Algebraic Varieties
Lecture Notes

Note taker: Jacky567

Qiuzhen College, Tsinghua University

2025 Spring

Contents

Chapter 1

Affine varieties

1.1 The Zariski topology

Notation 1.1.1. We use k to denote an algebraic closed field, e.g. $k = \mathbb{C}, \bar{\mathbb{F}}_p, \overline{\mathbb{C}(x)}$, etc.

Def 1.1.1. An affine space for the k-vector space k^n is a set A together with an action of k^n on A, say $k^n \times A \to A, (v, a) \mapsto v + a$, such that

(1) for any $a \in A$, $0 + a = a$.

(2) for any $v, w \in k^n$, $a \in A, v + (w + a) = (v + w) + a$

(3) for any $a \in A$, the map $k^n \to A, v \mapsto v + a$ is bijection.

Def 1.1.2. $\mathbb{A}^n_k$ is the underlying affine space of k^n, call an affine $n-$space over k.

Remark 1.1.1. The underlying set of k^n and $\mathbb{A}^n_k$ are actually the same, but we need to "forget" the rule of 0 as origin on $\mathbb{A}^n_k$.

Def 1.1.3. A polynomial $f \in k[x_1, \cdots, x_n]$ gives a map $f : \mathbb{A}^n \to k$, and we call a k-valued function on $\mathbb{A}^n$ regular if it is defined by a polynomial.

Prop 1.1.1. *A polynomial $f \in k[x_1, \cdots, x_n]$ is completely determined by the regular function it defines.*

Proof. Let g be another polynomial such that the regular function of f, g agree at every point.
When $n = 1$, $f - g \in k[x_1]$ has infinity many roots, *i.e.* $f = g \in k[x_1]$.
Assume $f = g \in k[x_1, \cdots, x_k]$ for $k < n$ and let

$$f - g = \sum_{i=0}^{d} h_i(x_1, \cdots, x_{n-1}) x_n^i,$$

where $h_i \in k[x_1, \cdots, x_{n-1}]$.
Then for any fixed $x_1, \cdots, x_{n-1}$, we must have $h_i(x_1, \cdots, x_{n-1}) = 0$.
So the regular function of h_i is zero at every point.
Therefore by the induction assumption, $h_i = 0, i.e. f = g$.
Hence f is completely determined by the regular function it defines. □

Def 1.1.4. For $f \in k[x_1, \cdots, x_n]$, denote $Z(f)$ be the zero locus of $f : \mathbb{A}^n \to k$ and $\mathbb{A}^n_f = \mathbb{A}^n \backslash Z(f)$.

Prop 1.1.2. *If* $\deg(f) > 0$, *then* $Z(f) \neq \mathbb{A}^n, \varnothing$.

Proof. If $Z(f) = \mathbb{A}^n$, then the regular function of f is zero everywhere, *i.e.* $f = 0$.
Let
$$f = \sum_{i=0}^{d} h_i(x_1, \cdots, x_{n-1})x_n^i,$$
where $h_i \in k[x_1, \cdots, x_{n-1}]$.
Then $h_d \neq 0$, *i.e.* $Z(h_d) \neq \mathbb{A}^{n-1}$ and fix $(x_1, \cdots, x_{n-1})$ such that $h_d(x_1, \cdots, x_{n-1}) \neq 0$.
So $f(x_1, \cdots, x_{n-1}, \bullet)$ has a root by fundamental theorem of algebra.
Hence $Z(f) \neq \mathbb{A}^n, \varnothing$. □

Def 1.1.5. A principal subset of $\mathbb{A}^n$ is a subset of form $\mathbb{A}^n_f$.

Def 1.1.6. A hypersurface of $\mathbb{A}^n$ is a subset of form $Z(f)$ with $\deg(f) > 0$.

Prop 1.1.3. *The collection of principal subsets of $\mathbb{A}^n$ form a basis of a topology on $\mathbb{A}^n$, called the Zariski topology on $\mathbb{A}^n$.*

Proof. $\mathbb{A}^n_{f_1} \cap \mathbb{A}^n_{f_2} = \mathbb{A}^n \backslash (Z(f_1) \cup Z(f_2)) = \mathbb{A}^n_{f_1 f_2}$. □

Prop 1.1.4. *For the Zariski topology, an open subset is a union of certain principal subsets, a closed subset is an intersection of certain $Z(f)$.*

Proof. By definition of the basis of topology. □

Def 1.1.7. For a subset $J \subset k[x_1, \cdots, x_n]$, denote $Z(J) = \bigcap_{f \in J} Z(f)$, these are exactly all Zariski-closed subsets.

Exam 1.1.1. *The Zariski topology on $\mathbb{A}^1$ is the cofinite topology: closed subsets are the finite subsets.*

Def 1.1.8. For subsets $X \subset \mathbb{A}^n$, denote by $I(X)$ the set of polynomials vanishing on X.

Prop 1.1.5. *$I(X)$ is an ideal of $k[x_1, \cdots, x_n]$.*

Proof. For any $f \in I(X)$ and $g \in k[x_1, \cdots, x_n]$, $Z(fg) \supset X$.
So $I(X)$ is the set of polynomials. □

Remark 1.1.2. We have the following commutative diagram:

$$\begin{array}{ccc}
\{\text{subsets of } \mathbb{A}^n\} & \xrightarrow{\quad I \quad} & \{\text{ideals of } k[x_1, \cdots, x_n]\} \\
\cup & & \cap \\
\{\text{closed subsets of } \mathbb{A}^n\} & \xleftarrow{\quad Z \quad} & \{\text{subsets of } k[x_1, \cdots, x_n]\}
\end{array}$$

Eventually, closed subsets of $\mathbb{A}^n \xleftrightarrow{1:1}$radical ideals of $k[x_1, \cdots, x_n]$(we will prove this later).

Prop 1.1.6. *(1) $X_1 \subset X_2 \subset \mathbb{A}^n$, then $I(X_1) \supset I(X_2)$.*

(2) $J_1 \subset J_2 \subset k[x_1, \cdots, x_n]$, then $Z(J_1) \supset Z(J_2)$.

(3) $I(X_1 \cup X_2) = I(X_1) \cap I(X_2)$.

(4) $Z(J_1 \cup J_2) = Z(J_1) \cap Z(J_2)$.

Proof. (1) For $f \in I(X_2)$, $Z(f) \supset X_2 \supset X_1, i.e. f \in I(X_1)$.

(2) $Z(J_2) = \bigcap_{f \in J_2} Z(f) \subset \bigcup_{F \in J_1 \subset J_2} Z(f) = Z(J_1)$.

(3) $I(X_1 \cup X_2) \subset I(X_1), I(X_2)$.
And for $f \in I(X_1) \cap I(X_2)$, $Z(f) \supset X_1 \cup X_2$, *i.e.* $f \in I(X_1 \cup X_2)$.

(4) $Z(J_1 \cup J_2) = \bigcap_{f \in J_1 \cup J_2} Z(f) = \left(\bigcap_{f \in J_1} Z(f) \right) \cap \left(\bigcap_{f \in J_2} Z(f) \right) = Z(J_1) \cap Z(J_2)$.

□

Def 1.1.9. For any $X \subset \mathbb{A}^n$, denote by $\bar{X}$ the Zariski closure of X.

Prop 1.1.7. *(1)* $Z(I(X)) = \bar{X}$.

(2) $I(Y) = I\left(\bar{Y}\right)$.

(3) two polynomials $f, g \in k[x_1, \cdots, x_n]$ *have same restriction to* Y *iff* $f - g \in I(Y) = I\left(\bar{Y}\right)$.

(4) $k[x_1, \cdots, x_n]/I(Y)$ *contains distinct* k*-valued functions on* Y*. (also on* $\bar{Y}$*)*

Proof. (1) Since $Z(f) \supset X$ for every $f \in I(X)$.
So $X \subset Z(I(X)) \subset Z\left(I\left(\bar{X}\right)\right) = \bar{X}$.
And since $Z(I(X))$ is closed.
Hence $Z(I(X)) = \bar{X}$.

(2) For $f \in I(Y)$, $Z(f) \supset \bar{Y}$, *i.e.* $f \in I(\bar{Y})$.
And since $I(Y) \supset I(\bar{Y})$.
So $I(Y) = I(\bar{Y})$.

(3) Since $f = g$ in Y.
So $f - g = 0$ in Y, *i.e.* $f - g \in I(Y) = I(\bar{Y})$.

(4) For $[f] \neq [g] \in k[x_1, \cdots, x_n]/I(Y)$, $[f - g] \neq 0$.
So $f - g \notin I(Y)$, *i.e.* f and g are distinct on Y.

□

Def 1.1.10. Let $Y \subset \mathbb{A}^n$ be closed, denote $k[Y] = k[x_1, \cdots, x_n]/I(Y)$, called the coordinate ring of Y, and k-valued function on Y is called regular if it is determined by a element in $k[Y]$.

Remark 1.1.3. We can say that the coordinate ring of Y is the set of regular functions on Y.

Def 1.1.11. Given a closed subset $Y \subset \mathbb{A}^n$, Y also has a topology.
denote $I_Y(X) = I(X)/I(Y)$ when $X \subset Y$, for subset $J \subset k[Y]$, let $Z_Y(J)$ be the zero locus of $J \cup I(Y)$, then $Z_Y(J)$ is a closed subset of Y.

Remark 1.1.4. Similar to remark 1.1.2, we have the commutative diagram:

$$\begin{array}{ccc} \{\text{subsets of } Y\} & \xrightarrow{I_Y} & \{\text{ideals of } k[Y] = k[\mathbb{A}^n]/I(Y)\} \\ \cup & & \cap \\ \{\text{closed subsets of } Y\} & \xleftarrow{Z_Y} & \{\text{subsets of } k[Y]\} \end{array}$$

Prop 1.1.8. $Z_Y(I_Y(X)) = \bar{X}$.

Proof. $Z_Y(I_Y(X)) = \left(\bigcap_{[f] \in I_Y(X)} Z(f) \right) \cap Y = Z(I(X)) \cap Y = \bar{X}$. □

Def 1.1.12. Let R be a ring, $J \subset R$ is an ideal, define the radical of J

$$\sqrt{J} = \{a \in R | \exists m \in \mathbb{Z}^+, s.t. a^m \in J\}.$$

We say J is a radical ideal if $J = \sqrt{J}$.
We say R is reduced ring if (0) is radical, *i.e.* R has no nonzero nilpotents.

Prop 1.1.9. *(1) A prime ideal is radical.*

(2) $J \subset R$ is a ideal, then J is radical iff R/J is reduced.

Proof. (1) Suppose $\mathfrak{p}$ is a prime ideal and $a^m \in \mathfrak{p}$ but $a \notin \mathfrak{p}$.

WLOG, we assume $a^{m-1} \notin \mathfrak{p}$.

Then $a \cdot a^{m-1} \notin \mathfrak{p}$, contradiction!

So $\mathfrak{p}$ is a radical ideal.

(2) J is radical$\Leftrightarrow$For any $a \notin J$ and $n \in \mathbb{Z}^+$, $a^n \notin J$

$\Leftrightarrow$For any $[a] \neq 0$ in R/J and $n \in \mathbb{Z}^+$, $[a]^n \neq (0)$.

$\Leftrightarrow$ R/J is reduced.

□

Prop 1.1.10. *(1) For subset $X \subset Y$, we have $I_Y(X) \subset k[Y]$ is radical.*

(2) For subset $J \subset k[Y]$, we have $Z_Y(J) = Z_Y(\langle J \rangle) = Z_Y\left(\sqrt{\langle J \rangle}\right)$

Proof. (1) Let $f \in \sqrt{I_Y(X)}$.

Then there exist $m \in \mathbb{Z}^+$, such that $f^m \in I_Y(X)$, *i.e.* $f^m\big|_X = 0$.

So $f\big|_X = 0$, *i.e.*$f \in I_Y(X)$.

(2) Let $[f] \in J$.

Then $Z_Y([fg]) \supset Z_Y([f]) \supset Z_Y(J)$ for $[g] \in k[Y]$.

And for $[h] \in k[Y]$ such that $[h]^n = [fg]$, $Z([h]) \supset Z([fg]) \supset Z_Y(J)$.

So $Z_Y\left(\sqrt{\langle J \rangle}\right), Z_Y(\langle J \rangle) \supset Z_Y(J)$.

And since $Z_Y\left(\sqrt{\langle J \rangle}\right), Z_Y(\langle J \rangle) \subset Z_Y(J)$.

Hence $Z_Y\left(\sqrt{\langle J \rangle}\right) = Z_Y(\langle J \rangle) = Z_Y(J)$.

□

Remark 1.1.5. We now have the correspondence

$$\{\text{close subsets of } \mathbb{A}^n\} \underset{Z}{\overset{I}{\rightleftarrows}} \{\text{radical ideals of } k[\mathbb{A}^n]\}$$

$$\{\text{close subsets of } Y\} \underset{Z_Y}{\overset{I_Y}{\rightleftarrows}} \{\text{radical ideals of } k[Y]\}$$

Actually, $I (I_Y$ resp.) and $Z (Z_Y$ resp.) are inverse to each other, thanks to:

Thm 1.1.1 (Hilbert's Nullstellensatz)**.** *For any ideal $J \subset k[x_1, \cdots, x_n]$, we have $I(Z(J)) = \sqrt{J}$*

We will prove this theorem in the third section.

Exam 1.1.2. *For a point $p = (a_1, \cdots, a_n) \in \mathbb{A}^n$, then $I(\{p\}) = (x_1 - a_1, \cdots, x_n - a_n)$ is a maximal ideal.*

Proof. Let $\mathfrak{m} = (x_1 - a_1, \cdots, x_n - a_n)$.
Then $Z(\mathfrak{m}) = p, i.e. \mathfrak{m} \subset I(\{p\})$.
And since $k[x_1, \cdots, x_n]/\mathfrak{m} = k$ is a field.
So $\mathfrak{m}$ is maximal.
And since $x_1 - q \notin I(\{p\})$ for $q \neq a_1$.
Hence $I(\{p\}) \neq k[x_1, \cdots, x_n], i.e. \mathfrak{m} = I(\{p\})$. □

Prop 1.1.11. *Given a maximal ideal $\mathfrak{m} \subset k[x_1, \cdots, x_n]$, $\mathfrak{m}$ corresponds to a point.*

Proof. Since $Z(\mathfrak{m})$ is a nonempty closed set of $\mathbb{A}^n$ and $\mathfrak{m}$ is maximal.
So there is no nonempty closed set strictly contained in $Z(\mathfrak{m})$, *i.e.* $Z(\mathfrak{m}) = \{p\}$.
Hence $\mathfrak{m} \subset I(Z(\mathfrak{m})) = I(\{p\}) = (x_1 - a_1, \cdots, x_n - a_n), i.e.\ \mathfrak{m} = (x_1 - a_1, \cdots, x_n - a_n)$. □

1.2 Irreducibility and decomposition

Def 1.2.1. Let Y be a nonempty topological space, we say that Y is irreducible if it is not the union of two closed proper subsets.

Prop 1.2.1. *nonempty Y is irreducible iff any nonempty open subset of Y is dense in Y.*

Proof. If $Y = Y_1$ with proper closed Y_1, Y_2, then $Y - Y_1 \subset Y_2$ is nonempty open subset of Y but not dense.
Conversely, suppose $U \subset Y$ is nonempty open and $\bar{U} \subsetneqq Y$, then $Y = \bar{U} \cup (Y - U)$. □

Def 1.2.2. We call a maximal irreducible subset of Y an irreducible component of Y.

Lemma 1.2.1. *If $A_1 \subset A_2 \subset \cdots \subset Y$, A_i is irreducible, then $\bigcup A_i$ is also irreducible.*

Proof. Suppose $\bigcup A_i = C_1 \cup C_2$ where C_1, C_2 are proper closed subsets.
Then $A_i = (A_i \cap C_1) \cup (A_i \cap C_2)$.
And since A_i are irreducible.
So $A_i \subset C_1$ or $A_i \subset C_2$.
Therefore C_1 or C_2 contains all A_i.
Hence $C_1 = \bigcup A_i$ or $C_2 = \bigcup A_i$, contradiction! □

Thm 1.2.1. *Every irreducible subset of Y is contained in an irreducible component.*
In particular, Y equals to the union of its irreducible components.

Proof. By Zorn's lemma. □

Prop 1.2.2. *A Hausdorff topological space is irreducible iff it is one point.*

Proof. Suppose X contain two points a, b.
Then there exist two disjoint open set U, V such that $a \in U, b \in V$.
So $(X \backslash U) \cup (X \backslash V) = X \backslash (U \cap V) = X$, *i.e.* X is not irreducible, contradiction!
Hence X consists of a single point. □

Lemma 1.2.2. *If Y is irreducible, then every open nonempty subset of Y is irreducible.*
Conversely, if $C \subset Y$ is an irreducible, then $\bar{C}$ is also irreducible.
In particular, an irreducible component of Y is closed.

Proof. Suppose Y is irreducible, $\varnothing \neq U \subset Y$ is open, then every nonempty open subset of U is dense in Y.

So it is also dense in U,*i.e.* U is irreducible.

Suppose $C \subset Y$ is irreducible subspace and $V \subset \bar{C}$ is nonempty open subset.

Then $V \cap C \neq \varnothing$ is open in C.

Therefore $V \cap C$ is dense in C and $\bar{C}$.

Hence V is dense in $\bar{C}$, *i.e.* $\bar{C}$ is irreducible. ◻

Prop 1.2.3. *A closed subset Y of $\mathbb{A}^n$ is irreducible iff $I(Y)$ is prime ideal$\Leftrightarrow$ $k[Y] = k[\mathbb{A}^n]/I(Y)$ is a domain.*

Proof. Suppose Y is irreducible, let $f, g \in k[x_1, \cdots, x_n]$ with $fg \in I(Y)$.

Then $Y \subset Z(fg) = Z(f) \cup Z(g)$.

So $Y \subset Z(f)$ or $Y \subset Z(g)$,*i.e.* $f \in I(Y)$ or $g \in I(Y)$.

Suppose $Y = Y_1 \cup Y_2$ with Y_i closed proper subsets.

Then for $i \in \{1, 2\}$, $\exists f_i \in I(Y_i)\backslash I(Y)$.

So $f_1 f_2 \in I(Y)$ but $f_1, f_2 \notin I(Y)$. ◻

Exam 1.2.1. *In $\mathbb{A}^n$, point $\xleftrightarrow{1:1}$ maximal ideal*

irreducible closed set $\xleftrightarrow{1:1}$ prime ideal

irreducible component $\xleftrightarrow{1:1}$ minimal prime ideal

$\mathbb{A}^n \xleftrightarrow{1:1} (0)$

Given closed $Y \subset \mathbb{A}^n$, $Y \xleftrightarrow{1:1} (0) \subset k[Y]$.

closed subset of Y $\xleftrightarrow{1:1}$ radical ideal of $k[Y]$.

point $\xleftrightarrow{1:1}$ maximal ideal of $k[Y]$

irreducible closed subset of Y $\xleftrightarrow{1:1}$ prime ideal of $k[Y]$.

irreducible components $\xleftrightarrow{1:1}$ minimal prime ideal of $k[Y]$

Def 1.2.3. A ring R is called a UFD if it has no zero divisors and each principal ideal is a product of principal prime ideals: $(a) = (p_1)\cdots(p_s)$ and $(p_1), \cdots, (p_s)$ is unique up to order.

Remark 1.2.1. (p) is principal prime ideal iff $p|ab \Rightarrow p|a$ or $p|b$ and we call p prime element.

Prop 1.2.4. *In UFD, irreducible element is equivalent to prime element.*

Proof. Suppose (p) is irreducible.

For $ab \in (p)$, let $ab = cp$ for some $c \in R$.

Then by the uniqueness of factorization, $a \in (p)$ or $b \in (p)$.

Suppose (p) is prime.

Then the factorization of (p) is (p), *i.e.* (p) is irreducible. ◻

Thm 1.2.2. *If R is UFD, then $R[x]$ is UFD.*

Proof. Let F be the field of fraction of R.

For $f \in R[x]$, we can uniquely factorize it into prime elements in $F[x]$.

And since $f \in F[x]$ can be written as $f = ag$ where $g \in R[x]$ is primitive and $a \in R$.

So we can write

$$f = \frac{r}{s} g_1 g_2 \cdots g_n,$$

where $g_i \in R[x]$ is primitive and irreducible in $F[x]$.

Let $f = a\tilde{f}$ where $\tilde{f}$ is primitive and $a \in R$.

Then by Gauss lemma, $r = usa$ for some unit u and so

$$f = uag_1 \cdots g_n.$$

And since R is UFD.
Hence $R[x]$ is UFD. □

Prop 1.2.5. *A principal prime ideal of $k[x_1, \cdots, x_n]$ is of form (f) with f is irreducible polynomial with positive degree.*

Proof. By theorem 1.2.2, $k[x_1, \cdots, x_n]$ is UFD and the proof is complete by proposition 1.2.4. □

Lemma 1.2.3. *Suppose $Y = Y_1 \cup \cdots \cup Y_s$ such that Y_i is closed and irreducible and $Y_i \nsubseteq Y_j$, then $Y_1, \cdots, Y_s$ are all irreducible components of Y.*

Proof. Suppose C is an irreducible component of Y.
Then $C = (C \cap Y_1) \cup \cdots \cup (C \cap Y_s)$.
So there exists i such that $C \subset Y_i, i.e. C = Y_i$.
Suppose Y_i is not irreducible component.
then $\exists$ irreducible component $C \supsetneqq Y_i$.
Therefore $Y_i \subsetneqq Y_j = C$, contradiction! □

Coro 1.2.1. *Let $f \in k[x_1, \cdots, x_n]$ has positive degree, then f is irreducible iff $Z(f)$ irreducible.*
More generally, if $f = f_1 \cdots f_s$ with f_i irreducible, then $Z(f_1), \cdots, Z(f_s)$ are all irreducible components of $Z(f)$, that is

$$Z(f) = \bigcup_{i=1}^{s} Z(f_i).$$

Proof. f is irreducible $\Leftrightarrow$ (f) is prime$\Leftrightarrow$ $Z(f)$ is irreducible subset of $\mathbb{A}^n$.
If $f = f_1 \cdots f_s$, then we have

$$Z(f) = \bigcup_{i=1}^{s} Z(f_i)$$

with each $Z(f_i)$ irreducible.
Assume $(f_1), \cdots, (f_s)$ distinct.
Then for $i \neq j$, we must have $Z(f_i) \nsubseteq Z(f_j)$.
Otherwise, $Z(f_i) \subsetneqq Z(f_j), i.e. f_j | f_i$ but f_i, f_j are irreducible, contradiction!
By lemma 1.2.3, $\{Z(f_i)\}$ is the set of irreducible components of $Z(f)$. □

Lemma 1.2.4. *For a partially ordered set $(A, \leqslant)$, TFAE:*

(1) $(A, \leqslant)$ satisfies ACC(ascending chain condition):

Every ascending chain $a_1 \leqslant a_2 \leqslant \cdots$ becomes stationary, that is, for n sufficiently large, $a_n = a_{n+1} = \cdots$.

(2) Every nonempty subset $B \subset A$ has a maximal element.

Proof. By Zorn's lemma. □

Remark 1.2.2. Similar for DCC(descending chain condition).

Def 1.2.4. We say a ring R is noetherian if its collection of ideals satisfies ACC.
We say a topological space Y is noetherian if its collection of closed subsets satisfies DCC.

Prop 1.2.6. *(1) A subspace of a noetherian set is noetherian.*

(2) A quotient of a noetherian ring is noetherian.

Proof. (1) Let $X \subset Y$ and Y is noetherian.

For any descending closed subset chain $\{U_i\}$ in X, let $U_i = V_i \cap X$ where V_i is closed in Y.

Then there exists i such that $V_i = V_{i+1} = \cdots$.

So $U_i = U_{i+1} = \cdots$, *i.e.* X is noetherian.

(2) Let R is noetherian and I is an ideal of R, $S = R/I$.

For any ascending ideal chain $\{J_i\}$ in S, let $I_i = \pi^{-1}(J_i)$ is an ideal of R, where $\pi : R \to S$ is the canonical homomorphism.

Then there exists i such that $I_i = I_{i+1} = \cdots$.

So $J_i = J_{i+1} = \cdots$, *i.e.* S is noetherian.

□

Thm 1.2.3 (Hilbert's basis)**.** *If R is noetherian, then $R[x]$ is noetherian.*

Coro 1.2.2. *If R is noetherian, so is any finitely generated R-algebra.*

Coro 1.2.3. *Any closed subspace Y of $\mathbb{A}^n$ is notherian.*

We will prove these three proposition in the next section.

Prop 1.2.7. *Let Y be a noetherian space, then its irreducible components are finite in number and their union equals Y.*

Proof. We first show: every closed subset of Y is a finite union of closed irreducible subset.

Let B be the collection of the closed subsets of Y which are not the finite union of closed irreducible subset.

If $B \neq \varnothing$, then there exists a minimal element $Z \in B$.

Let $Z = Z_1 \cup Z_2$ and then $Z_1, Z_2 \notin B$.

So Z_1, Z_2 is a finite union of closed irreducible subset, so is Z, contradiction!

Now $Y = Y_1 \cup \cdots \cup Y_s$ with Y_i is closed and irreducible, $Y_i \nsubseteq Y_j$.

Hence $\{Y_1, \cdots, Y_s\}$ is the set of all irreducible components of Y. □

Coro 1.2.4. *Every subset of $\mathbb{A}^n$ has a finite number of irreducible components.*

Proof. Follows by corollary 1.2.3 and proposition 1.2.7. □

Def 1.2.5. R is a ring, $S \subset R$ is multiplicative and $1 \in S$, the ring $S^{-1}R$ and homomorphism $R \to S^{-1}R$ as follows:

elements in $S^{-1}R$ are equivalence classes of $\frac{r}{s}$ with $r \in R, s \in S$ and $\frac{r}{s} \sim \frac{r'}{s'}$ iff there exists $s'' \in S$ such that $s''(rs' - r's) = 0$

$\phi : R \to S^{-1}R, r \mapsto \left[\frac{r}{1}\right]$ and image of elements of S in $S^{-1}R$ is invertible, *i.e.* $\left[\frac{s}{1}\right] \cdot \left[\frac{1}{s}\right] = 1$.

Exam 1.2.2. *If $0 \in S$, then $S^{-1}R = (0)$.*

If $S = \{s^n | n \in \mathbb{N}\}$ for certain $s \in R$, denote $R\left[\frac{1}{s}\right] = S^{-1}R$.

For $S = S(R) := R - \{zero\ divisors\}$, write $\mathrm{Frac}(R) = S^{-1}R$ called fraction ring.

If R is a domain, $\mathrm{Frac}(R)$ is the fraction field.

If $\mathfrak{p}$ is a prime ideal of R, then $R - \mathfrak{p}$ is multiplicative, denote $R_{\mathfrak{p}} = (R - \mathfrak{p})^{-1}R$.

Lemma 1.2.5. *Let I be an ideal of a ring R, then $\sqrt{I} = \bigcap\limits_{\substack{\mathfrak{p} \supset I \\ \mathfrak{p}\ is\ prime}} \mathfrak{p}$.*

In particular, $\sqrt{(0)} = \bigcap\limits_{\mathfrak{p}\ prime} \mathfrak{p} = \bigcap\limits_{\mathfrak{p}\ is\ minimal} \mathfrak{p}$.

Proof. First we prove $\sqrt{(0)} = \bigcap\limits_{\mathfrak{p} \text{ is prime}} \mathfrak{p}$.

It is easy to see that $\sqrt{(0)}$ is contained in any prime ideal.

Now for a non-nilpotent $a \in R$, consider $R \to R\left[\frac{1}{a}\right]$.

Since $R\left[\frac{1}{a}\right] \neq (0)$.

So there exists a maximal ideal $\mathfrak{m} \subset R\left[\frac{1}{a}\right]$.

Consider $R \to R\left[\frac{1}{a}\right] \to R\left[\frac{1}{a}\right]/\mathfrak{m} =: F$.

Then image of a is nonzero in F,*i.e.* $\ker(R \to F)$ is a prime ideal not containing a.

So $\bigcap\limits_{\mathfrak{p} \text{ is prime}} \mathfrak{p} = \{\text{all nilpotent elements in } R\} = \sqrt{(0)}$.

For any ideal $I \subset R$, consider $\sqrt{(0)}$ in R/I, then $\sqrt{I} = \bigcap\limits_{\substack{\mathfrak{p} \supset I \\ \mathfrak{p} \text{ is prime}}} \mathfrak{p}$ in R. ☐

Prop 1.2.8. *R is a noetherian ring, then for every ideal $I \subset R$, the minimal elements of the collection of prime ideals containing I are finite in number.*

In particular, the minimal prime ideals of R are finite in number with intersection $\sqrt{(0)}$.

Proof. If R is noetherian, then R/I is noetherian.

Let B be the collection of radical ideals that cannot be written as intersection of finitely many prime ideals.

Suppose $B \neq \varnothing$, then $R \notin B$ and prime ideal is not in B.

And since R is noetherian

So B has a maximal element and $I_0 \neq R$ is not prime.

Therefore $\exists a_1, a_2 \in R \backslash I_0$ with $a_1 a_2 \in I_0$.

Consider $J_i = \sqrt{I_0 + Ra_i}$.

Then $J_1, J_2 \supsetneqq I_0$.

So $J_1, J_2 \notin B$, *i.e.*J_i can be written as intersection of finitely many prime ideals.

We claim that $I_0 = J_1 \cap J_2$, then this lead to the contradiction.

If $a \in J_1 \cap J_2$, then $\exists n_1, n_2 \in \mathbb{N}^+$, *s.t.* $a^{n_1} \in I_0 + Ra_1, a^{n_2} \in I_0 + Ra_2$.

So $a^{n_1+n_2} = (I_0 + Ra_1)(I_0 + Ra_2) \subset I_0$, *i.e.*$a \in I_0$.

We conclude $B = \varnothing$,*i.e.* every radical ideal of R is an intersection of finitely many prime ideals.

Now take arbitrary ideal $I \subset R$ and let $\sqrt{I} = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_s$.

WLOG, we assume $\mathfrak{p}_i \not\supseteq \mathfrak{p}_j$ for $i \neq j$.

Suppose $\mathfrak{p}$ is a prime ideal containing I, we show $\mathfrak{p}$ contains certain $\mathfrak{p}_i$.

If not, suppose for any i, $\mathfrak{p} \not\supseteq \mathfrak{p}_i$.

Then we can take $a_i \in \mathfrak{p}_i \backslash \mathfrak{p}$.

So $a_1 \cdots a_s \in \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_s = \sqrt{I} \subset \mathfrak{p}$, contradiction!

Hence a minimal prime ideal containing I must belong to $\{\mathfrak{p}_1, \cdots, \mathfrak{p}_s\}$. ☐

1.3 Finiteness properties and the Hilbert theorems

Def 1.3.1. We say an R-module M is noetherian, if the collection of R-submodules of M satisfies ACC.

Prop 1.3.1. *(1) Every quotient of a noetherian R-module is still noetherian.*

(2) A ring R is noetherian as ring iff R is noetherian as an R-module.

Proof. (1) Let M be noetherian R-module and M' be an submodule of M, $N = M/M'$.

For any ascending module chain $\{N_i\}$ in N, let $M_i = \pi^{-1}(N_i)$ is a submodule of M, where $\pi : M \to N$ is the canonical homomorphism.

Then there exists i such that $M_i = M_{i+1} = \cdots$.

So $N_i = N_{i+1} = \cdots$, *i.e.* N is a noetherian R-module.

(2) R-submodules of R are the ideals of R.

So R is noetherian as an R-module iff R is noetherian.

□

Prop 1.3.2. *An R-module M is noetherian iff every R-submodule of M is finitely generated as R-module.*

Proof. Suppose M is noetherian, take $N \subset M$ is a submodule, let N_0 be a maximal element in the collection of finitely generated R-submodule of N.

Then N_0 is finite generated as R-module.

If $N_0 \subsetneqq N$, take $x \in N \backslash N_0$, then $N_0 + Rx$ is finitely generated, contradiction!

So $N = N_0$.

Suppose every R-submodule of M is finite generated.

Take $N_1 \subset N_2 \subset \cdots$, let $N = \bigcup N_i$ be finite generated by $\{s_1, \cdots, s_k\}$.

Then $\exists j, s.t. \{s_1, \cdots, s_k\} \subset N_j, i.e. N = N_j = N_{j+1} = \cdots$.

Therefore M is noetherian. □

Prop 1.3.3. *Suppose R is noetherian ring, then every finitely generated R-module is noetherian.*

Proof. Let $M = RS$ for finite set $S \subset M$, we induct on $\#S$.

If $\#S = 0$, then it is trivial.

Suppose $\#S \geqslant 1$, take $s \in S$, let $S' := S \backslash \{s\}, M' = RS' \subset M$.

Then M' is noetherian as R-module.

Since $R \to M/M', 1 \mapsto [s], r \mapsto [rs]$ is epimorphism of R-module.

So M/M' is noetherian as R-module.

Now take $N_1 \subset N_2 \subset \cdots$ in M.

Then $N_1 \cap M' \subset N_2 \cap M' \subset \cdots$ in M' is stabilizes.

Therefore there exists $j_1 \in \mathbb{Z}^+$, such that $N_k \cap M' = N_{j_1} \cap M'$ for $k \geqslant j_1$.

For $k \geqslant j_1$, $N_k/(N_{j_1} \cap M) = N_k/(N_k \cap M') \cong (N_k + M')/M' \subset M/M'$.

When k is large, $(N_k + M')/M'$ is stabilizes, *i.e.* N_k stabilizes. □

Thm 1.3.1 (Hilbert basis)**.** *R is noetherian$\Rightarrow$ $R[x]$ is noetherian.*

Proof. $R[x]$ is noetherian ring$\Leftrightarrow$ $R[x]$ is noetherian as $R[x]$-module$\Leftrightarrow$ every ideal I of $R[x]$ is finitely generated as $R[x]$-module.

For polynomial $f \in R[x]$, denote $\operatorname{in}(f)$ is the initial coefficient of f,*i.e.* the highest degree coefficient.

And let $\operatorname{in}(I) := \{\operatorname{in}(f) | f \in I\}, \operatorname{in}(0) = 0$.

Then $\operatorname{in}(I)$ is an ideal of R.

So $\operatorname{in}(I)$ is finitely generated as R-module.

Therefore there exist $f_1, \cdots, f_k \in I \backslash \{0\}$ such that $\operatorname{in}(I) = R\{\operatorname{in}(f_1), \cdots, \operatorname{in}(f_k)\}$.

Let $d_0 = \max\{\deg f_1, \cdots, \deg f_k\}$.

We claim that $I = R[x]f_1 + \cdots + R[x]f_k + (I \cap R[x]_{<d_0})$.

Actually any polynomial in I with $\deg \geqslant d_0$ can be reduced to a polynomial in I with lower degree by modulo $R[x]f_1 + \cdots + R[x]f_k$ by induction.

So $I \cap R[x]_{<d_0}$ is finite generated as R-module, take generators set as $f_{k+1}, \cdots, f_{k+l}$.

Hence $I = R[x]\{f_1, \cdots, f_{k+l}\}$ is finitely generated. □

Thm 1.3.2 (Artin-Tate)**.** *R is noetherian ring, B is an R-algebra, $A \subset B$ is R-subalgebra.*

Assume B is finite generated as A-module, then A is finite as R-algebra iff B is so.

Proof. Suppose $b_1, \cdots, b_m \in B, s.t. B = Ab_1 + \cdots + Ab_m$.

Now assume B is finitely generated as R-algebra by $b_1, \cdots, b_m$, WLOG.

Then $b_i b_j \in B$, let

$$b_i b_j = \sum_{k=1}^{m} a_{ij}^k b_k$$

for $a_{ij}^k \in A$.

Let $A_0 \subset A$ be a R-subalgebra of A generated by a_{ij}^k.

By Hilbert basis theorem, A_0 is a noetherian ring.

Since $b_i b_j \in A_0 b_1 + \cdots A_0 b_m$ for any i, j.

So B is finitely generated A_0-module, *i.e.* B is noetherian as A_0-module.

And since $A \subset B$ as A_0-submodule, *i.e.* A is finitely generated as A_0-module.

Hence A is finitely generated as R-module. $\square$

Lemma 1.3.1 (Zariski)**.** *Field extension L/K is finite iff L is finite generated as a K-algebra.*

Proof. $\Rightarrow$ is obvious, now assume L is finitely generated as K-algebra.

Take $b_1, \cdots, b_m \in L$ generates L as K-algebra.

We need to show $b_1, \cdots, b_m$ are algebraic over K, so that $L = K[b_1, \cdots, b_m] = K(b_1, \cdots, b_m)$ is finite over K.

If not, WLOG, assume $b_1, \cdots, b_r$ are algebraic independent over K and $b_{r+1}, \cdots, b_m$ are algebraic over $K(b_1, \cdots, b_r)$.

Then $L/K(b_1, \cdots, b_r)$ is finite.

By Artin-Tate theorem, $K(b_1, \cdots, b_r)$ is finitely generated as K-algebra.

Let S generates $k(b_1, \cdots, b_r)$ and $g \in K[b_1, \cdots, b_r]$ be a common denominator of S.

Then $K(b_1, \cdots, b_r) = K[S] = K[b_1, \cdots, b_r]\left[\frac{1}{g}\right]$.

Consider $\frac{1}{1-g} \in K(b_1, \cdots, b_r)$.

So $\frac{1}{1-g} = \frac{f}{g^N}$ for certain $f \in K[b_1, \cdots, b_r], N \in \mathbb{N}$.

Therefore $f = g^N + fg$ But $g \nmid f$, contradiction! $\square$

Coro 1.3.1. *A is a finitely generated k-algebra, then for every maximal ideal $\mathfrak{m} \subset A$, the map $k \hookrightarrow A \to A/\mathfrak{m}$ is an isomorphism of fields.*

Proof. $A/\mathfrak{m}$ is a field and a finitely generated as k-algebra.

By Zariski lemma, $A/\mathfrak{m} \supset k$ is finite.

So $A/\mathfrak{m} = k$ since k is algebraic closed. $\square$

Coro 1.3.2. *A is finitely generated k-algebra, then there is bijection:*

$$\{m | m \text{ is maximal ideal of } A\} \leftrightarrow \{\text{surjective morphism } A \to k \text{ as } k\text{-algebra}\}$$
$$m \mapsto (A \twoheadrightarrow A/\mathfrak{m} \cong k)$$

Thm 1.3.3 (Hilbert Nullstellensatz)**.** *$I(Z(J)) = \sqrt{J}$.*

Proof. $I(Z(J)) \supset \sqrt{J}$ is clear.

Suppose $I(Z(J)) \supsetneq \sqrt{J}$, let $f \in I(Z(J)) \backslash \sqrt{J}$.

Then the image $\bar{f}$ of f in $k[x_1, \cdots, x_n]/J$ is not nilpotent.

Let $A = (k[x_1, \cdots, x_n]/J)\left[\frac{1}{\bar{f}}\right]$, which is not (0) and finitely generated as k-algebra.

Take $\mathfrak{m} \subset A$ be a maximal ideal, then we have $A \to A/\mathfrak{m} \cong k$.

Consider $\phi : k[x_1, \cdots, x_n] \to A \to A/\mathfrak{m} \cong k$.

Let $p_i = \phi(x_i) \in k, p = (p_1, \cdots, p_n) \in \mathbb{A}^n$.

For any polynomial $g \in k[x_1, \cdots, x_n]$, the image $\phi(g) \in k$ equals to $g(p)$.

If $g \in J \subset k[x_1, \cdots, x_n]$, then $\phi(g) = 0, i.e. g(p) = 0$.

So $p \in Z(J)$.
And since $\bar{f}$ invertible in A.
Therefore $\phi(f) \neq 0, i.e. f(p) \neq 0$.
But $f \in I(Z(J))$, contradiction! □

1.4 The affine category

Def 1.4.1. $X \subset \mathbb{A}^m, Y \subset \mathbb{A}^n$ are closed, a map $f : X \to Y$ is called regular if the components $f_1, \cdots, f_n$ of f are regular functions on X.

Lemma 1.4.1. *For $X \xrightarrow{f} Y \xrightarrow{g} Z$, if f, g is regular, then $g \circ f : X \to Z$ is regular.*

Proof. It suffices to show each components of $g \circ f$ is regular function.
Only need to consider case $Z = \mathbb{A}^1$.
Then g is the restriction of a polynomial function on $\mathbb{A}^n$ to Y.
Let $f = (f_1, \cdots, f_n)$ where f_i is the restriction of the polynomial function $F_i(x_1, \cdots, x_n)$ defined on $\mathbb{A}^m$ to X.
So $g \circ f : X \to k$ is the restriction of the polynomial $G(F_1(x_1, \cdots, x_m), \cdots, F_n(x_1, \cdots, x_m))$ to X. □

Def 1.4.2. A affine category is consist of

(1) objects: closed subsets of affine spaces

(2) morphism: regular maps $X \to Y$.

Remark 1.4.1. For any $X \xrightarrow{f} Y$ and regular function $Y \to k$, we have a regular function $X \xlongequal{f} Y \to k$, that is, f induces a k-algebra morphism $f^* : k[Y] \to k[X]$.
So we have the contravariant functor $Y \mapsto k[Y], f \mapsto f^*$.

Def 1.4.3. A regular map $f : X \to Y$ is called an isomorphism if f is bijective and $f^{-1} : Y \to X$ is regular.

Prop 1.4.1. *Isomorphism $f : X \to Y$ induce isomorphism $f^* : k[Y] \to k[X]$.*

Proof. $(f^{-1})^*(f^*(p)) = f^*(p) \circ f^{-1} = p \circ f \circ f^{-1} = p$.
And $f^*((f^{-1})^*(p)) = (f^{-1})^*(p) \circ f = p \circ f^{-1} \circ f = p$.
So $(f^{-1})^*$ and f^* are isomorphism. □

Prop 1.4.2. *$f : X \to Y$ is any map, if for any regular function $g : Y \to k$, the composition $g \circ f : X \to k$ is regular, then f is a regular map.*

Proof. Take $g = y_i$, then $g \circ f = f_i$ is the i-th component of f. □

Prop 1.4.3. *Given $X \subset \mathbb{A}^m, Y \subset \mathbb{A}^n$ and k-algebra homomorphism $\phi : k[Y] \to k[X]$.*
Then there is a unique regular map $f : X \to Y$ with $\phi = f^*$.
That is, $\mathrm{Hom}_{reg}(X, Y) \xrightarrow{\cong} \mathrm{Hom}_{k\text{-}alg}(k[Y], k[X])$.

Proof. The inclusion $j : Y \subset \mathbb{A}^n$ defines $j^* : k[y_1, \cdots, y_n] \to k[Y] = k[y_1, \cdots, y_n]/I(Y)$.
Then $\ker(j^*) = I(Y)$.
Consider $k[X] \xleftarrow{\phi} k[Y] \xleftarrow{j^*} k[y_1, \cdots, y_n], f_i \leftarrow\!\shortmid y_i$.
Let $f = (f_1, \cdots, f_n) : X \to \mathbb{A}^n$ is a regular map.
Then $k[y_1, \cdots, y_n] \to k[X], y_i \mapsto f^*(y_i) = y_i \circ f = f_i = (\phi j^*)(y_u)$.
So $f^* = \phi j^*$,*i.e.* $f^*(I(Y)) = (0)$.

Therefore $\forall g \in I(Y), g \circ f \equiv 0, i.e. f(X) \subset Y = Z(I(Y))$ and $f^* = \phi$.
Suppose $f, f' : X \to Y$ are different regular map.
Then there exists i such that $f_i \neq f_i'$.
So $f^*([y_i]) \neq (f')^*([y_i]), i.e. f^* \neq (f')^*$.
Hence f is unique. □

Coro 1.4.1. *(1) isomorphism $k[Y] \xrightarrow{\cong} k[X]$ comes from a unique isomorphism $X \xrightarrow{\cong} Y$.*

(2) For $Z \subset Y \subset \mathbb{A}^n$, the induced surjective map $k[Y] \to k[Z]$ has kernel $I_Y(Z) = I(Z)/I(Y)$.

Proof. (1) Let $\phi : k[Y] \xrightarrow{\cong} k[X]$ and $f^* = \phi, g^* = \phi^{-1}$.
So $(g \circ f)^* = f^* \circ g^* = \mathrm{Id}_{k[X]}, (f \circ g)^* = g^* \circ f^* = \mathrm{Id}_{k[Y]}$.
And since $f \circ g, g \circ f$ are the unique regular map such that $(g \circ f)^* = \mathrm{Id}_X^*, (f \circ g)^* = \mathrm{Id}_Y^*$.
Hence f is the unique isomorphism with $f^{-1} = g$.

(2) Let $\phi : k[Y] \to k[Z]$ such that $\phi = i^*$.
Then $\phi(p) = p \circ i = p\big|_Z$.
So $\ker \phi = \big\{p \in k[Y] \big| p\big|_Z \equiv 0\big\} = I_Y(Z)$.

□

Def 1.4.4. A regular map $f : X \to Y$ is called a closed immersion if $f(X) \subset Y$ is closed and $f : X \to f(X)$ is an isomorphism.

Prop 1.4.4. *$f : X \to Y$ is a closed immersion iff $f^* : k[Y] \to k[X]$ is surjective.*

Proof. If f is closed immersion, then $f^* : k[X] \xleftarrow{\cong} k[f(X)] \twoheadleftarrow k[Y]$ with $\ker = I_Y(f(X))$.
So $k[Y] \to k[X]$ is surjective.
Conversely, if f^* is surjective, then $\ker(f^*)$ is a radical ideal of $k[Y]$, let it corresponds to a closed subset $Z \subset Y$.
By definition of f^*, every element in $\ker(f^*)$ vanishes on $f(X)$.
So $f(X) \subset Z$.
And since morphism $k[Y] \twoheadrightarrow k[Z]$ also has kernel $I_Y(Z) = \ker(f^*)$.
Hence $k[Z] \to k[X]$ is isomorphism, *i.e.* $f : X \xrightarrow{\cong} Z \to Y$ is a closed immersion. □

Exam 1.4.1. *Consider the map$f : \mathbb{A}^1 \to \mathbb{A}^2, t \mapsto (t^2, t^3)$.*
The image is an irreducible curve C defined by $x^3 - y^2 = 0$ and the inverse map $C \to \mathbb{A}^1$ is given by $(0,0) \mapsto 0, (x, y) \mapsto \frac{y}{x}$ if $x \neq 0$.
The Zariski topology on both C and $\mathbb{A}^1$ are the cofinite topology.
So $f : \mathbb{A}^1 \to C$ is a homeomorphism, but not an isomorphism:
Since $k[C] = k[x, y]/(x^3 - y^2), k[\mathbb{A}^1] = k[t]$.
And $f^* : k[C] \to k[\mathbb{A}^1]$ is given by $[x] \mapsto t^2, [y] \mapsto t^3$.
Therefore image of f^* does not contain t, i.e. *f^* is not surjective.*

Prop 1.4.5. *For regular map $f : X \to Y$ with $f^* : k[Y] \to k[X]$, for any point $x \in X$, we have $\mathfrak{m}_{f(x)} = (f^*)^{-1}(\mathfrak{m}_x)$.*

Proof. First $k[Y] \xrightarrow{f^*} k[X] \xrightarrow{\rho_x} k[X]/\mathfrak{m}_x \cong k$
So $\ker(\rho_x \circ f^*) = (f^*)^{-1}(\mathfrak{m}_x)$ is a maximal ideal.
It suffices to check $f^*(\mathfrak{m}_{f(x)}) \subset \mathfrak{m}_x$.
Actually, for any $g \in \mathfrak{m}_{f(x)}$, $g(f(x)) = 0$.
So $f^*(g)$ vanishes at x, *i.e.* $f^*(g) \in \mathfrak{m}_x$. □

Def 1.4.5. For any ring R, let $\mathrm{Spm}(R)$ be the set of maximal ideals of R.
For $x \in \mathrm{Spm}(R)$, we also denote $\mathfrak{m}_x$ the corresponding maximal ideal .
For any ideal $I \subset R$, let $Z(I)$ be the set of $x \in \mathrm{Spm}(R)$ with $\mathfrak{m}_x \supset I$.
For $s \in R$, write $Z(s) = Z(Rs) = \{x | s \in \mathfrak{m}_x\}$, apparently: $Z(0) = \mathrm{Spm}(R), Z(R) = \varnothing$.

Prop 1.4.6. *For arbitrary ideals $I, J, \{I_\alpha\}_{\alpha\in A}$ of R, we have*

$$Z(I) \cup Z(J) = Z(I \cap J), \bigcap_{\alpha\in A} Z(I_\alpha) = Z\left(\sum_{\alpha\in A} I_\alpha\right).$$

So $\{Z(I)\}$ forms all closed subsets for a topology: Zariski topology on $\mathrm{Spm}(R)$.

Proof. If $I \cap J \subset \mathfrak{m}_x$, then $IJ \subset \mathfrak{m}_x$.
So $I \subset \mathfrak{m}_x$ or $J \subset \mathfrak{m}_x$.
Therefore $Z(I \cap J) = Z(I) \cup Z(J)$.
Moreover, $I_\alpha \subset \mathfrak{m}_x$ for every $\alpha \in A$ $\Leftrightarrow$the ideal generates by $\{I_\alpha\}_{\alpha\in A}$ contains in $\mathfrak{m}_x$.
Hence $\bigcap\limits_{\alpha\in A} Z(I_\alpha) = Z\left(\sum\limits_{\alpha\in A} I_\alpha\right)$. ☐

Def 1.4.6. Denote $\mathrm{Spm}(R)_s := \mathrm{Spm}(R)\backslash Z(s)$ are the principal open subsets.

Remark 1.4.2. Principal open subsets form a basis of Zariski topology on $\mathrm{Spm}(R)$.

Lemma 1.4.2. $\mathrm{Spm}(R)$ *is quasi-compact: every open covering admits a finite subcovering.*

Proof. It suffices to show an open covering by principal open subsets admits a finite subcovering.
Suppose $\mathrm{Spm}(R) = \bigcup\limits_{s\in S} \mathrm{Spm}(R)_s$, then

$$\mathrm{Spm}(R) = \bigcup_{s\in S} \mathrm{Spm}(R)_s = \mathrm{Spm}(R)\backslash\left(\bigcap_{s\in S} Z(s)\right) = \mathrm{Spm}(R)\backslash Z\left(\sum_{s\in S} sR\right).$$

So $\sum\limits_{s\in S} sR = R$.
Let $1 = \sum\limits_{i=1}^{n} r_i s_i$ for $r_i \in R, s_i \in S$.
Hence $\sum\limits_{i=1}^{n} s_i R = R$, *i.e.* $\mathrm{Spm}(R) = \bigcup\limits_{i=1}^{n} \mathrm{Spm}(R)_{s_i}$. ☐

Remark 1.4.3. Bourbaki use this notion "quasi-compact" for non-Hausdorff space. One reason of doing this is that when we consider the complex varieties, they also have a topology induced by the euclidean topology of $\mathbb{C}^n$. So we use "quasi-compact" to distinguish the compactness of these two topology structures.

Now consider a finitely generated k-algebra A(may be not reduced), a choice of generators gives $A \cong k[x_1, \cdots, x_n]/I$.

For any $x \in \mathrm{Spm}(A)$, we have a unique isomorphism $A/\mathfrak{m}_x \cong k$ as k-algebra by Artin-Tate theorem. So we have the correspondence $x \leftrightarrow \mathfrak{m}_x \leftrightarrow \left(A \xrightarrow{\rho_x} k\right)$.

Any $f \in A$ defines a "regular function" $\bar{f} : \mathrm{Spm}(A) \to k$ which takes $x \in \mathrm{Spm}(A)$ to $\rho_x(f) \in k$. The zero set of $\bar{f} : \mathrm{Spm}(A) \to k$ is $Z(f)$ and $f \mapsto \bar{f}$ is a k-algebraic homomorphism from A to the algebraic of k-valued functions on $\mathrm{Spm}(A)$. The kernel of this homomorphism is exactly $\sqrt{(0)} \subset A$ since we have the proposition:

Prop 1.4.7.

$$\sqrt{(0)} = \bigcap_{x\in\mathrm{Spm}(A)} \mathfrak{m}_x.$$

Proof. If $f \notin \sqrt{(0)}$, then consider the map $\varphi : A \to A\left[\frac{1}{f}\right] \to A\left[\frac{1}{f}\right]/\mathfrak{m} \cong \mathfrak{m}$ where $\mathfrak{m}$ is a maximal ideal of $A\left[\frac{1}{f}\right]$.

So $f \notin \ker\varphi$ since $\varphi(f)$ is invertible.

Therefore $f \notin \mathfrak{m}_x$ for x such that $\rho_x = \varphi$.

And since $\sqrt{(0)} = \bigcap_{\mathfrak{p}\text{ prime}} \mathfrak{p} \subset \bigcap_{x\in\mathrm{Spm}(A)} \mathfrak{m}_x$.

Hence $\sqrt{(0)} = \bigcap_{x\in\mathrm{Spm}(A)} \mathfrak{m}_x$. ∎

Remark 1.4.4. We have used this trick while proving the Hilbert nullstellensatz.

Let $\bar{A} = A/\sqrt{(0)}$ reduced, then $\bar{A}$ is the set of regular functions on $\mathrm{Spm}(A)$, also denote $\bar{A} = k[\mathrm{Spm}(A)]$. So $\bar{A} \cong k[x_1, \cdots, x_n]/\sqrt{I} = k[Z]$, *i.e.* $\mathrm{Spm}(A) \cong \mathrm{Spm}(\bar{A}) \cong Z(I) \cong Z(\sqrt{I}) \subset \mathbb{A}^n$ as set. This gives $(X, k[X])$ in an intrinsic way: $(\mathrm{Spm}(A), \bar{A})$.

Now consider a morphism $\phi : A \to B$ of finitely generated k-algebra, we have $\mathrm{Spm}(\phi) : \mathrm{Spm}(B) \to \mathrm{Spm}(A), \mathfrak{m}_y \mapsto \phi^{-1}(\mathfrak{m}_y)$. So for regular function $f \in A$ and its induced map $\bar{f} \in \bar{A}$, the composite of $\mathrm{Spm}(B) \xrightarrow{\mathrm{Spm}(\phi)} \mathrm{Spm}(A) \xrightarrow{\bar{f}} k$ is $\overline{\phi(f)}$ and so it is regular.

In particular, the preimage of $Z(f)$ in $\mathrm{Spm}(B)$ under $\mathrm{Spm}(\phi)$ is $Z(\phi(f))$. So the preimage of $\mathrm{Spm}(A)_f$ is $\mathrm{Spm}(B)_{\phi(f)}$ and preimage of $Z(I)$ is $Z(\phi(I))$. Thus $\mathrm{Spm}(\phi)$ is continuous.

We refer to the pair $(\mathrm{Spm}(\phi), \phi)$ as a morphism from $(\mathrm{Spm}(B), B)$ to $(\mathrm{Spm}(A), A)$. In particular, $\mathrm{Spm}(\phi)$ is a geometric map and ϕ is an algebraic morphism.

Prop 1.4.8. *Let A be a finitely generated k-algebra, then for any $g \in A$, $A\left[\frac{1}{g}\right]$ is a finitely generated k-algebra.*

If A reduced, then $A\left[\frac{1}{g}\right]$ is also reduced, then natural k-algebra homomorphism $A \to A\left[\frac{1}{g}\right]$ induces a morphism $\mathrm{Spm}\left(A\left[\frac{1}{g}\right]\right) \to \mathrm{Spm}(A)$, which is a homeomorphism onto $\mathrm{Spm}(A)_g$.

Moreover, for $g, g' \in A$, TFAE:

(1) $\mathrm{Spm}(A)_g \subset \mathrm{Spm}(A)_{g'}$.

(2) g' divides some positive power of g, i.e. $g \in \sqrt{(g')}$.

(3) $\exists$an A-homomorphism $A\left[\frac{1}{g'}\right] \to A\left[\frac{1}{g}\right]$. (which must then be unique)

Proof. If g nilpotent, then $A\left[\frac{1}{g}\right] = (0), \mathrm{Spm}\left(A\left[\frac{1}{g}\right]\right) = \varnothing, \mathrm{Spm}(A)_g = \varnothing$.

So $A\left[\frac{1}{g}\right]$ is clearly finitely generated over k.

If A reduced, take $\frac{f}{g^r} \in A\left[\frac{1}{g}\right]$, suppose $\left(\frac{f}{g^r}\right)^m = 0$ in $A\left[\frac{1}{g}\right]$.

Then f^m is annihilated by a power of g in A.

We assume $f^m g^n = 0$.

Then $(fg^n)^m = 0$ in A, *i.e.* $fg^n = 0$.

Hence $\frac{f}{g^r} = 0$ in $A\left[\frac{1}{g}\right]$,*i.e.* $A\left[\frac{1}{g}\right]$ is reduced.

Since an element of $\mathrm{Spm}\left(A\left[\frac{1}{g}\right]\right)$ can maps to a map $A \to A\left[\frac{1}{g}\right] \to k$.

And it corresponds to the kernel of this map, which is an element in $n\mathrm{Spm}(A)_g$.

So we have $\mathrm{Spm}\left(A\left[\frac{1}{g}\right]\right) \to \mathrm{Spm}(A)_g \subset \mathrm{Spm}(A)$, which is clearly continuous.

A principal subset of $\mathrm{Spm}\left(A\left[\frac{1}{g}\right]\right)$ is of form $\mathrm{Spm}\left(A\left[\frac{1}{g}\right]\right)_\phi$ with $\phi = \frac{f}{g^n}$ in $A\left[\frac{1}{g}\right]$.

Suppose ϕ is not nilpotent in $A\left[\frac{1}{g}\right]$, *i.e.* f is not nilpotent in A.

Let $A\left[\frac{1}{g}\right]\left[\frac{1}{\phi}\right] \cong A\left[\frac{1}{fg}\right]$.

Then $\mathrm{Spm}\left(A\left[\frac{1}{g}\right]\right)_\phi$ is naturally identified with $\mathrm{Spm}(A)_{fg}$.
Hence the morphism $\mathrm{Spm}\left(A\left[\frac{1}{g}\right]\right) \to \mathrm{Spm}(A)_g$ is open, *i.e.* homeomorphism.
Next we check (1) $\Rightarrow$ (2) $\Rightarrow$ (3) $\Rightarrow$ (1).
(1) $\Rightarrow$ (2): Since $\mathrm{Spm}(A)_g \subset \mathrm{Spm}(A)_{g'}$.
So $Z(g) \supset Z(g')$, *i.e.* $g \in I(Z(g')) = \sqrt{(g')}$.
(2) $\Rightarrow$ (3): Suppose $g^n = fg', f \in A$.
Then there exists an A-homomorphism $A\left[\frac{1}{g'}\right] \to A\left[\frac{1}{fg'}\right] = A\left[\frac{1}{g^n}\right] = A\left[\frac{1}{g}\right]$ which is independent of choices of n and f.
(3) $\Rightarrow$ (1): Since we have $A \to A\left[\frac{1}{g'}\right] \to A\left[\frac{1}{g}\right]$ and $A \to A\left[\frac{1}{g}\right]$.
They induce $\mathrm{Spm}\left(A\left[\frac{1}{g}\right]\right) \to \mathrm{Spm}\left(A\left[\frac{1}{g'}\right]\right) \xrightarrow{1:1} \mathrm{Spm}(A)_{g'}$ and $\mathrm{Spm}\left(A\left[\frac{1}{g}\right]\right) \xrightarrow{1:1} \mathrm{Spm}(A)_g$.
So $\mathrm{Spm}(A)_g \subset \mathrm{Spm}(A)_{g'}$.
Lastly, the image of $\frac{1}{g'}$ in $A\left[\frac{1}{g}\right]$ is the inverse of $\frac{g'}{1} \in A\left[\frac{1}{g}\right]$. □

Now we consider the non-reduced cases: let $X = \mathrm{Spm}(A), Y = \mathrm{Spm}(B)$ and $f : X \to Y$ be regular. Then a fiber $f^{-1}(\{y\})$ or the preimage $f^{-1}(Z)$ of closed subset $Z \subset Y$ is closed and $I_Y(Z) \subset k[Y] \cong \bar{B}$. We claim that $f^{-1}(Z)$ is actually the zero locus of $f^*I_Y(Z) \subset I_X(f^{-1}(Z))$, which may be not radical. So we should think of $f^{-1}(Z)$ as $\mathrm{Spm}(k[X]/f^*I_Y(Z))$, which has a bijection to $\mathrm{Spm}\left(k[X]/\sqrt{f^*I_Y(Z)}\right)$.

Exam 1.4.2. *Consider $f : \mathbb{A}^1 \to \mathbb{A}^1, a \mapsto a^2$ with $\mathrm{char}(k) \neq 2$.*
Then $f^* : k[y] \to k[x], y \mapsto x^2$ and for $a \in Y$, the fiber is

$$f^{-1}(a) = \begin{cases} 2 \text{ different points} & a \neq 0 \\ 0 & a = 0 \end{cases}$$

So $f^{-1}(a)$ should be thought as zero locus defined by $f^*\langle y - a\rangle = \langle x^2 - a\rangle$.
For $a \neq 0$, $\langle x^2 - a\rangle$ is radical ideal.
And for $a \neq 0$, $f^{-1}(a)$ should be thought as a point $0 \in X = \mathbb{A}^1$ with multiplicity 2.

Exam 1.4.3 (Frobenius morphism)**.** *Assume $\mathrm{char}(k) = p$, consider $\Phi_p : \mathbb{A}^1_k \to \mathbb{A}^1_k, a \mapsto a^p$.*
Then $\Phi_p(a - b) = (a - b)^p = a^p + (-b)^p = a^p - b^p = \Phi_a(a) - \Phi_b(b), \Phi_p(ab) = \Phi_p(a)\Phi_p(b)$
So Φ_p is injective, and Φ_p is also surjective since k is algebraic closed.
And since $\Phi_p^* : k[x] \to k[x], x \mapsto x^p$ with image $k[x^p]$.
Therefore Φ_p^* is not surjective, i.e. *Φ_p is homeomorphism but not isomorphism.*
Consider $\Phi_p \curvearrowright \mathbb{A}^1$, $\mathrm{Fix}(\Phi_p) = \{a \in \mathbb{A}^1 | a^p = a\} \xrightarrow{1:1} \mathbb{F}_p \subset k$.
Denote $\mathrm{Fix}(\Phi_p) = \mathbb{A}^1(\mathbb{F}_p)$ and $\mathbb{A}^1(\mathbb{F}_{p^r}) := \mathrm{Fix}\left(\Phi_p^r\right) = \left\{a \in \mathbb{A}^1 \middle| a^{p^r} = a\right\}$.
If $k = \bar{\mathbb{F}}_p$, then $k = \bigcup_{r=1}^{\infty} \mathbb{F}_{p^r}$ and $\mathbb{A}'_k = \bigcup_{r=1}^{\infty} \mathbb{A}^1(\mathbb{F}_{p^r})$.
Every Φ_p-orbit in $\mathbb{A}'_k$ is finite.
For higher dimension, $\Phi_p : \mathbb{A}^n_k \to \mathbb{A}^n_k, \mathbb{A}^n(\mathbb{F}_{p^r}) = \mathrm{Fix}(\Phi_p^r)$.
If $k = \bar{\mathbb{F}}_p$, then $\mathbb{A}^n_k = \bigcup_{r=1}^{\infty} \mathbb{A}^n(\mathbb{F}_{p^r})$ and every Φ_p-orbit in $\mathbb{A}^n_k$ is finite.

Prop 1.4.9. *For $\mathrm{char}(k) = p$ and $q = p^r$, we write Φ_q for Φ_p^r, prove that:*

(a) $f \in k[x_1, \cdots, x_n]$ is in $\mathbb{F}_q[x_1, \cdots, x_n]$ iff $\Phi_q f = f^q$.

(b) an affine-linear transformation of $\mathbb{A}^n$ with coefficients in $\mathbb{F}_q$ commutes with Φ_q.

(c) *let* $Y \subset \mathbb{A}^n_k$ *be common zero locus of a subset of* $\mathbb{F}_q[x_1, \cdots, x_n] \subset k[x_1, \cdots, x_n]$*, then* $\Phi_q = \Phi_p^r : \mathbb{A}^n \to \mathbb{A}^n$ *restricts to a bijection* $\Phi_{Y,q} : Y \to Y$ *and the set of* $\mathbb{F}_q$*-points of* Y *is* $Y(\mathbb{F}_q) := \mathrm{Fix}(\Phi_{Y,q}) = Y \cap \mathrm{Fix}(\Phi_q) = Y \cap \mathbb{A}^n(\mathbb{F}_q)$.

(d) *If* $k = \bar{\mathbb{F}}_p$*, then any closed subset* $Y \subset \mathbb{A}^n$ *is defined over certain* $\mathbb{F}_q$ *and so* Y *is invariant under* Φ_q.

Proof. (a) Let $f = \sum\limits_{i_1, \cdots, i_n} c_{i_1 \cdots i_n} x_1^{i_1} \cdots x_n^{i_n}$, then

$$\Phi_q f = \sum_{i_1, \cdots, i_n} c_{i_1 \cdots i_n} x_1^{qi_1} \cdots x_n^{qi_n}, f^q = \sum_{i_1, \cdots, i_n} c^q_{i_1 \cdots i_n} x_1^{qi_1} \cdots x_n^{qi_n}.$$

So $\Phi_q f = f \Leftrightarrow c^q_{i_1 \cdots i_n} = c_{i_1 \cdots, i_n} \Leftrightarrow c_{i_1 \cdots i_n} \in \mathbb{F}^q$, *i.e.* $f \in \mathbb{F}_q[x_1, \cdots, x_n]$.

(b) Let $f = (f_1, \cdots, f_n), f \in \mathbb{F}_q[x_1, \cdots, x_n]$.

Then $\Phi_q f = (\Phi_q f_1, \cdots, \Phi_q f_n) = (f_1^q, \cdots, f_n^q) = (f_1, \cdots, f_n)\Phi_q = f\Phi_q$.

(c) Let $Y = Z(X)$ with $x \in \mathbb{F}_q[x_1, \cdots, x_n]$.

For any $f \in X, y \in Y$, $f(\Phi_q(y)) = (\Phi_q f)(y) = f^q(y) = 0$.

So $\Phi_q(y) \in Y$.

And $f^q(\Phi_q^{-1}(y)) = (\Phi_q f)(\Phi_q^{-1}(y)) = f(y) = 0$.

Therefore $f(\Phi_q^{-1}(y)) = 0, i.e. \Phi_p^{-1}(y) \in Y$.

Hence $\Phi_{Y,q} : Y \to Y$ is bijective and fixed point set is the intersection of Y and fixed point set of Φ_q, *i.e.* $Y \cap \mathbb{A}^n(\mathbb{F}_{q^m})$.

(d) By Hilbert theorem, $I(Y)$ is finite generated by certain $\{f_1, \cdots, f_n\}$.

So there are only finitely many coefficients.

Let $q = p^r$ such that all coefficients of $f_1, \cdots, f_n$ are contain in $\mathbb{F}^q$.

Then Y is the common zero set of $I(Y) \subset \mathbb{F}_q[x_1, \cdots, x_n]$.

Hence by (c), Y is invariant under some positive power of Φ_p.

□

Def 1.4.7 (Weil Zeta function)**.**

$$Z_Y(t) := \exp\left(\sum_{m=1}^{\infty} |Y(\mathbb{F}_{q^m})| \frac{t^m}{m}\right).$$

In particular,

$$\zeta(Y, s) := Z_Y(q^{-s}) = \exp\left(\sum_{m=1}^{\infty} |Y(\mathbb{F}_{q^m})| \frac{1}{m} q^{-ms}\right).$$

Thm 1.4.1 (Weil conjecture)**.** *Y is smooth, then*

(1) *$Z_Y(t)$ is rational function(Dwork 1960)*

(2) *functional equation(Grothendieck 1965)*

(3) *"Riemann hypothesis": roots of numberator and denominator of $Z_Y(t)$ has absolute value $q^{-\frac{k}{2}}$ with $k \in \mathbb{Z}^{\leqslant 0}$. (proved by Deligne 1974)*