

Problem Set 1

D. Zack Garza

Sunday 6th September, 2020

Source: Section 1 of Gathmann

1 Exercises

Exercise 1.1 (Gathmann 1.19).

Prove that every affine variety $X \subset \mathbb{A}^n/k$ consisting of only finitely many points can be written as the zero locus of n polynomials.

Hint: Use interpolation. It is useful to assume at first that all points in X have different x_1 -coordinates.

Solution:

Let $X = \{\mathbf{p}_1, \dots, \mathbf{p}_d\} = \{\mathbf{p}_j\}_{j=1}^d$, where each $\mathbf{p}_j \in \mathbb{A}^n$ can be written in coordinates

$$\mathbf{p}_j := [p_j^1, p_j^2, \dots, p_j^n].$$

Remark.

Proof idea: for some fixed k with $2 \leq k \leq n$, consider the pairs $(p_j^1, p_j^k) \in \mathbb{A}^2$. Letting j range over $1 \leq j \leq d$ yields d points of the form $(x, y) \in \mathbb{A}^2$, so construct an interpolating polynomial such that $f(x) = y$ for each tuple. Then $f(x) - y$ vanishes at every such tuple.

Doing this for each k (keeping the first coordinate always of the form p_j^1 and letting the second coordinate vary) yields $n - 1$ polynomials in $k[x_1, x_k] \subseteq k[x_1, \dots, x_n]$, then adding in the polynomial $p(x) = \prod_j (x - p_j^1)$ yields a system that vanishes precisely on $\{\mathbf{p}_j\}$.

Claim: Without loss of generality, we can assume all of the first components $\{p_j^1\}_{j=1}^d$ are distinct.

Todo: follows from "rotation of axes"?

We will use the following fact:

Theorem 1.1 (Lagrange).

Given a set of d points $\{(x_i, y_i)\}_{i=1}^d$ with all x_i distinct, there exists a unique polynomial of degree d in $f \in k[x]$ such that $f(x_i) = y_i$ for every i .

This can be explicitly given by

$$\tilde{f}(x) = \sum_{i=1}^d y_i \left(\prod_{\substack{0 \leq m \leq d \\ m \neq i}} \left(\frac{x - x_m}{x_i - x_m} \right) \right).$$

Equivalently, there is a polynomial f defined by $f(x_i) = \tilde{f}(x_i) - y_i$ of degree d whose roots are precisely the x_i .

Using this theorem, we define a system of n polynomials in the following way:

- Define $f_1 \in k[x_1] \subseteq k[x_1, \dots, x_n]$ by

$$f_1(x) = \prod_{i=1}^d (x - p_i^1).$$

Then the roots of f_1 are precisely the first components of the points p .

- Define $f_2 \in k[x_1, x_2] \subseteq k[x_1, \dots, x_n]$ by considering the ordered pairs

$$\{(x_1, x_2) = (p_j^1, p_j^2)\},$$

then taking the unique Lagrange interpolating polynomial \tilde{f}_2 satisfying $\tilde{f}_2(p_j^1) = p_j^2$ for all $1 \leq j \leq d$. Then set $f_2 := \tilde{f}_2(x_1) - x_2 \in k[x_1, x_2]$.

- Define $f_3 \in k[x_1, x_3] \subseteq k[x_1, \dots, x_n]$ by considering the ordered pairs

$$\{(x_1, x_3) = (p_j^1, p_j^3)\},$$

then taking the unique Lagrange interpolating polynomial \tilde{f}_3 satisfying $\tilde{f}_3(p_j^1) = p_j^3$ for all $1 \leq j \leq d$. Then set $f_3 := \tilde{f}_3(x_1) - x_3 \in k[x_1, x_3]$.

- ...

Continuing in this way up to $f_n \in k[x_1, x_n]$ yields a system of n polynomials.

Proposition 1.2.

$$V(f_1, \dots, f_n) = X.$$

Proof .

Claim: $X \subseteq V(f_i)$:

This is essentially by construction. Letting $p_j \in X$ be arbitrary, we find that

$$f_1(p_j) = \prod_{i=1}^d (p_j^1 - p_i^1) = (p_j^1 - p_j^1) \prod_{\substack{i \leq d \\ i \neq j}} (p_j^1 - p_i^1) = 0.$$

Similarly, for $2 \leq k \leq n$,

$$f_k(p_j) = \tilde{f}_k(p_j^1) - p_j^k = 0,$$

which follows from the fact that $\tilde{f}_k(p_j^1) = p_j^k$ for every k and every j by the construction of \tilde{f}_k .

Claim: $X^c \subseteq V(f_i)^c$:

This follows from the fact the polynomials f given by Lagrange interpolation are unique, and thus the roots of \tilde{f} are unique. But if some other point was in $V(f_i)$, then one of its coordinates would be another root of some \tilde{f} . ■

Exercise 1.2 (Gathmann 1.21).

Determine \sqrt{I} for

$$I := \langle x_1^3 - x_2^6, x_1x_2 - x_2^3 \rangle \trianglelefteq \mathbb{C}[x_1, x_2].$$

Solution:

For notational purposes, let \mathcal{I}, \mathcal{V} denote the maps in Hilbert's Nullstellensatz, we then have

$$(\mathcal{I} \circ \mathcal{V})(I) = \sqrt{I}.$$

So we consider $\mathcal{V}(I) \subseteq \mathbb{A}^2/\mathbb{C}$, the vanishing locus of these two polynomials, which yields the system

$$\begin{cases} x^3 - y^6 &= 0 \\ xy - y^3 &= 0. \end{cases}$$

In the second equation, we have $(x - y^2)y = 0$, and since $\mathbb{C}[x, y]$ is an integral domain, one term must be zero.

1. If $y = 0$, then $x^3 = 0 \implies x = 0$, and thus $(0, 0) \in \mathcal{V}(I)$, i.e. the origin is contained in this vanishing locus.
2. Otherwise, if $x - y^2 = 0$, then $x = y^2$, with no further conditions coming from the first equation.

Combining these conditions,

$$P := \{(t^2, t) \mid t \in \mathbb{C}\} \subset \mathcal{V}(I).$$

where $I = \langle x^3 - y^6, xy - y^3 \rangle$.

We have $P = \mathcal{V}(I)$, and so taking the ideal generated by P yields

$$(\mathcal{I} \circ \mathcal{V})(I) = \mathcal{I}(P) = \langle y - x^2 \rangle \in \mathbb{C}[x, y]$$

and thus $\sqrt{I} = \langle y - x^2 \rangle$.

Exercise 1.3 (Gathmann 1.22).

Let $X \subset \mathbb{A}^3/k$ be the union of the three coordinate axes. Compute generators for the ideal $I(X)$ and show that it can not be generated by fewer than 3 elements.

Solution:

Claim:

$$I(X) = \langle x_2x_3, x_1x_3, x_1x_2 \rangle.$$

We can write $X = X_1 \cup X_2 \cup X_3$, where

- The x_1 -axis is given by $X_1 := V(x_2x_3)$,
- The x_2 -axis is given by $X_2 := V(x_1x_3)$,
- The x_3 -axis is given by $X_3 := V(x_1x_2)$,

We also have, for example

$$I(V(x_2x_3)) = \sqrt{\langle x_2x_3 \rangle} = \langle x_2x_3 \rangle$$

by applying the Nullstellensatz and noting that (claim) $\langle x_2, x_3 \rangle$ is radical.

We then have

$$\begin{aligned} I(X) &= I(X_1 \cup X_2 \cup X_3) \\ &= I(X_1) \cap I(X_2) \cap I(X_3) \\ &= \sqrt{IV(x_2x_3) + IV(x_1x_3) + IV(x_1x_2)} \\ &= \sqrt{IV(x_2x_3, x_1x_3, x_1x_2)} && \text{since } \langle a \rangle + \langle b \rangle = \langle a, b \rangle \\ &= IV(x_2x_3, x_1x_3, x_1x_2) \\ &= \sqrt{\langle x_2x_3, x_1x_3, x_1x_2 \rangle} \\ &= \langle x_2x_3, x_1x_3, x_1x_2 \rangle, \end{aligned}$$

where in the last step we've used

Exercise 1.4 (Gathmann 1.23: Relative Nullstellensatz).

Let $Y \subset \mathbb{A}^n/k$ be an affine variety and define $A(Y)$ by the quotient

$$\pi : k[x_1, \dots, x_n] \longrightarrow A(Y) := k[x_1, \dots, x_n]/I(Y).$$

- a. Show that $V_Y(J) = V(\pi^{-1}(J))$ for every $J \trianglelefteq A(Y)$.
- b. Show that $\pi^{-1}(I_Y(X)) = I(X)$ for every affine subvariety $X \subseteq Y$.
- c. Using the fact that $I(V(J)) \subset \sqrt{J}$ for every $J \trianglelefteq k[x_1, \dots, x_n]$, deduce that $I_Y(V_Y(J)) \subset \sqrt{J}$ for every $J \trianglelefteq A(Y)$.

Conclude that there is an inclusion-reversing bijection

$$\left\{ \begin{array}{c} \text{Affine subvarieties} \\ \text{of } Y \end{array} \right\} \iff \left\{ \begin{array}{c} \text{Radical ideals} \\ \text{in } A(Y) \end{array} \right\}.$$

Exercise 1.5 (Extra).

Let $J \trianglelefteq k[x_1, \dots, x_n]$ be an ideal, and find a counterexample to $I(V(J)) = \sqrt{J}$ when k is not algebraically closed.

Solution:

Take $J = \langle x^2 + 1 \rangle \trianglelefteq \mathbb{R}[x]$, noting that J is nontrivial and proper but \mathbb{R} is not algebraically closed. Then $V(J) \subseteq \mathbb{R}$ is empty, and thus $I(V(J)) = I(\emptyset)$.

Claim: $I(V(J)) = \mathbb{R}[x]$.

Checking definitions, for any set $X \subset \mathbb{A}^n/k$ we have

$$I(X) = \left\{ f \in \mathbb{R}[x] \mid \forall x \in X, f(x) = 0 \right\}$$

and so we vacuously have

$$I(\emptyset) = \left\{ f \in \mathbb{R}[x] \mid \forall x \in \emptyset, f(x) = 0 \right\} = \{f \in \mathbb{R}[x]\} = \mathbb{R}[x].$$

Claim: $\sqrt{J} \neq \mathbb{R}[x]$.

This follows from the fact that maximal ideals are radical, and $\mathbb{R}[x]/J \cong \mathbb{C}$ being a field implies that J is maximal. In this case $\sqrt{J} = J \neq \mathbb{R}[x]$.

That maximal ideals are radical follows from the fact that if $J \trianglelefteq R$ is maximal, we have $J \subset \sqrt{J} \subset R$ which forces $\sqrt{J} = J$ or $\sqrt{J} = R$.

But if $\sqrt{J} = R$, then

$$1 \in \sqrt{J} \implies 1^n \in J \text{ for some } n \implies 1 \in J \implies J = R,$$

contradicting the assumption that J is maximal and thus proper by definition.