Lecture 1

Runi Malladi

April 16, 2023

1 Galois connections

Definition 1.1. Let X, Y be partially-ordered sets, and suppose we have maps

$$X \underset{g}{\overset{f}{\rightleftarrows}} Y$$

such that

- (order reversing)

$$\begin{aligned} x_1 \leq x_2 \quad &\Rightarrow \quad f(x_1) \geq f(x_2) \\ y_1 \leq y_2 \quad &\Rightarrow \quad g(y_1) \geq g(y_2) \end{aligned}$$

- (inflationary)

$$\begin{aligned} g(f(x)) \geq x \quad &\forall x \in X \\ f(g(y)) \geq y \quad &\forall y \in Y \end{aligned}$$

In this case, we say that f and g form an *antitone Galois connection.*

Proposition 1.2. Let f, g be an antitone Galois connection. Then they restrict to bijections on their images:

$$\mathrm{im}(g) \underset{\tilde{g}}{\overset{\tilde{f}}{\rightleftarrows}} \mathrm{im}(f).$$

Proof. We show that f restricts to a bijection, and the case for g is analagous. By the inflationary property, $x \leq g(f(x))$ for any $x \in X$. Then by the order reversing property, $f(x) \geq f(g(f(x)))$. But applying the inflationary property to $y = f(x)$ yields $f(x) \leq f(g(f(x)))$, and so $f(x) = f(g(f(x)))$. □

Remark 1.3. Since $g \circ f$ is the identity on $\mathrm{im}(g)$, we have $g \circ f \circ g = g$ on all of Y. Then $g \circ f) \circ (g \circ f) = g \circ f$, so $g \circ f$ is idempotent on all of X. We often associate idempotent operators with closure-like qualities. So we may think about

$$g(f(X)) \subset X$$

as a sort of "closed object" in X.

Example 1.4 (classical Galois theory)**.** Let K/k be a finite Galois extension with Galois group $\mathrm{Gal}(K/k)$. Then there is an antitone Galois connection between the intermediate fields $k \subset F \subset K$ and the subgroups $H < \mathrm{Gal}(K/k)$, given by sending $F \mapsto \mathrm{Gal}(K/F)$ and $H \mapsto K^H$ (the subfield of K fixed by the automorphisms in H).

By the above, this statement is straightforward, provided we can show that every subgroup of $\mathrm{Gal}(K/k)$ is isomorphic to $\mathrm{Gal}(K/F)$ for some intermediate field F, and that every intermediate field of K/k consists exactly of the elements of K fixed by the automorphisms in a subgroup of $\mathrm{Gal}(K/k)$.

Corollary 1.5. Suppose f, g are

- (order preserving)
- (inflationary on X)
$$g(f(x)) \geq x \quad \forall x \in X$$
- (deflationary on Y)
$$f(g(y)) \leq y \quad \forall y \in Y$$

Then f, g restrict to bijections on their images.

Proof. Apply Proposition 1.2 to X and Y, with the order on Y reversed. □

Example 1.6 (extension/contraction of ideals)**.** Let $\phi : A \to B$ be a ring map (under our assumptions). Consider the pair

$$\begin{gathered}\{\text{ideals in } A\} \rightleftarrows \{\text{ideals in } B\} \\ \mathfrak{a} \mapsto \mathfrak{a}^e \\ \mathfrak{b}^e \leftarrow \mathfrak{b}\end{gathered}$$

where

- $\mathfrak{a}^e$ is the extension of $\mathfrak{a}$ in B, i.e. $B\phi(\mathfrak{a})$ which means the B-ideal generated by $\phi(\mathfrak{a})$.
- $\mathfrak{b}^e$ is the ... this

Example 1.7. As an extension of the previous example, let $\mathfrak{a}$ be an ideal and consider the quotient map $A \to A/\mathfrak{a}$... finish

2 motivating example: the Gelfand-Kolmogorov theorem

Definition 2.1. Let (X, d) be a compact metric space. Let

$$\begin{aligned}\mathcal{O}_X &:= C(X) := C(X, \mathbb{R}) \\ \mathcal{X} &:= \mathrm{Spec}_m(\mathcal{O}_X) := \{\text{maximal ideals } \mathfrak{m} \subset \mathcal{O}_X\}.\end{aligned}$$

Definition 2.2. For all $x \in X$, consider the evaluation map

$$\begin{aligned} \mathcal{O}_X &\xrightarrow{\epsilon_x} \mathbb{R} \\ f &\mapsto f(x) \end{aligned}$$

We write $\mathfrak{m}_x \coloneqq \ker(\epsilon_x) \subset \mathcal{O}_X$.

Proposition 2.3. $\mathfrak{m}_x \subset \mathcal{O}_X$ is a maximal ideal.

Proof. The quotient $\mathcal{O}_X / \mathfrak{m}_x \cong \mathbb{R}$ is a field. □

Definition 2.4. For $\mathfrak{m} \in \mathrm{Spec}_m(\mathcal{O}_X)$, define

$$v(\mathfrak{m}) \coloneqq \{x \in X : f(x) = 0 \text{ for all } f \in \Updownarrow\}.$$

We call $v(\mathfrak{m})$ the *vanishing locus* of $\mathfrak{m}$.

Remark 2.5. $\mathfrak{m}_x \subset \mathcal{O}_X$ and $v(\mathfrak{m}) \subset X$ are in some sense dual notions: $\mathfrak{m}_x$ is the set of functions which vanish at x, while $v(\mathfrak{m})$ is the set of points x on which each $f \in \mathfrak{m}$ vanishes.

Proposition 2.6 (weak Nullstellensatz)**.** For $\mathfrak{m} \in \mathfrak{X}$, the vanishing locus $v(\mathfrak{m})$ is nonempty.

Proof. Suppose $v(\mathfrak{m})$ is empty. Then for all $x \in X$ there exists $f_x \in \mathfrak{m}$ such that $f_x(x) \neq 0$. Then also $f_x^2(x) \neq 0$ (and $f_x^2 \in \mathfrak{m}$). For the sake of notation we replace f_x with f_x^2, whence we can now assume $f_x(x) > 0$ strictly.

We claim $f_x \geq 0$ on all of X. Let's show this. Since $f_x(x) > 0$ and f_x is continuous, there exists a neighborhood U_x of x such that $f_x|_{U_x} > 0$. Doing this process for all $x \in X$ yields an open cover $\{U_x\}_{x \in X}$ such that $f_x|_{U_x} > 0$. Since X is compact, we may find a finite subcover $U_1, \dots U_N$. Define

$$f = f_{x_1} + \cdots + f_{x_N}.$$

By construction $f \in \mathfrak{m}$. Also $f(x) > 0$ for all $x \in X$, since there exists j such that $x \in U_j$ and so $f_{x_j}(x) > 0$ and $f_{x_i}(x) \geq 0$ for all $i \neq j$. But then $1/f$ is continuous, so $1 \in \mathfrak{m}$ which contradicts the maximality of $\mathfrak{m}$. □

Remark 2.7. Compare with Theorem 2.12 in cstar . ref

Proposition 2.8. The map

$$\begin{aligned} X &\longrightarrow \mathrm{Spec}_m(\mathcal{O}_X) \\ x &\mapsto \mathfrak{m}_x \end{aligned}$$

is bijective.

Proof. First we show injectivity. Suppose $p \neq q \in X$. Consider the functions

$$f_{q,\delta} = \begin{cases} \delta - d(x,q) & d(x,q) > 0 \\ 0 & \text{otherwise} \end{cases}.$$

For any $\delta > 0$ and $q \in X$ it then follows that $f_{q,\delta} \in \mathcal{O}_X$. Now let $\delta = \frac{1}{3}d(p,q)$. Then $f_{q,\delta} \in \mathfrak{m}_p$ but not in $\mathfrak{m}_q$. This shows injectivity.

For surjectivity, pick some $\mathfrak{m} \in \operatorname{Spec}_m(\mathcal{O}_X)$. By Proposition 2.6, there exists $x \in v(\mathfrak{m})$, so in particular $\mathfrak{m} \subset \mathfrak{m}_x := \ker(\epsilon_x)$. But since $\mathfrak{m}$ is maximal, it must be that $\mathfrak{m} = \mathfrak{m}_x$. □

We have thus achieved a setwise correspondence. One way of thinking about this is that we can recover the points of X from $\operatorname{Spec}_m(\mathcal{O}_X)$ (and vice versa). A natural next question is whether we can recover the topology on X as well.

Definition 2.9. For $S \subset X$, define

$$I(S) = \{f \in \mathcal{O}_X : f|_S = 0\} \subset \mathcal{O}_X.$$

For $E \subset \mathcal{O}_X$, define

$$V(E) = \{x \in X : f(x) = 0 \text{ for all } f \in E\} \subset X.$$

Proposition 2.10. We make the following observations:

1. For $x \in X$,
$$I(\{x\}) = \mathfrak{m}_x.$$

2. For $S \subset X$,
$$I(S) = \bigcap_{x \in S} I(\{x\}) = \bigcap_{x \in S} \mathfrak{m}_x \subset \mathcal{O}_X$$
is an ideal (). It is proper if S is nonempty, by Proposition 2.6. ref

3. I is order reversing:
$$S_1 \subset S_2 \subset X \quad \Rightarrow \quad I(S_1) \supset I(S_2).$$

4. The pair I, V is inflationary on X:
$$S \subset X \quad \Rightarrow \quad S \subset V(I(S)).$$

5. E is order reversing:
$$E_1 \subset E_2 \subset \mathcal{O}_X \quad \to \quad V(E_1) \supset V(E_2).$$

6. The pair I, V is inflationary on $\mathcal{O}_X$:
$$E \subset \mathcal{O}_X \quad \Rightarrow \quad E \subset I(V(E)).$$

Corollary 2.11. The maps

$$\left\{ \begin{matrix} \text{subsets of} \\ X \end{matrix} \right\} \underset{V}{\overset{I}{\rightleftarrows}} \left\{ \begin{matrix} \text{ideals in} \\ \mathcal{O}_X \end{matrix} \right\}$$

form an antitone Galois connection.

Proposition 2.12. If $E \subset \mathcal{O}_X$, then $V(E) = V(\mathcal{O}_X E)$, where $\mathcal{O}_X E \subset \mathcal{O}_X$ is the ideal generated by E.

Proof. Since $E \subset \mathcal{O}_X E$ and V is order reversing, we have that $V(E) \supset V(\mathcal{O}_X E)$. Conversely, let $a \in V(E)$. Then there $f(a) = 0$ for all $f \in E$. But any $h \in \mathcal{O}_X E$ has the form $h = \sum_i g_i f_i$, where $g_i \in \mathcal{O}_X$ and $f_i \in E$. Then it follows that $h(a) = 0$, so $a \in V(\mathcal{O}_X E)$, and hence $V(E) \subset V(\mathcal{O}_X E)$. □

Recall that we though of images of maps belonging to an antitone Galois connection as "closed" in some sense. The next proposition shows that this notion coincides with the topological one in this case:

Proposition 2.13. For $\mathfrak{a} \subset \mathcal{O}_X$ an ideal, $V(\mathfrak{a}) \subset X$ is closed in the topological sense.

Proof. The arbitrary union of closed sets is closed, and

$$V(\mathfrak{a}) = \bigcap_{f \in \mathfrak{a}} V(f) = \bigcap_{f \in \mathfrak{a}} f^{-1}(\{0\})$$

and $\{0\} \subset X$ is closed and f is continuous, hence $f^{-1}(\{0\})$ is closed. □

So "closed" in the sense of Galois connections implies closed in the topological sense. Recall that the composition of the two functions in a Galois connection were thought of as acting like closures. This following makes this concrete in the topological sense:

Proposition 2.14. If $S \subset X$, then $V(I(S)) = \overline{S}$.

Proof. By the previous proposition, we know $V(I(S))$ is closed, and by the inflationary property $S \subset V(I(S))$, and so $\overline{S} \subset V(I(S))$. Conversely, it suffices to show that if $x \notin \overline{S}$ then $x \notin V(I(S))$. So $x \notin \overline{S}$ implies there exists an ϵ-ball centered at x which avoids S. Take $\delta = \epsilon/2$. Then the bump function $f_{x,\delta}$ is 0 on S, and hence $f_{x,\delta} \in I(S)$. But also $f_{x,\delta}(x) = \delta > 0$, and so $x \notin V(I(S))$. □

Corollary 2.15. Let $\mathfrak{a} \subset \mathcal{O}_X$. Then points in $V(\mathfrak{a}) \subset X$ corresponds to maximal ideals $\mathfrak{a} \subset \mathfrak{b} \subset \mathcal{O}_X$ containing $\mathfrak{a}$.

Proof. Let $x \in V(\mathfrak{a})$. Then $\{x\} \subset V(\mathfrak{a})$ and by the order-reversing property $I(\{x\}) \supset I(V(\mathfrak{a})) \supset \mathfrak{a}$. But $I(\{x\}) = \mathfrak{m}_x$. □

Definition 2.16. For an ideal $\mathfrak{a} \subset \mathcal{O}_X$, define

$$\mathcal{V}(\mathfrak{a}) = \{\mathfrak{m} \in \operatorname{Spec}_m(\mathcal{O}_X : \mathfrak{m} \supset \mathfrak{a})\} \subset \operatorname{Spec}_m(\mathcal{O}_X).$$

The previous corollary suggests $\mathcal{V}(\mathfrak{a}) \subset \mathcal{O}_X$ corresponds to the points of $V(\mathfrak{a}) \subset X$.

Corollary 2.17. $\mathcal{V}(-)$ is order reversing.

Recalling the bijection in Proposition 2.8, denote by $m(V(f))$ the image of $V(f) \subset X$ under the map $x \mapsto \mathfrak{m}_x$.

Proposition 2.18. $\mathfrak{m}(V(f)) = \mathcal{V}((f))$.

Proof. $x \in V(f)$ if and only if $f(x) = 0$ if and only if $f \in \mathfrak{m}_x$ if and only if $(f) \subset \mathfrak{m}_x$ if and only if $\mathfrak{m}_x \in \mathcal{V}((f))$. □

Corollary 2.19. If $\mathfrak{a} \subset \mathcal{O}_X$ is an ideal, then $\mathfrak{m}(V(\mathfrak{a})) = \mathcal{V}(\mathfrak{a})$.

Proof. We calculate

$$\mathfrak{m}(V(\mathfrak{a})) = m\left(\bigcap_{f\in\mathfrak{a}} V(f)\right) = \bigcap_{f\in\mathfrak{a}} m(V(f)) = \bigcap_{f\in\mathfrak{a}} \mathcal{V}(f) = V(\mathfrak{a},$$

where the commuting with $\bigcap$ is justified since $\mathfrak{m}(-)$ is bijective (Proposition 2.8) and we also used the fact that $V(f) = V((f))$. □

ref

So since $V(\mathfrak{a}) \subset X$ is closed, and $\mathcal{V}(\mathfrak{a}) \subset \mathcal{O}_X$ corresponds to it, we may think of $\mathcal{V}(a)$ as closed too:

Definition 2.20. The topology on $\mathrm{Spec}_m(\mathcal{O}_X)$ whose closed sets are of the form $\mathcal{V}(\mathfrak{a})$ for some ideal $\mathfrak{a} \subset \mathcal{O}_X$ is called the *Zariski topology* on $\mathrm{Spec}_m(\mathcal{O}_X)$.

Corollary 2.21. $\mathfrak{m}(-) : X \to \mathrm{Spec}_m(\mathcal{O}_X)$ is a homeomorphism.

Proof. It is bijective by Proposition 2.8. Suppose $S \subset X$ is closed. Then it is equal to $V(I(S))$. Since $I(S)$ is an ideal, it follows that $\mathfrak{m}(V(I(S))) = \mathcal{V}(I(S))$ which is closed by definition. Hence the map is closed. □

Definition 2.22. For $f \in \mathcal{O}_X$, define the *distinguished* open set in X by

$$D(f) := X - V(f).$$

Dually, define an open set in $\mathrm{Spec}_m(\mathcal{O}_X)$ by

$$\mathcal{D}(f) := X - \mathcal{V}(f).$$

Corollary 2.23. $m(D(f)) = \mathcal{D}(f)$.

Proposition 2.24. The distinguished open sets form a basis for the topology on X.

Proof. The open balls are a basis for the topology on X. But $B(x, \epsilon) = D(f_{x,\epsilon})$. □

check holo

So we have built up that for a compact metric space X, we may associate a commutative $\mathbb{R}$-algebra $\mathcal{O}_X$, and can again obtain a (space homeomorphic to our original) compact metric space. An outstanding question is whether a continuous function $\phi : X \to Y$ induces a continuous map $\mathrm{Spec}_m(\mathcal{O}_X) \to \mathrm{Spec}_m(\mathcal{O}_Y)$.

Proposition 2.25. A continuous function $\phi : X \to Y$ induces a ring homomorphism $\phi^{\#} : \mathcal{O}_Y \to \mathcal{O}_X$ in the other direction sending $f \mapsto f \circ \phi$.

Corollary 2.26. $\phi : X \to Y$ induces a function from the ideals of $\mathcal{O}_X$ to the ideals of $\mathcal{O}_Y$, sending $\mathfrak{a}$ to its contraction $(\phi^{\#})^{-1}(\mathfrak{a})$.

This is almost what we want: we want this to restrict to maximal ideals.

Proposition 2.27. $\tilde{\phi}$ carries maximal ideals to maximal ideals, hence restricts to a map

$$\tilde{\phi} : \operatorname{Spec}_m(\mathcal{O}_X) \to \operatorname{Spec}_m(\mathcal{O}_Y).$$

Moreover, $\tilde{\phi}(\mathfrak{m}_x) = \mathfrak{m}_{\phi(x)}$. diagram

The last statement of the propositionis telling us that the algebraic map $\tilde{\phi}$ on maximal ideals encodes all the information about our initial continuous function ϕ. This is reliant on the crucial fact, which is false in general, that the contraction of a maximal ideal along is maximal.

Proof. Now we will show $(\phi^{\#})^{-1} = \mathfrak{m}_{\phi(x)}$. Let $f \in \mathfrak{m}_{\phi(x)}$. Then $0 = f(\phi(x)) = (\phi^{\#}(f))(x)$, which shows $\phi^{\#}(f) \in \mathfrak{m}_x$ and hence $f \in (\phi^{\#})^{-1}(\mathfrak{m}_x)$ since the contraction of a maximal ideal is maximal by the first part of the proof. So $\mathfrak{m}_{\phi(x)} \subset (\phi^{\#})^{-1}(\mathfrak{m}_x)$. Equality follows since $\mathfrak{m}_{\phi(x)}$ is maximal. □ first part

Corollary 2.28. We have a pair contravariant functors

$$\left\{\begin{matrix}\text{compact metric}\\ \text{spaces}\end{matrix}\right\} \underset{\operatorname{Spec}_m(-)}{\overset{\mathcal{O}_{(-)}}{\rightleftarrows}} \left\{\begin{matrix}\text{commutative}\\ \mathbb{R}\text{-algebras}\end{matrix}\right\}$$

and $\operatorname{Spec}_m(-) \circ \mathcal{O}_{(-)}$ is naturally equivalent to the identity on the category of compact metric spaces.

Remark 2.29. It is not true that this is an equivalence of categories. why?

3 affine algebraic varieties

Just as one may begin to consider manifolds as embedded in Euclidean space, we will begin to consider varieties within affine space.

In the following, fix the field k to be an algebraically closed field.

Definition 3.1. *Affine n-space* (over k) is, as a set, $\mathbb{A}^n = k^n$. We will write its elements as $\underline{a} = (a_1, \dots, a_n)$ where $a_i \in k$.

Observe that every polynomial $f \in k[X_1, \dots, X_n]$ determines a function $\hat{f} : \mathbb{A}^n \to k$ on affine space by evaluation:

$$\hat{f}(a_1, \dots, a_n) = f(a_1, \dots, a_n).$$

It is not immediately obvious that $\hat{f} = 0$ implies $f = 0$. For instance, consider the finite field $\mathbb{F}_p$ of p elements. In this field we have the identity $x^p = x$ for all elements x. In particular, the polynomial $X^p - X$ vanishes on all of $\mathbb{F}_p$, even though this is not 0 in the polynomial ring $\mathbb{F}_p[X]$. However, this situation is impossible under our assumptions:

Proposition 3.2. The map

$$\begin{gathered} k[X_1, \ldots, X_n] \to \operatorname{Hom}(\mathbb{A}^n, k) \\ f \mapsto \hat{f} \end{gathered}$$

is injective. [1]

Proof. We induct on n.

For $n = 1$, consider a nonzero $f \in k[X]$. This has only finitely many roots, and since k is infinite it must be that $\hat{f} \neq 0$.

For $n > 1$. consider a nonzero $f \in k[X_1, \ldots, X_n]$. We may regard this as a polynomial in $k[X_1, \ldots, X_{n-1}][X_n]$. Now if $\deg_{X_n}(f) = 0$, then $f \in k[X_1, \ldots, X_{n-1}]$ which is already handled by the induction hypothesis. So suppose $d = \deg_{X_n}(f) > 0$. Then

$$f = \sum_{j=0}^{d} f_j X_n^j$$

for some $f_j \in k[X_1, \ldots, X_n]$ with $f_d \neq 0$. By induction, $\hat{f}_d \neq 0$ so there exists $(a_1, \ldots, a_{n-1}) \in \mathbb{A}^{n-1}$ such that $f_d(a_1, \ldots, a_{n-1}) \neq 0$. Let

$$g = f(a_1, \ldots, a_{n-1}, X_n) = \sum_{j=1}^{d} f_j(a_1, \ldots, a_{n-1}) X_n^j \in k[X_n].$$

Then $g \neq 0$. By the $n = 1$ case there exists $b \in k$ such that

$$0 \neq g(b) = f(a_1, \ldots, a_{n-1}, b) = \hat{f}(a_1, \ldots, a_{n-1}, b)$$

which shows $\hat{f} \neq 0$. □

Definition 3.3. The *coordinate ring* of $\mathbb{A}^n$ is

$$\Gamma(\mathbb{A}^n) = k[X_1, \ldots, X_n].$$

The *function field* of $\mathbb{A}^n$ is the fraction field of its coordinate ring, i.e.

$$K(\mathbb{A}^n) = \operatorname{Frac}(\Gamma(\mathbb{A}^n)) = k(X_1, \ldots, X_n).$$

Definition 3.4. For a subset $E \subset \Gamma(\mathbb{A}^n)$, we define its *vanishing locus* as

$$\mathbf{V}(E) \coloneqq \{\underline{a} \in \mathbb{A}^n : f(\underline{a}) = 0 \text{ for all } f \in E\}.$$

Conversely, any subset of $\mathbb{A}^n$ that is a vanishing locus as above is called an *affine algebraic set.*

[1] this proposition is true for any infinite field

Definition 3.5. Given a subset $S \subset \mathbb{A}^n$, define its *vanishing ideal* to be

$$\mathbf{I}(S) \coloneqq \{f \in \Gamma(\mathbb{A}^n) : f|_S = 0\}.$$

Proposition 3.6. $\mathbf{I}(S)$ is an ideal.

Proof. Suppose $f, g \in \mathbf{I}(S)$. Then for any $s \in S$, we have $(f+g)(s) = f(s) + g(s) = 0$ hence $f + g \in \mathbf{I}(S)$. Now let $h \in \Gamma(\mathbb{A}^n)$. Then $fg(s) = f(s)g(s) = 0$ so $fg \in \mathbf{I}(S)$. □

Proposition 3.7. The pair

$$\begin{tikzcd} \left\{ \begin{array}{c} \text{subsets of} \\ \mathbb{A}^n \end{array} \right\} \arrow[r, shift left, "\mathbf{I}(-)"] & \left\{ \begin{array}{c} \text{ideals in} \\ \Gamma(\mathbb{A}^n) \end{array} \right\} \arrow[l, shift left, "\mathbf{V}(-)"] \end{tikzcd}$$

forms an antitone Galois connection.

Proof. □

prove

Corollary 3.8. $\mathbf{V}(E) = \mathbf{V}(\langle E \rangle)$, where $\langle E \rangle$ is the ideal generated by E.

Theorem gives us an inverse bijection on the images of these functions, but we still need to determine what those images are. Based on Remark , we want $\operatorname{im}(\mathbf{V}(-)) \subset \mathbb{A}^n$ to be like "closed sets" and $\operatorname{im}(\mathbf{I}(-))$ to be like "closed ideals". One direction is not so difficult:

ref

ref

Proposition 3.9. $\operatorname{im}(\mathbf{V}(-))$ is the set of affine algebraic sets.

Proof. It is clear by definition that everything in $\operatorname{im}(\mathbf{V}(-))$ is an affine algebraic set. It remains to show that every affine algebraic set has this form. Well by definition every affine algebraic set has the form $\mathbf{V}(E)$ for some subset $E \subset \Gamma(\mathbb{A}^n)$. By Corollary 3.8, this is the same as $\mathbf{V}(\langle E \rangle)$, and we are done. □

If we consider $\mathbf{I}(-)$, the situation is more subtle, and is essentially the content of Hilbert's Nullstellensatz. For example, we can imagine the following situation to believe that the image is not all ideals in $\Gamma(\mathbb{A}^n)$:

Example 3.10. Consider a nonzero $f \in \mathfrak{a}$. Consider the ideal $\mathfrak{a} = \langle f^N \rangle$ for some $N > 1$. By construction it is an ideal in $\Gamma(\mathbb{A}^n)$.

Suppose $\underline{a} \in \mathbf{V}(\mathfrak{a})$. Then

$$0 = f^N(\underline{a}) = f(\underline{a})^N,$$

implying $f(\underline{a})$ by our assumptions on k (in particular it is a field, hence has no zero divisors). Since this holds for all $\underline{a} \in \mathbf{V}(\mathfrak{a})$, we see that $f \in \mathbf{I}(\mathbf{V}(\mathfrak{a}))$.

However, the point of our construction was that f is not necessarily in $\mathfrak{a}$, while f^N is. In other words, $f \in \sqrt{a}$. This suggests we should be considering the radical ideals instead of all ideals.

Corollary 3.11. If $V \subset \mathbb{A}^n$ is an algebraic subset, then $\mathbf{I}(V)$ is radical, i.e. $\mathbf{I}(V) = \sqrt{\mathbf{I}(V)}$.

Now observe that a function $\frac{f}{g} \in K(\mathbb{A}^n)$ defines a function

$$\mathbb{A}^n - \mathbf{V}(\{g\}) \to k.$$

Definition 3.12. An element of $K(\mathbb{A}^n)$ defined on all of $\mathbb{A}^n$ is called a *regular function.*

By the above observation, a function $\frac{f}{g}$ is regular if g is nowhere-vanishing. conversely?

Definition 3.13. Let $V \subset \mathbb{A}^n$ be an algebraic set. A function $f : V \to k$ is called *regular* if it is the restriction of a regular function on $K(\mathbb{A}^n)$.

Eventually we will want to define regular functions independently of the ambient affine space. For the moment, we have a surjection

$$\Gamma(\mathbb{A}^n) \xrightarrow{\text{res}} \Gamma(V)$$

whose kernel consists of regular functions vanishing on V.

Corollary 3.14.

$$\Gamma(V) \cong \frac{\Gamma(\mathbb{A}^n)}{\mathbf{I}(V)} \cong \frac{k[X_1, \ldots, X_n]}{\mathbf{I}(V)}.$$

Example 3.15. Consider the algebraic set $V = \mathbf{V}(Y - X^2) \subset \mathbb{A}^2$, where $(Y - X^2) \subset \Gamma(\mathbb{A}^2) = k[X, Y]$ is an ideal. We will show that the geometric correspondence in affine space

$$\mathbb{A}^1 \underset{\phi}{\overset{\psi}{\rightleftarrows}} V \subset \mathbb{A}^2$$

corresponds to the algebraic correspondence of rings

$$\Gamma(\mathbb{A}^1) \underset{\psi^\#}{\overset{\phi^\#}{\rightleftarrows}} \Gamma(V).$$

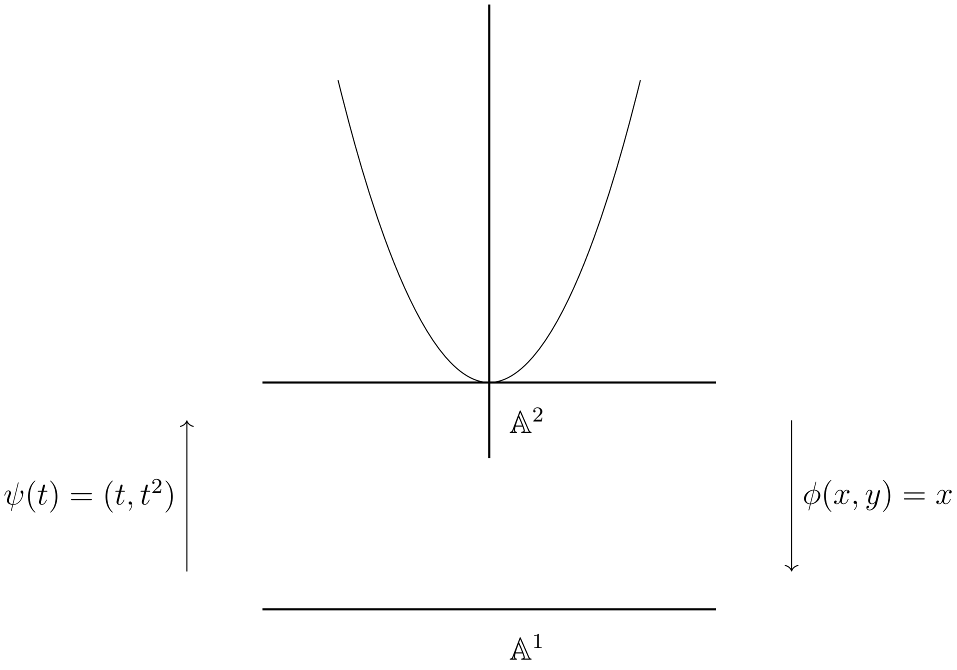
First consider the situation on rings. By Corollary 3.14, we know

$$\Gamma(V) = \frac{k[X, Y]}{(Y - X^2)}.$$

As a ring, this is generated by $\{1, X\}$, since $k[X, Y]$ is generated by $\{1, X, Y\}$ and in the quotient ring $Y - X^2 = 0$, i.e. $Y = X^2$. This provides an explicit isomorphism

$$\begin{gathered} \frac{k[X, Y]}{(Y - X^2)} \to k[T] \\ X \mapsto T. \end{gathered}$$

On the level of affine space, consider the maps



One verifies that this determines a bijection $\mathbb{A}^1 \to V$.

How do we connect these two correspondences? Consider the map

$$\begin{aligned} \phi^{\#} : \Gamma(\mathbb{A}^1) &\to \Gamma(V) \\ T &\mapsto T \circ \phi. \end{aligned}$$

Intuitively, this sends the polynomial T to the polynomial which picks out the first coordinate, i.e. the polynomial X. Now consider the map

$$\begin{aligned} \psi^{\#} : \Gamma(V) &\to \Gamma(\mathbb{A}^1) \\ \bar{f} &\mapsto \bar{f} \circ \psi. \end{aligned}$$

In particular, this sends the polynomial Y (which picks out the second coordinate) to T^2.

If we regard $\{1, X, Y\}$ as generators of $k[X, Y] = \Gamma(\mathbb{A}^2)$, then the correspondence on the level of rings is given by $X \mapsto T$ and $Y \mapsto T^2$.

Which rings arise as $\Gamma(V)$ for some algebraic set $V \subset \mathbb{A}^n$? For one, we know every $\Gamma(V)$ must hhave the following form:

$$\Gamma(V) = \frac{\Gamma(\mathbb{A}^n)}{I(V)} = \frac{k[X_1, \ldots, X_n]}{I(V)},$$

which is in particular a finitely-generated k-algebra. From Corollary 3.11, we know that $\mathbf{I}(V) = \sqrt{\mathbf{I}(V)}$. So in particular if $f \in \Gamma(V)$ is such that $f^N = 0$ on V, i.e. $f^N \in \mathfrak{I}(V)$, then $f = 0$, i.e. $f \in \mathfrak{I}(V)$. Since polynomial rings over a field are reduced, it then follows that $\Gamma(V)$ is reduced [2]. To summarize:

[2] i.e. it has no nilpotent elements

- $\Gamma(V)$ is finitely generated.
- $\Gamma(V)$ is reduced.

The big question is: if some k-algebra has these two properties, is it of the form $\Gamma(V)$?

Definition 3.16. An *affine k-algebra* is a finitely generated reduced k-algebra, i.e.

$$A \cong \frac{k[X_1, \ldots, X_n]}{I}$$

for some radical ideal ideal $I \subset k[X_1, \ldots, X_n]$.

Definition 3.17. Let X be a topological space. We call a nonempty subset of X *irreducible* if X cannot be written as a union of two proper closed subsets.

Remark 3.18. Note that spaces that have such a property are quite pathological!

Proposition 3.19. An algebraic set $Y \subset \mathbb{A}^n$ is irreducible if and only if $\mathbf{I}(Y)$ is prime.

Proof. First we will do the forward direction. Suppose Y is irreducible. Suppose $fg \in \mathbf{I}(Y)$. We want to show that either $f \in \mathbf{I}(Y)$ or $g \in \mathbf{I}(Y)$. First, $fg \in \mathbf{I}(Y)$ implies $(fg) \subset \mathbf{I}(Y)$, and so $\mathbf{V}(\mathbf{I}(Y)) \subset \mathbf{V}(fg) = \mathbf{V}(f) \cup \mathbf{V}(g)$. Since $Y \subset \mathbf{V}(\mathbf{I}(Y))$, we get

$$Y = Y \cap (\mathbf{V}(f) \cup \mathbf{V}(g)) = (Y \cap \mathbf{V}(f)) \cap (Y \cap \mathbf{V}(g))$$

Now by the definition of the Zariski topology, $\mathbf{V}(f)$ and $\mathbf{V}(g)$ are closed. Since Y is an algebraic set, it is also closed. Hence the above expresses Y as the union of two closed sets. By our assumption that Y is irreducible, either:

- $Y = Y \cap \mathbf{V}(f)$, which implies $Y \subset \mathbf{V}(f)$ so $f|_Y = 0$ so $f \in I(Y)$.
- analagous.

This proves the forward direction.

For the reverse direction, suppose $\mathbf{I}(Y) = \mathfrak{p}$ is prime. We need to show Y is irreducible. Since Y is closed, by () we know $Y = \mathbf{V}(\mathbf{I}(Y)) = \mathbf{V}(\mathfrak{p})$. Suppose that we can write $Y = Y_1 \cup Y_2$, ref where Y_1 and Y_2 are closed in Y (hence in $\mathbb{A}^n$). Then

$$\mathfrak{p} = \mathbf{I}(Y) = \mathbf{I}(Y_1 \cup Y_2) = \mathbf{I}(Y_1) \cap \mathbf{I}(Y_2).$$

But $\mathfrak{p}$ is prime, so by () $\mathfrak{p} = \mathbf{I}(Y_1)$ or $\mathfrak{p} = \mathbf{I}(Y_2)$. But then either $Y = \mathbf{V}(\mathfrak{p}) = \mathbf{V}(I(Y_1)) = Y_1$ ref or $Y = \mathbf{V}(\mathfrak{p}) = \mathbf{V}(I(Y_2)) = Y_2$. □

Definition 3.20. An *affine algebraic variety* is an irreducible affine algebraic set.

4 Hilbert basis theorem

Proposition 4.1. Let $(P, \leq)$ be a poset. Then the following are equivalent:

- (ascending chain condition, ACC) Every increasing sequence

$$x_1 \leq x_2 \leq x_3 \leq \cdots$$

stabilizes, i.e. there exists $N \in \mathbb{N}$ such that $x_N = x_{N+1} = \cdots$.

- Every nonempty subset of P has a maximal element.

Proof. ($1 \Rightarrow 2$) We prove the contrapositive, so suppose there exists a nonempty subset $\Sigma \subset P$ which does not have a maximal element. Let $x_1 \in \Sigma$. Then there exists $x_2 \in \Sigma$ such that $x_1 < x_2$ strictly. Repeating this procedure produces a sequence which does not stabilize.

($2 \Rightarrow 1$) Let $x_1 \leq x_2 \leq \cdots$ be an ascending chain. By assumption, the set $\{x_i\}_i$ has a maximal element, call it x_N. But then it must be that $x_N = x_{N+1} = \cdots$, i.e. the chain stabilizes. □

We will want to apply Proposition 4.1 to the situation where we have an A-module M and our partially ordered set is the submodules of M with ordering coming from inclusion.

Definition 4.2. An A-module M is called *Noetherian* if it satisfies the ascending chain condition (equivelently, every collection of submodules of M has a maximal element). A ring is called Noetherian if it is Noetherian as a module over itself.

Proposition 4.3. The following are equivalent:

1. M is Noetherian.
2. All submodules of M are finitely-generated.

Proof. ($1 \Rightarrow 2$) Suppose M is Noetherian. Let $N \subset M$ be a submodule. Let Σ be the set of all finitely generated submodules of N. Then Σ is nonempty, since for instance it contains a cyclic submodule [3]. Since every submodule of N is a submodule of M, it follows by the assumption on M that Σ has a maximal element $\bar{N}$. We claim that $\bar{N} = N$, which will show that N is finitely generated. Suppose otherwise. Then there exists $x \in N - \bar{N}$. But then $\bar{N} + \langle x \rangle$ is finitely generated, violating the maximality of $\bar{N}$. Hence $N = \bar{N}$, and N is finitely generated.

($2 \Rightarrow 1$) Now suppose that submodules of M are finitely-generated. Let $M_1 \subset M_2 \subset \cdots$ be an ascending chain of submodules. Let

$$M_\infty = \bigcup_{n \geq 0} M_n.$$

Then M_∞ is finitely-generated, since it is also a submodule. Call its set of generators $\{x_1, \ldots, x_n\}$. Since each x_i must be in some M_{k_i}, let $k = \max\{k_1, \ldots, k_n\}$. But then $\{x_1, \ldots, x_n\} \subset M_k$, which shows that $M_\infty \subset M_k \subset M_\infty$. Hence $M_k = M_{k+1} = \cdots$ which shows the chain stabilizes, hence M is Noetherian. □

[3] i.e. a submodule generated by a single element (which lies in N)

Example 4.4. $\mathbb{Z}$ is Noetherian as a module over itself. Submodules of a ring regarded as a module over itself are just its ideals, and every ideal in $\mathbb{Z}$ is principal.

Example 4.5. $\mathbb{Z}_{p^\infty}$, the p-primary part of $\mathbb{Q}/\mathbb{Z}$, is not Noetherian.

Proposition 4.6. If

$$0 \to M' \to M \to M'' \to 0$$

is exact, then M is Noetherian if and only if M' and M'' are Noetherian.

Proof. HW □

hw

Theorem 4.7 (Hilbert basis theorem)**.** If A is a Noetherian ring, then $A[X]$ is also Noetherian.

Proof. For an ideal $E \subset A[X]$, define $C_nI \subset A$ to be the set of coefficents of X^n for functions $f \in I$ of degree $\leq n$. In other words, it is the set of leading coefficents for degree n polynomials in I along with 0.

Lemma 4.8. $C_nI \subset A$ is an ideal.

Proof. Exercise. □

Lemma 4.9. $C_0I \subset C_1I \subset C_2I \subset \cdots$ for any ideal $I \subset A[X]$.

Proof. Exercise. □

Lemma 4.10. Let $I, J \subset A[X]$ be ideals, with $I \subset J$. Then

1. $C_iI \subset C_iJ$ for all i.
2. If $C_iI = C_iJ$ for all i, then $I = J$.

Proof. The first statement is clear after unwrapping definitions. For the second, suppose $C_iI = C_jJ$ for all i. Let $f \in J$. In light of the first statement, it suffices to show $f \in I$. We will do this by inducting on $\deg(f) = n$.

For $n = 0$, we know $f \in I$ because then f is a constant, so its leading coefficient is itself. Since $C_iI = C_iJ$, we know $f \in C_0I$. So then there must be a degree 0 polynomial $g \in I$ whose leading coefficient is f. But there is only one, namely f, i.e. $f = g$, so $f \in I$.

In the general case, let

$$f = a_nX^n + \cdots + a_1X + a_0 \in J,$$

with $a_n \neq 0$ (if $a_n = 0$ then we are done by induction). This means $a_n \in C_nJ = C_nI$, and so there exists $g \in I$ of the form

$$g = a_nX^n + b_{n-1}X^{n-1} + \cdots + b_1X + b_0 \in I \subset J.$$

Then $f - g \in J$, and since $\deg(f - g) < n$ strictly we have by induction that $f - g \in I$. But then $f = (f - g) + g \in I$ too. □

Let $I_0 \subset I_1 \subset \cdots$ be an ascending chain of ideals in $A[X]$. Consider the diagram

$$\begin{tikzcd}
\vdots & \vdots & \vdots & \\
I_2 \arrow[u, hook] & C_0I_2 \arrow[u, hook] \arrow[r, hook] & C_1I_2 \arrow[u, hook] \arrow[r, hook] & \cdots \\
I_1 \arrow[u, hook] & C_0I_1 \arrow[u, hook] \arrow[r, hook] & C_1I_1 \arrow[u, hook] \arrow[r, hook] & \cdots \\
I_0 \arrow[u, hook] & C_0I_0 \arrow[u, hook] \arrow[r, hook] & C_1I_0 \arrow[u, hook] \arrow[r, hook] & \cdots
\end{tikzcd}$$

If we can show that the square on the right stabilizes "uniformly" at a certain height, then so will $I_0 \subset I_1 \subset \cdots$ by the previous lemma. We can stabilize each column individually, but we need to show that there is a single $N > 0$ after which all columns stabilize.

Consider the chain formed on the diagonal, i.e.

$$C_0I_0 \subset C_1I_1 \subset \cdots$$

This is an ascending chain in A by the above lemma, hence stabilizes at some index k. But this means all arrows in above and right of (k, k) are equalities, by the principle that $A \subset B \subset A$ implies $A = B$:

$$\begin{tikzcd}
\vdots & \vdots & \\
C_kI_{k+1} \arrow[u, hook] \arrow[r, hook] & C_{k+1}I_{k+1} \arrow[u, hook] \arrow[r, hook] & \cdots \\
C_kI_k \arrow[u, hook] \arrow[r, hook] \arrow[ur, equal] & C_{k+1}I_k \arrow[u, hook] \arrow[r, hook] & \cdots
\end{tikzcd}$$

Now we only need to uniformly stabilize the first k columns. Since they each individually stabilize, and there's finitely many of them, we can just take the max of the indices after which they stabilize. □

5 Nullstellensatz

For now let k be a field. Eventually we will require it to be algebraically closed.

Example 5.1. Recall that $k[X]$ is the free k-algebra on the one-element set $\{X\}$ (as an algebra it is generated by one element, but as a module it is generated by countably infinite many). Consider the diagram

$$\begin{tikzcd}
\{X\} \arrow[r, "i"] \arrow[dr, "\alpha"'] & k[X] \arrow[d, "\epsilon_\alpha"] \\
 & A
\end{tikzcd}$$

where A is any k-algebra. Here α is any function. Since it is a function out of a one-element set, it amounts to picking out an element in A. To make this diagram commute, ϵ_α must send $X \mapsto \alpha$, which on a polynomial amounts to evaluating that polynomial at the point α.

Now suppose we take $A = K$ to be monogenic, i.e. generated by one elment α. There are two cases.

1. ϵ_α is injective. Then since it also maps to the generater of K, it's surjective, hence $K \cong k[X]$. But then K is not a field, and in particular is not an algebraic extension of $k[X]$. We may think of this as the case where α is transcendental.
2. ϵ_α is not injective. Then α is the root of some polynomial, hence "by definition" $K = k(\alpha)$ is a finite algebraic extension of k.

Zariski's lemma can be seen as a multivariable analogue of this property:

Theorem 5.2 (Zariski's lemma)**.** Let K be a finitely generated k-algebra. If K is a field, then it is a finite algebraic extension of k.

We now assume k is algebraically closed.

Theorem 5.3 (weak Nullstellensatz)**.** Let $I \subsetneq k[X_1, \ldots, X_n]$ be a proper ideal. Then $\mathbf{V}(I) \neq \emptyset$, i.e. there exists at least one point in $\mathbb{A}^n_k$ which on which all of I vanishes.

Proof. The idea is to reduce to considering maximal ideals. The quotient of these with the polynomial ring is a field, hence a finite algebraic extension by Zariski's lemma. Since we algebraically closed, this field must be k itself. We then pull back each inderminate to k to find a point $\underline{a}$ such that $\mathfrak{m}_{\underline{a}} \subset \mathfrak{m}$, hence the two are equal, hence $\underline{a} \in \mathbf{V}(\mathfrak{m})$.

Since I is proper, it's contained in a maximal ideal $\mathfrak{m}$. Then $\mathbf{V}(\mathfrak{m}) \subset \mathbf{V}(I)$, so it suffices to consider maximal ideals.

Let $K \coloneqq k[X_1, \ldots, X_n]/\mathfrak{m}$. Consider the composite

$$\begin{tikzcd}
k \arrow[r, "i"] \arrow[rd, dashed, "\phi"'] & k[X_1, \ldots, X_n] \arrow[d, "\pi"] \\
& K
\end{tikzcd}$$

By Zariski's lemma, K is a finite algebraic extension of k. Since k is algebraiclly closed, $K \cong k$ and in particular ϕ is an isomorphism.

Let $a_i = \phi^{-1}(\bar{X_i})$. This means $a_i + \mathfrak{m} = X_i + \mathfrak{m}$, i.e. $X_i - a_i \in \mathfrak{m}$ for all i. The the maximal ideal $m_{\underline{a}} = (X_1 - a_1, \ldots, X_n - a_n)$ is contained in $\mathfrak{m}$, hence $\mathfrak{m}_{\underline{a}} = \mathfrak{m}$. But certainly $\underline{a} \in \mathbf{V}(\mathfrak{m}_{\underline{a}})$, so we're done. □

Corollary 5.4. If k is algebraically closed, then *all* maximal ideals are of the form $\mathfrak{m}_{\underline{a}} = (X_1 - a_1, \ldots, X_n - a_n)$.

Theorem 5.5 (strong Nullstellensatz)**.** Let $\mathfrak{a} \subset k[X_1, \ldots, X_n]$. Then $\mathbf{I}(\mathbf{V}(\mathfrak{a})) = \sqrt{\mathfrak{a}}$.

Proof. ($\supset$) Follows by Corollary 3.11.

($\subset$) Let $h \in \mathbf{I}(\mathbf{V}(\mathfrak{a}))$ be nonzero. We want to show $h \in \sqrt{\mathfrak{a}}$. To that end, consider $\tilde{\mathfrak{a}} \in k[X_1, \ldots, X_n][Y]$ given by

$$\tilde{\mathfrak{a}} \coloneqq \langle \mathfrak{a} \cup \{1 - hY\} \rangle \subset k[X_1, \ldots, X_n][Y],$$

i.e. the ideal generated by $\mathfrak{a}$ and $1 - hY$.

We claim $\mathbf{V}(\tilde{\mathfrak{a}})) \subset \mathbb{A}_k^{n+1}$ is empty. Suppose otherwise, i.e. there exists an element $(a_1, \ldots, a_n, b) \in \mathbf{V}(\tilde{\mathfrak{a}})$. Then since $\mathfrak{a} \subset \tilde{\mathfrak{a}}$, we have that $\tilde{f}(a_1, \ldots, a_n, b) = f(a_1, \ldots, a_n, b) = 0$ for any $f \in \mathfrak{a}$. But then $(a_1, \ldots, a_n) \in \mathbf{V}(\mathfrak{a})$. But then $0 = (1 - hY)(a_1, \ldots, a_n, b) = 1 - h(a_1, \ldots, a_n)b = 1$, a contradiction. This proves the claim.

Now, by the weak Nullstellensatz we know that $\tilde{\mathfrak{a}} = k[X_1, \ldots, X_n][Y]$, and in particular $1 \in \tilde{\mathfrak{a}}$. Then using the fact that $\tilde{\mathfrak{a}} = \langle \mathfrak{a} \cup \{1 - hY\} \rangle$, we can write

$$1 = \sum_{i=1}^{r} F_i(X_1, \ldots, X_n, Y) g_i(X_1, \ldots, X_n) + F(X_1, \ldots, X_n)(1 - h(X_1, \ldots, X_n)Y)$$

for some $g_i \in \mathfrak{a}$ and some $F_i \in k[X_1, \ldots, X_n][Y]$. Consider the Laurent ring $k[X_1, \ldots, X_n][Y, 1/Y]$ and the evaluation map

$$\begin{gathered}\epsilon : k[X_1, \ldots, X_n][Y] \to k[X_1, \ldots, X_n][Y, 1/Y] \\ Y \mapsto \frac{1}{Y}.\end{gathered}$$

In this new ring,

$$1 = \sum_{i=1}^{r} F_i(X_1, \ldots, X_n, \frac{1}{Y}) g_i(X_1, \ldots, X_n) + F(X_1, \ldots, X_n, \frac{1}{Y})(1 - h(X_1, \ldots, X_n)\frac{1}{Y}).$$

We may multiply both sides by Y^N for some large enough N such that

$$Y_N = \sum_{i=1}^{r} G_i(X_1, \ldots, X_n, Y) g_i(X_1, \ldots, X_n) + G(X_1, \ldots, X_n, Y)(Y - h(X_1, \ldots, X_n))$$

for some $G_i \in k[X_1, \ldots, X_n, Y]$.

Now consider the evaluation map

$$\begin{gathered}\eta : k[X_1, \ldots, X_n][Y] \to k[X_1, \ldots, X_n] \\ Y \mapsto h.\end{gathered}$$

Then the above becomes

$$\begin{aligned}h^N = \sum_{i=1}^{r} & G_i(X_1, \ldots, X_n, h(X_1, \ldots, X_n)) g_i(X_1, \ldots, X_n) \\ & + G(X_1, \ldots, X_n, h(X_1, \ldots, X_n))(0).\end{aligned}$$

Since $g_i \in \mathfrak{a}$, it follows that $h^N \in \mathfrak{a}$, so $h \in \mathfrak{a}$. □

Corollary 5.6. Let k be an algebraically closed field. Then there exist inverse bijections

$$\left\{\begin{array}{c}\text{algebraic subsets}\\ X\subset\mathbb{A}^n_k\end{array}\right\}\underset{\mathbf{V}}{\overset{\mathbf{I}}{\rightleftarrows}}\left\{\begin{array}{c}\text{radical ideals}\\ \mathfrak{a}\subset\Gamma(\mathbb{A}^n_k)\end{array}\right\}$$

Corollary 5.7. If $\mathfrak{a},\mathfrak{b}\subset k[X_1,\dots,X_n]$ are ideals, then $\mathbf{V}(\mathfrak{a})=\mathbf{V}(\mathfrak{b})$ if and only if $\sqrt{a}=\sqrt{b}$.

6 affine schemes: as spaces

Our goal will be to realize a commutative ring A as the "ring of functions" on some space (which will be $\mathrm{Spec}(A)$).

6.1 summary so far

Let k be an algebraically closed field.

1. Points $\underline{a}=(a_1,\dots,a_n)\in\mathbb{A}^n_k$ correspond naturally to maximal ideals $\mathfrak{m}_{\underline{a}}=(X_1-a_1,\dots,X_n-a_n)\subset\Gamma(\mathbb{A}^n)$.
2. A polynomial map $F=(F_1,\dots,F_n):\mathbb{A}^n\to\mathbb{A}^n$, where $F_i\in k[X_1,\dots,X_n]$, induces a k-algebra map

$$\begin{aligned}F^{\#}:\Gamma(\mathbb{A}^m)&\to\Gamma(\mathbb{A}^n)\\ Y_j&\mapsto F_j\end{aligned}$$

   ref

   ref

3. We can recover F from $F^{\#}$ in the following way: $F^{\#}$ induces a map

$$\begin{aligned}\tilde{F}:\mathrm{Spec}_m(k[X_1,\dots,X_n])&\to\mathrm{Spec}_m(k[Y_1,\dots,Y_m])\\ \mathfrak{m}&\mapsto(F^{\#})^{-1}(\mathfrak{m}),\end{aligned}$$

   where we then identity $\mathrm{Spec}_m(k[X_1,\dots,X_n])\cong\mathbb{A}^n$ and $\mathrm{Spec}_m(k[Y_1,\dots,Y_m])\cong\mathbb{A}^m$.

4. Let $\mathfrak{a}\subset A=k[X_1,\dots,X_n]$ be an ideal. Consider the bijection

$$\begin{aligned}\mathbb{A}^n&\leftrightarrow\mathrm{Spec}_m(k[X_1,\dots,X_n])\\ \underline{a}&\mapsto\mathfrak{m}_{\underline{a}}.\end{aligned}$$

   Then $\underline{a}\in\mathbf{V}(\mathfrak{a})$ if and only

$$\begin{aligned}\underline{a}\in\mathbf{V}(\mathfrak{a})\Leftrightarrow&\{\underline{a}\}\subset\mathbf{V}(\mathfrak{a})\\ \Leftrightarrow&\mathbf{I}(\{\underline{a}\})\supset\mathbf{I}(\mathbf{V}(\mathfrak{a}))\\ \Leftrightarrow&\mathfrak{m}_{\underline{a}}\supset\sqrt{\mathfrak{a}}\\ \Leftrightarrow&\mathfrak{m}_{\underline{a}}\supset\mathfrak{a}.\end{aligned}$$

6.2 Zariski topology

Definition 6.1. Let A be a ring. For a subset $E \subset A$, define

$$V(E) := \{\mathfrak{p} \in \operatorname{Spec}(A) : \mathfrak{p} \supset E\}.$$

Note $\mathfrak{p} \supset E$ iff $\mathfrak{p}$ contains the ideal generated by E, so we may as well consider E to be an ideal above.

6.2. The idea now is to view an element $f \in A$ as a "function" on $\operatorname{Spec}(A)$ with values in a field: the value of $f \in A$ at the point $\mathfrak{p} \in \operatorname{Spec}(A)$ is the image of f under the natural maps to the residue field:

$$A \xrightarrow{\pi} A/\mathfrak{p} \xrightarrow{i} \kappa(\mathfrak{p}) := \operatorname{Frac}(A/\mathfrak{p}).$$

This is a generalization of usual function evaluation: for $f \in \Gamma(\mathbb{A}^n)$, the value of f at $\underline{a}$ could be considered as the image of f under the map

$$k[X_1, \dots, X_n] \to k[X_1, \dots, X_n]/\mathfrak{m}_{\underline{a}} \to \operatorname{Frac}(k[X_1, \dots, X_n]/\mathfrak{m}_{\underline{a}}) = k$$
$$f \mapsto f(\bar{X}_1, \dots, \bar{X}_n) = f(a_1, \dots, a_n).$$

The simplification being that since $\mathfrak{m}_{\underline{a}}$ is maximal, we already have a field before we take the field of fractions (taking the field of fractions does nothing).

In this context, the notation in the above notation is justified: $V((f))$ consists of prime ideals containing (f), hence f will be killed in the quotient above, hence the value of f at those primes is 0. More generally, for a subset $E \subset A$, note

$$V(E) = \bigcap_{f \in E} V(f) = \bigcap_{f \in E} \{\mathfrak{p} \in \operatorname{Spec}(A) : f \in \mathfrak{p}\} = \{\mathfrak{p} \in \operatorname{Spec}(A) : E \supset \mathfrak{p}\}$$

and we recover the definition.

6.3. The sets $V(E)$ will be the closed sets in the topology we define on $\operatorname{Spec}(A)$. This topology will also be called the Zariski topology for the following reason: recall that $\underline{a} \in \mathbf{V}(\mathfrak{a})$ iff $\mathfrak{m}_{\underline{a}} \supset \mathfrak{a}$. Hence

$$V(A) \cap \operatorname{Spec}_m(\mathbb{A}^n) = \mathbf{V}(\mathfrak{a})$$

Hence the earlier Zariski topology is nothing but the subspace topology of the new Zariski topology on $\operatorname{Spec}(A)$, specifically the one on the subspace $\operatorname{Spec}_m(A) \cong \mathbb{A}^n$.

Proposition 6.4. Let A be a ring, let $X = \operatorname{Spec}(A)$.

1. (order reversing) If $E_1 \subset E_2 \subset A$, then $V(E_1) \supset V(E_2)$.
2. $V(\emptyset) = X$ and $V(A) = \emptyset$.
3. $V(E) = V\langle E \rangle$
4. For ideals $\mathfrak{a}, \mathfrak{b} \subset A$, we have $V(\mathfrak{a} \cap \mathfrak{b}) = V(\mathfrak{a}) \cup V(\mathfrak{b})$.
5. For ideals $\mathfrak{a}_\alpha \subset A$, we have $V(\sum_\alpha \mathfrak{a}_\alpha) = \bigcap_\alpha V(\mathfrak{a}_\alpha)$.

Definition 6.5. The *Zariski topology* on $X = \text{Spec}(A)$ is the topology whose closed sets are the sets $V(\mathfrak{a})$ for some ideal $\mathfrak{a} \subset A$.

Remark 6.6. Recall from () that points in $\mathbb{A}^n$ correspond to maximal ideals of A. The set of prime ideals include the maximal ideals; so this Zariski topology includes all the points of $\mathbb{A}^n$ but also certain "smeared out" points, e.g. varieties such as $\mathbf{V}(Y - X^2)$.

ref

Proposition 6.7. The Zariski open sets

$$D(f) = X - V(f) = \{\mathfrak{p} \in \text{Spec}(A) : f \notin \mathfrak{p}\},$$

called *distinguished open sets*, form a basis for the Zariski topology on X.

Proof. We want to show than an arbitrary open set $U \subset X$ is a union of distinguished open sets. Let $U = X - V(\mathfrak{a})$ for some $\mathfrak{a} \subset A$. Let $\{f_i\}_i$ be a set of generators of $\mathfrak{a}$ (perhaps it is the set of all elements in $\mathfrak{a}$). Then $\mathfrak{a} = \sum_i (f_i)$, implying

$$V(\mathfrak{a}) = V(\sum_i (f_i)) = \bigcap_i V(f_i),$$

so

$$U = X - V(\mathfrak{a}) = X - \bigcap_i V(f_i) = \bigcup_i (X - V(f_i)) = \bigcup_i D(f_i).$$

This shows what we want. □

Proposition 6.8. $D(fg) = D(f) \cap D(g)$.

Proof. HW. □

Proposition 6.9. $X = \text{Spec}(A)$ is quasicompact[4].

Proof. It suffices to show an open cover of X by basic open sets admits a finite subcover (since any open set is a union of basic open sets). Say $U = \{D(f_\alpha)\}_{\alpha \in \Lambda}$ covers X. Then

$$\emptyset = X - \bigcup_\alpha D(f_\alpha) = \bigcap_\alpha (X - D(f_\alpha)) = \bigcap_\alpha V(f_\alpha) = V(\sum_\alpha (f_\alpha)),$$

so $\sum_\alpha (f_\alpha) = A$. Thus there exist $\alpha_1, \dots, \alpha_n \in \Lambda$ and $c_1, \dots, c_n \in A$ such that

$$1 = c_1 f_{\alpha_1} + \cdots + c_n f_{\alpha_n}.$$

So $A = (f_{\alpha_1}) + \cdots + (f_{\alpha_n})$. So

$$\emptyset = V(A) = V(\sum_{i=1}^n (f_{\alpha_i})) = \bigcap_{i=1}^n V(f_{\alpha_i}).$$

[4] i.e. compact but not necessarily Hausdorff; apparently Bourbaki used "compact" to refer to compact Hausdorff spaces

So

$$X = X - \emptyset = X - \bigcap_{i=1}^{n} V(f_{\alpha_i}) = \bigcup_{i=1}^{n} (X - V(f_{\alpha_i})) = \bigcup_{i=1}^{n} D(f_{\alpha_i}).$$

This exhibits a finite subcover. □

Proposition 6.10. $X = \text{Spec}(A)$ is disconnected if and only if A admits a ring product decomposition $A \cong A_1 \times A_2$.

Proof. For the reverse direction, suppose $A = A_1 \times A_2$. By (), ref hw

$$\begin{aligned}\text{Spec}(A) =& \{\mathfrak{p}_1 \times A_2 : \mathfrak{p}_1 \in \text{Spec}(A_1)\} \sqcup \{A_1 \times \mathfrak{p}_2 : \mathfrak{p}_2 \in \text{Spec}(A_2)\} \\ =& V(0 \times A_2) \sqcup V(A_1 \times 0).\end{aligned}$$

This expresses X as the disjoint union of two nontrivial closed sets, hence X is disconnected.

For the forward direction, suppose $X = V(\mathfrak{a}) \sqcup V(\mathfrak{b})$ for some ideal $\mathfrak{a}, \mathfrak{b} \subset A$. Then

$$X = V(\mathfrak{a}) \cup V(\mathfrak{b}) = V(\mathfrak{a} \cap \mathfrak{b})$$

implying $\mathfrak{a} \cap \mathfrak{b} \subset \text{Nil}(A)$, since it lies inside every prime ideal and the nilradical can be characterized as the intersection of all prime ideals (). Also ref

$$\emptyset = V(\mathfrak{a}) \cap V(\mathfrak{b}) = V(\mathfrak{a} + \mathfrak{b}),$$

implying $\mathfrak{a} + \mathfrak{b} = A$. Hence there exists $a \in \mathfrak{a}$ and $b \in \mathfrak{b}$ such that $a + b = 1$. Pulling these two observations together, we can find a, b such that $a + b = 1$ and $(ab)^N = 0$ for some N.

We now claim $(a^N, b^N) = A$, where the notation denotes the ideal generated by the two elements. Suppose not. Then there exists a maximal ideal $\mathfrak{m} \supset (a^N, b^N)$. But $a^N \in \mathfrak{m}$ implies $a \in \mathfrak{m}$, and similarly if $b^N \in \mathfrak{m}$ then $b \in \mathfrak{m}$. But then $(a, b) = A \subset \mathfrak{m}$, which is a contradiction.

So there exists $c, d \in A$ such that $1 = ca^N + db^N$. Write $\alpha := ca^N$ and $\beta = db^N$ for convenience. Then

$$\alpha\beta = ca^N \cdot db^N = cd(ab)^N = 0.$$

Now

$$\alpha = \alpha \cdot 1 = \alpha(\alpha + \beta) = \alpha^2 + \alpha\beta = \alpha^2,$$

so α is idempotent. Similarly $\beta = \beta^2$. Hence α, β are a complete set of orthogonal idempotents, so by () $A \cong A_1 \times A_2 = A\alpha \times A\beta$. □ ref

6.3 upgraded Galois connection

6.11. () shows us how $V(-)$ extended our previous $\mathbf{V}(-)$. How should we extend $\mathbf{I}(-)$? For ref a subset $S \subset X = \text{Spec}(A)$, we want to think of this as the set of elements in A on which S vanishes. In the case where S is a single element:

$$I(\{\mathfrak{p}\}) = \{f \in A : f(\mathfrak{p}) = 0\}$$

$$= \{f \in A : f \in \mathfrak{p}\} = \mathfrak{p},$$

where we have used (). The natural way to extend this is

ref

$$\begin{aligned} I(S) =& \{f \in A : f(\mathfrak{p}) = 0 \text{ for all } \mathfrak{p} \in S\} \\ =& \bigcap_{\mathfrak{p}\in S} \{f : f(\mathfrak{p}) = 0\} = \bigcap_{\mathfrak{p}\in S} \mathfrak{p} \\ =& \bigcap S. \end{aligned}$$

This motivates the following:

Definition 6.12. For $S \subset X$, define (the ideal)

$$I(S) \coloneqq \bigcap_{\mathfrak{p}\in S} \mathfrak{p} = \bigcap S \subset A.$$

Corollary 6.13.

1. If $E \subset A$, then $V(E) \subset X$ is closed.
2. If $S \subset X$, then $I(S)$ is an intersection of prime ideals, hence radical.
3. I, V are order reversing.
4. IV and VI are inflationary.
5. $\mathrm{im}(V) = \{$closed subsets of $X\}$.
6. (formal Nullstellensatz) $\mathrm{im} I = \{$radical ideals of $A\}$.

Proof.

1. x
2. x
3. x
4. Note

$$\begin{aligned} I(V(\mathfrak{a})) =& I(\{\mathfrak{p} \in \mathrm{Spec}(A) : \mathfrak{p} \supset \mathfrak{a}\}) \\ =& \bigcap \{\mathfrak{p} \in \mathrm{Spec}(A) : \mathfrak{p} \supset \mathfrak{a}\} \\ =& \sqrt{\mathfrak{a}} \supset \mathfrak{a}. \end{aligned}$$

5. x
6. The forward inclusion follows from (2). For the reverse inclusion, suppose $\mathfrak{a} \subset A$ is radical. Then $\mathfrak{a} = \sqrt{\mathfrak{a}}$, hence by the proof of (4) $I(V(\mathfrak{a})) = \sqrt{\mathfrak{a}}$.

□

6.14. We thus have the following correspondences:

- Zariski closed subsets of Spec(A) and radical ideals of A
- irreducible closed subsets of Spec(A) and prime ideals of A
- closed points of Spec(A) and maximal ideals of A

6.4 Noetherian spaces

Definition 6.15. A space X is *Noetherian* if it satisfies the ascending chain condition (ACC) on open sets.

Remark 6.16. This is equivalent to satisfying the descending chain condition (DCC) on closed sets. We will often use this property instead, because the closed sets we work with are easier to describe than the open ones.

Proposition 6.17. If A is a Noetherian ring, then Spec(A) is a Noetherian space.

Proof. Let A be a Noetherian ring. Let $X_1 \supset X_2 \supset \cdots$ be a descending chain of closed suspaces of X. Then $I(X_1) \subset I(X_2) \subset \cdots$ is an ascending chain of ideals in A, hence stabilizes. So there exists N such that $I(X_N) = I(X_{N+1}) = \cdots$. Hence also $VI(X_N) = VI(X_{N+1}) = \cdots$. Thus $X_N = X_{N+1} = \cdots$, since VI is the identity on closed subsets. □

Proposition 6.18. Let X be a Noetherian space. Then

1. X is a finite union $X = X_1 \cup \cdots \cup X_n$ of irreducible closed subspaces.
2. If the above union (decomposition) is irredundant[5], then it is unique up to permutation.

Proof.

1. Let Σ denote the set of nonempty, closed subsets of X which are note a finite union of irreducible closed subsets. It suffices to show Σ is empty. Suppose otherwise. Then, since X is Noetherian, Σ has a minimal element X_M. By assumption X_M is not irreducible, hence can be written as $X_M = X_1 \sqcup X_2$ for some nontrival closed $X_1, X_2 \subset X_M$. Then $X_1, X_2 \notin \Sigma$ by minimality, hence are themselves both finite unions of closed irreducible subspaces. But then so is X_M, a contradiction.
2. Suppose $X = X_1 \cup \cdots \cup X_n$ and $X = Y_1 \cup \cdots \cup Y_m$ are both irredundant decompositions. Then for each i

$$X_i = (X_i \cap X) = X_i \cap (Y_1 \cup \cdots \cup Y_m) = (X_i \cap Y_1) \cup \cdots \cup (X_i \cap Y_m),$$

which expresses X_i as a finite union of closed sets. Since X_i is irreducible, it must be that $X_i = X_i \cap Y_j$ for some j, hence $X_i \subset Y_j$. We can thus define a function α such that $X_i \subset Y_{\alpha(i)}$ for all $i = 1, \ldots, n$. We can analagously get a function β such that $Y_j \subset X_{\beta(j)}$ for all $j = 1, \ldots, m$. Then $X_i \subset Y_{\alpha(i)} \subset X_{\beta(\alpha(i))}$, and by the irredundancy

[5] i.e. we can't remove any X_i, i.e. $X_i \not\subset X_j$ for any $i \neq j$

assumption it must be that $\beta \circ \alpha = 1$. Similarly $\alpha \circ \beta = 1$. Hence $m = n$, and $X_i = Y_j$ for all i and some $j = 1, \ldots, n$.

$\square$