Algebraic Geometry

Jubayer Ibn Hamid

1 Terminology

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

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

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

For a subset $X \subseteq \mathbb{A}_k^n$, consider the ideal in $k[x_1, ..., x_n]$ generated by polynomials that vanish on X. This ideal is called the 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) $I(\emptyset) = k[x_1, ..., x_n], I(\mathbb{A}^n) = \emptyset, I(\{a\}) = (x_1 - a_1, ..., x_n - a_n)$.

A polynomial mapping $p : V \to W$, 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 $\text{Map}(V, W)$ is the set of all morphisms from V to W and in our case this is the set of all polynomial maps from V to W.

2 Hilbert Basis Theorem

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

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

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 $\{f_{jm}\}$ 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 $g \in I'$. □

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. □

3 Modules Revision

Definition 2. *R-Module.*

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

Definition 3. *Submodule.*

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

One can check that $0_R m = 0_M$ 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 $\{\sum_i r_i s_i | r_i \in R, s_i \in S\}$.

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 $S = \sum Rv_i$ where $v_1, ..., v_n \in S$.

(2) S is <u>ring-finite over R</u> if $S = R[v_1, ..., v_n] = \{\sum_i a_i v_1^{i_1} \cdots v_n^{i_n} | a_i \in R\}$ 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 $v_1, ..., v_n \in S$.

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, $K(X)$ is a finitely-generated field extension of K. Now, suppose K is ring-finite over K. Then, $L = K[v_1, ..., v_n]$. Then, there exists $\frac{s_i}{t_i} \in K(X)$ that generate

L where $i = 1, ..., n$. Define $p := 1/q$. Then, as $p \in K(X)$, $p = \frac{h}{t_1^{e1} \cdots t_n^{en}}$. Now, if we choose q to be an irreducible polynomial that has a higher degree than all 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 $a_i \in R$.

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

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

(1) v is integral over R.

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

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

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

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

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

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

We will require the following results:

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

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

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

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

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

Lastly,

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

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

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

4 Nullstellensatz Version 1

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. $\square$

Assume k is algebraically closed.

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

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

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

The fact that every proper ideal in the polynomial ring over n variables is of the form $(x_1 - a_1, ..., x_n - a_n)$ is an interesting takeaway.

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

5 Irreducible Components of Algebraic Sets

Definition 7. *Irreducible decomposition of a set. Let $V \in \mathbb{A}_k^n$ 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 $\mathbb{A}_k^n$ i.e $V_i \neq V$ for $i = 1, 2$. If V is not irreducible, we call it reducible.*

Theorem 11. *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. $\square$

Theorem 12. *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. $\square$

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 13. *Let V be an algebraic set in $\mathbb{A}_k^n$. 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 $\mathcal{F} := \{\text{algebraic set} V \in \mathbb{A}_k^n : V \text{is not the union of finitely many irreducible algebraic sets}\}$.

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

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

Furthermore, we use the following terms:

Definition 8. *An idea $I \subset k[x_1, ..., x_n]$ 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 14. *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 morphisms:

Definition 9. *Isomorphic affine varieties. Two affine varieties $V \subset \mathbb{A}^n$ and $W \subset \mathbb{A}^m$ are isomorphic if there exists morphism $f : V \to W$ and $g : W \to V$ such that $f \circ g = g \circ f = i_d$.*

Lastly, we will require the following useful result for the section on Zariski topology.

Theorem 15. *Let $Z \subset \mathbb{A}^n$ be an affine variety and let $x \in \mathbb{A}^n - Z$. Then, there exists $f \in k[x_1, ..., x_n]$ such that $f(Z) = 0$ and $f(x) \neq 0$.*

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

6 Zariski Topology

Definition 10. *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, $V(f_1, ..., f_m) \cup V(h_1, ..., h_r) = V(\sum_{i,j} f_i h_j)$

Theorem 16. *The pre-image of an affine variety under a morphism $p : V \to W$ is a variety.*

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. □

Definition 11. *Coordinate Ring. Let $V \subset \mathbb{A}^n$ be an affine variety. The coordinate ring of functions on V is*

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

is the quotient ring of polynomials in n-variables.

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

Definition 12. *First, we define $\underline{V(f)_X := V(f) \cap X}$ where $X \subset \mathbb{A}^n$ is an affine variety. Now, we define basic closed sets of X be sets of the form $V(f)_X$. 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 $D(f)_X = X - V(f)$.*

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 17. *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. □

7 Coordinate Rings

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

Definition 13. *Let k be a field. Let R be a vector space over k equipped witha binary operation $R \times R \to R$ such that for any $x, y, z \in R$ and $a, b \in k$, we have $(x+y)z = xz+yz, z(x+y) = zx + zy, (ax)(by) = (ab)(xy)$.*

Theorem 18. *$O(X) \cong Map(X, \mathbb{A}^1)$. Here, $Map(X, \mathbb{A}^1)$ is a commutative k-algebra under addition and multiplication on $\mathbb{A}^1$. Furthermore, $O(X)^m \cong Map(X, \mathbb{A}^m)$*

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

Corollary 19. *Given X and Y are affine varieties, $X \cong Y$ implies $O(X) \cong O(Y)$.*

Let $\mathrm{Mor}_k(R_1, R_2)$ be th set of morphisms between 2 k-algebras R_1 and R_2. With this, we can define the pullback function:

Definition 14. *Given $X \in \mathbb{A}^n$, $Y \in \mathbb{A}^m$ are affine varieties, $p \in Map(X, Y)$, define p^* to be the map $p^* : Mor_k(O(Y), O(X))$, $p^*(f) = f \circ p$.*

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

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

Theorem 20. *Let $V \subset \mathbb{A}^n$ and $W \subset \mathbb{A}^m$ be affine varieties. There exists a natural 1-1 correspondence between $Map(V, W)$ and $Mor_k(O(W), O(V))$.*

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

Let $s, s' \in \mathrm{Map}(V, W)$ 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 $f_1 = x_i \circ s = s^*(x_1) = s'^*(x_i) = x_i \circ s' = f'_i$. 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 $\lambda \in \mathrm{Mor}_k(O(W), O(V))$. We construct a map $s \in \mathrm{Map}(V, W)$ 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 $g(f_1, ..., f_m) = g(\lambda(y_1), ..., \lambda(y_m)) = \lambda g = 0$.

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

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

$\square$

8 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.*