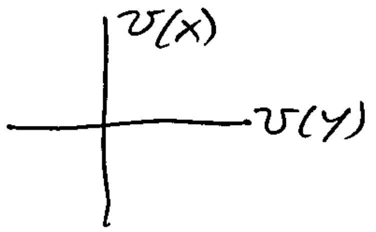
Thm 5.4 Let $V \subseteq k^n$ be algebraic. Then:

a) $V = V_1 \cup \dots \cup V_m$ for some irreducible sets $V_1, \dots, V_m \subseteq V$ with $V_i \nsubseteq V_j$ for all $i \neq j$.

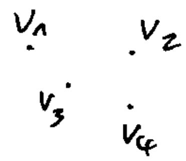
b) This decomposition is unique. The sets $V_1, \dots, V_m$ are called the irreducible components of V.

c) Any irreducible subset W of V is contained in some V_i.

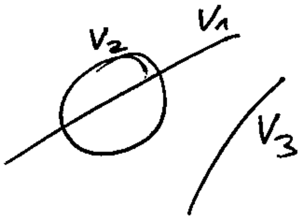
Ex $\mathcal{V}(X)$ and $\mathcal{V}(Y)$ are the irreducible components of $\mathcal{V}(XY)$.



Ex If V is a finite set, its irreducible components are its one-point subsets.



Ex



Pf a) Idea: Keep splitting V into smaller alg. sets until ending up with irreducible sets.

Why does this process terminate?

By Hilbert's Basis Theorem, there is no chain of ideals $I_1 \subsetneq I_2 \subsetneq \dots$ of $K[x_1, \dots, x_n]$.

$\Rightarrow$ There is no chain of alg. subsets $W_1 \supsetneq W_2 \supsetneq \dots$ of K^n. (I)

Formalistic proof: If some V is bad (= can't be ~~decomposed into~~ written as the union of finitely many irreducible sets), then (by (I)) there is an inclusion-minimal bad set V (such that no alg. $W \subsetneq V$ is bad).

V is reducible, so write $V = A \cup B$ with $A, B \subsetneq V$.

Both A and B can't be bad, so they're the union of finitely many irreducible sets.

$\Rightarrow V$ is! $\Rightarrow V$ isn't bad $\lightning$

c) $W = \bigcup_{i=1}^{n} \underbrace{(V_i \cap W)}_{\text{algebraic}}$

$\underset{W \text{ irreducible}}{\Longrightarrow}$ $W = V_i \cap W$ for some i

$\Longrightarrow$ $W \subseteq V_i$ — " —

d) Let $V = V_1 \cup \ldots \cup V_m = W_1 \cup \ldots \cup W_l$ as above.

Say V_i doesn't occur among $W_1, \ldots, W_l$.

$\left.\begin{array}{l} \text{By c), } V_i \subseteq W_j \text{ for some } j. \\ \text{By c), } W_j \subseteq V_k \text{ for some } k. \end{array}\right\} \Longrightarrow V_i \subseteq W_j \subseteq V_k$

$\Longrightarrow i = k \Longrightarrow V_i \subseteq W_j \subseteq V_i \Rightarrow V_i = W_j$ ↯ $\square$

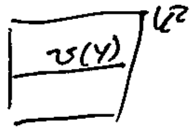
6. Coordinate rings

<u>Def</u> The <u>coordinate ring</u> of an algebraic subset V of K^n is $\Gamma(V) := K[X_1, \dots, X_n] / \mathcal{J}(V)$.

<u>Ex</u> $\Gamma(K^n) = K[X_1, \dots, X_n]$

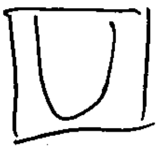
<u>Ex</u> $\Gamma(\underbrace{\mathcal{V}(Y)}_{\subseteq K^2}) = K[X,Y]/(Y) \cong K[X]$

$$\begin{aligned} X &\mapsto X \\ Y &\mapsto 0 \end{aligned}$$



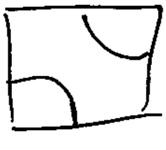
<u>Ex</u> $\Gamma(\mathcal{V}(X^2 - Y)) = K[X,Y]/(X^2 - Y) \cong K[X]$

$$\begin{aligned} X &\mapsto X \\ Y \ (= X^2) &\mapsto X^2 \end{aligned}$$



<u>Ex</u> $\Gamma(\mathcal{V}(XY - 1)) = K[X,Y]/(XY-1) \cong K[X, \frac{1}{X}]$

$$\begin{aligned} X &\mapsto X \\ Y &\mapsto \tfrac{1}{X} \end{aligned}$$



$K[X, \frac{1}{X}] = \{ a_r X^r + a_{r+1} X^{r+1} + \dots + a_s X^s \mid r, s \in \mathbb{Z}, \ a_r, \dots, a_s \in K \}$

is called the <u>ring of Laurent polynomials</u> in X.

<u>Warning</u>: $\frac{1}{X+1} \in K(X)$, but $\frac{1}{X+1} \notin K[X, \frac{1}{X}]$.

Ex $\Gamma(\{(a_1,\dots,a_n)\}) = K[X_1,\dots,X_n]/(X_1-a_1,\dots,X_n-a_n) \cong K$

Ex $\Gamma(\emptyset) = K[X_1,\dots,X_n]/K[X_1,\dots,X_n] = 0$

(the zero ring)

Ex Assume $K=\mathbb{C}$ so that X^2+Y^2-1 is irreducible.

$\Gamma(V(X^2+Y^2-1)) = K[X,Y]/(X^2+Y^2-1) \cong K[X][\sqrt{1-X^2}]$.

$X \mapsto X$
$Y \mapsto \sqrt{1-X^2}$

Thm 6.1 $\Gamma(V)$ is the ring of maps $f: V \to K$ that are described by a polynomial:

$$\Gamma(V) = \{ f: V \to K \mid \exists g \in K[X_1,\dots,X_n] : \underbrace{\forall P \in V : f(P)=g(P)}_{\text{"}f=g|_V\text{"}} \}.$$

Pf Two polynomials $g_1, g_2 \in K[X_1,\dots,X_n]$ correspond to the same function $V \to K$ if and only if $g_1 - g_2 \in I(V)$. (equivalently: $g_1 \equiv g_2 \bmod I(V)$). $\square$

Ex The i-th coordinate function $V \overset{\subseteq K^n}{\longrightarrow} K$, $(a_1,\dots,a_n) \mapsto a_i$ lies in $\Gamma(V)$.

Ex The function $\mathbb{C} \to \mathbb{C}$, $a \mapsto \exp(a)$ doesn't lie in $\Gamma(V)$ because on $\mathbb{R}$ it grows faster than any polynomial.

Rmk If $V \subseteq W$, we get a surjective ring hom.

$$\Gamma(W) \longrightarrow \Gamma(V)$$
$$f \longmapsto f|_V$$
$$f \bmod \mathcal{I}(W) \longmapsto f \bmod \mathcal{I}(V) \qquad (\mathcal{I}(V) \supseteq \mathcal{I}(W))$$

Rmk a) $\Gamma(V)$ is a reduced ring: for any $f \in \Gamma(V)$: if $f^n = 0$ for some $n \geq 1$, then $f = 0$.

b) V is irreducible if and only if $\Gamma(V)$ is an integral domain.

c) $|V| = 1$ if and only if $\Gamma(V)$ is a field if and only if $\Gamma(V) = K$.

Def The vanishing locus of an ideal $I \subseteq \Gamma(V)$ is $\mathcal{V}_V(I) := \{P \in V \mid \forall f \in I : f(P) = 0\}$.

The vanishing ideal of a subset $W \subseteq V$ is $\mathcal{I}_V(W) := \{f \in \Gamma(V) \mid \forall P \in W : f(P) = 0\}$.

Rmk Ideals I of $\Gamma(V) = K[X_1, \ldots, X_n]/\mathcal{I}(V)$ correspond to ideals I' of $K[X_1, \ldots, X_n]$ containing $\mathcal{I}(V)$.

<u>Rmk</u> We obtain maps

$$\left\{\begin{array}{c}\text{subset}\\ V\subseteq W\end{array}\right\} \underset{\mathcal{V}_V}{\overset{\mathcal{I}_V}{\rightleftarrows}} \left\{\begin{array}{c}\text{ideal}\\ I\subseteq\Gamma(V)\end{array}\right\}$$

$$\mathcal{V}_V(\mathcal{I}_V(W)) = \overline{W}$$

$$\mathcal{I}_V(\mathcal{V}_V(I)) = \sqrt{I}$$

We obtain bijections

$$\left\{\begin{array}{c}\text{alg.}\\ \text{subset}\\ W\subseteq V\end{array}\right\} \rightleftarrows \left\{\begin{array}{c}\text{radical}\\ \text{ideal}\\ I\subseteq\Gamma(V)\end{array}\right\}$$

$$\Gamma(W) = \Gamma(V)/I$$

$$\left\{\begin{array}{c}\text{irred.}\\ \text{alg.}\\ \text{subset}\\ W\subseteq V\end{array}\right\} \rightleftarrows \left\{\begin{array}{c}\text{prime}\\ \text{ideal}\\ I\subseteq\Gamma(V)\end{array}\right\}$$

$$\left\{\begin{array}{c}\text{one-point}\\ \text{subset}\\ W\subseteq V\end{array}\right\} \rightleftarrows \left\{\begin{array}{c}\text{maximal}\\ \text{ideal}\\ I\subseteq\Gamma(V)\end{array}\right\}$$

Chinese remainder theorem

Let $I_1, \dots, I_m$ be ideals of a ring R. If they are pairwise coprime ($I_i + I_j = R$ for all $i \neq j$), then we have a ring isomorphism

$$R/I_1 \cap \dots \cap I_m \cong R/I_1 \times \dots \times R/I_m$$
$$r \bmod I_1 \cap \dots \cap I_m \mapsto (r \bmod I_1, \dots, r \bmod I_m)$$

Furthermore, $I_1 \cdots I_m = I_1 \cap \dots \cap I_m$.

Rmk The interesting part is surjectivity.
(Injectivity is obvious.)

Ex $\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

Ex $K[X]/(X(X+1)) \cong K[X]/(X) \times K[X]/(X+1) \cong K \times K$

Cor 6.2 Let $V_1, \dots, V_m$ be alg. subsets of K^n. If they are pairwise disjoint, then

$$\Gamma(V_1 \cup \dots \cup V_m) \cong \Gamma(V_1) \times \dots \times \Gamma(V_m)$$
$$f \mapsto (f|_{V_1}, \dots, f|_{V_m})$$

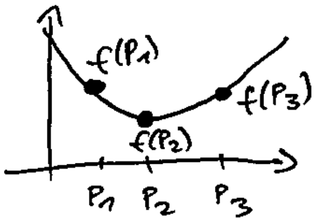
Pf Let $I_i = \mathcal{I}(V_i)$.

$\emptyset = V_i \cap V_j = \mathcal{V}(I_i + I_j) \underset{\text{weak Nots}}{\Rightarrow} I_i + I_j = K[X_1, \dots, X_n]$

$\mathcal{I}(V_1 \cup \dots \cup V_m) = I_1 \cap \dots \cap I_m$. $\square$

Cor 6.3

If V is a finite set, then every function $f: V \to K$ can be interpolated by a polynomial.



$(V = \{P_1, P_2, P_3\})$

Equivalently: The map

$$\begin{aligned} \Gamma(V) &\longrightarrow K \times \dots \times K \\ f &\longmapsto (f(P_1), \dots, f(P_m)) \end{aligned}$$

is an isomorphism (for $V = \{P_1, \dots, P_m\}$).

Pf Take $V_i = \{P_i\}$. $\square$