Introduction to Algebraic Geometry

George Voutsadakis[1]

[1]Mathematics and Computer Science
Lake Superior State University

LSSU Math 500

1. Affine Varieties
   - Hilbert's Nullstellensatz
   - Polynomial Functions and Maps
   - Rational Functions and Maps

Subsection 1

Hilbert's Nullstellensatz

The Map V

- Denote by
$$A := k[x_1, \ldots, x_n]$$
the polynomial ring in n variables over the field k.
- We defined the **zero set** of an ideal $J \subseteq A$,
$$V(J) := \{P \in \mathbb{A}_k^n : f(P) = 0, \text{ for all } f \in J\}.$$
- We showed that this gives rise to a surjective map
$$\begin{array}{rcl} V : \{\text{ideals in } A\} & \to & \{\text{algebraic sets in } \mathbb{A}_k^n\}, \\ J & \mapsto & V(J). \end{array}$$

The Map I

- In the reverse direction, consider a subset $X \subseteq \mathbb{A}_k^n$.
- Define an ideal

$$I(X) := \{f \in A : f(P) = 0, \text{ for all } P \in X\}.$$

- We now have a map

$$\begin{array}{rcl} I : \{\text{subsets of } \mathbb{A}_k^n\} & \to & \{\text{ideals in } A\}, \\ X & \mapsto & I(X). \end{array}$$

On the Injectivity and Surjectivity of V and I

- The map V is not injective.

  Example: For all $k \geq 1$, we have

$$V(x_1, \ldots, x_n) = V(x_1^k, \ldots, x_n^k).$$

- The map I is neither injective nor surjective.

  Example: In the case of $\mathbb{A}_k^1$, we have

$$I(\mathbb{Z}) = I(\mathbb{A}_k^1) = (0).$$

  For $n \geq 2$, the ideal (x^n) is not in the image of I.

- As a corollary of Hilbert's Nullstellensatz, we will see that, when restricted to certain subclasses of ideals and algebraic sets, respectively, V and I become mutually inverse bijections.

Properties of the Map V

Lemma

The map V satisfies the following:

(1) $V(0) = \mathbb{A}_k^n$, $V(A) = \emptyset$;

(2) $I \subseteq J \Rightarrow V(J) \subseteq V(I)$;

(3) $V(J_1 \cap J_2) = V(J_1) \cup V(J_2)$;

(4) $V(\sum_{\lambda \in \Lambda} J_\lambda) = \bigcap_{\lambda \in \Lambda} V(J_\lambda)$.

- The only nontrivial statement is (3).
  - $\supseteq$: Let $P \in V(J_1) \cup V(J_2)$. We may assume that $P \in V(J_1)$.
    Then, for any $g \in J_1 \cap J_2$, we have $g(P) = 0$.
    It follows that $P \in V(J_1 \cap J_2)$.
  - $\subseteq$: Take $P \notin V(J_1) \cup V(J_2)$.
    Then there exist $f \in J_1$ and $g \in J_2$, with $f(P) \neq 0$ and $g(P) \neq 0$.
    This implies that $fg(P) \neq 0$.
    Since $fg \in J_1 \cap J_2$, $P \notin V(J_1 \cap J_2)$.

Composing I and V

Lemma

The maps I and V have the following properties:

(1) $X \subseteq Y \Rightarrow I(X) \supseteq I(Y)$;

(2) For every subset $X \subseteq \mathbb{A}_k^n$, we have $X \subseteq V(I(X))$.
Equality holds if and only if X is algebraic.

(3) If $J \subseteq A$ is an ideal, then $J \subseteq I(V(J))$.

- Statements (1) and (3) are obvious.
  The relationship $X \subseteq V(I(X))$ is also clear.
  Suppose $X = V(I(X))$. Then X is algebraic by definition.
  Conversely, suppose X is closed. Then $X = V(J_0)$, for some ideal J_0.
  In particular, $J_0 \subseteq I(X)$. So $V(I(X)) \subseteq V(J_0) = X$.

Example

- In general
$$J \subseteq I(V(J))$$
is a strict inclusion.
- Consider
$$J = (x_1^k, \ldots, x_n^k), \quad k \geq 2.$$
- Then
$$I(V(J)) = (x_1, \ldots, x_n).$$

Radical Ideals

Definition (Radical Ideal)

For an ideal J in a ring R, the **radical** of J is defined by

$$\sqrt{J} := \{r : \text{there exists } k \geq 1, \text{ with } r^k \in J\}.$$

We call an ideal J a **radical ideal** if $J = \sqrt{J}$.

- It follows from the binomial theorem that $\sqrt{J}$ is an ideal.
- Clearly, we always have $J \subseteq \sqrt{J}$.
- Any ideal of the form $I(X)$ is automatically a radical ideal.
- So radical ideals play a significant role in the relationship between ideals and varieties.

Prime Ideals are Radical

- Consider a prime ideal J in a ring R.

  This means that, for all $x, y \in R$,

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

  In particular, for all $x \in R$ and all $k \geq 1$,

  $$x^k \in J \quad \text{implies} \quad x \in J.$$

  Now, let $x \in \sqrt{J}$.

  Then $x^k \in J$, for some $k \geq 1$.

  Hence, $x \in J$.

  This shows that $\sqrt{J} \subseteq J$.

  Therefore, J is radical.

The Zariski Topology

- Algebraic sets are called **Zariski closed** because they satisfy the axioms for the closed sets of a topology.
- The associated topology on $\mathbb{A}_k^n$ is called the **Zariski topology**.
- A subset of $\mathbb{A}_k^n$ is called **Zariski open** if its complement is Zariski closed.
- The Zariski topology is very different from the topology studied in real or complex analysis.
- E.g., the Zariski topology is not Hausdorff.
- The Zariski topology on $\mathbb{A}_k^n$ induces a topology on every subset of $\mathbb{A}_k^n$.

Example

- Consider the Zariski topology on $\mathbb{A}_k^1$.
- The empty set and $\mathbb{A}_k^1$ are simultaneously open and closed.
- Since k is algebraically closed, every ideal $J \subseteq k[x]$ is a principal ideal. It can be written as

$$J = ((x - a_1) \cdot \cdots \cdot (x - a_n)).$$

- Thus, the Zariski closed subsets of $\mathbb{A}_k^1$, different from $\emptyset$ and $\mathbb{A}_k^1$, are precisely the finite subsets.
- Hence, every nonempty Zariski open subset of $\mathbb{A}_k^1$ is dense.

Irreducible Algebraic Sets

Definition (Irreducible Algebraic Set)

An algebraic subset X is called **irreducible** if there is no decomposition

$$X = X_1 \cup X_2, \quad X_1, X_2 \subsetneq X$$

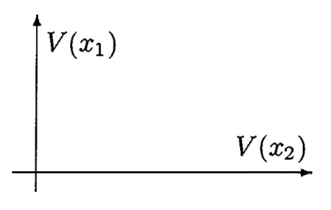
into proper algebraic subsets X_1, X_2. Otherwise X is called **reducible**.

Example: Consider the subset

$$V(x_1 x_2) \subseteq \mathbb{A}_k^2.$$

It is reducible, since

$$V(x_1 x_2) = V(x_1) \cup V(x_2).$$



Irreducible Algebraic Sets and Prime Ideals

Proposition

Let $X \neq \emptyset$ be an algebraic set, with corresponding ideal $I(X)$. Then X is irreducible if and only if $I(X)$ is a prime ideal.

- Assume X is reducible.

  Then, there is a decomposition

  $$X = X_1 \cup X_2,$$

  for some algebraic subsets $X_1, X_2 \subsetneq X$.

  Since $X_1 \subsetneq X$, there exists $f \in I(X_1) \backslash I(X)$.

  Since $X_2 \subsetneq X$, there exists $g \in I(X_2) \backslash I(X)$.

  Thus, fg vanishes on $X_1 \cup X_2 = X$. So $fg \in I(X)$.

  This shows that $I(X)$ is not prime.

Irreducible Algebraic Sets and Prime Ideals (Cont'd)

- Suppose that $I(X)$ is not prime.

  Then, there exist $f, g \in A$, with $fg \in I(X)$, but $f, g \notin I(X)$.

  Let
  $$J_1 := (I(X), f) \quad \text{and} \quad J_2 := (I(X), g).$$

  Then $X_1 = V(J_1)$ and $X_2 = V(J_2)$ are proper subsets of X.

  On the other hand, for $P \in X$ we have $fg(P) = 0$.

  So $f(P) = 0$ or $g(P) = 0$.

  This implies that $P \in X_1$ or $P \in X_2$.

  It follows that $X \subseteq X_1 \cup X_2$.

  Thus X is reducible.

Noetherian Rings

- Let R be a ring.
- An ascending chain

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots \subseteq I_n \subseteq \cdots$$

of ideals in R is **stationary** if, for some n_0, we have

$$I_{n_0+k} = I_{n_0}, \quad \text{for all } k \geq 0.$$

- A ring R is **Noetherian** if and only if it satisfies the **ascending chain condition** (**acc**), namely, every ascending chain

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots \subseteq I_n \subseteq \cdots$$

of ideals becomes stationary.
- The ring $A = k[x_1, \ldots, x_n]$ is a Noetherian ring.

Descending Chain of Algebraic Sets

- Consider a descending chain of algebraic sets

$$X_1 \supseteq X_2 \supseteq \cdots \supseteq X_n \supseteq \cdots .$$

- We have a corresponding ascending chain of ideals,

$$I(X_1) \subseteq I(X_2) \subseteq \cdots \subseteq I(X_n) \subseteq \cdots .$$

- Suppose $X_n \supsetneqq X_{n+1}$ is a proper inclusion.
- Since X_n and X_{n+1} are algebraic sets,

$$I(X_n) \subsetneqq I(X_{n+1})$$

  is also a proper inclusion.
- But the ring $A = k[x_1, \ldots, x_n]$ is Noetherian.
- Thus, every descending sequence of closed sets becomes stationary.

Noetherian Topological Spaces

- A topological space in which every descending sequence of closed sets becomes stationary is called a **Noetherian topological space**.
- Thus, the Zariski topological space $\mathbb{A}_k^n$ is a Noetherian topological space.
- It follows from the axiom of choice that every nontrivial system Σ of algebraic sets in $\mathbb{A}_k^n$ has a minimal element (an element $X \in \Sigma$, such that, there is no $Y \in \Sigma$, with $Y \subsetneq X$.)

Irreducible Components

Proposition

Every algebraic set $X \subseteq \mathbb{A}_k^n$ has a decomposition

$$X = X_1 \cup \cdots \cup X_r,$$

where:

- The X_i are irreducible algebraic sets;
- $X_i \nsubseteq X_j$, for $i \neq j$.

This decomposition is unique up to the order of the factors.

- The X_i are called the **irreducible components** of X.
- First we show the existence of such a decomposition.

  Let Σ be the set of all algebraic sets not having such a representation.

  Suppose, to the contrary, that $\Sigma \neq \emptyset$.

Irreducible Components (Cont'd)

- Then, Σ has a minimal element X, which is reducible.

  Thus, there exist $X_1, X_2 \subsetneqq X$ with $X = X_1 \cup X_2$.

  Since X is a minimal element of Σ, it follows that $X_1, X_2 \notin \Sigma$.

  Thus, X_1 and X_2 can be decomposed into a union of irreducible components.

  This means that X also has such a decomposition.

  This contradicts $X \in \Sigma$.

  It remains to show that such a decomposition is unique.

Irreducible Components (Uniqueness)

- Suppose there is another decomposition

$$X = Y_1 \cup \cdots \cup Y_\ell.$$

with Y_i irreducible and $Y_i \not\subseteq Y_j$, for $i \neq j$. Then

$$X_i = X_i \cap X = \bigcup_{m=1}^{\ell} (X_i \cap Y_m).$$

Since X_i is irreducible, we have $X_i \cap Y_m = X_i$, for some m.

In particular, $Y_m \supseteq X_i$.

By exchanging the roles of the two decompositions we can similarly show that for some j, we have $X_j \supseteq Y_m \supseteq X_i$.

Thus, $i = j$ and $X_i = Y_m$.

- The proposition is true for any Noetherian topological space, since the proof only uses the fact that the Zariski topology is Noetherian.

Characterization of Irreducible Subsets

Lemma

For a closed set $V \subseteq \mathbb{A}_k^n$, the following are equivalent:

(1) V is irreducible.

(2) For any two open sets $U_1, U_2 \neq \emptyset$ of V we have $U_1 \cap U_2 \neq \emptyset$.

(3) Every open set $\emptyset \neq U \subseteq V$ is dense in V.

- The equivalence of (1) and (2) follows from

$$U_1 \cap U_2 = \emptyset \quad \text{iff} \quad (V - U_1) \cup (V - U_2) = V.$$

On the other hand, by definition, a subset $U \subseteq V$ is dense if and only if it meets every nonempty open subset of V.

This gives the equivalence of (2) and (3).

Affine Varieties and Finite Generation

Definition (Affine Variety)

An **affine variety** (over k) is an affine algebraic set.

Definition (Finite Generation)

Let B be a subring of A.

(1) A is **finitely generated** over B (or **finitely generated as a B-algebra**) if there are finitely many elements $a_1, \ldots, a_n$, such that $A = B[a_1, \ldots, a_n]$.

(2) A is a **finite B-algebra** if there are finitely many elements $a_1, \ldots, a_n$ with $A = Ba_1 + \cdots + Ba_n$.

Example: The polynomial ring $k[x_1, \ldots, x_n]$ is a finitely generated k-algebra, but not a finite k-algebra.

The Algebraic Foundation of the Nullstellensatz

Theorem

Let k be a field with infinitely many elements. Let $A = k[a_1, \ldots, a_n]$ be a finitely generated k-algebra. If A is a field, then A is algebraic over k.

- For now, we give a brief heuristic argument.

  Suppose that $t \in A$ is transcendental over k.

  Then $k[t]$ is a polynomial ring over k.

  Now k has infinitely many elements.

  By Euclid's Theorem, $k[t]$ has infinitely many primes.

  Suppose $k(t)$ was generated over k by finitely many elements $r_i = \frac{p_i}{q_i}$.

  This is impossible, since there is a finite set of primes (the prime divisors of the q_i) which contains all primes in the denominator of any element constructed as a polynomial in the r_i.
- This argument can be made rigorous, but we will give a different proof.

Hilbert's Nullstellensatz

Theorem (Hilbert's Nullstellensatz)

Let k be an algebraically closed field. Let $A = k[x_1,\ldots,x_n]$. Then the following hold:

(1) Every maximal ideal $m \subseteq A$ is of the form

$$m = (x_1 - a_1,\ldots,x_n - a_n) = I(P),$$

for some point $P = (a_1,\ldots,a_n) \in \mathbb{A}_k^n$.

(2) If $J \subsetneq A$ is a proper ideal, then $V(J) \neq \varnothing$.

(3) For every ideal $J \subseteq A$, we have $I(V(J)) = \sqrt{J}$.

- The crucial point is (2), which says that every nontrivial ideal has at least one point in its zero locus.
- This explains the name of the theorem, which can be translated as the "theorem about the existence of zeros".

Remark

- The result is clearly false for non algebraically closed fields.
- This is illustrated by the ideal

$$(x^2+1) \subsetneq \mathbb{R}[x].$$

Proof of Hilbert's Nullstellensatz (1)

(1) First note that any ideal of the form $(x_1 - a_1, \ldots, x_n - a_n)$ is maximal.

This follows from the fact that the evaluation map

$$k[x_1, \ldots, x_n] \to k; \quad f \mapsto f(P)$$

induces an isomorphism $k[x_1, \ldots, x_n]/(x_1 - a_1, \ldots, x_n - a_n) \cong k$.

Note that, by a linear transformation, we may assume all a_i are zero.

Then the map $f \mapsto f(0, \ldots, 0)$ simply maps f to its constant term.

So its kernel is the set of functions with zero constant.

These are precisely the functions divisible by x_i, for some i.

Proof of Hilbert's Nullstellensatz (1) (Cont'd)

- Now suppose that $m \subseteq k[x_1,\ldots,x_n]$ is any maximal ideal in A.
  This implies that $K := k[x_1,\ldots,x_n]/m$ is a field.
  Moreover K is also a finitely generated k-algebra (generated by the residue classes $x_i \mod m$).
  By the theorem, K is algebraic over k.
  By hypothesis, k is algebraically closed.
  So the natural map
  $$\varphi : k \hookrightarrow k[x_1,\ldots,x_n] \xrightarrow{\pi} k[x_1,\ldots,x_n]/m = K$$
  is an isomorphism between k and K.
  Let $b_i := x_i \mod m \in K$ and let $a_i := \varphi^{-1}(b_i)$.
  Then, for each i, we have $x_i - a_i \in \ker\pi = m$.
  So $(x_1 - a_1,\ldots,x_n - a_n) \subseteq m$.
  But $(x_1 - a_1,\ldots,x_n - a_n)$ is a maximal ideal.
  So we have the equality $(x_1 - a_1,\ldots,x_n - a_n) = m$.

Proof of Hilbert's Nullstellensatz (2)

(2) Suppose $J \subsetneq A = k[x_1,\ldots,x_n]$.

We know $k[x_1,\ldots,x_n]$ is a Noetherian ring.

So there exists a maximal ideal m with $J \subseteq m$.

From Part (1), we have $m = I(P)$, for some point $P \in \mathbb{A}_k^n$.

So

$$\{P\} = V(I(P)) \subseteq V(J).$$

This shows that $V(J)$ is nonempty.

Proof of Hilbert's Nullstellensatz (3)

(3) This step is usually proved by **Rabinowitsch's trick**.
Let $J \subseteq k[x_1,\ldots,x_n]$ be an ideal and $f \in I(V(J))$.
We want to show that $f^N \in J$, for some N.
The trick is to introduce an additional variable t.
We then define an ideal $J_f \supseteq J$ by

$$J_f := (J, ft-1) \subseteq k[x_1,\ldots,x_n,t],$$

We have

$$V(J_f) = \{Q = (a_1,\ldots,a_n,b) = (P,b) \in \mathbb{A}_k^{n+1} : P \in V(J), bf(P) = 1\}.$$

Projection onto the first n coordinates maps $V(J_f)$ to the subset of $V(J)$ of points P, with $f(P) \neq 0$.
But f is an element of $I(V(J))$.
So $V(J_f) = \varnothing$.

Proof of Hilbert's Nullstellensatz (3)

- Thus, by Part (2), $J_f = k[x_1,\ldots,x_n,t]$.
  In particular, $1 \in J_f$.
  Thus, we can write

$$1 = \sum_{i=1}^{r} g_i f_i + g_0(ft-1) \in k[x_1,\ldots,x_n,t],$$

  for some $g_i \in k[x_1,\ldots,x_n,t]$ and $f_i \in J$.
  Let t^N be the highest power of t appearing in g_i, for $0 \le i \le r$.
  Multiplying by t^N gives

$$f^N = \sum_{i=1}^{r} G_i(x_1,\ldots,x_n,ft)f_i + G_0(x_1,\ldots,x_n,ft)(ft-1),$$

  where the $G_i = f^N g_i$ are polynomials in $x_1,\ldots,x_n,ft$.
  This equation holds in $k[x_1,\ldots,x_n,t]$.

Proof of Hilbert's Nullstellensatz ((3) Cont'd)

- We have

$$f^N = \sum_{i=1}^{r} G_i(x_1,\ldots,x_n,ft)f_i + G_0(x_1,\ldots,x_n,ft)(ft-1),$$

where the $G_i = f^N g_i$ are polynomials in $x_1,\ldots,x_n,ft$.
Consider this equation modulo $(ft-1)$.
That is, consider its reduction in the ring $k[x_1,\ldots,x_n,t]/(ft-1)$.
We obtain the relationship

$$f^N \equiv \sum h_i(x_1,\ldots,x_n)f_i \mod (ft-1),$$

where $h_i(x_1,\ldots,x_n) := G_i(x_1,\ldots,x_n,1)$.
The natural map $k[x_1,\ldots,x_n] \to k[x_1,\ldots,x_n,t]/(ft-1)$ is injective.
So we must already have $f^N = \sum h_i(x_1,\ldots,x_n)f_i$ in $k[x_1,\ldots,x_n]$.
Thus, $f^N \in J$.

Bijections

Corollary

For $A = k[x_1, \ldots, x_n]$, the maps V and I

$$\{\text{ideals of } A\} \overset{V,I}{\leftrightarrow} \{\text{subsets of } \mathbb{A}_k^n\}$$

induce the following bijections:

$$\begin{array}{ccc}
\{\text{radical ideals of } A\} & \overset{1:1}{\longleftrightarrow} & \{\text{subvarieties of } \mathbb{A}_k^n\} \\
\cup & & \cup \\
\{\text{prime ideals of } A\} & \overset{1:1}{\longleftrightarrow} & \{\text{irreducible subvarieties of } \mathbb{A}_k^n\} \\
\cup & & \cup \\
\{\text{maximal ideals of } A\} & \overset{1:1}{\longleftrightarrow} & \{\text{points of } \mathbb{A}_k^n\}.
\end{array}$$

Bijections (Cont'd)

- For every algebraic set $X \subseteq \mathbb{A}_k^n$, we have

$$V(I(X)) = X.$$

Conversely, by Hilbert's Nullstellensatz, Part (3), for every ideal J, we have

$$I(V(J)) = \sqrt{J}.$$

Thus we obtain the first bijection.

The second bijection follows from a preceding proposition.

The third follows from Hilbert's Nullstellensatz, Part (1).

Affine Hypersurfaces in $\mathbb{A}_k^n$

- An **affine hypersurface** in $\mathbb{A}_k^n$ is an algebraic subset given by a single equation:

$$V(f) = \{P \in \mathbb{A}_k^n : f(P) = 0\}, \quad 0 \neq f \in k[x_1, \ldots, x_n].$$

- If the prime decomposition of f is given by $f = f_1^{r_1} \cdots f_m^{r_m}$, then

$$\sqrt{(f)} = (f_1 \cdot \cdots \cdot f_m).$$

- The ideal (f) is prime if and only if f is irreducible, that is, if $m = 1$ and $r_1 = 1$.
- Thus, we have the following bijection:

$$\left\{ \begin{array}{c} \text{irreducible} \\ \text{hypersurfaces in } \mathbb{A}_k^n \end{array} \right\} \overset{1:1}{\longleftrightarrow} \{f \in k[x_1, \ldots, x_n] : f \text{ irreducible}\}/k^*.$$

The Finite Algebra Lemma

Lemma

Let $C \subseteq B \subseteq A$ be rings.

(1) If B is a finite C-algebra and A is a finite B-algebra, then A is also a finite C-algebra.

(2) If A a finite B-algebra, then A is integral over B, i.e., every element $x \in A$ satisfies an equation of the form

$$x^n + b_{n-1}x^{n-1} + \cdots + b_1 x + b_0 = 0, \quad b_i \in B.$$

(3) Conversely, if $x \in A$ satisfies an equation of the above form, then $B[x]$ is a finite B-algebra.

The Finite Algebra Lemma (Cont'd)

(1) Suppose

$$B = Cb_1 + \cdots + Cb_m.$$

Suppose, also, that

$$A = Ba_1 + \cdots + Ba_n.$$

Then

$$A = Ca_1 b_1 + \cdots + Ca_n b_m.$$

(3) Suppose $x \in A$ satisfies an equation

$$x^n + b_{n-1}x^{n-1} + \cdots + b_1 x + b_0 = 0, \quad b_i \in B.$$

Then

$$x^n = -b_{n-1}x^{n-1} - \cdots - b_1 x + b_0.$$

So we have

$$B[x] = B + Bx + \cdots + Bx^{n-1}.$$

The Finite Algebra Lemma (Cont'd)

(2) We prove this using a "determinant trick".
Suppose that

$$A = Ba_1 + \cdots + Ba_n.$$

Then, for any $x \in A$, we have $xa_i \in A$, for $i = 1, \ldots, n$.
Thus, there are elements $b_{ij} \in B$, such that

$$xa_i = \sum_{j=1}^{n} b_{ij} a_j.$$

We get a single polynomial equation for x from these n linear equations:

- We express this in matrix notation;
- We take the determinant of the matrix.

The lat equation is equivalent to

$$\sum_{j=1}^{n} (x\delta_{ij} - b_{ij}) a_j = 0.$$

The Finite Algebra Lemma (Cont'd)

- In matrix notation, it can be written as

$$Ma = 0,$$

where:
  - M is the matrix given by $M := (x\delta_{ij} - b_{ij})_{i,j}$;
  - a is the column vector with transpose ${}^t a = (a_1, \ldots, a_n)$.

Let M^{adj} be the adjoint matrix of M.
Then, since $Ma = 0$, $\det Ma = M^{\text{adj}} Ma = 0$.
Thus, $\det M a_i = 0$, for $i = 1, \ldots, n$.
But the a_i generate the B-algebra A.
Hence $\det M = \det M \cdot 1 = 0$.
Expanding the determinant, we also have, for some $b_i \in B$,

$$\det M = x^n + b_{n-1} x^{n-1} + \cdots + b_1 x + b_0.$$

Thus, x satisfies a polynomial equation with coefficients in B.
So $B[x]$ is a finite B-algebra.

Nakayama's Lemma

Definition (Monic Polynomial)

A polynomial $f \in B[x]$ is called **monic** if the coefficient of the leading term is 1.

Lemma (Nakayama's Lemma)

Let $A \neq 0$ be a finite B-algebra. Then, for all proper ideals m of B we have $mA \neq A$.

- Suppose A is a finite B-algebra.

  We can write

$$A = Ba_1 + \cdots + Ba_n,$$

  for some $a_i \in A$.

Nakayama's Lemma (Cont'd)

- Suppose that

$$mA = A.$$

Then, there exist $b_{ij} \in m$, $1 \leq i, j \leq n$, such that

$$a_i = \sum_{j=1}^{n} b_{ij} a_j, \quad 1 \leq i \leq n.$$

From this we can conclude that

$$\det(\delta_{ij} - b_{ij}) = 0.$$

Expanding the determinant shows that $1 \in m$, a contradiction.

Subrings over which Fields are Finite Algebras

Lemma

Let A be a field and $B \subseteq A$ a subring, such that A is a finite B-algebra. Then B is also a field.

- Let $0 \neq b \in B$.

  Since A is a field, there exists $b^{-1} \in A$.

  We must show that b^{-1} lies in B.

  By Part (2) of the Finite Algebra Lemma, there exist $b_i \in B$, such that

$$b^{-n} + b_{n-1} b^{-(n-1)} + \cdots + b_1 b^{-1} + b_0 = 0.$$

  Multiplication by b^{n-1} gives

$$b^{-1} = -(b_{n-1} + b_{n-2} b + \cdots + b_0 b^{n-1}) \in B.$$

The Degree

- The **degree** of a monomial

$$x_1^{\nu_1} \cdots x_n^{\nu_n}$$

  is defined to be the sum $\sum \nu_i$.
- The **degree** of a polynomial is the maximum of the degrees of all its monomials terms.

The Univariate Leading Term Lemma

Lemma

Suppose that f is a nonzero element of $k[x_1,\dots,x_n]$, with $d = \deg f$. Then there is a change of variables

$$x_i' = x_i - \alpha_i x_n, \quad 1 \le i \le n-1,$$

where $\alpha_1,\dots,\alpha_{n-1} \in k$, such that

$$f(x_1' + \alpha_1 x_n,\dots,x_{n-1}' + \alpha_n x_n, x_n) \in k[x_1',\dots,x_{n-1}',x_n]$$

has a term of the form cx_n^d, for some nonzero $c \in k$.

- In fact "almost any" choice of α_i will work (see, also, below). Let
$$x_i' = x_i - \alpha_i x_n$$
for some $\alpha_i \in k$, $1 \le i \le n-1$.

The Univariate Leading Term Lemma (Cont'd)

- Since $d = \deg f$, we can write

$$f = F_d + G,$$

where:

  - F_d is a sum of monomials of degree d (i.e., F_d is **homogeneous** of degree d);
  - $\deg G \leq d - 1$.

Then we have

$$\begin{aligned} & f(x_1' + \alpha_1 x_n, \ldots, x_{n-1}' + \alpha_{n-1} x_n, x_n) \\ & = F_d(\alpha_1, \ldots, \alpha_{n-1}, 1) x_n^d + \text{terms of lower order in } x_n. \end{aligned}$$

Now $F_d(\alpha_1, \ldots, \alpha_{n-1}, 1)$ is a nonzero polynomial in $\alpha_1, \ldots, \alpha_{n-1}$. So its zero set is not $\mathbb{A}_k^{n-1}$ (k has infinitely many elements). This means we can choose $\alpha_1, \ldots, \alpha_{n-1} \in k$ with

$$F_d(\alpha_1, \ldots, \alpha_{n-1}, 1) \neq 0.$$

This completes the proof, since then $c = F_d(\alpha_1, \ldots, \alpha_{n-1}, 1) \neq 0$.

Noether Normalization

- *Noether normalization* relates the geometric idea of dimension to the algebraic structure of the coordinate ring of a variety.

Theorem (Noether Normalization)

Let k be an infinite field. Let $A = k[a_1, \ldots, a_n]$ be a finitely generated k-algebra. Then there exist $y_1, \ldots, y_m \in A$, with $m \leq n$, such that:

(1) $y_1, \ldots, y_m$ are algebraically independent over k;

(2) A is a finite $k[y_1, \ldots, y_m]$-algebra.

- The fact that $y_1, \ldots, y_m$ are algebraically independent (i.e., they do not satisfy any polynomial equation with coefficients in k), is equivalent to the statement that the map from the polynomial ring $k[t_1, \ldots, t_m]$ in m variables over k to $k[y_1, \ldots, y_m]$, given by $t_i \mapsto y_i$, is an isomorphism.

Proof of Noether Normalization

- We use induction on n.

  Let $k[x_1,\ldots,x_n]$ be the polynomial ring over k in n variables.

  Let

  $$I := \ker(k[x_1,\ldots,x_n] \to k[a_1,\ldots,a_n] = A)$$

  be the kernel of the homomorphism given by $x_i \mapsto a_i$.

  - Suppose $I = 0$.
    We can take $m = n$ and $y_1 = a_1,\ldots,y_n = a_n$.
    Then Statements (1) and (2) hold.
  - Suppose $I \neq 0$.
    Then there is some nonzero element $f \in I$.
    - If $n = 1$, then we have $f(a_1) = 0$.
      The result follows from Part (3) of the Finite Algebra Lemma, with $m = 0$.
      That is, the set of y_i is empty.
    - Suppose, next, that $n > 1$.
      Assume the result holds for $n-1$.

Proof of Noether Normalization

- By the preceding lemma, there exist $\alpha_1,\ldots,\alpha_{n-1} \in k$, such that, setting $a'_i = a_i - \alpha_i a_n$ and $A' := k[a'_1,\ldots,a'_{n-1}] \subseteq A$, we have that, for some nonzero constant $c \in k$,

$$F(x_n) := \frac{1}{c} f(a'_1 + \alpha_1 x_n, \ldots, a'_{n-1} + \alpha_{n-1} x_n, x_n)$$

  is a monic polynomial in $A'[x_n]$, and $F(a_n) = 0$.

  By Part (3) of the Finite Algebra Lemma, a_n is integral over A'.

  By the inductive hypothesis, there are $y_1,\ldots,y_m \in A'$, such that:
  (1) $y_1,\ldots,y_m$ are algebraically independent over k;
  (2) A' is a finite $k[y_1,\ldots,y_m]$-algebra.

  By Part (3) of the Finite Algebra Lemma, $A = A'[a_n]$ is a finite A'-algebra. Then, by Part (1) of the Finite Algebra Lemma, A is a finite $k[y_1,\ldots,y_m]$-algebra.

General Set of Linear Forms With Respect to a Property

- In the proof, the collection of m-tuples of linear forms in $a_1, \ldots, a_n$ forms an affine space $\mathbb{A}_k^{nm}$.
- So the successive linear changes of variables given by the preceding lemma can all be taken to be "general".
- Consequently, $y_1, \ldots, y_m$ can be taken to be any "general" choice of linear forms in $a_1, \ldots, a_n$.
- To say that a set of linear forms is **general with respect to some property**, or **in general satisfies the property**, means that, there is a Zariski open subset of $\mathbb{A}_k^{nm}$, such that, for any point in this set, the corresponding set of linear forms satisfies the given property.
- That is, the property is true for a dense set of linear forms, or, colloquially, "in general".

Fields that are Finitely Generated Algebras

Theorem

Let k be a field with infinitely many elements. Let $A = k[a_1, \ldots, a_n]$ be a finitely generated k-algebra. If A is a field, then A is algebraic over k.

- Let $A = k[a_1, \ldots, a_n]$ be a finitely generated k-algebra.

  Suppose that A is a field.

  By Noether Normalization, we get $y_1, \ldots, y_m \in A$, for some $m \leq n$, such that, setting

  $$B = k[y_1, \ldots, y_m] \subseteq A,$$

  we have that A is a finite B-algebra.

  By a preceding lemma, B is a field.

  This can only be the case if $m = 0$.

  So A is a finite extension of k.

  Thus, A is algebraic over k.

Geometric Meaning of Noether Normalization

- Let $X \subseteq \mathbb{A}_k^n$ be a variety.

  For simplicity we assume X to be irreducible.

  I.e., we assume that the ideal $I = I(X) \subseteq k[x_1, \ldots, x_n]$ is prime.

  We consider the ring

  $$A = k[a_1, \ldots, a_n] = k[x_1, \ldots, x_n]/I,$$

  where $a_i := x_i \mod I$.

  Later A will be termed the **coordinate ring** of X.

  By Noether Normalization, there exist algebraically independent linear forms $y_1, \ldots, y_m$ in $a_1, \ldots, a_n$ (which can be taken to be general), such that A is a finite $k[y_1, \ldots, y_m]$-algebra.

Geometric Meaning of Noether Normalization (Cont'd)

- The linear forms obtained from Noether Normalization lift (nonuniquely) to linear forms $\overline{y}_1,\ldots,\overline{y}_m$ in $x_1,\ldots,x_n$, where

$$\overline{y}_i = y_i \mod I.$$

The forms $\overline{y}_1,\ldots,\overline{y}_m$ define a linear projection

$$\pi := (\overline{y}_1,\ldots,\overline{y}_m) : \mathbb{A}_k^n \to \mathbb{A}_k^m.$$

By restricting $\overline{y}_1,\ldots,\overline{y}_m$ to X, we obtain a map

$$\phi := \pi\mid_X : X \to \mathbb{A}_k^m.$$

On X we have

$$y_i\mid_X = \overline{y}_i\mid_X .$$

So ϕ is independent of the choice of lifts $\overline{y}_i$.

Finiteness of the Fibers of ϕ

Proposition

Suppose $k = \overline{k}$. Let ϕ be the mapping of the preceding slide. Then, for every point $P \in \mathbb{A}_k^m$, the fiber $\phi^{-1}(P)$ is finite and nonempty.

- We first show that $\phi^{-1}(P)$ is finite.

  By Part (2) of the Finite Algebra Lemma, there exist an integer N and polynomials $f_0^i, \ldots, f_{N-1}^i$, for $1 \leq i \leq n$, such that for $i = 1, \ldots, n$, we have

$$a_i^N + f_{N-1}^i(y_1, \ldots, y_m) a_i^{N-1} + \cdots + f_0^i(y_1, \ldots, y_m) = 0.$$

  This means that, with $I = I(X)$, we have, for some $g_i \in I$,

$$x_i^N + f_{N-1}^i(\overline{y}_1, \ldots, \overline{y}_m) x_i^{N-1} + \cdots + f_0^i(\overline{y}_1, \ldots, \overline{y}_m) = g_i(x_1, \ldots, x_n).$$

Finiteness of the Fibers of ϕ (Cont'd)

- For $I = I(X)$, we have, for some $g_i \in I$,

$$x_i^N + f_{N-1}^i(\overline{y}_1, \ldots, \overline{y}_m) x_i^{N-1} + \cdots + f_0^i(\overline{y}_1, \ldots, \overline{y}_m) = g_i(x_1, \ldots, x_n).$$

Suppose $(x_1, \ldots, x_n) \in X$. Then $g_i(x_1, \ldots, x_n) = 0$.
So x_i is a solution of the equation $f^i(x) = 0$, where

$$f^i(x) := x^N + f_{N-1}^i(y_1, \ldots, y_m) x^{N-1} + \cdots + f_0^i(y_1, \ldots, y_m).$$

Since I is prime, $A = k[a_1, \ldots, a_n]$ is an integral domain.
So it has a field of fractions $k(a_1, \ldots, a_n)$.
We can thus consider $f^i(x) \in k(a_1, \ldots, a_n)[x]$.
By the Fundamental Theorem of Algebra, there are only a finite number of solutions x_i^0 to $f^i(x) = 0$.
Thus, for any point $\boldsymbol{y} = (y_1, \ldots, y_m) \in \mathbb{A}_k^m$, we have only finitely many points $\boldsymbol{x} = (x_1^0, \ldots, x_n^0) \in X$, with $\phi(\boldsymbol{x}) = \boldsymbol{y}$.

Nonemptiness of the Fibers of ϕ

- Finally, we show that $\phi^{-1}(P)$ is always nonempty.

  It is enough to show that for every point $P = (b_1, \ldots, b_m) \in \mathbb{A}_k^m$,

  $$I_P := I + (y_1 - b_1, \ldots, y_m - b_m) \neq k[x_1, \ldots, x_n].$$

  Then Hilbert's Nullstellensatz implies that $\phi^{-1}(P) = V(I_P) \neq \emptyset$.

  The displayed condition is equivalent to

  $$(y_1 - b_1, \ldots, y_m - b_m) \neq k[a_1, \ldots, a_n].$$

  Now $(y_1 - b_1, \ldots, y_m - b_m)$ is a maximal ideal in $k[y_1, \ldots, y_m]$.

  In particular, it is a proper ideal.

  So the condition follows from Nakayama's Lemma, with

  $$B = k[y_1, \ldots, y_m], \quad A = k[a_1, \ldots, a_n], \quad m = (y_1 - b_1, \ldots, y_m - b_m).$$

Example

- Let
$$f = x_1x_2 + x_2x_3 + x_3x_1 \in k[x_1, x_2, x_3].$$
For the quadric hypersurface $S := V(f) \subseteq \mathbb{A}_k^2$, we have
$$A = k[x_1, x_2, x_3]/(f).$$
We use the notation
$$a_i := x_i \mod (f), \quad i = 1, 2, 3.$$
In the proof of Noether Normalization, since f does not contain any terms of the form x_i^m, we must make a change of variables.

Example (Cont'd)

- E.g., let
$$z = x_2 + x_1.$$
Then we have
$$f = z(x_1 + x_3) - x_1^2.$$
Now A is algebraic over $k[a_1 + a_2, a_3]$.
Moreover, the corresponding map ϕ is given by
$$\begin{array}{rccc} \phi : & S & \to & \mathbb{A}_k^2, \\ & (x_1, z, x_3) & \mapsto & (z, x_3). \end{array}$$
The fiber
$$\phi^{-1}(a, b) = \{(x, a, b) : x^2 - ax - ab\}$$
consists of at most 2 points.

Example (Cont'd)

- S contains the coordinate axes.

  So for any choice of $1 \le i < j \le 3$, the projection to the x_i, x_j plane,

$$\begin{array}{rcl} S & \to & \mathbb{A}_k^2, \\ (x_1, x_2, x_3) & \mapsto & (x_i, x_j), \end{array}$$

  has an infinite fiber over $(0, 0)$.

  Similarly, suppose $(a, b, c) \in S$.

  Then S contains the line $L := \{(\lambda a, \lambda b, \lambda c) : \lambda \in k\}$.

  Thus, the projection

$$(x_1, x_2, x_3) \mapsto (bx_1 - ax_2, cx_1 - ax_3)$$

  maps L to $(0, 0)$.

  However, there is a dense set of hyperplanes such that the corresponding projection has finite fibers.

Fields of Positive Characteristic

- The **characteristic** of a field k, $\mathrm{char}(k)$, is the minimal prime p, such that
$$p \cdot 1 = \underbrace{1 + \cdots + 1}_{p \text{ times}} = 0,$$
- The characteristic is 0 if there is no such prime.

  Example: For any prime p, the field $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ and its algebraic closure both have positive characteristic p.

  The field $\mathbb{C}$ and its subfields all have characteristic 0.

Separability

Definition

A nonconstant irreducible polynomial

$$f = a_n x^n + \cdots + a_1 x + a_0 \in k[x]$$

is called **separable** if the formal derivative is nonzero, that is,

$$f' = n a_n x^{n-1} + \cdots + a_1 \neq 0.$$

Otherwise f is called **inseparable**.
An arbitrary polynomial is called **separable** if every factor is separable.
An irreducible polynomial

$$f \in k[x_1, \ldots, x_n]$$

is called **separable with respect to** x_i if the formal derivative with respect to this variable is nonzero.

Remarks

- Clearly all polynomials over a field of characteristic 0 are separable.
- An irreducible polynomial $f \in k[x]$ over a field of characteristic p is inseparable if and only if

$$f(x) = g(x^p), \quad \text{for some } g \in k[x].$$

- E.g., $f(x) = x^p - t \in \mathbb{F}_p(t)[x]$ is an irreducible inseparable polynomial in characteristic p.
- In characteristic p the Frobenius identity $a^p + b^p = (a+b)^p$ implies that if k is algebraically closed then we can write

$$f(x) = g(x^p) = h(x)^p,$$

where $h(x)$ is obtained from $g(x)$ by replacing all coefficients by their p-th roots.

Separable Elements and Separable Extensions

Definition (Separable Elements)

Suppose K/k is a field extension and $x \in K$ is algebraic over k. Then x is called **separable** over k, if the minimal polynomial of x is separable over k. Otherwise x is called **inseparable**.

Definition (Separable Extensions)

An algebraic extension K/k is called **separable** if all elements of K are separable over k.

Noether Normalization for Positive Characteristic

Proposition

Let k be an algebraically closed field. Let $A = k[a_1,\ldots,a_n]$ be an integral domain with field of fractions K. Then there are $y_1,\ldots,y_m \in A$, such that:

(1) $y_1,\ldots,y_m$ are algebraically independent over k;

(2) A is a finite $k[y_1,\ldots,y_m]$-algebra;

(3) K is a separable extension of $k(y_1,\ldots,y_m)$.

- In characteristic 0 all algebraic extensions are separable.
  So assume that the characteristic p of k is positive.
  Let x_i be algebraically independent over k.
  Define a map $\pi : k[x_1,\ldots,x_n] \to k[a_1,\ldots,a_n]$ by setting $\pi(x_i) = a_i$.
  Since A is an integral domain, the ideal $I := \ker(\pi)$ is prime.
  In particular, we can choose an irreducible element $f \in I$.
  Suppose that f has degree d.

Normalization for Positive Characteristic (Cont'd)

- By a preceding lemma, there is a change of variables of the form

$$\widetilde{x}_i = x_i + \alpha_i x_n,$$

such that $\widetilde{f}(\widetilde{x}_1, \widetilde{x}_2, \ldots) = f(x_1, x_2, \ldots, x_n)$ has a term of the form $c(\widetilde{x}_n)^d$.

Note that if f has a term of the form cx_i^d, then $\widetilde{f}$ has a term of the form $c(\widetilde{x}_i)^d$.

Exchanging the role of x_n with x_j, for $j = 1, \ldots, n-1$, we can make a sequence of changes of variables to obtain a polynomial in $\widetilde{x}_1, \ldots, \widetilde{x}_n$, where

$$\widetilde{x}_i = x_i + \sum_{\substack{j=1 \\ j \neq i}}^{n} \beta_{ij} x_j,$$

for some constants β_{ij}, $1 \le i, j \le n$, $i \neq j$, such that, for each i, as a polynomial in $\widetilde{x}_i$ over $k[\{x_j : j \neq i\}]$, the leading term is of the form $c_i(\widetilde{x}_i)^d$, for some nonzero $c_i \in k$.

Normalization for Positive Characteristic (Cont'd)

- Now f is irreducible.

  So $k[x_1,\ldots,x_n]/(f)$ is an integral domain.

  The change of variables induces an isomorphism

  $$k[x_1,\ldots,x_n]/(f) \cong k[\widetilde{x}_1,\ldots,\widetilde{x}_n]/(\widetilde{f}).$$

  Hence, $k[\widetilde{x}_1,\ldots,\widetilde{x}_n]/(\widetilde{f})$ is also an integral domain.

  Thus $\widetilde{f}$ is also irreducible.

  But $k[\widetilde{x}_1,\ldots,\widetilde{x}_n] = k[x_1,\ldots,x_n]$.

  So we can replace x_i by $\widetilde{x}_i$ and f by $\widetilde{f}$.

  So we may assume that f is irreducible and has a leading term of the form $c_i(x_i)^d$, for $c_i \in k$, with respect to each variable.

Normalization for Positive Characteristic (Induction)

Claim: f is separable with respect to at least one variable x_i.

Otherwise we would have $f \in k[x_1, \ldots, x_i^p, \ldots, x_n]$, for all i.

So there would be polynomials g and h with

$$f = g(x_1^p, \ldots, x_n^p) = h(x_1, \ldots, x_n)^p.$$

This would contradict the irreducibility of f.

Thus, we may assume that f is separable with respect to x_n.

We view the equation

$$f(a_1, \ldots, a_{n-1}, a_n) = 0$$

as a separable equation for a_n over the field of fractions of $A' = k[a_1, \ldots, a_{n-1}]$.

Now we apply an inductive argument.

We need to use the fact that the composition of two separable extensions is again a separable extension.

Theorem of the Primitive Element

Theorem (Theorem of the Primitive Element)

Let K be a field with infinitely many elements. Let $L \supseteq K$ be a finite separable extension. Then there is an element $x \in L$, with $L = K(x)$. Moreover, if L is generated over K by a finite set of elements $z_1, \ldots, z_n$, then x can be chosen to be an element of the form $x = \sum \alpha_i z_i$, with $\alpha_i \in K$.

- Let $K \subseteq M$ be the normal closure of L over K.

  Then $K \subseteq M$ is a finite Galois extension.

  By the Fundamental Theorem of Galois Theory, there are only finitely many fields between K and M.

  The fields $\{K_i\}$ between K and L form finitely many K-subspaces of the vector space L.

  If K has infinitely many elements, then there exists $x \in L$ which does not lie in the union of the K_i.

  Then $L = K(x)$.

Theorem of the Primitive Element (Cont'd)

- Suppose $z_1, \ldots, z_n$ generate L.

  Then they cannot all be contained in any single K_i.

  So, there is some linear combination

  $$x = \sum \alpha_i z_i$$

  which is not contained in any K_i.

  Hence $L = K(x)$.

Additional Result on Noether Normalization

Corollary

Let k be an algebraically closed field. Let $A = k[a_1, \ldots, a_n]$ be an integral domain with field of fractions K. Then there exist $y_1, \ldots, y_{m+1} \in A$, such that:

(1) $y_1, \ldots, y_m$ are algebraically independent over k;

(2) A is a finite $k[y_1, \ldots, y_m]$-algebra;

(3) K is a separable extension of $k(y_1, \ldots, y_m)$;

(4) The field of fractions K of A is generated over k by $y_1, \ldots, y_{m+1}$.

- By the preceding proposition, we can assume K is a separable field extension of $k(y_1, \ldots, y_m)$.

Additional Result on Noether Normalization (Cont'd)

- By hypothesis $A = k[a_1, \ldots, a_n]$.

  So the a_i generate K as a field extension of $k(y_1, \ldots, y_m)$.

  By the theorem, we can write y_{m+1} as a linear combination of the a_i with coefficients in $k(y_1, \ldots, y_m)$.

  Multiply this linear equation through by the common denominator.

  We then obtain an expression for y_{m+1} as a linear combination of the a_i with coefficients in $k[y_1, \ldots, y_m]$.

A Geometric Interpretation

- The corollary means the extension $k \subseteq K$ can be decomposed as

$$k \subseteq K_0 = k(y_1, \ldots, y_m) \subseteq K = K_0(y_{m+1}),$$

  where:
  - The first extension is purely transcendental;
  - The second is a *primitive* algebraic extension.
    That is, an algebraic extension generated by a single element.
- In other words, $K = k(y_1, \ldots, y_{m+1})$, where there is only one algebraic relation between the y_i.
- Geometrically:
  - If y_i are the coordinates of $\mathbb{A}^{n+1}$, then this relation describes a hypersurface in $\mathbb{A}^{n+1}$.
  - Thus, the displayed decomposition means that every irreducible variety is "almost" isomorphic to a hypersurface.

Subsection 2

Polynomial Functions and Maps

Polynomial Functions on Varieties

- Let V denote an affine variety in $\mathbb{A}_k^n$.

Definition (Polynomial Function)

A **polynomial function** on V is a map $f : V \to k$, such that, there exists a polynomial $F \in k[x_1, \ldots, x_n]$, with

$$f(P) = F(P), \quad \text{for all } P \in V.$$

- The polynomial F is not uniquely determined by the values it takes on V.
- In particular, for F and $G \in k[x_1, \ldots, x_n]$, we have

$$\begin{aligned} F|_V = G|_V \quad & \text{iff} \quad (F - G)|_V = 0 \\ & \text{iff} \quad F - G \in I(V). \end{aligned}$$

The Coordinate Ring of a Variety

Definition (Coordinate Ring)

The **coordinate ring** of V is defined by

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

- From preceding remarks we can make the following identification:

$$k[V] = \{f : f : V \to k \text{ is a polynomial function}\}.$$

- We also have

$$V \text{ is irreducible iff } k[V] \text{ is an integral domain.}$$

- The coordinate functions $x_1,\ldots,x_n$ generate $k[V]$.
- This explains the terminology "coordinate ring".

Correspondence Between Sets and Ideals

- The ring $k[V]$ plays the same role for V that $k[x_1,\ldots,x_n]$ plays for $\mathbb{A}_k^n$.
- In particular, there is a correspondence between:
  - The closed sets W contained in V;
  - The ideals of $k[V]$.
- The projection $\pi : k[x_1,\ldots,x_n] \to k[V] = k[x_1,\ldots,x_n]/I(V)$ induces a bijection

$$\{\text{ideals } J \subseteq k[x_1,\ldots,x_n] : J \supseteq I(V)\} \stackrel{1:1}{\longleftrightarrow} \{\text{ideals } J' \subseteq k[V]\}.$$

- It is defined by

$$J \mapsto J/I(V).$$

- Its inverse map is

$$J' \mapsto \pi^{-1}(J').$$

Correspondence Between Sets and Ideals (Cont'd)

- This mapping preserves radical ideals, prime ideals and maximal ideals,

$$\begin{array}{ccc}\{\text{radical ideals } J' \subseteq k[V]\} & \stackrel{1:1}{\longleftrightarrow} & \{\text{closed sets } W \subseteq V\} \\ \cup & & \cup \\ \{\text{prime ideals } J' \subseteq k[V]\} & \stackrel{1:1}{\longleftrightarrow} & \{\text{irreducible sets } W \subseteq V\} \\ \cup & & \cup \\ \{\text{maximal ideals } J' \subseteq k[V]\} & \stackrel{1:1}{\longleftrightarrow} & \{\text{points of } V\}.\end{array}$$

- Closed sets of V in the topology induced by the Zariski topology on $\mathbb{A}_k^n$ are the same as those defined by taking the closed sets of V to be sets of the form $V(J)$, where J is a radical ideal in $k[V]$.

Properties of Coordinate Rings

Definition (Reduced Algebra)

An algebra A is **reduced** if A contains no nilpotent elements.
That is, for $x \in A$,

$$x^n = 0, \text{ for some } n \geq 1, \quad \text{implies} \quad x = 0.$$

- The algebra $k[x_1, \ldots, x_n]/I$ is reduced if and only if I is a radical ideal.
- Since $I(V)$ is a radical ideal, the coordinate ring is a reduced algebra.
- By construction, the coordinate ring $k[V]$ of an affine variety V is a finitely generated k-algebra.

Characterization of Coordinate Rings

- Being finitely generated and reduced characterize coordinate rings of varieties.
- Let A be a finitely generated reduced k-algebra.
- We can construct a corresponding algebraic variety as follows.
- Choosing generators $a_1,\ldots,a_n$, we can write
$$A = k[a_1,\ldots,a_n].$$
- We then have a surjective homomorphism
$$\begin{array}{rrcl} \pi: & k[x_1,\ldots,x_n] & \to & A = k[a_1,\ldots,a_n] \\ & x_i & \mapsto & a_i. \end{array}$$
- Let $I = \ker(\pi)$. Then $V = V(I)$ is a variety.
- It is irreducible if and only if A is an integral domain.
- Since A is reduced, I is a radical ideal. So $I(V) = I$.
- By construction $A = k[V]$.

Example

- Consider the usual **parabola**

$$C_0 = \{(x,y) \in \mathbb{A}_k^2 : y - x^2 = 0\}.$$

We have

$$k[C_0] = k[x,y]/(y - x^2) \cong k[x] \cong k[\mathbb{A}_K^1].$$

- Consider the **semicubical parabola**, given by

$$C_1 = \{(x,y) \in \mathbb{A}_k^2 : y^2 - x^3 = 0\}.$$

We have

$$k[C_1] = k[x,y]/(y^2 - x^3).$$

- Notice that $k[C_1]$ is not a UFD.

Example (Cont'd)

- C_0 has a rational parametrization
$$t \mapsto (t, t^2).$$
- C_1 has a rational parametrization,
$$t \mapsto (t^2, t^3).$$
- So there are bijections between each of C_0 and C_1 and $\mathbb{A}_k^1$.
- However, as algebraic varieties C_0 and C_1 behave differently.
- We will see that C_0 is isomorphic to $\mathbb{A}_k^1$, but C_1 is not.

Polynomial Maps

- Let $V \subseteq \mathbb{A}_k^n$ and $W \subseteq \mathbb{A}_k^m$ be closed sets.
- Denote by x_i, for $1 \leq i \leq n$, the coordinate functions on $\mathbb{A}_k^n$.
- Denote by y_j, for $1 \leq j \leq m$, the coordinate functions on $\mathbb{A}_k^m$.

Definition (Polynomial Map)

A map $f : V \to W$ is called a **polynomial map** if there are polynomials $F_1, \ldots, F_m \in k[x_1, \ldots, x_n]$, such that

$$f(P) = (F_1(P), \ldots, F_m(P)) \in W \subseteq \mathbb{A}_k^m,$$

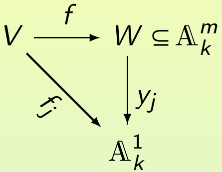
for all points $P \in V$.

A Characterization of Polynomial Maps

Lemma

Let $y_1, \ldots, y_m$ be the coordinate functions on $\mathbb{A}_k^m$. A map $f : V \to W$ is a polynomial map if and only if $f_j := y_j \circ f \in k[V]$, for $j = 1, \ldots, m$.

- Composing f with y_j gives the projection onto the j-ih coordinate. Let $f_j = y_j \circ f$. Then if f is a polynomial map, we have $f_j(P) = F_j(P)$, for some $F_j \in k[x_1, \ldots, x_n]$. Thus f_j is a polynomial map. So $f_j \in k[V]$.



  Suppose, conversely, $f_j = y_j \circ f$ is a polynomial map, for every j.

  Then by definition, there are polynomials $F_1, \ldots, F_m$, such that $f(P) = (F_1(P), \ldots, F_m(P))$, for all $P \in V$.

- Thus, any polynomial map $f : V \to W$ can be written in the form $f = (f_1, \ldots, f_m)$, with $f_1, \ldots, f_m \in k[V]$.

Continuity of Polynomial Maps

Lemma

A polynomial map $f : V \to W$ is continuous in the Zariski topology.

- We must show that if $Z \subseteq W$ is closed, then $f^{-1}(Z)$ is also closed. Suppose
$$Z = \{h_1 = \cdots = h_r = 0\}.$$
Then
$$f^{-1}(Z) = \{h_1 \circ f = \cdots = h_r \circ f = 0\}.$$
So $f^{-1}(Z)$ is also closed.

Example

- We revisit the curves C_0 and C_1.

  Consider the maps:
  - $f : \mathbb{A}_k^1 \to C_0;\ t \mapsto (t, t^2)$;
  - $g : \mathbb{A}_k^1 \to C_1;\ t \mapsto (t^2, t^3)$.

  They are both bijective polynomial maps.
- Let $y_1, \ldots, y_m$ be linear forms in the variables $x_1, \ldots, x_n$.

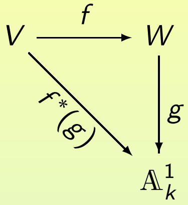
  The map
  $$f = (y_1, \ldots, y_m) : \mathbb{A}_k^n \to \mathbb{A}_k^m$$
  is a polynomial map.

  We saw that, for every irreducible variety V, there is some integer m, such that, for a general choice of $y_1, \ldots, y_m$, the map $\phi = f|_V$ is surjective with finite fibers.

Composition of Polynomial Maps

- Let $V \subseteq \mathbb{A}_k^n$, $W \subseteq \mathbb{A}_k^m$ and $X \subseteq \mathbb{A}_k^\ell$ be algebraic sets.
- Let $f : V \to W$ and $g : W \to X$ be polynomial maps.
- Then $g \circ f : V \to X$ is also a polynomial map.
- This follows immediately from the fact that the composition of a polynomial with a polynomial is again a polynomial.

From a Map Between Varieties to One Between Functions



- Let $f : V \to W$ be a polynomial map.
- For $g \in k[W]$, define

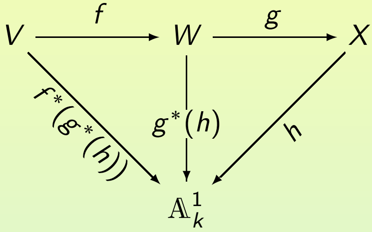
$$f^*(g) := g \circ f.$$

- g is a polynomial function.
- So $g \circ f$ is also a polynomial function.
- Thus, we have a map

$$\begin{array}{rccc} f^* : & k[W] & \to & k[V]; \\ & g & \mapsto & f^*(g) = g \circ f. \end{array}$$

Contravariant Functoriality of Star

- Let $f : V \to W$ and $g : W \to X$ be polynomial maps.
- Then
$$(g \circ f)^* = f^* \circ g^* : k[X] \to k[V].$$



- This follows immediately from the fact that, for $h \in k[X]$, we have
$$(g \circ f)^*(h) = h \circ (g \circ f) = (h \circ g) \circ f = g^*(h) \circ f = f^*(g^*(h)).$$

f^* is a k-Algebra Homomorphism

- The map f^* is a ring homomorphism.
  - $f^*(g_1+g_2)=(g_1+g_2)\circ f=g_1\circ f+g_2\circ f=f^*(g_1)+f^*(g_2)$;
  - $f^*(g_1\cdot g_2)=(g_1\cdot g_2)\circ f=(g_1\circ f)\cdot(g_2\circ f)=f^*(g_1)\cdot f^*(g_2)$.
- For any constant $c\in k$, we have $f^*(c)=c$.
- So f^* is also a k-algebra homomorphism.
- Thus, every polynomial map $f:V\to W$ gives rise to a k-algebra homomorphism
$$f^*:k[W]\to k[V].$$

Every Algebra Homomorphism is of Form f^*

Proposition

Let $\varphi : k[W] \to k[V]$ be a k-algebra homomorphism. Then there exists a unique polynomial map $f : V \to W$, such that

$$\varphi = f^*.$$

- Suppose that $W \subseteq \mathbb{A}_k^m$.
  Let $y_1, \ldots, y_m$ be the coordinate functions on $\mathbb{A}_k^m$.
  Letting $\overline{y}_i = y_i + I(W)$, we have

  $$k[W] = k[y_1, \ldots, y_m]/I(W) = k[\overline{y}_1, \ldots, \overline{y}_m].$$

  Set

  $$f_i := \varphi(\overline{y}_i) \in k[V], \quad i = 1, \ldots, m.$$

  Then $f := (f_1, \ldots, f_m) : V \to \mathbb{A}_k^m$ is a polynomial map.

Every Algebra Homomorphism is of Form f^* (Cont'd)

- First we show that $f(V) \subseteq W$.

  Suppose that $G = G(y_1, \ldots, y_m) \in I(W)$.

  Then in $k[W]$, we have $G(\overline{y}_1, \ldots, \overline{y}_m) = 0$.

  Thus,

$$G(f_1, \ldots, f_m) = G(\varphi(\overline{y}_1), \ldots, \varphi(\overline{y}_m)) = \varphi(G(\overline{y}_1, \ldots, \overline{y}_m)) = 0.$$

  So $f(V) \subseteq W$.

  Next, we show that $\varphi = f^*$.

  The elements $\overline{y}_1, \ldots, \overline{y}_m$ generate the k-algebra $k[W]$.

  So it is enough to show that $\varphi(\overline{y}_i) = f^*(\overline{y}_i) = f_i$.

  This is precisely the definition of the f_i.

  This also shows that $f = (f_1, \ldots, f_m)$ is the unique polynomial map with $\varphi = f^*$.

A Bijection

Corollary

There is a bijection

$$\left\{ f \;\middle|\; \begin{array}{l} f : V \to W \\ \text{a polynomial map} \end{array} \right\} \stackrel{1:1}{\longleftrightarrow} \left\{ \varphi \;\middle|\; \begin{array}{l} \varphi : k[W] \to k[V] \\ \text{a } k\text{-algebra hom.} \end{array} \right\}$$

$$f \quad \mapsto \quad f^*.$$

Isomorphisms

Definition (Isomorphism)

A polynomial map $f : V \to W$ is an **isomorphism** if there is a polynomial map $g : W \to V$, such that

$$f \circ g = \mathrm{id}_W \quad \text{and} \quad g \circ f = \mathrm{id}_V.$$

Corollary

A polynomial map $f : V \to W$ is an isomorphism of varieties if and only if $f^* : k[W] \to k[V]$ is an isomorphism of k-algebras.

- This follows from the fact that

$$(f \circ g)^* = g^* \circ f^*.$$

Example

- Let $A = (\alpha_{ij})$ be an invertible $(n \times n)$ matrix.
- Consider the linear forms

$$y_i = \sum_{j=1}^{n} \alpha_{ij} x_j.$$

- They define a bijective polynomial map

$$f = (y_1, \ldots, y_n) : \mathbb{A}_k^n \to \mathbb{A}_k^n.$$

Example

- Consider the parabola $C_0 = \{y - x^2 = 0\}$ in $\mathbb{A}_k^2$.
- Consider, also, the parametrization

$$\begin{array}{rccc} f: & \mathbb{A}_k^1 & \to & C_0; \\ & t & \mapsto & (t, t^2). \end{array}$$

- The projection $p: \mathbb{A}_k^2 \to \mathbb{A}_k^1$ to the first coordinate, restricted to C_0, gives an inverse map

$$\begin{array}{rccc} g: & C_0 & \to & \mathbb{A}_k^1; \\ & (x, y) & \mapsto & x. \end{array}$$

- Thus, f is an isomorphism.
- We can also see this by considering the map $f^*: k[C_0] \to k[\mathbb{A}_k^1]$.
- Note that

$$\begin{array}{rccc} f^*: & k[C_0] \cong k[x] & \to & k[\mathbb{A}_k^1] = k[t]; \\ & x & \mapsto & t, \end{array}$$

is an isomorphism.

Example

- Now consider the semicubical parabola
$$C_1 = \{(x, y) : y^2 = x^3\}.$$
- The map
$$\begin{array}{rccl} f: & \mathbb{A}_k^1 & \to & C_0; \\ & t & \mapsto & (t^2, t^3), \end{array}$$
is a bijection.
- The image $f^*(k[C_1]) \subseteq k(\mathbb{A}_k^1) = k[t]$ is generated by $f^*(x) = t^2$ and $f^*(y) = t^3$.
- So $f^*(k[C_1]) \neq k[t]$, and, thus, f is not an isomorphism.
- Though f is a bijection, the inverse map $g : C_1 \to \mathbb{A}_k^1$, with
$$g(x, y) = \begin{cases} \frac{y}{x}, & \text{if } (x, y) \neq (0, 0) \\ 0, & \text{if } (x, y) = (0, 0) \end{cases}$$
is not a polynomial map.

Categories

Definition (Category)

A **category** $\mathscr{C}$ consists of the following data:

(1) A class of **objects** $\mathrm{Ob}\mathscr{C}$;

(2) For any two objects $A, B \in \mathrm{Ob}\mathscr{C}$, a set $\mathrm{Mor}_{\mathscr{C}}(A, B)$.

The elements of these sets are called **morphisms**.

(3) For any three objects $A, B, C \in \mathrm{Ob}\mathscr{C}$, there is a map

$$\begin{array}{rcl} \circ : \mathrm{Mor}_{\mathscr{C}}(A,B) \times \mathrm{Mor}_{\mathscr{C}}(B,C) & \to & \mathrm{Mor}_{\mathscr{C}}(A,C); \\ (f,g) & \mapsto & g \circ f. \end{array}$$

Categories (Cont'd)

Definition (Category Cont'd)

These data satisfy the following axioms.

(a) $\circ$ is associative, i.e.

$$(g \circ f) \circ h = g \circ (f \circ h);$$

(b) for all $A \in \mathrm{Ob}\mathscr{C}$, there is a morphism

$$\mathrm{id}_A \in \mathrm{Mor}_{\mathscr{C}}(A, A),$$

called the **identity** of A, such that, for all $B \in \mathrm{Ob}\mathscr{C}$ and for all $f \in \mathrm{Mor}_{\mathscr{C}}(A, B)$ and $g \in \mathrm{Mor}_{\mathscr{C}}(B, A)$, we have

$$f \circ \mathrm{id}_A = f \quad \text{and} \quad \mathrm{id}_A \circ g = g.$$

Example

Among the categories of interest to us are:

(1) The category of sets and maps;
(2) The category of topological spaces and continuous maps;
(3) The category of groups and group homomorphisms.

Functors

Definition (Functor)

For categories $\mathscr{C}$ and $\mathscr{D}$ a **functor** $F:\mathscr{C}\to\mathscr{D}$, which may be either **covariant** or **contravariant**, is given by:

(1) a map $F:\mathrm{Ob}\mathscr{C}\to\mathrm{Ob}\mathscr{D}$;
(2) a collection of maps

$$\begin{array}{ll}\mathrm{Mor}_{\mathscr{C}}(A,B)\to\mathrm{Mor}_{\mathscr{D}}(F(A),F(B)), & \text{in the covariant case,}\\ \mathrm{Mor}_{\mathscr{C}}(A,B)\to\mathrm{Mor}_{\mathscr{D}}(F(B),F(A)), & \text{in the contravariant case,}\end{array}$$

having the following properties:

(1) $F(\mathrm{id}_A)=\mathrm{id}_{F(A)}$.
(2) $F(f\circ g)=\begin{cases}F(f)\circ F(g), & \text{in the covariant case,}\\ F(g)\circ F(f), & \text{in the contravariant case.}\end{cases}$

Examples of Functors

- For every category $\mathscr{C}$, we have the functor $\mathrm{id}_{\mathscr{C}}$ given by the identity.
- For many categories there is a "forgetful" functor, which simply "forgets" some of the structure of the objects in the domain of the functor.
- An example is given by the functor

$$F : \{\text{groups, homomorphisms}\} \to \{\text{sets, maps}\},$$

which maps a group to its underlying set.

Varieties and Ideals

- The relationship between varieties and ideals can now be expressed by the following contravariant functor:

$$F : \left\{ \begin{array}{c} \text{affine varieties;} \\ \text{polynomial maps} \end{array} \right\} \longrightarrow \left\{ \begin{array}{c} \text{finitely generated} \\ \text{reduced } k\text{-algebras;} \\ k\text{-algebra homomorphisms} \end{array} \right\},$$

$$\begin{array}{rcl} V & \mapsto & k[V] \\ (f : V \to W) & \mapsto & (f^* : k[W] \to k[V]). \end{array}$$

- The category on the left is the **category of affine varieties**.
- The category on the right is the **category of finitely generated reduced k-algebras**.
- Often we will refer to a category by referring only to its objects.
- The morphisms are then understood to be the usual morphisms between the objects in question.

Functorial Morphisms or Natural Transformations

Definition (Functorial Morphism)

For two functors $F, G : \mathscr{C} \to \mathscr{D}$, which are both covariant or both contravariant, a **functorial morphism**, or **natural transformation**, $\varphi : F \to G$ is a family of morphisms

$$\{\varphi(A) : F(A) \to G(A) : A \in \mathrm{Ob}\mathscr{C}\},$$

such that, for every morphism $f : A \to B$, with $A, B \in \mathrm{Ob}\mathscr{C}$, we have a commutative diagram (covariant and contravariant case, respectively):

$$\begin{array}{ccc} F(A) & \xrightarrow{\varphi(A)} & G(A) \\ {\scriptstyle F(f)}\downarrow & & \downarrow{\scriptstyle G(f)} \\ F(B) & \xrightarrow[\varphi(B)]{} & G(B) \end{array} \qquad \begin{array}{ccc} F(B) & \xrightarrow{\varphi(B)} & G(B) \\ {\scriptstyle F(f)}\downarrow & & \downarrow{\scriptstyle G(f)} \\ F(A) & \xrightarrow[\varphi(A)]{} & G(A) \end{array}$$

Functorial Isomorphisms and Equivalence of Categories

Definition (Functorial Isomorphism)

The functorial morphism

$$\varphi : F \to G$$

defines a **functorial isomorphism** $\varphi : F \cong G$, if there is a functorial morphism $\psi : G \to F$, such that

$$\psi \circ \varphi = \mathrm{id}_F \quad \text{and} \quad G \circ F = \mathrm{id}_G.$$

Definition (Equivalence of Categories)

A functor $F : \mathscr{C} \to \mathscr{D}$ defines an **equivalence of categories** if there is a functor $G : \mathscr{D} \to \mathscr{C}$, such that

$$G \circ F \cong \mathrm{id}_{\mathscr{C}} \quad \text{and} \quad F \circ G \cong \mathrm{id}_{\mathscr{D}}.$$

A Contravariant Equivalence of Categories

Proposition

The functor defined by

$$\begin{array}{rcl} V & \mapsto & k[V], \\ (f : V \to W) & \mapsto & (f^* : k[W] \to k[V]), \end{array}$$

induces the following contravariant equivalences of categories:

$$\left\{ \begin{array}{l} \text{category of} \\ \text{affine varieties} \end{array} \right\} \leftrightarrow \left\{ \begin{array}{l} \text{category of finitely} \\ \text{generated reduced} \\ k\text{-algebras} \end{array} \right\}$$

$$\left\{ \begin{array}{l} \text{category of irreducible} \\ \text{affine varieties} \end{array} \right\} \leftrightarrow \left\{ \begin{array}{l} \text{category of finitely} \\ \text{generated } k\text{-algebras} \\ \text{which are integral domains} \end{array} \right\}$$

Proof of the Equivalence (Sketch)

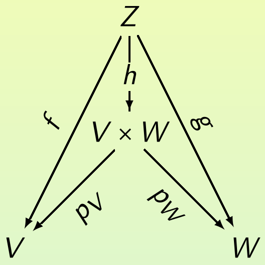
- We construct an inverse functor G.
  Let A be a finitely generated reduced k-algebra.
  Choose generators $a_1,\ldots,a_n$ of A and consider the homomorphism

$$\begin{array}{rcl} \pi : k[x_1,\ldots,x_n] & \to & A = k[a_1,\ldots,a_n]; \\ x_i & \mapsto & a_i. \end{array}$$

  The ideal $I = \ker\pi$ is then a radical ideal.
  It defines a variety $V = V(I)$.
  V is irreducible if and only if I is a prime ideal.
  I.e., V is irreducible if and only if A is an integral domain.
  We set $G(A) = V$.
  By the preceding proposition, every homomorphism $\varphi : A \to B$ of finitely generated reduced k-algebras gives rise to a unique morphism $f : G(B) \to G(A)$, with $\varphi = F(f)$. So we set $G(\varphi) = f$.
  It is easy to check that F and G define an equivalence of categories.

The Product of Two Varieties

- Consider the category of affine varieties.
- Let V and W be affine varieties.
- An affine variety $V \times W$ is the **categorical product** of V and W if there exist polynomial maps $p_V : V \times W \to V$ and $p_W : V \times W \to W$ (the **projection maps**), such that, for any affine variety Z, mapping to both V and W via polynomial maps $f : Z \to V$, $g : Z \to W$, there is a unique polynomial map $h : Z \to V \times W$, such that the diagram commutes.



- For affine varieties V and W, the categorical product of V and W is given by the set-theoretic product $V \times W$.

The Product Variety

Proposition

For varieties $V \subseteq \mathbb{A}_k^n$ and $W \subseteq \mathbb{A}_k^m$, we have:

(1) The set-theoretic product $V \times W \subseteq \mathbb{A}_k^n \times \mathbb{A}_k^m = \mathbb{A}_k^{n+m}$ is a variety;

(2) If V and W are irreducible, then $V \times W$ is also irreducible.

(1) Consider varieties $V \subseteq \mathbb{A}_k^n$ and $W \subseteq \mathbb{A}_k^m$.

Let $f_1, \ldots, f_\ell \in k[x_1, \ldots, x_n]$ and $g_1, \ldots, g_r \in k[y_1, \ldots, y_m]$ be polynomials, such that

$$V = \{f_1 = \cdots = f_\ell = 0\} \quad \text{and} \quad W = \{g_1 = \cdots = g_r = 0\}.$$

Then

$$V \times W = \{f_1 = \cdots = f_\ell = g_1 = \cdots = g_r = 0\}.$$

So $V \times W \subseteq \mathbb{A}_k^n \times \mathbb{A}_k^m = \mathbb{A}_k^{n+m}$ is a variety.

The Product Variety (Cont'd)

(2) First we remark that, for all $w \in W$, the projection onto the first factor defines an isomorphism between $V \times \{w\}$ and V.

Similarly, $\{v\} \times W$ is isomorphic to W, for all $v \in V$.

Suppose there is a decomposition $V \times W = Z_1 \cup Z_2$.

This induces a decomposition

$$V \times \{w\} = (V \times \{w\} \cap Z_1) \cup (V \times \{w\} \cap Z_2).$$

$V \times \{w\}$, being isomorphic to V, is irreducible.

So either $V \times \{w\} \cap Z_1 = V \times \{w\}$ or $V \times \{w\} \cap Z_2 = V \times \{w\}$.

I.e., $V \times \{w\} \subseteq Z_1$ or $V \times \{w\} \subseteq Z_2$.

The Product Variety (Cont'd)

- $V \times \{w\} \subseteq Z_1$ or $V \times \{w\} \subseteq Z_2$.

  We now define

  $$W_i := \{w \in W : V \times \{w\} \subseteq Z_i\}, \quad i = 1, 2.$$

  Then $W_1 \cup W_2 = W$. If we show that the W_i are closed, then, by the irreducibility of W, $W_1 = W$ or $W_2 = W$.

  In the first case $V \times W = Z_1$ and in the second $V \times W = Z_2$.

  For each point $v \in V$, let

  $$W_i^v := \{w \in W : (v, w) \in Z_i\}, \quad i = 1, 2.$$

  Then the sets W_i^v are closed, since $\{v\} \times W_i^v = (\{v\} \times W) \cap Z_i$.

  Since $W_i = \bigcap_{v \in V} W_i^v$, the sets W_i are also closed.
- Note that the Zariski topology on $V \times W$ is not the product topology.

Subsection 3

Rational Functions and Maps

The Function Field of a Variety

- Let V be an irreducible variety.
- Then the coordinate ring $k[V]$ is an integral domain.
- Hence $k[V]$ has a field of fractions.

Definition

The **function field** of V is the field of fractions of $k[V]$, denoted $k(V)$. Elements $f \in k(V)$ are called **rational functions** on V.

- Any rational function can be written as $f = \frac{g}{h}$, with $g, h \in k[V]$.
- In general $k[V]$ need not be a UFD.
- So the representation $f = \frac{g}{h}$, $g, h \in k[V]$ is not necessarily unique.
- We can only give f a well defined value at a point P if there is a representation $f = \frac{g}{h}$, with $h(P) \neq 0$.

Representation of Rational Functions

Definition (Regular Function)

Let $f \in k(V)$ and $P \in V$. The rational function f is called **regular** at P if there is a representation $f = \frac{g}{h}$, with $h(P) \neq 0$. The **domain of definition** of f is defined to be the set

$$\text{dom}(f) := \{P \in V : f \text{ is regular at } P\}.$$

Definition

For every polynomial function $h \in k[V]$, we define

$$V_h := \{P \in V : h(P) \neq 0\}.$$

- Clearly V_h is an open subset of V.

Properties of Rational Functions

Theorem

For a rational function $f \in k(V)$, the following hold:

(1) $\mathrm{dom}(f)$ is open and dense in V.

(2) $\mathrm{dom}(f) = V$ iff $f \in k[V]$.

(3) $\mathrm{dom}(f) \supseteq V_h$ iff $f \in k[V][h^{-1}]$.

(1) For $f \in k(V)$, we define the **ideal of denominators** of f by

$$D_f := \{h \in k[V] : fh \in k[V]\} \subseteq k[V].$$

By definition we have

$$D_f = \{h \in k[V] : \text{there is a representation } f = \frac{g}{h}\} \cup \{0\}.$$

Moreover,

$$V \setminus \mathrm{dom}(f) = \{P \in V : h(P) = 0, \text{for all } h \in D_f\} = V(D_f).$$

Hence, $V \setminus \mathrm{dom}(f)$ is closed. So $\mathrm{dom}(f)$ is open.

Properties of Rational Functions (Cont'd)

Since $\operatorname{dom}(f)$ is obviously nonempty, it is also dense in V.

(2) We have $\operatorname{dom}(f) = V$ if and only if $V(D_f) = 0$.

By Hilbert's Nullstellensatz, this is equivalent to $1 \in D_f$.

This is, in turn, equivalent to $f \in k[V]$.

(3) We have $\operatorname{dom}(f) \supseteq V_h$ if and only if h vanishes on $V(D_f)$.

By Hilbert's Nullstellensatz, this holds iff $h^n \in D_f$, for some $n \geq 1$.

This implies that $f = \frac{g}{h^n} \in k[V][h^{-1}]$.

- Part (2) of the theorem says that the polynomial functions are precisely the rational functions that are "everywhere regular".
- We refer to polynomial functions as **regular functions**.

Local Ring of a Variety at a Point

- We will define the ring $\mathscr{O}(U)$ of functions regular on an open set $U \subseteq V$.
- This will lead to the concept of the *structure sheaf* of a variety.
- We first define the ring of functions on V regular at a point $P \in V$.

Definition (The Local Ring)

The **local ring of** V **at a point** $P \in V$ is the ring

$$\mathscr{O}_{V,P} := \{f \in k(V) : f \text{ is regular at } P\}.$$

Locality of the Local Ring of a Variety at a Point

- Recall that a ring is **local** if it has a unique maximal ideal.
- The local ring $\mathscr{O}_{V,P} \subseteq k(V)$ is a subring of $k(V)$.
- Moreover, we have

$$\mathscr{O}_{V,P} = k[V]\{h^{-1} : h(P) \neq 0\}.$$

- The ring $\mathscr{O}_{V,P}$ is in fact a local ring.
- Its unique maximal ideal is

$$m_P := \left\{ \frac{f}{g} \in k(V) : f, g \in k[V], f(P) = 0, g(P) \neq 0 \right\}.$$

Multiplicatively Closed Systems

Definition (Multiplicatively Closed System)

Let R be a ring. A **multiplicatively closed system** in R is a subset $S \subseteq R^* = R \setminus \{0\}$, with the following properties:

(1) $a, b \in S$ implies $ab \in S$.

(2) $1 \in S$.

Example: A ring R is an integral domain if and only if $R^* = R \setminus \{0\}$ is multiplicatively closed.

Example: An ideal $\mathfrak{p} \neq R$ is a prime ideal if and only if $R \setminus \mathfrak{p}$ is a multiplicatively closed system.

Localization of Rings

- Let R be a ring.
- Let $S \subseteq R \setminus \{0\}$ a multiplicatively closed system.
- Define the following equivalence relation on the product $R \times S$:

$$(r', s') \sim (r'', s'') \Leftrightarrow \text{there exists } s \in S, \text{ with } s(r's'' - r''s') = 0.$$

- The set of equivalence classes is denoted by

$$R_S := R \times S/\sim.$$

- We write

$$\frac{r}{s}$$

to denote the equivalence class of (r, s).

Localization of Rings (Cont'd)

- We can then define addition and multiplication in R_S.
  - Addition is defined by
$$\frac{r}{s}+\frac{r'}{s'}:=\frac{rs'+r's}{ss'};$$
  - Multiplication is defined by
$$\frac{r}{s}\cdot\frac{r'}{s'}:=\frac{rr'}{ss'}.$$
- It is straightforward to check that these operations are well defined.
- The ring R_S is a commutative ring with identity element $1=\frac{1}{1}$.

Definition (Localization)

The ring R_S is called the **localization of** R **with respect to the multiplicative system** S.

Natural Map

- Let R be a ring.
- Let S be a multiplicatively closed system in R.
- The natural map is a ring homomorphism,

$$\begin{array}{rcl} R & \to & R_S; \\ r & \mapsto & \frac{r}{1}. \end{array}$$

Example

- Let R be an integral domain.
- Let
$$S = R^* = R \setminus \{0\}.$$
- Then R_S is the field of fractions of R.
- In this case, the map
$$R \to R_S$$
is injective.
- So R may be identified with its image in R_S.

Example

- Let R be a ring.
- Let $\mathfrak{p} \subsetneq R$ be a prime ideal.
- Let
$$S_{\mathfrak{p}} = R \backslash \mathfrak{p}.$$
- The ring
$$R_{\mathfrak{p}} := R_{S_{\mathfrak{p}}}$$
is called the **localization of R at $\mathfrak{p}$**.
- In fact $R_{\mathfrak{p}}$ is a local ring.
- Its unique maximal ideal is
$$m_{\mathfrak{p}} := \left\{ \frac{p}{s} : p \in \mathfrak{p}, s \in S \right\} \subsetneq R_{\mathfrak{p}}.$$
- To see this, consider an element of $R_{\mathfrak{p}}$ not in $m_{\mathfrak{p}}$.
It is of the form $\frac{s'}{s}$, with $s' \in S$.
So it has an inverse $\frac{s}{s'}$ and is, therefore, a unit.

Example

- Let R be an integral domain.
- Let $0 \neq f \in R$.
- Set
$$S_f := \{f^n : n \geq 0\}.$$
- We define
$$R_f := R_{S_f}.$$
- Since R is an integral domain, the map
$$\begin{array}{rcl} R & \to & R_f; \\ r & \mapsto & \frac{r}{1} \end{array}$$
is injective.
- Identifying R with its image in R_f and in the field of fractions, we have an equality
$$R_f = R[f^{-1}] \subseteq \text{field of fractions of } R.$$

Construction of the Local Ring by Localization

- The local ring $\mathscr{O}_{V,P}$, was defined as a subring of the function field $k(V)$.
- $\mathscr{O}_{V,P}$ may also be constructed by localization.
- Consider a point $P \in V$.
- The ideal corresponding to P is

$$\overline{M}_P = \{f \in k[V] : f(P) = 0\} = \overline{I(\{P\})} = I(\{P\}) + I(V) \subseteq k[V].$$

- This ideal is maximal.
- We have an equality

$$\mathscr{O}_{V,P} = k[V]_{\overline{M}_P}.$$

- I.e., $\mathscr{O}_{V,P}$ arises through localization of the coordinate ring at $\overline{M}_P$.
- The maximal ideal of $\mathscr{O}_{V,P}$ is given by

$$m_P = \{f \in \mathscr{O}_{V,P} : f(P) = 0\}.$$

The Structure Sheaf of a Variety

- For every nonempty open set $U \subseteq V$, we define

$$\mathscr{O}(U) := \mathscr{O}_V(U) := \{f \in k(V) : f \text{ is regular on } U\}.$$

- Further, we set

$$\mathscr{O}_V(\emptyset) := \{0\}.$$

- Then $\mathscr{O}_V(U)$ is a ring.
- In addition it is a k-algebra.
- The set of rings $\mathscr{O}_V(U)$, together with the natural restriction homomorphisms, forms the **structure sheaf** $\mathscr{O}_V$.
- The local ring $\mathscr{O}_{V,P}$ is called the **stalk** of the structure sheaf at the point P.
- The elements of $\mathscr{O}_{V,P}$ are called **function germs**.

Reformulation of the Theorem

- The preceding theorem can be formulated as follows.
  - Part 2:
$$\mathscr{O}(V) = k[V];$$
  - Part 3:
$$\mathscr{O}(V_h) = k[V][h^{-1}] = k[V]_h,$$
    where the ring $k[V]_h$ is the localization of the coordinate ring $k[V]$ with respect to the multiplicative system $\{h^n : n \geq 0\}$.

Rational Maps

- We consider maps on V which are not everywhere defined.

Definition (Rational Map)

(1) A **rational map** $f : V \dashrightarrow \mathbb{A}_k^n$ is an n-tuple

$$f = (f_1, \dots, f_n)$$

of rational functions $f_1, \dots, f_n \in k(V)$.

The map f is called **regular at the point** P if all f_i are regular at P.

The **domain of definition** $\text{dom}(f)$ is the set of all regular points of f, i.e.

$$\text{dom}(f) = \bigcap_{i=1}^{n} \text{dom}(f_i).$$

(2) For an affine variety $W \subseteq \mathbb{A}_k^n$, a **rational map** $f : V \dashrightarrow W$ is a rational map $f : V \dashrightarrow \mathbb{A}_k^n$, such that $f(P) \in W$, for all regular points $P \in \text{dom}(f)$.

- By the theorem, $\text{dom}(f)$ is a nonempty open subset of V.

Definability of Composition

- In contrast to the situation for polynomial maps, for rational maps $f : V \dashrightarrow W$ and $g : W \dashrightarrow X$, the composition

$$g \circ f : V \overset{f}{\dashrightarrow} W \overset{g}{\dashrightarrow} X$$

cannot always be defined in a meaningful way.
Example: Consider two rational maps.

- f is defined by

$$\begin{array}{rccc} f: & \mathbb{A}_k^1 & \to & \mathbb{A}_k^2; \\ & x & \mapsto & (x,0). \end{array}$$

- g is defined by

$$\begin{array}{rccc} g: & \mathbb{A}_k^2 & \dashrightarrow & \mathbb{A}_k^1; \\ & (x,y) & \mapsto & \frac{x}{y}. \end{array}$$

Note that

$$f(\mathbb{A}_k^1) \cap \mathrm{dom}(g) = \emptyset.$$

So the composition is nowhere defined.

Star for Rational Maps

- Consider a rational map $f : V \dashrightarrow W$.
- We want to define a map $f^* : k(W) \to k(V)$ with

$$f^*(g) = g \circ f.$$

- We have constructed a homomorphism $f^* : k[W] \to k[V]$.
- So we know that, for $g \in k[W]$, the function $f^*(g) \in k(V)$ is well defined.
- It is possible that $f^*(h) = 0$, for some $h \in k[W]$, with $h \neq 0$.
- In that case, we cannot define $f^*(\frac{g}{h})$ to be $\frac{f^*(g)}{f^*(h)}$.

Dominant Rational Maps and Inverse Images

Definition (Dominant Rational Map)

A rational map $f : V \dashrightarrow W$ is called **dominant** if $f(\mathrm{dom}(f))$ is a Zariski dense subset of W.

Definition (Inverse Image)

For a rational map $f : V \dashrightarrow W$ and a subset $U \subseteq W$, we define the **inverse image** of U under f by

$$f^{-1}(U) := \{P \in \mathrm{dom}(f) : f(P) \in U\}.$$

Dominant Rational Maps and Definability

- Suppose $f : V \dashrightarrow W$ is dominant.
- Let $g : W \dashrightarrow \mathbb{A}^1_k$ be a rational map.
- By a preceding theorem, $\text{dom}(g)$ is a nonempty open subset of W.
- By a preceding lemma, $f^{-1}(\text{dom}(g))$ is a dense open subset of $\text{dom}(f)$.
- Thus, the composition $g \circ f : V \dashrightarrow \mathbb{A}^1_k$ is defined on the dense open subset
$$f^{-1}(\text{dom}(g)) \subseteq V.$$

Algebraic Reformulation

- Let $f : V \dashrightarrow W$ be a rational map.
- Consider the corresponding homomorphism $f^* : k[W] \to k(V)$.
- For all $g \in k[W]$, we have
$$f^*(g) = 0 \Longleftrightarrow f(\mathrm{dom}(f)) \subseteq V(g).$$
- Thus,
$$f^* : k[W] \to k(V) \text{ is injective} \Leftrightarrow f \text{ is dominant.}$$
- Hence, if f is dominant, then we can extend f^* to a homomorphism $f^* : k(W) \to k(V)$ by setting
$$f^*\left(\frac{g}{h}\right) := \frac{f^*(g)}{f^*(h)}.$$
- If $f : V \dashrightarrow W$ and $g : W \dashrightarrow X$ are dominant, then $g \circ f : V \dashrightarrow X$ is also dominant.

The Map f^*

Theorem

Let V and W be irreducible affine varieties.

(1) Every dominant rational map $f : V \dashrightarrow W$ defines a k-linear homomorphism $f^* : k(W) \to k(V)$.

(2) Conversely, if $f : k(W) \to k(V)$ is a k-linear homomorphism, then there exists a unique dominant rational map $\varphi : V \dashrightarrow W$, with

$$\varphi = f^*.$$

(3) If $f : V \dashrightarrow W$ and $g : W \dashrightarrow X$ are dominant, then $g \circ f : V \dashrightarrow X$ is also dominant and

$$(g \circ f)^* = f^* \circ g^*.$$

The Map f^* (Cont'd)

- Parts (1) and (3) have already been discussed.

(2) Suppose that $W \subseteq \mathbb{A}_k^m$.
The coordinate functions $y_1, \ldots, y_m$ generate the field $k(W)$.
We set $f_i := \varphi(y_i) \in k(V)$ and

$$f := (f_1, \ldots, f_m) : V \dashrightarrow W.$$

This map has image in W.
By construction $f^* = \varphi$.
It remains to show that f is dominant.
Since $f^* = \varphi$, we have

$$f^* |_{k[w]} = \varphi |_{k[w]} .$$

Since φ is a field homomorphism, φ is injective.
So $f^* |_{k[w]}: k[W] \to k(V)$ is also injective.
Hence, f is dominant.

Quasi-Affine Varieties

- Open subsets of affine varieties behave similarly to affine varieties.

Definition (Quasi-Affine Variety)

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

Morphisms of Quasi-Affine Varieties

Definition

Let U_1 and U_2 be irreducible quasi-affine varieties, contained in the affine varieties V and W, respectively.

(1) A **morphism** $f : U_1 \to W$ is a rational map $f : V \dashrightarrow W$, with $U_1 \subseteq \mathrm{dom}(f)$, i.e., f is regular at every point $P \in U_1$.

(2) A **morphism** $f : U_1 \to U_2$ is a morphism $f : U_1 \to W$, with $f(U_1) \subseteq U_2$.

(3) An **isomorphism** of quasi-affine varieties is a morphism $f : U_1 \to U_2$, such that, there is a morphism $g : U_2 \to U_1$, with

$$g \circ f = \mathrm{id}_{U_1} \quad \text{and} \quad f \circ g = \mathrm{id}_{U_2}.$$

- For two irreducible affine varieties V and W,

$$\{f : f : V \to W \text{ a morphism}\} = \{f : f : V \to W \text{ a polynomial map}\}.$$

Example

- Consider again the semicubical parabola
$$C_1 = \{(x,y) \in \mathbb{A}_k^2 : y^2 - x^3 = 0\}.$$
Recall that it has a parametrization
$$\begin{array}{rccc} f: & \mathbb{A}_k^1 & \to & C_1; \\ & t & \mapsto & (t^2, t^3). \end{array}$$
This parametrization is not an isomorphism.
So $k[\mathbb{A}_k^1]$ and $k[C_1]$ are not isomorphic.
However, the restriction
$$f : \mathbb{A}_k^1 \backslash \{0\} \to C_1 \backslash \{(0,0)\}$$
is an isomorphism of quasi-affine varieties.
Its inverse is
$$g(x,y) = \frac{y}{x}.$$
- In terminology to come, $\mathbb{A}_k^1$ and C_1 are **birationally equivalent**.

Example (Cont'd)

- We saw $\mathbb{A}_k^1$ and C_1 are birationally equivalent.
  The theorem gives us a map
  $$f^* : k(C_1) \to k(\mathbb{A}_k^1),$$
  with
  $$f^*\left(\frac{x}{y}\right) = t.$$
  Thus f^* is surjective.
  Moreover, f^* is a nonzero field homomorphism.
  So f^* is also injective.
  So the function fields $k(\mathbb{A}_k^1) = k(t)$ and $k(C_1)$ are isomorphic.
  We will see that the function fields of any birationally equivalent varieties are isomorphic, and vice versa.

The Quasi-Affine Variety V_f

- Let V be an affine variety.
- Let $f \in k[V]$.
- We defined the quasi-affine variety

$$V_f = V \setminus V(f) = \{P \in V : f(P) \neq 0\}.$$

Proposition

The quasi-affine variety V_f is isomorphic to an affine variety with coordinate ring

$$k[V_f] = k[V][f^{-1}] = k[V]_f.$$

- In the proof we use again Rabinowitsch's trick.

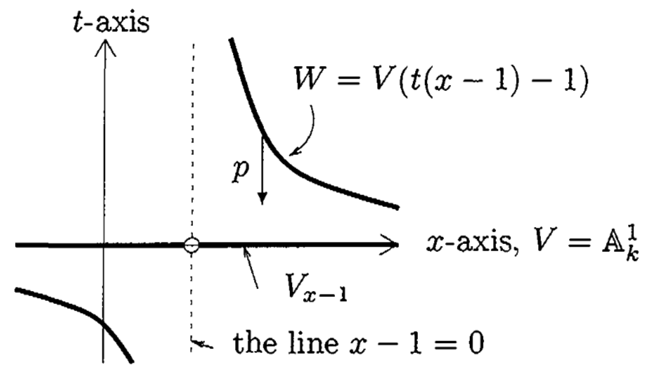
The Quasi-Affine Variety V_f (Cont'd)

- Let
$$J := I(V) \subseteq k[x_1,\ldots,x_n]$$
be the ideal of the variety $V \subseteq \mathbb{A}_k^n$.
Let $F \in k[x_1,\ldots,x_n]$ be a polynomial, with $F|_V = f$.
We set
$$J_f := (J, tF-1) \subseteq k[x_1,\ldots,x_n,t].$$
Claim: V_f is isomorphic to the affine variety $W = V(J_F) \subseteq \mathbb{A}_k^{n+1}$.
Consider the maps:
    - $p : W \to V_f$, with $(x_1,\ldots,x_n,y) \mapsto (x_1,\ldots,x_n)$;
    - $q : V_f \to W$, with $(x_1,\ldots,x_n) \mapsto \left(x_1,\ldots,x_n,\frac{1}{F(x_1,\ldots,x_n)}\right)$.

  These are mutually inverse morphisms.
  The conclusion now follows.

Illustration of the Proposition

- The figure illustrates the proposition for $V = \mathbb{A}_k^1$ and $f = x - 1$.



- The quasi-affine variety $\mathbb{A}_k^1 \setminus \{1\} = (\mathbb{A}_k^1)_{(x-1)} \subseteq \mathbb{A}_k^1$ is isomorphic to the affine variety $W \subseteq \mathbb{A}_k^2$, given by $t(x-1) = 1$.
- In this case the map p is the projection to the x-axis.

Affine Basis of the Zariski Topology

- Every open set in V is a union of sets of the form V_f.
- Hence, the sets V_f form a basis of the Zariski topology of V.

Corollary

The Zariski topology on V has a basis of affine sets.

- By the corollary, we may, without loss of generality, restrict attention to affine varieties.
- There are quasi-affine varieties which are not affine.

  Example: $\mathbb{A}_k^2 \setminus \{(0,0)\}$ is a quasi-affine variety that is not affine.

Abstract Affine Varieties

- We give a possible definition of an *abstract affine variety*.
- It allows considering affine varieties without reference to a surrounding affine space.

Definition (Abstract Affine Variety)

An **abstract affine variety** over a field k is a pair $(V, k[V])$ consisting of:

- A set V;
- A k-algebra $k[V]$ of functions on V, such that:
  - $k[V]$ is generated by finitely many elements $x_1, \ldots, x_n$ over k;
  - The map

$$\begin{array}{rcl} V & \to & \mathbb{A}_k^n; \\ P & \mapsto & (x_1(P), \ldots, x_n(P)), \end{array}$$

  defines a bijection between V and a Zariski closed subset of $\mathbb{A}_k^n$.