# Algebraic Geometry

Jubayer Ibn Hamid

# Contents

# 1 Introduction

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.

Geometry becomes interesting when local properties reveal to us global properties. Algebra provides us a very powerful tool to do that.

## 1.1 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 $\mathbb{A}^n_k$ 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 $V(S) := \{p \in \mathbb{A}^n_k \mid f(p) = 0, \forall f \in S\}$. 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 $X \subseteq \mathbb{A}^n_k$ 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 $\mathbb{A}^n_k$ 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 $X \subseteq \mathbb{A}^n_k$, 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.

*Example:* **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).

*Exercise:*

Define

$$R[[x]] = \{f(x) = \sum_{n=0}^{\infty} a_n x^n : a_n \in R\}.$$

Prove (1) Given $f \in R[[x]]$, $f(x) = \sum_{n=0}^{\infty} a_n x^n$ and suppose there exists $b_0$ s.t $a_0 b_0 = 1$. Then, there exists $g \in R[[x]]$ s.t $fg = 1$. (2) Given R is Noetherian, R[[x]] is also Noetherian. *Hint: Similar proof to Theorem 1, but use trailing coefficient (coefficient of the smallest power) instead of leading coefficient.*

# 3 Module-finite, Ring-finite, Field extensions

**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 <u>module-finite over R</u> 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 <u>ring-finite over R</u> 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 <u>finitely-generated field extension of R</u> 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, $f(v) = 0 \implies v^n \in \sum_{i=0}^{n-1} Rv^i$. Therefore, for any integer m, $v^m \in \sum_{i=0}^{n-1} Rv^i$. This implies R[v] is module-finite over R.

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 $\sum_{j=1}^{n} \delta_i jvw_j - vw_i = 0$ 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. □

We will need one result from linear algebra: if $A = (r_{ij})$ is an $n \times n$ matrix over R and V is a column vector s.t $AV = 0$, then $\det(A)V = 0$. This is because $\det(A)V = \det(A)I_nV = \text{adj}(A)AV = 0$

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: suppose the generators of S are $s_1, ..., s_n$ (where we take $s_1 = 1$ because we enlarge the set of generators as we please as long as it's finite) so $S = \sum_{i=1}^{n} Rs_i$. Then, for any $s \in S$, we can write s as $s = r_1s_1 + \cdots + r_ns_n$.

Now, $ss_i = \sum_{j=1}^{n} r_{ij}s_j$ because $ss_i \in S$ so can be written as a linear combination of $s_i$. Then, let $I_n$ be the $n \times n$ identity matrix, V is the n dimensional column vectors where $V_i = s_i$ and $B = (r_{ij})$. Then, we can write these equations as $sIV = BV \implies (sI - B)V = 0$. Then, $\det(sI - B)V = 0$. However, $v_1 = s_1 = 1$, so $\det(sI - B) = 0$ which implies s is the root of a characteristic polynomial of B over R so s is integral over R.

Conversely, suppose S is integral over R and we are told that S is ring-finite over R i.e $S = R[s_1, ..., s_n]$. Then, for each $s_i \in S$, we have a monic polynomial from which we can write, after rearranging $s_i^{k_i} = a_{1,i}s_i^{k_i-1} + \cdots + a_{k_i-1,i}s_i + a_{k_i,i}$. Therefore, $s_i^{k_i}$ is in the submodule of S generated by $\{s_i, \cdots, s_i^{k_i-1}\}$ i.e $s_i^m$ is in this submodule for any m. Now, we know S is ring-finite over R with $s_1, ..., s_n$ as the generators. Now, the direct sum of the submodules (as we saw for each $s_i$) is also a finitely generated as an R-module and so S is itself module-finite over R. □

**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, $p^n + a_1p^{n-1} + \cdots + a_n = 0$ with $a_i \in k$. This is a polynomial in k[x] with a root, so by definition of algebraic closure, $p \in k$.

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. □

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. □

# 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 $\psi$ 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. In fact, we will often use the fact that points in affine varieties correspond to maximal ideals made rigorous in the following:**

**Lemma 11.** There is a natural bijection between a point $a \in \mathbb{A}^n$ and k-algebra homomorphisms $k[x_1, \cdots, x_n] \to k$. We say the point a corresponds to the maximal ideal defined by the kernel of this homomorphism.

*Proof.* Let $\phi : k[x_1, ..., x_n] \to k$ be a k-algebra homomorphism defined by $\phi(x_i) = a_i$, so $x_i - a_i \in \ker(\phi)$. Given $\phi$ is surjective (since it's k-algebra homomorphism), $k[x_1, ..., x_n]/\ker(\phi) \cong k$ so $\ker(\phi)$ is a maximal ideal. □

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 12.** (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 13.** 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 14.** 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 15.** 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 $\mathbb{A}^n_k$.

**Corollary 16.** 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 17.** 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 18.** The affine space $\mathbb{A}^n_k$ is irreducible if k is infinite.

**Theorem 19.** 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 20.** 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$V \in \mathbb{A}^n_k$ : Vis 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 21.** 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 22.** 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 23.** 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 $x \in Z$. □

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 24.** 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 $V \subseteq \mathbb{A}^n_k$, $W \subseteq \mathbb{A}^m_k$ 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. □

For an example, consider the Zariski topology on $\mathbb{A}^1_k$ and let $V(f_1, ..., f_m) \subset \mathbb{A}^1_k$. 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 $\mathbb{A}^1_k$ 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 $\mathbb{A}^1_k$ are of the form $\emptyset$, $\mathbb{A}^1_k$ and finite subsets of $\mathbb{A}^1_k$.

**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. *Intuitively, two polynomials in O(X) are equivalent as long as they have the same values at every point of V.*

Note that, for a point $a = (a_1, ..., a_n) \in X$ and $f \in O(X)$, the value $f(a) \in k$ 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 $V(f)_X := V(f) \cap X$ where $X \subset \mathbb{A}^n$ is an affine variety. Now, we define basic closed sets of X 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 the Zariski topology is a union of basic closed sets for some set of functions. On the other hand, the basic open sets of X 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 Zariski topology 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 25.** 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 26.** (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 27.** $D(1) = V, D(0) = \emptyset, D(fg) = D(f) \cap D(g)$.

**Definition 14.** Zariski Closure. 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 $\bar{X} \subseteq V$.

**Proposition 28.** S is irreducible if and only if $\bar{S} \subseteq V$ is irreducible.

# 7 Coordinate Rings

## 7.1 Coordinate rings as k-algebra homomorphisms

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 $\mathbb{A}^n_k$.

One can easily prove that the coordinate ring O(V) is Noetherian.

**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 $\psi$ is a ring homomorphism that is identity on k.

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

**Theorem 29.** $O(X) \cong Map(X, \mathbb{A}^1)$. 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 $\varphi : O(X) \to Map(X, \mathbb{A}^1)$. Then, define $\varphi(f)(a) = f(a)$ for any $a \in X$. This is a homomorphism by design. To show surjectivity, by definition of $Map(X, \mathbb{A}^1)$, $f \in Map(X, \mathbb{A}^1)$

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 30.** 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 $O(X) \cong \text{Map}(X, \mathbb{A}^1)$.

Furthermore, just as before, a point p in a variety X corresponds to a maximal ideal in $R = O(X)$, $m_p = \{f \in O(X) : f(p) = 0\} \subseteq O(X)$. This can be seen by considering the k-algebra homomorphism $\phi : O(X) \to k$ such that $\phi(x_i) = p_i$. Then, $m_p = \ker(\phi)$.

## 7.2 Pullback, relationship between $\text{Map}(V, W)$ and $\text{Mor}_k(O(W), O(V))$

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

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 $p^* : \text{Map}(Y, \mathbb{A}^1 \to \text{Map}(X, \mathbb{A}^1)$.

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

**Theorem 31.** Let $V \subset \mathbb{A}^n$ and $W \subset \mathbb{A}^m$ be affine varieties. There exists a natural 1-1 correspondence between $\text{Map}(V, W)$ and $\text{Mor}_k(O(W), O(V))$.

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

Let $s, s' \in \text{Map}(V, W)$ 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 $\lambda \in \text{Mor}_k(O(W), O(V))$. We construct a map $s \in \text{Map}(V, W)$ 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 $\lambda$ 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 $s \mid_V \in Map(V, W)$.

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). □

## 7.3 Product of varieties

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

**Theorem 32.** 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 $O(X \times Y) = k[x_1, ..., x_n] \times k[y_1, ..., y_m]/(I(X \times Y)) = k[x_1, ..., x_n] \times k[y_1, ..., y_m]/(I(X) \otimes_k k[y_1, .., y_m] + k[x_1, .., x_n] \otimes_k I(Y)) = O(X) \otimes_k O(Y)$. □

**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 33.** 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 34.** 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 $\psi(f) \neq 0$.

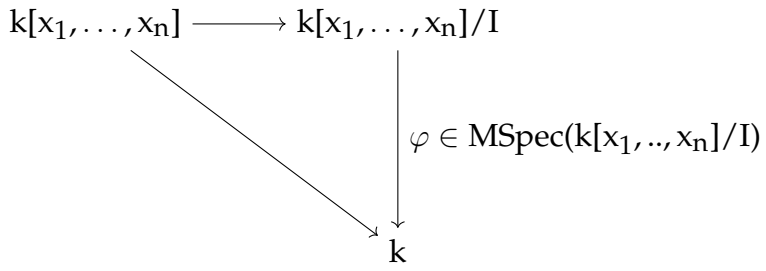
**Theorem 35.** Let $p : V \to W$ be a morphism between 2 varieties where $p = (p_1, ..., p_m)$. Let $w \in W$ be a point with the vanishing ideal $m_w = (x - w_1, ..., x - w_m) \subset I(W)$, then the fiber $p^{-1}(w) \subset V$ is defined by $p^*(m_w) = (p_1(x) - w_1, ..., p_m(x) - w_m) \subset O(V)$.

## 7.4 MSpec(R) and abstract varieties

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 $\varphi$ as:




With this in mind, we note that we can associate an element of $MSpec(k[x_1, ..., x_n]/I)$ 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:

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

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

**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 $\psi : V = \text{MSpec}(R) \to W = \text{MSpec}(S)$.

## 7.5 Localization

**Theorem 36.** (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 37.** 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 $\text{Im}(g) \in S^\times$ i.e g is mapped to a unit in S. In other words,

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

(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 $\phi$ 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 38.** 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, $MSpec(R_f) = D(f)$. 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, $MSpec(R_f)$ 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 39.** $I \subset R$ 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

## 8.1 Krull Dimension

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. (recall: irreducible closed subsets of X are closed subsets $Y \subseteq X$ such that Y cannot be written as the union of two closed subsets $Y_1, Y_2$ such that one of these is empty.)

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

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

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

*Example:* $\dim(\mathbb{A}^1) = 1$ since the irreducible closed subsets are $\emptyset$, finite subsets, $\mathbb{A}^1$ i.e the maximal chains look like $\emptyset \subset \{p\} \subset \mathbb{A}^1$.

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

*Example:* Let $X := \{xy = 0\} \subseteq \mathbb{A}^2$. This has two irreducible components only - $\{x = 0\} \cong \mathbb{A}^1$ and $\{y = 0\} \cong \mathbb{A}^1$. Both the irreducible components are of dimension 1, so X is equi-dimensional of dimension 1.

With this definition of dimension, we get the following:

**Proposition 40.** If $X \subseteq Y$ are closed, then $\dim(X) \leq \dim(Y)$. If Y is irreducible and X is a proper closed subset of Y (i.e $X \neq Y$ is closed), then $\dim(X) < \dim(Y)$.

*Proof.* For the first part, any strictly increasing chain of non-empty irreducible closed subsets of X is also a strictly increasing chain of non-empty irreducible closed subsets of Y. For

the second part, note that we are working with a ring with identity and so every proper ideal is contained in some maximal ideal (which is also prime). □

Given we have defined Zariski topology over affine varieties, we can now use Krull Dimension as a notion of dimension over affine varieties.

**Definition 29.** Krull dimension of an affine variety. Using Zariski topology,

$$\dim(V) = \max\{k : X_0 \subsetneq X_2 \subsetneq \cdots X_k \subsetneq V, X_i \text{ irreducible closed subsets of } V\}$$

**Definition 30.** Krull dimension of ring. Let R be any ring. The Krull dimension dim(R) is the maximal length of strict chains of prime ideals of R.

**Proposition 41.** 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.

**Proposition:** Let X be an affine variety and let R = O(X). Then, dim(X) = dim(R) = dim(O(X)).

*Proof.* There is a natural correspondence between irreducible closed subsets of X and prime ideals of R. Suppose dim(X) = n. Then, we have a maximal chain $(V_0 = \emptyset) \subsetneq \cdots \subsetneq V_n \subsetneq X$. Then, $I(X) \subsetneq I(V_n) \subsetneq \cdots \subsetneq I(V_0) = R$ is a maximal chain. □

**Definition 31.** 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 42.** Let k be a field. Any finitely generated k-algebra R is catenary.

**Note: This means $k[x_1, ..., x_n]/I$ is catenary.**

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

**Corollary 43.** 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 32.** Algebraically independent and algebraic over. Let $L/k$ be a field extension (i.e k is a subfield of L). Then, $a_1, ..., a_n \in L$ are **algebraically independent** over k if $f \in k[x_1, \cdots, x_n]$ such that $f(a_1, ..., a_n) = 0$ implies $f = 0$. Otherwise, $a_1, ..., a_n$ are algebraically dependent over k. (recall: $a \in L$ is **algebraic over** k if there exists a monic polynomial $f \in k[x]$ such that $f(a) = 0$)

**Definition 33. Transcendence degree.**

$$\text{tr.deg}(L/k) := \max\{r : \exists a_1, ..., a_r \in L \text{ algebraically independent over k}\}.$$

To get a sense of this, note that $\dim(k(\mathbb{A}^n)) = n$. This is because the maximal set of algebraically independent elements of $k(\mathbb{A}^n)$ is of length n. Choose $x_1, ..., x_n \in k(\mathbb{A}^n)$. Then, $p(x_1, ..., x_n) = 0$ implies $p = 0$ (note that $x_i$ are variables here, so $p(x_1) = 0$ would also imply p is 0). On top of that, if we chose any other $f \in k(\mathbb{A}^n)$, we could write it as a combination of $x_i'$s so $p(T_1, ..., T_n, T_{n+1}) = f(T_1, ..., T_n) - T_{n+1} = 0$ is a non-zero polynomial that vanishes at $(x_1, ..., x_n, f)$.

With this, we have the following:

**Theorem 44.** Let V be an irreducible affine variety. Let $R = O(V)$.

$$\dim(R) = \text{tr.deg}(k(V)).$$

Note: here we are treating k(V) as a field extension of k.

*Sketch of proof: It can be easily seen that* $\text{tr.deg}(k(V)) \geq \dim(R)$. *This is because* $\text{tr.deg}(\text{Frac}(R)) \geq \text{tr.deg}(R)$. *Now, consider the number of algebraically independent elements of* R. *Suppose,* $x_1, ..., x_r \in R/P$ *(where* P *is a prime ideal) are algebraically independent. Then, for any* $y \neq 0, y \in P$, *we have* $\{x_1, ..., x_r, y\}$ *is an algebraically independent set so the number of algebraically independent elements of* R *is greater than or equal to the number of prime ideals. Now, we need to show* $\text{tr.deg}(k(V)) \leq \dim(R)$. *Proving this requires Noether Normalization which we will do later.*

**Corollary 45.**

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

**Corollary 46.** $f : X \to Y$ 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 34.** 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 47.** 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 $\dim(V) - 1$.

## 8.2 Noether Normalization

**Lemma 48.** Let $f \in k[x_1, ..., x_n]$ where $n \geq 2$ be a non-zero polynomial over an infinite field k. Then, there are elements $\lambda, a_1, ..., a_{n=1} \in k$ such that $\lambda f(y_1 + a_1 y_n, \cdots, y_{n-1} + a_{n-1} y_n, y_n) \in k[y_1, ..., y_n]$ is monic in $y_n$.

*Proof.* Let $f_d$ be the homogenous part of f of the highest degree. We have $f_d(\lambda x_1, ..., \lambda x_n) = \lambda^d f_d(x_1, ..., x_n)$ where d is the degree of f. Since k is infinite, we can always fine $a_1, ..., a_{n-1}$ such that $f_d(a_1, ..., a_{n-1}, 1) \neq 0$. Then, let $y_j = x_j - a_j x_n$ for $j = 1, 2, ..., n-1$ and $y_n = x_n$ and $\lambda = f_d(a_1, ..., a_{n-1}, 1)^{-1}$. Then, $\lambda f(y_1 + a_1 y_n, ...., y_{n-1} + a_{n-1} y_n, y_n) = \lambda f_d(a_1, ..., a_{n-1}, 1) y_n^d$+lower order (in degree of $y_n$ terms. This is a monic polynomial in $y_n$. □

**Theorem 49.** (Noether Normalization). Let R be a finitely generated algebra over a infinite field k with generators $x_1, ..., x_n \in R$. Then, there exists an injective k-algebra homomorphism $\phi : k[t_1, .., t_r] \to R$ from a polynomial ring to R such that R is integral over $k[t_1, ..., t_r]$.

*Proof.* Proceed by induction. For $n = 1$, let $t_1 = x_1$. Now suppose $n > 1$. If $x_1, ...., x_n$ are algebraically independent, we can choose $t_i = x_i$ and the result follows. Now suppose there exists some algebraic dependence between the generators $x_1, ..., x_n$ i.e there exists a non-zero polynomial f over k such that $f(x_1, ..., x_n) = 0$. Let $f_d$ be the homogenous part of the highest degree of f. Then, by the previous lemma, we can fine $\lambda, a_1, ..., a_{n-1}$ such that $\lambda f(y_1 + a_1 y_n, \cdots, y_{n-1} + a_{n-1} y_n, y_n) \in k[y_1, ...y_n]$ is monic in $y_n$. The new coordinates are then given by $y_1 = x_1 - a_1 x_n, \cdots, y_{n-1} = x_{n-1} - a_{n-1} x_n, y_n = x_n$ and so $\lambda f(x_1, ..., x_n) = 0$. Furthermore, $y_n$ is integral over $k[y_1, ..., y_{n-1}]$ by the previous lemma. By inductive hypothesis, there exists an injective algebra homomorphism $\phi : k[t_1, ..., t_r] \to k[y_1, ..., y_{n-1}]$ s.t $k[y_1, ..., y_{n-1}]$ is integral over $k[t_1, ..., t_r]$. But $y_n$ is integral over $k[y_1, ..., y_{n-1}]$ and so $y_n$ is integral over $k[t_1, ..., t_r]$. □

*Example 1:* Let $R = k[x_1, x_2]/(x_1 x_2 - 1) \cong k[x, \frac{1}{x}]$. Then, R is not integral over k[x] - if $1/x$ were integral over k[x] with the polynomial $(\frac{1}{x})^n + a_1(x)(\frac{1}{x})^{n-1} + \cdots + a_n(x) = 0$ with $a_i(x) \in k[x]$. After multiplying both sides by $x^{n-1}$, we can see that $\frac{1}{x} \in k[x]$ which is impossible. Let $x_1 := t_1 + t_2, x_2 := t_2$, then, $R = k[t_1, t_2]/(t_2^2 + t_1 t_2 - 1)$ and there is injective map $\phi : k[t_1] \to R$ with R integral over $k[t_1]$.

# 9 Sheaves

## 9.1 Presheaf, Germs, Stalks and Sheaves

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 $f \in \text{Map}(X, Y)$, we would like to localize f i.e $f|_U \in \text{Map}(X, Y)$ 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 $\text{Map}(U, \mathbb{A}^1)$ as:

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

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 $O(X) \cong \text{Map}(X, \mathbb{A}^1)$, so $O(U) \cong \text{Map}(U, \mathbb{A}^1)$.

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 $\text{res}_{U,V} : \mathscr{O}(U) \to \mathscr{O}(V)$. 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 $\text{Map}(D(f), \mathbb{A}^1)$.

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 35. 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 $\text{res}_{U,W} f = \text{res}_{V,W} g$. 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 36. 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.

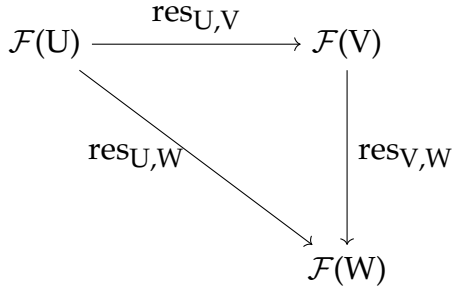
(2) For each inclusion $U \subseteq V$, we have the **restriction** map:

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

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

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

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




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 $\text{res}_{U,W} f = \text{res}_{V,W} g$.

Now we finally define sheaf:

**Definition 37. 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 $\text{res}_{U,U_i} f = f_i$ for all i.

## 9.2 Structure Sheaf

**Sheaf of functions $\mathscr{O}$ on X = MSpec(R).** (Recall: given R is an k-algebra (and integral domain), X = MSpec(R) is the set of all homomorphisms from R to k.) So, X is an affine variety. The sheaf of functions $\mathscr{O}$ on X = MSpec(R) has sections $\mathscr{O}(U) \subset \text{Frac}(R)$ 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 50.** If R is an integral domain, then $\mathscr{O}(X = \text{MSpec}(R)) = R$.

*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 $f \in \mathscr{O}(X) \subset \text{Frac}(R)$. We want to show $f \in R$.

Define the ideal of denominators of f to be $I := \{r \in R : rf \in R\} \subset R$. 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 51.** Let $S = k[x_1, ..., x_n]/I(V)$. Recall that we can write MSpec(S) as $V \subset \mathbb{A}^n$. Then, consider any open set $U \subset$ 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 52.** 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 $f \in$ 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 $rf \in R$. 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 53.** 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.* We assume k is algebraically closed so that we can use Hilbert's Nullstellensatz. Let R be the coordinate ring of D(f) and let $U_i := D(f_i), i = 1, ..., m$ be a collection of open sets covering D(f). Then, $V(f_1, ...., f_m) = \emptyset$ in D(f) so by Hilbert's Nullstellensatz, $(f_1, ..., f_m) = 1$. Now, we check the two axioms of sheaves:

(1) injectivity: we need to show that the map $R \to \Pi_i R_{f_i}$ is injective. Suppose $x \in R$ is 0 in every $R_{f_i}$. Then, $x = \frac{a}{f_i^N} = 0$, so $f_i^N x = 0$ (since $f_i \neq 0$ in $U_i$) for all i (given N is large enough). But we know $f_i$ are non-zero, so $x = 0$.

(2) Gluability: Suppose we have $x_i \in R_{f_i}$ such that $x_i = x_j \in R_{f_i f_j}$ (caution: $x_i$ is not a variable, it's a section/function over $U_i$). We want to show there exists $f \in R$ such that $f|_{U_i} = x_i$. To see this, we first write $x_i = \frac{s_i}{f_i^{n_i}}$. Now, if we take N large enough,

we can write all $x_i = \frac{s_i}{f_i^N}$. Then, $x_i = x_j$ implies $(s_i f_j^N - s_j f_i^N) f_i^N f_j^N = 0$. Replace $s_i$ with $s_i$ with $s_i f_i^N$ and $f_i$ with $f_i^{2N}$, we may assume that $s_i f_j - s_j f_i = 0$ in R for all i, j. Now, $f \in \sqrt{(f)} = \sqrt{(x_1, ..., x_m)}$ (since we already argued that $(x_1, ..., x_m) = 1$ so it generates (f)), therefore, we can write $f^N = c_1 x_1 + \cdots + c_m x_m$ where $c_i \in R$. Let $a = c_1 s_1 + \cdots c_m s_m$. Then, $af_i = \sum_j c_j s_j x_i = \sum_j c_j x_j s_i = f^N s_i$. So, $\frac{a}{f^N} = \frac{s_i}{f_i} = \frac{s_i f_i^N}{f_i^{2N}} = \frac{s_i}{f_i^N} = x_i$. □

Now, we put this all under a suitable dictionary:

**Definition 38.** Spec(R). Let R be any ring. Denote by Spec(R) the set of all prime ideals of R. For any subset $T \subset R$, define $V_{prime}(T) = \{p \in Spec(R) : \forall f \in T, f \in p\}$ i.e the set primes of R that contain T. Similarly, $D_{prime}(T)$ is the set of primes of R *not* containing T.

Spec(R) is equipped with its Zariski topology: a subset $Z \subseteq Spec(R)$ is closed if $Z = V(I)$ for some $I \subset R$

With the last proposition, we have:

**Theorem 54.** The presheaf of rings $\mathscr{O}$ on Spec(R) sending D(f) to $\mathscr{O}(D(f)) = R_f$ is a sheaf ccalled the structure sheaf of Spec(R).

**Definition 39.** Ringed space. Ring spectrum. A ringed space $(X, \mathscr{O}_X)$ is a topological space with a sheaf of rings $\mathscr{O}_X$ (called structure sheaves). The ring spectrum for any ring R is the ringed space $(Spec(R), \mathscr{O})$.

**Definition 40.** Prevariety. A prevariety over k is a ringed space $(X, \mathscr{O}_X)$ over k such that the pair $(X, \mathscr{O}_X)$ is locally isomorphic to ring spetrum of affine varieties.

# 10 Local Rings and Valuations

## 10.1 Local Rings

We first provide a series of definitions:

**Definition 41.** Rational Function. Let V be an affine variety and let O(V) be its coordinate ring. A rational function f on V is an element in k(V) = Frac(O(V)) = Frac($k[x_1, ..., x_n]/I(V)$) i.e $f \in k(V)$ can be expressed as $f = g/h$ where $h \neq 0$. A rational f is **defined at a point** $p \in V$ if $f = \frac{g_p}{h_p}$ with $g_p, h_p \in R$ and $h(p) \neq 0$.

**Definition 42.** Birational equivalence. We say two varieties X and Y are birational or birationally isomorphic if there exists rational maps $f : X \to Y$ and $g : Y \to X$ such that $f \circ g = id, g \circ g = id$. If X and Y are irreducible, this is equivalent to $k(X) \cong k(Y)$.

**Definition 43.** Ideal of denominators. For $f \in k(V)$, we have the ideal of denominators $Deno_R(f) = \{r \in R : rf \subseteq R\} \subseteq R$. Here R = O(V).

**Theorem 55.** For an open subset $U \subseteq X$, the ring of polynomial functions/regular functions $\mathcal{O}(U)$ on U can be identified with the subring of Frac($\mathbb{O}(X)$) consisting of all rational functions defined on all points of U.

**Definition 44.** Localization $S^{-1}R$. Let R be a ring. A subset $S \subset R$ is a multiplicative subset of R if $1 \in S$ and $g, h \in S \implies gh \in S$. Define the localization $S^{-1}R$ of R at S to be the set $\{a/s : a \in R, s \in S\}$ under the equivalence relation $a_1/s_1 = a_2/s_2 \leftrightarrow \exists s \in S, s(a_1s_2 - a_2s_1) = 0$.

Note that this localization is, at least on face value, defined differently from the definition of localization before where we had $R_f$. Fortunately, they are not different:

*Example:* If $S = \{f^n\}_{n \geq 0}$, then $S^{-1}R = R_f$.

*Example:* Let q be a prime ideal of R. Then, $S = R - q$ gives $R_q := (R - q)^{-1}R$ which is the localization of R at q.

**Definition 45.** Local ring. A ring R is called a local ring if it has a unique maximal ideal.

We now look at two examples of local rings: (1) $R_q$ and (2) $\mathcal{O}_p(V)$

**Theorem 56.** Let R be a ring and q be a prime ideal. Then, $R_q(R-q)^{-1}R$ is a local ring with maximal ideal $qR_q$.

*Proof.* Recall : $R_q = (R-q)^{-1}R$. First, we claim $qR_q$ is a maximal ideal. Note, $qR_q = q(R-q)^{-1}R = (R-q)^{-1}qR = (R-q)^{-1}q$. This is an ideal because $(R-q)^{-1}qR = (R-q)^{-1}q$ (similarly for left ideal). Furthermore, $qR_q \neq R_q$. To do so, we will show that $1 = 1/1 \notin qR_q$. Suppose, $1/1 = r/s$ where $r \in q, s \in R-q$. Then, $\exists t \in R-q$ s.t $(s-r)t = 0$ (using the equivalence relation in localizations), so $rt = st$. This is impossible as $rt \in q$ and $st \notin q$ (since neither s nor t are in q but q is prime).

Suppose $r/s \in R_q$ such that $r/s \notin qR_q$. Then, $r \notin q$ since if it were, then $r/s = (r/1)(1/s) \in qR_q$.

Now, $s/r \in R_q$ and so $r/s$ is invertible. Therefore, if an ideal contains any element that is not in $qR_q$, it contains a unit and therefore, the ideal becomes all of R i.e not a maximal ideal. □

We know germs already.

**Definition 46.** Local ring $\mathcal{O}_p(V)$. For $p \in V$, we define the local ring $\mathcal{O}_p(V)$ of V to be the germs at p (see previous chapter).

$$\mathcal{O}_p := \{(f, U) : p \in U \text{ open subset of } V, f \in \mathcal{O}(U) \text{ a regular function}\}$$

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

(Recall: V an affine variety, $U \subset V$ open, we have $\mathcal{O}(U) \subset \text{Frac}(R)$ where $f \in \mathcal{O}(U)$ if for any $x \in U$, we can write $f = \frac{g}{h}, g, h \in R$ and $h(x) \neq 0$.)

Basically, $\mathcal{O}_p(V)$ is the set of rational functions on V that are defined at p.

The set of points $z \in V$ where a rational function f is not defined is called the *pole set* of f.

Furthermore, define

$$m_p = (t-p)\mathcal{O}_p$$

and define

$$M_p = (\text{Vanishing ideal of } p \in V) \subset \mathcal{O}(V)$$

*Example:* Consider $p \in \mathbb{A}^1$. Then, $\mathcal{O}_p = \{f(t)/g(t) : g(p) \neq 0\} \subset k(t)$. Then, we identify $\mathcal{O}_p^\times = \{f(t)/g(t) : f(p) \neq 0, g(p) \neq 0\}$ and the complement $\mathcal{O}_p \setminus \mathcal{O}_p^\times = \{f(t)/g(t) : f(p) = 0, g(p) \neq 0\} = (t-p)\mathcal{O}_p$. Any proper ideal $I \subset \mathcal{O}_p$ does not contain a unit so it must be contained in $(t-p)\mathcal{O}_p$ and so $(t-p)\mathcal{O}_p$ is the unique maximal ideal $m_p \subset \mathcal{O}_p$.

We have the following immediate properties:

**Proposition 57.** (1) The pole set of a rational function is an algebraic subset of V.
(2) $O(V) = \cap_{p \in V} \mathscr{O}_p(V)$.

*Proof.* (1) Suppose $V \subseteq \mathbb{A}^n$. For $G \in k[x_1, .., x_n]$, let $\bar{G}$ be the residue of G in O(V). Now, let $f \in k(V)$ and let $J_f = \{G \in k[x_1, .., x_n] : \bar{G}f \in O(V)\}$. Then, $J_f$ is an ideal of $k[x_1, .., x_n]$ containing I(V) and the points of $V(J_f)$ are the points where f is not defined.
(2) Suppose $f \in \cap_{p \in V} \mathscr{O}_p(V)$, then $V(J_f) = \emptyset$ (since if f is defined everywhere in V, then $\bar{G} \neq 0 \implies$ G is not 0 on V. Then, by Nullstellensatz, $1 \in J_f$, so $1 \cdot f = f \in O(V)$. □

**Lemma 58.** The following conditions on a ring R are equivalent:
(1) The set of non-units in R forms an ideal. (2) R has a unique maximal ideal that contains every proper ideal of R.

*Proof.* If m = {non-units of R}. Then, every proper ideal of R is contained in m (since proper ideal does not contain units). □

**Proposition 59.** $\mathrm{Spec}(R_q) = \{p \subseteq R_q : p \subseteq q\}$

**Theorem 60.** The following are true for any point $p \in V$:
(1) $\mathscr{O}_p$ is a Noetherian local ring with unique maximal ideal $m_p \subset \mathscr{O}_p$ of pairs (U, f) with f(p) = 0 and $m_p$ is generated by the image of the vanishing ideal $M_p \subset \mathscr{O}(V)$ of p.
(2) For any k-algebra, a homomorphism $\mathscr{O}_p \to R$ is the same as a homomorphism $\mathscr{O}(V) \to R$ with all elements in $\mathscr{O}(V) \backslash M_p$ sent to units i.e $\mathscr{O}_p$ is the localization $S^{-1}O(V)$ for the multiplicatively closed set $S = \mathscr{O}(V) \backslash M_p$. *(Note: these are backslashes i.e complements, not quotients)*
(3) If $V_1, ..., V_i$ are the irreducible components of V containing p, then the map $\mathscr{O}(V) \to \mathscr{O}_p$ factors $\mathscr{O}(V) \to \mathscr{O}(V_1 \cup \cdots \cup V_i) \to \mathscr{O}_p$.
(4) $\mathscr{O}(V)/M_p^i = \mathscr{O}_p/m_p^i$ for all i with $M_p^j/M_p^i = m_p^j/m_p^i$ and $T_pV := (M_p/M_p^2)^\vee = (m_p/m_p^2)^\vee$.

*Proof.* (1) Consider a germ in $\mathscr{O}_p$, (f, U), that does not vanish at p when restricted $(U \cap D(f), f|_{U \cap D(f)})$. Then, $(U \cap D(f), f|_{U \cap D(f)})$ has an inverse $(U \cap D(f), f|^{-1}_{U \cap D(f)})$ and ideals that contain points not in $m_p$ (i.e contains regular functions that do not vanish at p) become all of $\mathscr{O}_p$. Therefore, $m_p$ is the unique maximal ideal.

Now, suppose $(D(g), \frac{f}{g})$ is a germ in $m_p$. Then this is equivalent up to a unit to (D(g), f) where $f \in \mathscr{O}(V)$. Therefore, $m_p$ is generated by $M_p$.

Now $\mathscr{O}_p$ is Noetherian. Suppose $(f_1/g_1) \subset (f_1/g_1, f_2/g_2) \subset \cdots \subset \mathscr{O}_p$ is an increasing sequence of ideals. This is equivalent to the sequence $(f_1) \subset (f_1, f_2) \subset \cdots \subset \mathscr{O}_p$ - this sequence stabilizes because $\mathscr{O}(V)$ is Noetherian.

(2) Follows from definition.

(3) There is a map $\mathcal{O}(V) \to \mathcal{O}_p/m_p^i$ with $M_p^i$ in the kernel. The other way, note that $\mathcal{O}(V)\backslash M_p$ are all units in $\mathcal{O}(V)\backslash M_p^i$ so we have a map $\mathcal{O}_p \to \mathcal{O}(V)/M_p^i$ and it is easy to see that $m_p^i$ lies in the kernel. □

## 10.2 Discrete Valuation Rings - application of local rings

We will require the following:

**Proposition 61.** Let R be an integral domain that is *not* a field. Then, the following are equivalent:
(1) R is Noetherian and local (i.e has a unique maximal ideal), and the maximal ideal is principal.
(2) There is an irreducible element $t \in R$ s.t every non-zero $z \in R$ may be written uniquely in the form $z = ut^n$ where u is a unit in R, and n is a non-negative integer.

*Proof.* (1) implies (2): let m be a maximal ideal and let t be a generator for m. Suppose $ut^n = vt^m$ for $n \geq m$ and $u, v$ are units. Then, $ut^{n-m} = v$ is a unit, so $n = m$ (since t is irreducible) and $u = v$. Thus the expression $z = ut^n$ is unique. Now we show there exists such an expression. Assume that z is not a unit. Now, every proper ideal is contained in a maximal ideal, so $z = z_1 t$ for some $z_1 \in R$. If $z_1$ is a unit, we are done. Otherwise, write $z_1 = z_2 t$. Continuing this way, we get an infinite sequence $z_1, z_2, ...$ with $z_i = z_{i+1} t$. Given R is Noetherian, the chain of ideals $(z_1) \subset (z_2) \subset\subset \cdots$ must have a maximal member so $(z_n) = (z_{n+1})$ for some n. Then, $z_{n+1} = vz_n$ and so $z_n = vtz_n$ and $vt = 1$. But t is not a unit.

(2) $m = (t)$ is the set of non-units. Then, the only ideals in R are the principal ideals $(t^n)$ where n is a non-negative integer so R is a PID. PIDs are Noetherian. □

**Definition 47. Discrete valuation ring.** A ring satisfying the conditions of the previous proposition is called a discrete valuation ring (DVR). Therefore, if ring R is a DVR, then:
(1) R is Noetherian and has a unique maximal ideal which is principal
(2) There exists an irreducible element $t \in R$ s.t for any non-zero $z \in R$, we can write it uniquely in the form $z = ut^n$ where $u \in R$ is a unit and $n \in \mathbb{Z}_{\geq 0}$
An element t as in the second condition is called a uniformizing parameter for R. Any other uniformizing parameter is of the form ut where u is a unit in R.

**Definition 48. Order function on DVR.** Let K be the quotient field of R which is a DVR. Then, when t is fixed, any non-zero element $z \in K$ has a unique expression $z = ut^n$ (u is a unit in R and $n \in \mathbb{Z}$). The exponent n is called the order of z and is written $n = \text{ord}(z)$ with $\text{ord}(0) = \infty$. Then, $R = \{z \in K : \text{ord}(z) \geq 0\}$ and $m = \{z \in K : \text{ord}(z) \geq 0\}$ is the maximal ideal in R.

**Now, we motivate why discrete valuation ring/order of vanishing is important**

Consider the curve $y = x^2$. we want to assign an "order of vanishing" at (1, 1) for every function in $k[x, y]/(y - x^2)$. We define the order of vanishing at (1, 1) to be the **largest i such that** $f \in (x-1, y-1)^i$. Here's the intuition - f is the sum of products of i linear functions vanishing at 1 and each linear function vanishes to order at least 1.

Let us compute some orders of vanishing:
(1) Order of vanishing of y at (1, 1): $y(1, 1) = 1 \neq 0$, so $y \notin (x - 1, y - 1)$ so the order of vanishing is 0.
(2) $y - x^2 = 0 \in (x - 1, y - 1)^i$ for all i, so the order is $\infty$.
(3) $y - 1 \in (x - 1, y - 1)$ so the order is $\geq 1$ although it is unclear if the order is exactly 1.
(4) $2x - y - 1 = -(x - 1)^2 \in (x - 1, y - 1)^2$ so the order is $\geq 2$ although it is unclear if $2x - y - 1 \in (x - 1, y - 1)^3$.
(5) $(2x - y - 1)^2 = -(x - 1)^4 \in (x - 1, y - 1)^4$ so the order is $\geq 4$ although it is unclear if $(2x - y - 1)^2 \in (x - 1, y - 1)^5$.

We then generalize discrete valuation:

**Definition 49. Discrete valuation**. A discrete valuation of a field K is a function $v : K \to \mathbb{Z} \cup \{\infty\}$ such that
(1) $v(x) = \infty$ exactly when $x = 0$,
(2) v is surjective,
(3) $v(fg) = v(f) + v(g)$,
(4) $v(f + g) \geq \min(v(f), v(g))$ and if $v(f) \neq v(g)$, this is an equality.

If L is a subfield of K, then $v(L^\times) = 0$.

We let $\mathcal{O}_v$ be the elements of K where $v(f) \geq 0$.

$$\mathcal{O}_v := \{x \in K : v(x) \geq 0\}.$$

We call v(x) the **order of vanishing** of x.

Lastly, we define the maximal ideal

$$m_v := \{x \in K : v(x) \geq 1\}$$

For $v : K \to \mathbb{Z} \cup \{\infty\}$ a discrete valuation of field K, $\mathcal{O}_v/m_v \cong k$.

# 11 Forms, product of Rings and operations on ideals

These sections are from Foulton [1]. Writing these down here for completeness.

## 11.1 Coordinate Changes

**Definition 50.** Change of coordinates. Let $T = (T_1, .., T_m)$ be a morphism/polynomial map from $\mathbb{A}^n$ to $\mathbb{A}^m$. Let f be a polynomial in $k[x_1, ..., x_m]$. Then, define

$$f^T = \tilde{T}(f) = f(T_1, ..., T_m).$$

Given $I \subset \mathbb{A}^m$ is an ideal and V is an algebraic set in $\mathbb{A}^m$, $I^T \subset \mathbb{A}^n$ will be the ideal in $k[x_1, ..., x_n]$ generated by $\{f^T : f \in I\}$. $V^T$ is the algebraic set $T^{-1}(V) = V(I^T)$ where $I = I(V)$. So if V is the hypersurface of f, then $V^T$ is the hypersurface of $f^T$ given $f^T$ is not constant.

**Definition 51.** Affine Change of coordinates. An affine change of coordiantes on $\mathbb{A}^n$ is a polynomial map $T = (T_1, \ldots, T_n) : \mathbb{A}^n \to \mathbb{A}^n$ where each $T_i$ is a polynomial of degree 1 and T is one-to-one and onto. If $T_i = \sum_{ij} a_{ij}x_j + a_{i0}$, then $T = T'' \circ T'$ where $T'$ is a linear map ($T'_i = \sum_{ij} a_{ij}$) and $T''$ is a translation ($T''_i = x_i + a_{i0}$). Translations are invertible. So T is one-to-one and onto if and only if $T'$ is invertible.

If T and U are affine change of coordinates on $\mathbb{A}^n$, then so are $T \circ U$ and $T^{-1}$.

## 11.2 Forms

(Treating forms to be the same as homogenous polynomials)

Let R be an integral domain. If $f \in R[x_1, .., x_{n+1}]$ is a form, we define $f_* \in R[x_1, .., x_n]$ by setting $f_* = f(x_1, ..., x_n, 1)$. Conversely, for any polynomial $f \in R[x_1, ..., x_n]$ of degree d, write $f = f_0 + \cdots + f_d$ where $f_i$ is a form of degree i and define $f^* \in R[x_1, ..., x_n, x_{n+1}]$ by setting

$$\begin{aligned} f^* &:= x_{n+1}^d f_0 + x_{n+1}^{d-1} f_1 + \cdots + f_d \\ &= x_{n+1}^d f(x_1/x_{n+1}, \cdots, x_n/x_{n+1}) \end{aligned}$$

and so, $f^*$ is a form of degree d.

So, $f_*$ gives us a way to make a form into a polynomial in lower dimensions while $f^*$ gives us a way to transform a polynomial into a form in higher dimensions.

**Proposition 62.** (1) $(fg)_* = f_* g_*$, and $(fg)^* = f^* g^*$
(2) if $f \neq 0$ and r is the highest power of $x_{n+1}$ that divides f, then $x_{n+1}^r (f_*)^* = f$. Also, $(f^*)_* = f$
(3) $(f+g)_* = f_* + g_*$, and $x_{n+1}^t (f+g)^* = x_{n+1}^r f^* + x_{n+1}^s g^*$ where $r = \deg(g), s = \deg(f)$ and $t = r + s - \deg(f+g)$

*Proof.* Proving just the first:
(1)

$$\begin{aligned}(fg)_* &= (fg)(x_1, ..., x_n, 1) \\ &= f(x_1, ..., x_n, 1) g(x_1, ..., x_n, 1) \\ &= f_* g_*\end{aligned}$$

$$\begin{aligned}(fg)^* &= x_{n+1}^d (fg)(x_1/x_{n+1}, ..., x_n/x_{n+1}) \\ &= x_{n+1}^{d_f} f(x_1/x_{n+1}, ..., x_n/x_{n+1}) x^{d_g} g(x_1/x_{n+1}, ..., x_n/x_{n+1}) \text{ where } d_f + d_g = d,\ d_f \text{ degree of } f \\ &= f^* g^*\end{aligned}$$

□

**Corollary 63.** Up to power of $x_{n+1}$, factoring a form $f \in R[x_1, ..., x)n]$ is the same as factoring $f_* \in R[x_1, ..., x_n]$. In particular, if $f \in k[x, y]$ is a form and k is algebraically closed then f factors into a product of linear factors.

*Proof.* Use previous proposition's part 1 and 2 to prove the first part. For the second, let y be st y does not divide g, then let $f = y^r g$. Then, $f_* = g_* = \epsilon \prod (x - \lambda_i)$ since k is algebraically closed, so $f = \epsilon y^r \prod (x - \lambda_i y)$ □

## 11.3 Direct Products of Rings

The cartesian product of rings is a ring with the operations $(a_1, ..., a_n) + (b_1, ..., b_n) = (a_1 + b_1, .., a_n + b_n)$ and $(a_1, ..., a_n)(b_1, ..., b_n) = (a_1 b_1, \cdots, a_n b_n)$. This ring is called the direct product of $R_1, \cdots, R_n$, denoted by $\prod_{i=1}^n R_i$.

Let $\pi_j : \prod_{i=1}^n R_i \to R_j$ which takes $a_1, \cdots, a_n$ to $a_j$ be the natural projection map which can easily be shown to be a ring homomorphism.

Given any ring R and ring homomorphisms $\psi_i : R \to R_i$ for $i = 1, \cdots, n$, there is a unique ring homomorphism $\psi : R \to \prod_{i=1}^{n} R_i$ such that $\pi_i \circ \psi = \psi_i$. In particular, if a field k is a subring of each $R_i$, k may be regarded as a subring of $\prod_{i=1}^{n} R_i$.

**Proposition 64.** Let I be an ideal in $k[x_1, ..., x_n]$ where k is algebraically closed. Suppose $V(I) = \{p_1, .., p_N\}$ is finite. Let $\mathscr{O}_i := \mathscr{O}_{p_i}(\mathbb{A}^n)$. Then, there is a natural isomorphism of $k[x_1, ..., x_n]/I$ with $\prod_{i=1}^{N} \mathscr{O}_i/I\mathscr{O}_i$.

The proof of this can be found in [1].

**Corollary 65.**

$$\dim_k(k[x_1, ..., x_n]/I) = \sum_{i=1}^{N} \dim_k(\mathscr{O}_i/I\mathscr{O}_i).$$

**Corollary 66.** If $V(I) = \{p\}$, then $k[x_1, ..., x_n]/I$ is isomorphic to $\mathscr{O}_p(\mathbb{A}^n)/I\mathscr{O}_p(\mathbb{A}^n)$.

# 12 Algebraic Curves I - plane curves

## 12.1 Preliminaries

**Definition 52.** Affine plane curve. First, we define an equivalence relation that is very reminscient of complex projective spaces:

An affine plane curve is the set of points in $\mathbb{A}^2$ at which $f \in k[x, y]$ vanishes. Therefore, the affine plane curve $X := \{(x, y) : f(x, y) = 0\}$.

Alternatively, we say that an affine plane curve is an equivalence class of non-constant polynomials under the equivalence relation of polynomials in $k[x, y]$: $f \sim g$ iff $f = \lambda g$ where $\lambda \in k$.

The degree of a curve is the degree of any representative of the curve. A curve of degree one is a line i.e $ax + by + c = 0$ or simply $ax + by + c$.

**Definition 53.** Components of an affine plane curve. If $f = \prod f_i^{e_i}$ where $f_i$ are irreducible factors of f, we say that $f_i$ are the components of f and $e_i$ is the multiplicity of the $f_i$.
If $e_i = 1$, $f_i$ is called a **simple component**. Otherwise, it is a **multiple component**.

If f is irreducible, then (f) is prime and so V(f) is irreducible variety in $\mathbb{A}^2$. We will often write O(f) to mean O(V(f)). Similarly, write k(f) instead of k(V(f)) and $\mathcal{O}_p(f)$ instead of $\mathcal{O}_p(V(f))$.

**Definition 54. Simple point, tangent line, non-singular curve.** Let f be a curve and let $p = (a, b) \in f$. The point p is called a simple point of f if either derivative $\frac{d}{dx}f(p) \neq 0$ or $\frac{d}{dy}f(p) \neq 0$. In this case, the line $\frac{d}{dx}f(p)(x - a) + \frac{d}{dy}f(p)(y - b) = 0$ is called the tangent line to f at p. A point that is not simple is called multiple (or singular). A curve with only simple points is called a non-singular curve.

**Definition 55. Multiplicity.** Let f be any curve and $p = (0, 0)$. Write $f = f_m + f_{m+1} + \cdots + f_n$, where $f_i \in k[x, y]$ of degree i and $f_m \neq 0$. We define m to be the multiplicity of f at $p = (0, 0)$ and write $m = m_p(f)$.

Couple of immediate properties (for p = (0,0)):
(1) $p \in f$ if and only if $m_p(f) > 0$.
(2) p is a simple point on f if and only if $m_p(f) = 1$ and in this case $f_1$ is the tangent line to f at p. If m = 2, p is called a double point. If m = 3, p is called a triple point and so on.

*Proof: Suppose* $p = (0,0) \in f$. *Then, if we write* $f = f_m + f_{m+1} + \cdot + f_n$ *and* $f_m \neq 0$, *then since* $f = 0$ *at* $p$, *each* $f_i$ *must disappear and so* $m > 0$ *(if* $m = 0$, *then* $f_m(p) \neq 0$ *since* $f_m \neq 0$*). Converse is straightforward.*

Given $f_m \in k[x,y]$ is a form, write $f_m = \prod_i g_i^{r_i}$ where each $g_i$ is a distinct line. The lines $g_i$ are called the tangent lines to f at $p = (0,0)$ and $r_i$ is called the multiplicity; $g_i$ is called simple tangent line if $r_i = 1$. If f has m distinct simple tangents at p, we say p is an ordinary multiple point of f. An ordinary double point is called a node.

Let $f = \prod_i f_i^{e_i}$ be the factorization of f into irreducible components. Then, $m_p(f) = \sum e_i m_p(f_i)$ and if L is a tangent line to $f_i$ with multiplicity $r_i$.

**Proposition 67.** A point p is a simple point of f if and only if p belongs to just one component $f_i$ of f where $f_i$ is a simple component of f and p is a simple point of $f_i$.

**Theorem 68.** Let f be an irreducible plane curve and let $p \in f$. Then, p is a simple point of f if and only if $\mathscr{O}_p(f) = \mathscr{O}_p(V(f))$ is a discrete valuation ring.

## 12.2 Intersection Number

Let f and g be plane curves with $p \in \mathbb{A}^2$. Our goal is to define what the intersection number of f and g is at p, denoted by $I(p, f \cap g)$.

**Desired properties of intersection number:**
We say that f and g intersect properly at p if f and g have no common component that passes through p.
(1) $I(p, f \cap g)$ is a nonnegative integer for any f, g and p such that f and g intersect properly at p. Also, $I(p, f \cap g) = \infty$ if f and g do not intersect properly at p.
(2) $I(p, f \cap g) = 0$ if and only if $p \notin f \cap g$. $I(p, f \cap g)$ depdends only on the components of f and g that pass through p. $I(p, f \cap g) = 0$ if f or g is a non-zero constant.
(3) If T is an affine change of coordinates on $\mathbb{A}^2$ and $T(q) = p$, then $I(p, f \cap g) = I(q, f^T \cap g^T)$.
(4) $I(p, f \cap g) = I(p, g \cap f)$

Two curves, f and g intersect transversally at p if p is a simple point on both f and on g and if the tangent line to f at p is different from the tangent line of g at p.

So,

(5) $I(p, f \cap g) \geq m_p(f) m_p(g)$, with equality occurring if and only if f and g have no tangent lines in common at p.

(6) If $f = \prod f_i^{r_i}$ and $g = \prod g_j^{s_j}$, then $I(p, f \cap g) = \sum_{i,j} r_i s_j I(p, f_i \cap g_j)$.

(7) $I(p, f \cap g) = I(p, f \cap (g + Af))$ for any $A \in k[x, y]$.

**Theorem 69.** There is a unique intersection number $I(p, f \cap g)$ defined for all plane curves $f, g$ and all points $p \in \mathbb{A}^2$ satisfying the properties (1) - (7). It is given by

$$I(p, f \cap g) = \dim_k(\mathscr{O}_p(\mathbb{A}^2)/(f, g))$$

# 13 Projective Space

## 13.1 Construction of Projective Space

Consider two curves: $y^2 = x^2 + 1$ and $y^2 = \alpha x$ where $\alpha \in k$. These two curves intersect at two points when $\alpha \neq \pm 1$. When $\alpha = \pm 1$, the curves do not intersect however the curve is asymptotic to the line. Our goal is to enlarge the xy plane to allow such curves to intersect *at infinity.*

Identity each $(x, y) \in \mathbb{A}^2$ with $(x, y, 1) \in \mathbb{A}^3$. Then, every point $(x, y, 1)$ determines a line that passes through itself and $(0, 0, 0)$. Note that every line through the origin in $\mathbb{A}^3$ corresponds to exactly one such point, unless the line is on the plane $z = 0$. We say that the lines through $(0, 0, 0)$ in $z = 0$ plane correspond to points at infinity.

**Definition 56. Projective n-space over** k, $\mathbb{P}^n_k$. This is defined to be the set of all lines through $(0, 0, \cdots, 0) \in \mathbb{A}^{n+1}_k$. Any point $(x) = (x_1, ..., x_n, x_{n+1}) \neq (0, \cdots, 0)$ determines a unique such line i.e $\{(\lambda x_1, \cdots, \lambda x_n) : \lambda \in k^\times\}$. Two such points are equivalent i.e determine the same line if and only if there exists a non-zero $\lambda \in k$ such that $y_i = \lambda x_i$ for $i = 1, ..., n, n+1$. Therefore, $\mathbb{P}^n$ is the set of equivalence classes of points in $\mathbb{A}^{n+1} \backslash \{(0, \cdots, 0)\}$. Elements of $\mathbb{P}^n$ are called points. If $p \in \mathbb{P}^n$ is determined by some $(x, \cdots, x_{n+1}) \in \mathbb{A}^{n+1}$, then we say $(x_1, ..., x_{n+1})$ are **homogenous coordinates** for p. We write $p = [x_1 : \cdots : x_{n+1}]$ to indicate that $(x_1, ..., x_{n+1})$ are homogenous coordinates for $p \in \mathbb{P}^n$. While $x_i$ itself is not well-defined (because of the equivalence), it is well-defined to say whether $x_i$ is 0 or not; if $x_i \neq 0$, then $\frac{x_j}{x_i}$ are well-defined

**Definition 57.** $U_i$. We let $U_i = \{[x_1 : \cdots : x_{n+1}] \in \mathbb{P}^n : x_i \neq 0\}$. Then, for any $p \in U_i$, p can be uniquely written as $p = [x_1 : \cdots : x_{i-1} : 1 : x_{i+1} : \cdots : x_{n+1}]$ which allows us to view $U_i$ as an affine n-space. Visualize $U_i$ as taking a sphere and cutting the space perpendicular to the i-th axis. The coordinates $(x_1, ..., x_{i-1}.x_{i+1}, ...., x_{n+1})$ are called the **non-homogenous coordinates** for p with respect to $U_i$.

If we define $\varphi_i : \mathbb{A}^n \to U_i$ by $\varphi_i(a_1, .., a_n) = [a_1 : \cdots : a_{i-1} : 1 : a_i : \cdots : a_n]$, then $\varphi_i$ sets up a one-to-one correspondence between points of $\mathbb{A}^n$ and the points of $U_i$. Note,

$$\mathbb{P}^n = \cup_i^{n+1} U_i$$

so $\mathbb{P}^n$ is covered by $n + 1$ sets each of which looks like affine n-space.

**Definition 58.** Hyperplane at infinity.

$$H_\infty = \mathbb{P}^n \backslash U_{n+1} = \{[x_1 : \cdots : x_{n+1}] : x_{n+1} = 0\}$$

Given there is a natural correspondence between $[x_1 : \cdots : x_n : 0]$ and $[x_1 : \cdots : x_n]$, $H_\infty$ can be indentified with $\mathbb{P}^{n-1}$ and so $\mathbb{P}^n = U_{n+1} \cup \mathbb{H}_\infty$

We will often use the following:

$$\mathbb{P}^n = H_\infty \cup U_{n+1}$$

*Examples:*
(1) $\mathbb{P}^0_k$ is a pont.
(2) $\mathbb{P}^1_k = \{[x : 1] : x \in k\} \cup \{[1 : 0]\}$. $\mathbb{P}^1_k$ is the affine line plus one point at infinity. $\mathbb{P}^1_k$ is the projective line over k.
(3) $\mathbb{P}^2_k = \{[x : y : 1] : (x, y) \in \mathbb{A}^2\} \cup \{[x : y : 0] : [x : y] \in \mathbb{P}^1\}$. Here $H_\infty$ is called the line at infinity. $\mathbb{P}^2_k$ is called the projective plane over k.
(4) Consider the line $y = mx + b$ in $\mathbb{A}^2$. Identify $\mathbb{A}^2$ with $U_3 \subset \mathbb{P}^2$, then the points on the line correspond to the points $y = mx + bz$ and $z \neq 0$. The set $\{[x : y : z] \in \mathbb{P}^2 : y = mx + bz\} \cap H_\infty = \{[1 : m : 0]\}$ so all lines with the same slope, when extended in this way, pass through the same point at infinity.
(5) Consider the curve $y^2 = x^2 + 1$. The corresponding set in $\mathbb{P}^2$ is given by the equation $y^2 = x^2 + z^2$ where $z \neq 0$. Then, $\{[x : y : z] \in \mathbb{P}^2 : y^2 = x^2 + z^2\}$ intersects $H_\infty$ in the two points $[1 : 1 : 0]$ and $[1 : -1 : 0]$. These are the points where the lines $y = x$ and $y = -x$ intersect the curve.

**Lemma 70.** $\mathbb{P}^n = \mathbb{P}^{n-1} \cup \mathbb{A}^n$

*Proof.*

$$\begin{aligned}\mathbb{P}^n &= H_\infty \cup U_{n+1} \\ &= \mathbb{A}^n \cup U_{n+1} \\ &= \mathbb{A}^n \cup \mathbb{P}^{n-1}\end{aligned}$$

□

**Proposition 71.** Let $L_1$ and $L_2$ be two projective lines in $\mathbb{P}^2$. Then, $L_1 \cap L_2 \neq \emptyset$; they intersect at a point if $L_1 \neq L_2$ or $L_1 \cap L_2 = L_1 = L_2$. However, in $\mathbb{A}^2$, two lines may have no intersection.

*Proof.* Let the 2 lines in $\mathbb{A}^2$ be $ax + by + c = 0$ and $a'x + b'y + c' = 0$. Now, if these lines are not parallel, they already intersect in $\mathbb{A}^2$. They would also intersect in $\mathbb{P}^2$ : replace x

and y with $\frac{x}{z}, \frac{y}{z}$ to write $ax + by + cz = 0, a'x + b'y + c'z = 0$, subtract the two equations to get $x = \frac{c-c'}{\frac{a}{b}-\frac{a'}{b'}}z$ where the denominator is not 0 since the two lines were not parallel. Now, suppose the two lines were parallel. Then, we can rewrite the lines in $\mathbb{P}^2$ as $ax+by+cz = 0$ and $ax + by + c'z = 0$ where $c \neq c'$. Take $z = 0$ and we now get $y = -\frac{a}{b}x$. So the two lines intersect [–b, a, 0]. Note that if $c = c'$, then the two lines are the same. □

## 13.2 Projective Variety

**Definition 59.** Zero of a polynomial in $\mathbb{P}^n$. A point $p \in \mathbb{P}^n$ is a zero of a polynomial $f \in k[x_1, ..., x_{n+1}]$ if $f(x_1, ...., x_{n+1}) = 0$ for every choice of homogenous coordinates $(x_1, ..., x_{n+1})$ for p. We say f(p) = 0. If f vanishes at one representative, then it vanishes at every representative of p.

**Proposition 72.** (1) Any polynomial $f \in k[x_1, \cdots, x_{n+1}]$ may be written as $f = f_0 + \cdots + f_r$ for $r = \deg(f)$ where $f_i$ is a homogenous polynomial of degree i.
(2) If f(p) = 0, then $f_i(p) = 0$ for any set of homogenous coordinates for p.

*Proof.* (1) follows from just writing f as a sum of monomials of degree i. We prove (2) now: given $f_i(p)$ is a homogenous polynomial, $f_i(tp) = t^i f_i(p)$. Then, $\psi(t) = f(tp) = \sum_i t^i f_i(p)$. Given f(tp) = 0 for all $t \neq 0$ i.e infinitely many t, then $\psi(t) \in k[t]$ has infinitely many 0s, so $\psi(t)$ is the zero polynomial i.e $f_i(p) = 0$ for all i. □

**Definition 60.** Projective varieties. For any set S of polynomials in $k[x_1, ..., x_{n+1}]$, we let

$$V(S) = \{p \in \mathbb{P}^n : p \text{ is a zero of each } f \in S\}.$$

Vanishing ideal. If I is the ideal generated by S, then V(I) = V(S). If $I = (f^{(1)}, \cdots, f^{(r)})$ where $f^{(i)} = \sum_j f_j^{(i)}$ where $f_j^{(i)}$ is a form of degree j, then $V(I) = V(\{f_j^{(i)}\}_{i,j})$ (see the first proposition of this section) is the set of zeros of a finite number of forms. Such sets are called projective varieties.

**Definition 61.** Vanishing ideal. Let $X \subset \mathbb{P}^n$, we let

$$I(X) = \{f \in k[x_1, ..., x_{n+1}] : f \text{ is zero on every p in X}\}.$$

An ideal $I \in k[x_1, .., x_{n+1}]$ is homogenous if for every $f = \sum_{i=0}^m f_i \in I$ where $f_i$ is a form of degree i, we also have $f_i \in I$. For any $X \subset \mathbb{P}^n$, I(X) is a homogenous ideal.

**Proposition 73.** An ideal $I \subset k[x_1, ..., x_{n+1}]$ is homogenous if and only if it is generated by a finite set of forms.

*Proof.* Suppose $I = (f^{(1)}, \cdots, f^{(r)})$ is homogenous, then I is generated by $\{f_j^{(i)}\}_{i,j}$. Conversely, suppose $S = \{f^{(\alpha)}\}$ be a set of forms generating an ideal I with $\deg(f^{(\alpha)}) = d_\alpha$ and suppose $f = f_m + \cdots + f_r \in I$ and $\deg(f_i) = i$. We need to show that $f_m \in I$ because then $f - f_m \in I$ and then by induction each $f_i$ would be in I. Let $f = \sum_\alpha a^{(\alpha)} f^{(\alpha)} \in I$. Comparing terms of the same degree, we can see that $f_m = \sum_\alpha a^{(\alpha)}_{m-d_\alpha} f^{(\alpha)}$, so $f_m \in I$. □

Similar to the affine case, $V \subset \mathbb{P}^n$ is irreducible if and only if I(V) is prime. Any algebraic variety can be written uniquely as a union of projective varieties, its irreducible components.

**Notation:** We use $V_p, I_p$ for projective operations and $V_a, I_a$ for affine ones.

**Definition 62.** Cone over V. If V is an algebraic variety in $\mathbb{P}^n$, we define

$$C(V) = \{(x_1, .., x_{n+1}) \in \mathbb{A}^{n+1} : [x_1 : \cdots : x_{n+1}] \in V \text{ or } (x_1, ..., x_{n+1}) = (0, \cdots, 0)\}.$$

If $V = \emptyset$, then $I_a(C(V)) = I_p(V)$,. If I is a homogenous ideal in $k[x_1, ..., x_{n+1}]$ s.t $V_p(I) \neq \emptyset$, then $C(V_p(I)) = V_a(I)$

## 13.3 Projective Nullstellensatz

**Theorem 74.** Projective Nullstellensatz. Let I be a homogenous ideal in $k[x_1, \cdots, x_{n+1}]$. Then,
(1) $V_p(I) = \emptyset$ if and only if there exists an integer N such that I contains all forms of degree $\geq N$.
(2) If $V_p(I) \neq \emptyset$, then $I_p(V_p(I)) = \sqrt{(I)}$.

*Proof.* For the first part: The following conditions are equivalent: (1) $V_p(I) = \emptyset$, (2) $V_a(I) \subset \{(0, \cdots, 0)\}$, (3) $\sqrt{(I)} = I_a(V_a(I)) \supset (x_1, ..., x_{n+1})$ (by taking I(–) of both sides in (2)) and (4) $(x_1, ..., x_{n+1})^N \subset I$.

For the second part: $I_p(V_p(I)) = I_a(C(V_p(I))) = I_a(V_a(I)) = \sqrt{I}$. □

## 13.4 Homogenous coordinate ring

**Definition 63.** Coordinate ring. Let I(V) be a **homogenous, prime** ideal and we call the residue ring $O_h(V) := k[x_1, \cdots, x_{n+1}]/I(V)$, which is an integral domain, is called the homogenous coordinate ring.

More generally, let I be any homogenous ideal in $k[x_1, \cdots, x_{n+1}]$ and let $k[x_1, ..., x_{n+1}]/I$ be a coordinate ring.

**Proposition 75.** Every element $f \in k[x_1, ..., x_{n+1}]/I$ (where I is homogenous) may be uniquely written as $f = f_0 + \cdots + f_r$ where $f_i$ is a form of degree i.

*Proof.* We already saw how to find one such decomposition. Suppose $f \in O_h(V)$ with $f = \sum_i f_i$. Suppose, we have another decomposition $f = \sum_i g_i$. Then, $f - \sum_i g_i = \sum_i (f_i - g_i) \in I$ and given I is homogenous, each $f_i - g_i \in I$ □

**Definition 64.** Homogenous function field. Let $k_h(V)$ be the quotient field of $O_h(V)$. This is called the homogenous function field of V. No elements of $O_h(V)$ except the constants determine functions on V (since we are in the projective space so $tx = x \in \mathbb{P}^n$ for nonzero t). However, if $f, g \in O_h(V)$ are both **forms** of the same degree d, then $\frac{f}{g}$ does define a function where g is not zero because then $\frac{f(\lambda s)}{g(\lambda s)} = \frac{\lambda^d f(x)}{\lambda^d g(x)} = \frac{f(x)}{g(x)}$ so $\frac{f}{g}$ is independent of our choice of homogenous coordinates in $\mathbb{P}^n$.

**Definition 65.** Function field. The function field of V, written k(V), is defined to be

$$\{z \in k_h(V) : \text{ for some forms of same degree } f, g \in O_h(V), z = \frac{f}{g}\}.$$

It is not difficult to verify that k(V) is a subfield of $k_h(V)$. So, $k \subset k(V) \subset k_h(V)$ but $O_h(V) \subsetneq k(V)$ and elements of k(V) are called rational functions on V.

Similarly, we can also define local rings and so on.

Let $p \in V$ and $z \in k(V)$. Then, z is defined at p if z can be written as $z = \frac{f}{g}$ where f, g are forms of the same degree and $g(p) \neq 0$. Then,

$$\mathcal{O}_p(V) = \{z \in k(V) : z \text{ is defined at p.}$$

We see that $\mathcal{O}_p(V)$ is a subring of k(V). It is a local ring, called the local ring of V at p, with the unique maximal ideal

$$m_p(V) = \{z \in k(V) : z = \frac{f}{g}, g(p) \neq 0, f(p) = 0\}$$

and the value z(p) of a function $z \in \mathcal{O}_p(V)$ is well-defined.

**Definition 66.** Homogenization. Given a polynomial $f(x_1, ..., x_n)$ of degree d, the homogenization with respect to $x_i$ is the polynomial $f(x_1/x_i, ...., x_n/x_i)x_i^d$. The dehomogenization of a polynomial $g(x_1, ..., x_n, z)$ is $g(x_1, ..., x_n, 1)$.

*Example:* $x^2 + y^2 + 1$ *can be homogenized to get* $z^2(x^2/x^2 + y^2/x^2 + 1) = x^2 + y^2 + z^2$. *On the other hand, the dehomogenizatino of* $x^2 + y^2 + z^2$ *is* $x^2 + y^2 + 1$.

**Definition 67.** Rational map between projective varieties. Let $X \subseteq \mathbb{P}^n$ and let $Y \subseteq \mathbb{P}^m$ be projective varieties. A rational map $f : X \to Y$ is a collection of homogenous polynomials of same degree :

$$[x_0, x_1, ..., x_n] \to [f_0(x), f_1(x), ..., f_m(x)],$$

such that $f(U) \subseteq V$ where U is an open subset of X where $f_i$ has no common zeros. We say two tuples $[f_i]$ and $[f_i']$ are equal if they agree on an open, dense subset of X. We say f is regular at $p \in X$ (or defined at $p \in X$) if we can find such $f_i$ with no common zero at p, so $f(p) \in Y$ is well-defined. A regular map $f : X \to Y$ is a rational map that is regular at every point of X.

# 14 Projective Plane Curves

**Definition 68.** Projective Plane Curve. A projective plane curve is a hypersurface in $\mathbb{P}^2$ but we allow multiple components: two non-constant forms $f, g \in k[x, y, z]$ are equivalent if there exists a nonzero $\lambda \in k$ such that $f = \lambda g$. So, a projective plane curve is an equivalence class of forms.

The degree of a curve is the degree of a defining form. Curves of degree 1, 2, 3 and 4 are called lines, conics, cubic and quartics, respectively.

**Notation: Once again, we will write $\mathscr{O}_p(f)$ to mean $\mathscr{O}_p(V(f))$ for an irreducible f.**

When $p = [x : y : 1]$, then $\mathscr{O}_p(f)$ is canonically isomorphic to $\mathscr{O}_{(x,y)}(f_*)$

If f is a projective plane curve and $p \in U_i$ where $i = 1, 2$ or 3, then, we can dehomogenize f with respect to $x_i$ and define the multiplicity of f at p, $m_p(f)$, to be $m_p(f_*)$. The multiplicitiy is independent of the choice of $U_i$ and invariant under projective change of coordinates.

We will require the following:

**Proposition 76.** Let $P = [x : y : z] \in \mathbb{P}^2$. Then, $\{(a, b, c) \in \mathbb{A}^3 : ax + by + cz = 0\}$ is a hyperplane in $\mathbb{A}^3$. Furthermore, for any finite set of points, $p_1, ..., p_n$, in $\mathbb{P}^2$, there is a line not passing through any of them.

*Proof.* The first part is straightforward. Write the set as $V(T_1x + T_2y + T_3z)$ which makes this a hyperplane. Now we prove the second part. Then, the proposition is saying, there exists $a, b, c \in k$ such that $p_i \cdot (a, b, c) \neq 0$ (these a, b and c determine the direction vector of the line). Let $p_i = (x_i, y_i, z_i)$. Suppose for contradiction this is false. Then, $p(x, y, z) = \prod_i^n (T_1x_i + T_2y_i + T_3z_i)$ vanishes at every point. Since k is infinite, this means $p(x, y, z) = 0$ so $(T_1x_i + T_2y_i + T_3z_i)$ is 0 for some i which means $p_i = 0$ which cannot be the case in $\mathbb{P}^2$. □

Let $p_1, ..., p_n \in \mathbb{P}^2$ be a finite set of points. Then, we can always find a line L that does not pass through any of the points. If f is a curve of degree d, then define

$$f_* := \frac{f}{L^d} \in k(\mathbb{P}^2).$$

If instead of L, we chose the line $L'$, then $f/L'^d = (L/L')^d f_*$ and $L/L'$ is a unit in each $\mathscr{O}_{p_i}(\mathbb{P}^2)$.

If p is a simple point on f i.e $m_p(f) = 1$ and f is irreducible, then $\mathscr{O}_p(f)$ is a discrete valuation ring (DVR). We let $\text{ord}_p^f$ be the corresponding order function on k(f). If g is a form in

$k[x, y, z]$ and $g_* \in \mathcal{O}_p(\mathbb{P}^2)$ is as defined above and $\bar{g_*}$ is the residue of $g_*$ in $\mathcal{O}_p(f)$ and we define $\text{ord}_p^f(g) = \text{ord}_p^f(\bar{g}_*)$.

## 14.1 Linear System of Curves

Let's work in projective space. Let $M_1, ..., M_N$ be a fixed ordering of a set of monomials in x, y, z of degree d where $N = \frac{1}{2}(d+1)(d+2)$. Given a curve f of degree d is the same thing as choosing $a_1, ..., a)N \in k$, not all zero, and letting $f = \sum_i a_i M_i$ except that $(a_1, ..., a_N)$ and $(\lambda a_1, ..., \lambda a_N)$ determine the same curve. So, each curve f of degree d corresponds to a unique point in $\mathbb{P}^{N-1} = \mathbb{P}^{d(d+3)/2}$ and, conversely, each point in $\mathbb{P}^{d(d+3)/2}$ represents a unique curve.

Therefore, we often identify the curve f of degree d with a point of $\mathbb{P}^{d(d+3)/2}$. This is why we often say

*Example:* (1) For d = 1, each line $ax + by + cz$ corresponds to the points $[a : b : c] \in \mathbb{P}^2$.
(2) For d = 2, the conic $ax^2 + bxy + cxy + dy^2 + eyz + fz^2$ corresponds to the points [a : b : c : d : e : f] $\in \mathbb{P}^5$. The conics form a $\mathbb{P}^5$. Similarly, the cubics form a $\mathbb{P}^9$ and the quartics form $\mathbb{P}^1 4$

**Lemma 77.** (1) Let $p \in \mathbb{P}^2$ be a fixed point. The set of curves of degree d that contain p forms a hyperplane in $\mathbb{P}^{d(d+3)/2}$.
(2) If $T : \mathbb{P}^2 \to \mathbb{P}^2$ is a projective change of coordinates, then the map $f \to f^T$ from {curves of degree d} to {curves of degree d} is a projective change of coordinates on $\mathbb{P}^{d(d+3)/2}$.

*Proof.* (1) If p = [x : y : z], thenthe curve corresponding to $(a_1, ..., a_N) \in \mathbb{P}^{d(d+3)/2}$ passes through p if and only if $\sum a_i M_i(x, y, z) = 0$. Since not all $M_i$ are 0, the $[a_1 : \cdots : a_N]$ satisfying this equation form a hyerplane. □

## 14.2 Bezout's Theorem

**Theorem 78.** Let f and g be projective plane curves of degree m and n respectively. Assume f and g have no common component. Then, $\sum_p I(p, f \cap g) = mn$.

**Corollary 79.** If f and g have no common component, then $\sum_p m_p(f)m_p(g) \leq \deg(f)\deg(g)$

**Corollary 80.** If f and g meet in mn distinct points, $m = \deg(f), n = \deg(g)$, then these points are all simple points on f and g.

**Corollary 81.** If two curves of degree m and n have more than mn points in common, then they have a common component.

# 15 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; $\text{Mor}(B, C) \times \text{Mor}(A, B) \to \text{Mor}(A, C)$. 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** $\text{id}_A : A \to A$ such that $f \circ \text{id}_A = f$ and $\text{id}_A \circ f = f$. 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 $f \circ g = \text{id}_B$ and $g \circ f = \text{id}_A$

**Definition: Automorphism.** The set of invertible elements of 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 $\text{Vec}_k$ 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 $F : \text{obj}(\mathscr{A}) \to \text{obj}(\mathscr{B})$ 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 $F(\text{id})_A = \text{id}_{F(A)}, \forall A \in \mathscr{A}$. 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 $F : \text{obj}(\mathscr{A}) \to \text{obj}(\mathscr{B})$. The other is mapping morphisms in one category to morphisms in another one by taking the "shadow" of the morphism i.e $F(\cdot) : \text{Mor}(\text{obj}(\mathscr{A}), \text{obj}(\mathscr{A})) \to \text{Mor}(\text{obj}(\mathscr{B}), \text{obj}(\mathscr{B}))$

*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 $\text{Vec}_k$ to the category of sets by sending each vector space to its underlying set. Furthermore, F sends each morphism m in $\text{Vec}_k$ 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 $\text{Mor}_{\mathscr{A}}(A, A') \to \text{Mor}_{\mathscr{B}}(F(A), F(A'))$ 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 $F : \text{obj}(\mathscr{A}) \to \text{obj}(\mathscr{B})$ 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 $F(id)_A = id_{F(A)}, \forall A \in \mathscr{A}$. Therefore, $F(m_1 \circ m_2) = F(m_2) \circ F(m_1)$.

*Example:* Consider the category $\text{Vec}_k$ 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 $A \in \text{obj}(\mathscr{C})$. We first define a covariant functor :
$h^A$ : obj$\mathscr{C}$ $\to$ (some morphism between sets in S) and in particular $h^A(B \in \text{obj}(\mathscr{C}) \in \text{Mor}(A, B)$. Furthermore, given $f \in \text{Mor}(B_1, B_2)$ in category $\mathscr{C}$, $h^A$ will send f to a morphism from $\text{Mor}(A, B_1)$ to $\text{Mor}(A, B_2)$ and in particular $h^A(f \in \text{Mor}(B_1, B_2)(g \in \text{Mor}(A, B_1)) = (f \circ g) \in \text{Mor}(A, B_2)$.

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

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:

$$\begin{array}{ccc} F(A) & \xrightarrow{F(f)} & F(A') \\ {\scriptstyle m_A}\downarrow & & \downarrow{\scriptstyle m_{A'}} \\ G(A) & \xrightarrow[G(f)]{} & G(A') \end{array}$$

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 $id_{\mathscr{B}}$ and $F' \circ F$ is naturally isomorphic to $id_{\mathscr{A}}$ 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 82.** 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.

## B.1 Rings, Ideals and Domains

**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 ∈ I}. A subset I of R is a left ideal of R if I is a subring of R and rI ⊆ I, ∀r ∈ R. A subset I of R is a right ideal of R if I is a subring of R and Ir ⊆ I, ∀r ∈ R. If I is both a left and right ideal, it is called an ideal of R.

If R is commutative, then RA = AR = RAR = (A).

**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), ∀r, s ∈ 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 → S is a ring homomorphism, then ker($\psi$) is an ideal of R, Im($\psi$) is a subring of S and R/ker($\psi$) ≅ $\psi$(R).
(2) If I is an ideal of R, then the map R → R/I defined by r → 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 ≠ R.

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

**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 ∩ B is an ideal of A and (A + B)/B ≅ A/(A ∩ B).

**Third Isomorphism Theorem for Rings.** Let I and J be ideals of R with I ⊆ J. Then, J/I is an ideal of R/I and (R/I)/(J/I) ≅ (R/J).

**Fourth/Lattice Isomorphism Theorem for Rings.** Let I be an ideal of R. The correspondence A ↔ A/I is an inclusion-preserving bijection between the sets of subrings A of R (if A ⊆ B and both contain I, then A/I ⊆ 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* $\bar{a}\bar{b} = \bar{a}\bar{b} = 0$ *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.*

(Skipping notes on Euclidean domains and only adding notes on PID, UFD insofar as they seemed immediately important to the the Algebraic Geometry notes)

**Definition: Principal Ideal Domain (PID).** A PID is an integral domain in which every

ideal is principal.

*Example:* $\mathbb{Z}$ is a PID.

**Proposition:** Every non-zero prime ideal in a PID is a maximal ideal.

**Corollary:** If R is any commutative ring such that the polynomial ring R[x] is a PID, then R is necessarily a field.

**Definition: Irreducible, prime and associate.** Let R be an integral domain.
(1) Let $x \in R$ such that x is not a unit. Then x is irreducible in R if $x = ab$ where $a, b \in R$ implies either a or b is a unit in R.
(2) A non-zero element $x \in R$ is called a prime in R if the ideal (x) generated by x is a prime ideal. Equivalently, $x \neq 0$ is a prime if it is not a unit and whenever x divides $ab \in R$, either x divides a or x divides b.
(3) Two elements x and y of R are associate if $x = uy$ for some unit $u \in R$.

**Proposition:** In an integral domain, a prime element is always irreducible.

**Proposition: prime = irreducible in PID.** In a PID, a non-zero element x is a prime if and only if it is irreducible.

**Definition: Unique factorization domain (UFD)** A unique factorization domain is an integral domain R in which every non-zero $x \in R$ which is not a unit has the following properties:
(1) x is a finite product of irreducible $p_i$ (not necessarily distinct) of R; $x = p_1 \cdots p_r$
(2) The decomposition is unique up to associates i.e $x = q_1 \cdots q_m$ is another decomposition, then m = r and after renumpering $p_i$ is associate to $q_i$ for all i.

*Example:* **A field** F **is a UFD.**

*Example:* **Every PID is a UFD**

*Example:* **When R is a UFD, R[x] is also a UFD.**

**Proposition: prime = irreducible in UFD.** In a UFD, a non-zero element x is a prime if and only if it is irreducible.

**Proposition:** Every PID is a UFD.

## B.2 Polynomial Rings

We already saw the following before:

**Proposition 1:** Let R be an integral domain. Then: (a) $\deg(p(x)q(x)) = \deg(p(x)) + \deg(q(x))$ given $p(x), q(x)$ are non-zero. (b) The units of R[x] are the units of R. (c) R[x] is an integral domain.

**Proposition 2: Quotient of polynomial ring.** Let I be an ideal of the ring R. Then, $R[x]/I[x] \cong (R/I)[x]$. In particular, if I is a prime ideal of R, then I[x] is a prime ideal of R[x].

*Proof: Consider map* $\varphi : R[x] \to (R/I)[x]$ *by taking each coefficient mod* I*; this is easily seen to be a ring homomorphism. Then,* $\ker(\varphi) = I[x]$ *proves first part. For the second, since* I *is prime,* R/I *is integral domain (by previous proposition) so* (R/I)[x] *is an integral domain and so* I[x] *is a prime ideal of* R[x].

**Note: It is *not* true that if** I **is a maximal ideal of** R**, then** I[x] **is a maximal ideal of** R[x]**. However, if** I **is maximal in** R**, then the ideal of** R[x] **generated by** I **and** x **is maximal in** R[x]**.**

**Definition: Polynomial ring of more than one variables.** The polynomial ring in the variables $x_1, \cdots, x_n$ with coefficients in R denoted by $R[x_1, \cdots, x_n]$ is defined inductively by $R[x_1, \cdots, x_n] = R[x_1, \cdots, x_{n-1}][x_n]$.

A polynomial in a polynomial ring of more than one variable is a finite sum of elements of the form $ax_1^{d_1} \cdots x_n^{d_n}$ where $a \in R, d_i \geq 0$ which are called the monomial terms. For a monomial term, if $a = 1$, we call it a monic term. A monomial term of this form is of degree $d = d_1 + \cdots + d_n$ and the n-tuple $(d_1, \cdots, d_n)$ is the multidegree of the term.

If f is a non-zero polynomial in n variables, the sum of all monomial terms in f of degree k is called the homogenous component of f of degree k. If f has degree d, then f may be written uniquely as the sum $f_0 + \cdots + f_d$ where $f_k$ is the homogenous component of f of degree k.

Now we look at polynomials whose coefficients are in a field:

**Theorem 3: Polynomial rings that are Euclidean Domains.** Let F be a field. The polynomial ring F[x] is a Euclidean Domain. If $a(x), b(x)$ are two polynomials in F[x] with $b(x) \neq 0$, then there are unique $q(x), r(x) \in F[x]$ such that $a(x) = q(x)b(x) + r(x)$ with $r(x) = 0$ or degree r(x) < degree b(x).

*Sketch of proof: Use induction. Let* $\deg(a(x)) = n, \deg(b(x)) = m$. *If* $a(x) = 0$, *then* $q(x) = r(x) = 0$. *If* $n < m$, *let* $q(x) = 0, r(x) = a(x)$. *So let* $n \geq m$. *Construct* q(x) - *if* $a(x) = \sum_{i=0}^{n} a_i x^i, b(x) =$

$\sum_{i=0}^{m} b_i x^i$. *Define* $a'(x) = a(x) - \frac{a_n}{b_m} x^{n-m} b(x)$ *designed to subtract leading term from* $a(x)$. *By inductive hypothesis,* $a'(x) = q'(x)b(x) + r(x)$. *With* $q(x) = q'(x) + \frac{a_n}{b_m} x^{n-m}$. *To prove uniqueness, assume there is another decomposition with* $q_1(x), r_1(x)$ *and leverage the fact that degree of* $f(x)g(x)$ *is the sum of degree* $f(x)$ *and degree* $g(x)$.

**Corollary 4:** If F is a field, then F[x] is a Principal Ideal Domain (PID) an a Unique Factorization Domain (UFD).

Now we look at polynomial rings that UFDs.

**Proposition 5: Gauss's Lemma.** Let R be a UFD with a field of fractions F and let $p(x) \in R[x]$. If $p(x)$ is reducible in F[x], then $p(x)$ is reducible in R[x]. More precisely, if $p(x) = A(x)B(x)$ for some non-constant polynomials $A(x), B(x) \in F[x]$, then there are non-zero elements $r, s \in F$ such that $rA(x) = a(x)$ and $sB(x) = b(x)$ both in R[x] and $p(x) = a(x)b(x)$ is a factorization in R[x].

*Sketch of proof for* R *a field: Let* $p(x) = A(x)B(x)$ *where on RHS, coefficients are in* F. *Multiply both sides by a common denominator for all coefficients to get* $dp(x) = a'(x)b'(x)$ *where on RHS we have elements in R[x],* $d \neq 0 \in R$. *If* d *is unit, we are done with* $a(x) = d^{-1}a'(x)b'(x)$. *Check Dummit and Foote for the proof in the case where* d *is not a unit.*

**Corollary:** Let R be a UFD. Let F be its field of fractions and let $p(x) \in R[x]$. Suppose the greatest common divisor of the coefficients of $p(x)$ is 1. Then $p(x)$ is irreducible in R[x] if and only if it is irreducible in F[x]. In particular, if $p(x)$ is a monic poynomial that is irreducible in R[x], then $p(x)$ is irreducible in F[x].

*Proof:* By Gauss's Lemma, if $p(x)$ is reducible in F[x], then it is reducible in R[x]. Conversely, suppose the gcd of coefficients of $p(x)$ is 1. If p is reducible with $p(x) = a(x)b(x)$, then neither $a(x)$ nor $b(x)$ are constant polynomials - this factorization also shows $p(x)$ is reducible in F[x].

**Theorem:** R is a UFD if and only if R[x] is a UFD.

**Corollary:** If R is a UFD, then a polynomial ring in an arbitrary number of variables with coefficients in R is also a UFD.

Now we look at **irreducible criteria** of polynomials.

We will require the following throughout the AG notes:

**Proposition:** Let R be a field. The prime ideals of R[y] are the zero ideal (0), the ideals (f(y)) where f is irreducible.

*Proof:* Given R is a field, R[x] is a PID. If (f) is a prime ideal in R[x], then f is prime which

means f is irreducible.

**Proposition:** Let F be a field and let $p(x) \in F[x]$. Then $p(x)$ has a factor of degree one if and only if $p(x)$ has a root in R i.e there is an $\alpha \in F$ with $p(\alpha) = 0$.

*Proof: If* $p(x)$ *has a factor of degree 1, then since* F *is a field, we may assume the factor is of the form* $(x - a), a \in F$. *Then,* $p(a) = 0$. *Conversely, if* $p(a) = 0$, *then by division algorithm in* F[x] - *theorem 3 in this section* - $p(x) = q(x)(x - a) + r$ *where* r *is constant and since* $p(a) = 0, r = 0$ *so* $(x - a)$ *is a factor.*

**Proposition:** A polynomial of degree two or three over a field F is reducible if and only if has a root in F.

**Proposition:** Let $p(x) = a_0 + a_1x + \cdots + a_nx^n$ be a polynomial of degree n with integer coefficients. If $r/s \in \mathbb{Q}$ is in its lowest term (i.e r and s are relatively prime integers) and r/s is a root of p(x), then r divides the constant term and s divides the leading coefficient of p(x) i.e $r \mid a_0$ and $s \mid a_n$. In particular, if p(x) is a monic polynomial with integer coefficients and $p(d) \neq 0$ for all integers d dividing the constant term of p(x), then p(x) has no roots in $\mathbb{Q}$.

The following are very important results:

**Proposition:** Let I be a proper ideal in the integer domain R and let p(x) be a nonconstant monic polynomial in R[x]. If the image of p(x) in (R/I)[x] cannot be factored in (R/I)[x] into two polynomials of smaller degree, then p(x) is irreducible in R[x].

*Proof: Suppose p(x) cannot be factored in (R/I)[x] but p(x) is reducible in R[x] so* $p(x) = a(x)b(x)$ *where both a(x) and b(x) are monic, nonconstant in R[x]. But then reducing the coefficients modulo I gives a factorization in (R/I)[x] - contradiction.*

**Proposition: Einsenstein's Criterion.** Let P be a prime ideal of the integral domain R and let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ be a polynomial in R[x] ($n \geq 1$). Suppose $a_{n-1}, a_n, \cdots, a_1, a_0$ are all elements of P and suppose $a_0$ is not an element of $P^2$. Then f(x) is irreducible in R[x].

**Proposition:** The maximal ideals in F[x] are the ideals (f(x)) generated by irreducible polynomials in f(x). In particular, F[x]/(f(x)) is a field if and only if f(x) is irreducible.

**Proposition:** Let g(x) be a nonconstant element of F[x] and let $g(x) = f_1(x)^{n_1}f_2(x)^{n_2}\cdots f_k(x)^{n_k}$ be its factorization into irreducibles, where the $f_i(x)$ are distinct. Then, we have the following isomorphism of things:

$$F[x]/(g(x)) \cong F[x]/(f_1(x)^{n_1}) \times F[x]/(f_2(x)^{n_2}) \times \cdots \times F[x]/(f_k(x)^{n_k})$$

**Proposition:** I the polynomial f(x) has roots $a_1, ..., a_k \in F$ (not necessarily distinct), then f(x) has $(x - a_1) \cdots (x_{a_k})$ as a factor. In particular, a polynomial of degree n in one variable over a field F has at most n roots in R, even counted with multiplicity.