Cor 2.3

a) The intersection of arbitrarily many alg. subsets of K^n is an algebraic subset of K^n.

b) The union of two (fin. many) algebraic subsets is an algebraic subset.

c) K^n is alg. subset

d) $\emptyset$ is alg. subset

Hences, the algebraic subsets are the closed sets of a topology on K^n, which is called the Zariski topology.

Rmk We've shown that any one-point set is Zariski closed. Hence, every finite subset of K^n is Zariski closed.

Lemma 2.4 If $K = \mathbb{R}$ or $\mathbb{C}$ and $X \subseteq K^n$ is Zariski closed, then $X \subseteq K^n$ is closed w.r.t. the usual (Euclidean) topology on K^n.

Pf For any $f \in K[x_1, \dots, x_n]$, the set $V(f)$ of zeros of f is closed w.r.t. the usual topology, because $f : K^n \to K$ is continuous w.r.t. the usual topology and $\{0\} \subseteq K$ is closed.

$$\Rightarrow V(I) = \bigcap_{f \in I} \underbrace{V(f)}_{\text{closed}} \text{ is closed for any } I.$$

$\square$

Thm 2.5 The algebraic subsets of K (so $n = 1$) are: K and the finite subsets of K.

Pf Consider any ideal I of $K[X]$.

The ring $K[X]$ is a principal ideal domain (in fact a unique factorization domain) because you can perform the Euclidean algorithm in $K[X]$.

$\Rightarrow I = (f)$ for some $f \in K[X]$.

<u>Case 1: $f = 0$</u> (constant zero polynomial)

$\Rightarrow V(I) = V(0) = K$

<u>Case 2: $f \neq 0$</u>

$\Rightarrow$ f has only finitely many roots.

$\square$

<u>Cor</u> The Zariski topology on K is the cofinite topology.

<u>Eg of Lemma 2.4</u>

$K = \mathbb{R}$, $n = 1$

Zariski closed: $\underbrace{\mathbb{R}, \text{ fin. subsets}}_{\text{closed w.r.t. usual topology.}}$

<u>Warning</u> The Zariski topology on K^n is <u>not</u> the product topology arising from the product topology on K!

2.2. Hilbert Basis Theorem

Goal: Every alg. set is defined by <u>finitely many</u> polynomial equations.

<u>Convention</u> Rings are commutative and have a mult. unit 1.

<u>Def</u> A ring R is <u>noetherian</u> if every ideal I of R is generated by finitely many elements.

<u>Ex</u> Any principal ideal domain (e.g. any field) is noetherian.

<u>Lemma 2.6</u> R is noetherian if and only if there is no chain of ideals

$$I_1 \subsetneqq I_2 \subsetneqq I_3 \subsetneqq \cdots$$

<u>Pf</u> "$\Rightarrow$" $I := \bigcup_{r \geq 1} I_r$ is an ideal of R

Let $I = (f_1, \dots, f_m)$.

Each f_i lies in some I_r

$\Rightarrow I \subseteq I_r$ for some r

$\Rightarrow I_r = I_{r+1} = \cdots$

"$\Leftarrow$" Assume I isn't finitely generated.

$\Rightarrow$ We can inductively construct

$$0 \subsetneq (f_1) \subsetneq (f_1, f_2) \subsetneq (f_1, f_2, f_3) \subsetneq \cdots$$

by taking any $f_r \in I \setminus (f_1, \dots, f_{r-1})$.

exists because I isn't finitely generated

$\square$

Thm 2.7 (Hilbert's Basis Theorem)

If R is noetherian, then $R[x]$ is noetherian.

By induction:

Cor 2.8

If R is noetherian, then $R[x_1, \dots, x_n]$ is noetherian.

Cor 2.9 Any alg. subset $X \subseteq K^n$ is defined by finitely many polynomial equations: $X = V(\{f_1, \dots, f_r\})$.

Pf of Thm 2.7

Assume $I \subseteq R[X]$ isn't finitely generated.

We inductively construct

$$0 \subsetneq (f_1) \subsetneq (f_1, f_2) \subsetneq \cdots$$

by taking $f_r \in I \setminus (f_1, \ldots, f_{r-1})$ of minimum degree.

Let $d_r := \deg(f_r)$.

$$\Rightarrow d_1 \leq d_2 \leq \cdots$$

The <u>leading coefficient</u> of a nonzero polynomial $a_n X^n + \ldots + a_0$ of degree n is $a_n \; (\neq 0)$.

Let $b_r :=$ leading coefficient of f_r.

We get a chain of ideals of R:

$$0 \subseteq (b_1) \subseteq (b_1, b_2) \subseteq \cdots$$

Since R is noetherian, we have equality somewhere:

$$(b_1, \ldots, b_r) = (b_1, \ldots, b_{r+1})$$

$$\Rightarrow b_{r+1} \in (b_1, \ldots, b_r)$$

$\rightsquigarrow$ Write $b_{r+1} = b_1 c_1 + \ldots + b_r c_r$ with $c_1, \ldots, c_r \in R$.

$$\Rightarrow g(X) := \underbrace{f_{r+1}(X)}_{\substack{\text{degree}=d_{r+1} \\ \text{l.c.}=b_{r+1} \\ \notin (f_1,\dots,f_r) \\ \in I}} - \sum_{i=1}^{r} \underbrace{f_i(X)\cdot c_i \cdot X^{d_{r+1}-d_i}}_{\substack{\text{degree}=d_i+d_{r+1}-d_i \\ =d_{r+1} \\ \text{l.c.}=b_i\cdot c_i \\ \in (f_1,\dots,f_r) \\ \in I}}$$

has degree $\deg(g) < d_{r+1} = \deg(f_{r+1})$

But $g(X) \in I \setminus (f_1, \dots, f_r)$, contradicting the assumption that f_{r+1} has minimum degree among the elements of $I \setminus (f_1, \dots, f_r)$. $\square$

Warning ~~For~~ every $n \geq 1$, there are ideals of $K\langle X, Y\rangle$ that aren't generated by n elements!

2.3. Vanishing ideals

$$\{\text{ideal } J \subseteq K[x_1, \dots, x_n]\} \underset{I}{\overset{V}{\rightleftarrows}} \{\text{(alg.) subset } X \subseteq K^n\}$$

<u>Def</u> The <u>vanishing ideal</u> of a set $X \subseteq K^n$ is the set

$$I(X) = \{f \in K[x_1, \dots, x_n] \mid \forall p \in X : f(p) = 0\}$$

of polynomials that vanish everywhere on X.

<u>Rmk</u> $I(X)$ is an ideal of $K[x_1, \dots, x_n]$.

<u>Ex</u> If $X = \{a_1, \dots, a_r\} \subseteq K$ (set consisting of r distinct points), then $I(X) \subseteq K[x]$ is generated by $f(x) = (x - a_1) \cdots (x - a_r)$.

<u>Ex</u> If $X \subseteq K$ consists of infinitely many points, then $I(X) = 0$.

<u>Rmk</u> If $X \subseteq X'$, then $I(X) \supseteq I(X')$.

<u>Rmk</u> $I(V(J)) \supseteq J$

<u>Rmk</u> $V(I(X)) \supseteq X$

Rmk $V(I(X)) = X$ if and only if X is algebraic.

2.4. Hilbert's Nullstellensatz

Given an ideal $J \subseteq k[x_1, \dots, x_n]$, what is $I(V(J))$?

Ex $J = (x^2(x-1)(x-2)^3) \subseteq \mathbb{R}[x]$

$\Rightarrow V(J) = \{0, 1, 2\}$

$\Rightarrow I(V(J)) = (x(x-1)(x-2)) \subseteq \mathbb{R}[x]$.

Note If $f^n \in J$ for some $n \geq 1$, then $f \in I(V(J))$.

Pf If $P \in V(J)$, then $f(P)^n = 0$.

$\Rightarrow f(P) = 0$.

$\Rightarrow f \in I(V(J))$. $\square$

Def The <u>radical</u> of an ideal I of any ring R is the set

$$\mathrm{Rad}(I) = \sqrt{I} := \{ f \in R \mid f^n \in I \text{ for some } n \geq 1 \}.$$

Lemma 2.10 $\sqrt{I}$ is an ideal.

Pf
- Let $f, g \in \sqrt{I}$.

$\Rightarrow f^n \in I,\ g^m \in I$ for some $n, m \geq 1$.

$$\Rightarrow (f+g)^{n+m} = \underbrace{\sum_{\substack{i,j \geq 0 \\ i+j = n+m}} \binom{n+m}{i} \underbrace{\underbrace{f^i}_{\substack{\in I \\ \text{for } i \geq n}} \underbrace{g^j}_{\substack{\in I \\ \text{for } j \geq m}}}_{\substack{\in I \\ \text{always}}}}_{\in I}$$

$\Rightarrow f+g \in \sqrt{I}$.

- Let $f \in \sqrt{I}$, $a \in R$.

$\Rightarrow f^n \in I$ for some $n \geq 1$.

$\Rightarrow (af)^n = a^n f^n \in I$

$\Rightarrow af \in \sqrt{I}$.

- Clearly, $0 \in \sqrt{I}$. $\square$

Rmk $\sqrt{\sqrt{I}} = \sqrt{I}$.

Def An ideal I is a radical ideal if $\sqrt{I} = I$.

Rmk $I \subseteq R$ is a radical ideal if and only if $I = \sqrt{J}$ for some ideal $J \subseteq R$.

Rmk If R is a unique factorization domain and we have factorization

$$f = u \cdot g_1^{e_1} \cdots g_r^{e_r},$$

then

$$\sqrt{(f)} = (g_1 \cdots g_r).$$