Algebraic Geometry

1. Overview

Let K be a field.

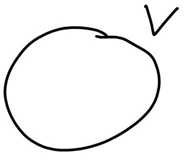
An <u>algebraic</u> <u>subset</u> of K^n is the set of solutions $(x_1, \dots, x_n) \in K^n$ to a system of polynomial equations:

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

<u>Ex</u>

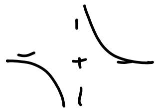
Conic (= conic section):

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

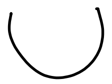


Ellipse $2x^2 + 3y^2 = 1$

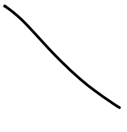
Hyperbola $xy = 1$



Parabola $y = x^2$



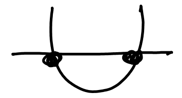
Line $x + 2y = 3$



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

$= \{ \quad \mid x = 1,\ y = 2\}$

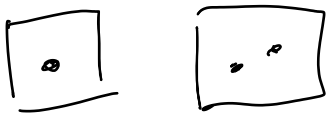
Two points $\{(0,0), (1,0)\} = \{ \quad \mid x(x-1) = y,\ y = 0\}$

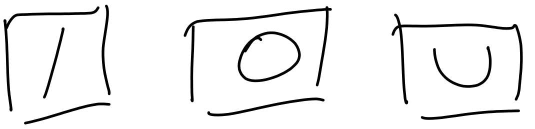


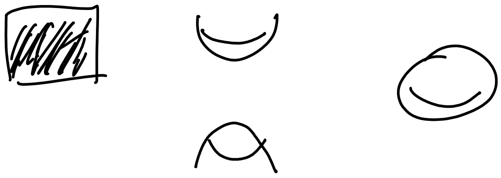
$\vdots$

Questions

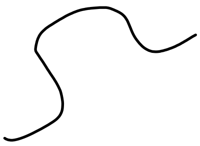
- Is V a set of just finitely many points?
  If so, how many?
- What is the "dimension" of V?

dim = 0: 

dim = 1: 

dim = 2: 

- Is V "smooth"?

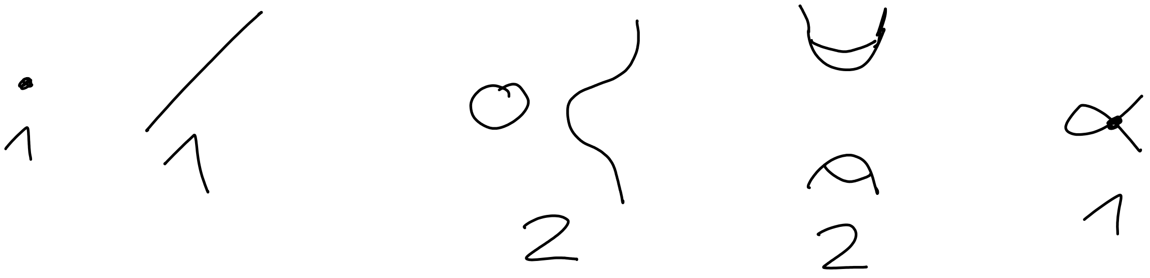
smooth 

not smooth 

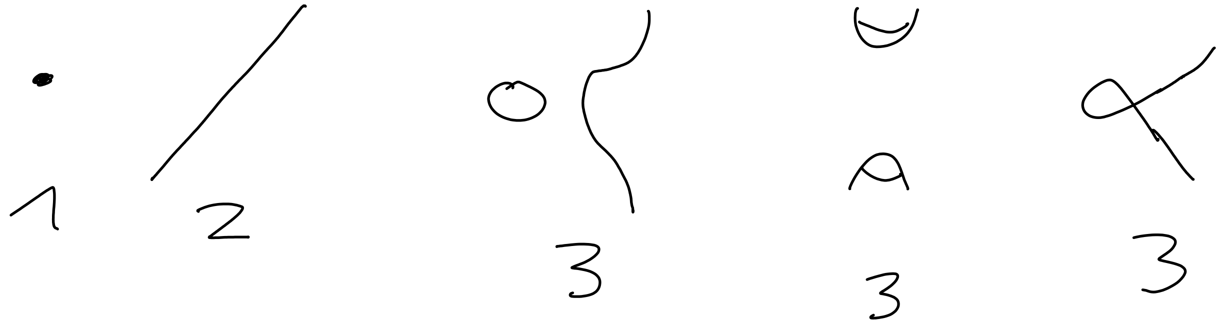
- If not, what can the "singularities" look like?

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

- How many connected components does V have?

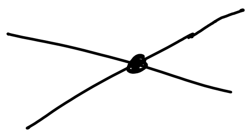


- How many connected components does the complement $\mathbb{R}^n \setminus V$ have?



Intersection theory

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

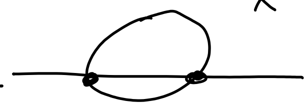
Usually 1 

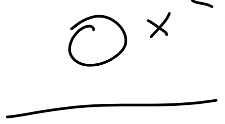
Occasionally 0  (if l_1, l_2 are parallel)

⇝ Always 1 in the projective plane.

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

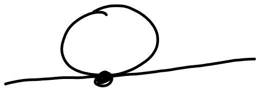
$x^2+(y-2)^2=100$

Sometimes 2  $y=1$

Sometimes 0  $x^2+(y-2)^2=100$

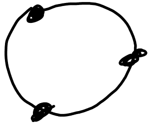
$y=-1000$

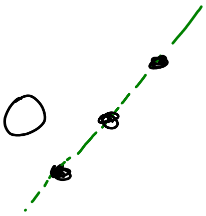
(can't happen in algebraically closed fields like $\mathbb{C}$)

Occasionally 1  (with "multiplicity" 2)

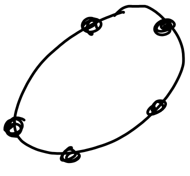
Enumerative geometry

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

Usually 1 

Occasionally 0 

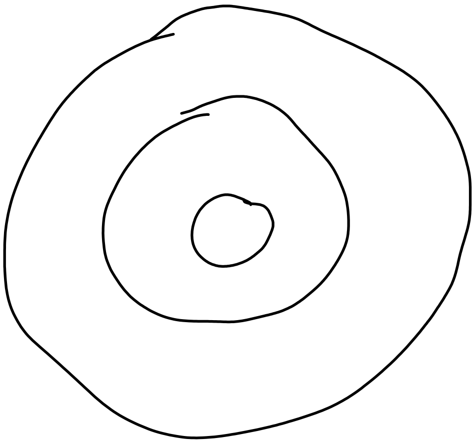
- How many conics are there through five given points p_1, p_2, p_3, p_4, p_5?

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

2. Affine varieties

2.1. Algebraic sets

Let K be a field.

Rmk 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 affine space (over K).

Def For a set $S \subseteq K[x_1, \dots, x_n]$ of polynomials, we denote by

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

the corresponding set of zeros.

Rmk If $S \subseteq S'$, then $V(S) \supseteq V(S')$.
(V is inclusion-reversing.)

Def A subset $X \subseteq K^n$ is algebraic if $X = V(S)$ 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 (in chapter 2.2) see

that the two definitions are equivalent!

Ex $V(\{x_2 - x_1^2\}) = \{(x_1, x_2) \in K^2 / x_2 = x_1^2\}$

if $n = 2$.

Ex $V(\{x_1 - a_1, \dots, x_n - a_n\}) = \{(a_1, \dots, a_n)\}$,

so every one-point subset $\{P\} \subseteq K^n$ is algebraic.

Note
- If $f(P) = 0$, then $f(P) \cdot g(P) = 0$ $\forall g \in K[x_1, \dots, x_n]$
- If $f(P) = 0$ and $g(P) = 0$, then $f(P) + g(P) = 0$.

Cor 2.1 If I is the ideal of $K[x_1, \dots, x_n]$ generated by S,

then $V(I) = V(S)$.

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

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

$$\underbrace{\underbrace{f_1}_{0 \text{ at } P} g_1 + \dots + \underbrace{f_r}_{0 \text{ at } P} g_r}_{0 \text{ at } P}$$

with $f_1, \dots, f_r \in S$, $g_1, \dots, g_r \in K[x_1, \dots, x_n]$

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

Lemma 2.2

a) For any collection of ideals I_α,

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

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

b) For any two ideals I, J

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

c) $V(0) = K^n$

d) $V(1) = \emptyset$.

Pf a) clear

b) $P \in LHS \iff P \in V(I)$ or $P \in V(J)$

$\iff \forall f \in I : f(P)=0$ or $\forall g \in J : g(P)=0$

$\iff \forall f \in I, g \in J:\ f(P)=0$ or $g(P)=0$

$\iff \forall f \in I, g \in J:\ f(P)\cdot g(P)=0$

$\iff P \in RHS$

c) $P \in V(0) \iff 0=0$ d) $P \in V(1) \iff 1=0$ $\square$

Cor 2.3

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

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

c) K^n is alg. subset

d) ϕ is alg. subset

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

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

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

Pf For any $f \in K[X_1, \dots, X_n]$, the set $V(f)$ of zeros of f is closed w.r.t. the usual topology, because $f : K^n \to K$ is continuous w.r.t. the usual topology and $\{0\} \subseteq K$ is closed.

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

$\square$

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

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

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

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

Case 1: $f = 0$ (constant zero polynomial)

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

Case 2: $f \neq 0$

$\Rightarrow$ f has only finitely many roots.

$\square$

Cor The Zariski topology on K is the cofinite topology.

Eg of Lemma 2.4

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

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

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

2.2. Hilbert Basis Theorem

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

Convention Rings are commutative and have a mult. 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 (e.g. any field) is noetherian.

Lemma 2.6 R is noetherian if and only if there is no chain of ideals

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

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

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

Each f_i lies in some I_r

$\Rightarrow I \subseteq I_r$ for some r

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

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

$\Rightarrow$ We can inductively construct

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

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

$\uparrow$ exists because I isn't finitely generated

$\square$

Thm 2.7 (Hilbert's Basis Theorem)

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

By induction:

Cor 2.8

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

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

Pf of Thm 2.7

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

We inductively construct

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

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

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

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

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

Let $b_r :=$ leading coefficient of f_r.

We get a chain of ideals of R:

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

Since R is noetherian, we have equality somewhere:

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

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

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

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

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

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

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

2.3. Vanishing ideals

$$\begin{tikzcd}\{\text{ideal } J \subseteq K[x_1,\dots,x_n]\} \arrow[r, shift left, "V"] & \{(\text{alg.}) \text{ subset } X \subseteq K^n\} \arrow[l, shift left, "I"]\end{tikzcd}$$

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

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

of polynomials that vanish everywhere on X.

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

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

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

Rmk If $X \subseteq X'$, then $I(X) \supseteq I(X')$.

Rmk $I(V(J)) \supseteq J$

Rmk $V(I(X)) \supseteq X$

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

2.4. Hilbert's Nullstellensatz

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

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

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

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

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

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

$\Rightarrow f(P) = 0$.

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

Def The 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 2.10 $\sqrt{I}$ is an ideal.

Pf • Let $f, g \in \sqrt{I}$.

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

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

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

• Let $f \in \sqrt{I}$, $a \in R$.

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

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

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

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

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

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

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

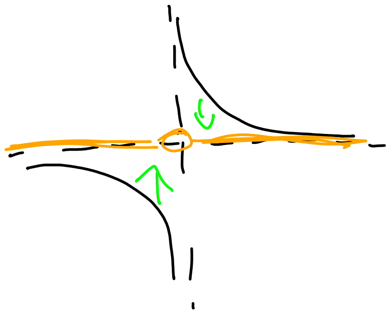
Rmk If R is a unique factorization domain and we have factorization
$f = u \cdot g_1^{e_1} \cdots g_r^{e_r}$, then

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

Warmup

$\mathbb{R}\setminus\{0\} \subseteq \mathbb{R}$

isn't an algebraic subset



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

Rmk For any ideal J of $K[x_1,\dots,x_n]$, we have $I(V(J)) \supseteq \sqrt{J}$.

Thm 2.11 (Hilbert's Nullstellensatz)

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

Exe If $n=1$, $J=(f)$ with

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

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

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

Rmk The Thm is wrong if K is not algebraically closed.

Pf Let $f \in K[X]$ be any irreducible pol. of degree ≥ 2.

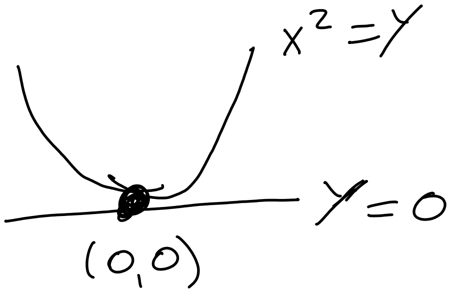
$\Rightarrow f$ has no roots in K : $V(f) = \emptyset$

$\Rightarrow I(V(f)) = K[X]$.

But $\sqrt{(f)} = (f) \neq K[X]$. $\square$

Exe $n=2$, $J = (X^2, Y) = (X^2 - Y, Y)$

$V(J) = \{(0,0)\}$.



$I(V(J)) = \{f \in K[X,Y] \mid f(0,0) = 0\} = (X, Y)$
$= \sqrt{J}$.

Cor 2.12 If K is algebraically closed, we get bijections

$$\{\text{radical ideal } J \subseteq K[X_1, \dots, X_n]\} \underset{I}{\overset{V}{\rightleftarrows}} \{\text{alg. subset of } K^n\}$$

which are each other's inverse.

Cor 2.13 (Weak Nullstellensatz)

If $J \subsetneq K[x_1, \dots, x_n]$, then $V(J) \neq \emptyset$.

Pf using Hilbert's Nsts

If $V(J) = \emptyset$, then

$$\sqrt{J} = I(V(J)) = I(\emptyset) = K[x_1, \dots, x_n].$$

$$\Rightarrow \underset{\substack{\uparrow \\ \text{constant polynomial}}}{1} \in \sqrt{J} \Rightarrow \underset{\substack{\shortparallel \\ 1}}{1^n} \in J \text{ for some } n \geq 1$$

$$\Rightarrow J = K[x_1, \dots, x_n].$$ $\square$

Thm 2.14 (Nichtnullstellensatz)

We have $I(K^n) = 0$.

Pf using Hilbert's Nsts

$$I(K^n) = I(V(0)) = \sqrt{0} = 0.$$ $\square$

Rmk Thm 2.14 holds for any infinite (not necessarily algebraically closed) field K.

Pf Use induction over n.

n = 0: clear.

n = 1: nonzero polynomials have only finitely many roots, and therefore have a non-root in K.

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

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

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

By induction, there exist $(a_1, \dots, a_{n-1}) \in K^{n-1}$ such that $g_d(a_1, \dots, a_{n-1}) \neq 0$.

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

(it has degree d).

By the n = 1 case, there exists $a_n \in K$ such that $f(a_1, \dots, a_{n-1}, a_n) \neq 0$. □

Rmk The weak Nsts implies Hilbert's (strong) Nsts.

Pf "$I(V(J)) \supseteq \sqrt{J}$" done earlier

"$I(V(J)) \subseteq \sqrt{J}$"

Let $f \in I(V(J))$.

$\Rightarrow \forall P \in V(J): f(P) = 0$.

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

We have a bijection

$$\{P \in V(J) \mid f(P) \neq 0\} \longleftrightarrow \{(P,t) \in \underbrace{V(J) \times K}_{\subseteq K^{n+1}} \mid f(P) \cdot t = 1\}$$

$$= \quad V(J') \subseteq K^{n+1}$$

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

$LHS = \emptyset \Rightarrow RHS = V(J') = \emptyset$

$\underset{\substack{\uparrow \\ \text{weak Nsts}}}{\Longrightarrow} \quad J' = K[X_1, \dots, X_n, T]$.

$\Rightarrow 1 \in J'$

$\Rightarrow$ We can write

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

with $p_i \in J$, $q \in K(x_1,\dots,x_n,T]$.

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

Plug in $T = \frac{1}{f}$:

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

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

$\Rightarrow f \in \sqrt{J}$. $\square$

2.5. 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

$$R[X_1, \dots, X_n] \longrightarrow S .$$
$$r \in R \longmapsto r$$
$$X_i \longmapsto a_i$$

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 $r a_i$ 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:

Rmk module-finite

$$\not\Uparrow$$

ring-finite

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

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

Rmk ring-finite

$$\not\Uparrow$$

field-finite

Pf $\mathbb{C}(X)$ 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 $q_1(X), \dots, q_n(X)$.

Plug in $X = t$.

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

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 $\left\{ a_i b_j \,\middle|\, \begin{matrix} 1 \le i \le n, \\ 1 \le j \le m \end{matrix} \right\}$ 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 ... $\square$

2.6. Integral and algebraic extensions

Def An element a of a ring S is called integral over a subring $R \subseteq S$ if there is a monic 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 integral if every $a \in S$ is integral over R.

The integral closure 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 integrally closed in S if its integral closure in S is R.

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

Rmks 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 a of R is integral over R.

Pf Take $f(X) = X - a$. □

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

Pf Take $f(X) = X^3 - 2$. □

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

Pf Let $a \in \mathbb{C}$. Take

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

□

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. □

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

Thm 2.15 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 $f\left(\frac{p}{q}\right) = 0$. $\quad (c_i \in R)$

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

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

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 2.16 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 $f(a) = 0$.

$$\parallel$$

$$X^n + c_{n-1} X^{n-1} + \dots + c_0$$

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

Clear out denominators:

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

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

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

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

Lemma 2.17 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 $f(a) = 0$.

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

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. $\Rightarrow e \geq n$.

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

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

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) ⇒ 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 matrise 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 $\mathbb{Z}$

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

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

<u>Cor 2.18</u> The integral closure of R in S is a ring (a ring ext. of R).

<u>Pf</u> 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 $c_1, \ldots, c_n$

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

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

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 2.19 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 2.20 Integrality / algebraicity are transitive: If S is an integral ring ext. of R,
and T —"— —"— S,
then T —"— —"— R.

Pf HW. $\square$

Cor 2.21 Let S' be the integral closure of R in S. Then, S' is integrally closed in S.

Pf HW. $\square$

Thm 2.22 Any *ring*-finite *field* extension L of a field K is *module*-finite (= finite-dimensional K-vector space).

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

Pf Let $L = K[a_1, \dots, a_n]$.

Use induction:

$n=1$: $L = K[a_1]$

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!

$n-1 \to n$: 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 $a_2, \ldots, a_n \in L$ are algebraic over $K(a_1) \cong K(X)$.

By Lemma 2.16, we can (for $i = 2, \ldots, n$) write $a_i = \frac{p_i}{q_i}$ 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 2.5):

The ring $K[a_1] \cong K[X]$ contains ∞ many maximal ideals ($\hat{=}$ monic irreducible polynomials).

$\Rightarrow$ There esists $r \in K[a_1] \cong K[X]$ 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 $\text{LHS} = \frac{q_2^{\cdots} \cdots q_n^{\cdots}}{r} \in K(a_1) \setminus K[a_1]$

$$\overset{\shortparallel\wr}{K(X) \setminus K[X]}$$

isn't integral over $K[a_1] \cong K[X]$ by Thm 2.15.

$\square$

2.7. Proof of Hilbert's Nullstellensatz

It only remains to prove the weak Nullstellensatz:

Thm 2.23 (= Cor 2.13) Assume K is algebraically closed. For any ideal $J \subsetneq K[X_1,\dots,X_n]$, we have $V(J) \neq \emptyset$.

Pf We can assume w.l.o.g. that J is a maximal ideal of $K[X_1,\dots,X_n]$.

$\Rightarrow L = K[X_1,\dots,X_n]/J$ is a field.

Consider L a field extension K. It is generated by the images of $X_1,\dots,X_n$ in L.

$\Rightarrow$ ring-finite field ext.

$\underset{\text{Thm 2.22}}{\Rightarrow}$ module-finite $\Rightarrow$ algebraic

$\Rightarrow L = K$. In other words, the map

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

is an isomorphism. Set $a_i \in K$ be the preimage of $(X_i \bmod J) \in L$.

$$\Rightarrow \quad X_i - a_i \in J \qquad \forall i = 1, \dots, n$$

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

But J' is a maximal ideal of $K[X_1, \dots, X_n]$ because

$$K[X_1, \dots, X_n]/J' \cong K$$
$$X_i \longleftrightarrow a_i$$

$$\Rightarrow \quad J = J' \Rightarrow V(J) = V(J') = \{(a_1, \dots, a_n)\}.$$

$J' \subseteq J$ are max. id.

$\square$

The kernel of the ring homomorphism

$$K[X_1, \dots, X_n] \longrightarrow K$$
$$X_i \longmapsto a_i$$

is the set of polynomials $f(X_1, \dots, X_n)$ such that $f(a_1, \dots, a_n) = 0$, which is the ideal $J' = (X_1 - a_1, \dots, X_n - a_n)$.

From now on, we'll always assume that the field K is algebraically closed.

(unless stated otherwise ...)

2.8. Irreducibility

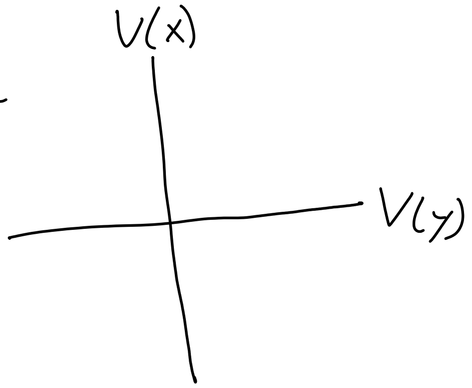
Def An algebraic set $\emptyset \neq X \subseteq K^n$ is *irreducible* if you can't write $X = X_1 \cup X_2$ with any algebraic sets $X_1, X_2 \subsetneq X$. Otherwise, it's *reducible*.

Ex Any one-point set $X = \{p\}$ is irreducible.

Ex $V(XY) \subseteq K^2$ is reducible

$\|$

$V(X) \cup V(y)$



Ex $K \subseteq K^1$ is irreducible.

Ex $V(X), V(y) \subseteq K^2$ are irreducible.

Thm 2.24 An algebraic subset $X \subseteq K^n$ is irreducible if and only if $I(X)$ is a prime ideal of $K[X_1,\dots,X_n]$.

Pf Recall ~~that~~ $X \neq \emptyset \Leftrightarrow V(I) \neq K[X_1,\dots,X_n]$.

$$\underset{\text{Weak Nullstellensatz}}{\uparrow}$$

"$\Rightarrow$" Assume $I(X)^{\neq K[X_1,\dots,X_n]}$ is not a prime ideal.

$$\begin{tikzcd}
 & \rightsquigarrow \text{Let } f,g \notin I(X), \text{ but } fg \in I(X). \arrow[dl, Rightarrow] \arrow[dr, Rightarrow] & \\
V(f), V(g) \not\supseteq X \arrow[d, Rightarrow] & & V(f) \cup V(g) = V(fg) \supseteq X \arrow[d, Rightarrow] \\
X \cap V(f), X \cap V(g) \subsetneq X & & X = \underbrace{(X \cap V(f))}_{} \cup \underbrace{(X \cap V(g))}_{\text{algebraic subsets of } X}
\end{tikzcd}$$

"$\Leftarrow$" Assume $X = X_1 \cup X_2$, $X_1, X_2 \subsetneq X$ algebraic subsets.

$$\Downarrow$$

$$I(X_1), I(X_2) \supsetneq I(X)$$

Let $f_i \in I(X_i) \setminus I(X)$. $\Rightarrow f_i(P) = 0 \ \forall P \in X_i$

Since $X = X_1 \cup X_2$, this implies $(f_1 f_2)(P) \ \forall P \in X$

$\Rightarrow f_1 f_2 \in I(X) \Rightarrow I(X)$ not prime. $\square$

Cor 2.25 $V(J) \subseteq K^n$ is irreducible if J is a prime ideal.

Pf Recall that $I(V(J)) = \sqrt{J}$ by Hilbert's Nullstellensatz.

But $\sqrt{J} = J$ for any prime ideal:

If $f^n \in J$, then $f \in J$. $\square$

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

Ex $V(x) \subseteq K^2$ is irreducible because (x) is a prime ideal of $K[X,Y]$ because

$$K[X,Y]/(X) \cong K[Y] \text{ is an integral domain}$$
$$X \mapsto 0$$

Lemma/Reminder 2.26 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 $f \in R$ is irreducible.

Ese $V(X^2+Y^2-1) \subseteq \mathbb{C}^2$ is irreducible because $X^2+Y^2-1 \in \mathbb{C}[X,Y]$ is.

Pf Assume $X^2+Y^2-1 = f(X,Y) \cdot g(X,Y)$ for some nonconstant polynomials $f(X,Y), g(X,Y) \in \mathbb{C}[X,Y]$. Since X^2+Y^2-1 has degree 2 in X, either a) both $f(X,Y)$ and $g(X,Y)$ have degree 1 in X, or

b) one of them (say $f(X,Y)$) has degree 0 in X, the other has degree 2 in X.

Case b) is impossible: If $f(X,Y) = f(Y)$ depends only on Y, take some root $b \in \mathbb{C}$ of $f(Y)$. Then, $a^2+b^2-1 = f(b) \cdot g(a,b) = 0 \quad \forall a \in \mathbb{C}$.

(false)

Hence, $f(X,Y)$ and $g(X,Y)$ have degree 1 in X.

Similarly, —"— Y.

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

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

$\Rightarrow$ Take $a = -\frac{qb+r}{p}$.

so the unit circle contains a line (over $\mathbb{C}$)

$$\Rightarrow \; 0 = p^2(a^2+b^2-1)$$

$$= (qb+r)^2 + p^2b^2 - p^2$$

$$= (q^2+p^2)b^2 + 2qrb + r^2 - p^2$$

$$\forall b \in \mathbb{C}$$

$$\Rightarrow \; q^2+p^2=0 \text{ and } 2qr=0 \text{ and } r^2-p^2=0$$

$$\begin{array}{ccc} 2qr=0 & & r^2-p^2=0 \\ \Downarrow \Leftarrow q\neq 0 & & \Downarrow \\ r=0 & \Longrightarrow & p=0 \\ & & ↯ \\ & & \square \end{array}$$

Warning / Correction

X^2+Y^2-1 is <u>not</u> irreducible over the field $\mathbb{F}_2$:

$$X^2+Y^2-1 \equiv (X+Y+1)^2 \mod 2.$$

Thm 2.27 Let $X \subseteq K^n$ be algebraic. Then:

a) $X = X_1 \cup \dots \cup X_m$ for some irreducible sets $X_1, \dots, X_m \subseteq X$ with $X_i \nsubseteq X_j$ for all $i \neq j$.

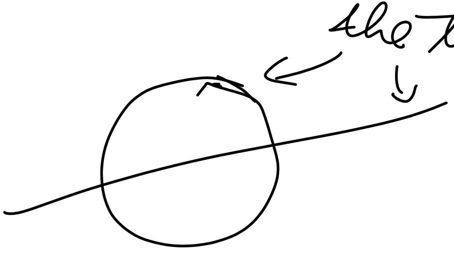
b) This decomposition is unique. The sets $X_1, \dots, X_m$ are called the irreducible components of X.

c) Any irreducible subset $Y \subseteq X$ is contained in some X_i.

Ex $V(X), V(Y)$ are the irreducible components of $V(XY)$.

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

Ex



Pf a) By Hilbert's Basis Theorem (Thm 2.7, Lemma 2.6), there is no chain of ideals $I_1 \subsetneqq I_2 \subsetneqq I_3 \subsetneqq \cdots$

Hence, there is no chain
$$Y_1 \supsetneqq Y_2 \supsetneqq Y_3 \supsetneqq \cdots$$

$\Rightarrow$ If some X can't be decomposed into (finitely many) irreducible components, there is an inclusion-minimal such set X.

$\Rightarrow$ X isn't irreducible

$\rightsquigarrow$ Write $X = A \cup B$ with $A, B \subsetneqq X$ algebraic.

$\Rightarrow$ Both A and B can be written as unions of finitely many irreducible subsets.

$\Rightarrow$ X can!

c) $$Y = \bigcup_{i=1}^{n} \underbrace{(X_i \cap Y)}_{\text{alg.}}$$

$$\underset{\substack{\uparrow \\ Y \text{ irred}}}{\Longrightarrow} \quad Y = X_i \cap Y \text{ for some } i$$

$$\Longrightarrow \quad Y \subseteq X_i \quad \text{for some } i$$

b) Let $X = X_1 \cup \dots \cup X_n = Y_1 \cup \dots \cup Y_m$ as above.

Say X_i doesn't occur among $Y_1, \dots, Y_m$.

By c), $X_i \subseteq Y_j$ for some j.
By c), $Y_j \subseteq X_k$ for some k.
$\Big\}\; X_i \subseteq Y_j \subseteq X_k$

Since $X_i \not\subseteq X_k$ for $i \neq k$, it follows that we have $i = k$ and therefore equality:
$X_i = Y_j$. □

Summary

We have bijections

$$\begin{tikzcd}
(\text{alg. subsets of } K^n) \arrow[r, leftrightarrow] \arrow[d, phantom, "\cup"] & (\text{radical ideals of } K[x_1, \dots, x_n]) \arrow[d, phantom, "\cup"] \\
(\text{irreducible alg. subsets of } K^n) \arrow[r, leftrightarrow] \arrow[d, phantom, "\cup"] & (\text{prime ideals of } K[x_1, \dots, x_n]) \arrow[d, phantom, "\cup"] \\
(\text{points in } K^n) \arrow[r, leftrightarrow] & (\text{maximal ideals of } K[x_1, \dots, x_n])
\end{tikzcd}$$

2.10. Coordinate rings

Def The *coordinate ring* of an algebraic subset V of K^n is $\Gamma(V) := K[X_1,\dots,X_n]/I(V)$.

Rmks 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*: if $fg = 0$, then f or $g = 0$.

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

Thm 2.31 $\Gamma(V)$ is the ring of functions $f : V \longrightarrow K$ given by some polynomial $g \in K[X_1,\dots,X_n]$: $f = g|_V$

Pf Two polynomials $g_1, g_2 \in K[X_1,\dots,X_n]$ agree on V if and only if $g_1 - g_2$ vanishes everywhere on V, i.e. $g_1 - g_2 \in I(V)$. □

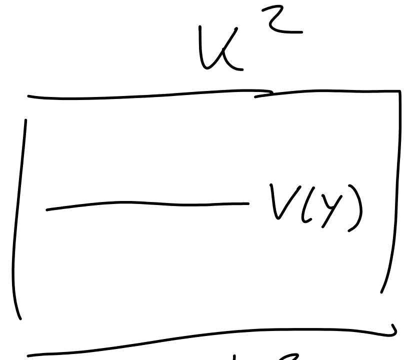
Ex The function X_i sending any point to its i-th coordinate.

Rmk If $V \subseteq W$ we get a surjective ring homomorphism

$$\begin{aligned} \Gamma(W) &\longrightarrow \Gamma(V). \\ f &\longmapsto f|_V \end{aligned}$$

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

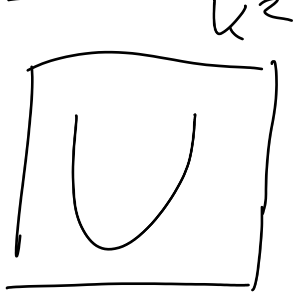
Ex



$$\Gamma(\underbrace{V(Y)}_{\text{X-axis in } K^2}) = K[X,Y]/(Y) \cong K[X]$$

$X \longmapsto X$
$Y \longmapsto 0$

Ex

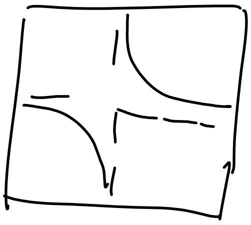


$$\Gamma(V(Y-X^2)) = K[X,Y]/(Y-X^2) \cong K[X]$$

$Y \longmapsto X^2$
$X \longmapsto X$

$$\left[\begin{aligned} R[T]/(T-r) &\cong R \qquad \text{for any } r \in R \\ T &\longmapsto r \end{aligned}\right]$$

Ex



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

$Y \longmapsto \frac{1}{X}$

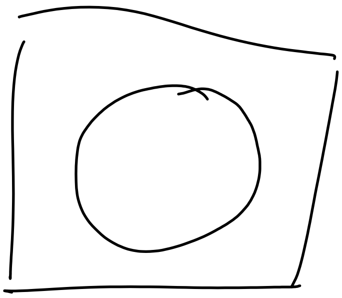
$$K[X,\tfrac{1}{X}] \ni 1 + 2X^3\cdot\left(\tfrac{1}{X}\right)^2 + 3X\cdot\left(\tfrac{1}{X}\right)^4 + \cdots$$

Warning

$$\underbrace{K(X)}_{\text{field of rational functions}} \ni \frac{1}{X+1} \notin \underbrace{K[X,\tfrac{1}{X}]}_{\text{ring of Laurent polynomials}}.$$

Ese Assume $K = \mathbb{C}$ (or at least $\mathrm{char}(K) \neq 2$).

Then, $\Gamma(V(X^2+Y^2-1)) = K[X,Y]/(X^2+Y^2-1)$



$$\cong K[X, \sqrt{1-X^2}] \qquad \begin{array}{c} Y \\ \downarrow \\ \sqrt{1-X^2} \end{array}$$

Fundamental principle

You can determine all "intrinsic" properties of an algebraic subset V of K^n from its coordinate ring.

Rmk There are bijections

$$\begin{array}{ccc} (\text{algebraic subsets } W \subseteq V \subseteq K^n) & \Longleftrightarrow & (\text{radical ideals of } \Gamma(V)) \\ \cup\!| & & \cup\!| \\ (\text{irred. alg. subsets } W \subseteq V) & \Longleftrightarrow & (\text{prime ideals of } \Gamma(V)) \\ \cup\!| & & \cup\!| \\ (\text{points on } V) & \Longleftrightarrow & (\text{maximal ideals of } \Gamma(V)) \end{array}$$

Pf Use the bijections

$(\text{ideals } I \subseteq J \subseteq R) \Longleftrightarrow (\text{ideals } J' \text{ of } R/I)$

for fixed I. (J = preimage of J' under the quotient map $R \twoheadrightarrow R/I$). $\square$

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

Cor 2.32 Let $V_1, \dots, V_m$ be algebraic 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 $I_i = I(V_i)$.

$\Rightarrow V_1 \cup \dots \cup V_m = V(I_1 \cap \dots \cap I_m)$

Each I_i is a radical ideal.

$\Rightarrow I_1 \cap \dots \cap I_m$ is a radical ideal

$\Rightarrow I(V_1 \cup \dots \cup V_m) = I_1 \cap \dots \cap I_m$.

$\Rightarrow \Gamma(V_1 \cup \dots \cup V_m) = K[x_1, \dots, x_n]/(I_1 \cap \dots \cap I_m)$

$\Gamma(V_i) = K[x_1, \dots, x_n]/_{I_i}$

Apply the Chinese remainder theorem. $\square$

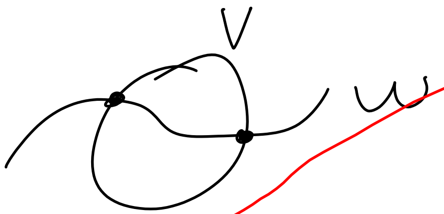
$/0$

~~More generally:~~

~~**Thm 2.33** Let V, W be algebraic subsets of K^n. Then,~~

~~$$\Gamma(V \cup W) \cong \{(f,g) \in \Gamma(V) \times \Gamma(W) \mid f|_{V\cap W} = g|_{V \cap W}\}$$~~

~~$$h \longmapsto (h|_V, h|_W)$$~~



~~Pf HW. "$\square$"~~

You can determine the number of points in V from $\Gamma(V)$:

Lemma 2.34 Let $V \subseteq K^n$ be a finite set consisting of m points. Then

$$\Gamma(V) = \underbrace{K \times \dots \times K}_{m \text{ times}}.$$

In particular, the dimension of $\Gamma(V)$ as a K-vector space is $\dim_K(\Gamma(V)) = m$.

Pf If $m=1$: The ring of functions $\underset{\{p\}}{\underset{\shortparallel}{V}} \longrightarrow K$ is K. (Any such function is given by a constant polynomial.)

For $m > 1$, apply Cor 2.32. $\square$

Cor 2.35 An algebraic subset $V \subseteq K^n$ is finite if and only if $\dim_K(\Gamma(V)) < \infty$.

Pf "$\Rightarrow$" clear

"$\Leftarrow$" If V contains at least m points $P_1, \dots, P_m$, we have a surjection

$$\Gamma(V) \longrightarrow \Gamma(\{P_1, \dots, P_m\}).$$

$$\dim_K(\Gamma(V)) \geq \dim_K(\Gamma(\{P_1, \dots, P_m\})) = m. \quad \square$$

Rmk This is equivalent to $\Gamma(V)$ being an integral (= algebraic) K-algebra.

More generally:

Thm 2.36 Let I be any ideal of $K(X_1, \dots, X_n]$. Then, $V(I)$ is finite if and only if $\dim_K(K(X_1, \dots, X_n]/I) < \infty$. In that case, $|V(I)| \leq \dim_K(K[X_1, \dots, X_n]/I)$.

Ex $I = (X(X-1)^2(X-2)^5)$
$= (X^8 + \dots + 0)$
$V(I) = \{0, 1, 2\}$

$K[X]/I$ has K-basis $1, X, \dots, X^7$

Always, $\#\{\text{roots of } f(x)\} \leq \deg(f)$.

$$\underset{V(f)}{\#\{\text{roots of } f(x)\}} \quad \underset{\dim_K(K[X]/(f))}{\deg(f)}$$

This follows from:

Lemma 2.37 Let I be an ideal of a ring extension S of a ring R. Then, S/I is an integral R-algebra if and only if $S/\sqrt{I}$ is an integral R-algebra.

Idea of pf If $\alpha \in S$, $f \in R[X]$ monic, $f(\alpha) = 0$ in $S/\sqrt{I}$ (so $f(\alpha) \in \sqrt{I}$).
$\Rightarrow f(\alpha)^n \in I$ for some n
$\Rightarrow f(\alpha)^n = 0$ in S/I, $f^n \in R[X]$ monic.
$\square$

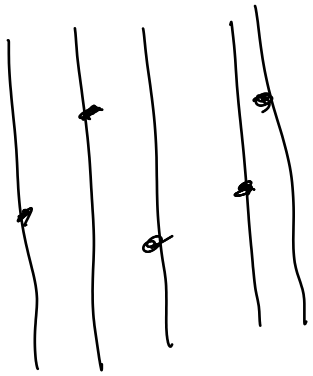
Direct pf of Thm 2.36

$$\sqrt{I} \supseteq I, \text{ so } \dim_K\big(\underbrace{K[X_1,\dots,X_n]/\sqrt{I}}_{\Gamma(V(I))}\big)$$

$$\leq \dim_K\big(K[X_1,\dots,X_n]/I\big)$$

Assume $V(I) = \{P_1,\dots,P_m\}$ with $P_j = (a_{1j},\dots,a_{nj})$.

$$\Rightarrow (X_i - a_{i1})\cdots(X_i - a_{im}) \in I(V(I)) = \sqrt{I}$$



$$\Rightarrow \exists N \geq 1\ \forall i: \big((X_i - a_{i1})\cdots(X_i - a_{im})\big)^N \in I$$

$$\Rightarrow \dim_K(\cdots/I) \leq \dim_K\Big(\cdots/\underbrace{(\text{id. gen. by } ((X_i - a_{i1})\cdots(X_i - a_{im}))^N)}_{T}\Big)$$

$$= (mN)^n .$$

$\uparrow$

basis: $\{X_1^{e_1}\cdots X_n^{e_n} \mid 0 \leq e_1,\dots,e_n < Nm\}$ of T

$\square$

2.11 Morphisms

Def Let $V \subseteq K^n$ and $W \subseteq K^m$ be algebraic subsets. A morphism (= regular map = polynomial map) $\varphi : V \to W$ 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
$$\begin{aligned} f : K &\longrightarrow V(Y - X^2) \subseteq K^2 \\ x &\longmapsto (x, x^2) \end{aligned}$$

Ex The identity $id : V \to V$

Ex An inclusion $V \to W$, where $V \subseteq W \subseteq K^n$.

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 $\varphi : \overset{K^n}{\overset{\cup\!\shortmid}{V}} \longrightarrow K^m$ correspond exactly to tuples $(f_1, \dots, f_m)$ of functions $f_i \in \Gamma(V) \quad (f_i : V \to K)$.

In particular, morphisms $\varphi : V \to K$ correspond exactly to elements of $\Gamma(V)$.

How to tell whether the image of $\varphi : V \to K^m$ is contained in W?

__Lemma 2.38__ $\varphi(V) \subseteq W$ 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 $h(y_1, \dots, y_m) \in I(W)$.

__Pf__ $\varphi(P) \in W = V(I(W)) \quad \forall P \in V$

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

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

__Def__ For any morphism $\varphi : V \to W$, we consider the K-algebra homomorphism

$$\varphi^* : \Gamma(W) \longrightarrow \Gamma(V)$$
$$f \longmapsto f \circ \varphi$$

$$\begin{tikzcd}
V \arrow[r, "\varphi"] \arrow[dr, dashed, "f \circ \varphi"'] & W \arrow[d, "f"] \\
 & K
\end{tikzcd}$$

φ^* is called the <u>pullback function</u> of φ.

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

Thm 2.40 We get a bijection

$$\left(\text{morphisms } V \to W\right) \longleftrightarrow \left(\begin{array}{c}K\text{-algebra homomorphisms} \\ \Gamma(W) \to \Gamma(V)\end{array}\right)$$

$$\varphi \qquad \longleftrightarrow \qquad \varphi^*$$

Pf How to determine φ from φ^*?

Let $y_i \in \Gamma(W)$ be the function mapping any point in $\underset{\substack{\cap \\ K^m}}{W}$ to its i-th coordinate.

Then, $\varphi(P) = (y_1(\varphi(P)), \dots, y_m(\varphi(P)))$

$$= (\varphi^*(y_1)(P), \dots, \varphi^*(y_m)(P))$$

$\boxed{\text{The m elements of } \Gamma(V) \text{ defining the morphism } \varphi: V \to W.}$

□

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

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

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

Rmk Hence,

$$\left\{\begin{matrix}\text{alg. subsets of } K^n \\ \text{for some } n\end{matrix}\right\} \longleftrightarrow \left\{\begin{matrix}\text{finitely generated} \\ \text{reduced } K\text{-algebras}\end{matrix}\right\}$$

$$V \longmapsto \Gamma(V)=K[x_1,\dots,x_n]/I(V)$$

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

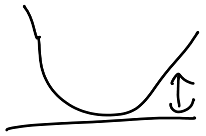
is a contravariant equivalence of categories.

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

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

Ex The inverse of $K \to V(Y-X^2)$

$$x \mapsto (x, x^2)$$



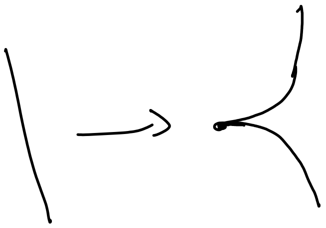
is $x \leftarrow\!\shortmid (x,y)$.

Ex Any translation in K^n is a isomorphism.

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

Warning Not every bijective morphism $f: V \to W$ is an isomorphism! (Just like not every bijective continuous map is a homeomorphism.)

Exe
$$\varphi: K \longrightarrow V(X^3 - Y^2) \subseteq K^2$$
$$t \longmapsto (t^2, t^3)$$



is a bijection with inverse
$$\frac{Y}{X} \longleftarrow\!\shortmid (X, Y)$$

because
$$\varphi^*: K[X,Y]/(X^3-Y^2) \longrightarrow K[T]$$
$$X \longmapsto T^2$$
$$Y \longmapsto T^3$$

is not an isomorphism because T does not lie in the image.

Thm 2.41 Any morphism $\varphi: \underset{\overset{\cap}{K^n}}{A} \to \underset{\overset{\cap}{K^m}}{B}$ is continuous (w.r.t. the Zariski topologies on A and B).

Pf
$$\varphi^{-1}(\underbrace{V(J)}_{\substack{\text{closed}\\ \text{subset of } K^m}}) = \{P \in A \mid \underbrace{\varphi(P) \in V(J)}\} = \underbrace{V(\varphi^*(J))}_{\substack{\text{closed}\\ \text{subset}\\ \text{of } A}}$$
$$\iff f(\varphi(P)) = 0 \ \forall f \in J$$
$$\iff \varphi^*(f)(P) = 0 \ \forall f \in J$$
$$\iff P \in V(\varphi^*(J))$$

$\square$

Thm 2.42 $\varphi^* : \Gamma(W) \longrightarrow \Gamma(V)$ is injective if and only if $\varphi(V)$ is (Zariski) dense in W.

Def Such a morphism φ is called *dominant*.

Pf Let $V \subseteq K^n$, $W \subseteq K^m$.

φ^* injective

$$\iff \forall f \in \Gamma(W) \text{ if } \underbrace{\underset{\overset{\shortparallel}{f\circ\varphi}}{\varphi^*(f)} = 0 \text{ on } V}_{f = 0 \text{ on } \varphi(V)}, \text{ then } f = 0 \text{ on } W$$

$$\iff \forall f \in K[Y_1, \dots, Y_m] \text{ if } \underbrace{f = 0 \text{ on } \varphi(V)}_{\iff f \in I(\varphi(V))}, \text{ then } \underbrace{f = 0 \text{ on } W}_{f \in I(W)}.$$

$$\iff I(\varphi(V)) \subseteq I(W)$$

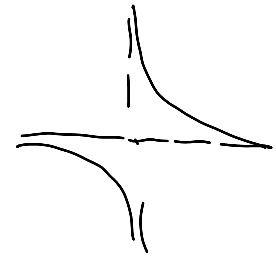
~~$\iff \varphi(V) \supseteq W$~~ $\cancel{\square}$

$$\Rightarrow \underset{\overset{\shortparallel}{\overline{\varphi(V)}}}{V(I(\varphi(V)))} \supseteq \underset{\overset{\shortparallel}{W}}{V(I(W))}$$

closure of $\varphi(V) \subseteq K^n$ w.r.t. the Zariski topology.

$$\boxed{\begin{array}{c} A \supseteq B \Rightarrow I(A) \subseteq I(B) \\ \cancel{\Leftarrow} \end{array}}$$

To do: show "$\Leftarrow$" $\square$



Exe $\varphi: V(XY-1) \longrightarrow K$

$(x,y) \longmapsto x$

has image $K\setminus\{0\}$ (dense in K).

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

$T \longmapsto X$

is injective.

Rmk The compositum of two dominant morphisms is dominant.

Thm 2.43 $\varphi^*: \Gamma(W) \to \Gamma(V)$ is surjective if and only if $\varphi: V \to \varphi(V)$ is an isomorphism (onto its image).

Pf Let $I \subseteq \Gamma(W)$ be the kernel of φ. Since $\Gamma(V)$ is reduced, the ideal I of $\Gamma(W)$ is a radical ideal. Let $\underset{V(I)}{\underset{\shortparallel}{W'}} \subseteq W$ be the corresponding algebraic subset of W.

We get a map $\varphi^*: \underset{\Gamma(W')}{\underset{\shortparallel}{\Gamma(W)/I}} \longrightarrow \Gamma(V)$

corr. to $\varphi: V \longrightarrow W'$ (the closure of the image of $\varphi: V \to W$ is W' by the previous theorem).

Then, $\varphi^* : \Gamma(W) \longrightarrow \Gamma(V)$ is surjective if and only if $\varphi^* : \Gamma(W') = \Gamma(W)/I \longrightarrow \Gamma(V)$ is an isomorphism. In other words:

$\varphi : V \longrightarrow W'$ is an isomorphism. $\square$

2.12. 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 $I = (f_1, \dots, f_m) \subseteq K[x_1, \dots, x_n]$?

Ex 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 $h \in I \Leftrightarrow g \mid h$.

Ex 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 monomial order 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 well-order: every $\emptyset \neq T \subseteq \mathcal{S}$ has a smallest element.

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

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

Ese Lexicographic order

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

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

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

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

Exe *Degree lexicographic order*

...

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

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

Exe *Degree reverse lexicographic order*

...

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

Rmk For $n=2$, deg. lex. $=$ deg. rev. lex.

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

A monomial M *occurs in* f if $c_M \neq 0$.

Let $f \neq 0$.

Its *leading monomial* (w.r.t. $\leq$) is

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

Its *leading coefficient* (w.r.t. $\leq$) is

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

Its *leading term* (w.r.t. $\leq$) is

$$lt(f) = lc(f)\cdot lm(f).$$

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

lt $\qquad$ lt $\qquad$ lt

lc $\qquad$ lc $\qquad$ 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 occuring 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 $$f^{(1)} := f - \frac{c_{N^{(1)}} N^{(1)}}{\mathrm{lt}(g)} \cdot g.$$

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

Continue this ~~pro~~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.

Def A reduction 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 $lm(g_i h_i) \leq lm(f)$.

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

Ex Use lex. order on $\mathbb{Q}(X,Y)$.

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

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

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

Warning Reductions aren't always unique!

Ex Use lex. order on $S(X,Y)$

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

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

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

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

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

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.

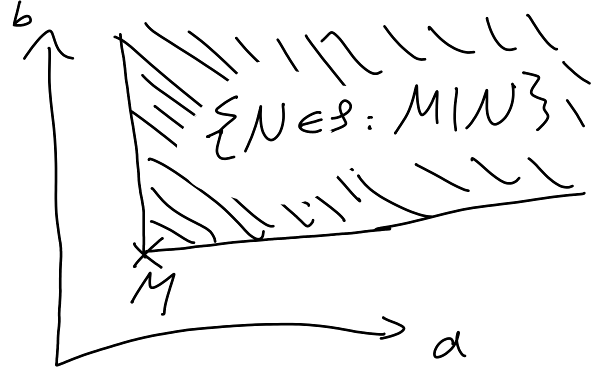
Rmk Let $A \subseteq S$. A monomial M is divisible by an element of A if and only if it is contained in the ideal (A) generated by the elements of A.

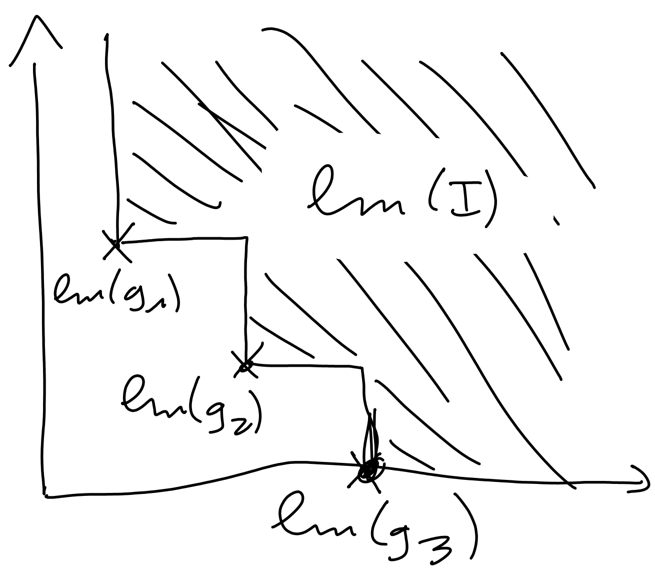
Cor 2.44 Any ideal $I \subseteq K[X_1, \dots, X_n]$ has a finite Gröbner basis.

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 $G = \{g_1, \dots, g_r\}$. □

Picture ($n=2$)

$M = X^a Y^b$





Thm 2.45 The monomials $M \notin \mathrm{lm}(I)$ 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 $M \notin \mathrm{lm}(I)$.

linearly independent:

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

$\Rightarrow f \notin I$. $\square$

Cor 2.46 $\dim_K(K[x_1, \dots, x_n]/I) = \#(S \setminus \mathrm{lm}(I))$.

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

Thm 2.47 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.

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

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

$\Rightarrow r_1$ or r_2 isn't reduced w.r.t. G! $\lightning$ $\square$

Cor 2.48 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 2.49 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 2.50 (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 2.48 to $S(f,g) \in I$.

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

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

with $0 \neq g_i \in G$ and monomials $H_i \in S$ with minimal $M := \max_{1 \leq i \leq r} (\mathrm{lm}(g_i H_i))$.

$\lambda_i \in K^{\times}$

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

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

Since the monomial M has to cancel in the RHS of (I).

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

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

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

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

$\square$

Similar to:

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

$$(lm(G_0)) \subsetneq (lm(G_1)) \subsetneq (lm(G_2)) \subsetneq \dots$$

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).

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

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

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

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

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

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

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

$f_2 = X^2Y+1$

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

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

Es $I = (X^3-2XY, X^2Y-2Y^2+X)$, 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.

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

Another aside

Thm Let $f \in K(X_1, \dots, X_n)$ and assume that

$$V\left(f, \frac{\partial f}{\partial X_1}, \dots, \frac{\partial f}{\partial X_n}\right) = \emptyset.$$

(There is no $P \in K^n$ with $f(P) = \frac{\partial f}{\partial X_1}(P) = \dots = \frac{\partial f}{\partial X_n}(P) = 0$.)

Then, (f) is a radical ideal. (f is squarefree.)

Eg $X^2 + Y^2 - 1$ is squarefree if $\mathrm{char}(K) \neq 2$:

$$V(X^2 + Y^2 - 1, 2X, 2Y) = \emptyset.$$

Warning The theorem is not an equivalence!

Pf of Thm Assume $f = g^2 h$, where g is a nonconstant polynomial and h is any polynomial.

Then $\frac{\partial f}{\partial X_i} = g^2 \frac{\partial h}{\partial X_i} + 2g \frac{\partial g}{\partial X_i} h$.

Let $P \in V(g)$. Then, $\frac{\partial f}{\partial X_i}(P) = 0$. $\square$

2.13. Rational functions

Let $V \subseteq K^n$ be an irreducible variety.
Recall that this means that $\Gamma(V)$ is an integral domain.

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

Ex $V = K^n \rightsquigarrow K(V) = K(X_1, \dots, X_n)$.

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

$$\rightsquigarrow K(V) = \left\{ \frac{a}{b} \;\middle|\; a, b \in K[X,Y,Z]/(XY-Z^2), \; b \neq 0 \right\}$$

$$= \left\{ \frac{a}{b} \;\middle|\; \begin{array}{l} a, b \text{ regular map on } V, \\ b \text{ not everywhere } 0 \text{ on } V \end{array} \right\}$$

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 $b(P) \neq 0$.
We then write $f(P) = \frac{a(P)}{b(P)} \in K$.

Rmk If $f = \frac{a}{b}$ for some a, b 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 $b'(P) \neq 0$.

$$\Rightarrow \underbrace{a(P)}_{\neq 0}\underbrace{b'(P)}_{\neq 0} = a'(P)\underbrace{b(P)}_{=0} \quad \lightning \qquad \square$$

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

It is not defined at $(x, 0, 0)$ for any $x \neq 0$.

Lemma 2.51 The set U_f of points $P \in V$ at which $f \in K(V)$ is defined is a nonempty open subset of V (open w.r.t. the subspace topology on V), i.e. it's the intersection of an open subset of K^n with V.

Rmk Equivalently: The set of points $P \in V$ at which f isn't defined is closed (= algebraic).

Pf If $f = \frac{a}{b}$ with $b \in \Gamma(V)$ not everywhere 0 on V.

$\Rightarrow$ f is defined (at least) at every point $Q \in V$ with $Q \notin V(b)$.

$\emptyset \neq V \setminus V(b)$ is an open subset of V.

For any $P \in U_f$, we can find a, b as above with $b(P) \neq 0$, so $P \in V \setminus V(b)$.

$\Rightarrow$ U_f is covered by open sets.

$\Rightarrow$ U is open. $\Box$

Ese A We know that f is not defined at any point in $\{(x,0,0) \mid x \neq 0\}$.

$\Rightarrow$ f is not defined at any point in the Zariski closure $\{(x,0,0) \mid x \in K\}$.

$\Rightarrow$ f is not defined at $(0,0,0)$.

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

$$P = (t,t,t) \in V \rightsquigarrow f(P) = \frac{t}{t} = 1 \xrightarrow{t \to 0} 1$$

$$\xrightarrow[t \to \infty]{} (0,0,0)$$

$$\neq$$

$$P = (t^{3/2}, t^{1/2}, t) \in V \rightsquigarrow f(P) = \frac{t^{3/2}}{t^{1/2}} = t \xrightarrow{t \to 0} 0$$

$$\xrightarrow[t \to 0]{} (0,0,0)$$

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

Pf 2 of Lemma 2.51

$I_f := \{b \in \Gamma(V) \mid f \cdot b \in \Gamma(V)\}$ is a nonzero ideal of $\Gamma(V)$ and $V(I_f) \subsetneqq V$ is the set of points $P \in V$ at which f is not defined. □

Any $f \in K(V)$ gives rise to a map $f : U_f \longrightarrow K$.

Lemma 2.52 If $U, U' \neq \emptyset$ are open subsets of an irreducible alg. subset $V \subseteq K^n$, then $U \cap U' \neq \emptyset$.

Pf $V \setminus U$ and $V \setminus U' \subsetneqq V$ are closed subsets of V. If $U \cap U' = \emptyset$, then $V = (V \setminus U) \cup (V \setminus U')$, so V is reducible. □

Lemma 2.53 If $f \in K(V)$ is zero on a nonempty open subset $U \subseteq U_f$, then $f = 0$.

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

$$\Rightarrow \underset{\nwarrow}{U} \cap \underset{\uparrow}{(V \setminus V(a))} \cap \underset{\nearrow}{(V \setminus V(b))} = \emptyset \Rightarrow \lightning \text{ by Lemma 2.52}$$

nonempty open subsets of V

if $a \neq 0$

□

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

Rmk This is similar to facts from complex analysis: If two meromophic functions $f, g : \mathbb{C} \to \mathbb{C}$ agree on a nonempty open subset of $\mathbb{C}$, then $f = g$.

Cor The elements of $K(V)$ correspond bijectively to 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

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

where we identify $(U, f), (U', f')$ if

$$f|_{U \cap U'} = f'|_{U \cap U'} .$$

Reminder
The field of fractions of an integral domain is the set of pairs (a, b) with $a, b \in R$, $b \neq 0$, where we identify (a, b) and (a', b') if $ab' = a'b$.
((a,b) corresponds to $\frac{a}{b}$.)

Rmk If $\varphi : V \to W$ is a dominant ($\overline{\varphi(V)} = W$) morphism,

then we obtain an injective ring homomorphism

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

which induces a field homomorphism

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

Rmk Dominance is important:

Otherwise, f might not be defined at any point in $\varphi(V)$, so $f \circ \varphi$ wouldn't be defined at any point in V!

Rmk We have $U_{\varphi^*(f)} \supseteq \varphi^{-1}(\underbrace{U_f}_{\substack{\neq \emptyset, \\ \text{open} \\ \text{subset} \\ \text{of } W}}) \underset{\boxed{\varphi \text{ dominant}}}{\neq} \emptyset$

(open subset of V).

Def The local ring of V at $P \in V$ is

$$\mathcal{O}_{V,P} := \{ f \in K(V) \text{ defined at } P \}.$$

(Fulton denotes it by $\mathcal{O}_P(V)$.)

Thm 2.54

a) $\mathcal{O}_{V,P}$ is a local ring (ring with exactly one maximal ideal) with maximal ideal $m_{V,P} = \{ f \in \mathcal{O}_{V,P} \mid f(P) = 0 \}$.

b) We have $\mathcal{O}_{V,P} / m_{V,P} \cong K$.

$$f \mapsto f(P)$$

Pf ring: if $b_1(P), b_2(P) \neq 0$, then $\frac{a_1}{b_1} + \frac{a_2}{b_2} = \frac{a_1 b_2 + a_2 b_1}{b_1 b_2}$

with $(b_1 b_2)(P) \neq 0$, ...

ideal: clear

map in b surj: constant fct.

inj: clear

$\Rightarrow$ max. ideal ✓

only max. ideal: Let $I \overset{m_{V,P}}{\underset{\ne}{\subsetneq}} \mathcal{O}_{V,P}$ be another maximal ideal. $\Rightarrow I \not\subseteq m_{V,P}$. Let $f \in I \setminus m_{V,P}$. $\Rightarrow f(P) \neq 0$.

$\Rightarrow \frac{1}{f}$ defined at $P \Rightarrow \frac{1}{f} \in \mathcal{O}_{V,P}$

$\overset{\uparrow}{\Rightarrow} 1 = f \cdot \frac{1}{f} \in I \Rightarrow I = \mathcal{O}_{V,P}$ ↯

I ideal

□

Exe $V = K$, $P = c \in K = V$

$\Rightarrow \Gamma(V) = K[X]$, $K(V) = K(X)$

$$\mathcal{O}_{V,P} = \left\{ \frac{a}{b} \mid a, b \in K[X],\ \underset{\overset{\Updownarrow}{\text{b not divisible by } X-c}}{b(c) \neq 0} \right\}$$

$$m_{V,P} = \left\{ \frac{a}{b} \mid a(c) = 0,\ b(c) \neq 0 \right\}$$

$= $ ideal of $\mathcal{O}_{V,P}$ generated by $X - c$.

Remk If $\varphi : V \to W$ is any morphism, and $P \in V$, then we obtain a ring homomorphism

$$\begin{aligned} \varphi^* : \mathcal{O}_{W,\varphi(P)} &\longrightarrow \mathcal{O}_{V,P} \\ \frac{a}{b} &\longmapsto \frac{\varphi^*(a)}{\varphi^*(b)} \\ f &\longmapsto f \circ \varphi \end{aligned}$$

with $\varphi^*(m_{W,\varphi(P)}) \subseteq m_{V,P}$.

Thm 2.55 $\Gamma(V) = \bigcap_{P \in V} \mathcal{O}_{V,P}$

($f \in \Gamma(V) \Leftrightarrow$ f defined at every $P \in V$)

Pf "$\Rightarrow$" clear

"$\Leftarrow$" Let $I_f = \{ b \in \Gamma(V) \mid f \cdot b \in \Gamma(V) \}$ as before.

$$\underset{\substack{\uparrow \\ \text{f defined everywhere}}}{\Rightarrow} V(I_f) = \emptyset \underset{\substack{\uparrow \\ \text{weak Nullstellensatz}}}{\Longrightarrow} 1 \in I_f \Rightarrow f \in \Gamma(V).$$

$\square$

Lemma 2.56 The ring $\mathcal{O}_{V,P}$ is noetherian.

Pf Let I be an ideal of $\mathcal{O}_{V,P}$.

$\Rightarrow I \cap \Gamma(V)$ is an ideal of $\Gamma(V)$.

$\Rightarrow I \cap \Gamma(V) = (g_1, \ldots, g_m)_{\Gamma(V)}$ for some $g_1, \ldots, g_m \in \Gamma(V)$.

The quotient $\Gamma(V)$ of $K[x_1, \ldots, x_n]$ is noetherian.

Let $f = \frac{a}{b} \in I$, $b(P) \neq 0$.

$\Rightarrow a = f \cdot b \in I \cap \Gamma(V) = (g_1, \ldots, g_m)$

$\Rightarrow \frac{a}{b} \in (g_1, \ldots, g_m)_{\mathcal{O}_{V,P}}$. $\square$

$\frac{1}{b} \in \mathcal{O}_{V,P}$

Def For any open subset $U \subseteq V$, $\mathcal{O}_V(U)$ is the ring of rational functions $f \in K(V)$ defined at every point $P \in U$.

Rmk If $\varphi : V \to W$ is any morphism between irreducible alg. sets and $U \subseteq W$ open, we obtain a ring homomorphism $\varphi^* : \mathcal{O}_W(U) \longrightarrow \mathcal{O}_V(\varphi^{-1}(U))$.

Def Let $V \subseteq K^n$ and $W \subseteq K^m$ be algebraic subsets. A rational map $\varphi : V \dashrightarrow W$ is a pair (U, φ), where $\emptyset \neq U \subseteq V$ is open, and $\varphi : U \to W$ is a map given by rational functions $f_1, \dots, f_m \in \mathcal{O}_V(U)$:

$$\varphi(P) = (f_1(P), \dots, f_m(P)) \quad \forall P \in U,$$

where we identify $(U, \varphi), (U', \varphi')$ if

$$\varphi|_{U \cap U'} = \varphi'|_{U \cap U'}.$$

Rmk A rat. map $V \to K^m$ "is" a tuple $(f_1, \dots, f_m)$ of rational functions $f_1, \dots, f_m \in K(V)$.

Ex Any morphism $\varphi : V \longrightarrow W$ is a rational map.

Def If $\varphi : A \dashrightarrow B$ and $\psi : B \dashrightarrow C$ are
(def. on U) (def. on U')
rational maps we get a composition

$$\psi \circ \varphi : A \dashrightarrow C$$

$$(\text{def. on } \underbrace{\varphi^{-1}(U')}_{\substack{\text{nonempty open} \\ \text{subset of } A \text{ if } \varphi \text{ is dominant}}})$$

and φ is dominant

Rmk If $\varphi : V \dashrightarrow W$ is dominant ($\overline{\varphi(U)} = W$), we get a field homomorphism

$$\varphi^* : K(W) \longrightarrow K(V).$$
$$f \longmapsto f \circ \varphi$$

Rmk We get a bijection

$$\left\{ \begin{array}{c} \text{dominant rational} \\ \varphi : V \dashrightarrow W \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{field hom.} \\ \varphi^* : K(W) \to K(V) \end{array} \right\}$$

Pf Same as for morphisms:
$f_i = \varphi^*(X_i)$, where $X_i \in \Gamma(W)$ is the

rational map sending any point P to its i-th coordinate. $\square$

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

Ex $V(X^3 - Y^2) \subset K^2$ is not isomorphic to K (see problem 1d on problem set 3).

But they are birational:

$$\varphi : K \longrightarrow V(X^3-Y^2)$$
$$t \longmapsto (t^2, t^3)$$

$$\psi : V(X^3-Y^2) \dashrightarrow K$$
$$(x,y) \longmapsto \frac{y}{x} \quad \text{(defined on } V(x^3-y^2)\setminus\{0,0\}\text{)}$$

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

2.14. Dimension and transcendence degree

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

($\Leftrightarrow$ a_1 algebraic if $n=1$)

Ex $X_1, \dots, X_n \in K(X_1, \dots, X_n)$ are algebraically independent over K.

Ex $X, Y \in K(V(X^2 - Y^3))$ are algebraically dependent over K: $X^2 - Y^3 = 0$ in $K(V(X^2 - Y^3))$.

Rmk $\pi, e \in \mathbb{C}$ are transcendental over $\mathbb{Q}$

It is unknown whether π, e are algebraically independent over $\mathbb{Q}$.

Thm 2.57 $a_1, \dots, a_n \in L$ are algebraically dependent if and only if some a_i is algebraic over $K(a_1, \dots, a_{i-1})$.

Analogy Let V be a K-vector space. Then, $v_1, \dots, v_n \in V$ are linearly dependent if and only if some v_i is contained in the span of $v_1, \dots, v_{i-1}$.

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

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

Clear out denominators to make

$0\neq f\in K[a_1,\dots,a_{i-1}][T]$.

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

If $g(X_n)=f(a_1,\dots,a_{n-1},X_n)\in K(a_1,\dots,a_{n-1})[T]$ is not the zero polynomial, then $g(a_n)=0$ is a pol. eq. satisfied by a_n with coeff. in $K(a_1,\dots,a_{n-1})$, so a_n is algebraic over $K(a_1,\dots,a_{n-1})$.

$\leadsto$ Assume $g(X_n)$ is the zero polynomial.

Let $f(X_1,\dots,X_n)=\sum_i f_i(X_1,\dots,X_{n-1})\cdot X_n^i$

with $f_j(X_1,\dots,X_{n-1})$ not the zero polynomial for some i

But because $g(X_n)$ is the zero polynomial, we have

$f_j(a_1,\dots,a_{n-1}]=0$.

$\Rightarrow a_1,\dots,a_{n-1}$ are algebraically dependent.

Proceed by induction over n. $\square$

Def Elements $a_1, \dots, a_n \in L$ form a transcendence basis of L over K if they are algebraically independent and L is an algebraic ext. of $K(a_1, \dots, a_n)$.

Rmk A transcendence basis is a maximal list of algebraically independent elements.

Exe $X_1, \dots, X_n$ form a transcendence basis of $K(X_1, \dots, X_n)$.

Lemma 2.58 ("Exchange lemma")

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

Pf Choose any maximal alg. independent sublist of $a_1, \dots, a_n, b_1, \dots, b_m$ among those containing $a_1, \dots, a_n$. The remaining b_j have to be algebraic over

K(the list you got).

$\Rightarrow K$(the list) $= L$. $\square$

Cor 2.59 Any finitely generated field extension has a transcendence basis.

Thm 2.60 If $a_1, \dots, a_n$ is a transcendence basis of L over K and $b_1, \dots, b_m \in L$ are algebraically independent, then $n \geq m$.

Cor 2.61 Any two transcendence bases of L over K have the same size, called the transcendence degree $\operatorname{trdeg}(L|K)$ of L over K.

Rmk $\operatorname{trdeg}(L|K) = 0 \Longleftrightarrow L$ is an algebraic extension of K

Pf of Thm 2.60

Use induction over n.

$n=0$: $\Rightarrow L$ is alg. over K $\Rightarrow$ there are no algebraically independent elements. $\Rightarrow m=0$

$n-1 \to n$: Let (w.l.o.g.) $b_1, a_1, \dots, a_r$ be a transcendence basis from the exchange lemma.

$\Rightarrow r \neq n$ because $b_1, a_1, \dots, a_n$ aren't alg. indep. because $a_1, \dots, a_n$ is a transcendence basis

$a_1, \dots, a_r \in L$ form a transcendence basis of L over $K(b_1)$.

$b_2, \dots, b_m \in L$ are alg. independent over $K(b_1)$.

Apply the induction hypothesis to the extension L of $K(b_1)$.

$\Rightarrow n-1 \geq r \geq m-1 \quad \Rightarrow n \geq m$. $\square$

Ex X is a transcendence basis of $K(V(X^2-Y^3))$

$\Uparrow$ Y —"— ——

- No nonzero pol. $f(X) \in K[X]$ becomes zero in $K(V(X^2-Y^3))$ because it doesn't become zero in $\Gamma(V(X^2-Y^3)) = K[X,Y]/(X^2-Y^3)$ because $f(X) \notin (X^2-Y^3)$.

$\Rightarrow X$ is alg. independent

- X, Y are algebraically dependent
- X, Y generate the field extension $K(V(X^2-Y^3))$

$\Rightarrow \operatorname{trdeg}(K(V(X^2-Y^3))) = 1$.

Thm 2.61 If L is a finitely generated field extension of K and M is a finitely generated field extension of L, then

$$\begin{tikzcd} M \arrow[d, dash] \\ L \arrow[d, dash] \\ K \end{tikzcd} \qquad \operatorname{trdeg}(M|K) = \operatorname{trdeg}(M|L) + \operatorname{trdeg}(L|K)$$

Pf If $a_1, \dots, a_n$ is a transcendence basis of M/L

and $b_1, \dots, b_m$ — " — $L|K$,

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

"□"

Def The dimension $\dim(V)$ of an irreducible algebraic set $V \subseteq K^n$ is the transcendence degree of $K(V)$ over K.

Ex $\dim(\underbrace{\mathbb{A}^n_K}_{K^n}) = n$

Cor $\mathbb{A}^n = K^n$ is not isomorphic (or even birational) to $\mathbb{A}^m = K^m$ for any $n \neq m$.

Analogy from topology

There is no homeomorphism between $\mathbb{R}^n$ and $\mathbb{R}^m$ for $n \neq m$. In fact, there is no homeomorphism between an open subset $\emptyset \neq U \subseteq \mathbb{R}^n$ and an open subset $\emptyset \neq V \subseteq \mathbb{R}^m$!

Thm 2.62 The dimension of an irreducible algebraic subset $V = V(f) \subsetneqq K^n$ defined by a single (irreducible) polynomial

$$0 \neq f \in K[X_1, \dots, X_n] \text{ is } \dim(V) = n - 1.$$

Pf W.l.o.g. the variable X_n occurs in f.

$$\Rightarrow X_1, \dots, X_{n-1} \in \underset{\displaystyle K(V)}{\underset{\cap}{\Gamma(V)}} = K[X_1, \dots, X_n]/(f)$$

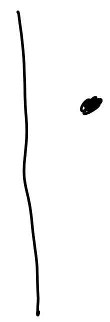
form a transcendence basis of $K(V)$ over K.

(They are algebraically independent because (f) contains no polynomial in just the variables $X_1, \dots, X_{n-1}$.
But $X_1, \dots, X_n$ are not algebraically independent.) $\square$

Rmk Why only define dim (V) when V is irreducible?

A) If V isn't irreducible, $\Gamma(V)$ is not an integral domain, and there is no field of fractions $K(V)$!

B) Say $V = \{(x,y) \in K^2 \mid x = 0\} \cup \{(1,2)\}$.



We define the dimension of a reducible alg. set $V \subseteq K^n$ to be $\dim(V) = \max(\dim(W_1), \dots, \dim(W_m))$, where $W_1, \dots, W_m$ are the irreducible components of V.

And $\dim(\emptyset) = -\infty$.

Thm 2.63 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.

"$\Leftarrow$" If $|V| < \infty$, then $|V| = 1$, $V = \{P\}$.

$$\Rightarrow \Gamma(V) = K, \quad K(V) \underset{\substack{\uparrow \\ \text{trdeg} = 0}}{=} K.$$

"$\Rightarrow$" $\dim(V) = 0 \Rightarrow K(V)$ is an alg. ext. of K

$$\underset{\substack{\uparrow \\ \boxed{\text{K algebraically closed}}}}{\Longrightarrow} K(V) = K \Longrightarrow \underset{\substack{\parallel \\ K[x_1,\dots,x_n]/I(V)}}{\Gamma(V)} = K$$

$$\Rightarrow |V| = 1. \qquad \square$$

Lemma 2.64 If there is a dominant rational map $\varphi : V \dashrightarrow W$, then $\dim(V) \geq \dim(W)$.

Pf Decompose V, W into irreducible components:

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

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

$$\Rightarrow \underbrace{W_j}_{\text{irreducible}} = \bigcup_{i=1}^{n} \underbrace{(\overline{\varphi(V_i)} \cap W_j)}_{\text{closed}}$$

$\Rightarrow W_j = \overline{\varphi(V_{r_j})} \cap W_j$ for some $r_j \in \{1, \dots,$ [illegible]$\}$

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

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

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

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

$\Rightarrow$ We obtain dominant morphisms

$$\varphi : V_{r_j} \longrightarrow W_j.$$

$\Rightarrow$ We can assume w.l.o.g. that V and W are irreducible.

$\varphi^* : K(W) \hookrightarrow K(V)$. If $a_1, \dots, a_d$ is a transcendence basis of $K(W)$ (over K), then $\varphi^*(a_1), \dots, \varphi^*(a_d)$ are still algebraically independent.

$\Rightarrow \dim(V) = \operatorname{trdeg}(K(V)|K) \geq d = \operatorname{trdeg}(K(W)|K) = \dim(W).$

$\square$

Lemma 2.65 If $V \subseteq W$, then $\dim(V) \leq \dim(W)$.

Pf W.l.o.g. V is irred. (replace by an irred comp.)

W.l.o.g. W is irred. (replace by some 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 elements of $\Gamma(V)$ generate $K(V)$ (the field ext. of k), there are elements $a_1, \dots, a_d \in \Gamma(V)$ which form a transcendence basis of $K(V)$.

Let $b_1, \dots, b_d \in \Gamma(W)$ such that $i^*(b_i) = a_i$. Then, $b_1, \dots, b_d \in K(W)$ are still algebraically independent: If $f \in k[X_1, \dots, X_d]$, $f(b_1, \dots, b_d) = 0$, then
$$f(a_1, \dots, a_d) = f(i^*(b_1), \dots, i^*(b_d))$$
$$= i^*(f(b_1, \dots, b_d)) = 0 . \quad \square$$

Thm 2.66 Let $V \subseteq K^n$ be an irreducible algebraic set. Then, dim(V) is the largest number $d \geq 0$ such that there is a dominant rational map $\varphi : V \dashrightarrow K^d$.

Pf Dominant rat. maps $\varphi : V \dashrightarrow K^d$ correspond to field homomorphisms $\varphi^* : \underset{\overset{\shortparallel}{K(K^d)}}{K(X_1, \dots, X_d)} \hookrightarrow K(V)$

which correspond to elements $a_i := \varphi^*(X_i)$ of $K(V)$. There is a well-defined field hom.

~~$\mathbb{C}(X) \longrightarrow \mathbb{C}$~~

~~$X \longmapsto \pi$~~

~~$\frac{1}{X-\pi} \longmapsto \frac{1}{\pi-\pi} = \frac{1}{0}$~~

$\varphi^* : K(X_1, \dots, X_d) \to K(V)$ sending X_i to $a_i \in K(V)$ if and only if the elements $a_i \in K(V)$ are algebraically independent over K (so that no nonzero denominator $0 \neq f \in K[X_1, \dots, X_d]$ can become $f(a_1, \dots, a_d) = 0$). $\square$

Rmk 2.67 There is in fact a dominant morphism $V^{\subseteq K^n} \longrightarrow K^d$ for $d = \dim(V)$.

Actually, there is a dominant projection $V \longrightarrow K^d$ 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 $V \to K^2$ is dominant

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

$n=3, d=2$ $\Rightarrow$ 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 $X_1, \dots, X_n$. $\Rightarrow$ There is a transcendence basis of the form $X_{i_1}, \dots, X_{i_d}$. Then, the projection

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

because

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

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

2.15. Finite morphisms

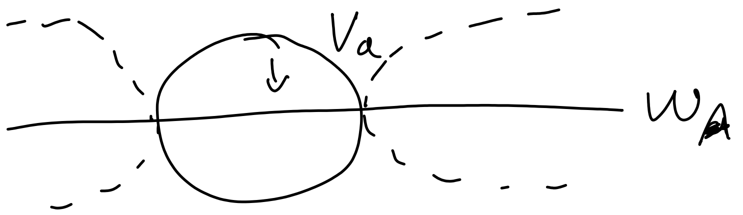
Some examples of dominant morphisms:

A) $\varphi_A : V_A = \{(x,y) \mid x^2+y^2=1\} \longrightarrow W_A = K$

$$(x,y) \longmapsto x$$

with image $\varphi_A(V_A) = K = W_A$

The preimage $\varphi^{-1}(t) \subseteq V_A$ of any $t \in K$ consists of at most 2 (and at least 1) points: $(t, \pm\sqrt{1-t^2})$.



$$\varphi_A^* : \Gamma(W_A) = K[T] \hookrightarrow K[X,Y]/(X^2+Y^2-1) = K[T][Y]/(T^2+Y^2-1)$$

$$T \longmapsto X \qquad \leftrightarrow T$$

B) $\varphi_B : V_B = \{(x,y) \mid xy=1\} \longrightarrow W_B = K$

$$(x,y) \longmapsto x$$

with image $\varphi_B(V_B) = K \setminus \{0\}$

The preimage $\varphi^{-1}(t) \subseteq V_B$ of any $t \in K$ consists of at most 1 point: $(t, \frac{1}{t})$.

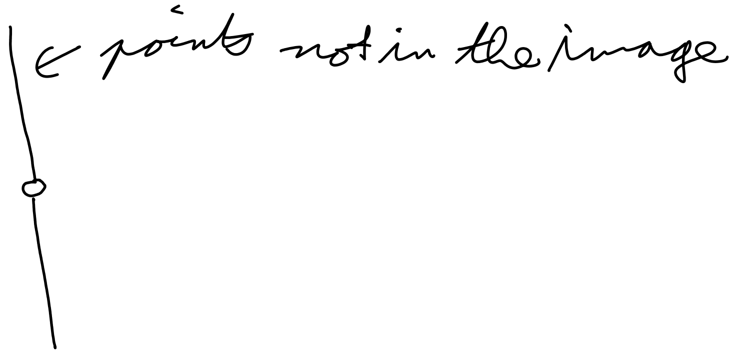
$$\varphi_B^* : K[T] \hookrightarrow K[X,Y]/(XY-1) = K[T][Y]/(TY-1)$$

$$T \longmapsto X \qquad \leftrightarrow T$$

c) $\varphi_C : V_C = K^2 \longrightarrow W_C = K^2$

$(x, y) \longmapsto (x, xy)$

with image $\varphi_C(V_C) = \{(t,u) \mid t \neq 0 \text{ or } u = 0\}$



The preimage $\varphi^{-1}(t,u)$ consists of exactly 1 point $(t, \frac{u}{t})$ if $t \neq 0$ and infinitely many points $(0, *)$ if $t = u = 0$.

$\varphi_C^* : K[T,U] \longrightarrow K[X,Y] \cong K[T,U][Y]/(TY-U)$

$T \longmapsto X \iff T$

$U \longmapsto XY \iff U$

What distinguishes A from B, C?

A) The ring ext. $\Gamma(V_A)$ of $\varphi_A^*(\Gamma(W_A))$ is integral since the polynomial T^2+Y^2-1 is monic when considered a polynomial in Y with variables in $K[T]$. Hence, for any t, the polynomial $t^2+Y^2-1 \in K[Y]$ still has degree 2 and therefore has 1 or 2 roots $y \in K$.

B) The pol. $TY-1$ is not monic "in Y" and for some $t (=0)$, the pol. $tY-1$ is -1, which has no root in y.

C) The pol. $TY-U$ is not monic "in Y" and for $t=u=0$, the $tY-u$ is 0, which has ∞ many roots $y \in K$.

Def A morphism $\varphi : V \longrightarrow W$ is finite if the ring extension $\Gamma(V)$ of $\varphi^*(\Gamma(W))$ is module-finite (or, equivalently, integral).

Ex φ_A is finite.

Ex Let $V \subseteq W$. Then, the inclusion morphism $i : V \hookrightarrow W$ is finite (because $i^* : \Gamma(W) \to \Gamma(V)$ is surjective).

Rmk The composition of two finite morphisms is finite.

Pf This follows from the transitivity of module-finiteness (or integrality). $\square$

Rmk In particular, the restriction of a finite morphism $V \longrightarrow W$ to an alg. subset $V' \subseteq V$ is finite. (It's the composition $V' \hookrightarrow V \longrightarrow W$.)

Rmk $\varphi : V \longrightarrow W \subseteq K^m$ is finite if and only if $\varphi : V \longrightarrow K^m$ is finite.

Pf $$\varphi^*(\underbrace{\Gamma(W)}_{K[X_1,\dots,X_m]/I(W)}) = \varphi^*(\underbrace{\Gamma(K^m)}_{K[X_1,\dots,X_m]}).$$ $\square$

Thm 2.68 If $\varphi : V \to W$ is a dominant finite morphism, then $\dim(V) = \dim(W)$.

Pf Decompose into irred. comp.:

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

As in the proof of Lemma 2.64, we obtain dom. finite morphisms $\varphi : V_{r_j} \longrightarrow W_j$ for $j = 1, \dots, b$.

$\Rightarrow$ We can assume w.l.o.g. that V, W are irreducible, so we get a field hom. $\varphi^* : K(W) \hookrightarrow K(V)$.

φ finite $\Longrightarrow$ $\Gamma(V)$ integral ext. of $\varphi^*(\Gamma(W))$.

$\Longrightarrow$ $K(V)$ algebraic over $\varphi^*(K(W))$.

If $b_1, \dots, b_d$ is a transcendence basis of $K(W)$, then $\varphi^*(b_1), \dots, \varphi^*(b_d)$ is a transcendence basis of $K(V)$.

$\square$

Cor 2.69 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 $Q \in \varphi(V)$.

$\Rightarrow$ The restriction $\varphi : \varphi^{-1}(Q) \longrightarrow \{Q\}$ is a surjective finite morphism.

$\Rightarrow \dim(\varphi^{-1}(Q)) = \dim(\{Q\}) = 0$

$\Rightarrow |\varphi^{-1}(Q)| < \infty$. $\square$

Thm 2.69 (Lying over property) Any dominant finite morphism $\varphi : V \to W$ is surjective.

Pf Let $Q \in W$ and let m be the maximal ideal of $\Gamma(W)$ corresponding to Q. (= the set of functions on W vanishing at Q)

Recall that $\varphi(P) = Q \Leftrightarrow \varphi(P) \in V(m) \Leftrightarrow P \in V(\underbrace{\varphi^*(m)}_{\subseteq \Gamma(V)})$

So $\varphi^{-1}(Q) = V(\varphi^*(m))$.

Let I be the ideal of $\Gamma(V)$ generated by $\varphi^*(m)$.

$\Rightarrow$ If $\varphi(Q) = \emptyset$, then $I = \Gamma(V)$.

$\uparrow$

Nullstellensatz

Let $\Gamma(V)$ be generated by $b_1, \dots, b_r$ as a $\varphi^*(\Gamma(W))$-module.

$\Rightarrow$ We can write any element of $\Gamma(V)$ as a lin. combination of $b_1, \dots, b_r$ with coeff. in $\varphi^*(\Gamma(W))$.

$\Rightarrow$ We can write any element of I as a lin. combination of $b_1, \dots, b_r$ with coeff. in $\varphi^*(m)$.

$\Rightarrow$ If $I = \Gamma(V)$, we can write

$b_i = \varphi^*(p_{i1})\, b_1 + \dots + \varphi^*(p_{ir})\, b_r$ with $p_{i1}, \dots, p_{ir} \in \varphi^*(m)$.

$$\Rightarrow \underbrace{\begin{pmatrix} \varphi^*(p_{11}) & \cdots & \varphi^*(p_{1r}) \\ \vdots & & \vdots \\ \varphi^*(p_{r1}) & \cdots & \varphi^*(p_{rr}) \end{pmatrix}}_{M} \begin{pmatrix} b_1 \\ \vdots \\ b_r \end{pmatrix} = \begin{pmatrix} b_1 \\ \vdots \\ b_r \end{pmatrix}$$

$$\Rightarrow (\underset{\substack{\uparrow \\ r \times r \text{ identity} \\ \text{matrise}}}{I_r} - M) \begin{pmatrix} b_1 \\ \vdots \\ b_r \end{pmatrix} = 0$$

$$\underset{\substack{\uparrow \\ \boxed{\text{as in the proof of Lemma 2.17}}}}{\Rightarrow} \det(I_r - M) = 0$$

But all entries of M lie $\varphi^*(m)$.

Expanding the determinant, we see that

$0 = \det(I_r - M) = 1 + c$ for some $c \in \varphi^*(m)$.

$\Rightarrow 1 \in \varphi^*(m)$

$\Rightarrow 1 \in m$ ↯

$\uparrow$

φ is dominant,
so φ^* is injective

□

Cor 2.70 Any finite morphism $\varphi : V \to W$ is *closed*: The image $\varphi(A) \subseteq W$ of every closed (=alg.) set $A \subseteq V$ is closed (=alg.)

Ex The proj. $K^2 \to K$ is *not* closed because the image of $\{(x,y) \mid xy = 1\}$ is not closed.

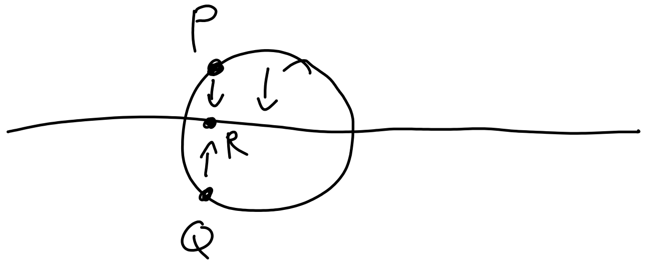
Pf $\varphi : A \longrightarrow \overline{\varphi(A)}$ is a dominant finite morphism, hence surjective.

$\Rightarrow \varphi(A) = \overline{\varphi(A)}$, so $\varphi(A)$ is closed. □

Lemma 2.72 (Incomparability)

Let $\varphi : V \longrightarrow W$ 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

$$f^n + \varphi^*(c_{n-1}) f^{n-1} + \dots + \varphi^*(c_0) = 0$$

with $c_{n-1}, \dots, c_0 \in \Gamma(W)$. Pick one of smallest possible degree n.

$\Rightarrow \varphi^*(c_0)\big|_{V_1} = -f^n - \varphi^*(c_{n-1})f^{n-1} - \dots - \varphi^*(c_1)f\big|_{V_1} = 0.$

If $\varphi(V_1) = W$, then $\Gamma(W) \xrightarrow{\varphi^*} \Gamma(V) \overset{i^*}{\twoheadrightarrow} \Gamma(V_1)$

$$g \mapsto g|_{V_1}$$

is injective because $V_1 \hookrightarrow V \longrightarrow W$ is dominant (actually surjective).

$\Rightarrow c_0 = 0$

$\Rightarrow f^{n-1} + \varphi^*(c_{n-1}) f^{n-2} + \dots + \varphi^*(c_1) = 0$

$f \neq 0$ and $\Gamma(V)$ is an integral domain because V is irreducible

monic pol. eq. of degree $n-1 < n$. ↯

□

<u>Lemma 2.73</u> Let $\varphi : V \to W$ be a dominant finite morphism and let B be an irreducible subset of W. Decompose $\varphi^{-1}(B)$ into irred. components: $\varphi^{-1}(B) = A_1 \cup \dots \cup A_r$.

Then, $\varphi(A_i) = B$ for <u>some</u> component A_i

<u>Pf</u> $$B \underset{\substack{\uparrow \\ \varphi \text{ surjective}}}{=} \varphi(\varphi^{-1}(B)) = \underbrace{\varphi(A_1)}_{\text{closed}} \cup \dots \cup \underbrace{\varphi(A_r)}_{\text{closed}}$$

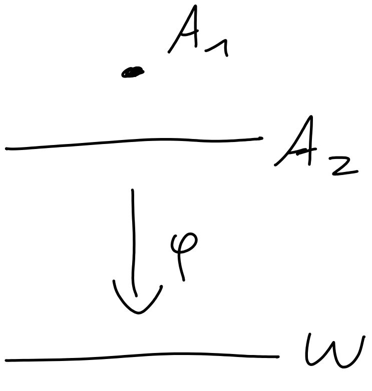
B irred, $\varphi(A_1), \dots, \varphi(A_r)$ closed

$\Rightarrow \varphi(A_i) = B$ for some i.

□

Rmk We might not have $\varphi(A_i)=B$ for all components A_i

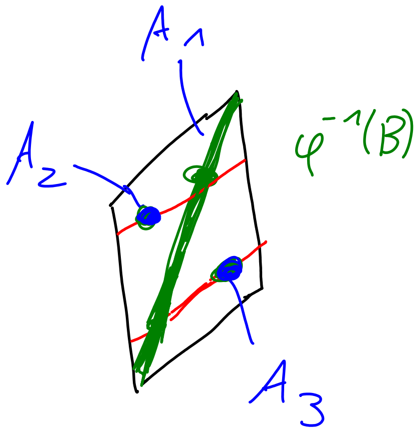
Exe



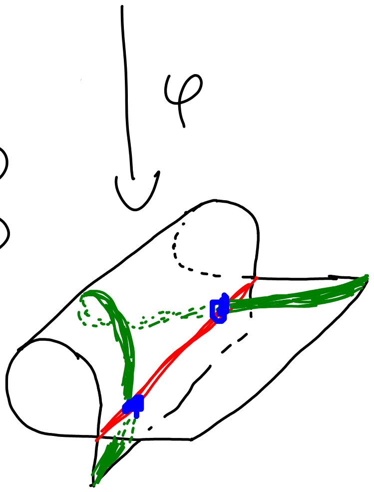
$$\begin{tikzcd} V=\{(x,y)\mid y=0\}\cup\{(0,1)\} \arrow[d] & (x,y) \arrow[d, mapsto] \\ B=W=K & x \end{tikzcd}$$ is finite

Problem: V not irreducible

Exe



$$\begin{tikzcd} V=K^2 \arrow[d, "\varphi"'] & (t,u) \arrow[d, mapsto] \\ W=\{(x,y,z)\mid x^2(x+1)=y^2\} & (t^2-1,t(t^2-1),u) \end{tikzcd}$$



φ is finite because $T,U\in\Gamma(V)$ is integral over $\varphi^*(\Gamma(W))$:
$$T^2-1-X=0$$
$$U-Z=0$$

$B=\varphi(\underbrace{\{(t,u)\mid t=u\}}_{\cong K})$ irreducible

$$\varphi^{-1}(B)=\underbrace{\{(t,u)\mid t=u\}}_{A_1}\cup\underbrace{\{(1,-1)\}}_{A_2}\cup\underbrace{\{(-1,1)\}}_{A_3}$$

Problem: W not normal

Def An irreducible algebraic 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.

Pf $\Gamma(V) = K[X_1, \dots, X_n]$ is a unique factorization domain and hence integrally closed in its field of fractions by Thm 2.15. $\square$

Thm 2.74 (Going down)

Let V be an irreducible alg. set and let W be a normal alg. set. Let $\varphi : V \to W$ be a dominant finite morphism. Let B be an irreducible 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.

Pf later...

2.16. Noether normalisation

Thm 2.75 (Noether normalisation)

Let R be a finitely generated ring ext. of K and an integral domain with field of fractions L. ($\Rightarrow L$ is a fin. gen. field ext. of K)

Let $n = \mathrm{trdeg}(L|K)$. Then, there are elements $a_1, \dots, a_n \in R$ such that R is an integral ext. of $K[a_1, \dots, a_n]$.

Rmk $a_1, \dots, a_n$ form a transcendence basis of L over K.

Pf of Rmk Every el. of R is algebraic over $K(a_1, \dots, a_n)$. $\Rightarrow$ Every el. of its field of fractions is alg. over $K(a_1, \dots, a_n)$. $\square$

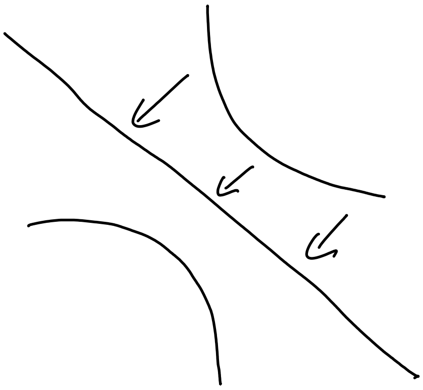
Cor 2.76 Let V be an irred. alg. set of dimension n. Then, there is a dominant finite morphism $V \longrightarrow K^n$.

Pf of Cor Apply Thm to $R = \Gamma(V)$ and use the finite morphism

$$\varphi : V \longrightarrow K^n \qquad p \longmapsto (a_1(p), \dots, a_n(p)) \qquad \Bigg| \qquad \varphi^* : K[X_1, \dots, X_n] \hookrightarrow \Gamma(V) \qquad X_i \longmapsto a_i$$

$\square$

Exe The projections of $V = \{(x,y) \mid xy = 1\}$ onto the x- or y-axis is dominant, but not surjective!



However, the projection

$$V \longrightarrow K$$
$$(x,y) \longmapsto x+y$$

is surjective:

The preimages of $t \in K$ are the points (x,y) where x is a solution to $x^2 - tx + 1 = 0$ and $y = t - x$.

It's actually a finite morphism.

Pf of Thm 2.75 Let $R = K[b_1, \dots, b_m]$.

$\Rightarrow L = K(b_1, \dots, b_m)$. $\Rightarrow m \geq n$

Induction over m.

$m = n$: done!

$m > n$: $\Rightarrow b_1, \dots, b_m$ are algebraically dependent over K.

Let $0 \neq f \in K[X_1, \dots, X_m]$ with $f(b_1, \dots, b_m) = 0$.

If $f(b_1, \dots, b_{m-1}, X) \in K[b_1, \dots, b_{m-1}][X]$ is monic, then b_m is integral over $K[b_1, \dots, b_{m-1}]$ and we can proceed by induction.

Let $d \geq 1$ be the degree of $f(X_1, \dots, X_m)$.

Consider the polynomial

$$g(X) := f(b_1 + c_1(X - b_m), \dots, b_{m-1} + c_{m-1}(X - b_m), X)$$

$$= f(b_1 - c_1 b_m + c_1 X, \dots, b_{m-1} - c_{m-1} b_m + c_{m-1} X, X)$$

$$\in K[b_1 - c_1 b_m, \dots, b_{m-1} - c_{m-1} b_m][X]$$

for $c_1, \dots, c_{m-1} \in K$.

Note that $g(b_m) = f(b_1, \dots, b_{m-1}, b_m) = 0$.

The degree of $g(X)$ is at most d and its

X^d-coefficient is some nonzero polynomial $h(c_1, \ldots, c_{m-1})$ in $c_1, \ldots, c_{m-1}$ with $h \in K[Y_1, \ldots, Y_{m-1}]$. (Just expand!)

By the Nichtnullstellensatz, there exist $c_1, \ldots, c_{m-1} \in K$ such that $\underset{l:=}{} h(c_1, \ldots, c_{m-1}) \neq 0$.

Then, $\frac{1}{l} \cdot g(X)$ is a monic polynomial with coeff. in $K[b_1 - c_1 b_m, \ldots, b_{m-1} - c_{m-1} b_m]$ which is zero for $X = b_m$.

$\Rightarrow b_m$ is integral over
$$K[b_1 - c_1 b_m, \ldots, b_{m-1} - c_{m-1} b_m].$$

$\Rightarrow$ We can proceed by induction.

$\square$

Nagata's trick In the proof, one could instead use
$$g(X) = f(b_1 + (X - b_m)^{d_1}, \ldots, b_{m-1} + (X - b_m)^{d_{m-1}}, X)$$
for appropriate $d_1, \ldots, d_{m-1} \geq 0$.

2.17. Another definition of dimension

Lemma 2.76 Let $V \subsetneqq W$ be irreducible alg. sets. Then, $\dim(V) \leq \dim(W) - 1$ and there is an irreducible alg. set $V \subseteq A \subsetneqq W$ of dimension $\dim(A) = \dim(W) - 1$.

Rmk. It's important that W is irreducible!
(Otherwise, take $V = \{P\}$, $W = \{P, Q\}$.)

Pf Let $n = \dim(W)$. By Noether Normalization, there is a dominant finite morphism $\varphi: W \to K^n$.

$$V \subsetneqq W \underset{\substack{\uparrow \\ \text{incomparability}}}{\Longrightarrow} \varphi(V) \underset{\substack{\nwarrow \\ \text{closed}}}{\subsetneqq} \varphi(W) = K^n$$

Take $0 \neq f \in K[X_1, \ldots, X_n]$ which vanishes on $\varphi(V)$: $\varphi(V) \subseteq V(f)$.

Since $\varphi(V)$ is irreducible, it is contained in some irreducible component of $V(f)$, which corresponds to some irreducible factor of f.

$\Rightarrow$ We can assume that f is irreducible.

$$\dim(V) \underset{\substack{\uparrow \\ \text{Thm 2.68}}}{=} \dim(\varphi(V)) \leq \dim(V(f)) = n - 1.$$

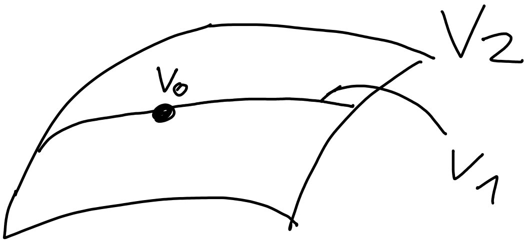
Since $V \subseteq \varphi^{-1}(V(f))$ is irreducible, it is contained in some irreducible component A of $\varphi^{-1}(V(f)) = V(\varphi^*(f))$.

$$\underset{\substack{\uparrow \\ \text{Thm 2.74} \\ \text{(Going down)}}}{\Longrightarrow} \varphi(A) = V(f) \Rightarrow \dim(A) = \underset{\substack{\shortparallel \\ \dim(V(f)) \\ \shortparallel \\ n-1}}{\dim(\varphi(A))}.$$

$\square$

<u>Cor 2.77</u> Let $V \neq \emptyset$ be any algebraic set. Then, $\dim(V)$ is the largest $d \geq 0$ such that there are irreducible alg. sets

$$V_0 \subsetneqq V_1 \subsetneqq \cdots \subsetneqq V_d \subseteq V.$$



<u>Pf</u> <u>$\dim(V) \geq d$:</u>

$0 \leq \dim(V_0) < \dim(V_1) < \ldots < \dim(V_d) \leq \dim(V)$

<u>$\dim(V) \leq d$:</u> W.l.o.g. V is irreducible. Take $V_d = V$.

If $\dim(V) \geq 1$, then $\{P\} \subsetneqq V$ for any $P \in V$.

$\Rightarrow \exists \{P\} \subseteq V_{d-1} \subsetneqq V_d$ of dimension $\dim(V)-1$.

Continue the chain (induction ...) $\square$

Cor 2.78 Let $V \subseteq W$ both be irreducible.

Then, the codimension

$$\operatorname{codim}(V,W) := \dim(W) - \dim(V)$$

of ~~V~~ in W is the largest $c \geq 0$ such that there are irreducible alg. sets

$$V = V_0 \subsetneq \cdots \subsetneq V_c = W.$$

Pf "as before" $\square$

2.18. Defining with few equations

Def An irreducible $(n-1)$-dimensional irreducible subset of K^n is called a hypersurface in K^n.

Thm 2.79 Any hypersurface $V \subseteq K^n$ is of the form $V = V(f)$ for some irreducible $0 \neq f \in K[X_1, \dots, X_n]$.

Pf Since $V \subsetneq K^n$, there exists some irreducible $f \neq 0$ s.t. $\underbrace{V}_{\text{irred.}} \subseteq \underbrace{V(f)}_{\text{irred.}}$.

If $V \subsetneq V(f)$, then $\dim(V) < \dim(V(f)) = n-1$. ↯

$\Rightarrow V = V(f)$. $\square$

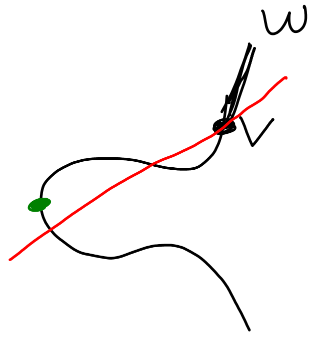
Cor 2.80 Let $V \subseteq W$ both be irreducible. Then, there are $c := \operatorname{codim}(V,W)$ functions $f_1,\dots,f_c \in \Gamma(W)$ such that V is an irreducible component of $V(f_1,\dots,f_c)$ $= \{p \in W \mid f_1(p) = \dots = f_c(p) = 0\} \subseteq W$ and all other irreducible components also have codimension c in W.

⇝ "Essentially, c functions suffice to define an irreducible subset of codimension c."

Rmk Let $K = \mathbb{C}$,

$W = \{(x,y) \mid y^2 = x^3 - 4x + 4\}$ (irred.)

$V = \{(2,2)\}$ or $\{(\pi, \sqrt{\pi^3 - 4\pi + 4})\}$.

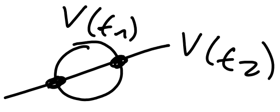


There is no function $f \in \Gamma(W)$ such that $V = V(f)$.

Pf Difficult!

Rmk Assuming $W = K^n$, I don't know whether there are always functions $f_1,\dots,f_c \in K[X_1,\dots,X_n]$ such that $V = V(f_1,\dots,f_c)$!

(Problem: Even if $f_1,\dots,f_c$ are irreducible, $V(f_1,\dots,f_c)$ might not be!



)

Pf of Cor 2.80

Induction over $c = \operatorname{codim}(V, W)$.

Let $c \geq 1$.

Let $\varphi : W \longrightarrow K^n$ be a dominant finite morphism with $n = \dim(W)$.

$\Rightarrow \operatorname{codim}(\varphi(V), K^n) = \operatorname{codim}(V, W) = c$.

Let $0 \neq g_1 \in K[X_1, \dots, X_n]$ be irreducible $\varphi(V) \subseteq V(g_1) \subsetneq K^n$.

$\Rightarrow \operatorname{codim}(\varphi(V), V(g_1)) = c - 1$.

By induction, there are $g_2, \dots, g_c \in K[X_1, \dots, X_n]$ such that $\varphi(V)$ is an irred. comp. of $V(g_1, \dots, g_c)$ and all other irred. comp. also have codimension c in K^n. The preimage $\varphi^{-1}(V(g_1, \dots, g_c)) = V(\underbrace{\varphi^*(g_1)}_{f_1}, \dots, \underbrace{\varphi^*(g_c)}_{f_c})$ has irreducible components of codimension c.

$V \subseteq \varphi^{-1}(V(g_1, \dots, g_c))$ is irreducible and hence contained in some irred. comp. Since dimensions match, V is actually equal to this component! $\square$

2.19. Subsets defined by few equations

Lemma 2.81 Let S be a module-finite ring extension of R and assume that S, R are integral domains with fields of fractions L, K (K not necessarily alg. closed).

Let $\overset{0}{\overset{\neq}{a}} \in S$ and $b := \mathrm{Nm}_{L|K}(a) \in K$, where the norm map $\mathrm{Nm}_{L|K} : L \longrightarrow K$ sends $a \in L$ to the determinant of the K-linear map $L \longrightarrow L$ sending x to ax. Assume that R is integrally closed in K.

$$\begin{tikzcd} S \arrow[r, phantom, "\subseteq"] \arrow[d, dash] & L \arrow[d, dash] \\ R \arrow[r, phantom, "\subseteq"] & K \end{tikzcd}$$

Then, $b \in R$ and

$a | b$ in S.

Pf later ...

(If $L|K$ is Galois, then $\mathrm{Nm}_{L|K}(a) = \prod_{\sigma \in \mathrm{Gal}(L|K)} \sigma(a)$.)

Thm 2.82 (Krull's principal ideal theorem)

Let W be an irreducible alg. set and V be an irred. subset of $V(f) \subseteq W$ for $0 \neq f \in \Gamma(W)$. Then, $\operatorname{codim}(V, W) = 1$ (so $\dim(V) = \dim(W) - 1$).

Pf Let $\varphi : W \longrightarrow K^n$ be a dominant finite morphism.

Goal: Find $0 \neq g \in K[X_1, \dots, X_n]$ s.t.

$$\varphi(V(f)) = V(g).$$

Then, $\dim(V) = \dim(\varphi(V(f))) = \dim(V(g))$
$= n - 1.$

Consider the field ext. $K(W) \mid \varphi^*(K(X_1, \dots, X_n))$.

We get a norm map

$$\mathrm{Nm} : K(W) \longrightarrow \varphi^*(K(X_1, \dots, X_n)) \cong K(X_1, \dots, X_n).$$

Let $0 \neq g = \mathrm{Nm}(f) \in K(X_1, \dots, X_n)$.

Then, g is integral over $K[X_1, \dots, X_n]$, so in fact $g \in K[X_1, \dots, X_n]$ (because $K[X_1, \dots, X_n]$ is integrally closed in $K(X_1, \dots, X_n)$ by Thm 2.15.)

Furthermore $\varphi^*(g) \mid f$ in $\Gamma(W)$, so

$V(f) \subseteq V(\varphi^*(g))$ and therefore $V(f) \subseteq V(\varphi^*(g))$,

so $\varphi(V(f)) \subseteq \varphi(\underbrace{V(\varphi^*(g))}_{\varphi^{-1}(V(g))}) \subseteq V(g)$.

Since $\varphi(V(f)) \subseteq V(g)$ is an algebraic set, if $\varphi(V(f)) \subsetneq V(g)$, there would exist some $h \in K[X_1, \dots, X_n]$ with $h|_{\varphi(V(f))} = 0$ but $h|_{V(g)} \neq 0$.

$$\swarrow$$

$$\varphi^*(h)|_{V(f)} = 0$$

$$\Downarrow \text{ Nullstellensatz}$$

$$\varphi^*(h)^m \in (f) \subseteq \Gamma(W) \quad \text{for some } m \geq 1$$

$$\Updownarrow$$

$$\varphi^*(h)^m = fe \text{ for some } e \in \Gamma(W)$$

$$\Downarrow$$

$$\underset{\substack{\| \\ h^{m\cdot[L:K]}}}{\mathrm{Nm}(\varphi^*(h)^m)} = \mathrm{Nm}(fe) = \underbrace{\mathrm{Nm}(f)}_{g}\,\underbrace{\mathrm{Nm}(e)}_{\substack{\in K[X_1, \dots, X_n] \\ \text{as before}}}$$

$$\Downarrow$$

$$h^{m\cdot[L:K]} \in (g) \subseteq K[X_1, \dots, X_n]$$

$$\Downarrow$$

$$V(g) \subseteq V(h)$$

$$\Downarrow$$

$$h|_{V(g)} = 0 \quad \lightning$$

$\square$

Thm 2.83 Let W be an irred. alg. set and let V be an irreducible component of $V(f_1, \dots, f_r) \subseteq W$ for some $f_1, \dots, f_r \in \Gamma(W)$. Then, $\mathrm{codim}(V, W) \leq r$.

Pf Let V_1 be an irred. comp. of $V(f_1)$ containing V.

$$\Rightarrow \dim(V_1) \geq \dim(W) - 1.$$

Let V_2 be an irred. comp. of $V_1 \cap V(f_2)$ containing V.

$$\Rightarrow \dim(V_2) \geq \dim(V_1) - 1 \geq \dim(W) - 2.$$

$\vdots$

Let V_r — " — $V_{r-1} \cap V(f_r)$ containing V.

$\subseteq V(f_1, \dots, f_r)$

$$\underset{\substack{\uparrow \\ V \subseteq V_r \subseteq V(f_1, \dots, f_r) \text{ irred. comp.}}}{\Rightarrow} V = V_r, \quad \dim(V_r) \leq \dim(W) - r.$$

$\square$

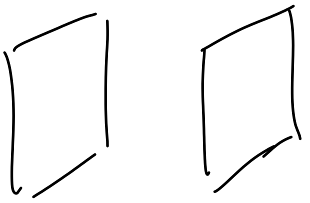
Rmk Even if $f_1, \dots, f_r \neq 0$ we might have $\mathrm{codim}(V, W) < r$ if $f_i|_{V_{i-1}} = 0$.

(E.g. if $f_1 = \dots = f_r$.)

Question (Matty) If $f_1, \dots, f_r$ are alg. indep. over K, is $\mathrm{codim}(V, W) = r$? No! Take $f_1 = x$, $f_2 = xy$.

Rmk $V(f_1, \dots, f_r)$ could be empty, even if $r < \dim(W)$.

E.g. $\emptyset = V(X, X-1) \subseteq K^3$.



Rmk The Thm would fail for fields K that are not algebraically closed:

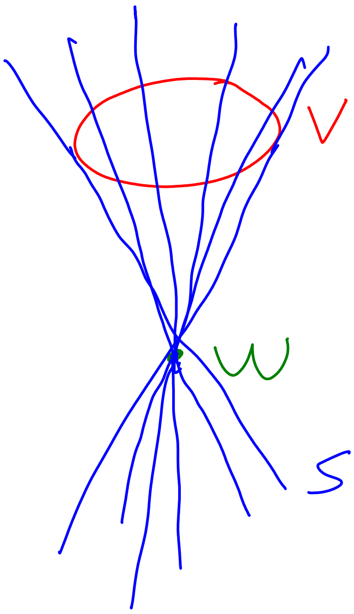
$\{(0,0)\} = V(x^2+y^2) \subseteq \mathbb{R}^2$.

2.20. Applications of dimensions, part 1

Thm 2.84 Let $V, W \subseteq K^n$ be irreducible of dimensions a, b and $S \subseteq K^n$ be the union of all straight lines $L \subseteq K^n$ joining a point $P \in V$ and a point $Q \in W$ with $P \neq Q$. (The set S is called the join of V, W.)

If $n \geq a+b+2$, then $S \subsetneqq K^n$.

Exe $a=1, b=0, n=3$



Pf Consider the morphism

$$\varphi : V \times W \times K \longrightarrow K^n$$
$$(P, Q, t) \longmapsto \underbrace{tP + (1-t)Q}_{\text{parametrization of the line } PQ}$$

Its image contains S. (actually, the image is S, unless $V=W=\{P\}$, in which case $S=\emptyset$...)

$\Rightarrow$ By Lemma 2.64,

$$\dim(S) \le \dim(\overline{\varphi(V\times W\times K)}) \le \dim(V\times W\times K)$$
$$= \dim(V) + \dim(W) + \dim(K)$$
$$= a+b+1 < n.$$

$\Rightarrow S \neq K^n$. $\square$

Thm 2.85 For any m points $P_1,\dots,P_m \in K^n$, if $m < \binom{d+n}{n}$, there is a polynomial $0 \neq f \in K[X_1,\dots,X_n]$ of degree $\leq d$ with $P_1,\dots,P_m \in V(f)$.

Ex $d = n = 2$, $m = 5$

$\Rightarrow \exists$ conic (or line) through any 5 points in K^2.

Pf Let F_d be the vector space of polynomials of degree $\leq d$.

Goal: $\exists\, 0 \neq f \in$ kernel of $F_d \subseteq \Gamma(K^n) \to \Gamma(\{P_1,\dots,P_m\})$

$$f \mapsto f|_{\{P_1,\dots,P_m\}}$$

$$\dim_K(F_d) = \#\text{ monomials of degree} \leq d$$

$$= \{(e_1,\dots,e_n) \mid e_1,\dots,e_n \geq 0,\ e_1+\dots+e_n \leq d\}$$

$$\underset{\uparrow}{=} \binom{d+n}{n}$$

$$\underbrace{0 \dots 0}_{e_1} \mid \underbrace{0 \dots 0}_{e_2} \mid \dots \mid \underbrace{0 \dots 0}_{e_n} \mid \underbrace{0 \dots 0}_{d-(e_1+\dots+e_n)}$$

In total: d 0's, n 1's

$$\dim_K(\Gamma(\{P_1,\dots,P_m\})) = m.$$

$\square$

Thm 2.86 For any points $P_1, \dots, P_m \in K^2$, there is an irreducible polynomial $0 \neq f \in K[X,Y]$ of degree $\leq m+2$ with $P_1, \dots, P_m \in V(f)$.

Pf The kernel T of $F_{m+2} \longrightarrow \Gamma(\{P_1, \dots, P_m\})$

has dimension $\dim(T) \geq \binom{m+4}{2} - m$.

Let $F_d' \subseteq F_d$ be the (algebraic!) set of pol. where at least one coeff. is 1.

Any reducible pol. $f \in F_{m+2}$ can be written as $f = gh$ with $g \in F_a$, $h \in F_b'$ where $a, b \geq 1$ with $a+b = m+2$.

The Zariski closure of the image of

$$\begin{aligned} \varphi_{a,b} : F_a \times F_b' &\longrightarrow F_{m+2} \\ (g,h) &\longmapsto gh \end{aligned}$$

has dimension ~~dim~~ $\left(\overline{\operatorname{im}(\varphi_{a,b})}\right) \leq \dim(F_a \times F_b')$

$$= \binom{a+2}{2} + \binom{b+2}{2} - 1$$

$$\Rightarrow \dim\Big(\bigcup_{\substack{a,b\geq 1:\\ a+b=m+2}} \overline{\operatorname{im}(\varphi_{a,b})}\Big)$$

$$= \max_{\substack{a,b\geq 1:\\ a+b=m+2}} \underbrace{\dim\big(\overline{\operatorname{im}(\varphi_{a,b})}\big)}_{\leq \binom{a+2}{2}+\binom{b+2}{2}-1}$$

$$= \ldots = \frac{(m+5)(m+2)}{2} - ab + 1$$

$$\leq \frac{(m+5)(m+2)}{2} - (m+1) + 1$$

$$= \binom{m+3}{2} + 2$$

But $\binom{m+4}{2} - m - \binom{m+3}{2} - 2 = \binom{m+3}{1} - m - 2 = 1 > 0.$

$$\Rightarrow T \notin \bigcup_{a,b} \operatorname{im}(\varphi_{a,b})$$

$$\Rightarrow \exists\ f \in T \setminus \bigcup \operatorname{im}(\varphi_{a,b}) \qquad \square$$

Rmk There's room for improvement! If $f=gh$ with $P_1,\ldots,P_m \in V(f)$, then $P_1,\ldots,P_m \in V(g)\cup V(h)$, so we could fix a subset $S \subseteq \{P_1,\ldots,P_m\}$ and consider only g,h with $S \subseteq V(g)$, $\{P_1,\ldots,P_m\}\setminus S \subseteq V(h)$ (and take $\bigcup_{a,b,S} \ldots$). ($\rightsquigarrow$ smaller dimension)

Rmk For any $m \geq 2$, there are points $P_1, \dots, P_m \in K^2$ s.t. there is no irreducible $0 \neq f \in K[X,Y]$ of degree $\leq m-2$ with $P_1, \dots, P_m \in V(f)$.

Pf Take $P_1, \dots, P_{m-1}$ on x-axis, P_m not on the x-axis.

The restriction $f(X,0)$ of f to the x-axis is a pol. of degree $\leq m-2$ with $\geq m-1$ roots. $\Rightarrow$ It's the zero polynomial.

$\Rightarrow f = Y \cdot g$ for some pol. g.

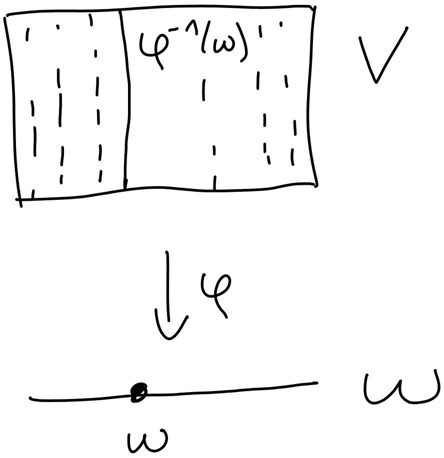
But $g \neq$ const. because $f(P_m) = 0$.

$\Rightarrow f$ is reducible.

$\square$

2.21. Dimensions of fibers

Def A *fiber* of $\varphi : V \to W$ is the preimage $\varphi^{-1}(w)$ of a point $w \in W$.



Thm 2.87 Let V, W be irreducible, $\varphi : V \to W$ a morphism, and A an irreducible component of $\varphi^{-1}(w)$ for some point $w \in W$. Then,

$$\operatorname{codim}(A, V) \leq \dim(W).$$

$$(\dim(A) \geq \dim(V) - \dim(W).)$$

In particular,

$\dim(\varphi^{-1}(w)) \geq \dim(V) - \dim(W)$ for every $w \in \varphi(V)$.

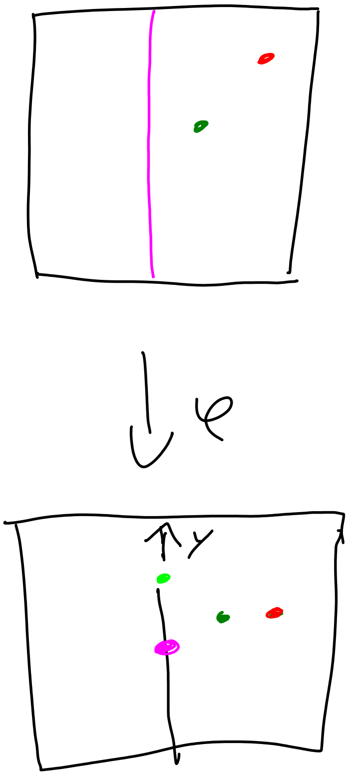
Ex $\varphi : K^2 \longrightarrow K^2$

$$(x,y) \longmapsto (x, xy)$$

🟦🟥 $\varphi^{-1}(a,b) = \left\{\left(a, \frac{b}{a}\right)\right\}$ if $a \neq 0$

🟩 $\varphi^{-1}(0,b) = \emptyset$ if $b \neq 0$

🟪 $\varphi^{-1}(0,0) = \{(0,y) \mid y \in K\}$



We'll actually prove something more general:

Thm 2.88 Let V, W, φ as above, $B \subseteq W$ irreducible, and A an irreducible component of $\varphi^{-1}(B)$ with $\overline{\varphi(A)} = B$. Then, $\operatorname{codim}(A, V) \leq \operatorname{codim}(B, W)$.

Rmk If $B = \{w\}$, then automatically $\varphi(A) = \{w\}$.

Rmk The condition $\overline{\varphi(A)} = B$ can't be omitted.
(Look at the example just before the def. of normal alg. sets.)

Pf Let $n = \operatorname{codim}(B, W)$.

By Cor. 2.80, there are functions $g_1, \dots, g_n \in \Gamma(W)$ s.t. B is an irred. comp. of $V(g_1, \dots, g_n) \subseteq W$.

$$\Rightarrow \underset{\substack{\uparrow \\ \text{irred.}}}{A} \subseteq \varphi^{-1}(B) \subseteq \varphi^{-1}(V(g_1, \dots, g_n)) = V(\underbrace{\varphi^*(g_1)}_{\overset{\shortparallel}{f_1}}, \dots, \underbrace{\varphi^*(g_n)}_{\overset{\shortparallel}{f_n}})$$

$\Rightarrow$ A is contained in some irred. comp. A' of $V(f_1, \dots, f_n)$

$$\Rightarrow \underset{\substack{\uparrow \\ \text{irred.} \\ \text{comp. of} \\ V(g_1, \dots, g_n)}}{B} = \overline{\varphi(A)} \subseteq \underset{\substack{\uparrow \\ \text{irred.}}}{\overline{\varphi(A')}} \subseteq V(g_1, \dots, g_n)$$

$$\Rightarrow B = \overline{\varphi(A')}$$

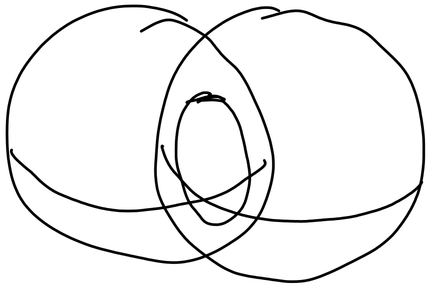
$$\Rightarrow \underset{\substack{\uparrow \\ \text{irred.} \\ \text{comp. of} \\ \varphi^{-1}(B)}}{A} \subseteq \underset{\substack{\uparrow \\ \text{irred.}}}{A'} \subseteq \varphi^{-1}(B)$$

$\Rightarrow A = A'$, which is an irred. comp. of $V(f_1, \dots, f_n)$

Thm 2.83 $\Rightarrow \operatorname{codim}(A, V) \le n$. □

Cor 2.89 Let $V_1, V_2 \subseteq W$ all be irred. and let A be an irred. comp. of $V_1 \cap V_2$.

Then, $\text{codim}(A, W) \leq \text{codim}(V_1, W) + \text{codim}(V_2, W)$.



Pf Consider the inclusion morphism

$$\varphi : V_1 \longrightarrow W.$$

We have $\varphi^{-1}(V_2) = V_1 \cap V_2$.

$$\Rightarrow \underset{\substack{\parallel \\ \text{codim}(A, W) - \text{codim}(V_1, W)}}{\text{codim}(A, V_1)} \leq \text{codim}(V_2, W)$$

$\square$

If φ is dominant, we have equality for a "generic" fiber.

Prop 2.90 Let V, W, φ as above and assume φ is dominant. Then, there is an open $\emptyset \neq U \subseteq W$ contained in $\varphi(V)$ and such that every irred. comp. A of every fiber $\varphi^{-1}(w)$ with $w \in U$ satisfies $\text{codim}(A, V) = \dim(W)$.

We won't prove this.

2.22. Applications of dimension, part 2

We obtain a "converse" of Thm 2.85:

<u>Thm 2.91</u> For any $n, d \geq 1$ and $m \geq \binom{d+n}{n}$,

then there are m points $P_1, \dots, P_m \in K^n$ such that there is no nonzero polynomial $0 \neq f \in K[X_1, \dots, X_n]$ of degree $\leq d$ with $P_1, \dots, P_m \in V(f)$.

<u>Pf</u> Let F_d' be the set of pol. of degree $\leq d$ where at least one coeff. is 1.

$\dim(F_d') = \binom{d+n}{n} - 1$

Consider the following algebraic subset A of $K^n \times \dots \times K^n \times F_d'$:

$$A = \{(P_1, \dots, P_m, f) \mid f(P_1) = \dots = f(P_m) = 0\}$$

~~For~~ an irred. comp. A' of A, consider the projection $\pi : A' \longrightarrow F_d'$. Its image is contained in the irred. set $\overline{\pi(A')}$. We'll apply Thm 2.87 to $\pi : A' \longrightarrow \overline{\pi(A')}$. Pick any $f \in \pi(A')$. Its preimage is

$$\pi^{-1}(f) = \underbrace{V(f) \times \dots \times V(f)}_{m} \times \{f\}.$$

$$\Rightarrow \dim(\pi^{-1}(f)) = m \cdot \dim(V(f))$$

$$\underset{\substack{\uparrow \\ f \neq 0}}{=} m \cdot (n-1)$$

On the other hand, by Thm 2,87,

$$\dim(\pi^{-1}(f)) \geq \dim(A') - \dim(\pi(A'))$$

$$\geq \dim(A') - \dim(F_d')$$

$$= \dim(A') - \left(\binom{d+n}{n} - 1\right).$$

$$\Rightarrow \dim(A') \leq m(n-1) + \binom{d+n}{n} - 1$$

$$\underset{\substack{\uparrow \\ m \geq \binom{d+n}{n}}}{\leq} mn - 1.$$

Since this holds for every irred. comp. A' of A, $\dim(A) \leq mn-1$.

$\Rightarrow$ The projection $A \longrightarrow \underbrace{K^n \times \dots \times K^n}_{m}$ is not surjective.

$\Rightarrow$ There are points $P_1, \dots, P_m \in K^n$ such that there is no $f \in F_d'$ with

$$f(P_1) = \dots = f(P_m) = 0.$$

$\square$

2.23. Some promised proofs

Pf of Lemma 2.81

Let $f \in R[X]$ be a monic pol. with $f(a)=0$ and let $g \in K[X]$ be the min. polynomial of a.

$\Rightarrow g \mid f$

$\Rightarrow$ Every root of g in $\overline{K}$ is a root of f and therefore integral over R.

Write $g(X) = \prod\limits_i (X - \underbrace{a_i}_{\in \overline{K}}) = X^n + c_{n-1}X^{n-1} + \dots + c_0$.

every coeff. $c_i \in K$ is $\pm$ a sum of products of roots, and therefore integral over R. Since R is integrally closed in K, this means that $c_i \in R$.

$$\Rightarrow b = \mathrm{Nm}_{L|K}(a) = \mathrm{Nm}_{K(a)|K}(\mathrm{Nm}_{L|K(a)}(a))$$

$$= \mathrm{Nm}_{K(a)|K}\left(a^{[L:K(a)]}\right) = \mathrm{Nm}_{K(a)|K}(a)^{[L:K(a)]}$$

$$= (\pm c_0)^{[L:K(a)]} \in R.$$

Furthermore, $0 = g(a) = a^n + c_{n-1}a^{n-1} + \dots + c_0$, so

$$a(\underbrace{a^{n-1} + \underbrace{c_{n-1}}_{\in R} a^{n-2} + \dots + \underbrace{c_1}_{\in R}}_{S \ni}) = -c_0 \in R \Rightarrow a \mid c_0 \mid b \text{ in } S.$$

$\square$

Pf of Thm 2.74 (Going down)

φ^* gives an inclusion $\Gamma(W) \hookrightarrow \Gamma(V)$ and
an inclusion $K(W) \hookrightarrow K(V)$.

W normal: $\Gamma(W)$ is integrally closed in $K(W)$.

φ finite: $\Gamma(V)$ is a module-finite ring ext. of $\Gamma(W)$
$K(V)$ is a finite field ext. of $K(W)$.

Let L be the normal closure of this field ext.
It's a finite field ext. of $K(W)$.

$$\begin{tikzcd}
L & \supseteq & S=\Gamma(V') & V' \arrow[d, "\psi"] & A'_1\cup\cdots\cup A'_s \arrow[d] \\
K(V) \arrow[u, dash] & \supseteq & \Gamma(V) \arrow[u, dash] & V \arrow[d, "\varphi"] & A_1\cup\cdots\cup A_r \arrow[d] \\
K(W) \arrow[u, dash] & \supseteq & \Gamma(W) \arrow[u, dash] & W & B
\end{tikzcd}$$

Let S be the integral closure of $\Gamma(W)$ in L.
Since $\Gamma(V)$ is an integral ext. of $\Gamma(W)$, we have $\Gamma(V) \subseteq S$.

We have $S \cap K(W) = \Gamma(W)$ because $\Gamma(W)$ is integrally closed in $K(W)$.

S is a module-finite ring ext. of $\Gamma(W)$ because it is integral and L is a finite field ext of $K(W)$.

$\Gamma(W) = K[x_1, \dots]/\dots$ is a finitely generated ring ext. of K.

$\Rightarrow$ S is a finitely generated ring ext. of K

$$\begin{matrix} S \\ \parallel \\ K[y_1, \dots]/\dots \end{matrix}$$

$\Rightarrow$ S corresponds to an irreducible algebraic set V' with $\Gamma(V') = S$.

$\Gamma(V') = S$ is an integral mod.-fin. ext. of $\Gamma(W)$ and therefore also $\Gamma(V)$.

The inclusion $\Gamma(V) \subseteq \Gamma(V')$ corresponds to a dominant finite morphism $\psi : V' \to V$.

Decompose $(\varphi \circ \psi)^{-1}(B)$ into irreducible components: $(\varphi \circ \psi)^{-1}(B) = A'_1 \cup \dots \cup A'_s$.

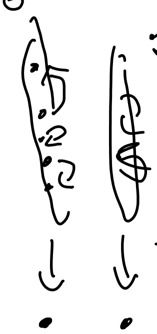
Claim Any A_i contains $\psi(A'_j)$ for some j.

Pf W.l.o.g. $i = 1$. Let $P \in A_1 \setminus (A_2 \cup \dots \cup A_r)$ (exists because $A_1 \not\subseteq A_2 \cup \dots \cup A_r$).
Since ψ is dom. + fin., it's surjective.
Let $P' \in \psi^{-1}(P)$. Let $P \in A'_j$.
$\psi(A'_j)$ is an irred. subset of $\varphi^{-1}(B) = A_1 \cup \dots \cup A_r$.
$\Rightarrow P \in \psi(A'_j) \subseteq A_i$ for some $i \underset{\substack{\uparrow \\ P \notin A_2, \dots, A_r}}{\Rightarrow} i = 1 \Rightarrow \psi(A'_j) \subseteq A_1$ $\square$

$\Rightarrow$ It suffices to show that $\varphi(\psi(A_j))=B$ for all j.

$\Rightarrow$ We can assume w.l.o.g. that $K(V)$ is a normal field ext. of $K(W)$ and $V'=V$, $L=K(V)$, $S=\Gamma(V)$.

$$\begin{tikzcd}
V \arrow[loop right, "\alpha_\sigma"] \arrow[d, "\varphi"'] \\
W
\end{tikzcd}$$



Let $G = \mathrm{Gal}(K(V)|K(W))$ be the group of automorphisms of $K(V)$ fixing every element of $K(W)$.

Note: If $a\in K(V)$ satisfies a monic polynomial equation with coefficients in $\Gamma(W)$, then $\sigma(a)\in K(V)$ satisfies the same equation for any $\sigma\in G$

$\Rightarrow$ $\sigma(\Gamma(V))\subseteq\Gamma(V)$ $\forall\sigma\in G$.

$\Rightarrow$ The automorphism σ of $K(V)$ restricts to a ring automorphism of $\Gamma(V)$ fixing every element of $\Gamma(W)$.

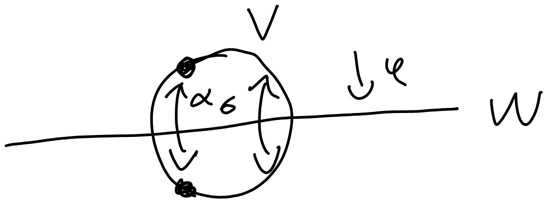
The hom. $\sigma:\Gamma(V)\longrightarrow\Gamma(V)$ corresponds to a morphism $\alpha_\sigma: V\longrightarrow V$ (with $\alpha_\sigma^*=\sigma$).

Since σ fixes $\Gamma(W)$, we have comm. diagrams

$$\begin{tikzcd}
 & \Gamma(V) \arrow[dd, "\sigma"] \\
\Gamma(W) \arrow[ur, hook] \arrow[dr, hook] & \\
 & \Gamma(V)
\end{tikzcd}
\qquad
\begin{tikzcd}
 & V \arrow[dl, "\varphi"'] \\
W & \\
 & V \arrow[ul, "\varphi"] \arrow[uu, "\alpha_\sigma"']
\end{tikzcd}$$

($\rightsquigarrow$ "deck transformation")

Ex Say $K = \mathbb{C}$, $V = \{(x,y) \in \mathbb{C}^2 \mid x^2+y^2=1\}$, $W = K$, $\varphi(x,y) = x$.



$\Gamma(W) = K[x]$, $\Gamma(V) = K[x,y]/(x^2+y^2-1) = K[x][\underbrace{\sqrt{1-x^2}}_{y}]$

$K(W) = K(x)$, $K(V) = \quad \dots = K(x)(\sqrt{1-x^2})$

$K(V)$ is a Galois ext. of $K(W)$ with Galois group $\{id, \sigma\}$ where $\sigma(\underbrace{\sqrt{1-x^2}}_{y}) = \underbrace{-\sqrt{1-x^2}}_{-y}$

corresponds to the reflection of V across the x-axis.

Then, $\alpha_\sigma(\varphi^{-1}(B)) = \varphi^{-1}(B)$, so α_σ permutes the irreducible components $A_1, \dots, A_r$ of $\varphi^{-1}(B)$.

Claim G acts transitively on the set of irred. components.

Pf Assume w.l.o.g. $A_1, \dots, A_l$ lie in different G orbits than $A_{l+1}, \dots, A_r$.

Pick points $P_1 \in A_1, \dots, P_l \in A_l$ with $P_1, \dots, P_l \notin A_{l+1}$. By the Chinese remainder theorem, since $\{P_1\}, \dots, \{P_l\}, A_{l+1}$ are pairwise disjoint, there is a function

$f \in \Gamma(V)$ with $f(P_1) = \dots = f(P_l) = 1$ and

$f|_{A_{l+1}} = 0$.

$f(P_i) = 1 \Rightarrow f|_{A_i} \neq 0$ for $i = 1, \dots, l$.

We have

$$g := \mathrm{Nm}_{K(V)|K(W)}(f) = \Big(\prod_{\sigma \in G} \sigma(f)\Big)^t,$$

where $t \geq 1$ is the degree of inseparability of $K(V)|K(W)$.

$$g \in \Gamma(V) \cap K(W) \underset{\uparrow}{=} \Gamma(W)$$

$\boxed{\Gamma(W) \text{ int. closed in } K(W)}$

(I) $g|_{A_j} = \big(\prod \sigma(f)\big)\big|_{A_j} \neq 0$ because $\Gamma(A_j)$ is an integral domain and $f|_{A_1}, \dots, f|_{A_l} \neq 0$ and α_σ permutes just $A_1, \dots, A_l$.

On the other hand,

$$g|_{A_{l+1}} = \big(\underbrace{\prod \sigma(f)}_{f \cdot \dots}\big)\big|_{A_{l+1}} = 0.$$

Since g is (the composition with φ of) a function on W, we have

$$g|_{\varphi(A_{c+1})} = 0 .$$

W.l.o.g. $\varphi(A_{c+1}) = B$ by Lemma 2.73.

$\Rightarrow g|_B = 0$

On the other hand, $\boxed{I}$ says that

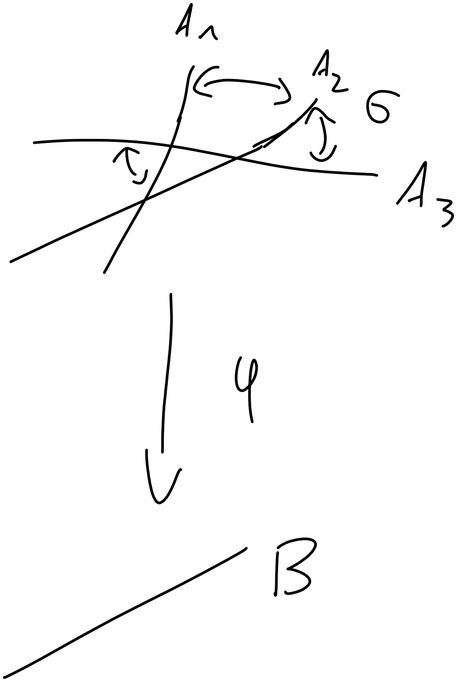
$$g|_{\underbrace{\varphi(A_i)}_{\subseteq B}} \neq 0 \quad \text{for } i = 1, \dots, c . \quad ↯$$

$\square$

G acts transitively on the irred. comp. $A_1, \dots, A_r$ of $\varphi^{-1}(B)$ and $\varphi(A_i) = B$ for some i. If $\alpha_\sigma(A_i) = A_j$, then

$$\varphi(A_j) = \varphi(\alpha_\sigma(A_i)) = \varphi(A_i) = B .$$

$\square$

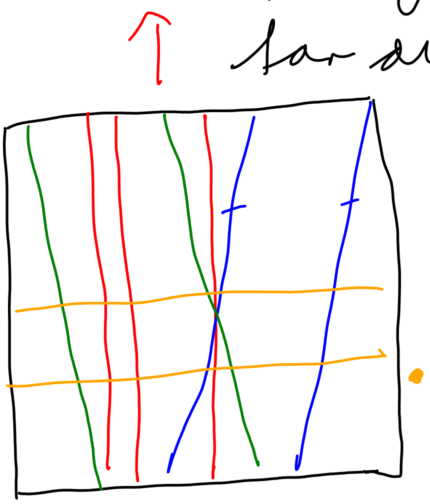


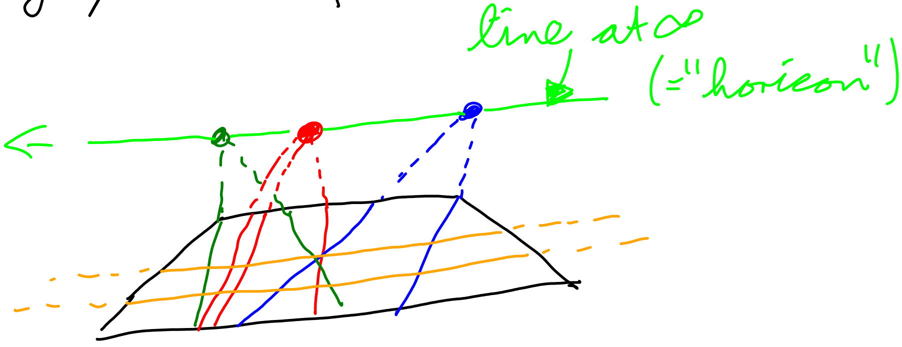
3. Projective varieties

3.1 Projective space

Two lines $L_1 \neq L_2$ in $\mathbb{R}^2$ intersect in exactly one point except if they are parallel.

Idea: Pretend they intersect in a point at infinity by adding one infinitely far away point for each direction.



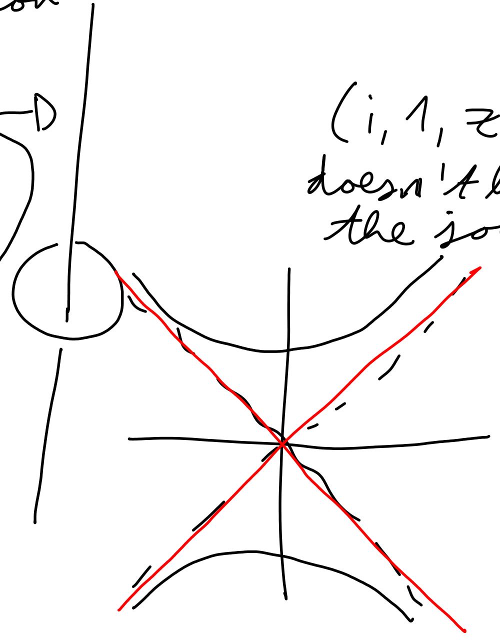


↳ Any line goes through one point at ∞ (corr. to its direction).

Matty's question on the double-bonus problem:

works for $\mathbb{R}^3$ but not for $\mathbb{C}^3$!

$(i, 1, z)$ doesn't lie in the join :(



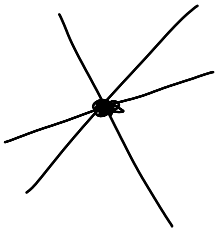
$$x^2+y^2=1$$

$$x' = ix$$
$$y' = y$$

$$-x'^2+y'^2=1$$
$$\|$$
$$(y'-x')(x'+y')$$

In this section, K can be any field (not necc. alg. closed).

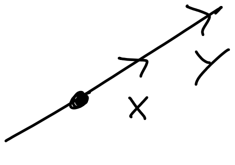
Def The n-dimensional projective space $\mathbb{P}^n_K$ over K is the set of lines in K^{n+1} through the origin. We call the elements of $\mathbb{P}^n_K$ the points in $\mathbb{P}^n_K$.



We denote the line spanned by $(0,\dots,0)\in(x_0,\dots,x_n)\in K^{n+1}$ by $[x_0:\dots:x_n]\in\mathbb{P}^n_K$.

Note $[x_0:\dots:x_n]=[y_0:\dots:y_n]$ if and only if $(x_0,\dots,x_n),(y_0,\dots,y_n)\in K^{n+1}$ are colinear, i.e.

$$(x_0,\dots,x_n)=\lambda(y_0,\dots,y_n) \text{ for some } \lambda\in K^\times.$$



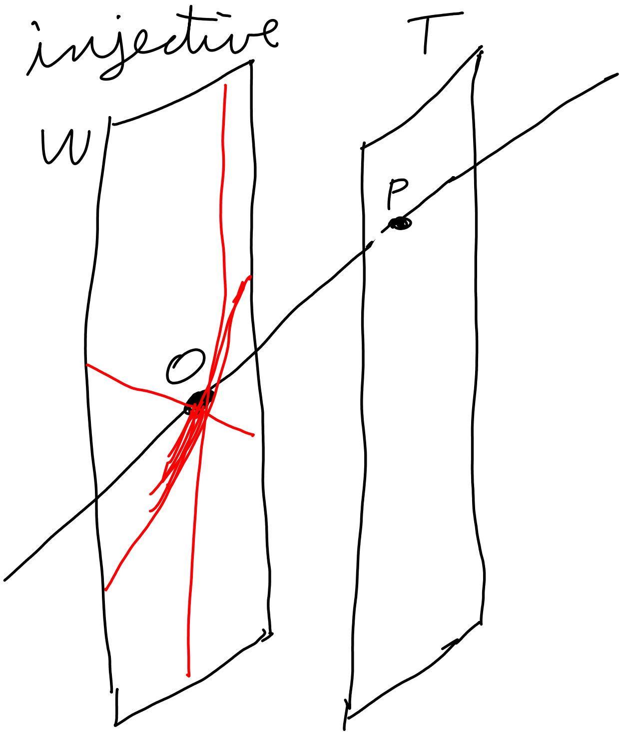
$x_0,\dots,x_n$ are called projective coordinates of the point $[x_0:\dots:x_n]\in\mathbb{P}^n_K$.

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



$$T \hookrightarrow \mathbb{P}^n_K$$
$P \longmapsto$ 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 <u>affine patch</u> 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>

$$\varphi_i : K^n \hookrightarrow \mathbb{P}^n_K$$

$$(x_0, \dots, x_{i-1}, x_{i+1}, \dots, x_n) \longmapsto [x_0 : \dots : x_{i-1} : 1 : x_{i+1} : \dots : x_n]$$

$$\left(\frac{x_0}{x_i}, \dots, \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, \dots, \frac{x_n}{x_i} \right) \longmapsto [x_0 : \dots : x_n]$$

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

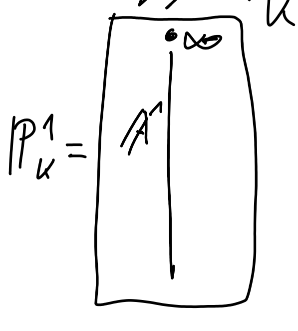
the n-dimensional linear subspace W of K^{n+1} parallel to T.

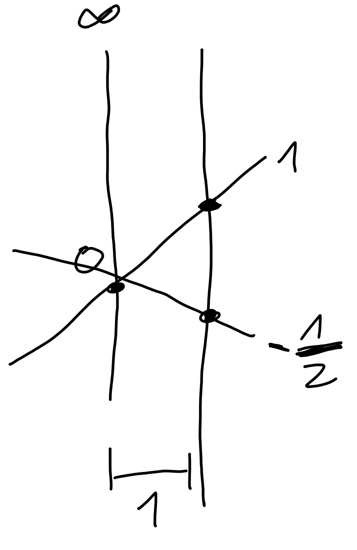
$\Rightarrow$ Identifying W with K^n, we obtain a bijection $\mathbb{P}^n_K \setminus \underbrace{U}_{\mathbb{A}^n_K} \cong (\text{lines through } 0 \text{ in } K^n) \cong \mathbb{P}^{n-1}_K$

$$\leadsto \mathbb{P}^n_K = \mathbb{A}^n_K \sqcup \underbrace{\mathbb{P}^{n-1}_K}_{\text{"set of points at } \infty\text{"}}$$

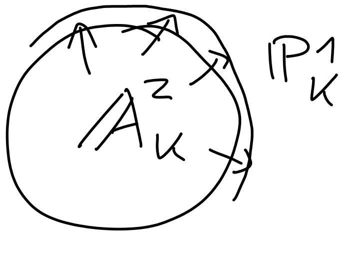
Ex $\mathbb{P}^0_K = \{\text{lines through } 0 \text{ in } K^1\} = \{\underset{\substack{\uparrow \\ \text{single pt.}}}{*}\}$

$$\mathbb{P}^1_K = \mathbb{A}^1_K \sqcup \{\infty\}$$





$$\mathbb{P}^2_K = \mathbb{A}^2_K \sqcup \underbrace{\mathbb{P}^1_K}_{\text{pts at } \infty}$$

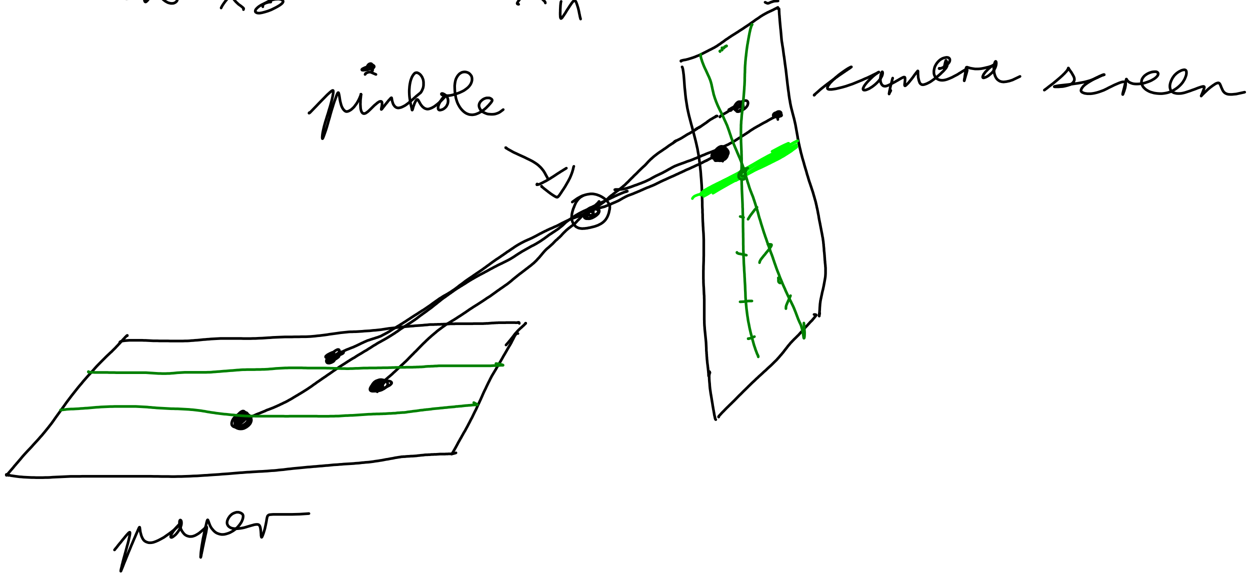


Rmk The standard affine patches $U_0, \dots, U_n$ cover $\mathbb{P}^n_k$: $\mathbb{P}^n_k = \bigcup_{i=0}^{n} U_i$.

Pf $U_i = \{[x_0 : \dots : x_n] \mid x_i \neq 0\}$.

$\Rightarrow \bigcup_{i=0}^{n} U_i = \{[x_0 : \dots : x_n] \mid x_i \neq 0 \text{ for some } i\}$

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 linear subspace 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 *lines* in $\mathbb{P}^n_K$.

Ex 2 *planes*

Ex $(n-1)$ *hyperplanes*

($\mathbb{P}^n_K \setminus U$ as above is a hyperplane in $\mathbb{P}^n_K$.)

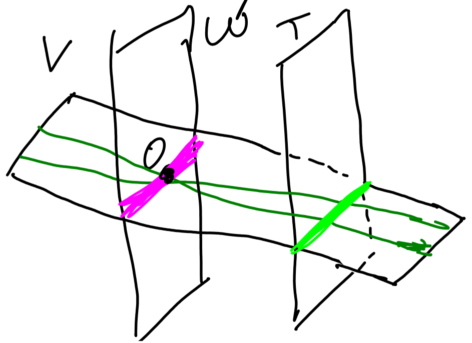
Ex (-1)-dim. lin. subsp. $= \emptyset$.

Lemma 3.1.1 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, *either*

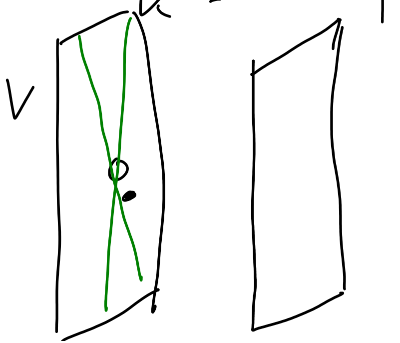
a) $\varphi^{-1}(L) \subseteq K^n$ is an affine d-dimensional linear subspace and $L \cap (\mathbb{P}^n_K \setminus U)$ is a $(d-1)$-dimensional linear subspace of $\mathbb{P}^n_K \setminus U \cong \mathbb{P}^{n-1}_K$.

or 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 $W \subset K^{n+1}$ be the n-dim. lin. subsp. of K^{n+1} parallel to the affine lin. subsp. $T \subset K^{n+1}$ defining the affine chart.

If $V \subseteq W$, then $V \cap T = \emptyset$, so $\varphi^{-1}(L) = \emptyset$.

$\Rightarrow$ b).

If $V \not\subseteq W$, then $V + W = K^{n+1}$, so

$$\dim(V \cap W) = \dim(V) + \dim(W) - \dim(V+W)$$
$$= (d+1) + n - (n+1) = d$$

and $V \cap T \neq \emptyset$ is a translate of $V \cap W$

$$\uparrow$$

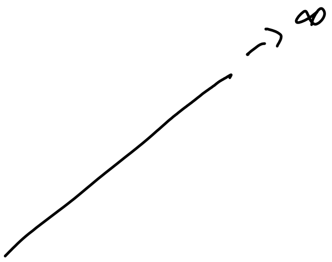
$$\begin{aligned} T &= W + s \text{ for some } s \in K^{n+1} \\ &= W + v \qquad \overset{\shortparallel}{v+w} \\ &\qquad\qquad \text{for some } v \in V, w \in W \end{aligned}$$

$\Rightarrow$ a) $\square$

Rmk Conversely, every d-dimensional affine linear subspace ℓ of K^n corr. to exactly one d-dimensional linear subspace L of $\mathbb{P}^n_K$, namely the set of lines through 0 contained in the subspace V of K^{n+1} spanned by the lines $\varphi(P)$ for $P \in \ell$.

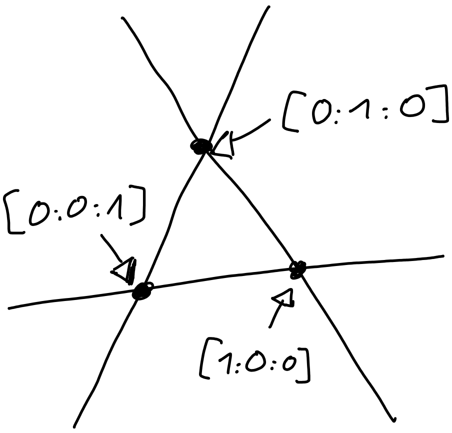
Exe The lines in $\mathbb{P}^2_k = \mathbb{A}^2_k \sqcup \mathbb{P}^1_k$ "are"

- The lines in $\mathbb{A}^2$ (with one point at ∞ each)



- The line $\mathbb{P}^1_k$ at ∞.

$$\mathbb{P}^2 \setminus U_0 = \{[x_0 : x_1 : x_2] \mid x_0 = 0\}$$



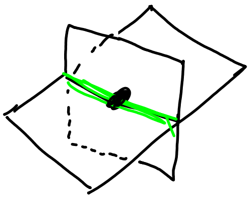
$$\mathbb{P}^2 \setminus U_1 = \{[x_0 : x_1 : x_2] \mid x_1 = 0\}$$

$$\mathbb{P}^2 \setminus U_2 = \{[x_0 : x_1 : x_2] \mid x_2 = 0\}$$

Lemma 3.1.2

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 $c \geq a+b-n$. $\left(\underset{n-c}{\underset{\|}{\mathrm{codim}(L\cap M, \mathbb{P}^n)}} \leq \underset{n-a}{\underset{\|}{\mathrm{codim}(L, \mathbb{P}^n)}} + \underset{n-b}{\underset{\|}{\mathrm{codim}(M, \mathbb{P}^n)}}\right)$

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 $V, W \subseteq K^{n+1}$

$\dim(V) = a+1, \quad \dim(W) = b+1$

$\mathrm{codim}(V, K^{n+1}) = n-a, \ \mathrm{codim}(W, K^{n+1}) = n-b$

$\Rightarrow V \cap W$ is a vector space with
$\mathrm{codim}(V \cap W, K^{n+1}) \leq (n-a) + (n-b)$

$\Rightarrow \dim(L \cap M) = n - \mathrm{codim}(V \cap W, K^{n+1}) \geq n - (n-a) - (n-b)$
$= a+b-n.$

$\square$

3.2. Algebraic sets

Def A polynomial $f \in K[X_0, \dots, X_n]$ is *homogeneous of degree $d \geq 0$* (or a *form of degree d*) if every monomial in f has degree (exactly) d.

Ex $2X + 3Y$ hom. of deg. 1

Ex $2X + 3Y + 1$ not hom.

Ex $X^3 + 2X^2Y + Y^3$ hom. of degree 3

Ex 0 is homogeneous of *every* degree $d \geq 0$.

Rmk The hom. degree d pol. form a K-vector space.

Rmk 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 *degree d part* of f).

Rmk If f is hom. of degree d and g is hom. of degree e, then fg is hom. of degree $d+e$.

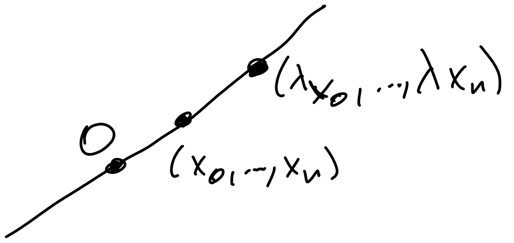
Rmk If $f \in K[Y_0, \dots, Y_m]$ is hom. of degree d and $g_1, \dots, g_m \in K[X_0, \dots, X_n]$ are hom. of degree e, then $f(g_1, \dots, g_m)$ is hom. of degree $d \cdot e$.

Rmk 3.2.1 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).

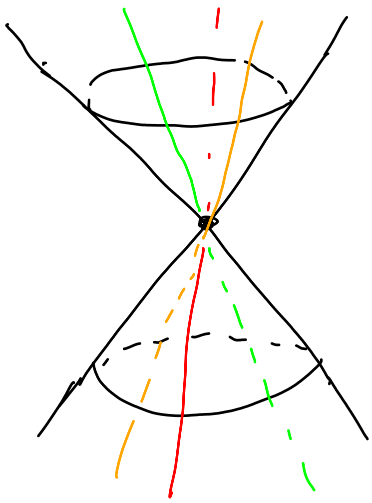
If $S \subseteq K[X_0, \dots, X_n]$ is a set of hom. pol., let

$$V_{\mathbb{P}^n_K}(S) = \{[x_0 : \dots : x_n] \in \mathbb{P}^n_K \mid f(x_0, \dots, x_n) = 0 \; \forall f \in S\}$$

$$= \bigcap_{f \in S} V_{\mathbb{P}^n_K}(f).$$

A subset $A = V_{\mathbb{P}^n_K}(S)$ of this form is called algebraic.

Ex $f = x_1^2 + x_2^2 - x_0^2$



$V(f) = V_{K^3}(f) =$ cone

$V_{\mathbb{P}^2}(f) =$ set of lines through 0 on the cone

Rmk $V_{\mathbb{P}^n_K}(S) \subseteq \mathbb{P}^n_K$ is the set of lines through 0 contained in $V(S) = V_{K^{n+1}}(S)$.

Ex Any linear subspace of $\mathbb{P}^n_K$ is algebraic.

Def Let $A \subseteq \mathbb{P}^n_K$ be any subset.

The set $\mathcal{C}(A) = \{0\} \cup \{0 \neq (x_0, \dots, x_n) \in K^{n+1} \,/\, [x_0 : \dots : x_n] \in A\}$
$\subseteq K^{n+1}$

(the union of $\{0\}$ and the lines in K^{n+1} representing the points in $A \subseteq \mathbb{P}^n_K$)

is called the affine cone of A.

Lemma 3.2.2 If $A \subseteq \mathbb{P}^n_K$ is algebraic, then $C(A) \subseteq K^{n+1}$ is algebraic.

Pf If $A = V_{\mathbb{P}^n_K}(S) \neq \emptyset$, then $C(A) = V_{K^{n+1}}(S)$.

If $A = \emptyset$, then $C(A) = \{0\}$. $\square$

Rmk $C(A \cap B) = C(A) \cap C(B)$

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.

Lemma 3.2.3 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.

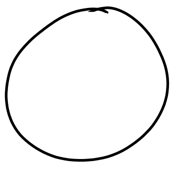
Pf $\varphi^{-1}(A) \subseteq K^n$ "is" the intersection of the affine cone $\mathcal{C}(A)$ with the affine linear subspace T corresponding to the chart. $\Box$

Concretely If $\varphi = \varphi_i$ is the i-th standard affine chart, $A = V_{\mathbb{P}^n}(S)$, then

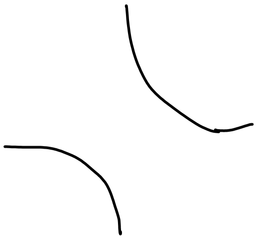
$$\varphi^{-1}(A) = \{(x_0, \dots, x_{i-1}, x_{i+1}, \dots, x_n) \in K^n \mid f(x_0, \dots, x_{i-1}, 1, x_{i+1}, \dots, x_n) = 0 \ \forall f \in S\}.$$

Exe $A = V_{\mathbb{P}^2}(x_1^2 + x_2^2 - x_0^2)$.

$$\varphi_0^{-1}(A) = V_{K^2}(x_1^2 + x_2^2 - 1)$$



$$\varphi_1^{-1}(A) = V_{K^2}(1 + x_2^2 - x_0^2)$$



The preimage $\varphi^{-1}(A)$ is a conic section for any affine chart φ.

We constructed a map

$$\{\text{alg. subset } A \text{ of } \mathbb{P}^n\} \longrightarrow \{\text{alg. subset } B \text{ of } K^n\}$$
$$A \longmapsto \varphi^{-1}(A)$$

Q How to produce $A \subseteq \mathbb{P}^n_K$ from $B \subseteq K^n$?

A 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 degree e (hom.) . The **homogenization** 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 3.2.4 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.

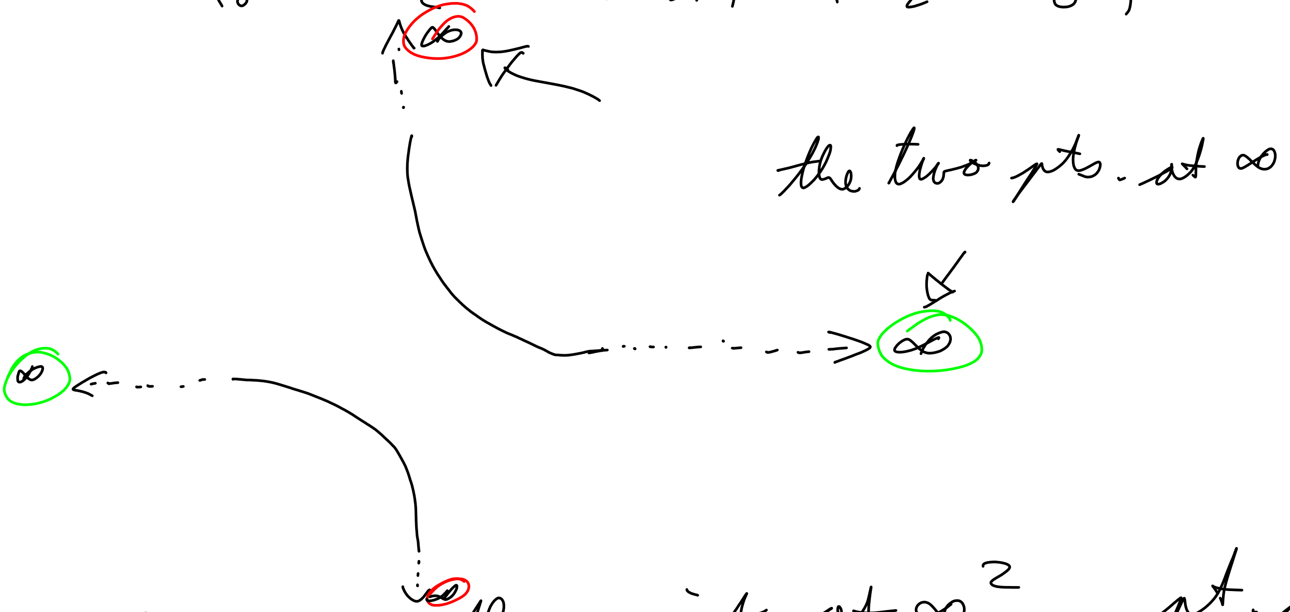
Cor 3.2.5

$\varphi^{-1}(\overline{\varphi(B)}) = B$ for any affine chart.

(We only add points at ∞ to B to obtain $\overline{\varphi(B)}$.)

Exe $B = \{(x_1, x_2) \mid x_1 x_2 = 1\}$

$\rightsquigarrow A = \overline{\varphi_0(B)} = \{[x_0 : x_1 : x_2] \mid x_1 x_2 = x_0^2\}$



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 $I = (f_1, --, f_m)$.

Then, S is the set of homogenizations of elements of I. Unfortunately, the homogenizations $\tilde{f}_1, \ldots, \tilde{f}_m$ don't always suffice!

Ex $I = (x_1^2 + x_2, x_1) = (x_2, x_1)$

$$\begin{tikzcd}
I = (x_1^2 + x_2 , x_1) \arrow[d, squiggly] & = (x_2 , x_1) \arrow[d, squiggly] \\
x_1^2 + x_0 x_2 = 0 , x_1 = 0 \arrow[d, Leftrightarrow] & x_2 = 0 , x_1 = 0 \arrow[d, squiggly] \\
x_0 x_2 = 0 , x_1 = 0 \arrow[d, squiggly] & \text{one point} \\
\text{two points} & {[1:0:0]} \\
{[0:0:1], [1:0:0]} &
\end{tikzcd}$$

Warning Let $I = (f_1, --, f_m)$.

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 $I = (x_1^2 + x_2, x_1) = (x_2, x_1)$

$$x_1^2 + x_0 x_2 = 0, x_1 = 0 \qquad\qquad x_2 = 0, x_1 = 0$$

$$\Updownarrow \qquad\qquad \rightsquigarrow$$

$$x_0 x_2 = 0, x_1 = 0 \qquad\qquad \text{one point } [1:0:0]$$

$\rightsquigarrow$ two points $[0:0:1], [1:0:0]$

Thm 3.2.6 Let $f \in K[X_1, \dots, X_n]$ with homogenization $\tilde{f}$ at X_0. Then, $\overline{\varphi_0(V(f))} = V_{\mathbb{P}^n_K}(\tilde{f})$.

Pf "$\subseteq$" clear

"$\supseteq$" Let $g \in (f)$ with homogenization $\tilde{g} = \tilde{f}\tilde{h}$

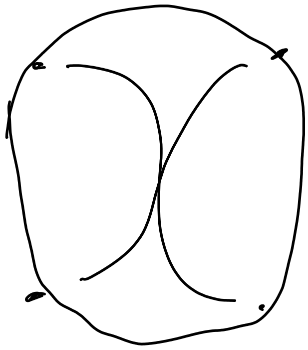
$\boxed{g = fh, \ h \in K[X_1, \dots, X_n]}$ $\quad \boxed{\text{Lemma } 3.2.4}$

If $\tilde{f}(P) = 0$, then $\tilde{g}(P) = 0$.

$$\Rightarrow V_{\mathbb{P}^n_K}(\tilde{f}) = V_{\mathbb{P}^n_K}(\{\text{hom. } \tilde{g} \text{ of } g \in (f)\}) = \overline{\varphi_0(V(f))}. \quad \square$$

Cor 3.2.7 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.

$\Rightarrow \varphi(U) = \mathbb{P}^n_K \setminus \left(\left(\mathbb{P}^n_K \setminus \operatorname{im}(\varphi) \right) \cup \varphi(\overline{U}) \right)$

is open in $\mathbb{P}^n_K$.

□

Cor 3.2.8 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.

⇝ You obtain the topology on $\mathbb{P}^n_K$ by glueing together the topologies on the affine charts.

3.3. 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 3.3.1 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.

$$\Rightarrow f_d = \sum_i \underset{\substack{\uparrow \\ \text{hom. of deg. } d_i}}{g_i} \; \underset{\substack{\uparrow \\ \text{deg. } d-d_i}}{h_{i,d-d_i}} \in I.$$

$\square$

Def For any homogeneous ideal $I \subseteq K[X_0, \dots, X_n]$, we let $V_{\mathbb{P}^n_K}(I) := V_{\mathbb{P}^n_K}(\{f \in I \text{ homogeneous}\})$.

Rmk $V_{\mathbb{P}^n_K}(\text{ideal gen. by } S) = V_{\mathbb{P}^n_K}(S)$ for any set S of hom. pol.

Rmk $C(V_{\mathbb{P}^n_K}(I)) = \{0\} \cup V_{K^{n+1}}(I)$

Def The vanishing ideal of a subset $A \subseteq \mathbb{P}^n_K$ is the ideal $I \subseteq K[X_0, \dots, X_n]$ generated by the homogeneous pol. f vanishing on A (s.t. $A \subseteq V_{\mathbb{P}^n_K}(f)$).

Lemma 3.3.2

If $A \neq \emptyset$, then $I(A) = I(C(A))$.

If $A = \emptyset$, then $I(A) = K[X_0, \dots, X_n]$.

(although $I(C(A)) = I(\{0\}) = (X_0, \dots, X_n)$).

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. $\square$

3.4. Projective Nullstellensatz

From now on, we again assume that K is algebraically closed.

Thm 3.4.1 (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) $(X_0,\dots,X_n)\subseteq\sqrt{I}$

$\nwarrow$ 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)$\iff$c): clear

a)$\iff$b):

$$V_{\mathbb{P}^n_k}(I)=\emptyset$$

$$\iff \underset{\substack{\parallel \\ \{0\}\cup V_{k^{n+1}}(I)}}{\ell(V_{\mathbb{P}^n_k}(I))} = \{0\}$$

$$\iff V_{k^{n+1}}(I) \subseteq \{0\}$$

$$\iff \underset{\substack{\parallel \leftarrow \text{Hilbert's Nsts} \\ \sqrt{I}}}{I(V_{k^{n+1}}(I))} \supseteq I(\{0\}) = (x_0,\dots,x_n)$$

$\square$

Cor 3.4.2 (Proj. Nsts) For any hom. id. I,

$$I(V_{\mathbb{P}^n_k}(I)) = \begin{cases} \sqrt{I}, & (x_0,\dots,x_n)\not\subseteq\sqrt{I}, \\ K[x_0,\dots,x_n], & (x_0,\dots,x_n)\subseteq\sqrt{I}. \end{cases}$$

Pf second case: $V_{\mathbb{P}^n_k}(I)=\emptyset \Rightarrow I(V_{\mathbb{P}^n_k}(I))=K[x_0,\dots,x_n]$

first case: $I(V_{\mathbb{P}^n_k}(I)) \underset{\substack{\uparrow \\ \text{Lemma 3.3.2}}}{=} I(\ell(V_{\mathbb{P}^n_k}(I))) = I(V_{k^{n+1}}(I))$

$$\underset{\substack{\uparrow \\ \text{Hilbert's Nsts}}}{=} \sqrt{I}.$$

$\square$

3.5. Irreducibility

Def An alg. subset $\overset{\emptyset \neq}{A} \subseteq \mathbb{P}^n_k$ is <u>irreducible</u> if you can't write $A = A_1 \cup A_2$ with any alg. sets $A_1, A_2 \subsetneqq A_2$.

Ex One point, $\mathbb{P}^n_K$

Thm 3.5.1 Let $A \neq \emptyset$ be an alg. subset of $\mathbb{P}^n_k$.
The following are equivalent:

a) A is irreducible.

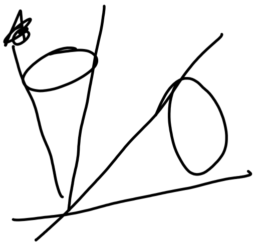
b) $C(A)$ is irreducible.

c) $I(A)$ is a prime ideal.

Pf b)$\Leftrightarrow$c) $\quad I(C(A)) = I(A)$

b)$\Rightarrow$a) $\quad A = A_1 \cup A_2, \quad A_1, A_2 \subsetneqq A$

$C(A) = C(A_1) \cup C(A_2), \quad C(A_1), C(A_2) \subsetneqq C(A)$



a)$\Rightarrow$c) Say $f, g \notin I(A)$ with $fg \in I(A)$.

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.

$$I(A) \text{ hom. ideal } \underset{\substack{\uparrow \\ \text{Thm 3.3.1}}}{\Rightarrow} f_d g_e \in I(A)$$

Take $A_1 = A \cap V_{\mathbb{P}^n_k}(f_d)$,

$A_2 = A \cap V_{\mathbb{P}^n_k}(g_e)$.

$$f_d g_e \in I(A) \Rightarrow A_1 \cup A_2 = A$$

$$f_d \notin I(A) \Rightarrow A_1 \subsetneq A$$

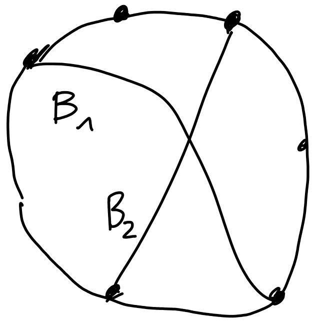
$$g_e \notin I(A) \Rightarrow A_2 \subsetneq A.$$

□

Thm 3.5.2 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 $\emptyset \neq \varphi^{-1}(A) = B_1 \cup B_2$, $B_1, B_2 \subsetneq \varphi^{-1}(A)$,



then

$$A = \overline{\varphi(B_1)} \cup \overline{\varphi(B_2)} \cup \underbrace{(A \setminus \mathrm{im}(\varphi))}_{\text{closed}}$$

with

$$\overline{\varphi(B_1)} \subsetneq A, \quad \overline{\varphi(B_2)} \subsetneq A,$$

$$A \setminus \mathrm{im}(\varphi) \subsetneq A. \qquad \square$$

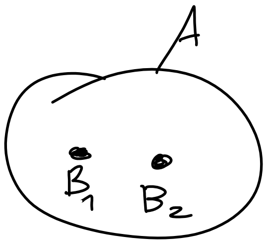
Rmk If $A \neq \emptyset$ and for every affine chart φ, $\varphi^{-1}(A) = \emptyset$ or $\varphi^{-1}(A)$ is irred., then A is irred.

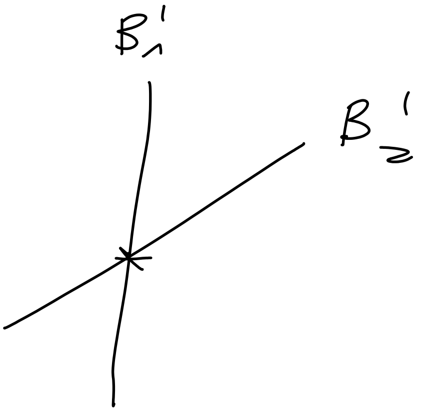
Warning It doesn't suffice to consider just the standard affine charts φ_i. For example $\{[0:1], [1:0]\} \subseteq \mathbb{P}^1_k$ is reducible although the intersections with $U_0 = \{[x_0 : x_1] \mid x_0 \neq 0\}$ and $U_1 = \{[x_0 : x_1] \mid x_1 \neq 0\}$ each consist of just one point.

Thm 3.5.3 We can define the irreducible components of an alg. set $A \subseteq \mathbb{P}^n_K$ like for $A' \subseteq K^n$ in Thm 2.27 and they satisfy the same properties. Furthermore, we have a bij.

$$\{\text{irred. comp. } B \text{ of } A\} \longleftrightarrow \{\text{irred. comp. } B' \overset{\{0\}}{\neq} \text{ of } C(A)\}$$

$$B \longleftrightarrow C(B)$$





3.6. Dimension

Def The dimension of an 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 3.6.1

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 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

$$\{0\} = C(\emptyset) \subsetneq C(V_0) \subsetneq \cdots \subsetneq C(V_d) \subseteq C(V) \text{ of irred. sets.}$$

$$\Rightarrow \dim(C(V)) \geq \dim(V)+1$$

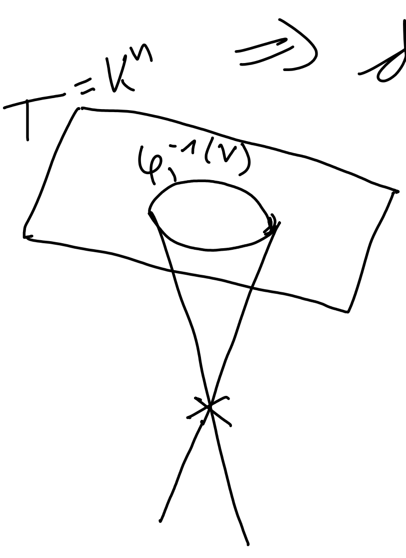
For any chain

$$W_0 \subsetneq \cdots \subsetneq W_d \subseteq \varphi^{-1}(V) \text{ of irred. sets,}$$

we obtain a chain

$$\overline{\varphi(W_0)} \subsetneq \cdots \subsetneq \overline{\varphi(W_d)} \subseteq V \text{ of irred. sets.}$$

$$\Rightarrow \dim(V) \geq \dim(\varphi^{-1}(V)).$$



Let $0 \notin T \subseteq K^{n+1}$ be an n-dim. affine lin. subspace corr. to φ. Then $C(V)$ is the Zariski closure of the join of $\{0\}$ and $C(V) \cap T = \varphi^{-1}(V)$.

By problem 4 on pset 8, we then have $\dim(C(V)) = \dim(\varphi^{-1}(V))+1$. $\square$

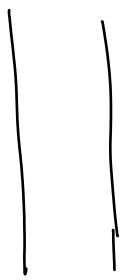
Thm 3.6.2 Let $f_1, \dots, f_m \in K[x_0, \dots, x_n]$ be nonconstant hom. pol. with $m \leq n$.

Then, $V_{\mathbb{P}^n_K}(f_1, \dots, f_m) \neq \emptyset$ and every irred. comp. A has $\dim(A) \geq n-m$.

of $V_{\mathbb{P}^n_K}(f_1, \dots, f_m)$

Rmk The first claim is wrong in K^n:

$\emptyset = V(x, x-1) \subseteq K^2$.



Pf By Thm 2.83, every irred. comp. A' of $V_{K^{n+1}}(f_1, \dots, f_m) \subseteq K^{n+1}$ has $\dim(A') \geq n+1-m$.

This shows the second claim because any irred. comp. A corr. to an irred. comp. $A' = C(A)$ with $\dim(A) = \dim(A') - 1$.

Since $f_1, \dots, f_m$ are homogeneous of degree ≥ 1, we have $0 \in V_{K^{n+1}}(f_1, \dots, f_m)$.

$\Rightarrow$ There is at ~~least~~ least one irred. comp. A'.

It satisfies $\dim(A') \geq n+1-m \geq 1$,

so $A' \neq \{0\}$.

It therefore corresponds to an irred. comp. A of $V_{\mathbb{P}^n_u}(f_1, \ldots, f_m)$, so in particular $V_{\mathbb{P}^n_u}(f_1, \ldots, f_m) \neq \emptyset$. $\square$

Def If $V, W \subseteq \mathbb{P}^n_u$ irred. alg. sets, the *codimension* of V in W is

$$\begin{aligned}\operatorname{codim}(V, W) &= \dim(W) - \dim(V) \\ &= \dim(C(W)) - \dim(C(V)) \\ &= \operatorname{codim}(C(V), C(W)).\end{aligned}$$

Thm 3.6.3 It's the largest length d of a chain $V = V_0 \subsetneq V_1 \subsetneq \cdots \subsetneq V_d = W$ of irred. alg. sets

Pf HW.

Thm 3.6.4 Let $V_1, V_2 \subseteq W \subseteq \mathbb{P}^n_k$ be irred. alg. with $\operatorname{codim}(V_1,W) + \operatorname{codim}(V_2,W) \leq \dim(W)$.

Then, $V_1 \cap V_2 \neq \emptyset$ and every irred. comp. A of $V_1 \cap V_2$ satisfies

$$\operatorname{codim}(A,W) \leq \operatorname{codim}(V_1,W) + \operatorname{codim}(V_2,W).$$

Pf ~~Apply~~ Apply Cor 2.8.9 to the affine cones:

Any irred. comp. B of $\ell(V_1) \cap \ell(V_2) = \ell(V_1 \cap V_2)$ satisfies

$$\begin{aligned}\operatorname{codim}(B,\ell(W)) &\leq \operatorname{codim}(\ell(V_1),\ell(W)) \\ &\quad + \operatorname{codim}(\ell(V_2),\ell(W)) \\ &= \operatorname{codim}(V_1,W) + \operatorname{codim}(V_2,W).\end{aligned}$$

This shows the second claim.

For the first claim, use that

$0 \in \ell(V_1) \cap \ell(V_2)$ and

$$\dim(B) \geq \dim(\ell(W)) - \underbrace{(\operatorname{codim}(V_1,W) + \operatorname{codim}(V_2,W))}_{\substack{\leq \dim(W) \\ = \dim(\ell(W)) - 1}}$$

$$\geq 1.$$

$\square$

Exe Any two curves in $\mathbb{P}^2_k$ intersect.

Exe Any curve and surface in $\mathbb{P}^3_k$ intersect.

Exe Any three surfaces in $\mathbb{P}^3_k$ intersect.

4. Multiplicities and tangent spaces

4.1. Multiplicity of a function at a point

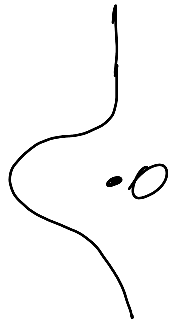
Def Let $0 \neq f \in K[X_1, \dots, X_n]$.

The multiplicity $m_0(f)$ of f at $P=(0,\dots,0)$ is the smallest degree of a monomial occurring in f.

The initial form $in_0(f)$ of f at $P=(0,\dots,0)$ is the hom. degree $m_0(f)$ part of f.

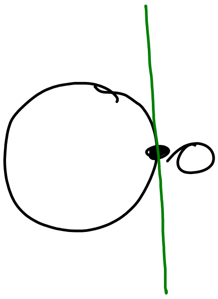
Rmk $in_0(f)$ is the lowest order (nonzero) approximation of f at 0.

Ex A $f(x,y) = 7 + x + 2xy^2$



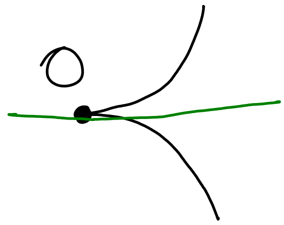
$\rightsquigarrow m_0(f) = 0$, $in_0(f) = 7$,
tangent cone $= \emptyset$

Ex B $f(x,y) = (x+1)^2 + y^2 - 1$
$= x^2 + 2x + y^2$



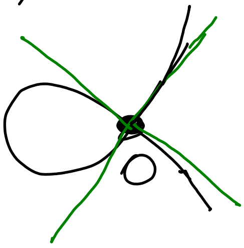
$\rightsquigarrow m_0(f) = 1$, $in_0(f) = 2x$
$in_0((f)) = (x)$, tangent cone $= \{x = 0\}$

Ex C $f(x,y) = y^2 - x^3$



$\rightsquigarrow m_0(f) = 2$, $in_0(f) = y^2$
$in_0((f)) = (y^2)$, tangent cone $= \{y = 0\}$

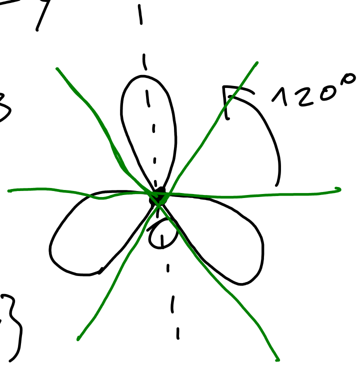
Ex D $f(x,y) = y^2 - x^3 - x^2$



$\rightsquigarrow m_0(f) = 2$, $in_0(f) = y^2 - x^2$
$in_0((f)) = ((y-x)(y+x))$, tangent cone $= \{y = \pm x\}$

Ex E $f(x,y) = (x^2+y^2)^2 + 3x^2y - y^3$

$\rightsquigarrow m_0(f) = 3$, $in_0(f) = 3x^2y - y^3$
$in_0((f)) = (y(\sqrt{3}x - y)(\sqrt{3}x + y))$,
tangent cone $= \{y = 0, \sqrt{3}x, -\sqrt{3}x\}$



Rmk $m_0(f) \geq 1 \Leftrightarrow f(0) = 0$

Rmk $m_0(fg) = m_0(f) + m_0(g)$

$\mathrm{in}_0(fg) = \mathrm{in}_0(f)\,\mathrm{in}_0(g)$

Def For any $P=(a_1,\dots,a_n)$, we let

$m_P(f) = m_0(g)$ for $g(X_1,\dots,X_n) = f(X_1+a_1,\dots,X_n+a_n) \in K[X_1,\dots,X_n]$

$\mathrm{in}_P(f) = \mathrm{in}_0(g)$.

Def $P \in K^n$ is a simple root of f if $m_P(f) = 1$.

Rmk $m_P(f)$ is the largest integer $t \geq 0$ such that $f \in \mathfrak{m}_P^t$, where $\mathfrak{m}_P = (X_1-a_1,\dots,X_n-a_n)$ is the max. id. corresponding to $P = (a_1,\dots,a_n)$.

$$\mathfrak{m}_P^t = (\underbrace{(X_1-a_1)^t, (X_1-a_1)^{t-1}(X_2-a_2), \dots}_{\text{mon. of deg. } t \text{ in } X_1-a_1,\dots,X_n-a_n}).$$

4.2. Tangent cones

Def The initial ideal $\mathrm{in}(I)$ of an ideal $I \subseteq K[X_1,\dots,X_n]$ is the homogeneous ideal gen. by the initial forms $\mathrm{in}(f)$ of the elements f of I. The tangent cone of I is $V_{K^n}(\mathrm{in}(I))$.

(at 0)

Rmk $\mathrm{in}_0((f)) = (\mathrm{in}_0(f))$.

Def The *tangent cone* of an alg. set V at O is the tangent cone of $I(V)$ at O.

The tangent cone of V at $P \in K^n$ is the tangent cone of the translate $V-P$ at O.

Lemma 4.2.1 For any ideal I, the tangent cones of I and $\sqrt{I}$ at P agree.

Pf $f \in \sqrt{I} \iff \exists m \geq 1 : f^m \in I$

$$\underset{\substack{\uparrow \\ in(f^m) = in(f)^m}}{\Longrightarrow} \quad V(in(I)) = V(in(\sqrt{I})).$$

$\square$

Lemma 4.2.2 The tangent cone of $A \cup B$ at P is the union of the tangent cones at A and B at P.

Pf HW.

Prop 4.2.3 If V is irred. of dimension d, then the tangent cone of V at any point $P \in V$ has dimension d.

4.3. Tangent spaces

Def Let $V \subseteq K^n$ be an alg. set containing O.

The tangent space $T_O(V)$ to V at O is the vector space

$$V_{K^n}(\{f_1 \text{ hom. deg. } 1 \text{ part of } f \in I(V)\}).$$

The tangent space $T_P(V)$ to V at $P \in V$ is the tangent space to $V-P$ at O.

Rmk The tangent space always contains the tangent cone.

Pf The hom. deg. 1 part f_1 of $f \in I(V)$ with $f(P)=0$ is

$$f_1 = \begin{cases} \mathrm{in}(f) & \text{if } m_P(f)=1 \\ 0 & \text{if } m_P(f) \geq 2. \end{cases}$$ □

Rmk Let $0 \neq f \in K[x_1,\dots,x_n]$ be squarefree. The tangent space to $V(f)$ at $P \in V(f)$ is

$$T_P(V(f)) = \begin{cases} \text{the tangent cone at } P & \text{if } m_P(f)=1, \\ K^n & \text{if } m_P(f) \geq 2. \end{cases}$$

Rmk In general,

$$V(\{f \text{ hom. deg. } 1 \text{ part of } f \in I\}) \overset{\not{}}{\cup} V(\{f \text{ hom. deg. } 1 \text{ part of } f \in \sqrt{I}\}).$$

$$\Big(\text{E.g. } \underset{\substack{\Downarrow \\ V(\ldots) = K}}{I = (x^2)}, \quad \underset{\substack{\Downarrow \\ V(\ldots) = \{0\}}}{\sqrt{I} = (x).}\Big)$$

Thm 4.3.1 Let $V \subseteq K^n$ be irreducible.

Then, $\dim_K(T_P(V)) \geq \dim(V)$.

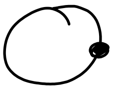
Pf $T_P(V) \supseteq \underbrace{\text{tangent cone}}_{\dim = d \text{ by Prop } 4.2.3}$ $\square$

Def An irred. alg. set $V \subseteq K^n$ is *smooth* at $P \in V$ if $\dim_K(T_P(V)) = \dim(V)$.

It is *smooth* if it is smooth at every $P \in V$.

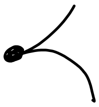
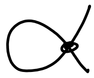
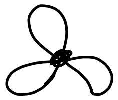
(otherwise *singular*)

Rmk If V is smooth at P, tangent space = tangent cone.

Ex B  smooth at 0:

$$V = \{(x,y)\in K^2 \mid \underbrace{(x-1)^2+y^2-1}_{x^2+y^2-2x}=0\}$$

$T_0(V) = \{(x,y)\in K^2 \mid x=0\}$ has dim 1.

Ex C, D, E    singular at 0.

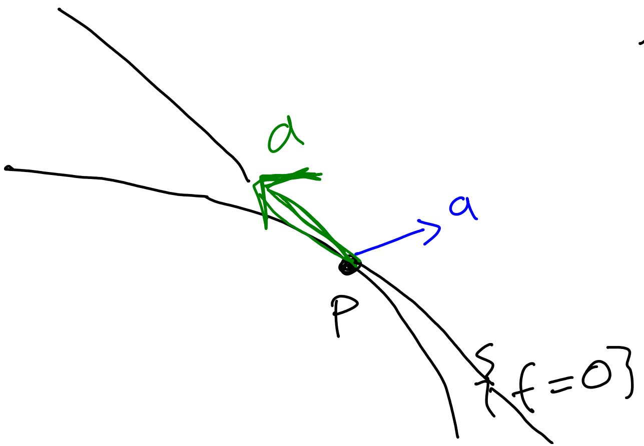
Note: The hom. deg. 1 part of $f\in K[X_1,\dots,X_n]$ is

$$\frac{\partial f}{\partial X_1}(0)\cdot X_1 + \dots + \frac{\partial f}{\partial X_n}(0)\cdot X_n$$

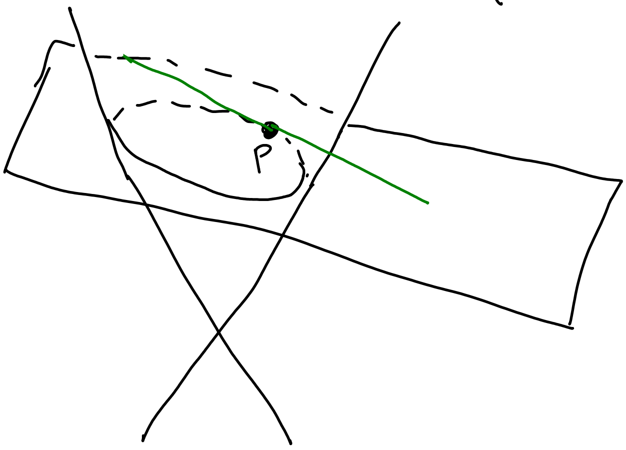
Rmk Hence, $T_P(V) = \bigcap_{f\in I(V)} \ker((Df)(P))$

where $(Df)(P): K^n \longrightarrow K$ denotes the derivative of $f: K^n \to K$ at P.

" $a \in T_P(V) \iff$ derivative of every $f\in I(V)$ in the direction a is 0 "



Eg $V = V(\underbrace{x^2+y^2-z^2}_{f}, \underbrace{2x+z-11}_{g})$



$P = (x, y, z)$

$$(Df)(x,y,z)(a,b,c) = 2xa + 2yb - 2zc$$

- -- $(dx, dy, dz) = 2x\,dx + 2y\,dy - 2z\,dz$

$$(Dg)(x,y,z) = (a,b,c) = 2a + c$$

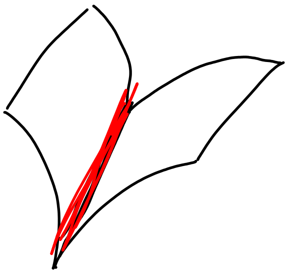
. . . - $2dx + dz$

$$T_{(x,y,z)}(V) = \ker \begin{pmatrix} 2x & 2y & -2z \\ 2 & 0 & 1 \end{pmatrix}$$

$P = (3,4,5) \in V$

$\rightsquigarrow T_p(V) = \left\langle \begin{pmatrix} -4 \\ 13 \\ 8 \end{pmatrix} \right\rangle$.

Lemma 4.3.2 The set $S \subseteq V$ of singular points is algebraic. (so the set of smooth points is an open subset of V.)



Pf Let $I(V) = (f_1, \ldots, f_m)$, $P \in V$.

$$T_P(V) = \bigcap_{g \in I(V)} \ker((Dg)(P)).$$

Write $g = h_1 f_1 + \ldots + h_m f_m$ with $h_i \in K[X_1, \ldots, X_n]$.

$$\underset{\text{product rule}}{(Dg)(P)(a)} = \sum_{i=1}^{m} \Big((Dh_i)(P)(a) \cdot \underset{=0 \text{ because } P \in V}{f_i(P)} + h_i(P) \cdot (Df_i)(P)(a) \Big)$$

$\Rightarrow T_P(V) = \bigcap_{i=1}^{m} \ker((Df_i)(P))$ is the kernel of the $m \times n$-matrix $M(P) = \left(\frac{\partial f_i}{\partial X_j}(P) \right)_{i,j}$

$\Rightarrow S$ is the set of points $P \in V$ for which $\mathrm{rk}(M(P)) \leq n - \dim(V) - 1 =: r$.

Equivalently: The set of $P \in V$ such that all $\underbrace{\text{determinants of } (r+1)\times(r+1)\text{-minors of } M(P)}_{\text{pol. in the coord. of } P}$ vanish.

$\square$

Prop 4.3.2 There is a smooth point on any irred. alg. set $V \subseteq K^n$.

Cor 4.3.3 The set of smooth points is a dense open subset of V.

4.4. Multiplicity in finite sets

Def Let I be an ideal of $K[X_1,\dots,X_n]$.

~~Assume $V(I) \subseteq K^n$ is a finite set.~~

The *multiplicity* of $P \in K^n$ in I is

$$m_P(I) := \dim_K \left(\mathcal{O}_{\mathbb{A}^n_K,P} / I\,\mathcal{O}_{\mathbb{A}^n_K,P} \right),$$

where

$$\mathcal{O}_{\mathbb{A}^n,P} = \{ f \in \overset{K(X_1,\dots,X_n)}{\overset{\shortparallel}{K(\mathbb{A}^n)}} \text{ def. at } P \}$$

$$= \{ \tfrac{a}{b} \mid a,b \in K[X_1,\dots,X_n],\ b(P) \neq 0 \}$$

is the local ring of $\mathbb{A}^n = K^n$ at P and

$$I\,\mathcal{O}_{\mathbb{A}^n,p} = \left\{ \frac{a}{b} \;\middle|\; a \in I,\ b \in K[x_1,\dots,x_n],\ b(p) \neq 0 \right\}$$

is the ideal of $\mathcal{O}_{\mathbb{A}^n,p}$ generated by I.

Ex Let $f(X) = \prod_{i=1}^{r} (X - c_i)^{e_i} \in K[X]$

with $c_1,\dots,c_r \in K$ distinct, $I = (f)$.

Let $t \in K$.

$$\mathcal{O}_{\mathbb{A}^1,t} = \left\{ \frac{a}{b} \;\middle|\; a,b \in K[X],\ b(t) \neq 0 \right\}$$

$$\mathcal{O}_{\mathbb{A}^1,t}^{X} = \left\{ \frac{a}{b} \;\middle|\; a,b \in K[X],\ a(t), b(t) \neq 0 \right\}$$

$$I\,\mathcal{O}_{\mathbb{A}^1,t} = \prod_{i=1}^{r} \underbrace{(X-c_i)^{e_i}}_{\text{unit unless } c_i = t} \cdot \mathcal{O}_{\mathbb{A}^1,t}$$

$$= \begin{cases} \mathcal{O}_{\mathbb{A}^1,t} & \text{if } t \notin \{c_1,\dots,c_r\} \\ (X-c_i)^{e_i}\mathcal{O}_{\mathbb{A}^1,t} & \text{if } t = c_i \end{cases}$$

$$= (X-t)^e \mathcal{O}_{\mathbb{A}^1,t} \text{ if } t \text{ is a root of mult. } e \text{ of } f.$$

Lemma 4.4.1 We have a K-algebra isom.

$$\mathcal{O}_{\mathbb{A}^1,t} \big/ (x-t)\mathcal{O}_{\mathbb{A}^1,t} \xrightarrow{\sim} K$$

$$g \longmapsto g(t)$$

Pf well-def.: If $g \in (x-t)\mathcal{O}_{\mathbb{A}^1,t}$, then $g(t)=0$.

injective: If $\frac{a(t)}{b(t)}=0$, then $a(t)=0$, so

$x-t \mid a(t)$ in $K[x]$, so

$$\frac{\frac{a}{x-t}}{b} \in \mathcal{O}_{\mathbb{A}^1,t}.$$

surjective: const. fct. $\in \mathcal{O}_{\mathbb{A}^1,t}$. $\square$

Cor 4.4.2 $\dim_K \left(\mathcal{O}_{\mathbb{A}^1,t} / (x-t)^e \mathcal{O}_{\mathbb{A}^1,t}\right) = e$ for any $e \geq 0$.

Pf Consider the chain of K-vector spaces

$$\mathcal{O}_{\mathbb{A}^1,t} \supseteq (x-t)\mathcal{O}_{\mathbb{A}^1,t} \supseteq (x-t)^2\mathcal{O}_{\mathbb{A}^1,t} \supseteq \dots \supseteq (x-t)^e\mathcal{O}_{\mathbb{A}^1,t}$$

It suffices to prove that

$$\dim_K \left((x-t)^i \mathcal{O}_{\mathbb{A}^1,t} \big/ (x-t)^{i+1} \mathcal{O}_{\mathbb{A}^1,t}\right) = 1 \quad \forall i \geq 0.$$

But we have an isomorphism

$$\mathcal{O}_{\mathbb{A}^1,t}/(x-t)\mathcal{O}_{\mathbb{A}^1,t} \xrightarrow{\sim} (x-t)^i\mathcal{O}_{\mathbb{A}^1,t}/(x-t)^{i+1}\mathcal{O}_{\mathbb{A}^1,t}$$

$$g \longmapsto (x-t)^i g$$

and the LHS has dimension 1 by Lemma 4.4.1. □

<u>Ex</u> (as before) $0 \neq f \in K[X]$, $I = (f)$

$\Rightarrow m_t(I) = e$ if f has a root of mult. e at t (with $e = 0$ if f doesn't have a root at t).

$1, X-t, \dots, (X-t)^{e-1}$ form a basis of $\mathcal{O}_{\mathbb{A}^n,p}/I\mathcal{O}_{\mathbb{A}^n,p}$.

Lemma 4.4.3 Let $I \subseteq k[X_1,\dots,X_n]$ and $P \in k^n$.

Then, $m_P(I) = 0 \iff P \notin V(I)$.

Pf $P \notin V(I) \iff \exists\, f \in I : f(P) \neq 0$

$$\Updownarrow$$

$m_P(I) = 0 \iff \mathcal{O}_{\mathbb{A}^n,P} = I\mathcal{O}_{\mathbb{A}^n,P} \iff \frac{f}{f} = 1 \in I\mathcal{O}_{\mathbb{A}^n,P}$

□

Rmk If $I \supseteq J$ (and therefore $V(I) \subseteq V(J)$),

then $m_P(I) \leq m_P(J)$.

Pf We have a quotient map

$$\mathcal{O}_{\mathbb{A}^n,P}/J\mathcal{O}_{\mathbb{A}^n,P} \twoheadrightarrow \mathcal{O}_{\mathbb{A}^n,P}/I\mathcal{O}_{\mathbb{A}^n,P},$$

which is surjective. □

Lemma 4.4.4 If $V \subseteq \mathbb{A}^n_k$ is an irreducible algebraic set with $I = I(V)$, then

$$m_P(I) = \dim_k(\mathcal{O}_{V,P}) \text{ for all } P \in V.$$

Pf We have an isomorphism

$$\mathcal{O}_{\mathbb{A}^n,P}/I\mathcal{O}_{\mathbb{A}^n,P} \xrightarrow{\sim} \mathcal{O}_{V,P}$$

$$\left[\frac{a}{b}\right] \longmapsto \frac{a}{b} \quad \text{for } a,b \in k[X_1,\dots,X_n],\ b(P) \neq 0.$$

well-def: $b(P) \neq 0 \Rightarrow$ b is not zero everywhere on V

$a \in I \Rightarrow$ a is zero everywhere on V

$\Rightarrow \frac{a}{b}$ is the zero fct. on V

injective: If $\frac{a}{b}$ is zero on V, then a is zero everywhere on V. $\Rightarrow a \in I$.

surjective: clear. $\square$

Ex $V = \{P\} \subseteq K^n \Rightarrow m_P(I(V)) = 1$.

Pf 1 is a basis of $\mathcal{O}_{V,P}$.

Any rat. fct. on V is given by its value at P. $\square$

Cor 4.4.5 If I is any ~~i~~ideal and W is an irred. comp. of $V(I)$ of dimension ≥ 1, then $m_P(I) = \infty$.

Ex $I = (0) \subset K[X]$, $W = K$, $P = 0$

$$\mathcal{O}_{\mathbb{A}^1,P} = \{\tfrac{a}{b} \mid b(0) \neq 0\}$$

is ∞-dimensional:

$1, X, X^2, \ldots$ are linearly independent.

Pf of Cor $W \subseteq V(I)$

$$\Rightarrow I(W) \supseteq I(V(I)) = \sqrt{I} \supseteq I$$

$$\Rightarrow m_p(I) \geq m_p(I(W)).$$

$\rightsquigarrow$ w.l.o.g. $I = I(W)$,

$$\underset{\substack{\uparrow\\ \text{Lemma}}}{\Rightarrow} \; m_p(I) = \dim_k(\mathcal{O}_{W,p})$$

$$\underset{\substack{\uparrow\\ \boxed{\mathcal{O}_{W,p} \supseteq \Gamma(W)}}}{\geq} \dim_k(\Gamma(W))$$

$$\underset{\substack{\uparrow\\ \boxed{\text{Lemma 2.34, Cor 2.35}}}}{=} \# W = \infty .$$

$\square$

Thm 4.4.6 Let $I \subseteq K[X_1, \dots, X_n]$ be any ideal. Then,

$$\sum_{P \in V(I)} m_P(I) = \dim_K(K[X_1, \dots, X_n]/I).$$

Rmk By Lemma 2.34, Cor. 2.35, if I is a radical ideal, then

$$\# V(I) = \dim_K(\cdots).$$

Ex $I = (f)$, $0 \neq f \in K[X]$, $\deg(f) = d$.

$\Rightarrow 1, X, \dots, X^{d-1}$ form a basis of $K[X]/I$, so $\dim(\dots) = d$.

And we have d roots with multiplicities.

Cor 4.4.7 If I is a radical ideal with $\# V(I) < \infty$, then $m_P(I) = 1 \ \forall P \in V(I)$.

Lemma 4.4.8 Let $P \in K^n$ with maximal ideal $m_P = V(\{P\}) \subset K[X_1, \dots, X_n]$. Then, any $f \in K[X_1, \dots, X_n]$ with $f \notin m_P$ is invertible in $\underbrace{K[X_1, \dots, X_n]/m_P^t}_{R_t :=}$ for all $t \geq 0$.

Analogy Any number $n \notin 3\mathbb{Z}$ is invertible in $\mathbb{Z}/3^t\mathbb{Z}$ for all $t \geq 0$.

Pf The mult. by f map $\alpha : R_t \longrightarrow R_t$

$$g \longmapsto fg$$

is K-linear.

R_t is a finite-dimensional K-vector spaces. (If $P=0$, the monomials of degree $< t$ form a basis of R_t.)

If the map α is not an isomorphism, it's not injective, so there is some $g \in K[x_1, \dots, x_n]$ with

$$g \notin m_P^t \quad \text{but} \quad fg \in m_P^t$$

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

$$m_P(g) < t \qquad\qquad \underset{\underbrace{m_P(f)}_{0} + m_P(g)}{\overset{\|}{m_P(fg)}} \geq t$$

$\lightning$ $\square$

Pf of Thm Let $V(I) = \{P_1, \dots, P_r\}$ and let $m_{P_1}, \dots, m_{P_r}$ be the corr. max. ideals.

Goal: $K[X_1, \dots, X_n]/I \xrightarrow{\alpha} \prod_{i=1}^{r} \mathcal{O}_{\mathbb{A}^n, P_i} / I \mathcal{O}_{\mathbb{A}^n, P_i}$

$$f \longmapsto (f, \dots, f)$$

$\sqrt{I} = I(V(I)) = I(\{P_1, \dots, P_r\}) = m_{P_1} \cap \dots \cap m_{P_r}$.

Let $I \supseteq (m_{P_1} \cap \dots \cap m_{P_r})^d$ with $d \geq 1$.

Since the sets $V(m_{P_1}), \dots, V(m_{P_r})$ are pairwise disjoint, the Chinese remainder theorem tells us that

$$\begin{aligned}(m_{P_1} \cap \dots \cap m_{P_r})^d &= (m_{P_1} \cdots m_{P_r})^d \\ &= m_{P_1}^d \cdots m_{P_r}^d \\ &= m_{P_1}^d \cap \dots \cap m_{P_r}^d\end{aligned}$$

and

$$K[X_1, \dots, X_n]/(m_{P_1} \cap \dots \cap m_{P_r})^d \cong \prod_{i=1}^{r} K[X_1, \dots, X_n]/m_{P_i}^d.$$

In particular, there are polynomials $e_1, \dots, e_n \in K[X_1, \dots, X_n]$ such that $e_i \equiv 1 \bmod m_{p_i}^d$ and $e_i \equiv 0 \bmod m_{p_j}^d$ for all $j \neq i$.

<u>α is injective:</u>

Let $f \in K[X_1, \dots, X_n]$,

$f = \frac{a_i}{b_i}$ where $a_i \in I$, $b_i(p_i) \neq 0$ for $i = 1, \dots, n$.

$b_i \notin m_{p_i} \Rightarrow b_i$ is invertible mod $m_{p_i}^d$, so

there is a polynomial $t_i \in K[X_1, \dots, X_n]$ with $t_i b_i \equiv 1 \bmod m_{p_i}^d$

and $t_i \equiv 0 \bmod m_{p_j}^d$ for $j \neq i$.

$\Rightarrow t_i b_i = e_i$

$$\Rightarrow f \equiv \underbrace{\Big(\sum_i e_i\Big)}_{\substack{1 \bmod (m_{p_1} \cap \dots \cap m_{p_r})^d \\ \Rightarrow 1 \bmod I}} f = \sum_i t_i b_i f = \sum_i \underbrace{t_i}_{\in K[X_1, \dots, X_n]} \underbrace{a_i}_{\in I} \in I$$

α surjective let $\frac{a_i}{b_i} \in \mathcal{O}_{\mathbb{A}^n, P_i}$, $b(P_i) \neq 0$.

Take t_i as before.

Let $f := \sum_i t_i a_i \mod m_{P_i}^d$ for all i

$\Rightarrow f \equiv \sum t_i a_i \mod I\mathcal{O}_{\mathbb{A}^n, P_i}$ for all i.

$\square$

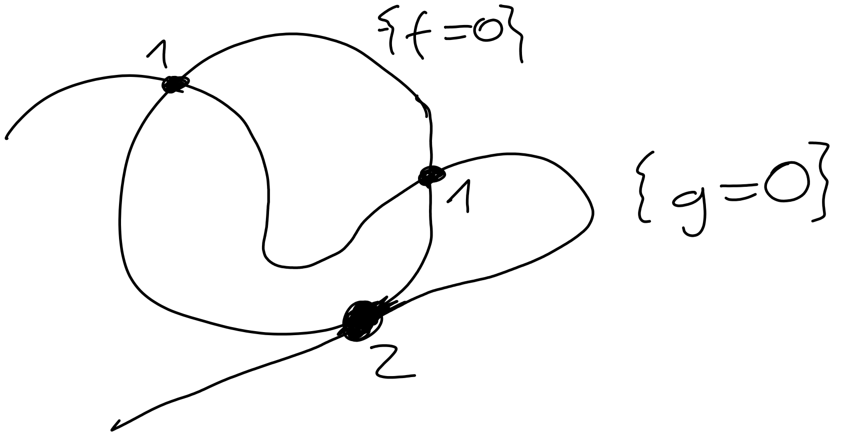
4.5. Intersection numbers

Def The intersection number of

$f \in k[X,Y]$ and $g \in k[X,Y]$ at $P \in k^2$ is

$$I_P(f,g) := m_P((f,g))$$

$$= \mathcal{O}_{\mathbb{A}^2, P} / (f,g)\mathcal{O}_{\mathbb{A}^2, P} \in \mathbb{Z}_{\geq 0} \cup \{\infty\}.$$



Lemma 4.5.1

a) $I_P(f,g)=0 \Longleftrightarrow P \notin V(f,g)$

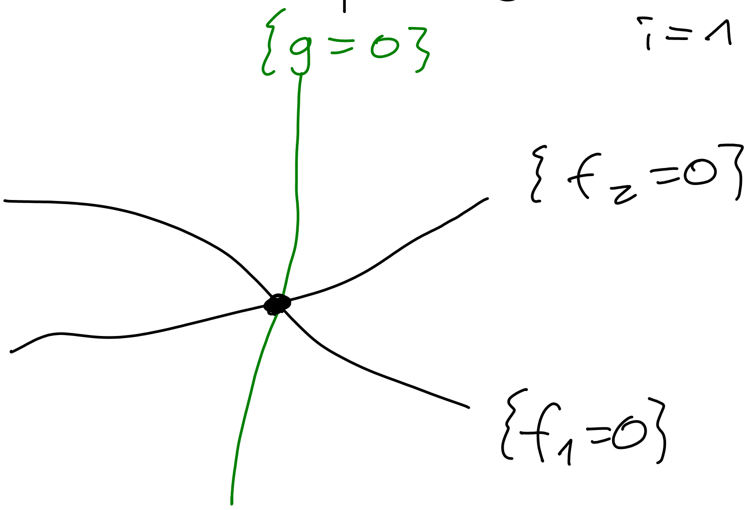
b) $I_P(f,g)=\infty \Longleftrightarrow$ P is contained in an irred. comp. of $V(f,g)$ of dimension ≥ 1

$\Longleftrightarrow h(P)=0$ for $h=\gcd(f,g)$.

Lemma 4.5.3

Let $f=f_1 \cdots f_n$ and $g=g_1 \cdots g_m$.

Then, $I_P(f,g)=\sum_{i=1}^{n}\sum_{j=1}^{m} I_P(f_i,g_j)$.



Pf By induction, it suffices to show that $I_P(f_1 f_2, g)=I_P(f_1,g)+I_P(f_2,g)$.

W.l.o.g., $h(P) \neq 0$ for $h = \gcd(f_1 f_2, g)$

(Otherwise, both sides are ∞.)

Consider the following maps

$$\begin{tikzcd}
0 \arrow[r] & \mathcal{O}_{\mathbb{A}^2,P}/(f_1,g)\dots \arrow[r, "\alpha"] & \mathcal{O}_{\mathbb{A}^2,P}/(f_1f_2,g)\dots \arrow[r, two heads, "\beta"] & \mathcal{O}_{\mathbb{A}^2,P}/(f_2,g)\dots \arrow[r] & 0
\end{tikzcd}$$

$[h] \longmapsto [f_2 h]$

(well-def. because $f_2(f_1,g) \subseteq (f_1 f_2, g)$)

$[h] \longmapsto [h]$

(well-def. because $(f_1f_2,g) \subseteq (f_2,g)$)

<u>β is surjective</u>: clear

<u>α is injective</u>:

Let $h \in \mathcal{O}_{\mathbb{A}^2,P}$ with $f_2 h \in (f_1 f_2, g)\mathcal{O}_{\mathbb{A}^2,P}$,

so $f_2 h = f_1 f_2 a + g b$ with $a, b \in \mathcal{O}_{\mathbb{A}^2,P}$.

Let $d \in K[X,Y]$ be the least common multiple of the denominators of h, a, b,

so $h = \frac{\tilde{h}}{d}$, $a = \frac{\tilde{a}}{d}$, $b = \frac{\tilde{b}}{d}$ with

$\tilde{h}, \tilde{a}, \tilde{b} \in K[X,Y]$. Since the denom. must be $\neq 0$ at P, we have $d(P) \neq 0$ as well.

$$\Rightarrow f_2 \tilde{h} = f_1 f_2 \tilde{a} + g \tilde{b}$$

$$\Rightarrow f_2(\hat{h} - f_1 \hat{a}) = g \tilde{b}$$

$$\Rightarrow g \mid f_2(\tilde{h} - f_1 \hat{a}) \text{ in } k[x,y]$$

Let $r = \cancel{\gcd}(f_2, g)$. $\Rightarrow r(P) \neq 0$

$$\Rightarrow \frac{g}{r} \mid \hat{h} - f_1 \tilde{a} \text{ in } k[x,y]$$

Write $\hat{h} - f_1 \hat{a} = \frac{g}{r} \cdot s$ with $s \in k[x,y]$.

$$\Rightarrow h = \frac{\tilde{h}}{d} = \frac{f_1 \tilde{a} + \frac{g}{r} \cdot s}{d} = f_1 \cdot \frac{\tilde{a}}{d} + g \cdot \frac{s}{rd}$$

$$\in (f_1, g)\mathcal{O}_{\mathbb{A}^2,P}$$

$$\uparrow$$

$$\boxed{\begin{array}{l} d(P) \neq 0 \Rightarrow \frac{\tilde{a}}{d} \in \mathcal{O}_{\mathbb{A}^2,P} \\ r(P) \neq 0 \Rightarrow \frac{s}{rd} \in \mathcal{O}_{\mathbb{A}^2,P} \end{array}}$$

$\Rightarrow h$ is zero in $\mathcal{O}_{\mathbb{A}^2,P} / (f_1, g)\mathcal{O}_{\mathbb{A}^2,P}$.

$\underline{\operatorname{im}(\alpha) = \ker(\beta):}$

"$\subseteq$" $f_2 h \in (f_2, g)\mathcal{O}_{\mathbb{A}^2,P}$ $\forall h \in \mathcal{O}_{\mathbb{A}^2,P}$

"$\supseteq$" Let $h \in \mathcal{O}_{\mathbb{A}^2,p}$ with $h \in (f_2, g)\mathcal{O}_{\mathbb{A}^2,p}$,

so $h = f_2 a + g b$ with $a, b \in \mathcal{O}_{\mathbb{A}^2,p}$.

$\Rightarrow h \equiv f_2 a \mod (f_1 f_2, g)\mathcal{O}_{\mathbb{A}^2,p}$,

so $h \in \mathrm{im}(\alpha)$.

Summary:

$$\dim(\mathrm{im}(\beta)) = \dim\left(\mathcal{O}_{\mathbb{A}^2,p} / (f_2, g)\mathcal{O}_{\mathbb{A}^2,p}\right)$$
$$= I_p(f_2, g)$$

$$\dim(\ker(\beta)) = \dim(\mathrm{im}(\alpha))$$
$$= \dim\left(\mathcal{O}_{\mathbb{A}^2,p} / (f_1, g)\mathcal{O}_{\mathbb{A}^2,p}\right)$$
$$= I_p(f_1, g)$$

$$\dim(\text{domain of } \beta) = \dim\left(\mathcal{O}_{\mathbb{A}^2,p} / (f_1 f_2, g)\mathcal{O}_{\mathbb{A}^2,p}\right)$$
$$= I_p(f_1 f_2, g)$$

$$\dim(\text{domain}) = \dim(\mathrm{im}) + \dim(\ker).$$

$\square$

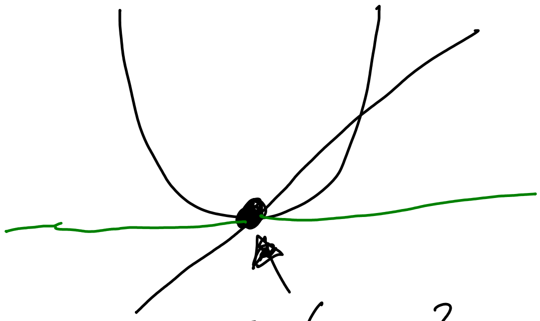
Def Let $0 \neq f, g \in K[x,y]$ be irreducible. Then, $V(f)$ and $V(g)$ intersect transversally at a point $P \in V(f,g)$ if

$$m_P(f) = m_P(g) = 1$$

and the tangent spaces of $V(f)$ and $V(g)$ at P (which are one-dimensional vector spaces) have "trivial" intersection $\{0\}$.

Thm 4.5.2 $I_P(f,g) = 1$ if and only if $V(f), V(g)$ intersect transversally at P.

Ex $V(y-x^2)$, $V(y-x)$ intersect transversally at $(0,0)$.



$$I_0(y-x^2, y-x) = I_0(x-x^2, y-x)$$

$I_P(f,g)$ only depends on the ideal (f,g)

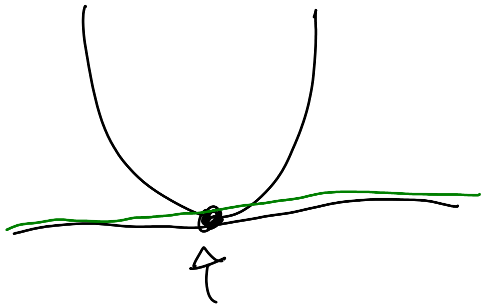
$(y-x^2, y-x) = (y-x^2-(y-x), y-x)$

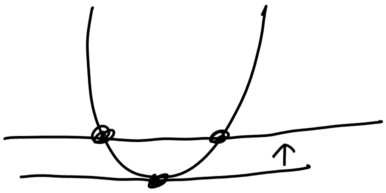
$$= I_0(x(1-x), y-x) = I_0(x, y-x) + I_0(1-x, y-x)$$

$$= I_0(x,y) + \underset{\uparrow \atop (0,0)\notin V(1-x,\,y-x)}{0}$$

$$= \dim_k \left(\mathcal{O}_{\mathbb{A}^2,0} \Big/ (x,y)\mathcal{O}_{\mathbb{A}^2,k} \right) = 1$$

Ex $V(y-x^2)$, $V(y)$ don't intersect transversally at $(0,0)$

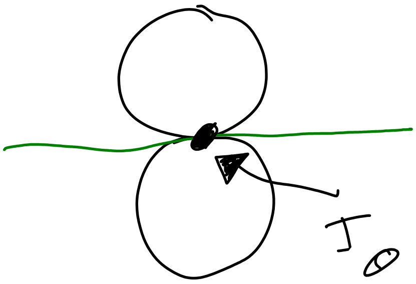




$$I_0(y-x^2, y) = I_0(x^2, y)$$
$$= 2\, I_0(x,y) = 2$$

Ex $V(\underbrace{x^2+(y-1)^2-1}_{x^2+y^2-2y})$, $V(\underbrace{x^2+(y+1)^2-1}_{x^2+y^2+2y})$

don't - - -



$$I_0(\dots) = I_0(x^2+y^2-2y,\ y)$$
$$= I_0(x^2, y) = 2 I_0(x,y) = 2.$$

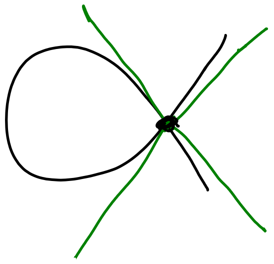
More generally:

Thm 4.5.3 Assume that $h(P) \neq 0$ for $h = \gcd(f, g)$.

Then:

a) $I_P(f,g) \geq m_P(f) \cdot m_P(g)$

b) $I_P(f,g) = m_P(f) \cdot m_P(g)$ if and only if the tangent cones of $V(f)$ and $V(g)$ have "trivial" intersection (no tangent lines in common).



Pf W.l.o.g. $P = (0,0)$.

Let $r = m_P(f)$, $s = m_P(g)$

and $m_P = (X,Y)$ the max. ideal corr. to P.

Consider the following maps:

$$\begin{tikzcd}
K[X,Y]/m_P^s \times K[X,Y]/m_P^r \arrow[r, "\alpha"] & K[X,Y]/m_P^{r+s} \arrow[r, "\beta"] & K[X,Y]/(m_P^{r+s}+(f,g)) \arrow[d, "\sim"', "\text{by pf of Thm 4.4.7 because } V(m_P^{r+s}+(f,g))=\{P\}"] \\
(a,b) \arrow[r, mapsto] & fa+gb & \\
& \mathcal{O}_{\mathbb{A}^2,P}/(f,g)\mathcal{O}_{\mathbb{A}^2,K} \arrow[r, two heads] & \mathcal{O}_{\mathbb{A}^2,P}/(m_P^{r+s}+(f,g))\mathcal{O}
\end{tikzcd}$$

We have $\operatorname{im}(\alpha) = \ker(\beta)$

$$I_p(f,g) = \dim\left(\mathcal{O}_{\mathbb{A}^2,p}/(f,g)\mathcal{O}_{\mathbb{A}^2,p}\right)$$

$$\overset{(I)}{\geq} \dim\left(\mathcal{O}_{\mathbb{A}^2,p}/(m_p^{r+s}+(f,g))\mathcal{O}_{\mathbb{A}^2,p}\right)$$

$$= \dim\left(k[X,Y]/(m_p^{r+s}+(f,g))\right)$$

$$= \dim\left(k[X,Y]/m_p^{r+s}\right) - \dim(\ker(\beta))$$

$$= \quad \text{''} \quad - \dim(\operatorname{im}(\alpha))$$

$$\overset{(II)}{\geq} \quad \text{''} \quad - \dim\left(k[X,Y]/m_p^{s}\right) - \dim\left(k[X,Y]/m_p^{r}\right)$$

$$= \underset{\substack{\uparrow \\ \#\,\text{mon. in } X,Y \\ \text{of deg.} < r+s}}{\binom{r+s+1}{2}} - \underset{\substack{\uparrow \\ \#\,\text{mon.} \\ \text{of deg} \leq s}}{\binom{s+1}{2}} - \underset{\substack{\uparrow \\ \#\,\text{mon.} \\ \text{of deg.} < r}}{\binom{r+1}{2}}$$

$$= \frac{(r+s+1)(r+s) - (s+1)s - (r+1)r}{2} = rs$$

$= m_p(f)\, m_p(g)$. This shows a).

For b):

Equality in (I) $\iff (f,g)\mathcal{O}_{\mathbb{A}^2,p} = (m_p^{r+s} + (f,g))\mathcal{O}_{\mathbb{A}^2,p}$

$\iff m_p^{r+s} \subseteq (f,g)\mathcal{O}_{\mathbb{A}^2,p}$

Equality in (II) $\iff$ $\alpha : K[x,y]/m_p^s \times K[x,y]/m_p^r \to K[x,y]/m_p^{r+s}$

$(a,b) \mapsto fa+gb$

is injective

Claim 2: α is injective if and only if the tangent cones of $V(f)$ and $V(g)$ have trivial intersection $\{0\}$

Pf "$\Rightarrow$" Assume that they have nontriv intersection.

$\Rightarrow$ The hom. pol. $in(f)$, $in(g)$ of degrees r, s have a linear factor L in common.

$$\Rightarrow \alpha\left(\frac{in(g)}{L}, -\frac{in(f)}{L}\right) = f \cdot \frac{in(g)}{L} - g \cdot \frac{in(f)}{L}$$

$$\equiv f \cdot \frac{g}{L} - g \cdot \frac{f}{L} + \underbrace{f \cdot \frac{in(g)-g}{L} - g \cdot \frac{in(f)-f}{L}}_{\text{only has mon. of deg.} \geq r+s}$$

$$\equiv 0 \mod m_p^{r+s}$$

On the other hand,

$\frac{in(g)}{l}$ has mon. of deg. $s-1$,

so $\frac{in(g)}{l} \neq 0$ in $k(x,y)/m_p^s$.

$\Rightarrow$ α is not injective.

"$\Leftarrow$" If they have triv. intersection, then $in(f)$, $in(g)$ have no common factors.

Let $(a,b) \in \ker(\alpha)$, so

$fa + gb \in m_p^{r+s}$.

If $a \notin m_p^s$, $b \notin m_p^r$, then

the lowest degree parts of

fa and gb have degrees

$< r+s$.

Hence, they need to cancel in $fa+gb$ (since $fa+gb \in m_p^{r+s}$).

$$\Rightarrow \underset{in(f)\,in(a)}{\underset{\shortparallel}{in(fa)}} = - \underset{-in(g)\,in(b)}{\underset{\shortparallel}{in(gb)}}$$

Because $\mathrm{in}(f)$, $\mathrm{in}(g)$ are relatively prime, this implies that $\mathrm{in}(f) \mid \mathrm{in}(b)$ and $\mathrm{in}(g) \mid \mathrm{in}(a)$, so in particular $m_p(b) \geq m_p(f) = r$ and $m_p(a) \geq m_p(g) = s$.

$\lightning$ because $a \notin \mathfrak{m}_p^s$, $b \notin \mathfrak{m}_p^r$. $\square$

(Claim 2)

Claim 1: $m_P^{r+s} \subseteq (f,g)\mathcal{O}_{\mathbb{A},P}$ if the tangent cones of $V(f)$ and $V(g)$ at P have intersection $\{0\}$.

Pf Let h be a polynomial which vanishes at every point in $V(f,g)\setminus\{P\}$ but not at P.

(exists by CRT!)

$$\Rightarrow h\cdot m_P \subseteq I(V(f,g)) = \sqrt{(f,g)}$$

$$\Rightarrow (h\cdot m_P)^t \subseteq (f,g) \text{ for suff. large } t.$$

$$\underset{\substack{\uparrow\\ h\in\mathcal{O}_{\mathbb{A},P}^{\times}}}{\Longrightarrow} \quad m_P^t \subseteq (f,g)\mathcal{O}_{\mathbb{A},P} \quad \text{''} \;—$$

We now use downward induction to show this for all $t \geq r+s$.

Assume $t \geq r+s$ and for all $t' > t$, we have $m_P^{t'} \subseteq (f,g)\mathcal{O}_{\mathbb{A},P}$.

Denote the space of hom. deg. d pol. in $K[X,Y]$ by R_d.

We obtain a map

$$\alpha : R_{t'-r} \times R_{t'-s} \longrightarrow R_{t'}$$

$$(a, b) \longmapsto in(f)a + in(g)b$$

Since the tangent cones have intersection $\{0\}$, the pol. $in(f)$, $in(g)$ are relatively prime. Hence, the kernel of α is $\{(in(g)q, -in(f)q) \mid q \in R_{t'-r-s}\}$ $\cong R_{t'-r-s}$.

But $\dim(R_{t'-r}) + \dim(R_{t'-s}) - \dim(R_{t'-r-s})$

$= (t'-r+1) + (t'-s+1) - (t'-r-s+1)$

$= t'+1 = \dim(R_{t'})$ for $t' \geq r+s$.

Hence, α is surjective for $t' \geq r+s$.

$\Rightarrow$ Any $q \in m_p^t$ can be written as

$q = in(f)a + in(g)b$ with $a, b \in K[X, Y]$ with $m_p(a) \geq t-r$, $m_p(b) \geq t-s$.

$$\Rightarrow q = \underbrace{fa + gb}_{\in (f,g)\mathcal{O}_{\mathbb{A},P}} - \underbrace{(f - in(f))a - (g - in(g))b}_{m_p(\cdot) \geq t+1}$$

$$\underset{\substack{\uparrow \\ \text{induction}}}{\in} (f,g)\,\mathcal{O}_{\mathbb{A}^2,P}.$$

$\square$ (Claim 1)

$\square$ (Thm)

4.6. Bézout's Theorem

We define intersection numbers in $\mathbb{P}^2$ by looking at affine patches.

Def Let $f, g \in K[X,Y,Z]$ be homogeneous. Let $\varphi : K^2 \xrightarrow{\sim} U \subset \mathbb{P}^2_K$ be a chart map arising from an identification $\psi : K^2 \xrightarrow{\sim} T \subset K^3$.

Let $\tilde{f} = f \circ \psi$, $\tilde{g} = g \circ \psi$

(so $\varphi^{-1}(V_{\mathbb{P}^2}(f)) = V_{K^2}(\tilde{f})$,

$\varphi^{-1}(V_{\mathbb{P}^2}(g)) = V_{K^2}(\tilde{g})$).

The intersection number of f, g at $P \in U$ is $I_P(f,g) := I_{\varphi^{-1}(P)}(\tilde{f}, \tilde{g})$.

Thm 4.6.1 The intersection number $I_P(f,g)$ depends only on f, g, P, not on φ, ψ.

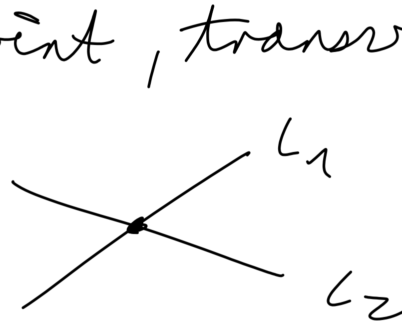
Rmk The intersection number is invariant under projective transformations.

Thm 4.6.2 (Bézout)

Let $f, g \in K[X,Y,Z]$ be hom. of degrees m, n. If $V_{\mathbb{P}^2}(f,g)$ is a finite set, then

$$\underbrace{\sum_{P \in \mathbb{P}^2_K} I_P(f,g)}_{\text{"number of points in } V_{\mathbb{P}^2}(f) \cap V_{\mathbb{P}}(g) \text{ with multiplicity"}} = m \cdot n.$$

Ex Any two lines $L_1 \neq L_2$ in $\mathbb{P}^2_K$ intersect in exactly one point, transversally ($m = n = 1$).



__Ex__ Let $g = Z$. $\rightsquigarrow$ $\underset{\overset{\wr\wr}{\mathbb{P}^1_K}}{V_{\mathbb{P}^2}(g)}$ is a line in $\mathbb{P}^2_K$.

$f(X,Y,0) \in K[X,Y]$ is hom. of deg. m.

Unless $f(X,Y,0) \neq 0$, this pol. has exactly m roots (with mult) in $\mathbb{P}^1 = V_{\mathbb{P}^2}(g)$.

__Ex__ Assume $\operatorname{char}(K) \neq 2$.

$$f = X^2 + (Y-Z)^2 - Z^2 = X^2 + Y^2 - 2YZ$$

$$g = X^2 + (Y+Z)^2 - Z^2 = X^2 + Y^2 + 2YZ$$

$$V_{\mathbb{P}^2}(f,g) = \{[0:0:1], [1:i:0], [1:-i:0]\}$$

$$I_{[0:0:1]}(f,g) = 2$$

$$I_{[1:\pm i:0]}(f,g) = 1$$

__Cor 4.6.3__ If $\# V_{\mathbb{P}^2}(f,g) > mn$ for hom f,g of degrees m,n, then $\# V_{\mathbb{P}^2}(f,g) = \infty$.

__Cor 4.6.4__ Let $S \subset \mathbb{P}^2_K$ be a finite set of points which don't all lie on the same line. If $\# S$ is a prime number, then there are no curves $V_{\mathbb{P}^2}(f)$, $V_{\mathbb{P}^2}(g)$ that intersect exactly in the points of S with intersection number 1 at each point in S.

<u>Pf of Thm 4.6.2</u> Assume f, g are nonconstant.

Consider the standard affine chart

$$\begin{aligned} \varphi : K^2 &\xrightarrow{\sim} U \subset \mathbb{P}^2 . \\ (x,y) &\longmapsto [x:y:1] \end{aligned}$$

W.l.o.g. $V_{\mathbb{P}^2}(f,g) \subseteq U$, so all common roots $[x:y:z]$ of f, g have $z \neq 0$.

$\Rightarrow f, g$ aren't divisible by Z

$\Rightarrow \tilde{f}(X,Y) = f(X,Y,1) \in K[X,Y]$,

$\tilde{g}(X,Y) = g(X,Y,1) \in K[X,Y]$

have degrees m, n.

$$\Rightarrow \sum_{P \in \mathbb{P}^2} I_P(f,g) = \sum_{P \in K^2} I_P(\tilde{f}, \tilde{g})$$

$$\underset{\uparrow \ \boxed{\text{Thm } 4.4.6}}{=} \dim_K\left(K[X,Y] / (\tilde{f}, \tilde{g}) \right).$$

Let $R = K[X,Y,Z]$, $R_d = \{h \in R \text{ hom. of deg. } d\}$

$$\Gamma = R/(f,g), \quad \Gamma_d = R_d/(R_d \cap (f,g)).$$

<u>Claim 1</u> $\dim(\Gamma_d) = mn$ for $d \geq m+n$.

<u>Pf</u> Consider the following maps:

$$\begin{tikzcd} R_{d-m-n} \arrow[r, hook, "\alpha"] & R_{d-m} \times R_{d-n} \arrow[r, "\beta"] & R_d \arrow[r, two heads, "\pi"] & \Gamma_d \end{tikzcd}$$

$$h \mapsto (gh, -fh)$$

$$r \mapsto r \bmod (f,g) \cap R_d$$

$$(a,b) \longmapsto fa + gb$$

$$\ker(\pi) = \operatorname{im}(\beta), \quad \ker(\beta) = \operatorname{im}(\alpha)$$

$$\Rightarrow \dim(\Gamma_d) = \dim(R_d) - \dim(R_{d-m}) - \dim(R_{d-n}) + \dim(R_{d-m-n})$$

$$\underset{d \geq m+n}{=} \binom{d+2}{2} - \binom{d-m+2}{2} - \binom{d-n+2}{2} + \binom{d-m-n+2}{2}$$

$$= mn.$$

$\square$ (Claim 1)

Claim 2 The map $\Gamma_d \longrightarrow \Gamma_{d+1}$

$r \longmapsto r\cdot z$

is injective for all $d \geq 0$

(hence an isom., for all $d \geq m+n$).

Pf Let $r\cdot z = fa+gb$ with

$a \in R_{d+1-m}$, $b \in R_{d+1-n}$.

$\Rightarrow 0 = f(x,y,0)\,a(x,y,0) + g(x,y,0)\,b(x,y,0)$

Since f, g have no common zeros $(x:y:z)$ with $z=0$, the pol. $f(x,y,0), g(x,y,0)$ must be relatively prime.

$\Rightarrow$ We have $a(x,y,0) = g(x,y,0)\,h(x,y)$

$b(x,y,0) = -f(x,y,0)\,h(x,y)$

for some $h \in k[x,y]$.

$$\Rightarrow \quad a \equiv g\cdot h \mod z$$

$$b \equiv -fh \mod z$$

$$\Rightarrow r = \frac{fa+gb}{z} = \frac{f(a-gh)+g(b+fh)}{z}$$

$$= f\cdot \underbrace{\frac{a-gh}{z}}_{\in k(x,y,z)} + g\cdot \underbrace{\frac{b+fh}{z}}_{\in k(x,y,z)} \in (f,g).$$

$\Rightarrow r = 0$ in Γ_d. $\square$

(Claim 2)

__Claim 3__ The map $\Gamma_d \longrightarrow K[X,Y]/(\tilde{f}, \tilde{g})$

$$r \longmapsto r(X,Y,1)$$

is a vector space isomorphism for $d \geq m+n$.

__Pf__ __inj__: Let $r(X,Y,1) = f(X,Y,1)\tilde{a}(X,Y) + g(X,Y,1)\tilde{b}(X,Y)$

with $\hat{a}, \hat{b} \in K[X,Y]$.

Let $a, b \in K[X,Y,Z]$ be homogenisations so that $\tilde{a}(X,Y) = a(X,Y,1)$, $\tilde{b}(X,Y) = b(X,Y,1)$.

Then, $Z^i r = Z^j fa + Z^k gb$ for some $i,j,k \geq 0$ (to make both sides hom. of the same degree).

$\Longrightarrow Z^i \cdot r = 0$ in Γ_{d+i}.

$\underset{\substack{\uparrow \\ \text{Claim 2}}}{\Longrightarrow} \quad r = 0$ in Γ_d.

surj.: Let $\tilde{s} \in K[X,Y]$ and let $s \in K[X,Y,Z]$ be homogeneous of degree $d+t$ $(t \geq 0)$ with $\tilde{s}(X,Y) = s(X,Y,1)$.

Let $r \in \Gamma_d$ be a preimage of s under the isomorphism

$$\Gamma_d \xrightarrow{\sim} \Gamma_{d+t}.$$
$$r \mapsto Z^t \cdot r$$

$\Rightarrow r(X,Y,1) = \tilde{s}$ in $K[X,Y]/(\tilde{f},\tilde{g})$.

$\square$
(Claim 3)

Summary:

$$\sum_{P \in \mathbb{P}^2} I_P(f,g) = \sum_{P \in K^2} I_P(\tilde{f},\tilde{g})$$
$$= \dim\left(K[X,Y]/(\tilde{f},\tilde{g})\right)$$
$$\underset{\substack{\uparrow \\ \text{Claim 3}}}{=} \dim(\Gamma_d) \underset{\substack{\uparrow \\ \text{Claim 1}}}{=} m \cdot n \text{ for } d \geq m+n.$$

$\square$

Ese Let $a_1, \dots, a_m$ be lines in $\mathbb{P}^2$

$b_1, \dots, b_n$ — " —

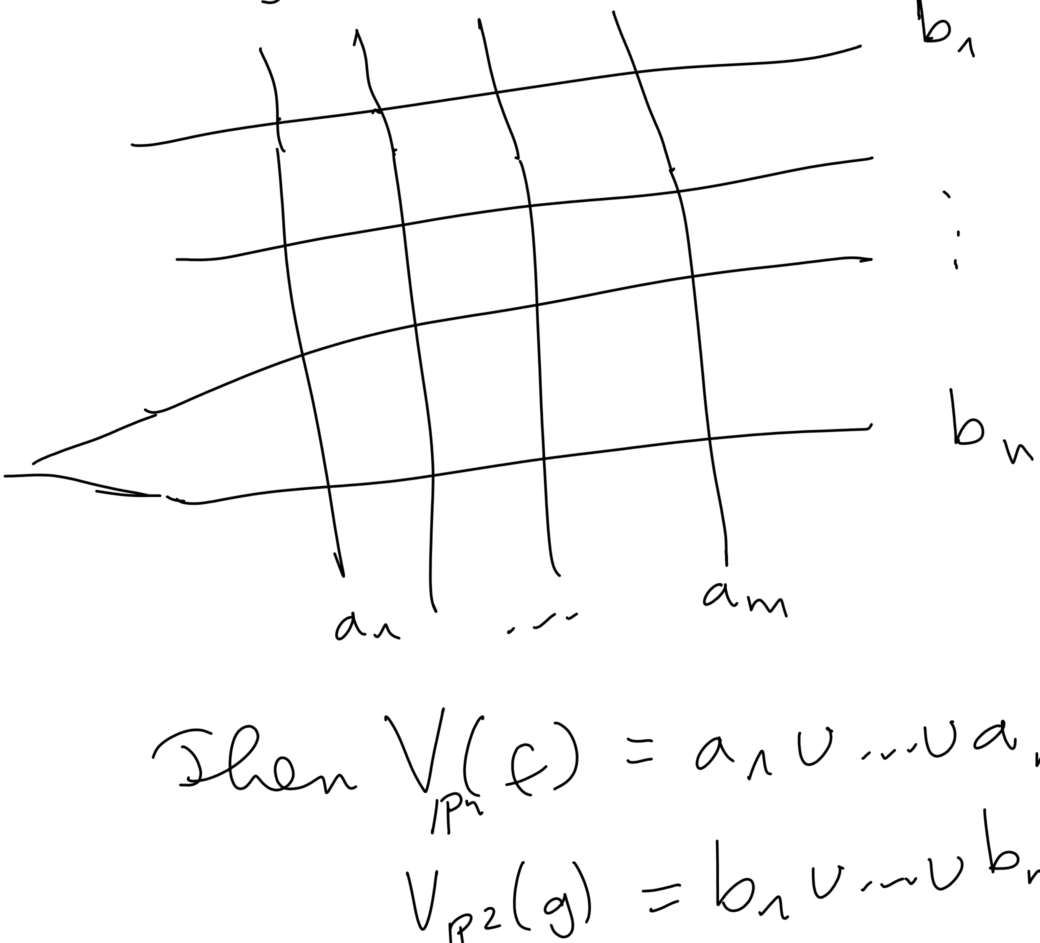
Assume $a_1, \dots, a_m, b_1, \dots, b_n$ are distinct.

Let f be the prod. of the lin. pol. corr. to $a_1, \dots, a_m$.

Let g - - - corr. to $b_1, \dots, b_n$.

$\rightsquigarrow$ f hom. of deg. m,

g — " — n.



Then $V_{\mathbb{P}^2}(f) = a_1 \cup \dots \cup a_m$

$V_{\mathbb{P}^2}(g) = b_1 \cup \dots \cup b_n$,

$\Rightarrow V_{\mathbb{P}^2}(f, g) = V_{\mathbb{P}^2}(f) \cap V_{\mathbb{P}}(g)$ consists of at most mn points.

Es $f = (\text{lin. pol})^m$, $g = (\text{lin. pol.})^n$.