Algebraic Geometry

1. Overview

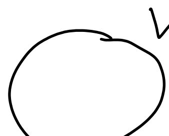
Let K be a field.

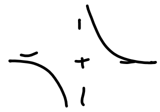
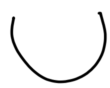
An <u>algebraic subset</u> of K^n is the set of solutions $(x_1,\dots,x_n)\in K^n$ to a system of polynomial equations:

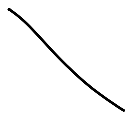
$$\begin{aligned} f_1(x_1,\dots,x_n)&=0, & f_1&\in K[x_1,\dots,x_n]\\ &\vdots & &\vdots\\ f_m(x_1,\dots,x_n)&=0, & f_m&\in K[x_1,\dots,x_n] \end{aligned}$$

<u>Ex</u>

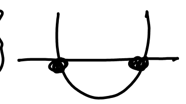
Conic (= conic section):

- Circle $V=\{(x,y)\in\mathbb{R}^2 \mid x^2+y^2=1\}$ 

- Ellipse $2x^2+3y^2=1$ 
- Hyperbola $xy=1$ 
- Parabola $y=x^2$ 

Line $x+2y=3$ 

Point $\{(1,2)\}=\{(x,y)\in\mathbb{R}^2 \mid y=2x,\ x+1=y\}$
$=\{\ \mid x=1,\ y=2\}$ 

Two points $\{(0,0),(1,0)\}=\{\ \mid x(x-1)=y,\ y=0\}$ 

$\vdots$

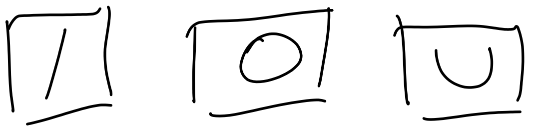
Questions

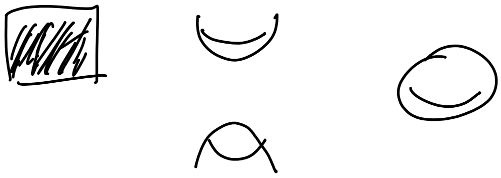
- Is V a set of just finitely many points?

  If so, how many?

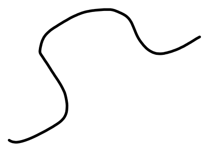
- What is the "dimension" of V?

  dim $= 0$: 

  dim $= 1$: 

  dim $= 2$: 

- Is V "smooth"?

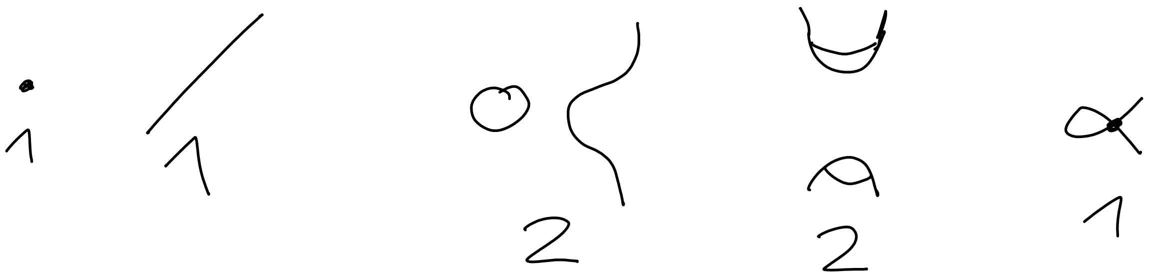
  smooth 

  not smooth 

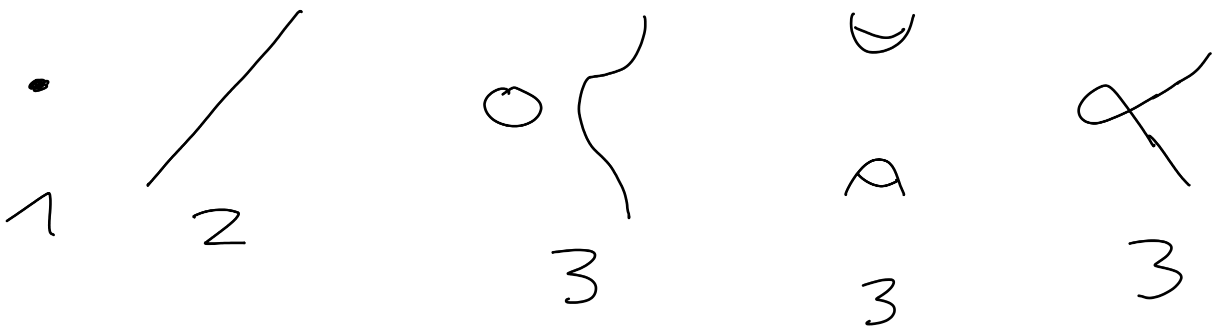
- If not, what are the "singularities" looks like?

Real algebraic geometry ($K = \mathbb{R}$)

- How many connected components does V have?

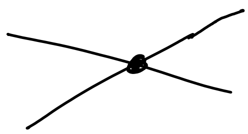


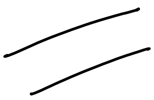
- How many connected components does the complement $\mathbb{R}^n \setminus V$ have?



Intersection theory

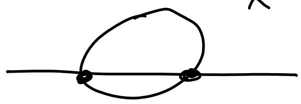
- In how many points do two lines $l_1 \neq l_2 \subseteq K^2$ intersect?

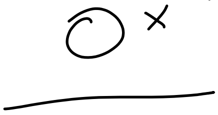
Usually 1 

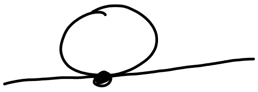
Occasionally 0  (if l_1, l_2 are parallel)

$\rightsquigarrow$ Always 1 in the projective plane.

- In how many points does a line intersect a conic?

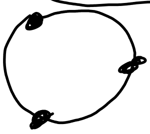
Sometimes 2  $x^2+(y-2)^2=100$, $y=1$

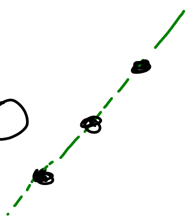
Sometimes 0  $x^2+(y-2)^2=100$, $y=-1000$ (can't happen in algebraically closed fields like $\mathbb{C}$)

Occasionally 1  (with "multiplicity" 2)

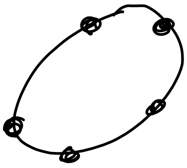
Enumerative geometry

- How many circles are there through three given points p_1, p_2, p_3? (distinct)

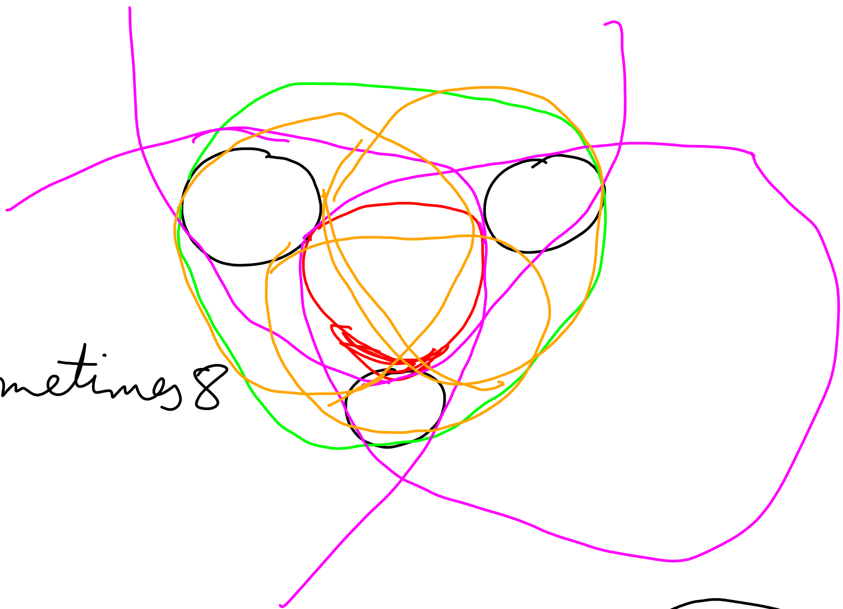
Usually 1 

Occasionally 0 

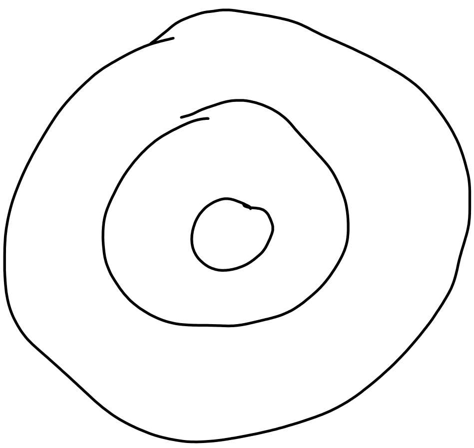
- How many conics are there through five given points p_1, p_2, p_3, p_4, p_5?

Usually 1 

- How many circles are there tangent to three given circles?



Sometimes 8



Sometimes 0

1

2

3

4

5

6

But 7 is impossible!

- How many lines are there that intersect four given lines in three-dimensional space?

Usually 2

- How many lines are there on a given cubic surface (surface defined by a pol. of degree 3)?

Usually 27 (if $K = \mathbb{C}$).

Prerequisites

Algebra: rings, modules, fields, ...
algebraically closed fields

References

Fulton
Brooke Ullery's lecture notes

Grade

70% weekly homeworks
(dropping the two lowest scores)

30% take-home exam

OH this week: Mo, Th 4-5pm in 233

Course assistants:

Raphael Tsiamis (rtsiamis@college.harvard.edu)
Raluca Vlad (rvlad@college.harvard.edu)

2. Basic definitions

Let K be a field.

<u>Rmk</u> In algebraic geometry, the set of points in K^n is often also denoted by $\mathbb{A}^n$ or $\mathbb{A}^n_K$ and called the n-dimensional <u>affine space</u> (over K).

<u>Def</u> The <u>vanishing locus</u> of a set $S \subseteq K[X_1, \dots, X_n]$ of polynomials is the corresponding set of zeros:

$$\mathcal{V}(S) = \{ P \in K^n \mid f(P) = 0 \ \forall f \in S \}$$

<u>Ex</u> $(n=2)$ $\mathcal{V}(\{X_2 - X_1^2\}) = \{(x_1, x_2) \in K^2 \mid x_2 = x_1^2\}$

<u>Ex</u> $\mathcal{V}(\{X_1 - a_1, \dots, X_n - a_n\}) = \{(a_1, \dots, a_n)\}$

<u>Def</u> The <u>vanishing ideal</u> of a set $X \subseteq K^n$ is the set of polynomials that vanish everywhere on X:

$$\mathcal{I}(X) = \{ f \in K[X_1, \dots, X_n] \mid f(P) = 0 \ \forall P \in X \}$$

<u>Lemma 2.1</u> $\mathcal{I}(X)$ is an ideal of $K[X_1, \dots, X_n]$.

<u>Pf</u>
- If $f(P) = 0$, then $f(P) \cdot g(P) = 0$ for all $g \in K[X_1, \dots, X_n]$.
  ($\Leftrightarrow f \in \mathcal{I}(X)$) ($\Leftrightarrow fg \in \mathcal{I}(X)$)
- If $f(P) = 0$ and $g(P) = 0$, then $f(P) + g(P) = 0$.
  ($\Leftrightarrow f \in \mathcal{I}(X)$) ($\Leftrightarrow g \in \mathcal{I}(X)$) ($\Leftrightarrow f + g \in \mathcal{I}(X)$)

$\square$

<u>Ex</u> $(n=2)$

$$\mathcal{I}(\{(0,0)\}) = \{ f(X_1, X_2) \in K[X_1, X_2] \mid \underset{\substack{\uparrow \\ \text{const.} \\ \text{coeff.} \\ \text{of } f}}{f(0,0)} = 0 \} = \underset{\substack{\uparrow \\ \text{ideal generated by } f}}{(X_1, X_2)}$$

Rmk $\mathcal{V}$ is inclusion-reversing:

$$\text{if } S \subseteq T, \text{ then } \mathcal{V}(S) \supseteq \mathcal{V}(T)$$

$\mathcal{I}$ is inclusion-reversing:

$$\text{if } X \subseteq Y, \text{ then } \mathcal{I}(X) \supseteq \mathcal{I}(Y)$$

Rmk If I is the ideal generated by $S \subseteq k[x_1, \dots, x_n]$, then $\mathcal{V}(I) = \mathcal{V}(S)$.

Pf "$\subseteq$" follows from $I \supseteq S$

"$\supseteq$" Every element of I can be written as

$$\underbrace{\underbrace{f_1}_{0 \text{ at } P} g_1 + \dots + \underbrace{f_r}_{0 \text{ at } P} g_r}_{0 \text{ at } P} \quad \text{with } f_1, \dots, f_r \in S \text{ and } g_1, \dots, g_r \in k[x_1, \dots, x_n]$$

for all $P \in S$. $\square$

__Def__ A subset $X \subseteq K^n$ is __algebraic__ if $X = \mathcal{V}(S)$ for some $S \subseteq K[x_1, \dots, x_n]$.

__Rmk__ This differs from the definition in chapter 1, where we only allowed __finitely many__ polynomial equations. We'll soon see that the two definitions are equivalent!

__Ex__ $\{(x_1, x_2) \mid x_2 = x_1^2\}$

__Ex__ Any one-point subset $\{P\} \subseteq K^n$.

Lemma 2.2

a) For any collection of ideals I_α, (of $K[x_1,\dots,x_n]$)

$$\bigcap_\alpha V(I_\alpha) = V\Big(\bigcup_\alpha I_\alpha\Big)$$

$$= V\Big(\text{ideal gen. by } \bigcup_\alpha I_\alpha\Big)$$

b) For any two ideals I, J [redacted],

$$V(I) \cup V(J) = V(I \cap J) = V(\underbrace{I \cdot J}_{\substack{\text{ideal generated by} \\ \text{polynomials of} \\ \text{the form } f\cdot g \\ \text{with } f\in I,\ g\in J}})$$

c) $V(0) = K^n$
d) $V(1) = \emptyset$

Pf a) clear

b) $\mathcal{V}(I) \cup \mathcal{V}(J) = \mathcal{V}(I \cdot J)$:

$p \in LHS \Leftrightarrow p \in \mathcal{V}(I)$ or $p \in \mathcal{V}(J)$

$\Leftrightarrow \forall f \in I : f(p) = 0$ or $\forall g \in J : g(p) = 0$

$\Leftrightarrow \forall f \in I, g \in J : f(p) = 0$ or $g(p) = 0$

$\Leftrightarrow p \in RHS$

$\mathcal{V}(I) \cup \mathcal{V}(J) \subseteq \mathcal{V}(I \cap J)$:

clear

$\mathcal{V}(I \cap J) \subseteq \mathcal{V}(I \cdot J)$:

clear because $I \cdot J \subseteq I \cap J$.

c) $p \in \mathcal{V}(0) \Leftrightarrow 0 = 0$

d) $p \in \mathcal{V}(1) \Leftrightarrow 1 = 0$ $\square$

Cor 2.3

a) [redacted] The intersection of arbitrarily many alg. subsets of K^n is alg.

b) The union of two (or finitely many) alg. subsets of K^n is alg.

c) K^n is an alg. subset

d) $\emptyset$ is an alg. subset

Hence, the alg. subsets of K^n are the closed [redacted] sets of a topology on K^n, which is called the Zariski topology.

Ex Every finite subset of K^n is Zariski closed because every one-point subset is.

<u>Lemma 2.4</u> 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.

<u>Pf</u> For any $f \in K[x_1, \dots, x_n]$, the set $V(f) = f^{-1}(\{0\})$ 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.

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

$\square$

<u>Thm 2.5</u> The alg. subsets of K (in $n=1$) are:

K and the finite subsets of K

In other words, the Zariski topology on K is the <u>cofinite topology</u>.

<u>Pf</u> 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: $f=0$</u>

$\Rightarrow f$ has only finitely many roots. $\square$

<u>Ex</u> of Lemma 2.4

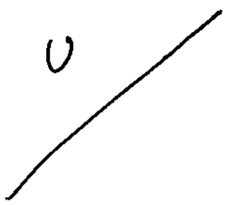
$K=\mathbb{R}$, $n=1$

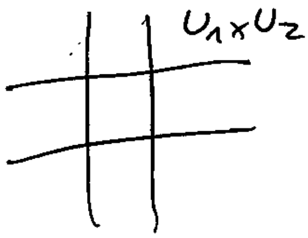
zar. closed: $\underbrace{\mathbb{R}, \text{ fin. subsets}}_{\text{closed w.r.t. usual top.}}$

<u>Warning</u> The Zariski topology on K^n is (in general) <u>not</u> the product topology arising from the product topology on K.

~~[illegible]~~

<u>Ex</u> $U = \mathbb{C}^2 \setminus \{(x,y) \in \mathbb{C}^2 \mid x = y\}$ is Zariski open, but doesn't contain any (nonempty) product $U_1 \times U_2$ with $\underbrace{U_1}_{= \mathbb{C} \setminus \text{fin. many pts}}, \underbrace{U_2}_{= \mathbb{C} \setminus \text{fin. many pts.}} \subseteq \mathbb{C}$ Zariski open.





3. Hilbert's Basis Theorem

Goal: Every alg. set is defined by finitely many polynomial equations.

Convention Rings are commutative and have a multiplicative unit 1.

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

Ex Any principal ideal domain is noetherian.
(e.g. any field K
or pol. ring over a field $K[x]$)

Lemma 3.1 R is noetherian if and only if there is no chain of ideals

$$I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \cdots$$

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

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

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

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

<u>Thm 3.2</u> (Hilbert's Basis Theorem)

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

By induction, this implies:

<u>Cor 3.3</u>

If R is noetherian, then $R[X_1, \dots, X_n]$ is noetherian.

<u>Cor 3.4</u>

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

Pf. of Thm 3.2

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

We inductively construct

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

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

of minimum degree.

Let $d_r = \deg(f_r)$.

$\Rightarrow d_1 \leq d_2 \leq \dots$

Let $b_r = lc(f_r)$.

The <u>leading coefficient</u> $lc(h)$ of a (nonzero) pol. $h(x) = a_n x^n + \dots + a_0$ with $a_n \neq 0$ is a_n.

We get a chain of ideals of R:

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

Since R is noetherian, we have equality somewhere:

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

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

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

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

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

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

<u>Warning</u> For every $n \geq 1$, there are ideals of $k[x,y]$ that aren't generated by n elements!

4. Nullstellensätze

German for: root theorems

4.1. Nichtnullstellensatz

German for: non-root theorem

Thm 4.1.1

Assume that K is infinite.

Then, $I(K^n) = 0$.

(In other words, there is no pol. $0 \neq f \in K[X_1, \dots, X_n]$ that vanishes everywhere.)

Rmk This is wrong for finite fields K:

$f(X_1, \dots, X_n) := \prod_{a \in K} (X_1 - a)$ vanishes everywhere.

Pf of Thm Use induction over n.

($n=0$: silly)

$n=1$: nonzero pol. have only finitely many roots

$n-1 \Rightarrow n$: Let $0 \neq f \in K[X_1, \dots, X_n]$.

Write $f(X_1, \dots, X_n) = \sum_{i=0}^{d} g_i(X_1, \dots, X_{n-1}) X_n^i$

with $g_i \in K[X_1, \dots, X_{n-1}]$, $g_d \neq 0$.

By induction, we have

$g_d(a_1, \dots, a_{n-1}) \neq 0$ for some $(a_1, \dots, a_{n-1}) \in K^{n-1}$.

$\Rightarrow 0 \neq f(a_1, \dots, a_{n-1}, X_n) \in K[X_n]$ (pol. of degree d)

By the $n=1$ case, we then have

$f(a_1, \dots, a_{n-1}, a_n) \neq 0$ for some $a_n \in K$. $\square$

4.2. Weak Nullstellensatz

Thm 4.2.1 (Weak Nullstellensatz)

German for: root theorem

Assume that K is algebraically closed. For any ideal $I \subsetneq K[x_1, \dots, x_n]$, we have $V(I) \neq \emptyset$.

Pf soon...

Rmk This is false if K is not algebraically closed.

Pf If K isn't alg. cl., there is a nonconstant pol. $f \in K[x]$ without roots.

$$\Downarrow \qquad\qquad\qquad\qquad \Downarrow$$

$$(f) \subsetneq K[x] \qquad\qquad V((f)) = \emptyset. \qquad \square$$

4.3 Hilbert's Nullstellensatz

Given an ideal $I \subseteq k[x_1, \dots, x_n]$, what is $\mathcal{I}(\mathcal{V}(I))$?
When is $\mathcal{I}(\mathcal{V}(I)) = I$?

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

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

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

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

Pf If $P \in \mathcal{V}(I)$, then $f(P)^n = 0$.

$\Rightarrow f(P) = 0$ $\quad / \!\!\Rightarrow f \in \mathcal{I}(\mathcal{V}(I))$. $\square$

Def The radical 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 4.1 $\sqrt{I}$ is an ideal.

Pf • Let $f, g \in \sqrt{I}$.

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

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

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

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

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

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

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

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

<u>Def</u> An ideal I is a <u>radical ideal</u> if $\sqrt{I} = I$.

<u>Rmk</u> $\sqrt{I}$ is a radical ideal: $\sqrt{\sqrt{I}} = \sqrt{I}$.

<u>Rmk</u> If R is a unique factorization domain and we have a factorization $f = u \cdot g_1^{e_1} \cdots g_r^{e_r}$, then $\sqrt{(f)} = (g_1 \cdots g_r)$.

Thm 4.3.2 (Hilbert's Nullstellensatz)

Assume that K is algebraically closed. Then, $\mathcal{J}(\mathcal{V}(I)) = \sqrt{I}$ for any ideal I of $K[x_1, \dots, x_n]$.

Ex If $n=1$, $I=(f)$ with

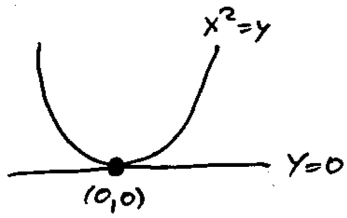
$f = c(x-a_1)^{e_1} \cdots (x-a_r)^{e_r}$, then

$\mathcal{V}(I) = \{a_1, \dots, a_r\}$,

$\mathcal{J}(\mathcal{V}(I)) = ((x-a_1)\cdots(x-a_r)) = \sqrt{(f)}$.

~~Rmk The Thm is wrong if K is not alg. closed.~~

Ex $n=2$, $I = (x^2-y, y) = (x^2, y)$



$\Rightarrow \mathcal{V}(I) = \{(0,0)\}$

$\Rightarrow \mathcal{J}(\mathcal{V}(I)) = (x,y) = \sqrt{I}$

Rmk Hilbert's Nsts (for k) $\Longrightarrow$ Weak Nsts (for k)

(In part., Hilbert's Nsts fails for fields that aren't alg. closed)

Pf If $V(I)=\emptyset$, then $\underbrace{J(V(I))}_{=\sqrt{I}} = k[x_1,\dots,x_n] \ni 1.$

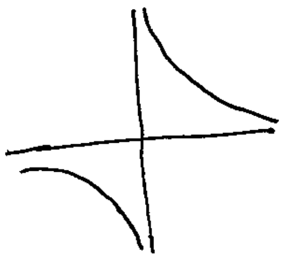
$\Longrightarrow \underset{1=}{}1^n \in I$ for some $n \geq 1$. $\square$

Rmk Hilbert's Nsts $\Longrightarrow$ Nichtnullstellensatz

Pf $J(k^n) = J(V(0)) = \sqrt{0} = 0.$ $\square$

Preparation

$\mathbb{R}\setminus\{0\}$ isn't an alg. subset of $\mathbb{R}$



$\{(x,y)\in\mathbb{R}^2 \mid xy=1\}$ is an alg. subset of $\mathbb{R}^2$ and its projection onto the x-axis is $\mathbb{R}\setminus\{0\}$.

Pf of Hilbert's Nsts (assuming Weak Nsts)

"$\mathcal{I}(\mathcal{V}(I)) \supseteq \sqrt{I}$": done earlier

"$\mathcal{I}(\mathcal{V}(I)) \subseteq \sqrt{I}$":

Let $f \in \mathcal{I}(\mathcal{V}(I))$.

$\Rightarrow \forall P \in \mathcal{V}(I): \ f(P) = 0$

$\Rightarrow \{P \in \mathcal{V}(I) \mid f(P) \neq 0\} \overset{\subseteq K^n}{=} \emptyset$

We have a bijection

$$\{P \in \mathcal{V}(I) \mid f(P) \neq 0\} \longleftrightarrow \{(P,t) \in \underbrace{\mathcal{V}(I) \times K}_{\subseteq K^{n+1}} \mid f(P) \cdot t = 1\} = \underset{\substack{\cap \\ K^{n+1}}}{\mathcal{V}(I')},$$

where $I' \subseteq K[X_1, \dots, X_n, T]$ is the ideal generated by the elements of I and by the polynomial $f(X_1, \dots, X_n) \cdot T - 1$.

$LHS = \emptyset \Rightarrow \underset{\substack{\shortparallel \\ \mathcal{V}(I')}}{RHS} = \emptyset$

$$\xRightarrow[\text{Weak Nsts}]{} \quad I' = K[X_1, \dots, X_n, T] \ni 1$$

$\Rightarrow$ We can write 1 as a lin. comb. of el. of I

and $f(x_1,\dots,x_n)\cdot T-1$, with coefficients in $K[x_1,\dots,x_n,T]$.

$\Rightarrow$ We can write

$$1=\sum_{i=0}^{d} p_i(x_1,\dots,x_n)\cdot T^i+\big(f(x_1,\dots,x_n)\cdot T-1\big)\cdot q(x_1,\dots,x_n,T)$$

with $p_i\in I$, $q\in K[x_1,\dots,x_n,T]$.

That's an eq. in $K[x_1,\dots,x_n,T]\subseteq K(x_1,\dots,x_n)[T]$.

Plug in $T=\frac{1}{f(x_1,\dots,x_n)}$:

$$1=\sum_{i=0}^{d} p_i(\dots)\cdot\frac{1}{f(\dots)^i}\quad\text{in } K(x_1,\dots,x_n)$$

$$\Rightarrow f^d=\sum_{i=0}^{d}\underbrace{p_i}_{\in I}\underbrace{f^{d-i}}_{\in K[x_1,\dots,x_n]}\in I$$

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

$\square$

4.4. Ring and field extensions

Def Let R be a ring. A ring extension of R is a ring S containing R as a subring.

Rmk A ring extension of R is also an R-module.

Def Let K be a field. A field extension of K is a field L containing K as a subfield.

Rmk A field ext. of K is also a ring ext. of K and a K-vector space ($= K$-module).

Def Let S be a ring extension of R. The ring extension generated by a subset A of S is the smallest (= inclusion-minimal) subring $R[A]$ of S containing R and A.

Rmk $R[A]$ is the set of sums of products of the form $r \cdot a_1 \cdots a_m$ with $r \in R$ and $a_1, \dots, a_m \in A$.

Rmk Take $A = \{a_1, \dots, a_n\}$.

$R[A]$ is the image of the R-algebra homomorphism

$$\begin{aligned} R[X_1, \dots, X_n] &\longrightarrow S. \\ r \in R &\longmapsto r \\ X_i &\longmapsto a_i \end{aligned}$$

Def Let L be a field extension of K. The field extension generated by a subset A of L is the smallest subfield $K(A)$ of L containing K and A.

Rmk $K(A)$ is the quotient field of the ring extension $K[A]$ generated by A.

Ex $R[X_1, \dots, X_n]$ is a ring extension of R generated by $X_1, \dots, X_n$.

Ex $K(X_1, \dots, X_n)$ is a field extension of K generated by $X_1, \dots, X_n$.

Rmk We now have three notions of being finitely generated:

- fin. generated as a module: $\exists a_1,\dots,a_n$: every el. can be written as a sum of terms ra_i with $r\in R$.
  ((module-)finite)

- fin. generated as a ring extension: $\exists a_1,\dots,a_n$ every el. can be written as a sum of products $r a_1^{e_1}\cdots a_n^{e_n}$ with $r\in R$, $e_i\geq 0$.
  (ring-finite)

- fin. generated as a field extension: $\exists a_1,\dots,a_n$: every el. can be written as the quotient of two such sums
  (field-finite)

Rmk module-finite

$\Downarrow$

ring-finite

$\Downarrow$

field-finite

However:

<u>Rmk</u> module-finite
$$\Uparrow\!\!\!\!/$$
ring-finite

<u>Pf</u> $\mathbb{C}[X]$ is a finitely generated ring ext. of $\mathbb{C}$, but not a finitely generated $\mathbb{C}$-module (= $\mathbb{C}$-vector space).

Basis: $1, X, X^2, \ldots$ $\square$.

<u>Rmk</u> ring-finite
$$\Uparrow\!\!\!\!/$$
field-finite

<u>Pf</u> $\mathbb{C}(X)$ is a finitely generated field ext. of $\mathbb{C}$, but not a fin. generated ring ext. of $\mathbb{C}$.

Assume $\mathbb{C}(X) = \mathbb{C}[a_1, \ldots, a_n]$.

Write $a_i(X) = \dfrac{p_i(X)}{q_i(X)}$ with $p_i, q_i \in \mathbb{C}[X]$, $q_i \neq 0$.

Let $t \in \mathbb{C}$ be <u>not</u> a root of $q_1(X) \cdots q_n(X)$.

By assumption, we can write

$$\mathbb{C}(X) \ni \frac{1}{X-t} = \sum_j c_j \left(\frac{p_1(X)}{q_1(X)} \right)^{e_{1,j}} \cdots \left(\frac{p_n(X)}{q_n(X)} \right)^{e_{n,j}}$$

with $c_j \in K$, $e_{i,j} \geq 0$.

Multiply by $X-t$ and sufficiently large powers of $q_1(X), \ldots, q_n(X)$.

Plug in $X = t$.

$\Rightarrow$ LHS $\neq 0$, RHS $= 0$ $\lightning$ $\square$

Rmk Module/ring/field-finiteness are transitive:

If S is a module/ring/field-finite ext. of R and T is a module/ring/field-finite ext. of S, then T is a module/ring/field-finite ext. of R.

$$\begin{tikzcd} T \arrow[d, dash, "\text{fin}"'] \arrow[dd, dash, dashed, bend left, "\Rightarrow \text{fin}"] \\ S \arrow[d, dash, "\text{fin}"'] \\ R \end{tikzcd}$$

Pf module-finite: S gen. by $a_1, \dots, a_n$ as R-mod

T gen. by $b_1, \dots, b_m$ as S-mod.

$\Rightarrow T$ gen. by $\left\{ a_i b_j \,\middle|\, \begin{array}{l} 1 \le i \le n, \\ 1 \le j \le m \end{array} \right\}$ as R-mod.

ring-finite: $S = R[a_1, \dots, a_n]$

$T = S[b_1, \dots, b_m]$

$\Rightarrow T = R[a_1, \dots, a_n, b_1, \dots, b_m]$.

field-finite: same ... $\square$

4.5 Integral and algebraic extensions

<u>Def</u> An element a of a ring S is called <u>integral over</u> a subring $R \subseteq S$ if there is a <u>monic</u> polynomial $f(x) \in R[x]$ (leading coeff. $= 1$: $f(x) = x^n + c_{n-1}x^{n-1} + \dots + c_0$) with $f(a) = 0$.

A ring extension S of R is <u>integral</u> if every $a \in S$ is integral over R.
The <u>integral closure</u> of a ring R in a ring extension S is the set of elements of S that are integral over R.
The ring R is called <u>integrally closed</u> in S if its integral closure in S is R.

<u>Def</u> If $R = K$ is a field, integral is also called <u>algebraic</u>. Numbers that aren't algebraic are transcendental (over K).

<u>Rmk</u> If $R = K$ is a field, one could allow any nonzero polynomial $f(x) \in K[x]$ (divide by the leading coefficient).

Rmk An algebraically closed field K has no algebraic field extensions $L \neq K$.

Ex Any element of R is integral over R.

Pf Take $f(X) = X - a$. $\square$

Ex $\sqrt[3]{2} \in \mathbb{R}$ is algebraic over $\mathbb{Q}$ and integral over $\mathbb{Z}$.

Pf Take $f(X) = X^3 - 2$. $\square$

Ex $\mathbb{C}$ is an algebraic extension of $\mathbb{R}$.

Pf Let $a \in \mathbb{C}$. Take $f(X) = (X-a)(X-\bar{a})$

$$= X^2 - \underbrace{(a+\bar{a})}_{\in \mathbb{R}}\cancel{X} + \underbrace{a\bar{a}}_{\in \mathbb{R}}.$$

$\square$

Thm $\mathbb{C}$ is not an algebraic ext. of $\mathbb{Q}$.

Thm (Hermite) $\pi \in \mathbb{R}$ is transcendental over $\mathbb{Q}$.

Ex $T \in K(T)$ is transcendental over K for any field K.

Pf If $f(X) \in K[X]$ is a nonzero pol. then $f(T) \in K(T)$ is "the same" nonzero pol. $\square$

Rmk For the same reason, $T \in K[T]$ is not integral over K.

Thm 4.5.1 A unique factorization domain R (e.g. $R = \mathbb{Z}$, $K[X_1, \dots, X_n]$) is integrally closed in its field of fractions K.

Pf Assume $\frac{p}{q} \in K$ is integral ($p, q \in R$).

W.l.o.g. $\gcd(p, q) = 1$.

Let $f(X) = X^n + c_{n-1} X^{n-1} + \dots + c_0$ with $f(\frac{p}{q}) = 0$. $\quad (c_i \in R)$

$$\Rightarrow \left(\frac{p}{q}\right)^n + c_{n-1}\left(\frac{p}{q}\right)^{n-1} + \dots + c_0 = 0$$

$$\Rightarrow p^n = -(c_{n-1} p^{n-1} q + \dots + c_0 q^n)$$

RHS is divisible by q.

If q is divisible by some prime element $t \in R$, then p^n and therefore p is also divisible by t. $\Rightarrow$ p, q aren't coprime. ↯

$\square$

Lemma 4.52 Let R be an integral domain with field of fractions K and let L be a field extension of K. Then, any element $a \in L$ that is algebraic over K can be written as $a = \frac{p}{q}$ with $p \in L$ integral over R and $0 \neq q \in R$.

Pf Let $f(X) \in K[X]$ be monic, and $f(a) = 0$.

$$f(X) = X^n + c_{n-1}X^{n-1} + \dots + c_0$$

$$\Rightarrow a^n + c_{n-1}a^{n-1} + \dots + c_0 = 0$$

Clear out denominators:

Pick $0 \neq q \in R$ such that $c_i q \in R \ \forall i$.

$$\Rightarrow q^n a^n + q c_{n-1} q^{n-1} a^{n-1} + q^2 c_{n-2} q^{n-2} a^{n-2} + \dots + q^n c_0 = 0.$$

$$\Rightarrow (qa)^n + \underbrace{q c_{n-1}}_{\in R} (qa)^{n-1} + \dots + \underbrace{q^n c_0}_{\in R} = 0$$

$\Rightarrow p := qa \in L$ is integral over R. $\square$

Lemma 4.5.3 Let S be a ring extension of R and let $a \in S$. The following are equivalent:

i) a is integral over R.

ii) The ring extension $R(a)$ of R is module-finite.

iii) There is a ring ext. $a \in S' \subseteq S$ of R which is module-finite.

Pf ii) $\Rightarrow$ iii): clear

i) $\Rightarrow$ ii): Let $f(X) = X^n + c_{n-1}X^{n-1} + \dots + c_0 \in R(X)$ with $f(a) = 0$.

$\Rightarrow a^n = -(c_{n-1}a^{n-1} + \dots + c_0)$. (I)

Repeatedly applying (I), we can show that any a^e with $e \geq 0$ lies in the R-module generated by $1, a, \dots, a^{n-1}$: Assume a^e is the first counterexample. $\Rightarrow e \geq n$.

$$a^e \underset{(I)}{=} -(c_{n-1}a^{n-1} + \dots + c_0)a^{e-n}$$

$$= -(c_{n-1}a^{e-1} + \dots + c_0 a^{e-n})$$

apply the induction hypothesis.

$\Rightarrow R[a]$ is gen. by $1, a, \dots, a^{n-1}$.

(Ese $\mathbb{Z}[\sqrt[3]{2}]$ is gen. by $1, \sqrt[3]{2}, \sqrt[3]{2}^2$ as a $\mathbb{Z}$-module.)

iii) $\Rightarrow$ i): Assume S' is generated by $b_1, \dots, b_n \in S'$ as an R-module. W.l.o.g. $1 \in b_1$.

Write $a\, b_i = r_{i1} b_1 + \dots + r_{in} b_n$ with $r_{ij} \in R$.

$$\Rightarrow \underbrace{\begin{pmatrix} r_{11} & \cdots & r_{1n} \\ \vdots & & \vdots \\ r_{n1} & \cdots & r_{nn} \end{pmatrix}}_{M} \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} = a \cdot \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}$$

$$\Rightarrow N \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} = 0, \text{ where } N = a I_n - M$$

$n \times n$ identity matrix

Let $\tilde{N}$ be the adjugate matrix of N.

$$\Rightarrow \tilde{N} N = \det(N) \cdot I_n$$

$$\Rightarrow 0 = \tilde{N} N \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} = \det(N) \cdot \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}$$

$$= \det(N) \cdot \begin{pmatrix} 1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}$$

$$\Rightarrow \det(N) = 0.$$

But $\det(N) = \det(aI_n - M)$ is a monic polynomial in a of degree n. with coefficients in R.

$\Rightarrow a$ is integral over R. $\square$

(Ex $\frac{1}{2} \in \mathbb{Q}$ is not integral over $\mathbb{Z}$

$\mathbb{Z}[\frac{1}{2}] = \{ \frac{a}{2^b} \mid a \in \mathbb{Z}, b \in \mathbb{Z} \}$

isn't a finitely gen. $\mathbb{Z}$-module.)

Cor 4.5.4 The integral closure of R in S is a ring (a ring ext. of R).

Pf Let $a, b \in S$ be integral over R.

$\overset{ii}{\Rightarrow}$ The ring ext. $R[a]$ of R is module-finite.

— " — $R[b]$ of R — " —

($R[a]$ gen. by $c_1, \dots, c_n$

$R[b]$ gen. by $d_1, \dots, d_m$)

$\Rightarrow R[a,b]$ gen. by $\{c_i d_j \mid {1 \le i \le n \atop 1 \le j \le m}\}$

But $a+b, a \cdot b \in R[a,b] \subseteq S$

$\overset{iii}{\Rightarrow} a+b, a \cdot b$ are integral over R. $\square$

Ex $\sqrt[3]{2} + \sqrt[3]{3}$ is integral over $\mathbb{Z}$.

Cor 4.5.5 The alg. closure of K in L is a field (a field ext. of K).

Pf Let $0 \neq a \in L$ be algebraic over K.

Let $f(X) = X^n + c_{n-1} X^{n-1} + \dots + c_0 \in K[X]$ with $f(a) = 0$.

$$\Rightarrow a^n + c_{n-1} a^{n-1} + \dots + c_0 = 0$$

$$\Rightarrow 1 + c_{n-1} \frac{1}{a} + \dots + c_0 \left(\frac{1}{a}\right)^n = 0.$$

$\Rightarrow \frac{1}{a}$ is algebraic over K. $\square$

Cor 4.5.6 Integrality / algebraicity are transitive: If S is an integral ring ext. of R,
and T —"— S,
then T —"— R.

Pf HW. $\square$

Cor 4.5.7 Let S' be the integral closure of R in S. Then, S' is integrally closed in S.

Pf HW. $\square$

Thm 4.58 Any <u>ring-finite</u> <u>field</u> extension L of a field K is <u>module-finite</u> (= finite-dimensional K-vector space).

($\Rightarrow L$ is an algebraic extension of K).

<u>Pf</u> Let $L = K[a_1, \dots, a_n]$.

Use induction:

<u>$n = 1$:</u> $L = K[a_1]$

If a_1 is algebraic, we're done.

If it isn't, then $1, a_1, a_1^2, \dots \in L$ are linearly independent over K.

$\Rightarrow$ The ring homomorphism

$$\begin{aligned} K[X] &\longrightarrow K[a_1] = L \\ X &\longmapsto a_1 \end{aligned}$$

is an isomorphism.

But $K[X]$ isn't a field!

<u>$n-1 \to n$:</u> Note that $L = K(a_1)[a_2, \dots, a_n]$.

$\Rightarrow$ By the induction hypothesis, the field extension $L = K(a_1)[a_2, \dots, a_n]$ of $K(a_1)$ is module-finite.

If a_1 is algebraic over K, then
$K(a_1) = K[a_1]$ is a module-fin. eset. of K.
Since L is a module-fin. eset. of $K(a_1)$,
L is a module-finite eset. of K.

If a_1 isn't algebraic over K:

$$K(a_1) = \text{field of fractions of } K[a_1]$$
$$\cong \quad \text{—— " ——} \quad \text{of } K[X]$$
$$= K(X).$$

The elements $a_2, \dots, a_n \in L$ are algebraic over $K(a_1) \cong K(X)$.
By Lemma 4.5.2, we can (for $i = 2, \dots, n$) write $a_i = \dfrac{p_i}{q_i}$ with $p_i \in L$ integral over $K[a_1] \cong K[X]$ and $0 \neq q_i \in K[a_1] \cong K[X]$.
Now, proceed as in the proof that the extension $\mathbb{C}(X)$ of $\mathbb{C}$ isn't ring-finite (cf. section 4.4):
The ring $K[a_1] \cong K[X]$ contains ∞ many maximal ideals ($\hat{=}$ monic irreducible polynomials).

$\Rightarrow$ There exists $r \in K[a_1] \cong K[X]$

relatively prime to $q_2, \dots, q_n$.

Since $\frac{1}{r} \in L = K[a_1, \dots, a_n] = K(a_1)[a_2, \dots, a_n]$,

we can write

$$\frac{1}{r} = \sum_j c_j \, a_2^{e_{2,j}} \cdots a_n^{e_{n,j}} \quad \text{with } c_j \in K[a_1], \; e_{ij} \geq 0.$$

$$\frac{1}{r} = \sum_j c_j \left(\frac{p_2}{q_2}\right)^{e_{2,j}} \cdots \left(\frac{p_n}{q_n}\right)^{e_{n,j}}$$

Multiply by large enough powers of $q_2, \dots, q_n$ to clear out denominators on the RHS.

$\Rightarrow$ Since $c_j \in K(a_1)$ and $p_2, \dots, p_n$ integral over $K[a_1]$, and since the integral closure of $K[a_1]$ in L is a ring, the RHS is then integral.

But $\text{LHS} = \dfrac{q_2^{\cdots} \cdots q_n^{\cdots}}{r} \in K(a_1) \setminus K[a_1]$

$$\begin{array}{c} K(a_1) \setminus K[a_1] \\ \text{\rotatebox{90}{$\cong$}} \\ K(X) \setminus K[X] \end{array}$$

isn't integral over $K[a_1] \cong K[X]$ by Thm ~~...~~ 4.5.1. $\square$

4.6. Proof of the weak Nullstellensatz

Reminder: We still need to show Thm 4.2.1:

Assume K is algebraically closed.

For any ideal $I \subseteq K[X_1, \dots, X_n]$,

if $I \neq K[X_1, \dots, X_n]$, then $V(I) \neq \emptyset$.

This immediately follows from:

<u>Lemma 4.6.9</u> Assume K is alg. closed.

a) If $I \subseteq K[x_1, \dots, x_n]$ is a maximal ideal, then $V(I) \subseteq K^n$ consists of exactly one point.

b) If $\underset{\{P\}}{\overset{\shortparallel}{V}} \subseteq K^n$ consists of exactly one point, then $J(V) \subseteq K[x_1, \dots, x_n]$ is a maximal ideal.

<u>Pf</u> b) $V = \{(a_1, \dots, a_n)\}$

$\Rightarrow J(V) = (x_1 - a_1, \dots, x_n - a_n)$.

$$\begin{aligned} K[x_1, \dots, x_n] &\longrightarrow K \\ f &\longmapsto f(a_1, \dots, a_n) \end{aligned}$$

has kernel $J(V)$.

$\Rightarrow K[x_1, \dots, x_n]/J(V) \cong K$ is a field.

$\Rightarrow J(V)$ is a max. ideal.

a) I maximal ideal

$\Rightarrow L := K[x_1, \dots, x_n]/I$ is a field.

There's an obvious embedding

$$\begin{aligned} K &\hookrightarrow L = K[x_1, \dots, x_n]/I \\ c &\longmapsto c \bmod I, \end{aligned}$$

so we will consider L a field extension of K.

In fact, L is a ring-finite field ext. of K, generated by $X_1, \dots, X_n \bmod I$.

$\Longrightarrow$ L is a finite-dimensional K-vector space (= module-finite)

Thm 4.5.8

$\Longrightarrow$ L is an algebraic ext. of K

Lemma 4.5.3

$\Longrightarrow$ $L = K$

K is algebraically closed

In other words, the embedding

$$\begin{aligned} K &\hookrightarrow L = K[X_1, \dots, X_n]/I \\ c &\longmapsto c \bmod I \end{aligned}$$

is an isomorphism.

Let a_i be the preimage of $X_i \bmod I$.

$\Rightarrow X_i - a_i \in I$ for all i

$\Rightarrow I' := (X_1 - a_1, \dots, X_n - a_n) \subseteq I$.

Both I and I' are maximal ideals, so this implies $I = I$!

$\Rightarrow \mathcal{V}(I) = \mathcal{V}(I') = \{(a_1, \dots, a_n)\}$. $\square$

$$\boxed{\text{From now on, we'll always assume that } K \text{ is algebraically closed.}}$$

(unless stated otherwise...)

Summary

$$\left\{\begin{matrix}\text{subset}\\ V\subseteq K^n\end{matrix}\right\} \underset{\mathcal{V}}{\overset{\mathcal{I}}{\rightleftarrows}} \left\{\begin{matrix}\text{ideal}\\ I\subseteq K[x_1,\dots,x_n]\end{matrix}\right\}$$

$\mathcal{V}(\mathcal{I}(V)) = \overline{V}$ (Zariski closure)
(= smallest alg. subset of K^n containing V)

$\mathcal{I}(\mathcal{V}(I)) = \sqrt{I}$ (radical ideal)

We obtain bijections:

$$\begin{array}{ccc}
\left\{\begin{matrix}\text{algebraic}\\ \text{subset}\\ V\subseteq K^n\end{matrix}\right\} & \underset{\mathcal{V}}{\overset{\mathcal{I}}{\rightleftarrows}} & \left\{\begin{matrix}\text{radical}\\ \text{ideal}\\ I\subseteq K[x_1,\dots,x_n]\end{matrix}\right\}\\
\cup\!\shortmid & & \cup\!\shortmid\\
\left\{\begin{matrix}\text{one-point}\\ \text{subset}\\ V\subseteq K^n\end{matrix}\right\} & \underset{\mathcal{V}}{\overset{\mathcal{I}}{\rightleftarrows}} & \left\{\begin{matrix}\text{maximal}\\ \text{ideal}\\ I\subseteq K[x_1,\dots,x_n]\end{matrix}\right\}
\end{array}$$

5. Irreducibility

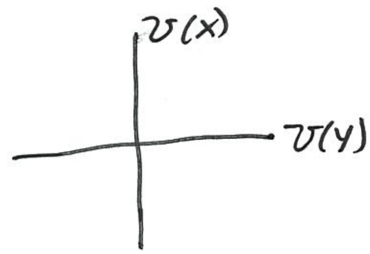
<u>Def</u> An algebraic set $\emptyset \neq V \subseteq K^n$ is <u>irreducible</u> if you can't write $V = V_1 \cup V_2$ with any algebraic sets $V_1, V_2 \subsetneq V$.

If you can, it is called <u>reducible</u>.

<u>Ex</u> Any one-point set $\underbrace{}_{V=\{P\}}$ is irreducible.

<u>Ex</u> $\mathcal{V}(XY) \subseteq K^2$ is reducible

$$\mathcal{V}(XY) = \mathcal{V}(X) \cup \mathcal{V}(Y)$$



<u>Ex</u> $\mathcal{V}(0) = K^n$ is irreducible

<u>Ex</u> $\mathcal{V}(X), \mathcal{V}(Y) \subseteq K^2$ are irreducible.

Thm 5.1 An algebraic subset $V \subseteq K^n$ is irreducible if and only if $\mathcal{I}(V)$ is a prime ideal of $K[x_1, \dots, x_n]$.

Pf First, note that $V = \emptyset \iff \mathcal{I}(V) = K[x_1, \dots, x_n]$.
(not prime)

"$\Rightarrow$" Assume $\mathcal{I}(V) \subsetneq K[x_1, \dots, x_n]$ is not prime.

$\Rightarrow$ There are $f, g \notin \mathcal{I}(V)$ with $fg \in \mathcal{I}(V)$.

$$\Downarrow \qquad\qquad\qquad\qquad \Downarrow$$

$$\underbrace{V \cap \mathcal{V}(f)}_{V_1}, \underbrace{V \cap \mathcal{V}(g)}_{V_2} \subsetneq V \qquad \underbrace{(V \cap \mathcal{V}(f))}_{V_1} \cup \underbrace{(V \cap \mathcal{V}(g))}_{V_2} = V$$

$\Rightarrow V$ is reducible.

"$\Leftarrow$" Assume $V = V_1 \cup V_2$ with algebraic subsets $V_1, V_2 \subsetneq V$.

$$\Downarrow$$

$$\mathcal{I}(V_1), \mathcal{I}(V_2) \supsetneq \mathcal{I}(V)$$

Let $f \in \mathcal{I}(V_1) \setminus \mathcal{I}(V)$ and $g \in \mathcal{I}(V_2) \setminus \mathcal{I}(V)$.

Then, $f, g \notin \mathcal{I}(V)$, but $fg \in \mathcal{I}(V)$.

$\Rightarrow \mathcal{I}(V)$ is not prime. $\square$

Rmk Prime ideals are radical ideals.

Cor 5.2 $\mathcal{V}(I) \subseteq K^n$ is irreducible if I is a prime ideal.

Pf $\mathcal{I}(\mathcal{V}(I)) = \sqrt{I} = I$ is prime. $\square$

Warning $(x^2) \subseteq K[x]$ is not a prime ideal, but nevertheless $\mathcal{V}(x^2) = \mathcal{V}(x) = \{0\}$ is irreducible.
($\sqrt{(x^2)} = (x)$ is prime.)

Ex $\mathcal{V}(x) \subseteq K^2$ is irreducible because (x) is a prime ideal of $K[X,Y]$ because $K[X,Y]/(x) \cong K[Y]$ is an integral domain.

Ex $\mathcal{V}(0) = K^n$ is irreducible.

Lemma/Reminder 5.3

If R is a unique factorization domain (such as $\mathbb{Z}$, $K[x_1, \dots, x_n]$), then (f) is a prime ideal if and only if $\underline{f = 0 \text{ or}}$ $f \in R$ is irreducible.

Ex $V(X^2+Y^2-1) \subseteq \mathbb{C}^2$ is irreducible because X^2+Y^2-1 is.


$V(X^2+Y^2-1)$

Pf Assume $X^2+Y^2-1 = fg$ for some nonconstant polynomials $f, g \in \mathbb{C}[X,Y]$.

Since X^2+Y^2-1 has degree 2 in X, either

a) f and g have degree 1 in X or

b) f has degree 0 in X and g has degree 2 in X or

c) f — " — 2 — " — g — " — 1 — " .

Case b) (and similarly case c) is impossible:

If $f = f(Y)$ only depends on Y, take some root $b \in \mathbb{C}$ of $f(Y)$.

Then, $a^2+b^2-1 = f(b)\,g(a,b) = 0$ for all $a \in \mathbb{C}$. ↯

Hence, f and g have degree 1 in X.

Similarly, — " — Y.

Since X^2+Y^2-1 has total degree 2, both f and g then must have total degree 1.

$\Rightarrow f(X,Y) = pX + qY + r$ for some $p, q, r \in \mathbb{C}$ with $p, q \neq 0$.

~~(So the unit circle $V(X^2+Y^2-1)$ contains a line $V(pX+qY+r)$)~~ ↯

$\Rightarrow a^2+b^2-1=0$ for all $(a,b)\in \mathbb{C}^2$ on the line given by $pa+qb+r=0$.

(The "unit circle" $V(X^2+Y^2-1)$ contains the line $V(pX+qY+r)$.)

$\to$ Plug in $a=-\dfrac{qb+r}{p}$:

$$\begin{aligned}0 &= p^2(a^2+b^2-1)\\ &= (qb+r)^2+p^2b^2-p^2\\ &= (q^2+p^2)b^2+2qrb+(r^2-p^2) \qquad \forall b\in\mathbb{C}\end{aligned}$$

$$\Rightarrow \begin{array}{ll} q^2+p^2=0, & \\ 2qr \;=0, & \overset{q\neq 0}{\Longrightarrow} \; r=0 \\ & \qquad\Downarrow \\ r^2-p^2\;=0 & \Rightarrow \; p=0 \; \lightning \end{array}$$

$\square$

Warning $X^2+Y^2-1=(X+Y+1)^2$ if $\mathrm{char}(K)=2$.

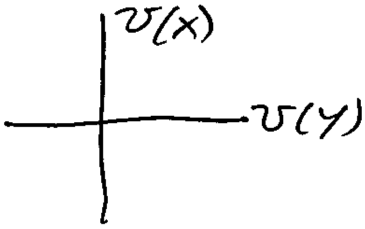
Thm 5.4 Let $V \subseteq k^n$ be algebraic. Then:

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 $i \neq j$.

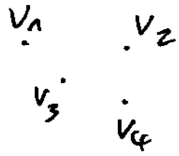
b) This decomposition is unique. The sets $V_1, \dots, V_m$ are called the irreducible components of V.

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

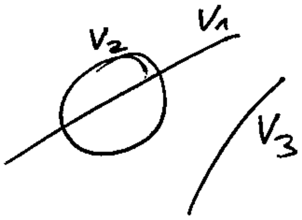
Ex $\mathcal{V}(X)$ and $\mathcal{V}(Y)$ are the irreducible components of $\mathcal{V}(XY)$.



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

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

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

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

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

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

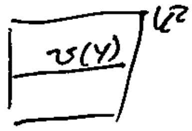
$\Longrightarrow i = k \Longrightarrow V_i \subseteq W_j \subseteq V_i \Rightarrow V_i = W_j$ ↯ $\qquad \square$

6. Coordinate rings

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

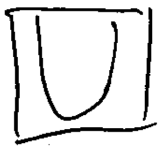
<u>Ex</u> $\Gamma(K^n) = K[X_1, \dots, X_n]$

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



$$X \mapsto X$$
$$Y \mapsto 0$$

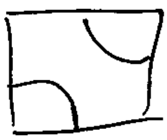
<u>Ex</u> $\Gamma(\mathcal{V}(X^2 - Y)) = K[X,Y]/(X^2-Y) \cong K[X]$



$$X \mapsto X$$
$$Y \; (=X^2) \mapsto X^2$$

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

$$X \mapsto X$$
$$Y \mapsto \tfrac{1}{X}$$



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

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.

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

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: $g_1 \equiv g_2 \mod I(V)$). $\square$

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.

$$\begin{aligned} \Gamma(W) &\longrightarrow \Gamma(V) \\ f &\longmapsto f|_V \\ f \bmod \mathcal{I}(W) &\longmapsto f \bmod \mathcal{I}(V) \quad (\mathcal{I}(V) \supseteq \mathcal{I}(W)) \end{aligned}$$

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 $\Gamma(V) = K[x_1, \dots, x_n]/\mathcal{I}(V)$ correspond to ideals I' of $K[x_1, \dots, x_n]$ containing $\mathcal{I}(V)$.

Rmk 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

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

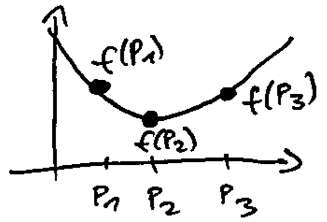
Pf Let $I_i = \mathcal{I}(V_i)$.

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

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

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

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

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

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

Cor 6.4 a) If $V \subseteq K^n$ is finite, then $\dim_{K\text{-vector space}}(\Gamma(V)) = |V|$.

b) If $V \subseteq K^n$ is infinite, then — " — $= \infty$.

Pf a) $\Gamma(V) = \{f : V \to K\} \cong K^{|V|}$

b) If $P_1, \dots, P_m$ are distinct points in V, then we get a surjection

$$\begin{array}{ccc} \Gamma(V) & \twoheadrightarrow & \Gamma(\{P_1, \dots, P_m\}) \\ f & \longmapsto & f|_{\{P_1, \dots, P_m\}} \end{array}$$

m-dimensional.

$\square$

7. Morphisms

Def Let $V \subseteq K^n$ and $W \subseteq K^m$ be algebraic subsets.

A <u>morphism</u> (= <u>regular map</u> = <u>polynomial map</u>)

$\varphi : V \to W$ is a map $V \to W$ which is given by

polynomials: There exist $f_1, \dots, f_m \in K[X_1, \dots, X_n]$

such that $\varphi(P) = (f_1(P), \dots, f_m(P)) \in W \quad \forall P \in V$.

Ex $f : K \longrightarrow V(X^2 - Y) \subseteq K^2$
$x \longmapsto (x, x^2)$

Ex A projection $K^n \longrightarrow K$.
$(a_1, \dots, a_n) \mapsto a_i$

Ex The identity $id : V \to V$.

Ex An inclusion $V \hookrightarrow W$, where $V \subseteq W$.

Rmk If $\varphi : A \to B$ and $\psi : B \to C$ are morphisms, then the composition $\psi \circ \varphi : A \to C$ is a morphism.

Rmk Morphisms $\varphi : \underset{\subseteq K^n}{V} \longrightarrow K^m$ correspond exactly to tuples $(f_1, \dots, f_m)$ of functions $f_i \in \Gamma(V)$.
$(f_i : V_i \to K)$

In particular, morphisms $\varphi : V \to K$ correspond exactly to functions $f \in \Gamma(V)$.

How to tell whether the image of $\varphi : V \overset{\subseteq K^n}{\longrightarrow} K^m$ is contained in W?

(corr. to $f_1, \dots, f_n$)

<u>Lemma 7.1</u> $\varphi(V) \subseteq W$ if and only if

$$h(f_1(x_1, \dots, x_n), \dots, f_m(x_1, \dots, x_n)) \in I(V)$$

for all $h \in I(W)$ if φ corr. to pol. $f_1, \dots, f_m \in K[x_1, \dots, x_n]$.

<u>Pf</u> $\varphi(P) \in W = V(I(W)) \quad \forall P \in V$

$$\iff \underset{\substack{\| \\ h(f_1(P), \dots, f_m(P))}}{h(\varphi(P))} = 0 \quad \forall h \in I(W),\ P \in V$$

$$\iff h(f_1, \dots, f_m) \in I(V) \quad \forall h \in I(W).$$

$\square$

<u>Def</u> For any morphism $\varphi : V \to W$, its <u>pullback function</u> is the K-algebra homomorphism

$$\begin{aligned} \varphi^* : \Gamma(W) &\longrightarrow \Gamma(V). \\ f &\longmapsto f \circ \varphi \end{aligned}$$

$$\begin{tikzcd} V \arrow[rr, "\varphi"] \arrow[dr, dashed, "f \circ \varphi = \varphi^*(f)"'] & & W \arrow[dl, "f"] \\ & K & \end{tikzcd}$$

(Sometimes, φ^* is denoted by $\tilde{\varphi}$ instead.)

[redacted]

Other description: If $\varphi = (f_1, \dots, f_m)$

$$\varphi^* : K[Y_1, \dots, Y_m]/J(W) \longrightarrow K[X_1, \dots, X_n]/J(V)$$

$$[g(Y_1, \dots, Y_m)] \longmapsto [\, g(f_1(X_1, \dots, X_n), \dots, f_m(X_1, \dots, X_n))]$$

Thm 7.2 We get a bijection

$$\{\text{morphisms } V \to W\} \longleftrightarrow \{K\text{-alg. hom. } \Gamma(W) \to \Gamma(V)\}.$$

$$\varphi \longmapsto \varphi^*$$

Pf How to determine φ from φ^*?

Let $Y_i \in \Gamma(W)$ be the function mapping any point in $W \subseteq K^m$ to its i-th coordinate.

Then, $\varphi(P) = (Y_1(\varphi(P)), \dots, Y_m(\varphi(P)))$

$$= (\underbrace{\varphi^*(Y_1)}(P), \dots, \underbrace{\varphi^*(Y_m)}(P))$$

The m elements of $\Gamma(V)$ defining the morphism φ. $\square$

Ex $\varphi : K \longrightarrow V(X^2 - Y)$

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

$$\varphi^* : \Gamma(V(X^2 - Y)) \longrightarrow \Gamma(K) = K[T]$$

$$X \longmapsto T$$

$$Y \longmapsto T^2$$

Rmk a) $id: V \to V$ corresponds to $id: \Gamma(V) \to \Gamma(V)$.

b) $(\psi \circ \varphi)^* = \varphi^* \circ \psi^*$

$$\begin{tikzcd} A \arrow[r, "\varphi"] \arrow[dr, dashed, "\varphi^* \circ \psi^*(f)"'] & B \arrow[r, "\psi"] \arrow[d, dashed, "\psi^*(f)"] & C \arrow[dl, "f"] \\ & K & \end{tikzcd}$$

Rmk Hence,

$$\left\{ \begin{array}{l} \text{alg. subsets of } K^n \\ \text{for some } n \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{fin. gen.} \\ \text{reduced} \\ K\text{-algebra} \end{array} \right\}$$

$$V \longmapsto \Gamma(V) = K[x_1, \ldots, x_n]/J(V)$$

$$\varphi \longmapsto \varphi^*$$

is a contravariant equivalence of categories.

Def A morphism $\varphi: V \to W$ is an <u>isomorphism</u> if it has an inverse morphism $\psi: W \to V$ (with $\varphi \circ \psi = id_W$, $\psi \circ \varphi = id_V$).

Rmk $\varphi: V \to W$ is an isomorphism if and only if $\varphi^*: \Gamma(W) \to \Gamma(V)$ is an isomorphism.

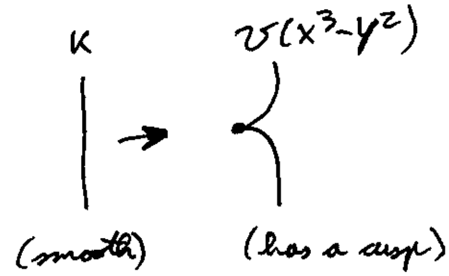
Ex The inverse of
$$K \longrightarrow V(x^2 - y)$$
$$x \longmapsto (x, x^2)$$
is
$$x \longleftarrow (x, y).$$

Ex Any translation in K^n is an isomorphism.

Ex Any invertible linear map $K^n \to K^n$ is an isomorphism.

<u>Warning</u> Not every bijective morphism is an isomorphism!
(Just like not every bijective continuous map is a homeomorphism.)

<u>Ex</u> $\varphi : K \longrightarrow V(x^3-y^2) \subseteq K^2$
$\quad t \longmapsto (t^2, t^3)$



is a bijection

~~Because $\frac{y}{x} \mapsto (x,y)$ iff $x^3-y^2=0$ and $(x,y)\neq 0$~~
~~and $0 \mapsto (0,0)$~~

with inverse map

$$\frac{y}{x} \longleftarrow\!\shortmid (x,y) \neq (0,0),$$
$$0 \longleftarrow\!\shortmid (0,0).$$

It is not an isomorphism because

$$\begin{aligned} \varphi^* : \Gamma(V(x^3-y^2)) &\longrightarrow \Gamma(K) = K[X] \\ X &\longmapsto T^2 \\ Y &\longmapsto T^3 \end{aligned}$$

isn't a isomorphism because T is not contained in the image.

Thm 7.3 Any morphism $\varphi: V \subseteq k^n \longrightarrow W \subseteq k^m$ is continuous (w.r.t. the Zariski topologies).

Pf For any ideal $J \subseteq \Gamma(W)$,

$$\varphi^{-1}\big(\underbrace{\mathcal{V}_W(J)}_{\substack{\text{closed}\\ \text{subset}\\ \text{of } W}}\big) = \{P \in V \mid \underbrace{\varphi(P) \in \mathcal{V}_W(J)}\} = \underbrace{\mathcal{V}_V(\varphi^*(J))}_{\substack{\text{closed}\\ \text{subset}\\ \text{of } V}}$$

$$\Updownarrow$$

$$f(\varphi(P)) = 0 \ \forall f \in J$$

$$\Updownarrow$$

$$\varphi^*(f)(P) = 0 \ \forall f \in J$$

$$\Updownarrow$$

$$P \in \mathcal{V}_V(\varphi^*(J))$$

$\square$

Thm 7.4 $\varphi^*: \Gamma(W) \longrightarrow \Gamma(V)$ is injective if and only if $\varphi(V)$ is (Zariski) dense in W.

Def Such a morphism is called <u>dominant</u>.

Pf Let $V \subseteq k^n$ and $W \subseteq k^m$.

φ^* injective

$\Longleftrightarrow \forall f \in \Gamma(W)$: if $\underset{f\circ\varphi}{\underset{\|}{\varphi^*(f)}} = \underset{(\text{on } V)}{0}$, then $f = \underset{(\text{on } W)}{0}$.

$$\Updownarrow$$

$$f = 0 \text{ on } \varphi(V)$$

$\Longleftrightarrow \mathcal{J}_W(\varphi(V)) = 0$

$$\|$$

$$\mathcal{J}_W(\overline{\varphi(V)})$$

$\Longleftrightarrow \overline{\varphi(V)} = W$.

$\uparrow$ bijection $\{\text{alg. subset of } W\} \longleftrightarrow \{\text{radical ideal of } \Gamma(W)\}$

$\square$

Ex $\varphi : \mathcal{V}(XY-1) \longrightarrow K$
$(x,y) \longmapsto x$

has image $K \setminus \{0\}$. $\Rightarrow \varphi$ is dominant

$\varphi^* : K[T] \longrightarrow K[X,Y]/(XY-1) \cong K[X, \tfrac{1}{X}]$
$T \longmapsto X$

is injective.

Rmk The composition of two dominant morphisms is dominant.

Thm 7.5 $\varphi^*: \Gamma(W) \to \Gamma(V)$ is surjective if and only if $\varphi(V) \subseteq W$ is an algebraic subset and $\varphi: V \to \varphi(V)$ is an isomorphism. (φ is an isom. onto its image)

Pf Let $I = \ker(\varphi^*) \subseteq \Gamma(W)$.

Let $W' = \mathcal{V}_W(I) \subseteq W$. Then, $\varphi(V) \subseteq W'$.

Note that I is a radical ideal of $\Gamma(W)$ because $\Gamma(V)$ is a reduced ring.

$\Rightarrow \Gamma(W') = \Gamma(W)/I$.

~~We have an isomorphism $\varphi^*: \Gamma(W)/I \to \Gamma(V)$, $\Gamma(W')$~~

~~which corresponds to φ:~~

The morphism $\varphi: V \to W'$ corr. to the injective ring hom. $\varphi^*: \underset{\Gamma(W')}{\underset{\parallel}{\Gamma(W)/I}} \longrightarrow \Gamma(V)$.

$\Rightarrow$ By Thm 7.4, we have $\overline{\varphi(V)} = W'$.

If φ^* is surjective, this map $\varphi: V \to W'$ is an isomorphism (in part. $\varphi(V) = W'$).

If $\varphi(V) \subseteq W$ is an alg. subset ($\Rightarrow W' = \varphi(V)$) and $\varphi: V \to \varphi(V)$ is an isom., then $\varphi^*: \Gamma(W') \to \Gamma(V)$ is an isom., in particular surjective. $\square$

<u>Exe</u> $\varphi : K \longrightarrow K^2$ is an isomorphism onto its image $V(X^2-Y)$

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

with inverse map

$x \leftarrow\!\shortmid (x, y)$.

$\varphi^* : K[X,Y] \longrightarrow K[T]$ is surjective.

$X \longmapsto T$

$Y \longmapsto T^2$

8. Gröbner bases

References:

- Sturmfels: What is a Gröbner basis?
- Cox, Little, O'Shea: Ideals, Varieties, and Algorithms (Chapter 2)

Question

How to determine whether a polynomial h lies in an ideal $I = (f_1, \dots, f_m) \subseteq K[x_1, \dots, x_n]$?

<u>Ex</u> If $n = 1$, we can compute $g := \gcd(f_1, \dots, f_m)$ using the Euclidean algorithm. Then, $I = (f_1, \dots, f_m) = (g)$, so $h \in I \iff g \mid h$.

<u>Ex</u> If the polynomials $f_1, \dots, f_m$ have degree ≤ 1, use Gaussian elimination to put the equations into row echelon form.

Def Let $\mathcal{S} := \mathcal{S}(X_1,\dots,X_n) = \{X_1^{e_1}\cdots X_n^{e_n} \mid e_1,\dots,e_n \geq 0\}$ be the set of monomials in $X_1,\dots,X_n$.

A <u>monomial order</u> is a total order $\leq$ on $\mathcal{S}$ such that:

a) $1 \leq M \quad \forall M \in \mathcal{S}$

b) If $M \leq N$, then $MU \leq NU \quad \forall U \in \mathcal{S}$.

Rmk Some people omit condition a), which ensures that $\leq$ is a <u>well-order</u>: every $\emptyset \neq T \subseteq \mathcal{S}$ has a smallest element.

Ex If $n=1$, there is just one monomial order:

$$1 < X_1 < X_1^2 < X_1^3 < \dots$$

Ex <u>lexicographic order</u>

$$X_1^{a_1}\cdots X_n^{a_n} < X_1^{b_1}\cdots X_n^{b_n}$$

$\iff (a_1,\dots,a_n) < (b_1,\dots,b_n)$ lexicographically

$\iff a_1 = b_1, \dots, a_{i-1} = b_{i-1},\ a_i < b_i$ for some $1 \leq i \leq n$.

$$1 < X_2 < X_2^2 < X_2^3 < \dots < X_1 < X_1X_2 < X_1X_2^2 < \dots < X_1^2 < \dots$$

Ex <u>Degree lexicographic order</u>

...

$\Longleftrightarrow (a_1+\dots+a_n, a_1, \dots, a_n) < (b_1+\dots+b_n, b_1, \dots, b_n)$
lexicographically

$$1 < X_2 < X_1 < X_2^2 < X_1X_2 < X_1^2 < X_2^3 < \dots$$

Ex <u>Degree reverse lexicographic order</u>

...

$\Longleftrightarrow (a_1+\dots+a_n, -a_n, \dots, -a_1) < (b_1+\dots+b_n, -b_n, \dots, -b_1)$
lexicographically

<u>Rmk</u> For $n=2$, deg. lex. = deg. rev. lex.

<u>Def</u> Let $f = \sum_{M \in S} c_M M \in K[X_1, \dots, X_n]$.

A monomial M <u>occurs in</u> f if $c_M \neq 0$.

Let $f \neq 0$.

Its <u>leading monomial</u> (w.r.t. $\leq$) is

$$\mathrm{lm}(f) := \max\{M \text{ occuring in } f\}.$$

Its <u>leading coefficient</u> (w.r.t. $\leq$) is

$$\mathrm{lc}(f) = c_{\mathrm{lm}(f)}.$$

Its <u>leading term</u> (w.r.t. $\leq$) is

$$\mathrm{lt}(f) = \mathrm{lc}(f) \cdot \mathrm{lm}(f).$$

Rmk $\mathrm{lm}(fg) = \mathrm{lm}(f)\cdot \mathrm{lm}(g)$ for any $f,g \neq 0$.
$\quad\ \mathrm{lt} \qquad\qquad \mathrm{lt} \qquad \mathrm{lt}$
$\quad\ \mathrm{lc} \qquad\qquad \mathrm{lc} \qquad \mathrm{lc}$

Def A polynomial $f \in K[X_1,\dots,X_n]$ is reduced w.r.t. a subset $G \subseteq K[X_1,\dots,X_n]$ if no monomial M occurring in f is divisible by the leading monomial of any $0 \neq g \in G$.

Ex X^3 is reduced w.r.t. $\{Y, XY+1\}$.

$X^2Y^3 + X^5$ isn't reduced w.r.t. $\{\underline{X^3}+Y\}$ and deg. lex. ordering.

(or any other order!)

Rmk For $f = \sum_M c_M M$, let

$$W(f) = \{ M : c_M \neq 0 \text{ and } \mathrm{lm}(g) \mid M \text{ for some } 0 \neq g \in G \}.$$

If $W(f) \neq \emptyset$, let $N^{(1)} = \max(W(f))$, $\mathrm{lm}(g) \mid N^{(1)}$, $0 \neq g \in G$.

Consider $f^{(1)} := f - \dfrac{c_{N^{(1)}} N^{(1)}}{\mathrm{lt}(g)} \cdot g$.

Then $M < N^{(1)}$ $\forall M \in W(f^{(1)})$.

Continue this process

$$(f \rightsquigarrow f^{(1)} \rightsquigarrow f^{(2)} \rightsquigarrow \dots)$$
$$N^{(1)} > N^{(2)} > N^{(3)} > \dots$$

Since $\leq$ is a well-order, this process has to terminate with some $f^{(k)}$ which is reduced w.r.t. G.

<u>Def</u> A <u>reduction</u> of f w.r.t. G is a polynomial r, which is reduced w.r.t. G and such that

$$r = f - g_1 h_1 - \dots - g_r h_r$$

for some $g_1, \dots, g_r \in G$, $h_1, \dots, h_r \in k[X_1, \dots, X_n]$ with $lm(g_i h_i) \leq lm(f)$.

<u>Rmk</u> $r \equiv f \bmod \underbrace{(G)}_{\text{ideal generated by } G}$.

<u>Ex</u> Use lex. order on $S(X,Y)$.

$f = XY^2 + 1$, $\quad G = \{XY+1, Y+1\}$

$f^{(1)} = XY^2 + 1 - Y(XY+1) = -Y+1$

$r = f^{(2)} = -Y+1+Y+1 = 2$

<u>or</u>: $f^{(1)} = XY^2+1 - XY(Y+1) = -XY+1$

$r = f^{(2)} = -XY+1+X(Y+1) = X+1$

$\rightsquigarrow$ <u>Warning</u>: Reductions aren't always unique!

~~**Warning** Reductions aren't always unique!~~

~~**Ex** Use lex. order on~~ $\cancel{S(X,Y)}$

$$\cancel{f = X^{2}Y^2, \qquad G = \{XY^2,\ X^2Y+1\}}$$

$$\cancel{r = f^{(1)} = X^2Y^2 - X\cdot XY^2 = 0}$$

~~**or**~~ $\cancel{r = f^{(1)} = X^2Y^2 - Y\cdot(X^2Y+1) = -Y}$

Def A Gröbner basis of an ideal I w.r.t. $\leq$ is a subset $G \subseteq I$ such that

$$\operatorname{lm}(I) = \{M : N \mid M \text{ for some } N \in \operatorname{lm}(G)\}.$$

Rmk "$\supseteq$" holds for any subset $G \subseteq I$.

Ex I is a Gröbner basis of I.

Ex $\{f\}$ is a Gröbner basis of (f) for any polynomial f.

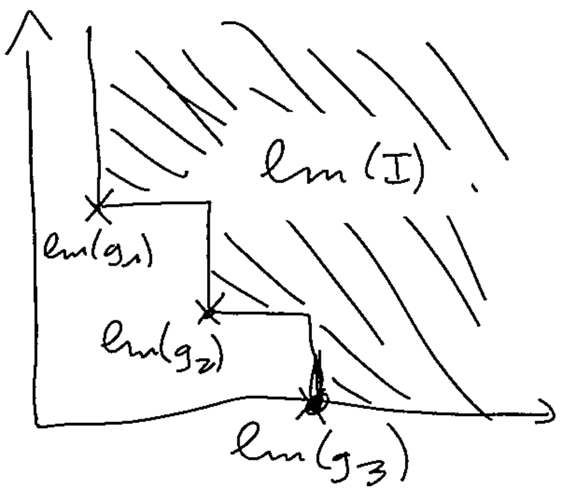
Rmk Let $A \subseteq S$. A monomial M is divisible by an element of A if and only if it is contained in the ideal (A) generated by the elements of A.

Cor 8.1 Any ideal $I \subseteq K[X_1,\dots,X_n]$ has a finite Gröbner basis.

Pf By Hilbert's Basis Theorem, the ideal $(\mathrm{lm}(I))$ is generated by finitely many elements $\mathrm{lm}(g_1),\dots,\mathrm{lm}(g_r)$ $(0\neq g_1,\dots,g_r\in I)$. Take $G=\{g_1,\dots,g_r\}$. $\square$

Picture ($n=2$)

$M = X^a Y^b$



Thm 8.[redacted]2 The monomials $M \notin lm(I)$ form a basis of the K-vector space $K[x_1,\dots,x_n]/I$.

Pf generators:

consider any $f \in K[x_1,\dots,x_n]$.
Let r be any reduction w.r.t. I.
$\Rightarrow r$ is a linear combination of monomials $M \notin lm(I)$.

linearly independent:

The leading monomial of any nonzero linear combination f of monomials $M \notin lm(I)$ is $lm(f) \notin lm(I)$.
$\Rightarrow f \notin I$. $\square$

Cor 8.[redacted]3 $\dim_K(K[x_1,\dots,x_n]/I) = \#(S \setminus lm(I))$.

Rmk Recall that $\# V(I) \le \dim_K(\dots)$!

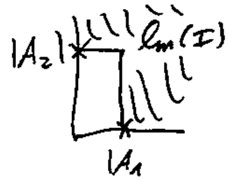
~~Thm 8.[redacted]5 Reduction w.r.t. a Gröbner basis is always unique.~~

~~Pf Let $r_1 \neq r_2$ be reductions of f w.r.t. G.~~
~~$\Rightarrow r_1 \equiv r_2 \bmod I$. $\Rightarrow r_1 - r_2 \in I$~~
~~$\Rightarrow lm(r_1 - r_2) \in lm(I)$.~~
~~$\Rightarrow r_1$ or r_2 isn't reduced w.r.t. G!~~ ~~$\square$~~

Cor 8.4 (Combinatorial Nullstellensatz)

Let $A_1, \dots, A_n \subseteq K$ be finite sets,

$V = A_1 \times \dots \times A_n \subset K^n$.



Then, $X_1^{e_1} \cdots X_n^{e_n}$ is a standard monomial for $I = \mathcal{J}(V)$ if and only if

$$0 \le e_1 < |A_1| \ , \ \dots, \ 0 \le e_n < |A_n|. \qquad (I)$$

Pf $f_i = \prod_{a \in A_i} (X_i - a)$ lies in I and has leading monomial $X_i^{|A_i|}$.

$\Rightarrow$ Every standard monomial satisfies (I).

There are $|V|$ standard mon., but only $|A_1| \cdots |A_n| = |V|$ mon. satisfy (I).

$\Rightarrow$ All of them are standard. $\square$

Thm 8.5 Reductions w.r.t. Gröbner bases are always unique.

Pf Let $r_1 \neq r_2$ be reductions of f w.r.t. G.

$\Rightarrow r_1 \equiv r_2 \mod I$. $\Rightarrow r_1 - r_2 \in I$

$\Rightarrow \mathrm{lm}(r_1 - r_2) \in \mathrm{lm}(I)$

$\Rightarrow r_1$ and r_2 can't both be reduced w.r.t. G. ↯ $\square$

Cor 8.6 Let G be a Gröbner basis of I. Then, $f \in I$ if and only if its reduction w.r.t. G is 0.

Pf Any reduction $r \equiv f \bmod I$ is a linear combination of monomials $M \notin lm(I)$. Then, $r \in I$ if and only if $r = 0$. $\square$

Cor 8.7 Any Gröbner basis G of I generates I.

Pf

If $f \in I$, then $0 \underset{\substack{\uparrow \\ f \in I}}{=} r \equiv f \bmod (G)$, so $f \in (G)$. $\square$

Thm 8.8 (Buchberger's Criterion)

A set G is a Gröbner basis for $I := (G)$ if and only if for all $0 \neq f, g \in G$, some/every reduction of

$$S(f,g) = \frac{M}{lt(f)} \cdot f - \frac{M}{lt(g)} \cdot g \text{ w.r.t. to } G$$

is 0, where $M = lcm(lm(f), lm(g))$.

Note: $lt\left(\frac{M}{lt(f)} \cdot f\right) = M = lt\left(\frac{M}{lt(g)} \cdot g\right)$, so the leading terms cancel.

Pf "$\Rightarrow$" Apply Cor 8.6 to $S(f,g) \in I$.

"$\Leftarrow$" Let $0 \neq f \in I$. Write

$$f = \lambda_1 g_1 H_1 + \dots + \lambda_r g_r H_r \qquad (I)$$

with $0 \neq g_i \in G$ and monomials $H_i \in S$ with $\lambda_i \in K^\times$

minimal $M := \max_{1 \le i \le r} (\mathrm{lm}(g_i H_i))$.

Clearly $\mathrm{lm}(f) \le M$.

If $\mathrm{lm}(f) = M$, then $\mathrm{lm}(f) = \mathrm{lm}(g_i H_i)$

$= \mathrm{lm}(g_i) \cdot H_i$,

so $\mathrm{lm}(f)$ is divisible by the leading mon. of an element of G.

Assume $\mathrm{lm}(f) < M$.

$\Rightarrow$ the monomial M has to cancel in the RHS of (I).

w.l.o.g. $\mathrm{lm}(g_i H_i) = M$ for $i = 1, \dots, t$

$\mathrm{lm}(g_i H_i) < M$ for $i = t+1, \dots, r$

$$\Rightarrow \sum_{i=1}^{t} \lambda_i \, \mathrm{lc}(g_i) = 0. \quad (\text{in part., } t \ge 2)$$

By assumption, we can write

$$\frac{M}{\mathrm{lcm}(\mathrm{lm}(g_i), \mathrm{lm}(g_1))} \cdot S(g_i, g_1) = \frac{M}{\mathrm{lt}(g_i)} \cdot g_i - \frac{M}{\mathrm{lt}(g_1)} \cdot g_1$$

$$= \sum_j p_j^{(i)} \cdot q_j^{(i)}$$

with $0 \neq p_j^{(i)} \in G$ and $q_j^{(i)} \in K[x_1, \dots, x_n]$,

and $\mathrm{lm}\left(p_j^{(i)} \cdot q_j^{(i)}\right) \leq \mathrm{lm}\left(\frac{M}{\mathrm{lt}(g_i)} g_i - \frac{M}{\mathrm{lt}(g_1)} \cdot g_1\right)$

$< M$.

$$\Rightarrow g_i H_i = \frac{\mathrm{lt}(g_i) H_i}{M} \cdot \sum p_j^{(i)} q_j^{(i)} + \frac{\mathrm{lt}(g_i) H_i H_1}{\mathrm{lt}(g_1) H_1} \cdot g_1 \qquad \text{for } i = 1, \dots, t$$

$$= \mathrm{lc}(g_i H_i) \cdot \sum p_j^{(i)} q_j^{(i)} + \frac{\mathrm{lc}(g_i) H_1}{\mathrm{lc}(g_1)} \cdot g_1$$

$$\Rightarrow \lambda_1 g_1 H_1 + \dots + \lambda_t g_t H_t$$

$$= \sum_{i=1}^{t} \underbrace{\lambda_i \mathrm{lc}(g_i H_i)}_{\in K} \cdot \underbrace{\sum \overbrace{p_j^{(i)}}^{\in G} q_j^{(i)}}_{\mathrm{lm}(\cdot) < M} + \underbrace{\sum_{i=1}^{t} \frac{\lambda_i \mathrm{lc}(g_i)}{\mathrm{lc}(g_1)}}_{0} \cdot g_1 H_1$$

$\Rightarrow$ We can rewrite f as a sum as in (I)

with smaller $M = \max\limits_{1 \leq i \leq r} (\mathrm{lm}(g_i H_i))$. $\lightning$

$\square$

<u>Similar to:</u>

$\{(a_1, \dots, a_n) \mid a_1 + \dots + a_n = 0\}$ is spanned by

$e_i - e_j$ for $1 \leq i, j \leq n$.

Buchberger's Algorithm

We can compute a finite Gröbner basis of $I = (f_1, \dots, f_m)$ as follows:

Construct sets
$$F = G_0, \quad G_1, \quad G_2, \dots$$
of polynomials generating I such that
$$(\operatorname{lm}(G_0)) \subsetneq (\operatorname{lm}(G_1)) \subsetneq (\operatorname{lm}(G_2)) \subsetneq \cdots$$

If G_k fails Buchbergers Criterion, there is a reduction $r \neq 0$ of some $S(g_1, g_2)$ with $g_1, g_2 \in G_k$ (w.r.t. G_k).

$\Rightarrow$ $\operatorname{lm}(r)$ is not divisible by any element of $\operatorname{lm}(G_k)$.

Take $G_{k+1} = G_k \cup \{r\}$.

$\Rightarrow$ $(\operatorname{lm}(G_{k+1})) \supsetneq (\operatorname{lm}(G_k))$.

By Hilbert's Basis Theorem, this process terminates after a finite number of steps.

<u>Rmk</u> You can also after each step replace any elements g of G_k by its reduction w.r.t. $G_k \setminus \{g\}$, one polynomial g at a time.

Ex $I = (XY^2, X^2Y+1)$, lex. order

$f_1 = XY^2$ $\quad G_0 = \{f_1, f_2\}$

$f_2 = X^2Y+1$

$r = S(f_1, f_2) = X\cdot f_1 - Y\cdot f_2 = -Y$

is reduced w.r.t. $\{f_1, f_2\}$.

$G_1 = \{\cancel{f_1}, f_2, r\}$

$f_2 + X^2\cdot r = 1$

$G_1' = \{1\}$.

is a gröbner basis

Ex $I = (X^3-2XY, X^2Y-2Y^2+X)$, deg. lex. order

$f_1 = X^3 - 2XY$

$f_2 = X^2Y - 2Y^2 + X$

$r = S(f_1, f_2) = Y\cdot f_1 - X\cdot f_2 = -2XY^2 + 2XY^2 - X^2$

$= -X^2$

is reduced w.r.t. $\{f_1, f_2\}$

$G_1 = \{f_1, f_2, r\}$

$f_1' = f_1 + X\cdot r = -2XY$

$G_1' = \{f_1', f_2, r\}$

$f_2' = f_2 + Y\cdot r = -2Y^2 + X$

$G_1'' = \{f_1', f_2', r\}$

$$S(f_1', f_2') = Y \cdot f_1' - X \cdot f_2' = -X^2$$

reduces to 0 w.r.t. $\{f_1', f_2', r\}$

$$S(f_1', r) = X \cdot f_1' - 2Y \cdot r = 0$$

$$S(f_2', r) = X^2 \cdot f_2' - 2Y^2 \cdot r = X^3$$

reduces to 0 w.r.t. $\{f_1', f_2', r\}$

$\Rightarrow$ $\{f_1', f_2', r\}$ is a Gröbner basis.
$= \{-2XY, -2Y^2+X, -X^2\}$

In particular, $I \neq (1)$, so $V(I) \neq \emptyset$.

Often, deg. rev. lex. order is faster than lex. order.

9. Rational functions

Let $V \subseteq K^n$ be an irreducible alg. set.

Recall that $\Gamma(V)$ is an integral domain.

Def The *field of rational functions* on V is the field of fractions $K(V)$ of $\Gamma(V)$. Formally:

the set of equivalence classes of pairs (a,b) with $a, b \in \Gamma(V)$, $b \neq 0$, where $(a,b) \sim (a',b')$ if $ab' = a'b$. (A pair (a,b) corr. to the fraction $\frac{a}{b}$.)

$K(V) = \{ \frac{a}{b} \mid a, b \in \Gamma(V), \underbrace{b \neq 0}_{\text{not everywhere } 0 \text{ on } V} \}$

Ex $V = K^n \rightsquigarrow K(V) = K(x_1, \dots, x_n)$

Ex A $V = \mathcal{V}(XY - Z^2) \subset K^3$

Note that $\frac{X}{Z} = \frac{Z}{Y}$ in $K(V)$ because $XY = Z^2$ in $\Gamma(V)$.

Def A rational function $f \in K(V)$ is *defined at* $P \in V$ if $f = \frac{a}{b}$ for some $a, b \in \Gamma(V)$ with $b(P) \neq 0$.

In this case, we write $f(P) = \frac{a(P)}{b(P)} \in K$.

(Note: The value $f(P)$ doesn't depend on the choice of a, b.)

Ex A $f = \frac{X}{Z} = \frac{Z}{Y}$ is defined at all points $(x,y,z) \in V$ with $z \neq 0$ or $y \neq 0$.

Rmk If $f = \frac{a}{b}$ for some $a, b \in \Gamma(V)$ with $a(P) \neq 0$ and $b(P) = 0$, then f is not defined at P.

Pf Assume $\frac{a}{b} = \frac{a'}{b'}$ with $b'(P) \neq 0$. Then,

$$\underbrace{a(P)}_{\neq 0}\underbrace{b'(P)}_{\neq 0} = a'(P)\underbrace{b(P)}_{=0}. \quad \text{↯} \qquad \square$$

Ex A $f = \frac{x}{z} = \frac{z}{y}$ is not defined at $(x,0,0) \in V$ for any $x \neq 0$.

Lemma 9.1 The set of points $P \in V$ at which $f \in K_V$ is not defined is closed.
Equivalently, the set $U_f \subseteq V$ of points at which f is defined is open (w.r.t. the subspace top. on V).
Also, $U_f \neq \emptyset$.

Pf Write $f = \frac{a}{b}$. Since $b \neq 0$ as a fct. on V, it is not zero everywhere on V. $\Rightarrow U_f \neq \emptyset$.

$$\{P \in V \mid f \text{ not def. at } P\} = \bigcap_{\substack{a, b \in \Gamma(V): \\ f = \frac{a}{b}}} \underbrace{V_V(b)}_{\text{closed}} \quad \text{is closed.}$$

$\square$

Ex A f is not defined at $(0,0,0)$, which lies in the closure of $\{(x,0,0) \mid x \neq 0\}$.

For $K = \mathbb{C}$, for example, the limit of $f(P)$ as $P \to (0,0,0)$ can depend on the path!

$$\begin{array}{ccc} P \doteq (t,t,t) \in V & \rightsquigarrow & f(P) = \dfrac{t}{t} = 1 \\ \Big\downarrow \; t \to 0 & & \Big\downarrow \\ (0,0,0) & & 1 \end{array}$$

$$\begin{array}{ccc} P \doteq (t^{3/2}, t^{1/2}, t) \in V & \rightsquigarrow & f(P) = \dfrac{t^{3/2}}{t} = t^{1/2} \\ \Big\downarrow \; t \to 0 & & \Big\downarrow \\ (0,0,0) & & 0 \end{array}$$

$\Rightarrow$ no cont. ext. to $(0,0,0)$

<u>Summary:</u> Any $f \in K(V)$ gives rise to a map $f : U_f \to K$.

<u>Lemma 9.2</u> If $f \in K(V)$ is zero on a nonempty open subset $U \subseteq U_f$, then $f = 0$.

<u>Pf</u> Write $f = \frac{a}{b}$. For any $P \in U$, we have $b(P) = 0$ or $a(P) = 0$.

$$\Rightarrow V = (V \setminus U) \cup \mathcal{V}_V(b) \cup \mathcal{V}_V(a)$$

closed

Since V is irreducible, this implies $\mathcal{V}_V(a) = V$, so $a = 0$. $\square$

<u>Cor 9.3</u> If $f, g \in K(V)$ agree on a nonempty open subset $U \subseteq U_f \cap U_g$, then $f = g$.

<u>Rmk</u> This is similar to a fact from complex analysis: If two meromorphic functions on a connected region U agree on a nonempty open subset $U' \subseteq U$, they agree on U.

<u>Cor 9.4</u> The elements of $K(V)$ correspond bijectively to equiv. classes of pairs (U, f) with $\emptyset \neq U \subseteq V$ open and $f : U \to K$ any map which is locally given by a quotient of regular functions

(i.e.: $\forall P \in U \ \exists P \in U' \subseteq U$ open, $a, b \in \Gamma(V)$:
$$\forall Q \in U' : b(Q) \neq 0, \ f(Q) = \frac{a(Q)}{b(Q)}. \text{)},$$

where we identify $(U, f), (U', f')$ if $f|_{U \cap U'} = f'|_{U \cap U'}$.

(Recall that the intersection of two nonempty open subsets of an irred. set is nonempty!)

Rmk If $\varphi: V \to W$ is a dominant morphism, we obtain an injective ring hom.

$$\varphi^*: \Gamma(W) \to \Gamma(V)$$
$$f \mapsto f \circ \varphi$$

which induces a field hom.

$$\varphi^*: K(W) \longrightarrow K(V)$$
$$\frac{a}{b} \longmapsto \frac{\varphi^*(a)}{\varphi^*(b)}$$
$$f \mapsto f \circ \varphi$$

Rmk Dominance of φ is important:
Otherwise, f might not be defined at any point in $\varphi(V)$, so $f \circ \varphi$ might not be defined anywhere!
(Or: $\varphi^*(b)$ might be 0 for $b \neq 0$.
$\Rightarrow \varphi^*(\frac{1}{b}) = \frac{1}{\varphi^*(b)}$ undefined.)

Rmk $\quad U_{\varphi^*(f)} \supseteq \varphi^{-1}(U_f) \neq \emptyset$

open subset of V

Def For any open subset $\emptyset \neq U \subseteq V$, let $\mathcal{O}_V(U)$ be the ring (!) of rational functions $f \in K(V)$ defined at every point in U.
For $U = \emptyset$, let $\mathcal{O}_V(U) = 1$, the one-element ring.

Rmk Elements of $\mathcal{O}_V(U)$ correspond to functions $f: U \to K$ which are (locally) given by a quotient of regular functions.

Rmk If $\varphi: V \to W$ is any morphism between alg. sets and $U \subseteq W$ is any open subset, we obtain a ring hom.

$$\varphi^*: \mathcal{O}_W(U) \longrightarrow \mathcal{O}_V(\varphi^{-1}(U)).$$

Def Let $V \subseteq K^n$ and $W \subseteq K^m$ be alg. subsets and let V be irreducible.
A rational map $\varphi: V \dashrightarrow W$ is a map $U \longrightarrow W$ for an open subset U of V which is given by m rational functions $f_1, \dots, f_m$ defined on U, where we identify two such maps $U_1 \to W$, $U_2 \to W$ if they agree on the (nonempty) intersection $U_1 \cap U_2$.

Ex
$$K^3 \longrightarrow K^2$$
$$(x,y,z) \longmapsto \left(\frac{x}{y+z^2}, \frac{1}{z}\right)$$

Ex
$$\mathcal{V}(X^3 - Y^2) \longrightarrow K$$
$$(x,y) \longmapsto \frac{y}{x}$$

Ex Any morphism $V \to W$.

Ex A rat. map $V \dashrightarrow K^m$ is the same as m rational functions on V.

Def A rat. map $\varphi : V \dashrightarrow W$ is *dominant* if $\overline{\varphi(U)} = W$ for any/every open $\emptyset \neq U \subseteq V$ where φ is defined.

Rmk If $\varphi : A \dashrightarrow B$ and $\psi : B \dashrightarrow C$ are rat. maps, and φ is dominant, we get a rat. map
$\psi \circ \varphi : A \dashrightarrow C$.

In particular: If $\varphi : V \dashrightarrow W$ is dominant, we get a field hom. $\varphi^* : K(W) \to K(V)$.

$$\begin{aligned} \varphi^* : K(W) &\to K(V) \\ f &\mapsto f \circ \varphi \end{aligned}$$

Rmk We get a bijection

$$\left\{ \begin{matrix} \text{dominant} \\ \text{rational} \\ \text{map} \\ V \dashrightarrow W \end{matrix} \right\} \longleftrightarrow \left\{ \begin{matrix} K\text{-algebra} \\ \text{hom.} \\ K(W) \to K(V) \end{matrix} \right\}.$$

Pf Same as for morphisms:
$f_i = \varphi^*(x_i)$, where $x_i \in \Gamma(W) \subseteq K(W)$ is the i-th coordinate map. $\square$

irreducible alg. sets

Def V, W are <u>birational</u> if there are dominant rational maps $\varphi: V \dashrightarrow W$ and $\psi: W \dashrightarrow V$ with $\psi \circ \varphi = id_V$ and $\varphi \circ \psi = id_W$.

Ex K and $\mathcal{V}(x^3-y^2) \subset K^2$ are not isomorphic (Problem 1d on Pset 4), but are birational:

$$\varphi: K \longrightarrow \mathcal{V}(x^3-y^2)$$
$$t \mapsto (t^2, t^3)$$

$$\psi: \mathcal{V}(x^3-y^2) \dashrightarrow K$$
$$(x,y) \mapsto \frac{y}{x} \quad (\text{def. on } \mathcal{V}(x^3-y^2) \setminus \{(0,0)\})$$

Rmk V, W are birational if and only if the K-algebras $K(V)$, $K(W)$ are isomorphic.

10. Dimension and transcendence degree

<u>Def</u> Let $L|K$ be a field extension.
Elements $a_1, \dots, a_n \in L$ are <u>algebraically dependent</u> over K if there is a pol. $0 \neq f \in K[X_1, \dots, X_n]$ such that $f(a_1, \dots, a_n) = 0$.

<u>Rmk</u> For $n=1$, this is equiv. to a_1 being algebraic over K.

<u>Ex</u> $X_1, \dots, X_n \in K(X_1, \dots, X_n)$ are alg. independent over K.

<u>Ex</u> $X, Y \in K(V(X^3 - Y^2))$ are alg. dep. because $X^3 - Y^2 = 0$ in $K(V(X^3 - Y^2))$.

<u>Ex</u> π, e are transcendental over $\mathbb{Q}$.
It is unknown whether π, e are alg. indep. over $\mathbb{Q}$.

<u>Thm 10.1</u> $a_1, \dots, a_n \in L$ are alg. dep. if and only if some a_i is alg. over $K(a_1, \dots, a_{i-1})$.

<u>Analogy</u> Let V be a K-vector space.
$v_1, \dots, v_n \in V$ are linearly dep. if and only if some v_i is a lin. comb. of $v_1, \dots, v_{i-1}$.

Pf "$\Leftarrow$" ~~...~~ a_i alg. over $K(a_1,\dots,a_{i-1})$

$\Rightarrow f(a_i)=0$ for some $0\neq f\in K(a_1,\dots,a_{i-1})[X]$.

Each coeff. of f is the quotient of two pol. in $a_1,\dots,a_{i-1}$ with coeff. in K.

We can clear out denominators so the coeff. are pol. in $a_1,\dots,a_{i-1}$.

"$\Rightarrow$" Let ~~...~~ $f(a_1,\dots,a_n)=0$ for some $0\neq f\in K[X_1,\dots,X_n]$.

Let $g(X_n)=f(a_1,\dots,a_{n-1},X_n)$. $(\Rightarrow g(a_n)=0)$

<u>Case 1:</u> $g\in K[X_n]$ is not the zero pol.

$\Rightarrow a_n$ is alg. over K

<u>Case 2:</u> $g\in K[X_n]$ is the zero pol.

Write $f=\sum_i f_i(X_1,\dots,X_{n-1})\cdot X_n^i$. Some $f_m\neq 0$.

$\Rightarrow 0=g(X_n)=\sum_i f(a_1,\dots,a_{n-1})\cdot X_n^i$. $\Rightarrow f_m(a_1,\dots,a_{n-1})=0$.

$\Rightarrow a_1,\dots,a_{n-1}$ are alg. dep.

Proceed by induction over n. $\square$

Def Elements $a_1, \ldots, a_n \in L$ form a transcendence basis of L over K if they are alg. indep. and L is an alg. ext. of $K(a_1, \ldots, a_n)$.

Rmk A transcendence basis is a maximal list of alg. indep. el. of K (a list to which we can't append any el. of L without destroying algebraic independence).

Ex $X_1, \ldots, X_n$ is a tr. basis of $K(X_1, \ldots, X_n)$ over K.

Lemma 10.2 ("Exchange lemma")

If $a_1, \ldots, a_n \in L$ are alg. indep. and L is alg. over $K(b_1, \ldots, b_m)$ (with $b_1, \ldots, b_m \in L$), then there are indices $1 \le i_1 < \ldots < i_r \le m$ $(r \geq 0)$ such that $a_1, \ldots, a_n, b_{i_1}, \ldots, b_{i_r}$ form a transcendence basis of L over K.

Pf Choose any max. alg. indep. sublist of $a_1, \ldots, a_n, b_1, \ldots, b_m$ containing $a_1, \ldots, a_n$. The remaining b_j are alg. over K (this list) $=: F$.

$\Rightarrow K(a_1, \ldots, a_n, b_1, \ldots, b_m)$ is alg. over F

Also, L is alg. over $K(b_1, \ldots, b_m) \subseteq K(a_1, \ldots, a_n, b_1, \ldots, b_m)$.

$\Rightarrow L$ is alg. over F. $\Rightarrow$ The list forms a tr. basis. $\square$

Cor 10.3 Any finitely generated field ext. has a (finite) tr. basis.

Thm 10.4 If $a_1, \dots, a_n$ is a tr. basis of L over K and $b_1, \dots, b_m \in L$ are alg. indep., then $n \geq m$.

Analogy If $v_1, \dots, v_n$ span V and $w_1, \dots, w_m \in V$ are lin. indep., then $n \geq m$.

Cor 10.5 Any two tr. bases of L over K have the same size, called the transcendence degree of L over K.

$\operatorname{trdeg}(L|K)$

Rmk $\operatorname{trdeg}(L|K) = 0 \iff L$ is an alg. ext. of K.

Ex $\operatorname{trdeg}(K(x_1, \dots, x_n)|K) = n$.

Pf of Thm 10.4   Use ind. over n.

$n=0$: $\Rightarrow L$ is alg. over K

$\Rightarrow$ There are no alg. indep. el.

$\Rightarrow m=0$.

$n-1 \to n$: ~~Use~~ By the exchange lemma, b_1 together with some of the a_i form a tr. basis of L over K.

W.l.o.g. $b_1, a_1, \ldots, a_r$ do.

We have $r<n$ because $a_1, \ldots, a_n$ already form a tr. basis, so b_1 is alg. over $K(a_1, \ldots, a_n)$.

Now, $a_1, \ldots, a_r$ form a tr. basis of L over $K(b_1)$.

Also, $b_2, \ldots, b_m \in L$ are alg. indep. over $K(b_1)$.

The ind. hypothesis shows that $\underset{\substack{\wedge\!| \\ n-1}}{r} \geq m-1$.

$\Rightarrow n \geq m$. $\square$

__Ex__ X is a tr. basis of $K(\mathcal{V}(X^3-Y^2))$. $\Rightarrow$ ~~tr~~deg $= 1$.

(~~So~~ is Y.)

~~Pf No pol. $f(X)$ lies in $\mathcal{I}(\mathcal{V}(X^3-Y^2))$, for example~~

__Pf__ No pol. $f(X)$ vanishes at every pt. in $\mathcal{V}(X^3-Y^2)$.

$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \ni (t^2, t^3)$

$\Rightarrow X$ is alg. indep.

$\underbrace{Y}_{\in K(\mathcal{V}(X^3-Y^2))}$ is alg. over $K(X) \subset K(\mathcal{V}(X^3-Y^2))$.

$\Rightarrow K(\mathcal{V}(X^3-Y^2))$ is alg. over $K(X)$.

gen. by X, Y.

$\square$

Thm 10.6 If L is a fin. gen. field ext. of K and M is a fin. gen. field ext. of L, then
$$\operatorname{trdeg}(M|K) = \operatorname{trdeg}(M|L) + \operatorname{trdeg}(L|K).$$

$$\begin{array}{c} M \\ | \\ L \\ | \\ K \end{array}$$

Ex ~~trdeg~~ $L = K(x_1, \dots, x_n)$

$$M = L(Y_1, \dots, Y_m) = K(x_1, \dots, x_n, Y_1, \dots, Y_m).$$

Pf If $a_1, \dots, a_n$ is a tr. basis of $L|K$

and $b_1, \dots, b_m$ ... $M|L$,

then $a_1, \dots, a_n, b_1, \dots, b_m$ ... $M|K$:

alg. indep.: follows from Thm 10.1

M alg. over $K(a_1, \dots, a_n, b_1, \dots, b_m)$:

The alg. closure of $K(a_1, \dots, a_n, b_1, \dots, b_m)$ in M contains L and $b_1, \dots, b_m$, hence contains $L(b_1, \dots, b_m)$, hence contains the alg. cl. of $L(b_1, \dots, b_m)$, which is M.

$\square$

Def The <u>dimension</u> of an irred. alg. set $V \subseteq K^n$ is $\dim(V) = \operatorname{trdeg}(K(V)|K)$.

Ex $\dim(K^n) = n$

Cor K^n, K^m are not isomorphic (or even birational) unless $n = m$.

Analogy $\mathbb{R}^n, \mathbb{R}^m$ are not homeomorphic unless $n=m$.
More generally, nonempty open subsets $U \subseteq \mathbb{R}^n$, $V \subseteq \mathbb{R}^m$ are not homeomorphic unless $n=m$.
(These facts are nontrivial!)

Thm 10.7 The dimension of an irred. alg. subset $V = \mathcal{V}(f) \subsetneq K^n$ def. by a single (irred.) pol. $0 \neq f \in K[X_1, \dots, X_n]$ is $\dim(V) = n-1$.

Pf w.l.o.g. the variable X_n occurs in f.
Then, $x_1, \dots, x_{n-1}$ form a tr. basis of $K(V)$ over K:
No pol. $g(x_1, \dots, x_{n-1})$ lies in $(f) = \mathcal{I}(V)$.
x_n is alg. over $x_1, \dots, x_{n-1}$ in $K(V)$ because it satisfies the nonzero pol. eq. $f(x_1, \dots, x_{n-1}, x_n) = 0$ in $K(V)$.

$\square$

Def The <u>dimension</u> of a reducible alg. set V with irred. components $V_1, \dots, V_m$ is
$$\dim(V) = \max(\dim(V_1), \dots, \dim(V_m)).$$
The empty set has dimension
$$\dim(\emptyset) = -\infty.$$

Ex $V = \{(0,y) \mid y \in K\} \cup \{(1,2)\}$ has dimension 1.

Thm 10.8 An alg. subset $\emptyset \neq V \subseteq K^n$ has dimension 0 if and only if $|V| < \infty$.

Pf W.l.o.g. V is irreducible.

"$\Leftarrow$" $|V| < \infty$, V irred. $\Rightarrow \underset{\text{(one-point set)}}{|V| = 1} \Rightarrow \Gamma(V) = K$
$\Rightarrow K(V) = K$, which has trdeg $= 0$.

"$\Rightarrow$" $\dim(V) = 0 \Rightarrow K(V)$ is an alg. ext. of K
$\underset{\text{K alg. cl.}}{\Rightarrow} K(V) = K \Rightarrow \Gamma(V) = K \Rightarrow J(V)$ max. ideal of $K[X_1, \dots, X_n]$
$\Rightarrow |V| = 1$.

$\square$

<u>Lemma 10.9</u> If V, W are alg. sets and

a) there is a dominant morphism $\varphi: V \to W$ or

b) V is irred. and there is a dom. rat. map $\varphi: V \dashrightarrow W$,

then $\dim(V) \geq \dim(W)$.

<u>Pf</u> Decompose V, W into irred. comp.:

$V = V_1 \cup \dots \cup V_a$, $\quad W = W_1 \cup \dots \cup W_b$.

$$W = \overline{\varphi(V)} = \bigcup_{i=1}^{a} \overline{\varphi(V_i)}$$

$$\Rightarrow \underbrace{W_j}_{\text{irred.}} = \bigcup_i \underbrace{(\overline{\varphi(V_i)} \cap W_j)}_{\text{closed}} \qquad \forall j$$

$\Rightarrow W_j = \overline{\varphi(V_{r_j})} \cap W_j$ for some r_j.

$\Rightarrow W_j \subseteq \overline{\varphi(V_{r_j})}$

Since $\overline{\varphi(V_{r_j})} \subseteq W$ is irred., it is contained in some W_{s_j}.

$\Rightarrow W_j \subseteq \overline{\varphi(V_{r_j})} \subseteq W_{s_j}$

$\Rightarrow j = s_j$, $W_j = \overline{\varphi(V_{r_j})}$

$\Rightarrow$ We obtain dom. rat. maps $\varphi: V_{r_j} \dashrightarrow W_j$,

so can assume w.l.o.g. that V, W are irred.

We then have a K-alg. hom. $\varphi^*: K(W) \hookrightarrow K(V)$.

If $a_1, \dots, a_d$ is a tr. basis of $K(W)$, then $\varphi^*(a_1), \dots, \varphi^*(a_d) \in K(V)$

are still alg. indep.

$\square$

Lemma 10.10 If $V \subseteq W$, then $\dim(V) \leq \dim(W)$.

Pf w.l.o.g. V is irred. (replace V by an irred. comp.)
w.l.o.g. W is irred. (replace W by an irred. comp. containing V)
The inclusion $i: V \hookrightarrow W$ induces a surjective ring hom. $i^*: \Gamma(W) \longrightarrow \Gamma(V)$

$$f \longmapsto f \circ i = f|_V$$

Since the el. of $\Gamma(V)$ generate the field ext. $K(V)$ of K, by Lemma 10.2, there are elements $a_1, \dots, a_d \in \Gamma(V)$ which form a tr. basis of $K(V)$.
Pick any preimages $b_1, \dots, b_d \in \Gamma(W)$ (ext. to W).
They are ~~...~~ alg. independent because their restrictions to V are.

$a_1, \dots, a_d$

$\square$

Thm 10.11 Let $V \subseteq K^n$ be an irred. alg. set.
Then, $\dim(V)$ is the largest number $d \geq 0$ such that there is a dom. rat. map $\varphi: V \dashrightarrow K^d$.

Pf Rat. maps $V \dashrightarrow K^n$ corr. to ~~tuples~~ $(f_1, \dots, f_d)$ of rat. functions $f_1, \dots, f_d \in K(V)$.

Such a rat. map is dominant if and only if the hom. $K[X_1, \dots, X_d] \longrightarrow K(V)$ is injective.
$x_i \longmapsto f_i$

That's equiv. to the alg. independence of $f_1, \dots, f_d$. $\square$

10.12

Rmk ~~[illegible]~~ There is in fact a dominant morphism $V \subseteq K^n \longrightarrow K^d$ for $d = \dim(V)$. Actually, there is a dominant <u>projection</u> $V \longrightarrow K^d$ onto a d-dimensional linear subspace H of K^n spanned by coordinate vectors!

Ex $n=2, d=1$: $\Rightarrow$ proj. onto x- or y-axis is dominant

$n=2, d=2$ $\Rightarrow$ The map $V \longrightarrow K^2$ is dominant

$$\Rightarrow \overline{V} = K^2 \underset{V \text{ closed}}{\Longrightarrow} V = K^2$$

$n=3, d=2$ $\Rightarrow$ proj. onto xy- or xz- or yz-plane is dominant

Pf W.l.o.g. V is irred.

The field ext. $K(V)$ of K is generated by $X_1, \dots, X_n$. $\Longrightarrow$ There is a transcendence basis of the form $X_{i_1}, \dots, X_{i_d}$. Then, the projection

$$\pi : V \longrightarrow K^d \quad (x_1, \dots, x_n) \longmapsto (x_{i_1}, \dots, x_{i_d})$$

is dominant because

$$\pi^* : K[Y_1, \dots, Y_d] = \Gamma(K^d) \longrightarrow \Gamma(V), \quad Y_j \longmapsto X_{i_j}$$

is injective because $X_{i_1}, \dots, X_{i_d}$ are algebraically independent over K. $\square$

11. Finite Morphisms

Thm 11.1. Let $f \in K[x_1,\dots,x_n]$

and consider the projection $\pi : V(f) \longrightarrow K^{n-1}$

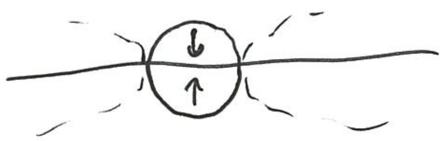
$$(a_1,\dots,a_n) \longmapsto (a_1,\dots,a_{n-1})$$

If f is monic of degree $d \geq 1$ as a pol. in x_n with coeff. in $K[x_1,\dots,x_{n-1}]$, then each $P \in K^{n-1}$ has at least one and at most d preimages $Q \in V(f)$ under the projection map.

Ex: $\pi : V(\underbrace{x^2+y^2-1}_{\text{monic of deg. 2 in } y}) \longrightarrow K$

$$(x,y) \longmapsto x$$

$$\pi^{-1}(t) = \underbrace{\{(t, \pm\sqrt{1-t^2})\}}_{\text{1 or 2 points}}$$



Exe B $\pi : \underbrace{\mathcal{V}(XY-1)}_{\text{not monic in } Y} \longrightarrow K$

$(x,y) \longmapsto x$

$\pi^{-1}(t) = \{(t, \frac{1}{t})\}$ for $t \neq 0$

$\pi^{-1}(0) = \emptyset$

Exe C $\pi : \mathcal{V}(\underbrace{XY}_{\substack{\text{not} \\ \text{monic} \\ \text{in } X}}) \longrightarrow K$

$(x,y) \longmapsto x$

$\pi^{-1}(t) = \{(t,0)\}$ for $t \neq 0$

$\pi^{-1}(0) = \{(0,y) \mid y \in K\}$

Pf of ~~[illegible]~~ Thm 11.1 Write $f(x_1,\dots,x_n) = \sum_{i=0}^{d} f_i(x_1,\dots,x_{n-1}) X^i$

with $f_d = 1$.

Let $(a_1,\dots,a_{d-1}) \in K^{n-1}$.

Then, $(a_1,\dots,a_d) \in \mathcal{V}(f)$ if and only if a_d is a root of the monic pol. $f(a_1,\dots,a_{n-1}, X) = \sum_{i=0}^{d} f_i(a_1,\dots,a_{n-1}) X^i$ of degree d. Such a pol. has ≥ 1 and $\leq d$ roots. $\square$

Def A morphism $\varphi : V \to W$ is finite if the ring ext. $\Gamma(V)$ of $\varphi^*(\Gamma(W))$ is module-finite. $\varphi^* : \Gamma(W) \to \Gamma(V)$

Ex A $\quad \pi^* : k[T] \longrightarrow k[X,Y]/(X^2+Y^2-1)$.

$$T \mapsto X$$

$k[X,Y]/(X^2+Y^2-1)$ is mod-fin. over $k[X]$ because it is the subring gen. by Y as a ring ext. and Y is int. over $k[X]$.

More generally:

Rmk For f, π as in Rmk 11.1, π is finite.

Pf $k[X_1, \dots, X_n]/(f)$ is gen. by X_n, which is int. over the subring $k[X_1, \dots, X_{n-1}]$ because $\sum_{i=0}^{d} f_i(X_1, \dots, X_{n-1}) X_n^i$ is a mon. eq. satisfied by X_n. $\square$

Ex B, C $\quad \pi$ is not finite.

Ex D $\varphi : K^2 \longrightarrow K^2$ is not finite:
$(x,y) \longmapsto (x, xy)$

Y is not integral over $K[X, XY]$.

~~[illegible]~~

~~$1, Y, Y^2, \dots$ are lin. indep. [illegible] over $K[X, XY]$~~

Ex If $V \subseteq W$, then the inclusion morphism $V \hookrightarrow W$ is finite (because $\Gamma(W) \to \Gamma(V)$ is surjective).

Rmk The composition of two fin. morphisms is finite.

Pf This follows from the transitivity of module-finiteness. $\square$

Rmk The restriction of a finite morphism $V \to W$ to V' is finite. (It's the composition $V' \hookrightarrow V \to W$.)

Rmk ~~[illegible]~~ $\varphi : V \to \underset{K^m}{\overset{\cap}{W}}$ is finite if and only if

$\varphi : V \to K^m$ is finite.

Pf ~~[illegible]~~ $\varphi^*(\Gamma(W)) = \varphi^*(\Gamma(K^m))$. $\square$

Thm 11.2 If $\varphi: V \to W$ is a dominant finite morphism, then $\dim(V) = \dim(W)$.

Pf As in the pf of Lemma 10.9, w.l.o.g. V, W are irreducible.

dominant $\Rightarrow \varphi^*: \Gamma(W) \to \Gamma(V)$ injective, we have a hom.

$$\varphi^*: K(W) \hookrightarrow K(V).$$

finite $\Rightarrow$ $\Gamma(V)$ int. ext. of $\Gamma(W)$ (or rather $\varphi^*(\Gamma(W))$)

$\Rightarrow$ $K(V)$ alg. ext. of $K(W)$ (or rather $\varphi^*(K(W))$)

$$\Rightarrow \underbrace{\operatorname{trdeg}(K(V)|K)}_{\dim(V)} = \underbrace{\operatorname{trdeg}(K(W)|K)}_{\dim(W)} \qquad \square$$

Cor 11.3 Let $\varphi: V \to W$ be a finite morphism. Then, any point $Q \in W$ has only finitely many preimages $P \in V$.

Pf Assume it has at least one.

$\Rightarrow \varphi|_{\varphi^{-1}(Q)}: \underbrace{\varphi^{-1}(Q)}_{\{P \in V : \varphi(P) = Q\}} \to \{Q\}$ is a finite surjective morphism
(⇒ dominant)

$$\Rightarrow \dim(\varphi^{-1}(Q)) = \dim(\{Q\}) = 0. \qquad \square$$

[Another proof, we showed for the special case of Thm 11.1:]

Thm 11.4 (lying over property)

Any dominant finite morphism $\varphi: V \to W$ is surjective.

Pf Let $Q \in W$ and let $m := I_W(\{Q\})$ be the corr. maximal ideal of $\Gamma(W)$.

Then, $\varphi^{-1}(Q) = V_V(\varphi^*(m))$. Goal: $\varphi^{-1}(Q) \neq \emptyset$.

Let $I = (\varphi^*(m))$ be the ideal of $\Gamma(V)$ generated by the el. of $\varphi^*(m)$.

By Hilbert's Nsts, it suffices to show that $I \neq \Gamma(V)$.

Assume $I = \Gamma(V)$.

~~Since $\Gamma(V)$ is a fin~~

φ finite $\Rightarrow$ $\Gamma(V)$ fin. gen. as $\varphi^*(\Gamma(W))$-mod.

Let $b_1, \dots, b_r \in \Gamma(V)$ be generators.

$\Rightarrow$ Every el. of $\Gamma(V)$ is a lin. comb. of $b_1, \dots, b_r$ with coeff. in $\varphi^*(\Gamma(W))$.

Every el. of I is a lin. comb. of el. of $\varphi^*(m)$ with coeff. in $\Gamma(V)$.

$\Rightarrow$ — " — of el. of the form

$$\varphi^*(\underset{\substack{\cap\\ m}}{p})\, b_i\, \varphi^*(\underset{\substack{\cap\\ \Gamma(W)}}{q}) = \varphi^*(\underbrace{pq}_{\in m})\, b_i .$$

Recall that $I = \Gamma(V) \ni b_i$.

Write $b_i = \sum_j \varphi^*(p_{ij}) b_j$ with $p_{ij} \in \varphi^*(m)$.

$\Rightarrow$ $Mv = v$ for $M = (\varphi^*(p_{ij}))_{i,j}$, $v = (b_i)_i$.

$\Rightarrow$ $(\underbrace{Id}_{\text{id. matrix}} - M)v = 0$

$\underset{\text{as in the pf of ...}}{\Rightarrow}$ $\det(Id - M) = 0$

The entries of M lie in $\varphi^*(m)$.

$\underset{\text{expand the det}}{\Rightarrow}$ $\underbrace{\det(Id - M)}_{=0} - 1 \in \varphi^*(m)$

$\Rightarrow 1 \in \varphi^*(m)$.

$\underset{\varphi \text{ dom.} \Rightarrow \varphi^* \text{ inj}}{\Rightarrow}$ $1 \in m$. ↯

$\square$

<u>Cor 11.5</u> Any finite morphism $\varphi: V \to W$ is <u>closed</u>:

The image $\varphi(A) \subseteq W$ of every closed set $A \subseteq V$ is closed.

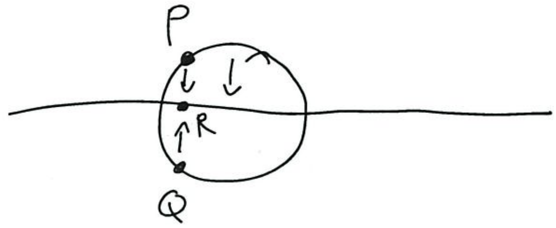
<u>Ex</u> The proj. $K^2 \to K$ is <u>not</u> closed because the image of $V(XY-1)$ is $K \setminus \{0\}$, which is not closed.

<u>Pf</u> $\varphi: A \to \overline{\varphi(A)}$ is a dominant finite morphism, hence finite. $\Rightarrow \varphi(A) = \overline{\varphi(A)} \Rightarrow \varphi(A)$ is closed. $\square$

Lemma 11.6 (Incomparability)

Let $\varphi : V \to W$ be a finite morphism and let $V_1 \subsetneqq V_2 \subseteq V$ be alg. subsets with V_2 irreducible. Then $\varphi(V_1) \subsetneqq \varphi(V_2) \subseteq W$.

Rmk This can fail if V_2 is reducible:



$V_1 = \{P\} \rightsquigarrow \varphi(V_1) = \{R\}$

$V_2 = \{P, Q\} \rightsquigarrow \varphi(V_2) = \{R\}$

Rmk We'll soon show that $V_1 \subsetneqq V_2$, V_2 irreducible implies that

$$\begin{array}{ccc} \dim(V_1) & < & \dim(V_2) \\ \shortparallel & & \shortparallel \\ \dim(\varphi(V_1)) & & \dim(\varphi(V_2)) \end{array}$$

Pf W.l.o.g. $V = V_2$, $\varphi(V) = W$.

Let $0 \neq f \in \Gamma(V)$ with $f|_{V_1} = 0$.

Since $\Gamma(V)$ is an integral ext. of $\varphi^*(\Gamma(W))$, there is a monic polynomial equation

$$f^n + \varphi^*(c_{n-1}) f^{n-1} + \dots + \varphi^*(c_0) = 0 \qquad (I)$$

with $c_{n-1}, \dots, c_0 \in \Gamma(W)$. Pick one of smallest possible degree n.

$f|_{V_1} = 0 \underset{(I)}{\Longrightarrow} \varphi^*(c_0)\big|_{V_1} = 0.$ $\cancel{-f^n - \varphi^*(c_{n-1}) f^{n-1} - \dots - \varphi^*(c_1) f|_{V_1} = 0.}$

$\Rightarrow \varphi(V_1) \subseteq \mathcal{V}_W(c_0)$.

$\Rightarrow$ If $\varphi(V_1) = W$, then $c_0 = 0$.

$\Rightarrow f^{n-1} + \varphi^*(c_{n-1}) f^{n-2} + \dots + \varphi^*(c_0) = 0$,

contradicting the minimality of n.

$f \neq 0$ and $\Gamma(V)$ is an integral domain because V is irreducible

$\square$

Thm 11.7 (Noether Normalisation)

Let $V \subseteq K^m$ be an irred. alg. set of dimension n.

Then, there is a <u>finite</u> morphism $\pi : V \to K^n$.

In fact, there is a finite linear projection onto K^n.

~~Pf surjectivity follows automatically~~

Rmk Any such morphism is surjective.

Pf of Rmk $\pi(V) \subseteq k^n$ is closed because π is finite. (Cor 11.5).

$\dim(\pi(V)) = \dim(V) = n$ by Thm 11.2.

If $\pi(V) \subseteq \mathcal{V}(f)$ for some $0 \neq f \in k[X_1, \ldots, X_n]$, Then

$$\dim(\pi(V)) \underset{\substack{\uparrow \\ \text{Lemma 10.10}}}{\leq} \dim(\mathcal{V}(f)) \underset{\substack{\uparrow \\ \text{Thm 10.7}}}{=} n-1 \quad \text{↯}.$$

$\Rightarrow \pi(V) = k^n$. $\square$

~~14. Noether normalization~~

~~Thm 14.1 Let V be an irred. alg. set of dimension n~~
~~Then, there is a finite morphism $\pi: V \to K^n$.~~
~~In fact, there is such a projection onto an n-dimensional linear subspace of K^m.~~

~~INSERT (*)~~

Exe The proj. of $V = \mathcal{V}(XY-1)$ onto the x-axis (or the y-axis) is dominant, but not surjective (hence not finite). However, the proj.

$$\pi: V \to K \quad (x,y) \mapsto x+y$$ is surjective:

The preimages of $t \in K$ are the points (x,y) with $x^2 - tx + 1 = 0$ and $y = t - x$.

In fact, it's finite because

$$X^2 - \pi^*(T)X + 1 = 0$$

and

$$Y^2 - \pi^*(T)Y + 1 = 0$$

in $\Gamma(V)$.

Pf of Thm 11.7: We have $n = \dim(V) \leq \dim(K^m) = m$.
We use induction over $m-n$.
If $n = m$, we're done. (Take $\pi = \mathrm{id}$.)

Assume $m \geq n+1$.

~~It suffices to construct a~~

~~We use induction~~

~~Let's construct a fin. mor~~

It suffices to construct a fin. proj. $\pi_1 : \overset{K^m}{\overset{\cup\!\!|}{V}} \longrightarrow K^{m-1}$:
$\Rightarrow \dim(\pi(V)) = \dim(V) = n$.
By ind., there is then a fin. proj. $\pi_2 : \pi(V) \to K^n$.
Then we can take $\pi := \pi_2 \circ \pi_1$.

To construct π_1:
Observe that $V \subsetneq K^m$, so there is a pol.
$0 \neq f \in K[X_1, \dots, X_m]$ which vanishes on V:
$f(x_1, \dots, x_m) = 0$ in $\Gamma(V)$.

Consider a proj. $\pi_1 : K^m \longrightarrow K^{m-1}$ of the form
$(a_1, \dots, a_m) \longmapsto (a_1 - c_1 a_m, \dots, a_{m-1} - c_{m-1} a_m)$
with $c_1, \dots, c_{m-1} \in K$.

Its pullback map is

$$\pi_1^* : K[Y_1, \dots, Y_{m-1}] \longrightarrow K[X_1, \dots, X_m]$$
$$Y_i \longmapsto X_i - c_i X_m .$$

In $\Gamma(V)$, we have ~~can write~~

$$0 = f(X_1, \dots, X_m) = f(X_1 - c_1 X_m + c_1 X_m, \dots, X_{m-1} - c_{m-1} X_m + c_{m-1} X_m, X_m)$$
$$= f(\pi_1^*(Y_1) + c_1 X_m, \dots, \pi_1^*(Y_{m-1}) + c_{m-1} X_m, X_m).$$

The RHS is a pol. in X_m with coeff. in $\pi_1^*(\Gamma(K^{m-1}))$.

(after expanding)

If the pol. f has degree d, then the RHS has degree $\leq d$.

The X_m^d-coeff. of the right-hand side lies in K.
[and depends on $c_1, \dots, c_{m-1}$.]
It is a nonzero pol. in $c_1, \dots, c_{m-1}$:

If $f = \sum r_{i_1 \cdots i_m} X_1^{i_1} \cdots X_m^{i_m}$, then

the X_m^d-coeff. is $\sum\limits_{\substack{i_1, \dots, i_m: \\ i_1 + \dots + i_m = d}} r_{i_1 \cdots i_m} c_1^{i_1} \cdots c_{m-1}^{i_{m-1}}$ (one of these is $\neq 0$ because $\deg(f) = d$)

(the hom. degree d part of f at $(c_1, \dots, c_{m-1}, 1)$).

$\Rightarrow$ By the Nichtnullstellensatz, there are values $c_1, \dots, c_{m-1} \in K$ such that the X_m^d-coeff.$^{\in K}$ is $\neq 0$.

Dividing by this coeff. gives us a monic pol. eq. for X_m in $\Gamma(V)$ with coeff. in $\pi_1^*(\Gamma(K^{m-1}))$.

$\Rightarrow X_m$ is int. over $\pi_1^*(\Gamma(K^{m-1}))$.

$\Rightarrow X_i$ — —

($X_i - c_i X_m \in \pi_1^*(\Gamma(\dots))$) $\Rightarrow \Gamma(V)$ is int. over $\pi_1^*(\Gamma(K^{m-1}))$. $\square$

Rmk In the Nichtnullstellensatz, we used that K is infinite. There is a generalisation to finite fields that instead of a projection uses a map of the form

$$(a_1, \dots, a_m) \mapsto (a_1 - a_m^{d_1}, \dots, a_{m-1} - a_m^{d_{m-1}})$$

for suitable $d_1, \dots, d_{m-1} \geq 0$.

integers

Cor 11.8 $\dim(V\times W) = \dim(V) + \dim(W)$

Pf Decompose $V = V_1 \cup \dots \cup V_a$,
$W = W_1 \cup \dots \cup W_b$.

Then, $V \times W = \bigcup_{i,j} \underbrace{(V_i \times W_j)}_{\text{irred.}}$.

$\Rightarrow \dim(V\times W) = \max_{i,j}(\dim(V_i \times W_j))$

and $\max_i(\dim(V_i)) + \max_j(\dim(W_j))$
$= \dim(V) + \dim(W)$.

$\Rightarrow$ We can assume that V, W are irreducible.

Let $n = \dim(V)$, $m = \dim(W)$.

$\Rightarrow$ There are surj. fin. morphisms

$\pi: V \to K^n$, $\rho: W \to K^m$.

Claim: $\sigma: V\times W \to K^n \times K^m = K^{n+m}$ is surj. and finite.
$(v, w) \mapsto (\pi(v), \rho(w))$

Pf surj.: clear
fin.: $\Gamma(V) = K[A_1, \dots, A_k]/I$ int. ext. of $\pi^*(K[X_1, \dots, X_n])$
$\Gamma(W) = K[B_1, \dots, B_l]/J$ int. ext. of $\rho^*(K[Y_1, \dots, Y_m])$.
$\Rightarrow \Gamma(V\times W) = K[A_1, \dots, A_k, B_1, \dots, B_l]/(I+J)$ int. ext. of
$\sigma^*(K[X_1, \dots, X_n, Y_1, \dots, Y_m])$.

$\Rightarrow \dim(V \times W) = n+m$. $\square$

12. Going down theorem

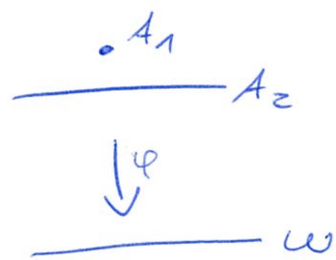
<u>Reminder</u> Let $\varphi: V \to W$ be a surjective finite morphism and let B be an irred. subset of W.
Decompose $\varphi^{-1}(B)$ into irred. comp.:

$$\varphi^{-1}(B) = A_1 \cup \dots \cup A_r.$$

Then, $\varphi(A_i) = B$ for <u>some</u> component A_i

<u>Rmk</u> We might not have $\varphi(A_i) = B$ for <u>all</u> components A_i.

<u>Ex</u> $V = \mathcal{V}(y) \cup \{(0,1)\}$



$W = K$

$\varphi: V \to K$, $(x,y) \mapsto x$ is finite because its restrictions to A_1, A_2 are.

$$V = \varphi^{-1}(W) = \underset{\substack{\text{im} = \{0\} \\ \neq W}}{A_1} \cup \underset{\text{im} = W}{A_2}$$

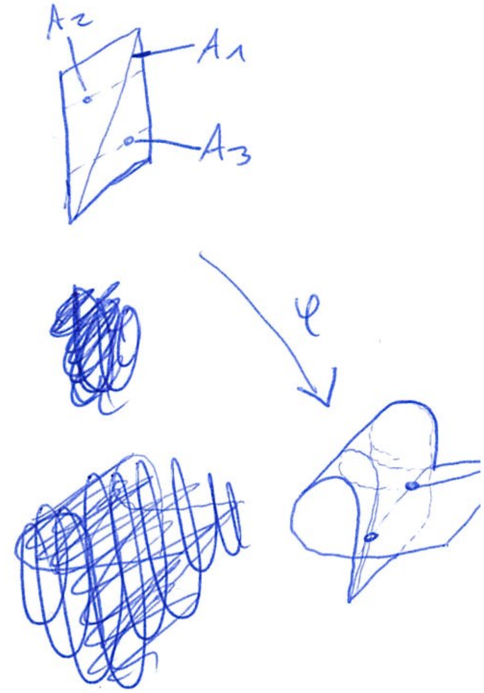
Cause: V not irreducible

Es $V = K^2$

$W = \mathcal{V}(x^2(x+1) - y^2)$

$\varphi : V \longrightarrow W$

$(t,u) \longmapsto (t^2-1,\ t(t^2-1),\ u)$



φ is finite: $T^2 - 1 - \varphi^*(X) = 0$

$U - \varphi^*(Z) = 0$

$B = \varphi(\underbrace{\mathcal{V}(T-U)}_{\text{irred.}})$ is irreducible

$$\varphi^{-1}(B) = \underset{\substack{\uparrow \\ im = B}}{A_1} \cup \underset{\substack{\uparrow \\ im \neq B}}{A_2} \cup \underset{\substack{\uparrow \\ im \neq B}}{A_3}$$

Cause: W not normal

__Def__ An irred. alg. set $V \subseteq K^n$ is __normal__ if the ring $\Gamma(V)$ is integrally closed in its field of fractions $K(V)$.

__Ex__ K^n is normal because $K[X_1, \dots, X_n]$ is a UFD.

__Thm 12.1__ (Going down)

Let V be an __irred__. alg. set and let W be a __normal__ alg. set. Let $\varphi : V \to W$ be a surj. finite morphism. Let B be an irred. alg. subset of W and decompose $\varphi^{-1}(B)$ into irred. comp.: $\varphi^{-1}(B) = A_1 \cup \dots \cup A_r$.
Then, $\varphi(A_i) = B$ for __every__ component A_i.

$$\begin{tikzcd}
V \arrow[d, two heads] & \supseteq & \varphi^{-1}(B) \arrow[d, two heads] & = A_1 \cup \dots \cup A_r \arrow[dl, two heads] \\
W & \supseteq & B &
\end{tikzcd}$$

Pf ~~φ* is an inclusion~~

φ dominant $\Rightarrow$ injections $\varphi^*: \Gamma(W) \hookrightarrow \Gamma(V)$

$\varphi^*: K(W) \hookrightarrow K(V)$

We'll consider $\Gamma(W), K(W)$ subsets of $\Gamma(V), K(V)$ via these injections.

W normal: $\Gamma(W)$ integrally closed in $K(W)$

φ finite: $\Gamma(V)$ integral ring ext. of $\Gamma(W)$

$K(V)$ alg. field ext. of $K(W)$

Let L be the normal closure of this field ext.
It is a finite alg. ext. of $K(W)$ containing $K(V)$.

Let S be the integral closure of $\Gamma(W)$ in L.

We show in Lemma 12.4 that S is a ring-finite ext. of k.
$\Rightarrow S = \Gamma(V')$ for some alg. set V'.

The inclusion $\Gamma(V) \hookrightarrow \Gamma(V') = S$ corr. to a dominant morphism $\psi: V' \longrightarrow V$.

Since $\Gamma(V') = S$ is an int. ext. of $\Gamma(W)$ and hence of $\Gamma(V)$, the morphism ψ is finite.

Now, decompose $(\varphi\circ\psi)^{-1}(B)$ into irred. comp.:

$$(\varphi\circ\psi)^{-1}(B) = A_1' \cup \dots \cup A_s'.$$

$$\begin{array}{ccccccc}
L & \supseteq & S = \Gamma(V') & \quad & V' & \supseteq & A_1' \cup \dots \cup A_s' \\
\uparrow & & \uparrow & & \downarrow\!\!\downarrow \text{fin.} & & \downarrow \\
K(V) & \supseteq & \Gamma(V) & & V & \supseteq & A_1 \cup \dots \cup A_r \\
\uparrow & & \uparrow & & \downarrow\!\!\downarrow \text{fin.} & & \downarrow \\
K(W) & \supseteq & \Gamma(W) & & W & \supseteq & B
\end{array}$$

<u>Claim</u> Any A_i contains $\psi(A_j')$ for some j.

Pf W.l.o.g. $i=1$. Let $P \in A_1 \setminus (A_2 \cup \dots \cup A_r)$.

Take any preimage P' in V'. It lies in some irred. comp. A_j'.

$\Rightarrow \psi(A_j') \subseteq A_1 \cup \dots \cup A_r$

$\Rightarrow P \in \psi(A_j') \subseteq A_k$ for some k

$\underset{\substack{\uparrow \\ P \notin A_2 \cup \dots \cup A_r}}{\Longrightarrow} k = 1.$

$\square$ (claim)

It then suffices to ~~prove the Theorem~~ show that $(\varphi\circ\psi)(A_j') = B \ \forall j$.

$\Rightarrow$ We may assume w.l.o.g. that $K(V)$ is a normal field ext. of $K(W)$ and that $\Gamma(V)$ is the int. closure of $\Gamma(W)$ in $K(V)$. This case will be handled in Cor 12.3 below. $\square$

Prob. Let V, W be normal alg. sets, $\varphi : V \to W$ a dominant finite morphism, $K(V)$ a normal field ext. of $\varphi^*(K(W))$.

Then, any automorphism $\sigma \in Gal(K(V) | \varphi^*(K(W)))$ of $K(V)$ fixing $\varphi^*(K(W))$ restricts to an automorphism of $\Gamma(V)$ fixing $\varphi^*(\Gamma(W))$.

This automorphism corresponds to a morphism

- $\psi_\sigma : V \to V$ with $\psi_\sigma^* = \sigma$

with $\varphi\psi_\sigma = \varphi$ because $\underbrace{\psi_\sigma^*}_{\sigma} \circ \varphi^* = \varphi^*$.

(a "deck transformation" of $\varphi : V \to W$).

$$\begin{tikzcd} V \arrow[loop right, "\alpha_\sigma"] \arrow[d, "\varphi"] \\ W \end{tikzcd}$$

We obtain an action of $Gal(\ldots)$ on V by

- deck transformations.

Note that this action permutes the irred. comp. of $\varphi^{-1}(B)$ for any alg. subset $B \subseteq W$.

Ese $K = \mathbb{C}$, $V = \mathcal{V}(x^2+y^2-1)$, $W = K$

$$\varphi : V \longrightarrow W$$
$$(x,y) \longmapsto x$$

$\Gamma(W) = K[x]$, $\quad K(W) = K(x)$

$$K(W) \overset{\varphi^*}{\hookrightarrow} K(x)(\sqrt{1-x^2})$$

$\Gamma(V) = K[X,Y]/(x^2+y^2-1)$,

$$\|$$

$$K[X][\sqrt{1-x^2}]$$

$Gal(K(x)(\sqrt{1-x^2}) \mid K(x)) = \{id, \sigma\}$, where the aut σ given by $\sigma(\sqrt{1-x^2}) = -\sqrt{1-x^2}$ (i.e. $\sigma(Y) = -Y$), corr. to the reflection across the x-axis.

<u>Ex</u> $V = K^n$, $W = K^n$

$$\varphi : V \longrightarrow W$$

$$(a_1, \dots, a_n) \longmapsto (b_0, \dots, b_{n-1}),$$

where $\prod_{i=1}^{n}(x - a_i) = X^n + b_{n-1}X^{n-1} + \dots + b_0$

($b_i = \pm$ elem. symm. pol. in $a_1, \dots, a_n$)

i-th

φ is surjective.

φ is finite because $A_i^n + \varphi^*(B_{n-1})A_i^{n-1} + \dots + \varphi^*(B_0) = 0$.

$K(V)$ is a Galois ext. of $\varphi^*(K(W)) = K($elem. symm. pol.$)$

$\quad\, \shortparallel$

$K(A_1, \dots, A_n)$

~~K(... symm. pol.)~~

~~(symm. el. of ...)~~

with Galois group S_n.

S_n acts on V by permuting $a_1, \dots, a_n$ and this action is by deck transformations (= leaves $b_0, \dots, b_{n-1}$ unchanged).

$K(V) = K(B_1, \dots, B_n)$(roots of $X^n + B_{n-1}X^{n-1} + \dots + B_0$ in $\overline{K(B_1, \dots, B_n)}$).

"$W = V/S_n$" (<u>Geometric Invariant Theory</u>)

Thm ~~...~~ 12.2 Let V, W, φ as in the ~~...~~ and let $B \subseteq W$ be irred. Then, $G := Gal(\dots)$ acts transitively on the irred. comp. $A_1, \dots, A_r$ of $\varphi^{-1}(B)$.

~~In part, the irred. comp.~~

Cor ~~...~~ 12.3 The irred. comp. have the same image:
$\varphi(A_1) = \dots = \varphi(A_r) = B$.

~~B) dim (A_1) = ... dim~~

Pf of Cor If $\varphi(A_1) = B$, $\alpha_\sigma(A_1) = A_i$, then $\varphi(A_i) = \varphi(\alpha_\sigma(A_1)) = \varphi(A_1) = B$. $\square$

Pf of Thm ~~Assume w.l.o.g. that $A_1, \dots, A_k$ ...~~

Assume w.l.o.g. that $A_1, \dots, A_k$ form a G-orbit, $\varphi(A_1) = B$, and $1 \leq k < r$.

Pick points $P_{k+1} \in A_{k+1} \setminus A_1, \dots, P_r \in A_r \setminus A_1$.

By Cor 6.2, there is a function $f \in \Gamma(V)$ with

$f|_{A_1} = 0$ and $f(P_{k+1}) = \dots = f(P_r) = 1$.

$$\Downarrow$$

$f|_{A_{k+1}}, \dots, f|_{A_r} \neq 0$

$\Downarrow$ G permutes $A_{k+1}, \dots, A_r$

$\sigma(f)|_{A_{k+1}}, \dots, \sigma(f)|_{A_r} \neq 0 \quad \forall \sigma \in G$

$\Downarrow$ $\Gamma(A_{k+1}), \dots, \Gamma(A_r)$ int. dom. because $A_{k+1}, \dots, A_r$ are irred.

$g|_{A_1} = 0 \qquad g|_{A_{k+1}}, \dots, g|_{A_r} \neq 0$

for $g := Nm_{K(V)|K(W)}(f) = \left(\prod_{\sigma \in G} \sigma(f)\right)^t$, where $t \geq 1$ is the degree of inseparability of $K(V) | \varphi^*(K(W))$.

~~But $g \in \varphi^*(K(W))$ ... $\varphi^*(K(W))$~~
~~is the composition of a rat. fct.~~

We have $g \in \varphi^*(K(W)) \cap \Gamma(V)$

$$= \varphi^*(\Gamma(W)).$$

$$\begin{aligned}
LHS &= \{ h \in \varphi^*(K(W)) \text{ int. over } \varphi^*(\Gamma(W)) \} \\
&= \{ \varphi^*(h) : h \in K(W) \text{ int. over } \Gamma(W) \} \\
&\underset{\Gamma(W) \text{ int. cl. in } K(W)}{=} \varphi^*(\Gamma(W))
\end{aligned}$$

Let $g = \varphi^*(h)$, $h \in \Gamma(W)$.

Now, $\underset{h \circ \varphi|_{A_1}}{\overset{\|}{g|_{A_1}}} = 0$ with $\varphi(A_1) = B$ implies $h|_B = 0$.

$\Rightarrow g|_{A_i} = 0 \;\forall i.$ $\lightning$

$\square$

We neglected one thing in the pf of Thm 12.1:

<u>Lemma 12.4</u>

Let R be an int. dom. with field of fractions F.

Let $L|F$ be a finite field ext.

Assume that R is a finitely generated ring ext. of K and integrally closed in F.

Then, the integral closure S of R in L is a) a fin. gen. ring ext. of K and b) a fin. gen. R-module.

<u>Rmk</u> It suffices to show b).

<u>Pf when $L|F$ is separable</u> (e.g. if $\mathrm{char}(K)=0$)

Since $R=K[x_1,\dots]/\dots$ is noetherian, submod. of fin. gen. R-mod. are fin. gen. $\Rightarrow$ we can replace L by its normal (= Galois) closure over F.

Let $n=[L:F]$. Pick a basis $b_1,\dots,b_n$ of $L|F$.

Multiplying by elements of R, we can make

$b_1,\dots,b_n\in S$ according to Lemma 4.5.2.

Let $c=\sum_{i=1}^n a_i b_i \in S$ with $a_1,\dots,a_n\in F$.

Note: For any $x\in S$, $\underset{\sum_{\sigma\in \mathrm{Gal}(L|F)}^n \sigma(x)}{\underset{\parallel}{\mathrm{Tr}(x)}}\in F$ is integral over R, so $\mathrm{Tr}(x)\in R$

Now, $\mathrm{Tr}(b_j c)=\sum_{i=1}^n a_i \,\mathrm{Tr}(b_i b_j)$ for all j.

~~This is a system of~~

$$\Rightarrow \underbrace{(\mathrm{Tr}(b_j c))_{j=1,\dots,n}}_{\in R^n\subseteq F^n} = \underbrace{(\mathrm{Tr}(b_i b_j))_{i,j=1,\dots,n}}_{\substack{n\times n\text{-matrix}\\ \text{with coeff. in } R\subseteq F}} \cdot \underbrace{(a_i)_{i=1,\dots,n}}_{\in R^n\subseteq F^n} \qquad (\mathrm{I})$$

The matrix $M = (\mathrm{Tr}(b_i b_j))_{i,j}$ is invertible because $L|F$ is separable. $\Rightarrow \det(M) \neq 0$.

Also, (*) implies that
$\det(M) \cdot a_i \in R$ for $i = 1, \dots, n$.

$$\Rightarrow S \subseteq \underbrace{\frac{1}{\det(M)} \cdot (b_1 R + \dots + b_n R)}_{\text{fin.-gen. } R\text{-mod.}}$$

$\Rightarrow S$ is a fin. gen. R-mod. $\square$

Pf for arbitrary $L|F$

By Problem 4a on Pset 7, there are alg. indep. elements $x_1, \dots, x_n$ of R s.t. R is an int. ext. of $K[x_1, \dots, x_n]$.

Replacing R by $K[x_1, \dots, x_n]$, F by $K(x_1, \dots, x_n)$, we can assume $R = K[x_1, \dots, x_n]$, $F = K(x_1, \dots, x_n)$.

Let $F \subseteq M \subseteq L$ be the largest purely inseparable subext. of $L|F$. Let $p = \mathrm{char}(K) \neq 0$.

$\Rightarrow M \subseteq K(x_1^{1/p^t}, \dots, x_n^{1/p^t})$ for some $t \geq 0$, and $L|M$ is separable.

The int. closure of $R = K[x_1, \dots, x_n]$ in $K(x_1^{1/p^t}, \dots, x_n^{1/p^t})$ is $K[x_1^{1/p^t}, \dots, x_n^{1/p^t}]$ (why?) and hence a fin. gen. $K[x_1, \dots, x_n]$-module $\Rightarrow$ The int. closure of R in M is a fin. gen. R-module. The result then follows from the separable case since $L|M$ is separable. $\square$

13. More about dimension

13.1. Another definition of dimension

Lemma 13.1.1 Let $V \subsetneq W$ be irreducible alg. sets.

Then, a) $\dim(V) < \dim(W)$

b) There is an alg. set $V \subseteq A \subsetneq W$ with

$$\dim(A) = \dim(W) - 1.$$

Cor 13.2 Let $V \neq \emptyset$ be any alg. set. Then, $\dim(V)$ is the largest $d \geq 0$ s.t. there are irreducible alg. sets

$$\emptyset \neq V_0 \subsetneq V_1 \subsetneq \cdots \subsetneq V_d \subseteq V.$$

Pf $\dim(V) \geq d$:

$$0 \leq \dim(V_0) < \dim(V_1) < \cdots < \dim(V_d) \leq \dim(V).$$

$\dim(V) \leq d$: Let $d' = \dim(V)$.

Let $V_{d'}$ be an irred. comp. of V of dimension $d' = \dim(V)$.

If $d' \geq 1$, let $P \in V_{d'}$, so $\{P\} \subsetneq V_{d'}$.

There is an irred. subset $\{P\} \subseteq V_{d'-1} \subsetneq V_{d'}$ of dimension $d'-1$.

$\vdots$

$\rightsquigarrow V_0 \subsetneq V_1 \subsetneq \cdots \subsetneq V_{d'} \subseteq V.$ $\square$

Rmk The cor ~~[illegible]~~ fails without the assumption that $V_0, \dots, V_d$ are irreducible:

If $P_1, \dots, P_n$ are points in V, then

$$\{P_1\} \subsetneqq \{P_1, P_2\} \subsetneqq \dots \subsetneqq \{P_1, \dots, P_n\} \subseteq V,$$

so there are arbitrarily long chains if $|V| = \infty$.

Cor 13.1.3 Let $V \subseteq W$ both be irreducible.

Then, the <u>codimension</u>

$$\operatorname{codim}(V,W) := \dim(W) - \dim(V)$$

of V in W is the largest $d \geq 0$ s.t. there are irred. alg. sets

$$V = V_0 \subsetneq \dots \subsetneq V_d = W.$$

Pf like Cor 13.1.2. $\square$

Pf of Lemma 13.1.1

Let $n = \dim(W)$. By Noether Normalization, there is a surjective finite morphism $\varphi : W \to K^n$.

$$V \subsetneq W \underset{\substack{\uparrow \\ \text{incomparability} \\ \text{(Lemma 11.6)}}}{\Longrightarrow} \varphi(V) \subsetneq \varphi(W) = K^n$$

Take any $0 \neq f \in K[x_1, \dots, x_n]$ with $\varphi(V) \subseteq \mathcal{V}(f)$.

(Since $\varphi(V)$ is irreducible, we may assume that f is irreducible.)

$\Rightarrow \dim(V) = \dim(\varphi(V)) \leq \dim(\mathcal{V}(f)) = n-1$.

V is contained in an irred. comp. A of $\varphi^{-1}(\mathcal{V}(f))$.

By Thm 12.1 (Going down), we have $\varphi(A) = \mathcal{V}(f)$.

$\Rightarrow \dim(A) = \dim(\varphi(A)) = \dim(\mathcal{V}(f)) = n-1$. $\square$

13.2. Defining with few equations

Def An irred. $(n-1)$-dimensional irred. subset of K^n is called a *hypersurface* in K^n.

Lemma 13.2.1 Any hypersurface $V \subseteq K^n$ is of the form $V = \mathcal{V}(f)$ for some irred. $0 \neq f \in K[X_1, \dots, X_n]$.

Pf $V \subsetneq K^n \Rightarrow V \subseteq \mathcal{V}(f)$ for some $0 \neq f$.

V irred. $\Rightarrow V \subseteq$ some irred. comp. of $\mathcal{V}(f)$.

$\Rightarrow$ w.l.o.g. f irreducible

If $V \subsetneq \mathcal{V}(f)$, then $\dim(V) < \dim(\mathcal{V}(f)) = n-1$. $\lightning$

$\Rightarrow V = \mathcal{V}(f)$. $\square$

Cor 13.2.2 Let $V \subseteq W$ both be irred. Then, there are $c := \operatorname{codim}(V,W)$ functions $f_1, \dots, f_c \in \Gamma(W)$ s.t. V is an irred. comp. of $\mathcal{V}_W(f_1, \dots, f_c)$ and all other irred. comp. also have codimension c in W.

Rmk Let $K = \mathbb{C}$, $W = \mathcal{V}(X^3 - 4X + 4 - Y^2) \subset K^2$,

$V = \{(2,2)\}$ or $\{(\pi, \sqrt{\pi^3 - 4\pi + 4})\}$ (easier).

Then, there is no $f \in \Gamma(W)$ with $V = \mathcal{V}_W(f)$.

(Of course, there are plenty of f s.t. $\mathcal{V}_W(f)$ is a finite set of pts. including V.)

Pf of Rmk skipped (not easy). "$\square$"

Pf of Cor 13.2.3 by induction over c.

$c=0$: clear ($V=W$).

$c-1\to c$: Let $n=\dim(W)$, $\varphi: W\to K^n$ a surjective finite morphism.

$\operatorname{codim}(\varphi(V), K^n)=\operatorname{codim}(V,W)=c\geq 1$.

Let $0\neq g_1\in K[x_1,\dots,x_n]$ be irreducible with $\varphi(V)\subseteq \mathcal{V}(g_1)$.

$\operatorname{codim}(\varphi(V),\mathcal{V}(g_1))=c-1$.

By induction, there are $g_2,\dots,g_c\in K[x_1,\dots,x_n]$ s.t. $\varphi(V)$ is an irred. comp. of $\mathcal{V}(g_1,\dots,g_c)=\mathcal{V}_{\mathcal{V}(g_1)}(g_2,\dots,g_c)$ and all other irred. comp. also have codimension $c-1$ in $\mathcal{V}(g_1)$, so codimension c in K^n.

$\Rightarrow$ By Thm 12.1 (going down), the irred. comp. of $\varphi^{-1}(\mathcal{V}(g_1,\dots,g_c))=\mathcal{V}(\underbrace{\varphi^*(g_1)}_{f_1},\dots,\underbrace{\varphi^*(g_c)}_{f_c})$

have the same dimension, so have codim. c in W.

$V\subseteq\varphi^{-1}(\mathcal{V}(g_1,\dots,g_c))$ is contained in, and hence equal to, one of them. □

(because of dimension)

Lemma 13.2.4

Let S be a module-finite ring ext. of R and assume that S, R are int. dom. with fields of fractions M, L.

$$\begin{array}{ccc} M & \supseteq & S \\ | & & | \\ L & \supseteq & R \end{array}$$

Let $a \in S$ and let $b = N_{M/L}(a) \in L$.
If R is integrally closed in L, then $b \in R$ and $a \mid b$ in S.

Pf when M/L is a Galois ext and S is the int. closure of R in M
~~If M/L is Galois ext~~. Then, $b = \prod_{\sigma \in Gal(M/L)} \underbrace{\sigma(a)}_{\in S}$.

This is integral over R because $a \in S$, and therefore each $\sigma(a)$, is. Hence, $b \in R$.
It is divisible by a because a is one of the factors in b.

Pf in general

Let $f \in R[X]$ be a monic pol with $f(a)=0$ and let $g \in L[X]$ be the min. pol. of a.

$\Rightarrow g \mid f$.

$\Rightarrow$ Every root a_i of g in M is integral over R.

$\Rightarrow$ Every coeff. of $g(X) = \prod_i (X - a_i)$ (with mult.) is integral over R and lies in L. $\Rightarrow$ Every coeff. lies in R: $g \in R[X]$.

Write $g(X) = X^n + c_{n-1}X^{n-1} + \dots + c_0$.

$\Rightarrow b = \mathrm{Nm}_{M|L}(a) = \mathrm{Nm}_{L(a)|L}(\mathrm{Nm}_{M|L(a)}(a))$

$= \mathrm{Nm}_{L(a)|L}(a^{[M:L(a)]})$

$= \mathrm{Nm}_{L(a)|L}(a)^{[M:L(a)]}$

$= (\pm c_0)^{[M:L(a)]} \in R$.

Also, $0 = g(a) = a^n + c_{n-1}a^{n-1} + \dots + ac_1 + c_0$.

$= a\underbrace{(a^{n-1} + c_{n-1}a^{n-2} + \dots + c_1)}_{\in S} + c_0$.

$\Rightarrow a \mid c_0 \mid b$ in S. $\square$

Thm 13.2.5 (Krull's principal ideal theorem)

Let W be an irred. alg. set and let V be an irred. comp. of $\mathcal{V}(f) \subseteq W$ for some $0 \neq f \in \Gamma(W)$.

Then, $\operatorname{codim}(V, W) = 1$. $(\Leftrightarrow \dim(V) = \dim(W) - 1)$.

Pf Let $n = \dim(W)$, $\varphi : W \to K^n$ a surj. fin. morphism.

$$\begin{array}{cccccc} W & K(W) & \supseteq & \Gamma(W) & \ni f \\ \varphi \big\downarrow & \big| & & \big| & \\ K^n & K(x_1, \dots, x_n) & \supseteq & K[x_1, \dots, x_n] & \end{array}$$

Let $g = N_{K(W)|K(x_1, \dots, x_n)}(f)$. Clearly, $g \neq 0$.

By Lemma 13.2.4, we have $g \in K[x_1, \dots, x_n]$,

$\varphi^*(g) \mid f$ in $\Gamma(W)$.

$\Rightarrow V \subseteq \mathcal{V}_W(f) \subseteq \mathcal{V}_W(\varphi^*(g)) = \varphi^{-1}(\mathcal{V}_{K^n}(g))$.

$\Rightarrow \varphi(V) \subseteq \varphi(\mathcal{V}_W(f)) \subseteq \mathcal{V}_{K^n}(g)$

It suffices to show that $\varphi(\mathcal{V}_W(f)) = \mathcal{V}_{K^n}(g)$: Then, by Thm 12.1 (going down), $\dim(V) = \dim(\varphi(V)) = \dim(\mathcal{V}_{K^n}(g)) = n-1$.

Assume that $\varphi(\mathcal{V}_W(f)) \subsetneq \mathcal{V}_{K^n}(g)$.

Take $0 \neq h \in K[x_1, \dots, x_n]$ with

$$h|_{\varphi(\mathcal{V}_W(f))} = 0, \text{ but } h|_{\mathcal{V}_{K^n}(g)} \neq 0.$$

$$h|_{\varphi(\mathcal{V}_W(f))} = 0 \implies \varphi^*(h)|_{\mathcal{V}(f)} = 0$$

$$\underset{\text{Nullstellensatz}}{\implies} \varphi^*(h)^m \in \mathcal{I}_W(\mathcal{V}_W(f)) = \sqrt{(f)} \subseteq \Gamma(W)$$

for some $m \geq 1$.

$$\implies \varphi^*(h)^m = fe \text{ for some } e \in \Gamma(W).$$

$$\implies \underbrace{Nm(\varphi^*(h))^m}_{\substack{\| \leftarrow h \in K(x_1,\dots,x_n) \\ h^{m\cdot[K(W):K(x_1,\dots,x_n)]}}} = \underbrace{Nm(f)}_{g} \underbrace{Nm(e)}_{\in K[x_1,\dots,x_n]}$$

$$\implies h^{\cdots} \in (g) \subseteq K[x_1,\dots,x_n]$$

$$\implies h \in \sqrt{(g)} = \mathcal{I}(\mathcal{V}(g))$$

$$\implies h|_{\mathcal{V}(g)} = 0 \ \lightning$$

$\square$

Rmk ~~$\mathcal{V}(f_1,\dots,f_r)$ can be empty, even if $r <$ dim(W).~~
$\mathcal{V}(f)$ can be empty.

Rmk The Thm can fail if K isn't alg. closed:
$$\underset{\substack{\| \\ \{(0,0)\}}}{\mathcal{V}(x^2+y^2)} \subseteq \mathbb{R}^2 \text{ has codimension } 2.$$

Cor 13.2.6 Let W be an irred. alg. set and let V be an irred. comp. of $\mathcal{V}_W(f_1,\dots,f_r)$ for some $f_1,\dots,f_r \in \Gamma(W)$.

Then, $\operatorname{codim}(V,W) \leq r$.

Pf (by induction over r): Assume $r \geq 1$. Let A be an irred. comp. of $\mathcal{V}_W(f_1)$ containing V.

$\underset{\text{Thm 13.2.5}}{\Longrightarrow} \operatorname{codim}(A,W) \leq 1$.

V is an irred. comp. of $\mathcal{V}_A(f_2,\dots,f_r)$.

By ind., $\operatorname{codim}(V,A) \leq r-1$.

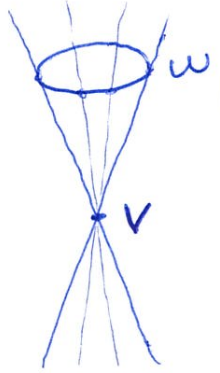
$\Rightarrow \operatorname{codim}(V,W) \leq r$. $\square$

Rmk Of course, we can have $\operatorname{codim}(V,W) < r$:
(E.g. could have $f_1^3 = f_2 + f_3^2$. $\rightsquigarrow$ f_1 redundant.)

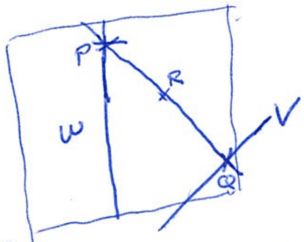
13.3. Applications, part 1

Thm 13.3.1 Let $V, W \subseteq K^n$ be irred. of dimensions a, b.
Let $S \subseteq K^n$ be the union of all straight lines $L \subseteq K^n$ joining a pt. $P \in V$ and a pt. $Q \in W$ with $P \neq Q$.
(S is called the join of V and W.)
If $a+b+2 \leq n$, then $\overline{S} \subsetneq K^n$.
In fact, $\dim(\overline{S}) \leq a+b+1$.

Ex $a=1, b=0, n=3$
$V=$pt., $W=$circle $\rightsquigarrow S=$ cone (2-dimensional)



Ex $a=1, b=1, n=3$
V, W skew lines
(non-intersecting, non-parallel)



$\rightsquigarrow S = (K^3 \setminus (A \cup B)) \cup V \cup W \underset{!}{\Rightarrow} \overline{S}=K^3$ (3-dimensional),
where $A =$ plane ~~through~~ containing V parallel to W,
$B =$ — " — W — " — V

Ex $a=1, b=1, n=3$
V, W parallel lines
$\rightsquigarrow S=$ plane containing V, W (2-dimensional)

Pf of Thm

Consider the morphism

$$\varphi : V \times W \times K \longrightarrow K^n$$

$$(P, Q, t) \longmapsto \underbrace{tP + (1-t)Q}_{\substack{\text{parametrisation} \\ \text{of the line } PQ \\ (\text{if } P \neq Q)}}$$

Its image contains S. (It's equal to S unless $V = W = pt.$)

$$\Rightarrow \dim(\overline{S}) \leq \dim\left(\overline{\varphi(V \times W \times K)}\right)$$

$$\underset{\text{Lemma 10.9}}{\leq} \dim(V \times W \times K)$$

$$= \dim(V) + \dim(W) + \dim(K)$$

$$= a + b + 1 < n.$$

$\square$

<u>Thm 13.3.2</u> let $d \geq 0$. For any m pts. $P_1, \dots, P_m \in K^n$, if $m < \binom{d+n}{n}$, there is a pol. $0 \neq f \in K[X_1, \dots, X_n]$ of degree $\leq d$ with $P_1, \dots, P_m \in \mathcal{V}(f)$.

<u>Ex</u> $d = n = 2$, $m = 5$

There is a conic (or union of two lines) containing $P_1, \dots, P_5 \in K^2$.

<u>Pf</u> let F_d be the vector space of pol. of deg. $\leq d$.
consider the linear map

$$\varepsilon : F_d \longrightarrow K^m$$
$$f \longmapsto (f(P_1), \dots, f(P_m))$$

The claim is that ε is not injective.

This follows because

$$\dim(F_d) = \#(\text{monomials } \underset{X_1^{e_1} \cdots X_n^{e_n}}{\underset{\shortparallel}{M}} \text{ of deg.} \leq d)$$

$$= \#\{(e_1, \dots, e_n) : e_1, \dots, e_n \geq 0,\ e_1 + \dots + e_n \leq d\}$$

$$\overset{\uparrow}{=} \binom{d+n}{n} > m = \dim(K^m).$$

$(e_1, \dots, e_n)$ can be encoded as the string

$$\underbrace{0 \dots 0}_{e_1} | \underbrace{0 \dots 0}_{e_2} | \dots | \underbrace{0 \dots 0}_{e_n} | \underbrace{0 \dots 0}_{d-(e_1+\dots+e_n)}$$

~~of length~~ consisting of d times the character '0' and n times the character '|'. $\square$

Rmk In the pf., we only used vector space dimensions. $\rightsquigarrow$ The Thm. holds over arbitrary fields!

Thm 13.3.3 For any points $P_1, \dots, P_m \in K^2$, there is an irreducible pol. $0 \neq f \in K[X,Y]$ of degree $\leq m+2$ with $P_1, \dots, P_m \in V(f)$.

Pf The kernel T of $\varepsilon : F_{m+2} \to K^m$, $f \mapsto (f(P_1), \dots, f(P_m))$

has dimension $\dim(T) \geq \dim(F_{m+2}) - m = \binom{m+4}{2} - m = \frac{m^2+5m+12}{2}$.

It suffices to show that the set

$V := \cancel{\{ f \in F_{m+2} \text{ not irreducible} \}}$

$= \{0\} \cup \{ f \in F_{m+2} \text{ reducible} \}$

satisfies $\dim(\overline{V}) < \dim(T)$ since we then can't have $T \subseteq V$. Any reducible f of $\deg \leq m+2$ can be written as $g \cdot h$ with $\deg(g) + \deg(h) \leq m+2$.

$\Rightarrow V = \{0\} \cup \bigcup_{\substack{a,b \geq 1: \\ a+b = m+2}} F_a \cdot F_b$

In fact, we can make one coeff. of h (say the "leading coefficient") equal to 1.

Let $F_d' = \{ f \in F_d$ with at least one coeff. equal to $1 \}$.

(This is an alg. subset of F_d,

$\dim(F_d') = \dim(F_d) - 1$.)

$$\Rightarrow V = \{0\} \cup \bigcup_{\substack{a,b \geq 1: \\ a+b \leq m+2}} F_a \cdot F_b' .$$

Now, $F_a \cdot F_b'$ is the image of the morphism

$$F_a \times F_b' \longrightarrow F_{m+2}, \qquad (g,h) \longmapsto gh$$

so
$$\begin{aligned}
\dim\left(\overline{F_a \cdot F_b'}\right) &\leq \dim(F_a) + \dim(F_b') \\
&= \binom{a+2}{2} + \binom{b+2}{2} - 1 \\
&= \frac{(a+2)(a+1)}{2} + \frac{(b+2)(b+1)}{2} - 1 \\
&= \frac{(a^2+b^2) + 3(a+b) + 2}{2} \\
&= \frac{(a+b)^2 + 3(a+b) + 2 - 2ab}{2} \\
&\overset{a+b=m+2}{=} \frac{(m+2)(m+5)}{2} + 1 - ab \\
&\leq \frac{(m+2)(m+5)}{2} + 1 - 1 \cdot (m+1) \\
&= \frac{m^2+5m+10}{2} < \frac{m^2+5m+12}{2} \leq \dim(T).
\end{aligned}$$

$\Rightarrow \dim(\overline{V}) < \dim(T)$. $\square$

Rmk There's some room for improvement:

~~We only~~

If $f = gh \in T \cap V$, then ($P_1, \dots, P_m \in \mathcal{V}(f) = \mathcal{V}(g) \cup \mathcal{V}(h)$, so) there is a subset $S \subseteq \{1, \dots, m\}$ such that $\{P_i \mid i \in S\} \subseteq \mathcal{V}(g)$ and

$$\{P_i \mid i \notin S\} \subseteq \mathcal{V}(h).$$

$\rightsquigarrow$ can replace F_a, F'_b by

$$F_{a,S} := \{g \in F_a : \forall i \in S : g(P_i) = 0\},$$

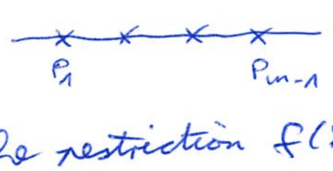
$$F'_{b,S} := \{h \in F'_b : \forall i \notin S : h(P_i) = 0\}.$$

(slightly smaller dimension.)

However, the degree can't be improved very much:

Rmk For any $m \geq 2$, there are pts. $P_1, \dots, P_m \in K^2$ s.t. there is no irred. $0 \neq f \in K[X,Y]$ of degree $\leq m-2$ with $P_1, \dots, P_m \in \mathcal{V}(f)$.

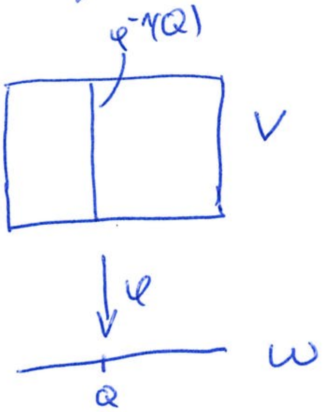
Pf Take $P_1, \dots, P_{m-1}$ on the x-axis, P_m not on the x-axis.



The restriction $f(X,0)$ of f to the x-axis is a pol. of deg. $\leq m-2$ vanishing at $m-1$ points $\Rightarrow f(X,0) = 0$
$\Rightarrow Y \mid f(X,Y)$. $\underset{f \text{ irreducible}}{\Rightarrow} f(X,Y) = c \cdot Y$ for some constant $c \in K^*$.
$\Rightarrow f(P_m) \neq 0$. ↯ $\square$

13.4. Dimension of fibers

Def A *fiber* of $\varphi: V \to W$ is the preimage $\varphi^{-1}(Q)$ of a point $Q \in W$.



Thm 13.4.1 Let V, W be irred, $\varphi: V \to W$ a morphism, and A an irred. comp. of $\varphi^{-1}(Q)$ for some pt. $Q \in W$. Then, $\operatorname{codim}(A, V) \leq \dim(W)$.

($\Leftrightarrow \dim(A) \geq \dim(V) - \dim(W)$.)

Rmk Compare this to linear maps from linear algebra!

Ex
$$\varphi: K^2 \longrightarrow K^2$$
$$(x, y) \longmapsto (x, xy)$$

$\varphi^{-1}(a, b) = \{(a, \frac{b}{a})\}$ if $a \neq 0$

$\varphi^{-1}(0, b) = \emptyset$ if $b \neq 0$ (fiber can be empty)

$\varphi^{-1}(0, 0) = \{(0, y) \mid y \in K\}$ (fiber can have larger dimension)

We'll prove sth. more general:

<u>Thm 13.4.2</u> Let V, W, φ as above, $B \subseteq W$ irred.,

A an irred. comp. of $\varphi^{-1}(B)$ with $\overline{\varphi(A)} = B$.

Then, $\operatorname{codim}(A, V) \leq \operatorname{codim}(B, W)$.

<u>Rmk</u> $\overline{\varphi(A)} = B$ is automatic if $B = \{Q\}$.

<u>Rmk</u> ~~In~~ In general, the condition $\overline{\varphi(A)} = B$ can't be omitted, as the 2^{nd} example in section 12 (right before the def. of normal alg. sets) shows.

<u>Idea of pf</u> B is almost def. by $r := \operatorname{codim}(B, W)$ equations. $\Rightarrow$ A is almost def. by r equations.

<u>Pf of Thm</u> Let $r = \operatorname{codim}(B, W)$.

By Cor 13.2.2, there are fcts. $g_1, \dots, g_r \in \Gamma(W)$ s.t. B is an irred. comp. of $\mathcal{V}_W(g_1, \dots, g_r)$.

$$\Rightarrow A \subseteq \varphi^{-1}(B) \subseteq \varphi^{-1}(\mathcal{V}_W(g_1, \dots, g_r)) = \mathcal{V}_V(\underbrace{\varphi^*(g_1)}_{= f_1}, \dots, \underbrace{\varphi^*(g_r)}_{= f_r})$$

~~A is …~~ Let A' be an irred. comp. of $\mathcal{V}_V(f_1, \dots, f_r)$ containing A.

$$\Rightarrow \underbrace{B}_{\substack{\uparrow \\ \text{irred. comp. of } \mathcal{V}_W(g_1, \dots, g_r)}} = \overline{\varphi(A)} \subseteq \underbrace{\overline{\varphi(A')}}_{\substack{\uparrow \\ \text{irred.}}} \subseteq \mathcal{V}_W(g_1, \dots, g_r)$$

$$\Rightarrow B = \overline{\varphi(A)} = \overline{\varphi(A')}$$

$$\Rightarrow \underbrace{A}_{\substack{\uparrow \\ \text{irred. comp. of } \varphi^{-1}(B)}} \subseteq \underbrace{A'}_{\substack{\uparrow \\ \text{irred.}}} \subseteq \varphi^{-1}(B)$$

$\Rightarrow A = A'$, which is an irred. comp. of $\mathcal{V}_V(f_1, \dots, f_r)$

$\underset{\text{Thm 13.2.6}}{\Rightarrow}$ $\operatorname{codim}(A, V) \leq r$. $\square$

If φ is dominant, we have equality in Thm 13.4.1 for a "generic" fiber.

Prop 13.4.4 Let V, W, φ as above and assume that φ is dominant. Then, there is a (dense) open subset $\emptyset \neq U \subset W$ such that for every $Q \in U$, the fiber $\varphi^{-1}(Q)$ is nonempty and every irred. comp. A of $\varphi^{-1}(Q)$ satisfies $\mathrm{codim}(A, V) = \dim(W)$.

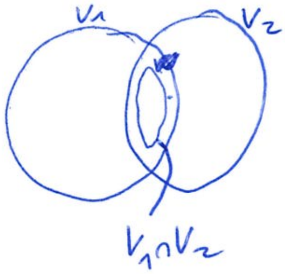
We won't prove this.
(See Thm 1.25 in Shafarevich: Basic Algebraic Geometry 1.)

Wrong Cor 13.4.3

Let $V_1, V_2 \subseteq W$ be irred. and let A be an irred. comp. of $V_1 \cap V_2$. Then,

$$\operatorname{codim}(A, W) \leq \operatorname{codim}(V_1, W) + \operatorname{codim}(V_2, W).$$

Ex



Counterexample

$W = \mathcal{V}(AB - CD) \subset K^4$ (dim $W=3$)

$V_1 = \mathcal{V}(A, C) \subset W$ (dim$=2$)

$V_2 = \mathcal{V}(B, D) \subset W$ (dim$=2$)

$V_1 \cap V_2 = \mathcal{V}(A, B, C, D) = \{0\}$ (dim$=0$)

Correct Cor 13.4.3 The above holds if $W = K^n$.

~~Pf shortly~~

(Pf will follow shortly ...)

Pf of Cor 13.4.3

Consider the morphism

$$\varphi : V_1 \cap V_2 \longrightarrow V_1 \times V_2 \subseteq K^n \times K^n,$$
$$P \longmapsto (P, P)$$

$$\varphi(V_1 \cap V_2) = \{(Q,R) \in V_1 \times V_2 \mid Q = R\}$$
$$= \mathcal{V}_{V_1 \times V_2}(X_1 - Y_1, \ldots, X_n - Y_n) =: B$$

if we denote the coord. in $K^n \times K^n$ by $X_1, \ldots, X_n, Y_1, \ldots, Y_n$.

$\varphi : V_1 \cap V_2 \to B$ is an isomorphism with inverse

$$\begin{array}{ccc} K^n \times K^n & & \\ \cup\!\text{I} & & \\ V_1 \times V_2 & & K^n \\ \cup\!\text{I} & & \cup\!\text{I} \\ B & \longrightarrow & V_1 \cap V_2 \\ (Q,R) & \longmapsto & Q \end{array}$$

$\Rightarrow \varphi(A)$ is an irred. comp. of $B = \mathcal{V}_{V_1 \times V_2}(X_1 - Y_1, \ldots, X_n - Y_n)$.

$$\Rightarrow \dim(A) = \dim(\varphi(A)) \geq \dim(V_1 \times V_2) - n$$
$$= \dim(V_1) + \dim(V_2) - n$$

Cor 13.2.6

$$\Rightarrow \operatorname{codim}(A, K^n) \leq \operatorname{codim}(V_1, K^n) + \operatorname{codim}(V_2, K^n).$$

$\square$

13.5. Applications, part 2

We obtain a "converse" to Thm 13.3.3:

Thm 13.5.1 For any $n, d \geq 1$ and $m \geq \binom{d+n}{n}$, there are points $P_1, \dots, P_m \in K^n$ s.t. there is no pol. $0 \neq f \in K[x_1, \dots, x_n]$ of degree $\leq d$ with $P_1, \dots, P_m \in \mathcal{V}(f)$.

Pf Let F_d' be the set of pol. of deg. $\leq d$ where at least one coeff. is 1.

Consider the following alg. subset A of $\underbrace{K^n \times \dots \times K^n}_{m} \times F_d'$:

$$A = \{(P_1, \dots, P_m, f) \mid f(P_1) = \dots = f(P_m) = 0\}.$$

We have projections

$$\begin{array}{ccc} A & \xrightarrow{\pi} & F_d' \\ \sigma \downarrow & & \\ K^n \times \dots \times K^n & & \end{array}$$

The goal is to show that σ is not surjective, which we'll do by proving $\dim(A) < \dim(K^n \times \dots \times K^n)$.

Recall that $\dim(F_d') = \binom{d+n}{n} - 1$.

Moreover, the preimage of any $f \in F_d'$ in A is

$$\pi^{-1}(f) = \underbrace{\mathcal{V}(f) \times \dots \times \mathcal{V}(f)}_{m} \times \{f\}.$$

Since $f \in F_d'$, we have $f \neq 0$, so $\dim(\mathcal{V}(f)) = n-1$.

$\Rightarrow \dim(\pi^{-1}(f)) = m(n-1)$.

Applying Thm 13.4.1 (to the irred. comp. W of F_d' and the irred. comp. V of $\pi^{-1}(W)$), it follows that

$$\dim(A) \leq \binom{d+n}{n} - 1 + m(n-1).$$

Using the assumption that $m \geq \binom{d+n}{n}$, we ~~get~~ indeed get

$$\dim(A) \leq mn - 1 < mn = \dim(K^n \times \dots \times K^n). \qquad \square$$

Remark Applying Prop 13.4.4, we see that in fact

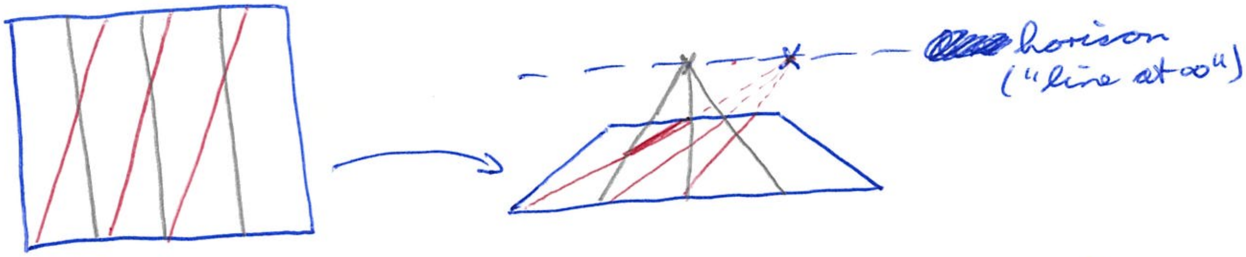
$$\dim(A) = \binom{d+n}{n} - 1 + m(n-1).$$

14. Projective varieties

14.1. Projective space

<u>Motivation</u> Two lines $L_1 \neq L_2$ in K^2 intersect in exactly one point <u>except if they are parallel.</u>

<u>Idea</u> Pretend they intersect in a point at ∞. (infinitely far away)



Any line goes through exactly one additional point at ∞ which depends on the direction (slope) of the line.

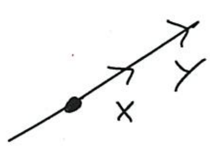
In this section, K can be any field (not necc. alg. closed).

<u>Def</u> The n-dimensional <u>projective space</u> $\mathbb{P}^n_K$ over K is the set of lines in K^{n+1} through the origin. We call the elements of $\mathbb{P}^n_K$ the <u>points</u> in $\mathbb{P}^n_K$.

We denote the line spanned by $\cancel{(0,\dots,0)\neq}\ (x_0,\dots,x_n)\in K^{n+1}$ by $[x_0:\cdots:x_n]\in\mathbb{P}^n_K$.

<u>Note</u> $[x_0:\cdots:x_n]=[y_0:\cdots:y_n]$ if and only if $(x_0,\dots,x_n),(y_0,\dots,y_n)\in K^{n+1}$ are colinear, i.e.

$$(x_0,\dots,x_n)=\lambda(y_0,\dots,y_n) \text{ for some } \lambda\in K^\times.$$



$x_0,\dots,x_n$ are called <u>projective coordinates</u> of the point $[x_0:\cdots:x_n]\in\mathbb{P}^n_K$.

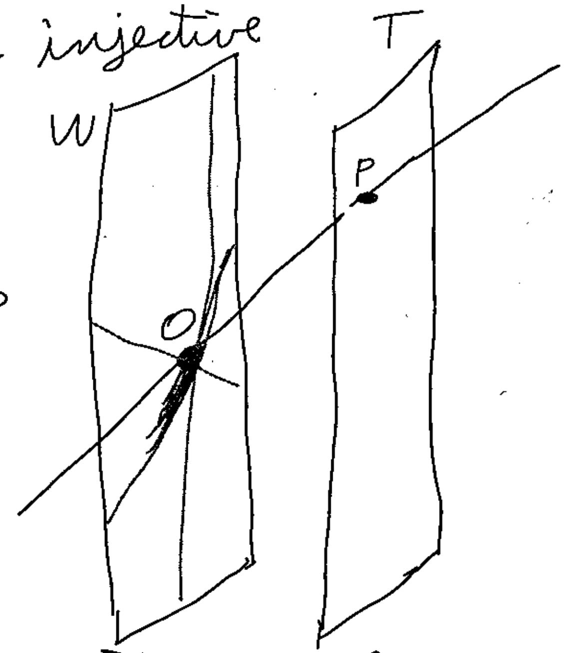
Rmk We could therefore equivalently have defined $\mathbb{P}^n_K$ to be the set of $(n+1)$-tuples $(0,\dots,0)\neq(x_0,\dots,x_n)\in K^{n+1}$ modulo the following equivalence relation:

$$(x_0,\dots,x_n)\sim(y_0,\dots,y_n) \text{ if } (x_0,\dots,x_n)=\lambda(y_0,\dots,y_n)$$
for some $\lambda\in K^\times$.

In short: $\mathbb{P}^n_K = \left(K^{n+1}\setminus\{0\}\right)/K^\times$.

Rmk For any n-dimensional affine linear subspace $T\subset K^{n+1}$ not containing the origin, we have an injective map

$$T \hookrightarrow \mathbb{P}^n_K$$
$$P \longmapsto \text{line spanned by } P$$
$$(x_0,\dots,x_n)\mapsto[x_0:\dots:x_n]$$



Its image $U\subset\mathbb{P}^n_K$ (consisting of the lines in K^{n+1} intersecting T) is an affine patch of $\mathbb{P}^n_K$.

For a choice of linear bijection $T \cong K^n$, we obtain a bijection between

$\mathbb{A}^n_K = K^n$ and U called a

<u>chart (map)</u> of $\mathbb{P}^n_K$.

<u>Ex</u> For $i = 0, \dots, n$, we can take

$$T_i = \{ (x_0, \dots, x_n) \in K^{n+1} \mid x_i = 1 \}$$

and the i-th <u>standard chart (map)</u>

$$\varphi_i : K^n \hookrightarrow \mathbb{P}^n_K$$

$$(x_0, \dots, x_{i-1}, x_{i+1}, \dots, x_n) \mapsto [x_0 : \dots : x_{i-1} : 1 : x_{i+1} : \dots : x_n]$$

$$\left(\frac{x_0}{x_i}, \dots, \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, \dots, \frac{x_n}{x_i}\right) \mapsto [x_0 : \dots : x_n]$$

with image $U_i = \{ [x_0 : \dots : x_n] \in \mathbb{P}^n_K \mid x_i \neq 0 \}$.

$$\mathbb{P}^n_K \setminus U_i = \{ [x_0 : \dots : x_n] \mid x_i = 0 \}$$

$$\cong \{ [x_0 : \dots : x_{i-1} : x_{i+1} : \dots : x_n] \} = \mathbb{P}^{n-1}_K .$$

<u>Rmk</u> More generally, the complement of U in $\mathbb{P}^n_K$ consists of the lines in K^{n+1} through 0 that are parallel to T, i.e. that lie in

the n-dimensional linear subspace W of K^{n+1} parallel to T.

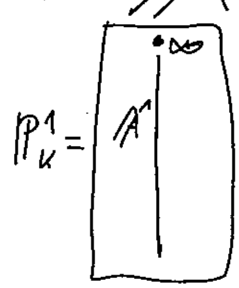
$\Rightarrow$ Identifying W with K^n, we obtain a bijection $\mathbb{P}^n_K \setminus \underbrace{U}_{\mathbb{A}^n_K} \cong (\text{lines through } 0 \text{ in } K^n) \cong \mathbb{P}^{n-1}_K$

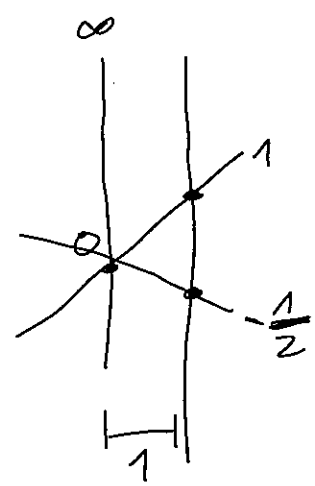
$$\rightsquigarrow \mathbb{P}^n_K = \mathbb{A}^n_K \sqcup \underbrace{\mathbb{P}^{n-1}_K}_{\text{"set of points at } \infty \text{"}}$$

__Ex__ $\mathbb{P}^0_K = \{\text{lines through } 0 \text{ in } K^1\} = \{*\}$

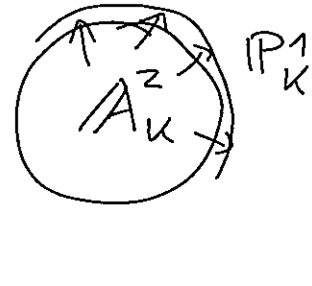
single pt.

$$\mathbb{P}^1_K = \mathbb{A}^1_K \sqcup \{\infty\}$$





$$\mathbb{P}^2_K = \mathbb{A}^2_K \sqcup \underbrace{\mathbb{P}^1_K}_{\text{pts at } \infty}$$

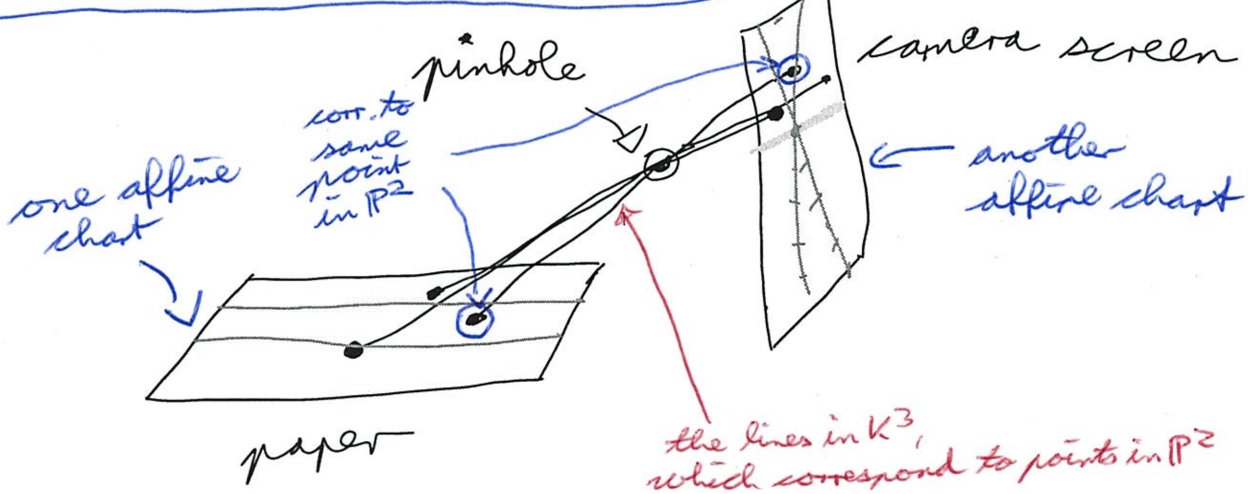


Rmk The standard affine patches $U_0, \dots, U_n$ cover $\mathbb{P}^n_K$: $\quad \mathbb{P}^n_K = \bigcup_{i=0}^n U_i$.

Def $U_i = \{[x_0 : \dots : x_n] \mid x_i \neq 0\}$.

$\Rightarrow \bigcup_{i=0}^n U_i = \{[x_0 : \dots : x_n] \mid x_i \neq 0 \text{ for some } i\}$

But there is (by def.) no point $[x_0 : \dots : x_n] \in \mathbb{P}^n_K$ with $x_0 = \dots = x_n = 0$. $\square$



Def A d-dimensional <u>linear subspace</u> L of $\mathbb{P}^n_K$ is the set of lines through 0 contained in a fixed $(d+1)$-dimensional linear subspace V of K^{n+1}.

Rmk Identifying V with K^{d+1}, we obtain a bijection $L \cong \mathbb{P}^d_K$.

Ex 0-dim. lin. subsp. of $\mathbb{P}^n$
$= $ single point in $\mathbb{P}^n_K$

Ex 1-dim. lin. subsp. are called <u>lines</u> in $\mathbb{P}^n_K$.

Ex 2 <u>planes</u>

Ex $(n-1)$ <u>hyperplanes</u>

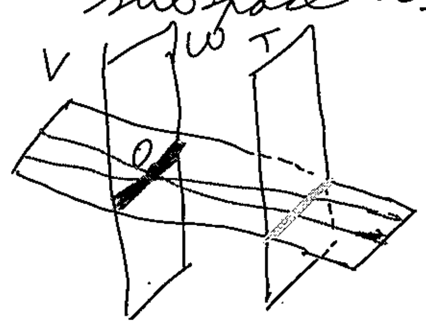
($\mathbb{P}^n_K \setminus U$ as above is a hyperplane in $\mathbb{P}^n_K$.)

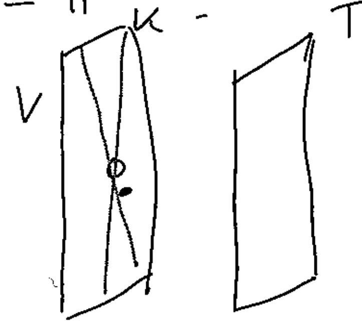
Ex (-1)-dim. lin. subsp. $= \emptyset$.

<u>Lemma 14.1.1</u> Let $\varphi: K^n \xrightarrow{\sim} U \subset \mathbb{P}^n_K$ be an affine chart and let $L \subseteq \mathbb{P}^n_K$ be a d-dimensional linear subspace. Then, <u>either</u>

a) $\varphi^{-1}(L) \subseteq K^n$ is an affine d-dimensional linear subspace and $L \cap (\mathbb{P}^n_K \setminus U)$ is a $(d-1)$-dimensional linear subspace of $\mathbb{P}^n_K \setminus U \cong \mathbb{P}^{n-1}_K$.

<u>or</u> b) $\varphi^{-1}(L) = \emptyset$ and L is a d-dimensional linear subspace of $\mathbb{P}^n_K \setminus U \cong \mathbb{P}^{n-1}_K$.

a) 

b) 

Pf Let T be an affine lin. subsp. of K^{n+1} corr. to the affine chart φ. Let W be the linear subspace of K^{n+1} containing 0 parallel to T. It corresponds to $\mathbb{P}^n \setminus U$.

Let V be the lin. subsp. of K^{n+1} corr. to L.

$\dim(T) = \dim(W) = n$

$\dim(V) = d+1$.

Either, a) $V \not\subseteq W$. $\Rightarrow$ $\dim(V \cap W) = d$, so $L \cap (\mathbb{P}^n \setminus U)$ is a $(d-1)$-dimensional linear subspace (consisting of the lines contained in $V \cap W$)

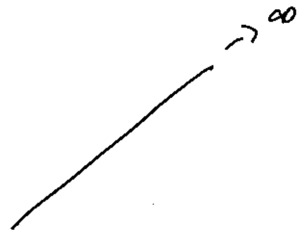
and $\dim(V \cap T) = d$, so $\varphi^{-1}(L) \cong V \cap T$ is an affine d-dimensional linear subspace of $K^n \cong T$.

Or, b) $V \subseteq W \Rightarrow L \subseteq \mathbb{P}^n \setminus U$, $\varphi^{-1}(L) = \emptyset$

$\square$

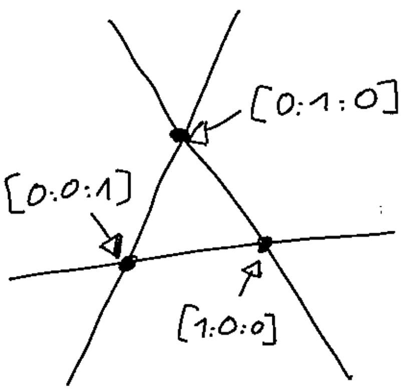
<u>Ex</u> The lines in $\mathbb{P}^2_k = \mathbb{A}^2_k \sqcup \mathbb{P}^1_k$ "are"

- The lines in $\mathbb{A}^2$ (with one point at ∞ each)



- The line $\mathbb{P}^1_k$ at ∞.

$$\mathbb{P}^2 \setminus U_0 = \{[x_0:x_1:x_2] \mid x_0 = 0\}$$



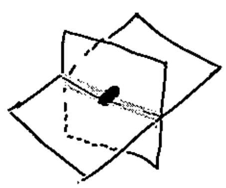
$$\mathbb{P}^2 \setminus U_1 = \{[x_0:x_1:x_2] \mid x_1 = 0\}$$

$$\mathbb{P}^2 \setminus U_2 = \{[x_0:x_1:x_2] \mid x_2 = 0\}$$

Lemma 14.1.2

Let L be an a-dim. lin. subspace of $\mathbb{P}^n$ and let M be a b-dim. lin. subspace of $\mathbb{P}^n$. Then, $L \cap M$ is a c-dimensional lin. subspace of $\mathbb{P}^n$ with $c \geq a+b-n$. $\left(\underbrace{\mathrm{codim}(L\cap M, \mathbb{P}^n)}_{= n-c} \leq \underbrace{\mathrm{codim}(L, \mathbb{P}^n)}_{= n-a} + \underbrace{\mathrm{codim}(M, \mathbb{P}^n)}_{= n-b}\right)$

Ex If L, M are lines in $\mathbb{P}^2$, then $L \cap M$ is a point or $L = M$.



Pf of Lemma Let $L, M \subseteq \mathbb{P}^n_K$ corr. to $V, W \subseteq K^{n+1}$

$\dim(V) = a+1$, $\dim(W) = b+1$

$\mathrm{codim}(V, K^{n+1}) = n-a$, $\mathrm{codim}(W, K^{n+1}) = n-b$

$\Rightarrow$ $V \cap W$ is a vector space with

$\mathrm{codim}(V \cap W, K^{n+1}) \leq (n-a) + (n-b)$

$$\Rightarrow \dim(L \cap M) = n - \mathrm{codim}(V \cap W, K^{n+1}) \geq n - (n-a) - (n-b) = a+b-n.$$

$\square$

14.2. Algebraic sets

<u>Def</u> A polynomial $f \in K[X_0, \dots, X_n]$ is <u>homogeneous of degree $d \geq 0$</u> (or a <u>form of degree d</u>) if every monomial in f has degree (exactly) d.

<u>Ex</u> $2X + 3Y$ hom. of deg. 1

<u>Ex</u> $2X + 3Y + 1$ not hom.

<u>Ex</u> $X^3 + 2X^2Y + Y^3$ hom. of degree 3

<u>Ex</u> 0 is homogeneous of <u>every</u> degree $d \geq 0$.

<u>Rmk</u> The hom. degree d pol. form a K-vector space.

<u>Rmk</u> Any pol. $f \in K[X_0, \dots, X_n]$ can be written uniquely as $f = \sum_{d=0}^{m} f_d$ with f_d hom. of degree d (called the <u>degree d part</u> of f).

<u>Rmk</u> If f is hom. of degree d and g is hom. of degree e, then fg is hom. of degree $d+e$.

Rmk If $f \in K[Y_0, \dots, Y_m]$ is hom. of degree d and $g_1, \dots, g_m \in K[X_0, \dots, X_n]$ are hom. of degree e, then $f(g_1, \dots, g_m)$ is hom. of degree $d \cdot e$.

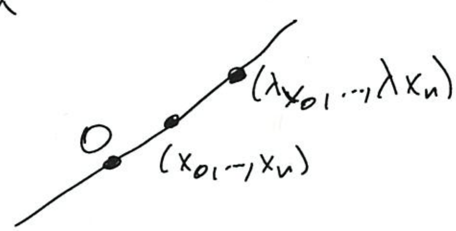
Rmk 14.2.1 If f is hom. of degree d, then

$$f(\lambda X_0, \dots, \lambda X_n) = \lambda^d f(X_0, \dots, X_n).$$

Def If $f \in K[X_0, \dots, X_n]$ is hom., we denote by

$$V_{\mathbb{P}^n_K}(f) = \{[x_0 : \dots : x_n] \in \mathbb{P}^n_K \mid f(x_0, \dots, x_n) = 0\}$$

independent of the choice of hom. coord. $x_0, \dots, x_n$ by Rmk 3.2.1!



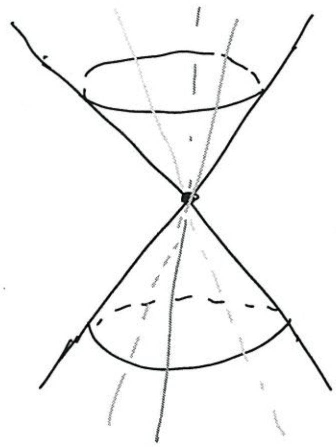
the corresponding set of zeros (the vanishing locus of f).

If $S \subseteq K[X_0, \dots, X_n]$ is a set of hom. pol., let

$$V_{\mathbb{P}^n_K}(S) = \{[x_0 : \dots : x_n] \in \mathbb{P}^n_K \mid f(x_0, \dots, x_n) = 0 \ \forall f \in S\} = \bigcap_{f \in S} V_{\mathbb{P}^n_K}(f).$$

A subset $A = V_{\mathbb{P}^n_K}(S)$ of this form is called algebraic.

Ex $f = x_1^2 + x_2^2 - x_0^2$



$\mathbb{V}(f) = \mathbb{V}_{k^3}(f) =$ cone

$\mathbb{V}_{\mathbb{P}^2}(f) =$ set of lines through O on the cone

Rmk $\mathbb{V}_{\mathbb{P}^n_k}(S) \subseteq \mathbb{P}^n_k$ is the set of lines through O contained in $\mathbb{V}(S) = \mathbb{V}_{k^{n+1}}(S)$.

Ex Any linear subspace of $\mathbb{P}^n_k$ is algebraic.

Def Let $A \subseteq \mathbb{P}^n_k$ be any subset.

The set $\mathcal{C}(A) = \{0\} \cup \{0 \neq (x_0, \dots, x_n) \in k^{n+1} \mid [x_0 : \dots : x_n] \in A\}$
$\subseteq k^{n+1}$

(the union of $\{0\}$ and the lines in k^{n+1} representing the points in $A \subseteq \mathbb{P}^n_k$)

is called the <u>affine cone</u> of A.

Rmk 14

~~Lemma 3~~.2.2 If $A \subseteq \mathbb{P}^n_k$ is algebraic, then $\ell(A) \subseteq k^{n+1}$ is algebraic. (def. by the same eqs.)

~~Pf If $A = V_{\mathbb{P}^n_k}(S) \neq \emptyset$, then $\ell(A) = V_{k^{n+1}}(S)$.~~

~~If $A = \emptyset$, then $\ell(A) = \{0\}$. ∎~~

Rmk $\ell(A \cap B) = \ell(A) \cap \ell(B)$

As before (Lemma 2.2):

Rmk a) $\bigcap_\alpha V_{\mathbb{P}^n}(S_\alpha) = V_{\mathbb{P}^n}\left(\bigcup_\alpha S_\alpha\right)$

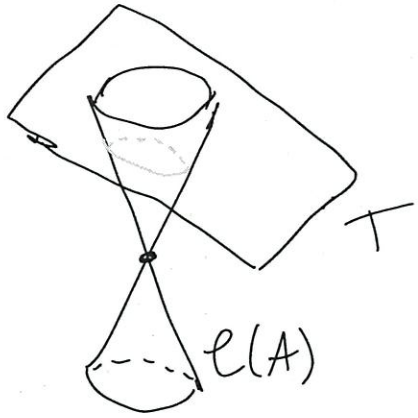
b) $V_{\mathbb{P}^n}(S) \cup V_{\mathbb{P}^n}(T) = V_{\mathbb{P}^n}(\{fg \mid f \in S, g \in T\})$

c) $V_{\mathbb{P}^n}(\emptyset) = V_{\mathbb{P}^n}(0) = \mathbb{P}^n$

d) $V_{\mathbb{P}^n}(1) = \emptyset$.

Hence, we again obtain a Zariski topology whose closed sets are the algebraic sets.

Ex Any affine patch $U \subseteq \mathbb{P}^n_k$ (complement of hyperplane) is open.



<u>Lemma 14.2.3</u> Any affine chart $\varphi : K^n \longrightarrow U \subseteq \mathbb{P}^n_K$

is continuous:

If $A \subseteq \mathbb{P}^n_K$ is algebraic, then $\varphi^{-1}(A) \subseteq K^n$ is algebraic.

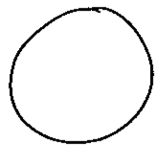
<u>Pf</u> $\varphi^{-1}(A) \subseteq K^n$ "is" the intersection of the affine cone $\mathcal{C}(A)$ with the affine linear subspace T corresponding to the chart. $\square$

<u>Concretely</u> If $\varphi = \varphi_i$ is the i-th standard affine chart, $A = V_{\mathbb{P}^n}(S)$, then

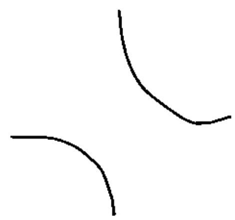
$$\varphi^{-1}(A) = \{(x_0, \dots, x_{i-1}, x_{i+1}, \dots, x_n) \in K^n \mid f(x_0, \dots, x_{i-1}, 1, x_{i+1}, \dots, x_n) = 0 \ \forall f \in S\}.$$

<u>Ex</u> $A = V_{\mathbb{P}^2}(x_1^2 + x_2^2 - x_0^2)$.

$$\varphi_0^{-1}(A) = V_{K^2}(x_1^2 + x_2^2 - 1)$$



$$\varphi_1^{-1}(A) = V_{K^2}(1 + x_2^2 - x_0^2)$$



The preimage $\varphi^{-1}(A)$ is a conic section for any affine chart φ.

We constructed a map

$$\{\text{alg. subset } A \text{ of } \mathbb{P}^n\} \longrightarrow \{\text{alg. subset } B \text{ of } K^n\}$$
$$A \longmapsto \varphi^{-1}(A)$$

<u>Q</u> How to produce $A \subseteq \mathbb{P}^n_K$ from $B \subseteq K^n$?

<u>A</u> Take $A = \overline{\varphi(B)}$. What are equations defining A?

Def Let $f \in K[X_1, \dots, X_n]$ be a polynomial of degree d and let f_e be its (hom.) degree e. The <u>homogenization</u> of $f = \sum_e f_e$ (at X_0) is the hom. degree d pol.

$$\tilde{f} = \sum_e f_e \cdot X_0^{d-e} = X_0^d f\left(\frac{X_1}{X_0}, \dots, \frac{X_n}{X_0}\right)$$

Ex $f = x_1^2 + x_2^2 - 1 \rightsquigarrow \tilde{f} = x_1^2 + x_2^2 - x_0^2$

Note $\tilde{f}(1, x_1, \dots, x_n) = f(x_1, \dots, x_n)$

Lemma 14.2.4 Let $B = V_{K^n}(I)$ for an ideal $I \subseteq K[X_1, \dots, X_n]$. Let $\varphi = \varphi_0$ be the 0-th standard chart of $\mathbb{P}^n_K$. Then,

$\overline{\varphi(B)} = V_{\mathbb{P}^n_K}(S)$ where $S \subseteq K[X_0, \dots, X_n]$ is the set of homogenizations $\tilde{f}$ of the elements $f \in I$ at X_0.

Pf HW.

Cor 14.2.5

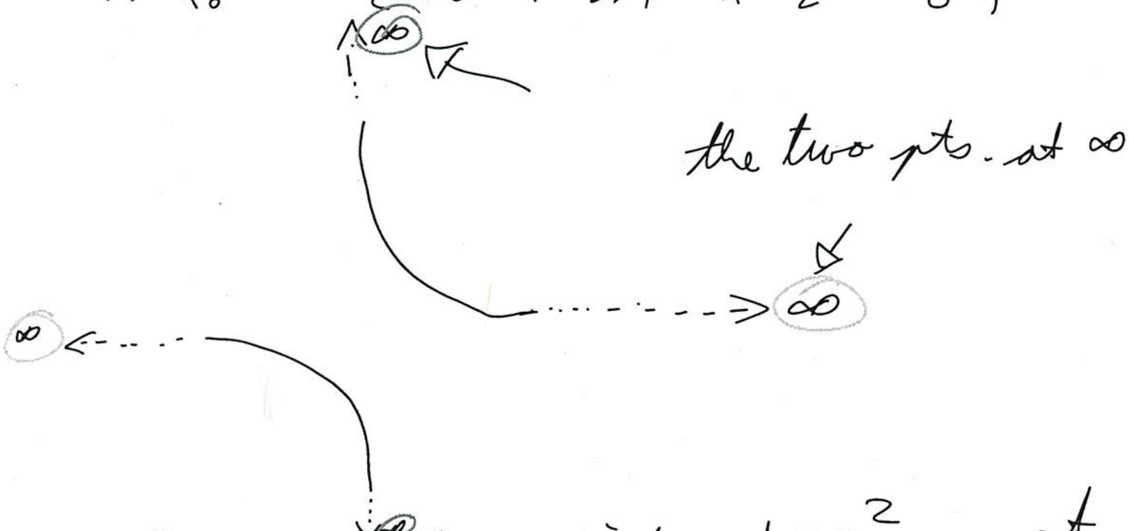
$$\varphi^{-1}\left(\overline{\varphi(B)}\right) = B \text{ for any affine chart.}$$

(We only add points at ∞ to B to obtain $\overline{\varphi(B)}$.)

Pf This follows from the lemma and the previous note. $\square$

Ex $B = \{(x_1, x_2) \mid x_1 x_2 = 1\}$

$\rightsquigarrow A = \overline{\varphi_0(B)} = \{[x_0 : x_1 : x_2] \mid x_1 x_2 = x_0^2\}$



What are the points at ∞?

pt. at ∞

$$A \setminus \varphi_0(B) = \{[x_0 : x_1 : x_2] \mid x_1 x_2 = x_0^2,\ x_0 = 0\}$$

$$= \{[0 : x_1 : x_2] \mid x_1 x_2 = 0\}$$

$$= \{[0:0:1], [0:1:0]\}$$

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

Then, S is the set of homogenizations of elements of I. Unfortunately, the homogenizations $\tilde f_1, \dots, \tilde f_m$ don't always suffice!

__Ex__ $I = (x_1^2 + x_2,\ x_1) \quad = (x_2, x_1)$

$\rightsquigarrow \quad x_1^2 + x_0 x_2 = 0,\ x_1 = 0 \qquad\qquad x_2 = 0,\ x_1 = 0 \quad \rightsquigarrow$ one point $[1:0:0]$

$\Updownarrow$

$x_0 x_2 = 0,\ x_1 = 0$

$\rightsquigarrow$ two points $[0:0:1], [1:0:0]$

__Thm 14.2.6__ Let $f \in K[x_1, \dots, x_n]$ with homogenization $\tilde f$ at x_0. Then, $\overline{\varphi_0(V(f))} = V_{\mathbb{P}^n}(\tilde f)$.

~~Pf "$\subseteq$" clear~~

Pf If $g = fh \in (f)$, then $\tilde g = \tilde f \tilde h$. $\Rightarrow \overline{\varphi_0(V(f))} = V_{\mathbb{P}^n_K}(\{\tilde f \tilde h \mid h \in K[x_1, \dots, x_n]\}) = V_{\mathbb{P}^n}(\tilde f)$. $\square$

~~"$\supseteq$" Let $g \in (f)$ with homogenization $\tilde g = \tilde f \tilde h$~~

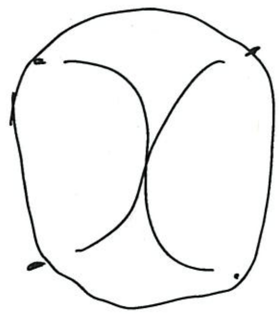
~~$g = fh,\ h \in K[x_1, \dots, x_n]$~~ ~~Lemma 3.2.4~~

~~If $\tilde f(P) = 0$, then $\tilde g(P) = 0$.~~

~~$\Rightarrow V_{\mathbb{P}^n_K}(\tilde f) = V_{\mathbb{P}^n_K}(\{\text{hom. } \tilde g \text{ of } g \in (f)\}) = \varphi_0(V(f))$.~~ $\square$

Cor 14.2.7 Any affine chart $\varphi : K^n \hookrightarrow \mathbb{P}^n_K$ is an open map (sending open sets to open sets).

Pf



Let $U = K^n \setminus A$ be open in K^n.

$\Rightarrow \varphi(U) = \mathbb{P}^n_K \setminus \left(\left(\mathbb{P}^n_K \setminus \operatorname{im}(\varphi) \right) \cup \overline{\varphi(U)} \right)$

is open in $\mathbb{P}^n_K$.

$\square$

Cor 14.2.8 A subset $A \subseteq \mathbb{P}^n_K$ is alg. if and only if $\varphi_i^{-1}(A) \subseteq K^n$ is alg. for all standard affine charts φ_i.

$\rightsquigarrow$ You obtain the topology on $\mathbb{P}^n_K$ by glueing together the topologies on the affine charts.

14.3. Vanishing ideals

Def An ideal $I \subseteq K[x_0, \dots, x_n]$ is homogeneous if it is generated by (finitely many) homogeneous polynomials.

Thm 14.3.1 I is hom. if and only if for every $d \geq 0$ and $f \in I$, the degree d part f_d also lies in I.

Pf "$\Leftarrow$" $f = \sum_d f_d$

$\Rightarrow$ I is gen. by the hom. parts of the elements of I

"$\Rightarrow$" Let $I = (g_1, \dots, g_m)$ with g_i hom. of degree d_i.

Let $f \in I$ with degree d part f_d.

Write $f = \sum_i g_i h_i$ with

$h_1, \dots, h_m \in K[x_0, \dots, x_n]$.

Let $h_{i,e}$ be the degree e part of h_i.

$$\Rightarrow f_d = \sum_i \underbrace{g_i}_{\text{hom. of deg. } d_i} \underbrace{h_{i,d-d_i}}_{\text{deg. } d-d_i} \in I.$$

$\square$

Def For any homogeneous ideal $I \subseteq K[X_0, \dots, X_n]$, we let $\mathcal{V}_{\mathbb{P}^n_K}(I) := \mathcal{V}_{\mathbb{P}^n_K}(\{f \in I \text{ homogeneous}\})$.

Rmk $\mathcal{V}_{\mathbb{P}^n_K}(\text{ideal gen. by } S) = \mathcal{V}_{\mathbb{P}^n_K}(S)$ for any set S of hom. pol.

Rmk $\mathcal{C}(\mathcal{V}_{\mathbb{P}^n_K}(I)) = \{0\} \cup \mathcal{V}_{K^{n+1}}(I)$

Def The <u>vanishing ideal</u> of a subset $A \subseteq \mathbb{P}^n_K$ is the ideal $\mathcal{J}_{\mathbb{P}^n}(A) \subseteq K[X_0, \dots, X_n]$ generated by the homogeneous pol. f vanishing on A (s.t. $A \subseteq \mathcal{V}_{\mathbb{P}^n_K}(f)$).

Lemma 14.3.2

If $A \neq \emptyset$, then $\mathcal{J}(A) = \mathcal{J}(\mathcal{C}(A))$.

If $A = \emptyset$, then $\mathcal{J}(A) = K[X_0, \dots, X_n]$.

(although $\mathcal{J}(\mathcal{C}(A)) = \mathcal{J}(\{0\}) = (X_0, \dots, X_n)$).

Pf $A = \emptyset$: clear

$A \neq \emptyset$: "$\subseteq$" If a hom. pol. f vanishes on A, it vanishes on $C(A)$.

"$\supseteq$" If a pol. $f \in K[X_0, \dots, X_n]$ vanishes on $C(A) \subseteq K^{n+1}$, so do its homogeneous parts. They must then vanish on A. $\square$

14.4. Projective Nullstellensatz

From now on, we again assume that K is algebraically closed.

Thm 14.4.1 (Weak proj. Nsts)

Let $I \subseteq K[X_0, \dots, X_n]$ be a hom. ideal. Then, the following are equivalent:

a) $V_{\mathbb{P}^n_K}(I) = \emptyset$

b) $(X_0, \dots, X_n) \subseteq \sqrt{I}$

vanishes only at 0 in K^{n+1} ($\Rightarrow$ at no point in $\mathbb{P}^n_K$)

c) $X_0^m, \dots, X_n^m \in I$ for some $m \geq 0$.

Pf b) $\Leftrightarrow$ c): clear

a) $\Leftrightarrow$ b):

$$V_{\mathbb{P}^n_k}(I)=\emptyset$$

$$\Leftrightarrow \ell(V_{\mathbb{P}^n_k}(I)) = \{0\}$$

$$\ell(V_{\mathbb{P}^n_k}(I)) = \{0\}\cup V_{k^{n+1}}(I)$$

$$\Leftrightarrow V_{k^{n+1}}(I) \subseteq \{0\}$$

$$\Leftrightarrow \mathbb{I}(V_{k^{n+1}}(I)) \supseteq \mathbb{I}(\{0\}) = (x_0,\dots,x_n)$$

$$\mathbb{I}(V_{k^{n+1}}(I)) \underset{\text{Hilbert's Nsts}}{=} \sqrt{I}$$

$\square$

Cor 14.4.2 (Proj. Nsts) For any hom. id. I,

$$\mathbb{I}(V_{\mathbb{P}^n_k}(I)) = \begin{cases} \sqrt{I}, & (x_0,\dots,x_n) \not\subseteq \sqrt{I}, \\ k[x_0,\dots,x_n], & (x_0,\dots,x_n) \subseteq \sqrt{I}. \end{cases}$$

Pf second case: $V_{\mathbb{P}^n_k}(I)=\emptyset \Rightarrow \mathbb{I}(V_{\mathbb{P}^n_k}(I)) = k[x_0,\dots,x_n]$

first case: $\mathbb{I}(V_{\mathbb{P}^n_k}(I)) \underset{\text{Lemma 14.3.2}}{=} \mathbb{I}(\ell(V_{\mathbb{P}^n_k}(I))) = \mathbb{I}(V_{k^{n+1}}(I)) \underset{\text{Hilbert's Nsts}}{=} \sqrt{I}$.

$\square$

14.5. Irreducibility

Def An alg. subset $\emptyset \neq A \subseteq \mathbb{P}^n_K$ is *irreducible* if you can't write $A = A_1 \cup A_2$ with any alg. sets $A_1, A_2 \subsetneq A_2$.

Ex One point, $\mathbb{P}^n_K$

Thm 14.5.1 Let $A \neq \emptyset$ be an alg. subset of $\mathbb{P}^n_K$.

The following are equivalent:

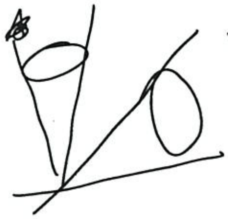
a) A is irreducible.

b) $C(A)$ is irreducible.

c) $J(A)$ is a prime ideal.

Pf b) $\Leftrightarrow$ c) $\quad J(C(A)) = J(A)$

b) $\Rightarrow$ a) $\quad A = A_1 \cup A_2, \quad A_1, A_2 \subsetneq A$



$C(A) = C(A_1) \cup C(A_2), \quad C(A_1), C(A_2) \subsetneq C(A)$

a) $\Rightarrow$ c) $\quad$ Say $f, g \notin J(A)$ with $fg \in J(A)$.

Let $\deg(f) = d$ and f_d be the degree d part of f.

Let $\deg(g) = e$ and g_e be the degree e part of g.

W.l.o.g. $f_d, g_e \notin I(A)$.

(Otherwise, replace f by $f-f_d$ or g by $g-g_e$, reducing the degree of f or g.)

$\Rightarrow$ $\deg(fg)=d+e$ and $f_d g_e$ is the degree $d+e$ part of fg.

$I(A)$ hom. ideal $\underset{\substack{\uparrow \\ \text{Thm 3.3.1}}}{\Rightarrow}$ $f_d g_e \in I(A)$

Take $A_1 = A \cap V_{\mathbb{P}^n_k}(f_d)$,

$A_2 = A \cap V_{\mathbb{P}^n_k}(g_e)$.

$f_d g_e \in I(A) \Rightarrow A_1 \cup A_2 = A$

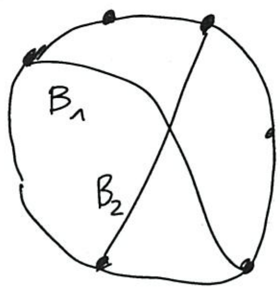
$f_d \notin I(A) \Rightarrow A_1 \subsetneq A$

$g_e \notin I(A) \Rightarrow A_2 \subsetneq A$. $\square$

Thm 14.5.2 Let $A \subseteq \mathbb{P}^n_k$ be irred. and let φ be an affine chart. Then,

$$\varphi^{-1}(A) = \emptyset \quad \text{or } \varphi^{-1}(A) \text{ is irreducible.}$$

Pf If $\emptyset \neq \varphi^{-1}(A) = B_1 \cup B_2$, $B_1, B_2 \subsetneqq \varphi^{-1}(A)$,



then

$$A = \overline{\varphi(B_1)} \cup \overline{\varphi(B_2)} \cup \underbrace{(A \setminus \mathrm{im}(\varphi))}_{\text{closed}}$$

with

$$\overline{\varphi(B_1)} \subsetneqq A, \quad \overline{\varphi(B_2)} \subsetneqq A,$$

$$A \setminus \mathrm{im}(\varphi) \subsetneqq A. \qquad \square$$

Rmk If $A \neq \emptyset$ and for <u>every</u> affine chart φ, $\varphi^{-1}(A) = \emptyset$ or $\varphi^{-1}(A)$ is irred., then A is irred.

Warning It doesn't suffice to consider just the standard affine charts φ_i. For example $\{[0:1], [1:0]\} \subseteq \mathbb{P}^1_k$ is reducible although the intersections with $U_0 = \{[x_0 : x_1] \mid x_0 \neq 0\}$ and $U_1 = \{[x_0 : x_1] \mid x_1 \neq 0\}$ each consist of just one point.

14.6. Dimension

Def The dimension of an (irred.) alg. set $\emptyset \neq V \subseteq \mathbb{P}^n_K$ is the largest length d of a chain

$$V_0 \subsetneq V_1 \subsetneq \dots \subsetneq V_d \subseteq V$$

of irred. alg. subsets V_i.

Thm 14.6.1

For any alg. $\emptyset \neq V \subseteq \mathbb{P}^n_K$:

a) $\dim(V) = \dim(C(V)) - 1$

b) If V is irreducible and $\varphi : K^n \longrightarrow \mathbb{P}^n_K$ is an affine patch with $\varphi^{-1}(V) \neq \emptyset$

$$\dim(V) = \dim(\varphi^{-1}(V)).$$

Rmk b) can fail if V is reducible:

e.g. $V = \{\text{point}\} \cup (\text{line at infinity})$

$\Rightarrow \varphi^{-1}(V) = \{\text{point}\}$.

Pf (for V irred.) ~~By Thm 3.5.3, we can assume that V is irreducible (even in a)).~~

For any chain

$$V_0 \subsetneq \cdots \subsetneq V_d \subseteq V \text{ of irred. sets,}$$

we obtain a chain

$$\{0\} = \ell(\emptyset) \subsetneq \ell(V_0) \subsetneq \cdots \subsetneq \ell(V_d) \subseteq \ell(V) \text{ of irred. sets.}$$

$$\Longrightarrow \dim(\ell(V)) \geq \dim(V) + 1$$

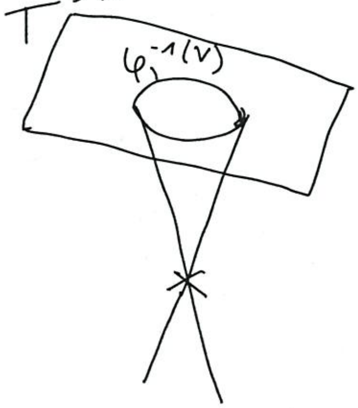
For any chain

$$W_0 \subsetneq \cdots \subsetneq W_d \subseteq \varphi^{-1}(V) \text{ of irred. sets,}$$

we obtain a chain

$$\overline{\varphi(W_0)} \subsetneq \cdots \subsetneq \overline{\varphi(W_d)} \subseteq V \text{ of irred. sets.}$$

$$\Longrightarrow \dim(V) \geq \dim(\varphi^{-1}(V)).$$



Let $0 \notin T \subseteq K^{n+1}$ be an n-dim. affine lin. subspace corr. to φ. Then $\ell(V)$ is the Zariski closure of the join of $\{0\}$ and $\ell(V) \cap T \cong \varphi^{-1}(V)$.

By problem 4 on pset 8, we then have $\dim(\ell(V)) = \dim(\varphi^{-1}(V)) + 1$. $\square$

Def Let $V, W \subseteq \mathbb{P}^n$ be irreducible alg. sets.

$$\begin{aligned}\operatorname{codim}(V, W) &:= \dim(W) - \dim(V) \\ &= \dim(\mathcal{C}(W)) - \dim(\mathcal{C}(V)) \\ &= \operatorname{codim}(\mathcal{C}(V), \mathcal{C}(W)).\end{aligned}$$

Rmk $\operatorname{codim}(V, W)$ is the largest $d \geq 0$ s.t. there is a chain $V = V_0 \subsetneq \cdots \subsetneq V_d = W$ of irred. alg. sets.

Thm 14.6.2 Let $V_1, V_2 \subseteq \mathbb{P}^n$ be irreducible alg. sets with $\operatorname{codim}(V_1, \mathbb{P}^n) + \operatorname{codim}(V_2, \mathbb{P}^n) \leq n$.

Then, a) $V_1 \cap V_2 \neq \emptyset$ and

b) every irred. comp. A of $V_1 \cap V_2$ satisfies

$$\operatorname{codim}(A, \mathbb{P}^n) \leq \operatorname{codim}(V_1, \mathbb{P}^n) + \operatorname{codim}(V_2, \mathbb{P}^n).$$

Pf Apply Cor 13.4.3 to the affine cones:

Any irred. comp. B of $\mathcal{C}(V_1) \cap \mathcal{C}(V_2) = \mathcal{C}(V_1 \cap V_2)$ satisfies

$$\operatorname{codim}(B, K^{n+1}) \leq \operatorname{codim}(\mathcal{C}(V_1), K^{n+1}) + \operatorname{codim}(\mathcal{C}(V_2), K^{n+1})$$
$$= \operatorname{codim}(V_1, \mathbb{P}^n) + \operatorname{codim}(V_2, \mathbb{P}^n),$$
$$\leq n.$$

This shows b) since $\mathcal{C}(A)$ is an irred. comp. of $\mathcal{C}(V_1 \cap V_2)$.

For a), note that $0 \in \mathcal{C}(V_1) \cap \mathcal{C}(V_2)$, so $\mathcal{C}(V_1) \cap \mathcal{C}(V_2) \neq \emptyset$, so $\mathcal{C}(V_1 \cap V_2)$ contains at least one irred. comp. B, which, as we have seen above, has dimension $\dim(B) \geq 1$. $\Rightarrow B \neq \{0\}$, so $\ell(V_1 \cap V_2) \neq \emptyset$. $\square$

Ex Any two curves in $\mathbb{P}^2$ intersect.

Any curve and surface in $\mathbb{P}^3$ intersect.

Any three surfaces in $\mathbb{P}^3$ intersect.

14.7. Products

For details, see Chapters 4 and 5 in Shafarevich (Basic Algebraic Geometry 1).

Rmk $K^n \times K^m = K^{n+m}$, but $\mathbb{P}^n \times \mathbb{P}^m$ is not $\mathbb{P}^{n+m}$!

Def A set $V \subseteq \mathbb{P}^n \times \mathbb{P}^m$ is algebraic if for each pair of (standard) chart maps φ, ψ of $\mathbb{P}^n, \mathbb{P}^m$, the subset

$\{(P,Q) \mid (\varphi(P), \psi(Q)) \in V\}$ of $K^n \times K^m = K^{n+m}$

is algebraic.

Exe $V := \{([x_0 : x_1 : x_2], [y_0 : y_1]) : x_0^3 y_0 y_1 + 2x_1 x_2^2 y_1^2 = 0\}$

is an algebraic subset of $\mathbb{P}^2 \times \mathbb{P}^1$.

More generally:

Rmk $V \subseteq \mathbb{P}^n \times \mathbb{P}^m$ is algebraic if and only if there are polynomials $f_1, \dots, f_k \in K[x_0, \dots, x_n, y_0, \dots, y_m]$ which are homogeneous in $x_0, \dots, x_n$ and homogeneous in $y_0, \dots, y_m$ (not necessarily of the same degree) such that

$V = \{([x_0 : \dots : x_n], [y_0 : \dots : y_m]) : \forall i : f_i(x_0, \dots, x_n, y_0, \dots, y_m) = 0\}$.

(Note: If f is hom. of deg. d in $x_0, \dots, x_n$ and of deg. e in $y_0, \dots, y_m$, then

$f(\lambda x_0, \dots, \lambda x_n, \mu y_0, \dots, \mu y_m) = \lambda^d \mu^e f(x_0, \dots, x_n, y_0, \dots, y_m)$,

so whether $f(x_0, \dots, x_n, y_0, \dots, y_m) = 0$ only depends on the points $[x_0 : \dots : x_n] \in \mathbb{P}^n$ and $[y_0 : \dots : y_m] \in \mathbb{P}^m$, not on the choice of projective coordinates.)

Def Let $V \subseteq \mathbb{P}^n \times \mathbb{P}^m$, $W \subseteq \mathbb{P}^N \times \mathbb{P}^M$ be alg. subsets.

A <u>morphism</u> $\alpha : V \to W$ is a map such that for all (standard) chart maps $\varphi_1, \varphi_2, \psi_1, \psi_2$ on $\mathbb{P}^n, \mathbb{P}^m, \mathbb{P}^N, \mathbb{P}^M$, the map

$$K^n \times K^m \supseteq \varphi^{-1}(V) \dashrightarrow K^N \times K^M$$

$$(P,Q) \longmapsto \psi^{-1}(\alpha(\varphi(P,Q)))$$

is a rational map, defined wherever the above map makes sense, i.e. wherever $\alpha(\varphi(P,Q)) \in \psi(K^N \times K^M)$.

Here, we let $\varphi(P,Q) = (\varphi_1(P,Q), \varphi_2(P,Q))$
and $\psi(P,Q) = (\psi_1(P,Q), \psi_2(P,Q))$.

$$\begin{tikzcd}
\varphi^{-1}(V) \arrow[r, dashed] \arrow[d, "\varphi"'] & K^N \times K^M \arrow[d, "\psi"] \\
V \arrow[r, "\alpha"'] & W
\end{tikzcd}$$

We similarly define alg. subsets of the product of any number of projective spaces and morphisms between any two such subsets.

Ese

$$\alpha : V^{\subseteq \mathbb{P}^n} \longrightarrow \mathbb{P}^m$$

$$[x_0 : \dots : x_n] \longmapsto [f_0(x_0, \dots, x_n) : \dots : f_m(x_0, \dots, x_n)]$$

is a morphism (well-defined) if $f_0, \dots, f_m \in K[x_0, \dots, x_n]$ are homogeneous polynomials of the same degree d which have no common root on V:

$V_V(f_0, \dots, f_m) = \emptyset$:

Using the 0-th std. chart maps on $\mathbb{P}^n$ and $\mathbb{P}^m$, the corr. rational map is given by

$$(x_1, \dots, x_n) \longmapsto \left(\frac{f_1(1, x_1, \dots, x_n)}{f_0(1, x_1, \dots, x_n)}, \dots, \frac{f_m(1, x_1, \dots, x_n)}{f_0(1, x_1, \dots, x_n)} \right)$$

(when $f_0(1, x_1, \dots, x_n) \neq 0$).

<u>Warning</u> The "projection" $\mathbb{P}^2 \dashrightarrow \mathbb{P}^1$, $[x_0 : x_1 : x_2] \mapsto [x_0 : x_1]$ is not well-defined at $[0:0:1]$.

<u>Warning</u> Not every morphism is of the above form!
You might need different hom. pol. at different points, just like a rat. fct. $f = \frac{a}{b}$ might be def. at points with $a(P) = b(P) = 0$ and there might not be a single choice of a, b that works for all points where f is defined. (HW).

~~Let M~~

For example:

<u>Def</u> Let $n \geq 1$. The <u>Veronese map</u> of degree $d \geq 1$ is the map $\mathbb{P}^n \longrightarrow \mathbb{P}^{m-1}$ defined by the $m := \binom{n+d-1}{d}$ monomials in $x_0, \dots, x_n$ of degree d.

<u>Ex</u>

$$\begin{aligned} \mathbb{P}^1 &\longrightarrow \mathbb{P}^3 \\ [x_0 : x_1] &\longmapsto [x_0^3 : x_0^2 x_1 : x_0 x_1^2 : x_1^3] \end{aligned}$$

is the degree 3 Veronese map on $\mathbb{P}^1$.

Another example:

<u>Def</u> Let $n, m \geq 1$. The <u>Segre map</u> is the map

$$\begin{aligned} \mathbb{P}^n \times \mathbb{P}^m &\longrightarrow \mathbb{P}^{(n+1)(m+1)-1} \\ ([x_0 : \dots : x_n], [y_0 : \dots : y_m]) &\longmapsto [x_0 y_0 : x_0 y_1 : \dots : x_n y_m] \end{aligned}$$

def. by the products $x_i y_j$.

Ese (Let $K=\mathbb{C}$.) $V = \mathcal{V}_{\mathbb{P}^2}(X_1^2+X_2^2-X_0^2) \longrightarrow \mathbb{P}^1$

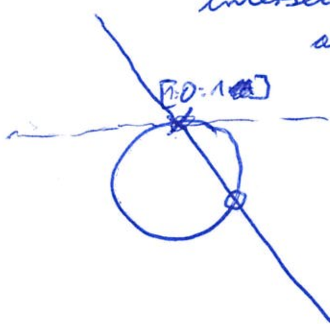
$[x_0 : x_1 : x_2] \longmapsto [x_1 : x_2 - x_0]$ unless $x_1 = x_2 - x_0 = 0$

$[x_2 + x_0 : -x_1]$ unless $x_2 + x_0 = x_1 = 0$

("The slope of the line connecting $[1:0:1]$ and $[x_0:x_1:x_2]$")

$[y_0^2+y_1^2 : -2y_0y_1 : y_0^2-y_1^2] \longleftarrow [y_0 : y_1]$

("The second pt. of intersection of V and the line of slope $\frac{y_1}{y_0}$ through $[1:0:1]$.")



Rmk Up to a change of basis, the inverse map is the degree 2 Veronese map $\mathbb{P}^1 \longrightarrow \mathbb{P}^2$.

$[2(x_2-x_0)x_1 : (x_2-x_0)^2 - x_1^2 : -((x_2-x_0)^2+x_1^2)]$

$x_1y_1 = (x_2-x_0)y_0$

$x_1^2+x_2^2-x_0^2=0$

$x_1^2y_1^2 + x_2^2y_1^2 - x_0^2y_1^2 = 0$

$(x_2-x_0)^2y_0^2 + (x_2^2 - x_0^2)y_1^2 = 0$

$(x_2-x_0)y_0^2 = (x_0+x_2)y_1^2$

$(x_0-x_2)y_0^2 = (x_2+x_0)y_1^2$

$x_0 = y_0^2 + y_1^2$

$x_2+x_0 = 2y_0^2$

$x_2-x_0 = 2y_1^2$

$x_0 = y_0^2 - y_1^2$

$x_2 = y_0^2 + y_1^2$

$x_1 = 2y_0y_1$

15. Images

Rmk We've seen before, that morphisms $\varphi: V \to W$ between alg. subsets V, W of affine space often have a nonclosed image.

(E.g. proj. of $V(XY-1)$ onto X-axis)

This can't happen if V is an alg. subset of projective space:

Thm 15.1 If V is an alg. subset of $\mathbb{P}^n$, then the image of any morphism $\varphi: V \to W$ ($W \subseteq \mathbb{P}^m$) is closed (= algebraic).

Rmk This implies that any such morphism is a closed map.

Pf The graph
$$\Gamma := \{(P, \varphi(P)) \mid P \in V\} = \{(P, Q) \mid Q = \varphi(P)\}$$
is an algebraic subset of $V \times W \subseteq \mathbb{P}^n \times \mathbb{P}^m$. (!)

It is therefore described by polynomials $f_1, \dots, f_k$ in $X_0, \dots, X_n, Y_0, \dots, Y_m$ which are homogeneous in $X_0, \dots, X_n$ and homogeneous in $Y_0, \dots, Y_m$.

Now:

$[b_0 : \ldots : b_m] \notin \psi(V)$

$$\Updownarrow$$

$f_1(X_0, \ldots, X_n, b_0, \ldots, b_m), \ldots \in K[X_0, \ldots, X_n]$ have no common root in $\mathbb{P}^n$

$$\Updownarrow \text{ Proj. Nsts.}$$

$$\underbrace{\exists\, e \geq 0 : (X_0, \ldots, X_n)^e \subseteq (f_1(X_0, \ldots, b_0, \ldots), f_2(\ldots), \ldots)}$$

$$\Updownarrow$$

Every hom. pol. $g \in K[X_0, \ldots, X_n]$ of degree e is a lin. comb.

$$g = \sum f_i(X_0, \ldots, b_0, \ldots)\, h_i(X_0, \ldots) \qquad (I)$$

with $h_i \in K[X_0, \ldots, X_n]$.

(If f_i is hom. of degree d_i in $X_0, \ldots, X_n$, taking the hom. degree e part of (I), w.l.o.g. h_i is hom. of degree $e - d_i$.)

let F_d be the vector space of hom. deg. d pol. in $X_0, \ldots, X_n$.

$$\Updownarrow$$

The linear map $F_{e-d_1} \times \cdots \times F_{e-d_k} \longrightarrow F_e$

$$(h_1, \ldots, h_k) \longmapsto \sum_i f_i(X_0, \ldots, b_0, \ldots)\, h_i(X_0, \ldots)$$

is surjective.

$$\Updownarrow$$

let $q = \dim(F_e)$.

Some $q \times q$ - minor of the matrix representing this linear map is $\neq 0$.

Note: The entries of the matrix are (hom.) pol. in $b_0, \ldots, b_m$ (of the same degree), so the set of such $(b_0, \ldots, b_m)$ is an open subset of K^{m+1}. $\square$

Cor 15.2 If $V \subseteq \mathbb{P}^n$ is an irreducible alg. subset, all morphisms $\psi: V \to K^m$ are constant (im. $= \{pt\}$).

Pf W.l.o.g. $m=1$. We have a morphism $\psi: V \to \cancel{K}\,\mathbb{P}^1$, whose image doesn't contain ∞.

$\psi(V) \subseteq \cancel{K}\,\mathbb{P}^1$ is closed.

$\Rightarrow \psi(V) = \cancel{K}\,\mathbb{P}^1$ or $\psi(V)$ is finite

(impossible)

$\Downarrow$ V irred. $\Rightarrow \overline{\psi(V)}$ irred.

$\psi(V)$ is a point.

$\square$

Cor 15.3 ~~Also~~ If V is an alg. subset of $\mathbb{P}^{n_1}\times\dots\times\mathbb{P}^{n_k}$, then any morphism $\varphi: V \to W$ is closed.

Pf (sketch) Compose with the Segre map
$$\mathbb{P}^{n_1}\times\dots\times\mathbb{P}^{n_k} \longrightarrow \mathbb{P}^{(n_1+1)\cdots(n_k+1)-1},$$
which is an isomorphism onto its image. (Apply the Thm to the image of V in the RHS.) $\square$

Cor 15.4 The join J of any disjoint alg. subsets V, W of $\mathbb{P}^n$ is closed (= algebraic).

~~J is the image of~~

$\cancel{V \times W \times \mathbb{P}^1 \longrightarrow \mathbb{P}^n}$

$\cancel{(P, Q, [u:t]) \longmapsto}$

Warning

$$V \times W \times \mathbb{P}^1 \longrightarrow \mathbb{P}^n$$
$$([P],[Q],[\lambda:\mu]) \longmapsto [\lambda P + \mu Q]$$

is not a well-defined map. (Think about what happens if you rescale P!)

Pf

J is the image of the alg. set

$$\{(P, Q, R) \in V \times W \times \mathbb{P}^n \mid P, Q, R \text{ colinear}\}$$

under the proj. $(P, Q, R) \longmapsto R$. $\square$

Cor 15.5 Identify the vector space F_d of hom. deg. d pol. in $X_0, \dots, X_n$ with $K^{f(d)}$, where $f(d) = \#\{\text{deg. } d \text{ monomials}\} = \binom{n+d}{n}$.

($\leadsto$ A point in $\mathbb{P}^{f(d)-1}$ then corresponds to an equivalence class $[f]$ of such polynomials $f \neq 0$ (modulo scaling).)

The points $[f] \in \mathbb{P}^{f(d)-1}$ for which f is reducible form an alg. subset.

Ex Let $d=2$ and $\mathrm{char}(K) \neq 2$. A polynomial $0 \neq f = \sum_{i \leq j} a_{ij} X_i X_j$ is reducible if and only if all 3×3-minors of the matrix

$$M = \begin{bmatrix} a_{00} & \frac{a_{01}}{2} & \frac{a_{02}}{2} & & \\ \frac{a_{01}}{2} & a_{11} & \frac{a_{12}}{2} & & \\ & & a_{22} & & \\ & & & \ddots & \\ & & & & a_{nn} \end{bmatrix}$$

are 0.

(Thanks, Jonas, for pointing out that the original criterion was wrong!) In part., for $n=1$, all f are reducible.

Pf of example Note: M is the matrix representing the bilinear map

$$K^{n+1} \times K^{n+1} \to K$$
$$(v, w) \mapsto \frac{1}{2}\big(f(v+w) - f(v) - f(w)\big)$$

The quadratic form f (and therefore the matrix M) can be diagonalized. This change of coordinates doesn't change whether f is reducible and doesn't change the rank of M.

$\Rightarrow$ Rescaling coordinates, we can assume that

$f = X_0^2 + \dots + X_{r-1}^2$ (where $1 \leq r \leq n+1$ is the rank of M, $M = \begin{bmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & 1 & & & \\ & & & 0 & & \\ & & & & \ddots & \\ & & & & & 0 \end{bmatrix}$

The polynomial f is clearly reducible if $r = 1$ ($f = X_0 \cdot X_0$) or $r = 2$ ($f = X_0^2 + X_1^2 = (X_0 + \sqrt{-1}X_1)(X_0 - \sqrt{-1}X_1)$).

If $r \geq 3$, it is irreducible: Say $f = gh$ with g, h hom. of deg. 1.

$V(g)$ is a hyperplane in K^{n+1}, say spanned by $v_1, \dots, v_n$.

Let $v_1, \dots, v_n, v_{n+1}$ be a basis of K^{n+1}. If we change to this basis, the matrix M then has the form

$$\begin{bmatrix} 0 & \cdots & 0 & * \\ \vdots & & \vdots & \vdots \\ 0 & \cdots & 0 & * \\ * & \cdots & * & * \end{bmatrix},$$

which clearly has rank ≤ 2.

$\square$

Pf of Cor The set of reducible $[f]$ is the union of the images of the maps $\mathbb{P}^{f(a)-1} \times \mathbb{P}^{f(b)-1} \to \mathbb{P}^{f(d)-1}$ with $a + b = d$,

$([g], [h]) \mapsto [gh]$ $\quad a, b \geq 1$.

$\square$

16. Tangent spaces

Def Let V be an alg. subset of K^n. The tangent space to V at $P \in V$ is the vector space

$$T_P(V) := \{ \vec{v} \in K^n \mid D_P(f)(\vec{v}) = 0 \quad \forall f \in J(V) \}$$

where

$$D_P(f) : K^n \longrightarrow K$$
$$(b_1, \dots, b_n) \longmapsto \frac{\partial f}{\partial x_1}(P) \cdot b_1 + \dots + \frac{\partial f}{\partial x_n}(P) \cdot b_n$$

is the derivative of f at P.

Lemma 16.1 If $J(V) = (f_1, \dots, f_m)$, then

$$T_P(V) = \{ \vec{v} \in K^n \mid D_P(f_i)(\vec{v}) = 0 \quad \forall i = 1, \dots, m \}.$$

Pf "$\subseteq$" clear

"$\supseteq$" Let $f = f_1 g_1 + \dots + f_m g_m$.

If $D_P(f_i)(\vec{v}) = 0$ and $f_i(P) = 0$ for all i, then

$$D_P(f)(\vec{v}) = \sum_i \left(D_P(f_i)(\vec{v}) \cdot g_i(P) + f_i(P) \cdot D_P(g_i)(\vec{v}) \right) = 0$$

by the product rule. $\square$

Ese $K=\mathbb{C}$.

$$V=\mathcal{V}(x^2+y^2-1) \implies \mathcal{I}(V)=(x^2+y^2-1)$$

~~$\mathcal{I}(V)=(x^2+y^2-1)$~~

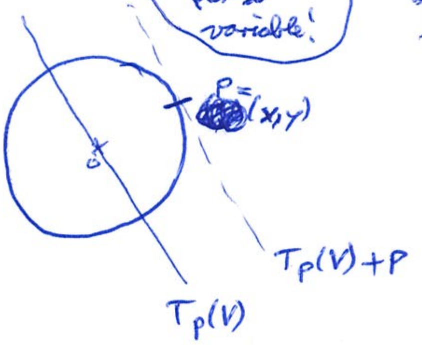
$P=(x,y)\in V$

$$\implies T_P(V)=\{\underset{(r,s)}{\cdot}\in K^2 \mid 2xr+2ys=0\}$$

$$=\{(dx,dy)\in K^2 \mid \underbrace{2x\,dx+2y\,dy}_{d(x^2+y^2-1)}=0\},$$

dx is notation for a variable!

the one-dim. vector space "parallel to the line tangent to the circle at (x,y)"



~~Ese $I=(x^2+y^2-1)^2 \implies \mathcal{V}(I)=$ same V as before~~

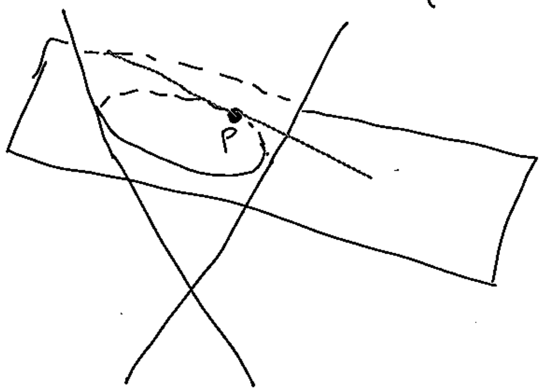
~~But $T_P(V)=\{(dx,dy)\in K^2 \mid \underbrace{2\underbrace{(x^2+y^2-1)}_{0}(2x\,dx+2y\,dy)}_{d(x^2+y^2-1)^2}=0\}=K^2$.~~

~~Ese $K=\mathbb{C}$, $V=\mathcal{V}(x^3-y^2)$, $P=(x,y)$~~

~~$T_P(V)=\{(dx,dy)\in K^2 \mid 3x^2dx=2y\,dy\}$~~

~~$\dim T_P(V)=\begin{cases}1, & P\neq(0,0),\\ 2, & P=(0,0).\end{cases}$~~

Eg $V = V(\underbrace{x^2+y^2-z^2}_{f}, \underbrace{2x+z-11}_{g})$



$P=(x,y,z)$

$(Df)(x,y,z)(a,b,c) = 2xa + 2yb - 2zc$

$\quad - \sim (dx,dy,dz) = 2x\,dx + 2y\,dy - 2z\,dz$

$(Dg)(x,y,z) = (a,b,c) = 2a + c$

$\quad \cdots \; 2dx + dz$

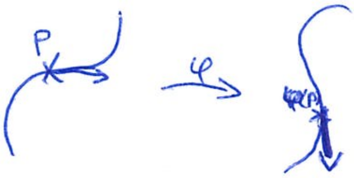
$$T_{(x,y,z)}(V) = \ker \begin{pmatrix} 2x & 2y & -2z \\ 2 & 0 & 1 \end{pmatrix}$$

$P = (3,4,5) \in V$

$\rightsquigarrow T_P(V) = \left\langle \begin{pmatrix} -4 \\ 13 \\ 8 \end{pmatrix} \right\rangle.$

Rmk If $\varphi: V \to W$ is a morphism, its derivative at $P \in V$ is a map $D_P(\varphi): T_P(V) \longrightarrow T_{\varphi(P)}(W)$.

Pf Let $\vec{v} \in T_P(V)$, $f \in J(W)$.



By the chain rule,

$$D_{\varphi(P)}(f)\big(D_P(\varphi)(\vec{v})\big) = D_P(\underbrace{f\circ\varphi}_{\substack{\in J(V)\\ \text{because}\\ \varphi: V\to W\\ \text{is well-def.}}})(\vec{v}) \underset{\substack{\uparrow\\ \vec{v}\in T_P(V)}}{=} 0.$$

$\square$

Rmk In particular, if φ is an isomorphism, then

$$T_P(V) \cong T_{\varphi(P)}(W).$$

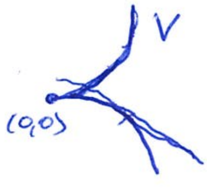
Ex There is no isomorphism $K^n \cong K^m$ (of alg. sets) for $n \neq m$ because the tangent spaces are K^n, K^m, which are nonisomorphic vector spaces.

Ex There is no isom $V = \mathcal{V}(X^3 - Y^2) \cong K$ because V has $T_{(0,0)}(V) = K^2$, but all tangent spaces of K are K^1.

Ex $K = \mathbb{C}$, $V = \mathcal{V}(X^3 - Y^2)$, $P = (x,y)$

$\Rightarrow T_P(V) = \{(dx, dy) \mid 3x^2 dx = 2y\,dy\}$

$$\dim T_P(V) = \begin{cases} 1, & P \neq (0,0), \\ 2, & P = (0,0). \end{cases}$$



Ex $K = \mathbb{C}$, $V = \mathcal{V}(Y^2 - X^2(X+1))$, $P = (x,y)$

$$\dim T_P(V) = \begin{cases} 1, & P \neq (0,0) \\ 2, & P = (0,0) \end{cases}$$

Def Let V be an irreducible alg. set.

V is <u>smooth at P</u> if $\dim T_P(V) = \dim(V)$.

Otherwise, V is <u>singular at P</u>.

V is <u>smooth</u> if it is smooth at every $P \in V$.

Rmk $\dim T_P(V) = \dim\ker\left(\frac{\partial f_i}{\partial x_j}(P)\right)_{i,j}$ if $I(V) = (f_1, \dots, f_m)$.

Rmk For any $d \geq 0$, the set $\{P \in V \mid \dim T_P(V) \geq d\}$ is an algebraic subset of V.

Prop 16.2 Let V be irreducible.

a) $\dim T_P(V) \geq \dim V$ for all $P \in V$.

b) $\dim T_P(V) = \dim V$ for some $P \in V$.
($\Rightarrow$ for all P in a nonempty open subset)

"V is smooth almost everywhere"

Pf See Thm 2.3 in Shafarevich. $\square$

Rmk This is great! For example:

Cor 16.3 Let $P \in V := \mathcal{V}(f_1, \dots, f_m) \subseteq K^n$.
If the matrix $\left(\frac{\partial f_i}{\partial x_j}(P)\right)_{i,j}$ has rank m, then every irred. comp. A of V containing P has codimension m in K^n.

Pf $m \geq \operatorname{codim}(A, K^n) \geq n - \dim T_P(V) = n - \dim\ker\left(\frac{\partial f_i}{\partial x_j}(P)\right)_{i,j} = \operatorname{rk}(\dots) = m$ $\square$

Cor 16.4 Let V be irreducible, smooth at $P \in V$, $\varphi : V \to W$ a dominant morphism. Then, $\dim(W) \geq \operatorname{rk}(D_P(\varphi))$.

Pf ~~Since~~ $\cancel{\varphi(\varphi^{-1}(\varphi}$

Let $Q = \varphi(P)$. ~~Since~~ $\cancel{\varphi(\varphi^{-1}(Q)) = \{Q\}}$ ~~and~~ $\cancel{T_Q(\{Q\})=0}$, ~~we have~~

$$\cancel{T_P(\varphi^{-1}(Q)) \subseteq \ker(D_P(\varphi))}.$$

$\cancel{\Rightarrow \dim \ker}$

Let A be an irred. comp. of $\varphi^{-1}(Q)$. Since $\varphi(A) = \{Q\}$ and $T_Q(\{Q\}) = 0$, we have

$$T_P(A) \subseteq \ker(D_P(\varphi)).$$

$$\Rightarrow \dim(T_P(A)) \leq \dim \ker(D_P(\varphi)) = \underbrace{\dim(T_P(V))}_{\dim(V)} - \operatorname{rk}(D_P(\varphi))$$

$$\dim(T_P(A)) \geq \dim(A) \geq \dim(V) - \dim(W)$$

$\square$

Rmk a) The assumption that V is smooth at P is necessary: Otherwise, take $\varphi = \mathrm{id}$. $\Rightarrow \operatorname{rk}(D_P(\varphi)) = \dim T_P(V) > \dim(V)$.

b) We can have $>$:

Take $\varphi : K \to K$, $x \mapsto x^2$, $\quad D_0(\varphi) = 0$ has rank 0

c) In char. 0, we have $=$ for some P, but in char. $p > 0$, even that can fail: Take $\varphi : K \to K$, $x \mapsto x^p$ $\Rightarrow D_x(\varphi) = p x^{p-1} = 0$ for all x.