be a ring and let I be an ideal of R. Then the additive quotient group R/I is a ring under the binary operations $(r + I) + (s + I) = (r + s) + I, (r + I)(s + I) = (rs + I), \forall r, s \in R$. Conversely, if I is any subgroup of R such that these two operations are well-defined, then I is an ideal of R.

Proposition: First Isomorphism Theorem for Rings.
(1)If $\psi : R \to S$ is a ring homomorphism, then $\ker(\psi)$ is an ideal of R, $\mathrm{Im}(\psi)$ is a subring of S and $R/\ker(\psi) \cong \psi(R)$.
(2) If I is an ideal of R, then the map $R \to R/I$ defined by $r \to r + I$ is a surjective ring homomorphism with kernel I. This is the natural projection of R onto R/I. Every ideal is the kernel of a ring homomorphism and vice-versa.

Definition: Proper ideal. An ideal I is proper if $I \neq R$.

Example: R and $\{0\}$ are ideals of R. $n\mathbb{Z}$ is an ideal of $\mathbb{Z}$ for any $n \in \mathbb{Z}$.

Proposition:

Second Isomorphism Theorem for Rings. Let A be a subring and let B be an ideal of R. Then, $A + B$ is a subring of R, $A \cap B$ is an ideal of A and $(A + B)/B \cong A/(A \cap B)$.

Third Isomorphism Theorem for Rings. Let I and J be ideals of R with $I \subseteq J$. Then, J/I is an ideal of R/I and $(R/I)/(J/I) \cong (R/J)$.

Fourth/Lattice Isomorphism Theorem for Rings. Let I be an ideal of R. The correspondence $A \leftrightarrow A/I$ is an inclusion-preserving bijection between the sets of subrings A of R (if $A \subseteq B$ and both contain I, then $A/I \subseteq B/I$). Furthermore, A (subring containing I) is an ideal of R iff A/I is an ideal of R/I.

Definition: Special ideals. Let R be a ring with identity 1. Let A be a subset of R. Let (A) be the smallest ideal of R containing A.

$$(A) = \cap_{(I \text{ is an ideal, } A \subseteq I)} I$$

. Define $RA = \{\sum_i r_i a_i : r_i \in R, a_i \in A, n \in \mathbb{Z}^+\}$. Define RA and RAR similarly. Principle ideals are ideals generated by a single element. A finitely general ideal is an ideal generated by a finite set. **If** R **is commutative,** $RA = AR = RAR = (A)$**.**

(Important) Proposition: Let I be an ideal of R, where R is a ring with identity 1. (1) $I = R$ if and only if I contains a unit. (2) If R is commutative, then R is a field if and only if its only ideals are the zero ideal $\{0\}$ and R.

(Important) Corollary: If R is a field, then any non-zero ring homomorphism from R into another ring is an injection.

Definition: Maximal Ideals An ideal M in an arbitrary ring R is called a maximal ideal if $M \neq R$ and the only ideals containing M are M and R.

Proposition: In a ring with identity 1, every proper ideal is contained in a maximal ideal.

Sketch of proof: Suppose I *is a proper ideal. Let* S *be the set of proper ideals containing* I*(S is clearly non-empty and has partial order by inclusion). Let* C *be a chain in* S *and let* J *be the union of all ideals in* C*. Show that* J *is an ideal -* $0 \in J$ *and elements are closed under subtraction and left/ring multiplication by elements of* R*. Then, show that* J *is a proper ideal since otherwise* $1 \in J$ *and therefore,* 1 *is in at least one of the ideals in* C *making that ideal not proper. Then, each chain has an upper bound in* S*. Use Zorn's lemma to conclude* S *has a maximal element which is our maximal proper ideal containing* I

Proposition: Let R be a commutative ring with identity 1. The ideal M is a maximal ideal if and only if the quotient ring R/M is a field.

Sketch of proof: ideal M *is maximal iff there are no ideals* I *st* $M \subset I \subset R$*. By lattice isomorphism, ideals of* R *containing* M *correspond bijectively with the ideals of* R/M*, so* M *is maximal if and only if the only ideals of* R/M *are 0 and* R/M*. But by a proposition above,* R/M *is a field iff the only ideals are* 0 *and* R/M*.*

Definition: Prime ideal. Suppose R is commutative with identity 1. An ideal P is called a prime ideal if $P \neq R$ and whenever $xy \in P$, we have $x \in P$ and/or $y \in P$.

Proposition: Assume R is commutative with identity $1 \neq 0$. Then, the ideal P is a prime ideal in R if and only if the quotient ring R/P is an integral domain.

Proof: P *is a prime ideal if and only if* $\bar{R} \neq \bar{0}$ *(since* $P \neq R$*) and* $\bar{ab} = \bar{a}\bar{b} = 0$ *implies either* $\bar{a} = 0$ *or* $\bar{b} = 0$ *which is if and only if* R/P *is an integral domain.*

Proposition: Assume R is commutative. Every maximal ideal of R is a prime ideal.

Proof: M *is maximal implies* R/M *is a field and a field is an integral domain so* M *must be prime.*