Chapter 1 - Algebraic sets

k = an algebraically closed field (e.g $\mathbb{C}$, $\overline{\mathbb{Q}}$, $\overline{\mathbb{F}_p}$, ...)

$\mathbb{A}^n = k^n$ = affine n-space.

Defn A (closed) algebraic set is a subset of $\mathbb{A}^n$ of the form

$$Z(S) = \left\{ x \in \mathbb{A}^n \;\middle|\; f(x) = 0 \;\; \forall f \in S \right\}$$

where S is a set of polynomials in $k[x_1, \ldots x_n]$.

Note: If $S = \{f_1, \ldots, f_r\}$, then

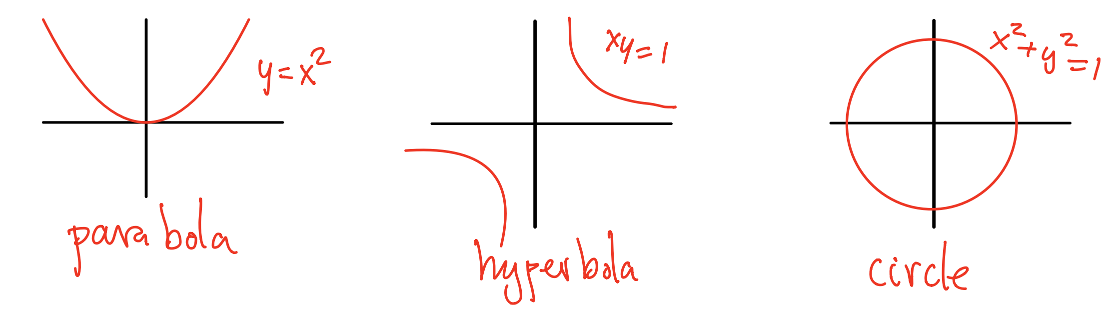
$$Z(S) = Z(I)$$ where $I = (f_1, \ldots, f_r)$ is the ideal generated by S.

ex $k[x]$ is a PID $\rightsquigarrow$ any ideal is of the form $I = (f(x))$

$\rightsquigarrow Z(I) = Z(f)$ = zeroes of $f(x)$

$\therefore$ closed algebraic subsets of $\mathbb{A}^1$ = finite subsets of $\mathbb{A}^1$.

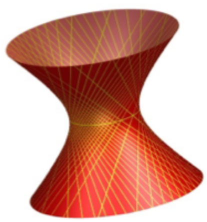
ex In $\mathbb{A}^2$, we have the conic sections



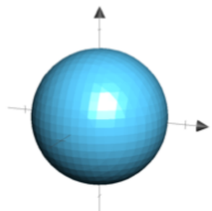
But also finite sets : $(a,b) \in \mathbb{A}^2 \leftrightarrow m = (x-a, y-b)$

union of r points in $\mathbb{A}^2 \leftrightarrow$ product $m_1 \cdots m_r \subset k[x,y]$

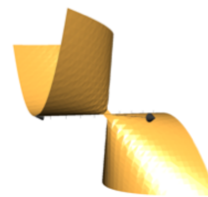
ex Plots of surfaces in $\mathbb{A}^3$



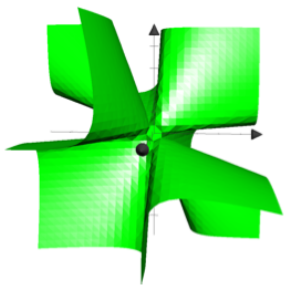
(a) $z - xy = 0$



(b) $x^2 + y^2 + z^2 = 1$



(c) $y^2 - xz = 0$



(a) $x^3 + y^3 + z^3 = 1$

(b) $(x + y + z)^3 - 3xyz = 0$

Here we only see the real points of $Z(I)$. With complex numbers, the solution sets are actually 4-dimensional (over $\mathbb{R}$).

Properties of $Z(I)$

(1) $I \subseteq J \Rightarrow Z(J) \subseteq Z(I)$ Z reverses inclusions

(2) $Z(I+J) = Z(I) \cap Z(J)$ intersection

(3) $Z(IJ) = Z(I \cap J) = Z(I) \cup Z(J)$ union

(4) $Z(I) = Z(\sqrt{I})$ $\sqrt{I} = \{ f \in A \mid f^N \in I \text{ for some } N \}$

taking $\sqrt{\ }$ does not change $Z(I)$.

(1) $x \in Z(J) \Rightarrow f(x) = 0 \ \forall f \in J \Rightarrow f(x) = 0 \ \forall f \in I$

$= x \in Z(I)$.

(2) $x \in Z(I+J) \Leftrightarrow f(x) = 0$ for $f \in I + J$

$\Leftrightarrow f(x) = 0$ for $f \in I$ and $f \in J$

$\Leftrightarrow x \in Z(I) \cap Z(J)$

(3) IJ is generated by products $f \cdot g$ $\quad f \in I,\ g \in J$

If $x \in Z(IJ)$ then $f(x) \cdot g(x) = 0 \Rightarrow$ either $f(x) = 0 \Rightarrow x \in Z(I) \cup Z(J)$
or $g(x) = 0$

Conversely, if $x \in Z(I) \cup Z(J)$ then $f(x) g(x) = 0 \Rightarrow x \in Z(IJ)$ also

and Z reverses inclusions.

(4) $Z(\sqrt{I}) \subseteq Z(I)$ since $I \subseteq \sqrt{I}$

If $x \in Z(I)$ and $f \in \sqrt{I}$, then $f^N \in I$

so $f(x)^N = 0 \Rightarrow f(x) = 0 \Rightarrow x \in Z(\sqrt{I})$ also.

The ideal of functions vanishing on a set

Given a subset $X \subseteq \mathbb{A}^n$, we also get an <u>ideal</u> $I(X)$ given by

$$I(X) = \{ f \in k[x_1 .. x_n] \mid f(x) = 0 \ \forall x \in X \}.$$

Properties of $I(X)$

(1) $X \subseteq Y \rightsquigarrow I(Y) \subseteq I(X)$ — I reverses inclusions

(2) $I \subseteq I(Z(I))$ $\quad (f \in I \Rightarrow f(x) = 0 \quad \forall x \in Z(I))$

— this is a tautological statement

(3) $Z(I(X)) = X$ for $X = Z(\mathfrak{a})$ for some ideal $\mathfrak{a}$.

not true in general: $X = \{1, 2, 3, \dots\} \subseteq \mathbb{A}^1 \Rightarrow I(X) = (0)$

$\supseteq$: $\mathfrak{a} \subseteq I(X)$

$\Rightarrow Z(\mathfrak{a}) \supseteq Z(I(X))$

$\Rightarrow X \supseteq Z(I(X))$

$\subseteq$: $X \subseteq Z(I(X))$ holds automatically

$x \in X \Rightarrow f(x) = 0$ for all $f \in I(X)$ — polynomials vanishing on X

$\Rightarrow x \in Z(I(X))$.

The coordinate ring of X

If $X \subseteq \mathbb{A}^n$ is an algebraic set, we define

$$A(X) = k[x_1 \dots x_n] / I(X)$$

Intuition:

We think of polynomials in $k[x_1, \dots, x_n]$ as <u>functions</u> $\mathbb{A}^n \to k$

$f, g \in k[x_1, \dots, x_n]$ restrict to the same function $X \longrightarrow k$

$$\iff f - g \in I(X).$$

$\therefore$ Elements of $A(X)$ give the polynomial functions $X \to k$.

Hilbert's Nullstellensatz

Assume k is an algebraically closed field, and that $\mathfrak{a} \subseteq k[x_1, \dots, x_n]$ is an ideal. Then

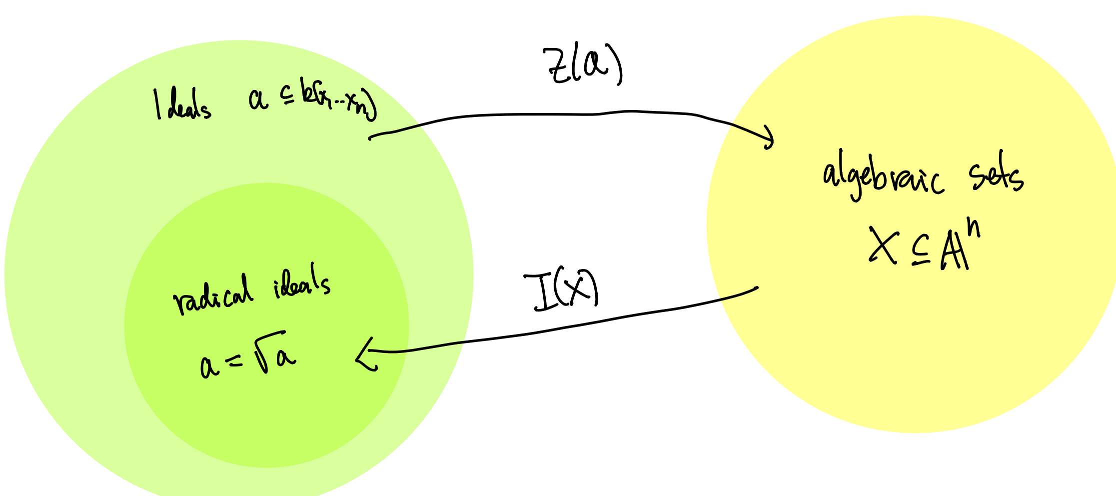
$$I(Z(\mathfrak{a})) = \sqrt{\mathfrak{a}}.$$ extremely important!

Note: this fails over other fields e.g $k = \mathbb{R}$:
$\mathfrak{a} = (x^2+1) \subseteq \mathbb{R}[x]$ has $Z(\mathfrak{a}) = \emptyset$.

$X \mapsto I(X)$ and $I \mapsto Z(I)$ give mutually inverse mappings

$$\left\{ \begin{array}{c} \text{algebraic sets} \\ \text{of } \mathbb{A}^n \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{radical ideals} \\ \text{of } k[x_1 \dots x_n] \end{array} \right\}$$

This bijection reverses inclusions: $\mathfrak{a} \subseteq \mathfrak{b} \Rightarrow Z(\mathfrak{b}) \subseteq Z(\mathfrak{a})$
$X \subseteq Y \Rightarrow I(Y) \subseteq I(X)$.



Other versions of the Nullstellensatz

Note: $I(\emptyset) = (1)$

If a is a proper ideal then $\sqrt{a} \neq (1)$ so Hilbert's Nullstellensatz says that $Z(a) \neq \emptyset$.

Weak Nullstellensatz (WN)

$k = \bar{k}$

again this fails over $\mathbb{R}[x]$ for instance.

$a \neq (1) \implies Z(a)$ is non-empty.

Since any ideal is contained in a maximal ideal, this follows from:

Weak Nullstellensatz II (WN2)

$k = \bar{k}$

The maximal ideals in $k[x_1, \ldots, x_n]$ are exactly the ideals

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

for $a_1, \ldots, a_n \in k$.

It's clear that these are maximal: $\dfrac{k[x_1 \ldots x_n]}{(x_1 - a_1, \ldots, x_n - a_n)} \cong k$ is a field

If $m \subseteq k[x_1 \ldots x_n]$ is maximal, then $Z(m) \neq \emptyset$ by WN

so $\exists\, (a_1, \ldots, a_n) \in Z(m) \implies (x_1 - a_1, \ldots, x_n - a_n) \subseteq I(Z(m)) = m$

but $(x_1 - a_1, \ldots, x_n - a_n)$ is maximal $\implies m = (x_1 - a_1, \ldots, x_n - a_n)$.

So in fact $WN \iff WN2$.

WN $\Rightarrow$ Nullstellensatz

introducing $\mathfrak{b}$ is known as the "Rabinowitsch trick"

$\mathfrak{a} \subseteq k[x_1, .., x_n]$ a proper ideal

$I(Z(\mathfrak{a})) \supseteq \sqrt{\mathfrak{a}}$ ok

$I(Z(\mathfrak{a})) \subseteq \sqrt{\mathfrak{a}}$:

Pick $g \in I(Z(\mathfrak{a}))$ and consider the ideal

$$\mathfrak{b} = \mathfrak{a} \cdot k[x_1, .., x_{n+1}] + (1 - x_{n+1} g) \subseteq k[x_1 \dots x_{n+1}]$$

$$\rightsquigarrow \quad Z(\mathfrak{b}) = \pi^{-1}(Z(\mathfrak{a})) \cap Z(1 - x_{n+1} g)$$

$$\begin{array}{ccc} (x_1 .. x_{n+1}) & & \mathbb{A}^{n+1} \\ \downarrow & & \downarrow \pi \\ (x_1 .. x_n) & & \mathbb{A}^n \end{array}$$

projection from the point $(0, .., 0, 1)$.

$Z(\mathfrak{b})$ must be empty, since $g \neq 0$ on $Z(1 - x_{n+1} g)$.

$\rightsquigarrow \quad 1 \in \mathfrak{b}$ by Weak Nullstellensatz

$\rightsquigarrow \exists$ relation of the form $\quad f_i \in \mathfrak{a}$

$$1 = \sum f_i (x_1 .. x_n) h_i (x_1 .. x_{n+1}) + h \cdot (1 - x_{n+1} g)$$

Set $x_{n+1} = 1/g$ and multiply by g^N for $N \gg 0$.

$$\rightsquigarrow \quad g^N = \sum f(x_1 .. x_n) H_i (x_1 .. x_n) \quad \text{in } k[x_1 .. x_n]$$

polynomials in $k[x_1 .. x_n]$

$$\rightsquigarrow \quad g \in \sqrt{\mathfrak{a}}.$$

Weak Nullstellensatz III (WN3)

k a field (not assumed to be alg. closed)

$m \subset k[x_1, \dots, x_n]$ maximal ideal

$\longrightarrow$ $k[x_1, \dots, x_n]/m$ is a <u>finite</u> field extension of k.

$L \supset K$ finite extension

$\Rightarrow L \supset K$ <u>algebraic</u> extension

$\Rightarrow L = K$ if $K = \bar{K}$.

WN3 $\Rightarrow$ WN2

Since $k = \bar{k}$ in WN2 we must have $k[x_1, \dots, x_n]/m \xrightarrow{\sim} k$.

Let $a_i \in k$ be the image of x_i under this isomorphism

$\Rightarrow$ $(x - a_1, \dots, x_n - a_n) \subseteq \ker\left(k[x_1 \dots x_n] \to k[x_1 \dots x_n]/m \to k \right) = m$

$\Rightarrow$ $m = (x - a_1, \dots, x_n - a_n)$ by maximality $\square$

Proof of WN3

Lemma $k \subset K$ finitely generated field extension which is not finite

$a_1, \dots, a_r \in K \Rightarrow k[a_1, \dots, a_n] \neq K$.

Case I $k \subset K$ has transcendence degree 1

$\longrightarrow \exists\, x \in K$ s.t $k(x) \subseteq K$ is finite

Let $\{e_0, \dots, e_n\}$ be a basis for K as a $k(x)$-vector space with $e_0 = 1$

$$e_i e_j = \sum c_{ijk} e_k \quad \text{for some } c_{ijk} \in k(x)$$

$s :=$ common denominator of all the $c_{ijk} \in k(x)$

$\longrightarrow \quad A = \bigoplus_i k[x]_s e_i \subset K$ subalgebra which is free over $k[x]_s$

Express $a_1, \dots, a_r$ in the basis $\{e_i\}$

$$a_j = \sum d_{ij} e_i \qquad d_{ij} \in k(x)$$

$t :=$ common denominator of the d_{ij}'s

$\Rightarrow \quad k[a_1,\dots,a_r] \subseteq A_t \subsetneq K$

If $u \in k[x]$ irreducible which is not a factor in s or t $\rightsquigarrow$ $u^{-1} \notin A_t$ but clearly $u^{-1} \in K$.

If the transcendence degree is > 1, let $k' \subseteq K$ be a field over which K has transcendence degree 1.

$\rightarrow \quad K \neq k'[a_1,\dots,a_r]$ and hence $K \neq k[a_1,\dots a_r]$

$\square$

This finishes the proof of the implications

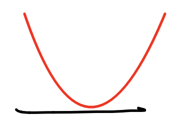
WN3 $\Rightarrow$ WN2 $\Leftrightarrow$ WN $\Rightarrow$ Nullstellensatz

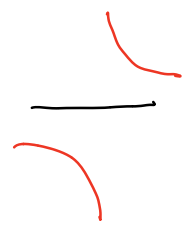
Examples

1. Conics in $\mathbb{A}^2$

$$X = Z(q) \quad \text{where} \quad q = a_0 x^2 + a_1 xy + a_2 y^2 + b_0 x + b_1 y + c$$

After a linear change of coordinates, we have two cases:

(i) $q = y - x^2$ (parabola) 

(ii) $q = xy - 1$ (hyperbola) 

We need $k = \bar{k}$ for this. For instance, we may write

$$x^2 + y^2 = (x+iy)(x-iy) = uv$$

2 The twisted cubic curve

There is a map $\mathbb{A}^1 \xrightarrow{\phi} \mathbb{A}^3$

$t \longmapsto (t, t^2, t^3)$

$C =$ image of ϕ.

Claim $I(C) = (y - x^2,\ z - x^3) =: \mathfrak{a}$

Pick $f \in k[x, y, z]$, then we can write

$$f(x, y, z) = g(x) + h(x, y, z)$$ (using $y - x^3$ and $z - x^3$ to eliminate y and z)

with $h \in \mathfrak{a}$

If $f \in I(C)$, then $f(t, t^2, t^3) = 0$ (the zero polynomial in t)

$0 = f(t, t^2, t^3) = g(t) + 0$

$\Rightarrow$ $g(t)$ is the zero polynomial

$\Rightarrow$ $f \in \mathfrak{a}$

$\Rightarrow$ Claim ok.

Note that $I(C)$ is prime: It is the kernel of the surjective map

$$\begin{aligned} k[x,y,z] &\longrightarrow k[t] \\ x &\longmapsto t \\ y &\longmapsto t^2 \\ z &\longmapsto t^3 \end{aligned}$$

and $k[t]$ is an integral domain.

Also, C is not contained in a plane in $\mathbb{A}^3$: there are no linear forms in $I(X)$ (this is probably the origin of the adjective "twisted")

$\square$