M277 Algebraic Geometry Notes.

Based on the 2014 spring lectures by
Dr A Yafeav.

15/01/13

Algebraic geometery

Andrei Yafaev. yafaev@math.ucl.ac.uk.

Office hour : Friday 11 - 12.

Coursework : Friday → Wednesday. (5 - 6 coursework)

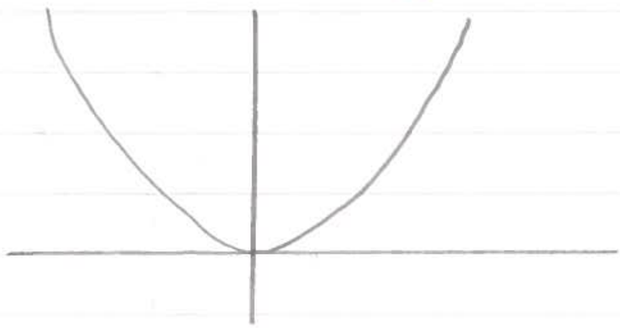
Textbook : W. Fulton "Algebraic curves"
www.math.lsa.umich.edu/~wfulton.

Introduction:
Algebraic geometry = study of "algebraic sets" = those defined by polynomials in serval variables.

ex: $F(x,y) = y - x^2$.

$$V = \{ (x,y) \in \mathbb{R}^2 : F(x,y) = 0 \}.$$

is an example of an algebraic set.



k a field

$k[x_1,\dots,x_n] = \{ \sum_{\text{finite}} a_{i_1 \dots i_n} x_1^{i_1} \dots x_n^{i_n} \}$

$F_1,\dots,F_r \in k[x_1,\dots,x_n]$

$V = \{ (x_1,\dots,x_n) : F_1(x_1 \dots x_n) = \dots = F_r(x_1 \dots x_n) = 0 \}$

is an algebric subset of k^n

<u>$n=2$, $r=1$</u>

$F \in k[x,y]$

$V(F) = \{ (x,y) \in k^2 : F(x,y) = 0$

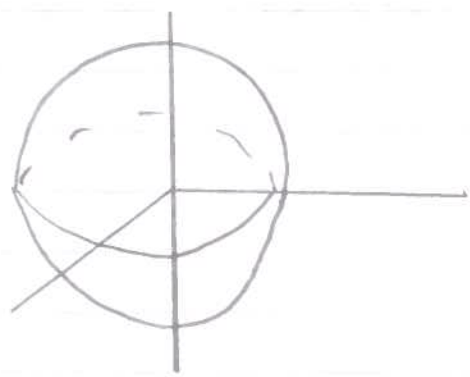
algebraic curve

<u>$n=3$. $r=1$</u>

$F \in k[x,y,z]$

$V(F)$ is an algebraic surface

ex: $k = \mathbb{R}$, $F = x^2+y^2+z^2-1$.



Remark

<u>Rk</u> if $k = \mathbb{R}$, $F = x^2 + y^2 + 1$

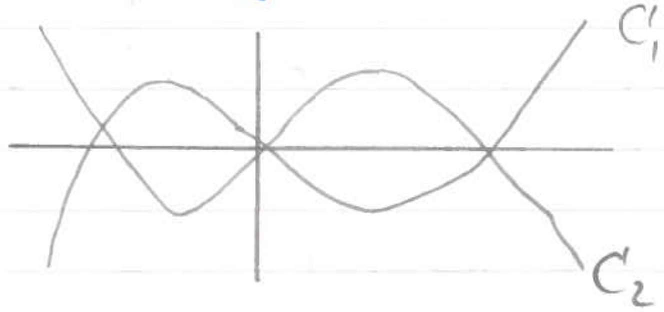
$V(F) = \emptyset$ $= \{(x,y) \in \mathbb{C}^2 : F(x,y) = 0\}$

but if $k = \mathbb{C}$, $V(F)$ consists of infinitely many points

<u>Reason</u>: Fix any $x \in \mathbb{C}$, then $x^2 + y^2 + 1 = 0$ has a root $y \in \mathbb{C}$.

<u>Aim of the course</u> = prove "Bézout's theorem"
k^2, $V(F) = C_1$, $V(G) = C_2$

$F, G \in k[x,y]$



At how many points C_1 and C_2 intersect?

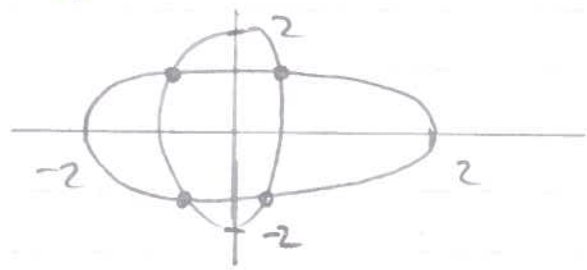
<u>Ex 1</u>: $k = \mathbb{R}$ $F = x^2 + y^2 - 1$, $\deg F = 2$
$G = y - x$, $\deg G = 1$

Exactly 2 points of intersection.
its also $\deg(F) \cdot \deg(G)$.

$\underline{Ex2}$: $k = \mathbb{R}$, $F = x^2 + \frac{y^2}{4} - 1$

$$G = \frac{x^2}{4} + y^2 - 1$$

$\deg F = 2 = \deg G$.



4 points of intersection $= (\deg F) \cdot (\deg G)$

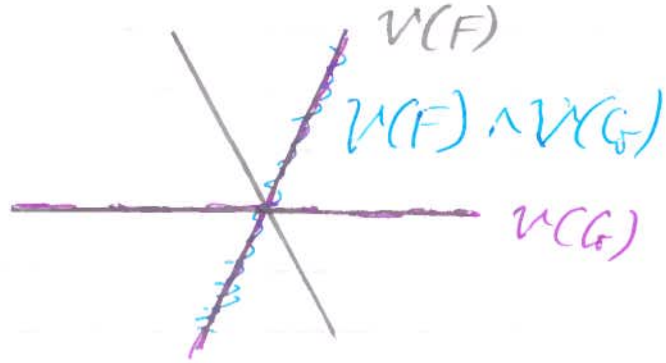
One may conjecture that $|C \cap C'|$ is always $(\deg F) \cdot (\deg G)$.

This is $\underline{\text{false}}$ in general

① $F = y - x$

$G = y(y-x)$

$V(F) \cap V(G) = V(F)$



is infinite.

$\Rightarrow$ Need a condition that $V(F)$ and $V(G)$ have no "common component"

② $k = \mathbb{R}$ $\quad F(x,y) = x^2 + y^2 - 1$
$\quad\quad\quad\quad\quad G(x,y) = x - 2$

$$V(F) \cap V(G) = \emptyset$$

But if $k = \mathbb{C}$, $V(F) \cap V(G) = (2, \pm\sqrt{3})$
Need an assumption that k is alg. closed
if any $F \in k[x]$ - has a root in k.

—/—

ex:

$k = \mathbb{C}$ is alg closed (F.T.A)
$\quad\ \cup$
$k = \overline{\mathbb{Q}} = \{ \alpha \in \mathbb{C} : \exists f \in \mathbb{Q}[x], f(\alpha) = 0 \}$

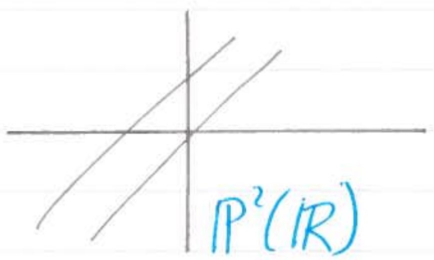
$$\overline{\mathbb{F}}_p = \bigcup_{q = p^n} \mathbb{F}_q$$

$\mathbb{R}$ is not alg. closed. $(x^2 + 1 = 0)$

③ $k = \mathbb{C}$

$$F = y - x, \quad G = y - x - 1$$

Do not intersect in $\mathbb{C}^2$



One needs to "compute" k^2 by adding points at ∞
$k^2 \subset \mathbb{P}(k)$

④ $F = x^2 + y^2 - 1$.
$G = x - 1$.

$$V(F) \cap V(G) = \{ x = 1,\ y^2 = 0 \}$$
$$= \{ (1, 0) \}$$

One needs to define $I(P, F, G)$ at a point P which will be called "multiplicity of intersection at P" or "intersection number" if $P \in V(F) \cap V(G)$ then $I(P, F, G)$.

Bézout's theorem.
Let k be a algebraically closed field. Let C_1, C_2 be two plane projective curve with no common component.

$$\sum_P I(P, C_1, C_2) = (\deg C_1)(\deg C_2)$$

Rem: Fundamental theorem of algebra: $f \in \mathbb{C}[x]$

$$f = a_n (x - \alpha_1)^{e_1} \dots (x - \alpha_r)^{e_r}$$

α_i's are distinct roots

$$\sum_{i=1}^{n} e_i = \deg(f).$$

—/—

$F = y - f(x) \in \mathbb{C}[x,y]$

$V(F) \cap V(\underbrace{y=0}_{G}) = \{\alpha_1, \ldots, \alpha_r\}$

F.T.A

$\sum \underbrace{e_i}_{\text{multiplicity root } \alpha_i} = (\deg f)(\underbrace{\deg G}_{=1})$

F. T. A = special case of Bézout's thm.

—/—

Chapter 1: Affine algebraic sets.

k is a field $n \geq 0$.

$\mathbb{A}^n(k) = k^n = \{(x_1, \ldots, x_n), x_i \in k\}$
affine space.

Let $k[x_1, \ldots, x_n]$ be the ring of polynomials in $x_1, \ldots, x_n$ with coefficients in k.

$F \in k[x_1, \ldots, x_n]$, $F = \sum_{I} a_I \underbrace{x^I}_{\text{monomials of multidegree } I}$.

$I = \{i_1, \ldots, i_n\}$
$x^I = x_1^{i_1} \ldots x_n^{i_n}$
$a_I \in k$.

$\deg(F) = \max\{i_1 + \ldots + i_r, a_I \neq 0\}$

ex: $F(x,y) = y - x^2 + xy$.

$\deg(F) = 2$.

$\deg(x+y) = 1$

$\deg(x^3+y+1) = 3$

$\deg(1+x^{10}+y) = 10$

$\deg(xy^3 + xy) = 4$

Prop: $\deg(F.G) = \deg F + \deg G$

Rem: $k[x]$ is a P.I.D

$k[x,y]$ is not a P.I.D

(x,y) is not principlal but it's a U.F.D

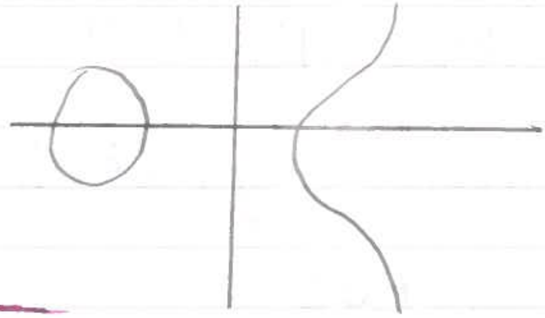
Def: Let $S \subset k[x_1, \dots, x_n]$

$$V(S) = \{(x_1, \dots, x_n) \in k^n : F(x_1, \dots, x_n) = 0 \quad \forall F \in S\}.$$

—/—

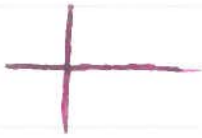
A set of the form $V(S)$ is called an affine algebraic set.

Ex: $\cdot\ V(y^2 - x(x-1))$



elliptic curve

$\cdot\ V(xy)$



$\cdot\ V(x,y) = \left\{ (x,y) \in k^2 : \begin{matrix} x=0, \\ y=0 \end{matrix} \right\} = \{(0,0)\}$

Prop Let I be the ideal generated by S. Then $V(S) = V(I)$

Def: Let R ring, $S \subset R$.

Ideal generated by S is

$$\left\{ \sum_{\text{finite}} r_i x_i \ , \ r_i \in R \ , \ x_i \in S \right\}$$

its the smallest ideal containing S.

Proof of proposition

$S \subset I$. If $P \in V(I)$ then $\forall F \in I$; $F(P) = 0$
Because $S \subset I$, for any $F \in S$

$$F(P) = 0 \ .$$

Hence $P \in V(S)$. $\boxed{V(I) \subset V(S)}$

Conversely, let $P \in V(S')$,

let $F \in I$.

$$F = \sum_{\text{finite}} r_i \cdot x_i \,, \quad r_i \in k[x_1 \dots x_n] \quad x_i \in S'$$

$$F(P) = \sum r_i(P) \cdot \underbrace{x_i(P)}_{=0 \text{ because } P \in V(S)} = 0$$

$\underline{P \in V(I)}$, $V(S) \subset V(I)$

Prop: If $I \subset J$, then $V(J) \subset V(I)$

Proof: Let $P \in V(J)$
$\forall F \in J$, $F(P) = 0$ and as $I \subset J$, for all $F \in I$, $F(P) = 0$.

$$\Rightarrow P \in V(I)$$

Prop: Let $I, J \subset k[x_1 \dots x_n]$ be two ideals.

$$V(I) \cup V(J) = V(I \wedge J)$$

Proof: As $I \wedge J \subset I$, $V(I) \subset V(I \wedge J)$

$I \wedge J \subset J$, $V(J) \subset V(I \wedge J)$

$\Rightarrow V(I) \cup V(J) \subset V(I \wedge J)$

Conversely, let $P \in V(I \wedge J)$ if $P \in V(I)$, then done, if $P \notin V(I)$, then $\exists F \in I$, $F(P) \neq 0$.

Let $G \in J$

$$F \cdot G \in I \wedge J \qquad \cancel{x}^0$$

As $P \in V(I \wedge J)$, $F(P) \cdot G(P) = 0$.

$\Rightarrow G(P) = 0 \Rightarrow P \in V(J)$

$$V(I \wedge J) \subset V(I) \cup V(J)$$

Induction shows that

$$\bigcup_{i=1}^{n} V(I_i) = V\left(\bigcap_{i=1}^{n} I_i\right)$$

only ture for finite unions

Eg $V(xy)$

$$(xy) = (x) \wedge (y)$$

$$V(xy) = V(x) \wedge V(y)$$

<u>Rem</u>: <u>Infinite</u> unions of algebraic sets are in general not algebraic.

$V \subsetneq \mathbb{A}^1(\mathbb{C})$ V infinite subset

$V = \bigcup_{\alpha \in V} \{\alpha\}$. Each $\{\alpha\}$ is an algebraic set, in fact it's $V(x-\alpha)$

V itself is not algebraic:

suppose it was:
$V(I)$, $I \subset \mathbb{C}[x]$
some ideal. I is principle $= (f)$
Then $f(\alpha) = 0$, $\forall \alpha \in V$
As V infinite, $f = 0$
$V(f) = V(0) = \mathbb{A}^1(\mathbb{C})$
<u>contradiction</u> $\square$

<u>Prop</u>: Let $\{I_i\}$ be any collection of ideal

$$\bigcap_i V(I_i) = V(\bigcup_i I_i)$$

<u>Proof</u>: Let $P \in \bigcap_i V(I_i)$

$\forall i$, $P \in V(I_i)$

$\Rightarrow \forall i$, $\forall F \in I_i$, $F(P) = 0$, $\Rightarrow P \in V(\bigcup I_i)$

Conversely: Let $P \in V(\bigcup I_i)$

$\forall F \in \bigcup I_i \ , \ F(P) = 0$

$\Rightarrow P \in \bigcap V(I_i)$

$\square$

Ex: Any finite subset of $\mathbb{A}^n(k)$ is algebraic
Because finite unions are algebraic it's enough to see that $P = (\alpha_1, \dots, \alpha_n)$ is algebraic.
Because $P = V(x_1 - a_1, \dots, x_n - a_n)$

Ex: $V = \{ (t, t^2, t^3) \in \mathbb{A}^3(k), t \in k \}$.

is algebraic

let $(t, t^2, t^3) \in V$. $\begin{cases} x = t \\ y = t^2 = x^2 \\ z = t^3 = x^3 \end{cases}$

$V \subset V(y - x^2, y - x^3)$

Conversely: let $P = (x, y, z) \in V(y - x^2, z - x)$

$y = x^2, \quad z = x^3$

in fact $P = (x, x^2, x^3) \in V$.

Hence $V = V(y - x^2, z - x^3)$

<u>Ex</u>: <u>$k=\mathbb{R}$</u>

$$V=\{(\cos t, \operatorname{sen} t),\ t\in\mathbb{R}\}$$

algebraic set, in fact it's $V(x^2+y^2+1)$

<u>Ex</u>: $V=\{P\in\mathbb{A}^1(\mathbb{R})$, with polar coordinates (r,θ), $r=\operatorname{sen}\theta\}$.

algebraic or not?

$$\begin{cases} x = r\cos\theta \\ y = r\operatorname{sen}\theta \end{cases}$$

$$\boxed{y = r\operatorname{sen}\theta = (\operatorname{sen}\theta)^2 = r^2 = x^2+y^2}$$

$$V\subset V(x^2+y^2-y)$$

Conversely: $(x,y)\in V(x^2+y^2-y)$

$$\begin{cases} x = r\cos\theta \\ y = r\operatorname{sen}\theta \end{cases}$$

$r^2 - r\sin\theta = 0$.

$\Rightarrow r(r - \sin\theta) = 0$.

$\Rightarrow r = \sin\theta$.

$P \in V = V(x^2 + y^2 - y)$

17/1/14

$V(S') \subset \mathbb{A}^n(k)$, $S' \subset k[x_1, \dots, x_n]$

$\{P \in \mathbb{A}^n : F(P) = 0, \forall F \in S'\}$

$V(S) = V(I)$, I = ideal generated by S'.

$V(I) \cup V(J) = V(I \wedge J)$

$V(\bigcup I_i) = \bigcap V(I_i)$

$V(S') = \bigcap_{F \in S'} V(F)$

$\emptyset$, $\mathbb{A}^n$ are algebraic

$\emptyset = V(1)$; $\mathbb{A}^n = V(0)$

—/—

Lemma: Let $C = V(F)$, $F \in k[x,y]$
Let L a line
Then $|L \wedge C| < \deg(F)$

Proof: L: $\overset{\text{Case (1)}}{y - ax + b = 0}$ or $\overset{\text{case (2)}}{x = a}$.
$P = (x,y) \in L \wedge C \iff$ Case (1), $F(x, a+xb) = 0$
Case (2), $F(a, y) = 0$

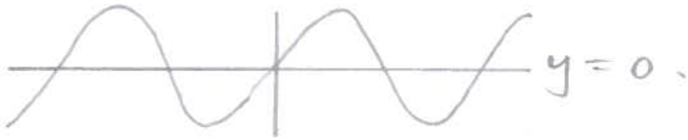
Each equation (1) or (2) has at most $\deg(F)$ solutions. Each of these solutions gives exactly one point

$\square$

Ex of application.

$V = \{(x,y) \in \mathbb{A}^2(\mathbb{R}) : y = \sin(x)\}$.

Is V algebraic ?



Suppose that V was algebraic

$$V = V(S') = \bigcap_{F \in S'} V(F)$$

As $V \neq \mathbb{A}^2(\mathbb{R})$, $\exists F \in S'$ st $F \neq 0$
$F \neq 1$ $(V \neq \emptyset)$

$V \subset V(F)$

Let $L = V(y)$

$$V \cap L \subset V(F) \cap L$$

$$\{(k\pi, 0) : k \in \mathbb{Z}\}.$$

Therefore $V(F) \cap L$ is infinite which contradicts the lemma.

V is not algebraic

$\square$.

Ex: $V = \{(x, e^x),\ x \in \mathbb{R}\}$ not algebraic.

$F \in k[x,y]$, $F(x, e^x) = 0$, $\forall x$

$F = y^n + p_{n-1}(x)\, y^{n-1} + \dots + p_0(x)$.

$p_i \in k[x]$.

$F(x, e^x) = e^{nx} + p_{n-1}(x)\, e^{(n-1)x} + \dots + p_0(x) = 0$

$1 + p_{n-1}(x) e^{-x} + \dots + p_0 e^{-nx} = 0$.

$x \to \infty$ all $p_i(x) e^{(i-n)x} \to 0$

$1 = 0$ contradiction. (This assumes that the leading coeff is 1)

If not; $p_n(x) y^n + \dots + p_0(x) = 0$.

$p_n(x) + \underbrace{(\quad)}_{\to 0}$ $\qquad x^\alpha \left(\frac{p_n}{x^\alpha}\right)(0) \neq 0$.

$\left(\frac{p_n}{x^\alpha}\right) + \underbrace{\frac{p_{n-1}(x)}{x^\alpha e^{-x}} + \dots + \frac{p_0(x)}{x^\alpha}}_{\to 0} = 0$.

$\Rightarrow \left(\frac{p_n}{x^\alpha}\right)(0) = 0$

contradiction

Forget about this!

—/—

Theorem: k algebraically closed field.
$F \in k[x_1, \dots, x_n]$ non-constant polynomial
Then: $\mathbb{A}^n(k) \setminus V(F)$ is infinite
$V(F)$ is also infinite when $n > 1$

Lemma: Any algebraically closed field k is infinite.

Proof: Suppose k is finite, $k = \{\alpha_1, \dots, \alpha_n\}$.
Consider $F = (x - \alpha_1) \dots (x - \alpha_n) + 1 \in k[x]$
$\forall i$, $F(\alpha_i) = 1$
F has no root in k, contradiction.
$\square$.

Lemma: Let k is an infinite field.
$F \in k[x_1, \dots, x_n]$ st $F(a_1, \dots, a_n) = 0$ for all $(a_1, \dots, a_n) \in k^n$. Then $F = 0$.

Proof: Induction on n,

$n=1$ This is known.

Suppose lemma known for n.
Let F a polynomial in $k[x_1, \dots, x_{n+1}]$ st
$F(a_1, \dots, a_{n+1}) = 0$, $\forall a_1, \dots, a_{n+1} \in k^{n+1}$
Write $F = \sum_{i=0}^{r} F_i(x_1 \dots x_n) x_{n+1}^i$

Suppose $\forall (a_1, \dots, a_n)$, $F_i(a_1, \dots, a_n) = 0$
Then by induction assumption, F_i's are 0 and so $F = 0$.

Suppose $\exists i$, $(a_1, \dots, a_n)$ st $F_i(a_1 \dots a_n) \neq 0$

$$\begin{cases} F(a_1, \dots, a_n, a_{n+1}) = 0, \ \forall a_{n+1} \\ F(a_1, \dots, a_n, x_{n+1}) \text{ is a non-zero polynomial.} \end{cases}$$

$\Rightarrow F(a_1, \dots, a_n, x_{n+1}) = 0$ contradiction!

$\square$.

Proof of Theorem:

(1). $\mathbb{A}^n(k) \setminus V(F)$ is infinite.

Suppose it was finite

$$\mathbb{A}^n(k) \setminus V(F) = \{ P_1, \dots, P_r \}$$

$$P_i = (p_i^1, \dots, p_i^n)$$

Consider:

$$G = F \cdot (x_1 - p_1^1) \dots (x_n - p_1^n) \cdot (x_1 - p_2^1) \cdot \dots \cdot (x_2 - p_2^n) \dots (x - p_n^1) \dots (x_n - p_n^n)$$

$\forall i$, $G(P_i) = 0$

$\forall P \in V(F)$, $F(P) = 0 \Rightarrow G(P) = 0$.

$\Rightarrow \forall P \in \mathbb{A}^n(k)$, $G(P) \Rightarrow G = 0$ by lemma

Contradiction!

22/1/14

Theorem. k alg closed field
$F \in k[x_1 \dots x_n]$ non-cst

① $\mathbb{A}^n(k) \setminus V(F)$ infinite
② If $n > 1$, $V(F)$ infinite.

Rem. To prove ① we only used that k is infinite.

Proof of (2)

$$F = \sum_{i=0}^{r} F_i(x_1 \dots x_{n-1}) x_n^i$$

Suppose all F_i's are constant.

Take any $(a_1, \dots, a_{n-1}) \in k^{n-1}$ and a root of (F is a polynomial in 1 var x_n) α
exists because k is alg closed

$(a_1, \dots, a_{n-1}, \alpha) \in V(F)$

There are ∞ many choices for $(a_1, \dots, a_{n-1})$

$\Rightarrow V(F)$ infinite

If some F_i is not constant

By (1), there are infinitely many $(a_1, \dots, a_{n-1})$ $\in k^{n-1}$ st $F_i(a_1 \dots a_n) \neq 0$

For each of those $F(a_1 \ldots a_{n-1}, x_n)$ has a root a and so $(a_1, \ldots, a_{n-1}, a) \in V(F)$
$\Rightarrow V(F)$ is infinite.

$\square$.

<u>Ex</u>: (2) not true if k is not alg. closed
$k = \mathbb{R}$. $F(x,y) = x^2 + y^2 + 1$.

$V(F) = \emptyset$.

but of course $V(F)$ is infinite if $k = \mathbb{C}$.

<u>Ideal of a subset of $\mathbb{A}^n(k)$</u>
Let $X \subset \mathbb{A}^n(k)$ be a subset.

<u>Def</u>: $I(x) = \{ F \in k[x_1 \ldots x_n] : F(P) = 0 \;\; \forall P \in X \}$.

<u>Prop</u>: $I(x)$ is an ideal of $k[x_1 \ldots x_n]$.
<u>Proof</u>
- $0 \in I(x)$
- $F, G \in I(x)$, $(F+G)(P) = \underbrace{F(P)}_{=0} + \underbrace{G(P)}_{=0} = 0 \quad \forall P \in X$

$\Rightarrow F + G \in I(X)$

Let $F \in I(X)$, $G \in k[x_1 \ldots x_n]$
$\forall P \in X$, $(F \cdot E)(P) = \underbrace{F(P)}_{=0} G(P) = 0$.

$F \cdot G \in I[X]$

$\square$

<u>Note</u>:

- $I(\emptyset) = k[x_1 \ldots x_n] = (1)$
- $I(\mathbb{A}^n(k)) = (0)$ when k = infinite field.

(Lemma from last time. $F(a_1, \ldots a_n) = 0$, $\forall (a_1, \ldots, a_n) \in k^n \Rightarrow F = 0$)

- if $k = \mathbb{F}_p$ $\quad I(\mathbb{A}^1(\mathbb{F}_p)) = \prod_{a \in \mathbb{F}_p} (x-a)$

<u>Prop</u>: $X \subset Y \Rightarrow I(Y) \subset I(X)$

<u>Proof</u>:

Let $F \in I(Y)$, $\forall P \in Y$, $F(P) = 0$

In part, $\forall P \in X$, $F(P) = 0 \Rightarrow F \in I(X)$

$\square$

<u>In part</u>: $X = Y \Rightarrow I(X) = I(Y)$

<u>Question</u>: Is it true that $I(X) = I(Y) \Rightarrow X = Y$?

<u>Answer</u> NO. $Y = \mathbb{A}^1(\mathbb{R})$ and $X = \mathbb{Z}$.

We know that $I(Y) = (0)$

$$I(X) = \{F \in \mathbb{R}[x] : F(k) = 0, k \in \mathbb{Z}\}$$

$I(X) = I(Y)$ but $X = Y$

Note:

$\cdot\ I(X \cup Y) = I(X) \cap I(Y)$

$\cdot$ Trival.

(*) $\forall S \in k[x_1, \dots, x_n]$, $S \subset I(V(S))$

Let $F \in S$, $F = 0$ on $V(S)$ by def of $V(S)$

(**) $\forall X \subset \mathbb{A}^n(k)$, $X \subset V(I(X))$

Let $P \in X$, $\forall F \in I(X)$, $F(P) = 0 \Rightarrow V(I(X))$

$\cdot\ \forall S \in k[x_1 \dots x_n]$, $V(S) = V(I(V(S)))$

By (*), $S \subset I(V(S))$

$\Rightarrow V(I(V(S))) \subset V(S)$

By (**) with $X = V(S)$, we got the other inclusion

$\boxed{\text{For an algebraic set } X,\ X = V(I(X))}$

Also, if X is algebraic,

$$I(X) = I(V(I(X)))$$

(apply $I(-)$ to previous equality)

Consequence. If X, Y are algebraic then $X = Y$ $\Leftrightarrow$ $I(X) = I(Y)$

$(\Rightarrow)$ Always true.

$(\Leftarrow)$ $I(X) = I(Y) \Rightarrow \underbrace{V(I(X))}_{= X} = \underbrace{V(I(Y))}_{= Y}$

Q: Is any ideal I of $k[x_1 \dots x_n]$ of the form $I(X)$ with X algebraic

A: NO!

$k[x] \ni (x^2)$ This is not an ideal of an algebraic set.

$V((x^2)) = (0) \in \mathbb{A}^1(k)$

$I(V(x^2)) = I(0) = (x)$ (Eucledian div)

$x \neq x^2$

Contradicts $I = I(V(I))$ if $I = I(X)$

—/—

Let $X \subset \mathbb{A}^n(k)$ subset, suppose $F^m \in I(X)$ for some $m > 0$.

Then $\forall P \in X$, $F^m(P) = 0 \Rightarrow F(P) = 0$
$\Rightarrow F \in I(X)$.

Def: Let R be a ring. $I \subset R$ ideal, I is called radical if whenever $a^m \in I$ $(m > 0) \Rightarrow a \in I$

We have seen that $I(X')$ is always a radical ideal.

Ex: $(x^2) \subset k[x]$ is not radical because $x^2 \in (x^2)$ but $x \notin (x^2)$.

Def: R any ring, $I \subset R$ an ideal. I is prime if whenever $ab \in I \Rightarrow a$ or $b \in I$.

A prime ideal is radical.

Ex: $(x) \in k[x]$ is prime, hence radical
$(x^2+1) \in \mathbb{R}[x]$ is prime.

$$P.Q \in (x^2+1) \Rightarrow P(i)Q(i) = 0.$$

$$\Rightarrow P(i) = 0 \text{ or } Q(i) = 0.$$

Suppose $P(i) = 0$. As $P \in \mathbb{R}[x]$, $P(-i) = 0$

$\Rightarrow x+i, x-i \mid P \Rightarrow x^2+1 \mid P \Rightarrow P \in (x^2+1)$

$\square$

Rem: $(x^2+1) \subset \mathbb{C}[x]$ is not a prime ideal.

$(x+i)(x-i) \in (x^2+1)$
$x+i, x-i \notin (x^2+1)$

$\square$.

Ex / Excercise

- $(x(x-1)) \subset \mathbb{R}[x]$ is radical, not prime.

Def: R ring $I \subset R$ ideal.

$\mathrm{Rad}(I) = \{a \in R,\ a^m \in I \text{ for some } m > 0\}$

Lemma: $\mathrm{Rad}(I)$ is an ideal.

- $0 \in \mathrm{Rad}(I)$
- $a \in \mathrm{Rad}(I)$, $b \in R$.

$a^m \in I$ for some $m > 0$

$(ab)^m = a^m b^m \in I$ because:

I is an ideal
$ab \in \mathrm{Rad}(I)$
$a, b \in \mathrm{Rad}(I)$ $\quad a^m \in I \quad m > 0$
$\qquad\qquad\qquad\quad b^n \in I \quad n > 0$.

$$(a+b)^{m+n} = \sum_{i=0}^{m+n} \binom{m+n}{i} a^i b^{m+n-i}$$

If $i < m$, $b^{m+n-i} \in I \Rightarrow a^i b^{m+n-1} \in I$.
If $i \geq m$, $a^i \in I \Rightarrow a^i b^{m+n-i} \in I$.

$(a+b)^{m+n} \in I$

Rad I is an ideal containing I.

Ex: In $k[x]$

$$\mathrm{Rad}(x^2) = (x)$$

Excercise: prove it.

Theorem: (generalised euclidean division)
Let R any ring.
$P \in R[x]$, $P \neq 0$ such that the leading coefficient of P is a unit. Let $F \in R[x]$. $\exists!(Q, R)$ s.t. $F = QP + R$ and $\deg(R) < \deg(P)$

We will use this when

$$R = k[x_1 \dots x_{n-1}]$$
$$R[x] = k[\underbrace{x_1 \dots x_{n-1},}_{R} x_n] = R[x_n]$$

Ex: In $k[x,y]$, one can divide by $y - x^2$ but not by $xy - 1$.

Ex: $V = \{(t^2, t), t \in k\}$.
k infinite.

Show that V is algebraic, find $I(V)$. We have seen that $V = V(y - x^2)$ so V is algebraic.

$$V = V(y - x^2) \Rightarrow I(V) \supset (y - x^2)$$

Conversely: let $F \in I(V)$

We do euclidean division of F by $y-x^2$ in $k[x][y]$

$$F = (y-x^2)Q + R$$

$\cdot \deg_y(R) < 1$

$\Rightarrow \deg_y(R) = 0 \Rightarrow R \in k[x]$

$F \in I(V)$, $\underset{\underset{0+R(t^2)}{\parallel}}{F(t^2,t)} = 0$, $\forall t \in k$.

$R(t^2) = 0 \quad \forall t \in k$.
k infinite, $R = 0 \Rightarrow F = (y-x^2)Q \in (y-x^2)$
$\underline{I(V) = (y-x^2)}$

Ex: $V = \{(t^3, t^2) \; t \in k\}$.
Show that V is algebraic
$\begin{pmatrix} x = t^3 \\ y = t^2 \end{pmatrix} \qquad V \subset V(y^3 - x^2)$

Conversely let $P = (x,y) \in V(y^3 - x^2)$
Find t st $\begin{cases} x = t^3 \\ y = t^2. \end{cases}$

If $x = 0$, then $y = 0$, take $t = 0$
$y = 0 \Rightarrow x = 0 \Rightarrow t = 0$.

$x, y \neq 0$
Take $t = x/y$.

$$t^3 = \frac{x^3}{y^3} = \frac{x^3}{x^2} = x.$$

because $y^3 = x^2$.

$$t^2 = \frac{x^2}{y^2} = \frac{y^3}{y^2} = y.$$

$V = V(y^3 - x^2)$, V is algebraic.

<u>Calculate $I(V)$</u>

- $(y^3 - x^2) \subset I(V)$
- Let $F \in I(V)$.

Divide F by $y^3 - x^2$ in $k[y][x]$.

$$F = (y^3 - x^2)Q + R \quad , \deg_x R < 2.$$

$R = a(y)x + b(y)$.
Evaluate at (t^3, t^2),

$$a(t^2)t^3 + b(t^2) = 0 \quad , \forall t \in k.$$

We need to show that $a = b = 0$
Write $a(y) = a_n y^n + \dots + a_0$.
$b(y) = b_m y^m + \dots + b_0$.

$$a_n t^{2n+3} + \dots + a_0 t^3 + b_m t^{2m} + \dots + b_0 = 0.$$

All coefficients a_i's appear with odd powers of t, All coeffs b_i's appear with even powers of t.

$\Rightarrow$ a_i's, b_i's are zero $\Rightarrow$ $R = 0$

$\Rightarrow$ $F \in (y^3 - x^2)$

$I(V) = (y^3 - x^2)$

<u>Ex</u>: $V = \{ (t^9, t^6, t^4), t \in k \}$.

k infinite.
Calculate $I(X)$

$V = V(x^2 - y^3, y^2 - z^3)$

$I(V) = \underbrace{(x^2 - y^3, y^2 - z^3)}_{= J} \supset$ always holds.

Let $F \in I(V)$. We need to show that the image $\bar{F}$ of F in $k[x,y,z]/J$ is zero.

Let $\bar{x}, \bar{y}, \bar{z}$ be images of x, y, z in $k[x,y,z]/J$
They satisfy $\bar{x}^3 = \bar{y}^3 = y\bar{z}^3$, $\bar{y}^2 = \bar{z}^3$.

That mean that:

$\bar{F} = \bar{P} + x\bar{R} + \bar{x}\bar{y}\bar{S} + \bar{y}\bar{Q}$

where $P, R, S, Q \in k[\bar{z}]$.

This means that:

$$F - P - xR - xyS' - yQ \in J(x^2 - y^3, y^2 - z^3)$$

Evaluate at (t^9, t^6, t^4)

$$F(t^9, t^6, t^4) = P(t^4) + t^9 R(t^4) + t^{15} S(t^4) + t^6 Q(t^4) = 0$$

In $P(t^4)$ all powers of t are $0 \bmod 4$
In $R(t^4)$ — // — $1 \bmod 4$
In $t^{15} S(t^4)$ — // — $3 \bmod 4$
In $t^6 Q(t^4)$ — // — $2 \bmod 4$.

There is not intersection, $P = R = S' = Q = 0$

$$F = 0 \Rightarrow F \in J.$$

29/1/14

Let $P \in \mathbb{A}^n(k)$, k infinite
Compute $I(P)$ $P = (a_1, \dots, a_n)$

$$I = (x_1 - a_1, \dots, x_n - a_n)$$
$$I \subset I(P).$$

Conversely
Induction on n.

$n=1$ $F \in k[x]$ satisfies $F(a) = 0$
$\iff x - a \mid F$
$\iff F \in (x-a)$

Suppose $I = I(P)$ for $P \in \mathbb{A}^{n-1}(k)$

$P = (a_1, \dots, a_n)$

Let $F \in k[x_1, \dots, x_n]$ st $F(P) = 0$.
Divide by $x_n - a_n$

$$F = (x_n - a_n) Q + R.$$

$\deg_{x_n}(R) < 1 \Rightarrow R \in k[x_1, \dots, x_{n-1}]$

$F(P) = 0 = 0 + R(a_1, \dots, a_{n-1})$

By ind. assumption, $R \in (x_1 - a_1, \dots, x_{n-1} - a_{n-1})$

$\square$

Irreducible algebraic sets.

Def: Let $V \subset \mathbb{A}^n(k)$ be a non-empty algebraic set. V is called reducible if $V = V_1 \cup V_2$ with V_1, V_2 non empty algebraic sets with $V_1 \neq V$ and $V_2 \neq V$.

Def: V is irreducible if it's not reducible.

Ex: · P a point is irreducible.

· $V(xy) = \underbrace{V(x)}_{= V_1} \cup \underbrace{V(y)}_{= V_2}$.

$V(xy)$ is reducible.

· In $\mathbb{A}^1$, take $P = (a)$, $Q = (b)$ $\quad a \neq b$

$$P \cup Q = V((x-a)(x-b)) = V(x-a) \cup V(x-b)$$

reducible.

Def: R ring. $I \subset R$ ideal.
I is prime if $\forall a, b \in I$ st $ab \in I$, either a or $b \in I$ equivalently: R/I is integral
(ab = 0 in R/I $\Rightarrow$ a or b is 0 in R/I)

Def: I is maximal if R/I is a field (any $a \in R/I$, $a \neq 0$ is invertible).

Ex: $R = \mathbb{Z}$

$I(p)$ p prime

I is prime, even maximal $\mathbb{Z}/I = \mathbb{F}_p$.

$I = (0)$ $\mathbb{Z}/(0) = \mathbb{Z}$ integral, I is prime, it's not maximal ($\mathbb{Z}$ is not a field).

$I = (6)$ not prime; $\mathbb{Z}/(6) = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ not integral.

$I = (9) = (3^2)$ not even radical.

$R = k[x]$

$I = (f)$ f irred, non zero. $I = (f)$ is maximal, hence prime (excercise in Bezout's identity).

$I = (0)$ prime but not maximal : $R/(0) = R = k[x]$ not a field.

$I = (x(x-1))$. I not prime. $k[x]/I \simeq k \times k$.

Take $\cdot$ $\underline{k = \mathbb{R}}$ $\quad I = (x^2+1)$

$$\mathbb{R}[x]/x^2+1 \simeq \mathbb{C} \leftarrow \text{field.}$$
$$P \mapsto P(i) \qquad (x^2+1) \text{ is maximal.}$$

$\cdot$ $\underline{k = \mathbb{C}}$ $\quad x^2+1 = (x-i)(x+i)$

$$\mathbb{C}[x]/I \simeq \mathbb{C} \times \mathbb{C}$$

$$I \text{ not prime.}$$

<u>Theorem</u>: Let V be a non-emtpy algebraic subset of $\mathbb{A}^n(k)$. V is irreducible $\Leftrightarrow$ $I(V)$ is a prime ideal.

<u>Proof</u>: We will prove V is irreducible iff $I(V)$ is not prime.

$(\Rightarrow)$

Suppose V reducible.

$$V = V_1 \cup V_2, \quad V_1 \neq V, \quad V_2 \neq V.$$

$$V_1 \subsetneq V \Rightarrow I(V) \subsetneq I(V_1)$$

$$V_2 \subsetneq V \Rightarrow I(V) \subsetneq I(V_2)$$

Let $F_1 \in I(V_1) \setminus I(V)$ and $F_2 \in I(V_2) \setminus I(V)$

$F_1 \cdot F_2 \in I(V)$ (Let $P \in V$. If $P \in V_1$, $(F_1F_2)(P) = F_1(P)F_2(P) = 0$) (If $P \in V_2$ $(F_1F_2)(P) = F_1(P)\underbrace{F_2(P)}_{=0} = 0$)

$F_1 F_2 \in I(V)$ but $F_1 \notin I(V)$, $F_2 \notin I(V$

$I(V)$ not prime.

$(\Leftarrow)$

Suppose $I(V)$ is not prime

$\exists F_1, F_2 \in k[x_1 \dots x_n] \setminus I(V)$

$$F_1 F_2 \in I(V)$$

Let $V_1 = V \cap V(F_1)$ and $V_2 = V \cap V(F_2)$

Let's show that $V = V_1 \cup V_2$.
Let $P \in V$. If $P \in V_1$ then O.K! If $P \notin V_1$ then $F_1(P) \neq 0$. $(F_1 \cdot F_2)(P) = 0$ and $F_1(P) \neq 0 \Rightarrow F_2(P) = 0 \Rightarrow P \in V_2$.

$V_1 \neq V$ because $F_1 \notin I(V)$ hence $\exists P \in V$ st $F_1(P) = 0$ and hence this $P \notin V_1$

Similarly $V_2 \neq V$

Hence V is reducible

$\square$.

Theorem Let V be an non-empty alg. set
There is a (unique up to numbering) collection of $V_1, \dots, V_r$ of algebraic subsets of V, different from V such that each V_i is irreducible and $V_i \not\subset V_j$, $\forall (i,j)$ and $V = V_1 \cup \dots \cup V_r$. V_i's are called irreducible

components of V.

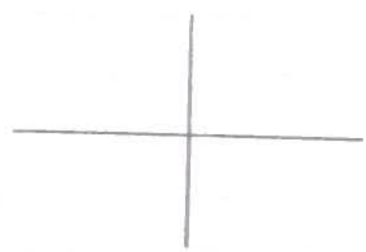
Examples

- $V = \mathbb{A}^n(k)$ is irreducible when k infinite.
$I(\mathbb{A}^n(k)) = (0)$ prime ideal of $k[x_1, \dots, x_n]$

- $P = (a_1, \dots, a_n)$ is irreducible
$I(P) = (x_1 - a_1, \dots, x_n - a_n)$
$I(P)$ is maximal : $k[x_1, \dots, x_n]/I(P) \simeq k$

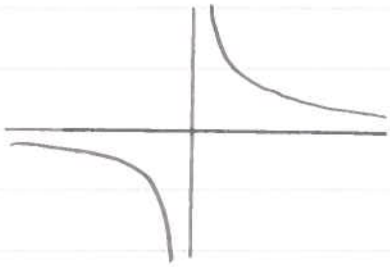
- P, Q two points. $P \neq Q$
$V = \{P\} \cup \{Q\}$ is reducible
Irreducible components are $\{P\}$ and $\{Q\}$.

- $V(xy) = V(x) \cup V(y)$ reducible
$V(x), V(y)$ are irreducible, they are irreducible components of $V(y)$



- $V = V(y - x^2)$
$I(V) = (y - x^2)$ prime.
$$k[x,y]/(y-x^2) \simeq k[x].$$

$\cdot$ <u>$V = V(xy-1)$</u>



Show that $I(V)$ is prime.

$V = \{(t, t^{-1}),\ t \in k \setminus \{0\}\}$

Let $F, G \in k[x,y]$ s.t. $FG \in I(V)$. $\forall t \in k \setminus \{0\}$, $F(t,t^{-1}) \cdot G(t,t^{-1}) = 0$.

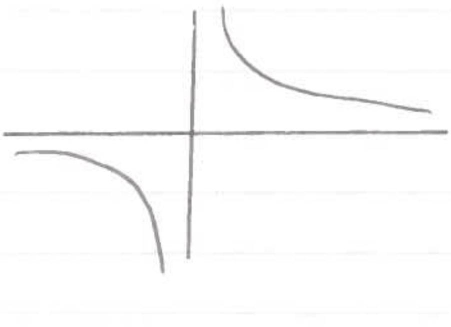
Let $n = \deg_y(F)$, $m = \deg_y G$.

$$\forall t \neq 0,\ \underbrace{t^n F(t,t^{-1})}_{\substack{F_1(t) \\ F_1 \in k[T]}} \cdot \underbrace{t^m G(t,t^{-1})}_{\substack{G_1(t) \\ G_1 \in k[T]}} = 0.$$

$F_1 \cdot G_1 = 0$ as a polynomial in $k[T]$

$$\Rightarrow \begin{cases} F_1 = 0 \Rightarrow \overset{\neq 0}{t^n} F(t,t^{-1}) = 0 \quad \forall t \neq 0 \\ \qquad \Rightarrow F \in I(V) \\ G_1 = 0 \Rightarrow t^m G(t,t^{-1}) = 0 \quad \forall t \neq 0. \\ \qquad \Rightarrow G \in I(V) \end{cases}$$

$I(V)$ is prime $\Rightarrow V$ irred.



29/1/14

Ex: $V = V(y^4 - x^2,\ y^4 - x^2y^2 + xy^2 - x^3) \subset \mathbb{A}^2(\mathbb{C})$

Q: Decompose into irreducible components.

Rem: $V(F, G) = V(F) \cap V(G)$

Note: $(F, G) = (F) + (G)$

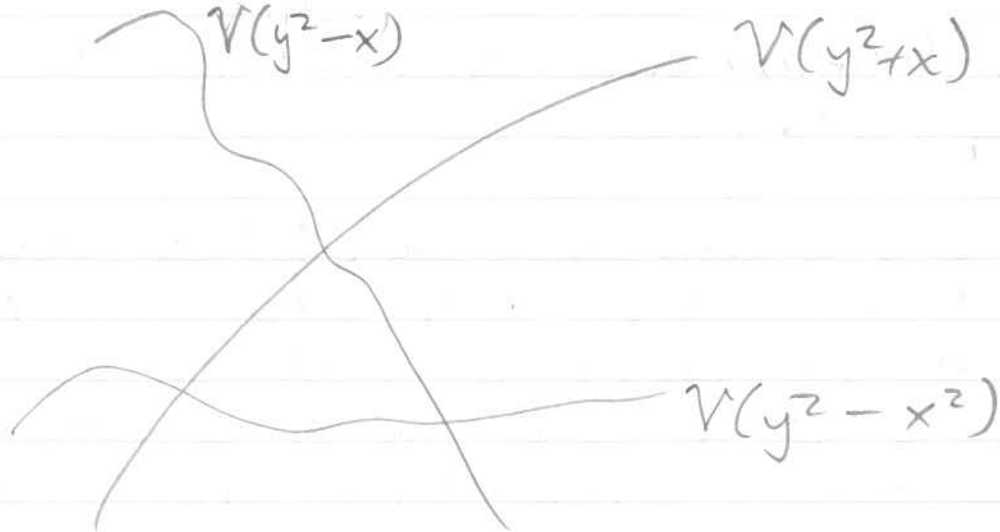
$$V = V(y^4 - x^2) \cap V(y^4 - x^2y^2 + xy^2 - x^3)$$

$$V(y^4 - x^2) = V((y^2 - x)(y^2 + x))$$

$$= V(y^2 - x) \cup V(y^2 + x)$$

$$V(y^4 - x^2y^2 + xy^2 - x^3) = V(y^2(y^2 - x^2) + x(y^2 - x^2))$$

$$= V(y^2 + x) \cup V(y^2 - x^2)$$



$$V = V(y^2+x) \cup [\underbrace{V(y^2-x) \cap V(y^2-x^2)}_{\begin{cases} y^2 = x \\ y^2 = x^2 \end{cases}}]$$

$x = x^2 \Rightarrow x = 0$ or $x = 1$

If $x=0$, then $y = 0$

If $x=1$, then $y = \pm 1$.

$$V(y^2-x) \cap V(y^2-x^2) = \{P_0\} \cup \{P_1\} \cup \{P_2\}$$

with $P_0 = (0,0)$, $P_1 = (1,1)$, $P_2 = (1,-1)$

$$V = V(y^2+x^2) \cup P_0 \cup P_1 \cup P_2$$

In fact $P_0 \in V(y^2+x)$ but $P_1, P_2 \notin V(y^2+x)$

Ex: Check that $V(y^2+x)$ is irred.

$$V = V(y^2+x) \cup P_1 \cup P_2$$

This is a decomposition into irreducible components.

—/—

Some revisions of commutative algebra.

Let R be a ring. R is integral $a \in R$ is called irreducible if whenever $a = bc$, then b or c is a unit. $a \in R$ is called prime if whenever $a | bc$ then $a | b$ or $a | c$

A prime element is irreducible.

Converse is false in general.

ex: $R = \mathbb{Z}[\sqrt{-5}]$, $3 \in R$ is irreducible, not prime. $3 \mid (2-\sqrt{-5})(2+\sqrt{-5})$ but $3 \nmid 2-\sqrt{-5}$ and $3 \mid 2+\sqrt{-5}$

Def: R is called a UFD (Unique Factorisation Domain) if any $a \in R$ can be writtern in a unique way as $a = u.p_1 \dots p_n$, p_i irreducible

If R is a UFD then prime $\Leftrightarrow$ irreducible

Ex: $\mathbb{Z}$, $k[x]$ are UFDs even PIDs

$\mathbb{Z}[x]$ is a UFD, not PID ($(2,x)$ is not principal)

In general: if R is a UFD, then $R[x]$ is also a UFD.

In particular: $k[x_1, \dots x_n]$ is a UFD.

Def: R is a UFD
$f \in R[x]$ is called primitive if
$f(x) = a_n x^n + \dots + a_0$
with $\gcd(a_0, \dots, a_n) = 1$

Ex: $R = \mathbb{Z}$ $2x^2+1$ is primitive
$2x^2+6$ is not.

Gauss Lemma.
If f, g are primitive, then fg is primitive, then fg is primitive.

$$K = \left\{ \frac{a}{b} : a, b \in R, b \neq 0 \right\}.$$

K is a field called field of fractions of K.

ex: $R = \mathbb{Z}$, $K = \mathbb{Q}$

$$R = k[x], \ K = k(x) = \left\{ \frac{f}{g}, f, g \in k[x], g \neq 0 \right\}$$

Lemma: If $f \in K[x]$, then $\exists \alpha \in K$, $\alpha f \in R[x]$ and αf is primitive.

Proof: $f(x) = f_n x^n + \ldots + f_0$.

$f_i = \frac{a_i}{b_i}$. Let $b = b_0, \ldots, b_n$

$b, f \in R[x]$.

Let $d = \gcd(bf_n, \ldots, bf_0)$

$\left(\frac{b}{a}\right) f \in R[x]$ and is primitive.

Take $\alpha = \frac{b}{d}$ $\square$.

Very important!

<u>Theorem</u>: $f, g \in R[x]$, f primitive
If $f | g$ in $K[x]$ then $f|g$ in $R[x]$.

This means that if $g = f \cdot \alpha$, $\alpha \in K[x]$ then in fact $\alpha \in R[x]$.

—/—

<u>Theorem</u>: (Very weak form of Bézout's theorem)
Let k be a field.
F, G non-zero in $k[x,y]$ with no common factor.
$V(F,G) = V(F) \cap V(G)$ is finite.

<u>Proof</u>: $k[x] = \underbrace{k[x]}_{R}[y] \subset \underbrace{k(x)}_{K}[y]$

<u>Claim</u>: F and G have no common factor in $k(x)[y]$

<u>Proof of claim</u>: Suppose F and G had a common factor H in $k(x)[y]$.

By lemma, $\exists \alpha \in k(x)$ st $\begin{cases} \alpha H \in k[x,y] \\ \alpha H \text{ is } \underline{\text{primitive}} \end{cases}$

$\alpha \in k(x)$, $\alpha \neq 0$ hence α is a unit in $k(x)[y]$
Hence

$$\left.\begin{cases} \alpha H | F \\ \alpha H | G \end{cases}\right\} \text{in } k(x)[y]$$

$\alpha H \in k[x,y]$ primitive.

By theorem $\alpha H \mid F$, $\alpha H \mid G$ in $k[x,y]$ but by assumption F, G have no common factor in $k[x,y]$, contradiction. This proves the claim.

F, G are coprime in $k(x)[y]$ which is a ring of polynomials over a field which is a PID.

Bezout's identity: $\exists\, U, V \in k(x)[y]$,

$$1 = UF + VG.$$

Let D be in $k[x]$ st $DU, DV \in k[x,y]$

$$D(x) = (DU)F + (DV)G.$$

Let $(x,y) \in V(F) \cap V(G)$

Then $D(x) = (DU)\underbrace{F(x,y)}_{=0} + (DV)\underbrace{G(x,y)}_{=0} \neq 0$

$D(x) = 0$ which gives finitely many possibilites for x. For an x like this, $F(x,y) = 0$ and $G(x,y) = 0$ give finitely many choices for y.

$\square$

<u>Consequence</u>: $F \in k[x]$ irreducible and $V(F)$ is <u>infinite</u> Then $I(V(F)) = (F)$ and $V(F)$ is irreducible.

Proof: $(F) \subset I(V(F))$ always
Let $G \in I(V(F))$
look at $V(F, G) = V(F) \cap V(G)$.

As $V(F)$ is infinite, $V(F, G)$ is infinite, by theorem just proved F and G have a common factor. As F is irreducible, $F \mid G$ hence $G \in (F)$. Therefore $I(V(F)) = (F)$
As F is irreducible, $k[x,y]$ is a UFD, F is prime and hence $(F) = I(V(F))$ is a prime ideal hence $V(F)$ is irreducible.

Consequence 2. k alg. closed
$F = F_1^{e_1} \dots F_r^{e_r}$, $F_i \in k[x,y]$ irred
$V(F) = V(F_1) \cup \dots \cup V(F_r)$
This is a decomposition into irred. components.
$I(V(F)) = (F_1 \dots F_r)$.

Proof: $V(F) = V(F_1^{e_1}) \cup \dots \cup V(F_r^{e_r})$

$$= V(F_1) \cup \dots \cup V(F_r)$$

As k alg. closed each $V(F_i)$ is irreducible by previous consequence, besides $I(V(F_i)) = (F_i)$.

Suppose $V(F_i) \subset V(F_j)$
$I(V(F_j)) \subset I V(F_i)$
$\quad ||$
$(F_j) \subset (F_i) \Rightarrow F_i \mid F_j$ contradiction!

That means that $V(F) = V(F_1) \cup \ldots \cup V(F_r)$
is a decomposition into irreducible components:

$$I(V(F)) = \bigcap_{i=1}^{r} I(V(F_i))$$
$$= \bigcap_{i=1}^{r} (F_i)$$
$$= (F_1 \ldots F_r)$$

because : F_i's are irreducible and distinct.

<u>Lemma</u> (compare to Alg 3)
R any UFD
A monic polynomial in $R[x]$ of deg 1 is irreducible.
A monic polynomial in $R[x]$ of deg 2 or 3 is irreducible if and only if it has no root in R.

<u>Proof</u> (Excerise).

<u>Example</u>:

① $F(x,y) = y^2 + x^2(x-1)$ in $\mathbb{R}[x,y] = \underbrace{\mathbb{R}[x]}_{R}[y]$

$F \in \mathbb{R}[x][y]$ is monic of deg 2
F is irreducible iff F has no root in $\mathbb{R}[x]$
Suppose F had a root $a(x) \in \mathbb{R}[x]$
$$a(x)^2 = -x^2(x-1)^2$$

Let $x \in \mathbb{R}$, $x \neq 0,1$, then

$$-x^2(x-1)^2 < 0.$$

can't be $a(x)^2$.

F has no root in $\mathbb{R}[x]$ hence irreducible in $\mathbb{R}[x,y]$.

$$V(F) = \{(0,0), (1,0)\}. \text{ finite.}$$

$$I(V(F)) = (x,y) \cap (x-1,y)$$
$$= (x(x-1), y)$$
$$\neq (F)$$

Consequence does not apply if $V(F)$ is finite.

Over $\mathbb{C}[x,y]$, $F = (y + ix(x-1))(y - ix(x-1))$

irreducible because degree 1 (in y) and monic

By consequence (2), $V(F) = V(y + ix(x-1)) \cup V(y - ix(x-1))$ which is a decomposition irred. components and $I(V(F)) = ((y + ix(x-1)) \cdot (y - ix(x-1))) = (F)$.

-/-

Ex: $\mathbb{A}^2(\mathbb{C}) \supset V(y^2 - x(x-1)(x-\lambda))$ $\lambda \in \mathbb{C}^*$.

$F = y^2 - x(x-1)(x-\lambda)$. Is $V(F)$ irreducible?

What is $I(V(F))$.

$V(F)$ is infinite because you're over $\mathbb{C}$.

Is F irreducible?

$y^2 - x(x-1)(x-\lambda) \in \mathbb{C}[x][y]$ monic of degree 2 in y. Enough to see that it has no roots in $\mathbb{C}[x]$.

Suppose you had $a(x)^2 = x(x-1)(x-\lambda)$ for some $a \in \mathbb{C}[x]$. L.H.S has even degree and R.H.S has degree 3. Impossible. F irred. and $I(V(F)) = (F)$.

Hilbert Nullstellensatz (theorem of zeros)
k is algebraic closed.

Weak Nullstellensatz.
Let $I \subset k[x_1, \dots x_n]$ be an ideal st $1 \notin I$ then $V(I) \neq \emptyset$.

Proof This will be assumed.

Rem: if $n=1$. I is principle, $I = (F)$
As k is alg closed $V(F) = \{x \in k, F(x) = 0\}$ $\neq \emptyset$.

· Does not hold for non-alg closed field:
$V(x^2+1) = \emptyset$ in $\mathbb{A}^1(\mathbb{R})$.

· If $I \subset k[x_1, \dots, x_n]$ is an ideal st $V(I)=\emptyset$, then $1 \in I$.

Strong Nullstellenstaz:

$$I(V(I)) = Rad(I).$$

Ex: Let $I = (x^2) \subset k[x]$

$$V(I) = \{0\}$$

$$I(V(I)) = I(\{0\}) = (x) = Rad(x^2)$$

—/—

Next time: Weak $\Rightarrow$ strong.

31/1/13.

Recall: Hilbert Nullstellensatz

Weak N: k alg. closed
$I \subset k[x_1, \dots, x_n]$, $1 \notin I$.
$V(I) \neq \emptyset$.

($\Leftrightarrow$ if $V(I) = \emptyset$ then $1 \in I$)

Strong N: k alg closed
$I \subset k[x_1, \dots, x_n]$ ideal
$I(V(I)) = Rad(I)$.

Consequence 1: If I radical, then $I = I(V(I))$

Consequence 2: If I is a prime ideal, then $V(I)$ is irreducible.

By strong N, $I(V(I)) = Rad(I) = I$ because I is prime therefore radical.

$I(V(I))$ is prime $\Rightarrow V(I)$ irreducible.

Consequence 3: Maximal ideals of $k[x_1, \dots, x_n]$ are precisely the ideals $(x_1 - a_1, \dots, x_n - a_n)$ for $(a_1, \dots, a_n) \in k^n$.

Proof: Any such ideal is maximal.

$$k[x_1, \dots, x_n] / (x_1 - a_1, \dots, x_n - a_n) \cong k.$$

Conversely, let M be a maximal ideal of $k[x_1, \dots, x_n]$

W.N $\Rightarrow V(M) \neq \emptyset$ (because, as M is maximal, $1 \notin M$).

Let $P \in V(M)$. $P = (a_1, \ldots, a_n)$

$I(V(M)) \subset I(P) = (x_1 - a_1, \ldots, x_n - a_n)$.

By S.N $I(V(M)) = \mathrm{Rad}(M) = M$.
because M is maximal.

$$\begin{cases} M \subset (x_1 - a_1, \ldots, x_n - a_n) \\ M \text{ is maximal.} \end{cases}$$

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

—/—

Rem: Not true if k is not closed.
e.g $k = \mathbb{R}$, $M = (x^2+1)$ is maximal.

Strong N $\Rightarrow$ Weak N:
Let I ideal s.t. $V(I) = \emptyset$.

$$I(V(I)) = k[x_1, \ldots, x_n] = \mathrm{Rad}(I) \text{ by SN.}$$

$$\Rightarrow 1 \in \mathrm{Rad}(I) \Rightarrow 1^n \in 1 \in I$$

$\square$

from Comm. alg.

<u>Hilbert basis theorem:</u> any field.
Any ideal I in $k[x_1, \dots, x_n]$ is finitely generated, i.e. of the form $(F_1, \dots, F_r)$ for some polynomials $F_1, \dots, F_r$.

<u>Proof by induction on n</u>

<u>$n=1$</u>: $k[x]$ is a P.I.D. Any ideal is generated by one element.

Suppose ture for $k[x_1, \dots, x_{n-1}] = R$.

We need to show that any ideal in $R[x]$ is finitely generated.

Assume there is an ideal I which is not finitely generated. Of course $I \neq (0)$. Let $f_0 \in I \setminus \{0\}$ an element of smallest degree. Let $J_0 = (f_0)$. Of course $J_0 \neq I$.

Let $f_1 \in I \setminus J_0$ of smallest degree. $J_1 = (f_0, f_1) \neq I$

Continue inductively.

Construct a sequence of ideals
$$J_0 \subset J_1 \subset \dots \subset I.$$
st $J_{i+1} = (J_i, f_{i+1})$ where f_{i+1} is in $I \setminus J_{i+1}$ of smallest degree.

Each J_i is finitely generated hence $I \neq J_i$ for any i.

Let $a_i \in R$ be the leading coefficient of f_i.
Let $J \subset R$ be an ideal generated by the a_i's.
By induction assumption. J is finitely generated.
$J = (a_0, \dots, a_N)$ for some N. Hence
$a_{N+1} = r_0 a_0 + \dots + r_N a_N$ for some $r_i \in R$.

Let $g = r_0 f_0 x^{n_0} + \dots + r_N f_N x^{n_N}$ where
$n_i = \deg f_{N+1} - \deg f_i \geq 0$.

$$\begin{cases} \deg g = \deg f_{N+1} \\ \text{leading coeff of } g \text{ is } r_0 a_0 + \dots + r_N f_N = a_{N+1} \\ \text{which is by def the leading coeff of } f_{N+1}. \end{cases}$$

Look at $g - f_{N+1} \in J_{N+1}$ because $g \in J_N \subset J_{N+1}$

$$\deg(g - f_{N+1}) < \deg f_{N+1}$$

contradicts the choice of f_{N+1} as being of smallest degree in $I \setminus J_N$.

$\square$

<u>Theorem</u>: W.N $\Rightarrow$ S.N.

<u>Proof</u>: Let I be an ideal in $k[x_1, \dots, x_n]$

$\mathrm{Rad}(I) \subset I(V(I))$ is easy. Let $F \in \mathrm{Rad}(I)$,
$F^N \in I \subset I(V(I))$. But $I(V(I))$ is
radical $\Rightarrow F \in I(V(I))$

for some N.

Conversley, let $F \in I(V(I))$. We need to show that $F^N \in I$ for some N. We will look at the ring $k[x_1, \dots, x_{n+1}]$ generated by I and $F \cdot x_{n+1} - 1$. (Trick!)

Write $I = (F_1, \dots, F_r)$, $F_i \in k[x_1, \dots, x_n]$

$$\tilde{I} = (F_1, \dots, F_r, F \cdot x_{n+1} - 1)$$

What is $V(\tilde{I}) \subset \mathbb{A}^{n+1}(k)$

Let $P \in V(\tilde{I})$. $= (a_1, \dots, a_n, a_{n+1})$

$$\begin{cases} F_i(a_1, \dots, a_n) = 0 \ (*), i = 1, \dots, r \\ F(a_1, \dots, a_n) a_{n+1} = 1 \quad (**) \end{cases}$$

$(*) \Rightarrow (a_1, \dots, a_n) \in V(I)$

$F \in I(V(I)) \Rightarrow F(a_1, \dots, a_n) = 0$.

$(**)$ impossible.

$V(\tilde{I}) = \emptyset$. W.N $\Rightarrow 1 \in \tilde{I}$

$$1 = \sum_{i=1}^{r} A_i(x_1, \dots, x_{n+1}) \cdot F_i$$

$$+ B(x \dots x_{n+1})(F \cdot x_{n+1} - 1)$$

Let $y = \frac{1}{x_{n+1}}$

By diving this relation by a sufficiently high power, say N of x_{N+1}. we find a relation

$$y^N = \sum A_i'(x_1 \dots x_n, y) \cdot F_i$$
$$+ B(x_1 \dots x_n, y)(F - y).$$

substitute F for y.

$$F^N = \sum_{i=1}^{r} \underbrace{A_i'(x_1, \dots, x_n; F)}_{\in k[x_1, \dots, x_n]} \cdot F_i \in I$$

$$F^N \in I \Rightarrow F \in Rad(I)$$

$\square$.

5/2/14.

Ex: $I = (x^2, y) \subset \mathbb{C}[x,y]$

Find $\mathrm{Rad}(I)$?

$\mathrm{Rad}(I) = I(V(I))$ (by N)

$V(I) = V(x^2, y) = (0,0) \in \mathbb{A}^2_{\mathbb{C}}$

$I(V(I)) = I(0,0) = (x,y)$

$\mathrm{Rad}(I) = (x,y)$

—/—

Comments on sheet 1.

$V(I) \cup V(J) = V(I, J)$ "ideal generated by $\{FG : F \in I, G \in J\}$.

$IJ \subset I \Rightarrow V(I) \subset V(IJ)$
$IJ \subset J \Rightarrow V(J) \subset V(IJ)$.

$\Rightarrow V(I) \cup V(J) \subset V(IJ)$.

Enough to show: $V(\{FG : F \in I, G \in J\}) \subset V(I) \cup V(J)$.

Let $P \in V(\{FG\})$. If $P \in V(I)$ done, otherwise $\exists F \in I$, $F(P) \neq 0$, then $P \in V(J)$ $(F(P)G(P) = 0 \ \forall G \in J)$.
$\neq 0$

— / —

From lectures $V(I) \cup V(J) = V(I \cap J)$

It's <u>not true</u> that $IJ = I \cap J$. Of course $IJ \subset I \cap J$.

Take $I = J = (x) \subset k[x]$

$$I \cdot J = (x^2)$$
$$\cap$$
$$I \cap J = (x)$$

$V(I \cap J) = V(IJ)$. Assume k alg. closed. By N. $\mathrm{Rad}(I \cap J) = \mathrm{Rad}(IJ)$. It's true that if $1 \in I + J$, then $IJ = I \cap J$ (Exercise)

— / —

$I \cup J$ is usually not an ideal, $I + J$ is an ideal and in fact the ideal generated by $I \cup J$.

— / —

Question 4: m, n two coprime integers

$V = \{ (t^m, t^n), t \in k \}$ k any field.

$\cancel{V(x - y^{\frac{m}{n}})}$ This does not exist !!!

From def: (Reason)
$F \in k[x,y]$

$V(F) = \{ (x,y) \in \mathbb{A}^2(k) : F(x,y) = 0 \}$.

For any $(x, y) \in k^2$, one evaluates $F(x, y) \in k$.
One picks out those (x, y) st $F(x, y) = 0$.

$\underbrace{V(x - \sqrt{y})}$? $k = \mathbb{R} \leftarrow$ what is this?

not defined at ex $(0, -1)$

NB: $V(x^2 - y)$ exist
$V(x - \sqrt{y})$ does not exist?

Similarly: $V(z - 1/x)$ does not exist;
$V(zx - 1)$ does.

$x^2 = y \Rightarrow y = \sqrt{x}$? (Don't do this!)
What is $\sqrt{1}$? reason.

Standard conv in analysis $\sqrt{1} = 1$

$(-1)^2 = 1 \Rightarrow -1 = \sqrt{1} = 1$?

Sol: $V(x^n - y^m)$

Suppose m, n are not coprime.

Is $V = \{(t^m, t^n), t \in k\}$ algebraic?

$V = \{(t^m, t^n)\}$ algebraic or not - k any infinite field.

$I(V) = (x-y)$

If V was algebraic, then $V(I(V)) = V = V(x-y)$.

If $k = \mathbb{R}$. No because $(-1,-1) \in V(x-y)$ but $(-1,-1) \neq (t^2, t^2)$ for any $t \in \mathbb{R}$.

If k is algebraically closed, then Yes, $t^2 - x$ has a root in k for any t.

—/—

$V = \{(t, t^2, t^3)\} \not\subset$ any plane, $k = \mathbb{R}$

$H: ax + by + cz + d = 0.$

$at + bt^2 + ct^3 + d = 0. \quad \forall t \in \mathbb{R}.$

$\Rightarrow a = b = c = d = 0.$

—/—

Back to lectures!

<u>Affine varieties</u>.

k alg. closed

An affine variety $V \subset \mathbb{A}^n(k)$ is an irreducible algebraic subset

—/—

$\underline{\text{Ex}}$: P a point, $\mathbb{A}^n(k)$, $V(x-y) \subset \mathbb{A}^2(k)$ etc...

Let $\mathcal{F}(V, k) = \{\text{Functions } V \to k\}$.

$\mathcal{F}(V, k)$ is a ring
It's also a k-vector space.

$\mathcal{F}(V, k)$ is a k-algebra.

Let $F \in k[x_1, \ldots, x_n]$, $P = (a_1, \ldots, a_n) \in V$, one can evaluate F at P. Hence F defines an element of $\mathcal{F}(V, k)$ called a polynomial function on V.

We have a map:

$$k[x_1 \ldots x_n] \xrightarrow{\varphi} \mathcal{F}(V, k)$$
$$F \longmapsto \text{Function defined by } F.$$

φ is clearly a ring homomorphism and it's <u>k-linear</u>.

$$\mathrm{Ker}(\varphi) = \{F \in k[x_1 \ldots x_n] : F(P) = 0, \ \forall P \in V\}.$$
$$= I(V).$$

Let $\Gamma(V) = k[x_1 \ldots x_n] / I(V)$.

φ induces an injection of $\Gamma(V)$ into $\mathcal{F}(V, k)$
$\Gamma(V)$ is an integral ring (because V irreducible)

$\Gamma(V)$ is called ring of polynomial functions on V.

Ex: $\Gamma(\mathbb{A}^n(k)) = k[x_1 \dots x_n]/(0)$

$$= k[x_1 \dots x_n]$$

$V = \{ P = (a_1, \dots, a_n) \}$

$I(P) = (x_1 - a_1, \dots, x_n - a_n)$.

$\Gamma(P) = k[x_1, \dots, x_n] / (x_1 - a_1, \dots, x_n - a_n) \simeq k$.

$$F \longrightarrow F(P)$$

$V = V(y - x^2)$

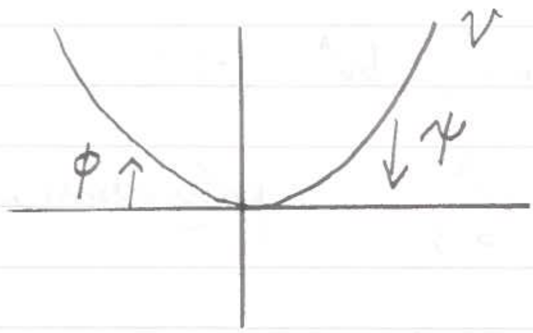
$\Gamma(V) = k[x,y]/(y - x^2) \simeq k[x]$.

Def: $V \subset \mathbb{A}^n(k)$, $W \subset \mathbb{A}^n(k)$ affine vars.
A map $f: V \to W$ is called polynomial if $\exists\, T_1, \dots, T_m \in k[x_1, \dots, x_n]$ st $f(a_1, \dots, a_n) = (T_1(a_1, \dots, a_n), \dots, T_m(a_1, \dots, a_n))$ for all $(a_1, \dots, a_n) \in V$.

Ex: $V = \mathbb{A}^1(k)$, $W = V(y - x^2)$

$V \xrightarrow{\phi} W$ is a polynomial map.
$t \mapsto (t, t^2)$

$W \xrightarrow{\psi} V$ is a polynomial map.
$(x, y) \to x$.



$\mathbb{A}^1(\mathbb{R}) \to \mathbb{A}^1(\mathbb{R})$ is <u>not</u> a poly map.
$t \to \sin(t)$.

Let $V \subset \mathbb{A}^n(k)$, $W \subset \mathbb{A}^m(k)$
Let $\phi : V \to W$ be a polynomial map.
Let $f \in \mathcal{F}(W, k)$.

$$\begin{tikzcd} V \arrow[r, "\phi"] \arrow[rr, bend right] & W \arrow[r, "f"] & k \end{tikzcd}$$

$$\tilde{\phi}(f) = f \circ \phi.$$

$\tilde{\phi}$ defines a map

$$\mathcal{F}(W, k) \to \mathcal{F}(V, k)$$
$$f \to \tilde{\phi}(f) = f \circ \phi.$$

If $f \in \Gamma(W)$, then $\tilde{\phi}(f) \in \Gamma(V)$. $\tilde{\phi}$ restricts to $\Gamma(W) \to \Gamma(V)$.

$\tilde{\phi}$ is a morphism of k-algebras (ring homomorphism and k-linear).

Ex: $V = \mathbb{A}^2(k)$, $W = \mathbb{A}^1(k)$

$\varphi : V \to W$ polynomial map.
$(x,y) \mapsto x$

$\Gamma(V) = k[x,y]$, $\Gamma(W) = k[x]$.

What is $\tilde{\varphi} : \Gamma(W) \to \Gamma(V)$?

$$\begin{array}{ccc} \Gamma(W) & \to & \Gamma(V) \\ \| & & \| \\ k[x] & \to & k[x,y] \\ x & \mapsto & x \end{array}$$

Theorem: $\mathbb{A}^n \supseteq V$, $W \subseteq \mathbb{A}^m$.

$\varphi \mapsto \tilde{\varphi}$ is a 1-1 correspondence between polynomial maps $V \to W$ and k-algebra homomorphism from $\Gamma(W) = \Gamma(V)$

Proof: We have already seen how to associate $\tilde{\varphi}$ to φ.

Conversely, let $\alpha : \Gamma(W) \to \Gamma(V)$ be a k-algebra homomorphism. Need to find $\varphi : V \to W$ st $\tilde{\varphi} = \alpha$.

$$\alpha : k[x_1, \dots x_n]/_{I(W)} \to k[x_1, \dots x_n]/_{I(V)}$$

k algebras homomorphism.

There exist $\tilde{\alpha} : k[x_1, \dots x_n] \to k[x_1, \dots x_n]$
st $\tilde{\alpha}(I(W)) \subset \underline{I(V)}$
and $\alpha(\bar{x}_i) = \tilde{\alpha}(x_i)$

Let $T_i = \tilde{\alpha}(x_i)$ $\quad i = 1, \dots, m$.

$T_i \in k[x_1, \dots, x_n]$

Define $\mathbb{A}^n(k) \xrightarrow{\phi} \mathbb{A}^m(k)$
$(a_1, \dots, a_n) \to (T_1(a_1, \dots, a_n), \dots, T_m(a_1, \dots, a_n))$

ϕ is a polynomial map

Because $\tilde{\alpha}(I(W)) \subset I(V)$, for any $(a_1, \dots, a_n) \in V$, $\phi(a_1, \dots, a_n) \in W$.

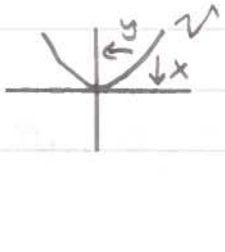
(because, as V, W algebraic, $V(I(V)) = V$ and $V(I(W)) = W$).

ϕ induces a polynomial map $V \xrightarrow{\phi} W$ and $\tilde{\phi} = \alpha$

$\square$.

<u>Examples</u> $V = \mathbb{A}^1(\mathbb{C}) \xrightarrow{\phi} \overbrace{V(y - x^2)}^{= W} \subset \mathbb{A}^2(\mathbb{C})$
$t \mapsto (t, t^2)$

$\tilde{\phi} : \Gamma(W) = k[x,y] \big/ (y - x^2) \to \Gamma(V) = k[x]$.



$\bar{x} \to t$
$\bar{y} \to t^2$.

$\cdot\ V = \mathbb{A}^1(\mathbb{C}) \xrightarrow{\phi} W = \{(t,t^2,t^3),\ t \in \mathbb{C}\}$
$= V(y-x^2,\ z-x^3)$

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

$$\Gamma(W) = k[x,y,z]\Big/(y-x^2,\ z-x^3) \xrightarrow{\phi} \Gamma(V) = k[t]$$

$$\bar{x} \to t$$
$$\bar{y} \to t^2$$
$$\bar{z} \to t^3.$$

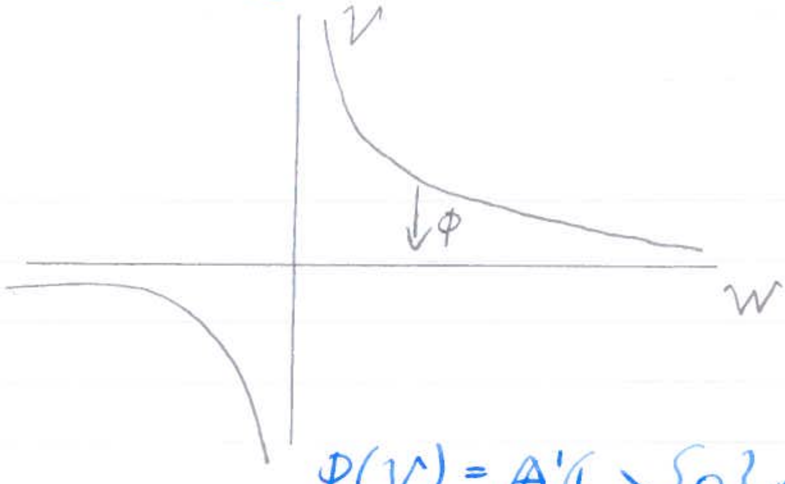
Q. : $V, W,\ \phi : V \to W$ polynomial.

Is it true that $\phi(V)$ is algebraic.

$$V = V(xy-1) \in \mathbb{A}^2(\mathbb{C})$$

$$W = \mathbb{A}^1(\mathbb{C})$$

$$V \xrightarrow{\phi} W$$
$$(x,y) \to x.$$



$\phi(V) = \mathbb{A}^1\mathbb{C} \setminus \{0\}$ not algebraic

Isomorphism of algebraic varieties.

V and W are isomorphic if there is a polynomial map $V \to W$ which has a polynomial inverse i.e $\varphi : V \to W$ and $\psi : W \to V$ st

$$\begin{cases} \psi \circ \varphi = id_V \\ \varphi \circ \psi = id_W . \end{cases}$$

By previous construction, this is equivalent to $\Gamma(V)$ being isomorphic to $\Gamma(V)$.

$F[x, x^2] \leftarrow F$

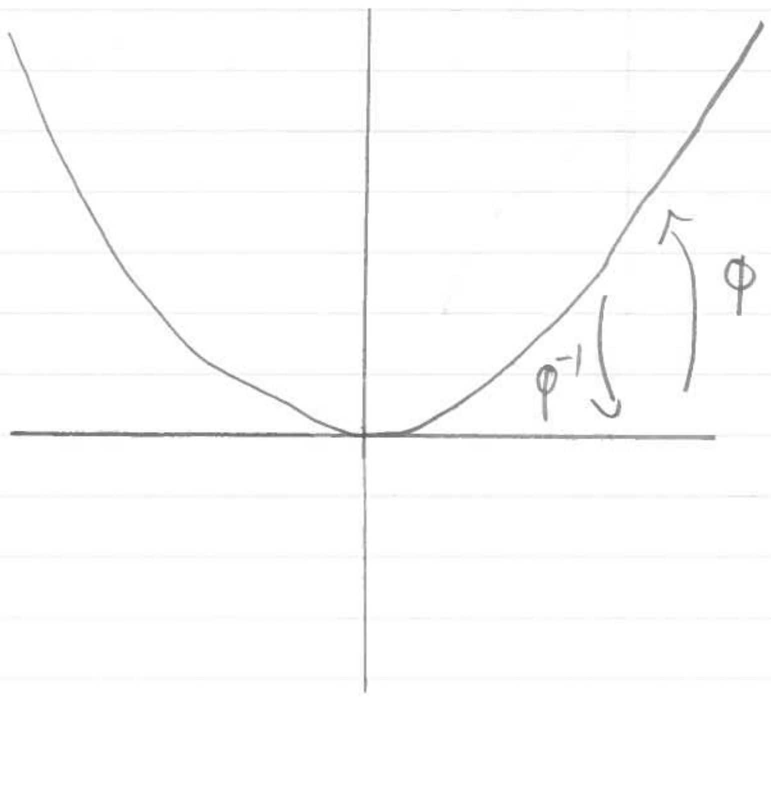
$k[x] \xleftarrow{\varphi} k[x,y]/(y-x^2)$

Ex : $V = \mathbb{A}^1(\mathbb{C}) \xrightarrow{\varphi} V(y - x^2) = W$

$t \longrightarrow (t, t^2)$.

$$\varphi^{-1} : V(y - x^2) \longrightarrow \mathbb{A}^1$$

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



If $\varphi : V \to W$ is an isomorphism then φ is bijective.

<u>Converse not true.</u>

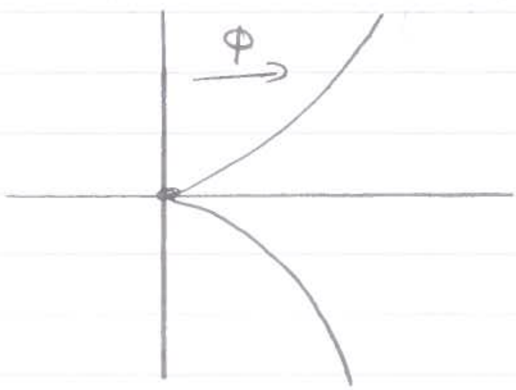
$$\begin{aligned} \mathbb{A}^1(\mathbb{C}) &\xrightarrow{\varphi} V(x^2 - y^3) \\ t &\to (t^3 - t^2) \end{aligned}$$

is a bijection. (see Q4 of HW1)

$$\tilde{\varphi} : \Gamma(V) = \mathbb{C}[x, y] \Big/ {x^2 - y^3} \to \Gamma(V) = k[x]$$

$$\begin{aligned} x &\to t^3 \\ y &\to t^2. \end{aligned}$$

$\tilde{\varphi}$ is not an isomorphism, in fact its not even surjective: t does not have a pre image.



7/02/14

Last time:

$\varphi : V \to W \qquad V \subset \mathbb{A}^n(k)\ ,\ W \subset \mathbb{A}^m(k)$

$V = V(xy-1) \xrightarrow{\varphi} \mathbb{A}^1(k)$

$(x,y) \to x$.

φ is not algebraic.

—/—

Prop: $\varphi : V \to W$ poly map
$X \subset W$ algebraic.
$\Rightarrow \varphi^{-1}(X)$ is algebraic.

Proof: $X = V(I)$, $I \subset k[x_1, \dots, x_m]$
$I = (F_1, \dots, F_r)$ (Hilbert basis theorem)
$X = V(F_1, \dots, F_r)$

$\varphi = (T_1, \dots, T_m)$, $T_i \in k[x_1 \dots x_m]$

$\varphi^{-1}(X) = V(F_1(T_1, \dots, T_m), \dots, F_r(T_1, \dots, T_m))$

$\varphi^{-1}(X)$ is algebraic.

$\square$.

Prop: $\varphi : V \to W$ polynomial map
φ is <u>surjective</u>
Let X be an algebraic subset of W st
$\varphi^{-1}(X)$ is irreducible, then X is irreducible.

<u>Proof</u>: We will prove X reducible $\Rightarrow \varphi^{-1}(X)$ is reducible

Assume X reducible $X = X_1 \cup X_2$
$X_1, X_2 \neq X$.

Then $\varphi^{-1}(X) = \varphi^{-1}(X_1) \cup \varphi^{-1}(X_2)$
By previous prop $\varphi^{-1}(X_1)$ and $\varphi^{-1}(X_2)$ are algebraic

Need to show that $\varphi^{-1}(X_1) \neq \varphi^{-1}(X)$, $\varphi^{-1}(X_2) \neq \varphi^{-1}(X)$.

Suppose $\varphi^{-1}(X_1) = \varphi^{-1}(X)$
Apply φ : $\underbrace{\varphi(\varphi^{-1}(X_1))}_{= X_1} = \underbrace{\varphi(\varphi^{-1}(X))}_{= X}$

Because φ is surjective

Then $X_1 = X$. Contraction.

$$\varphi^{-1}(X) \neq \varphi^{-1}(X_1)$$

Similarly : $\varphi^{-1}(X) = \varphi^{-1}(X_2)$

$\varphi^{-1}(X)$ is reducible.

$\square$

Rem: Is it ture that if X is irreducible then φ^{-1} is irreducible (Is the converse to the prop true)?

No! $V = W = \mathbb{A}^1(\mathbb{C})$

$$\mathbb{A}^1(\mathbb{C}) \xrightarrow{\varphi} \mathbb{A}^1(\mathbb{C})$$
$$x \longmapsto x^2$$

φ is polynomial and surjective.

$X = \{1\} \in \mathbb{A}^1(\mathbb{C})$ irreducible.

$\varphi^{-1}(X) = \{1\} \cup \{-1\}$ not irreducible.

Does the proposition hold without assumption that φ is surjective?

No! $V = \mathbb{A}^1(\mathbb{C})$, $W = \mathbb{A}^2(\mathbb{C})$

$$\varphi : \mathbb{A}^1 \to \mathbb{A}^2$$
$$x \longrightarrow (x, 0)$$

φ is polynomial, not surjective.

Take $X = V(x,y)$ 

$= V(x) \cup V(y)$ <u>not</u> irreducible.

$\varphi^{-1}(X) = \mathbb{A}^1(\mathbb{C})$ definitely irreducible.
(in this case $\varphi(\varphi^{-1}(X_2)) = (0,0) \neq X_2'$

<u>Examples</u>: <u>$k = \mathbb{C}$</u>

1. Show that $V = V(x^2 - y, x^3 - z)$ is irreducible

$$\mathbb{A}^1(\mathbb{C}) \xrightarrow{\varphi} V$$
$$t \to (t, t^2, t^3)$$
polynomial map

φ is surjective. Let $(x,y,z) \in V$
Take $t = x$, $(x,y,z) = \varphi(t)$

$\varphi^{-1}(V) = \mathbb{A}^1\mathbb{C}$ irreducible

By propositon, V is irreducible.

2. $V = V(y^3 - x^4, z^3 - x^5, z^4 - y^5) \subset \mathbb{A}^3\mathbb{C}$.

$$\varphi : \mathbb{A}^1(\mathbb{C}) \to V$$
$$t \to (t^3, t^4, t^5) \quad \text{Polynomial.}$$

φ surjective

Let $(x,y,z) \in V$
If $x = 0$ then $y = z = 0$; $\varphi(0) = (0,0,0)$

May assume $x \neq 0$, let $t = y/x$

$$\begin{cases} t^3 = \frac{y^3}{x^3} = \frac{x^4}{x^3} = x. \\ t^4 = \frac{y^4}{x^4} = \frac{y^4}{y^3} = y \\ t^5 = \frac{y^5}{x^5} = \frac{z^4}{z^3} = z \end{cases}$$

$\varphi^{-1}(V) = \mathbb{A}^1 \mathbb{C}$ irreducible

By prop. V is irreducible.

—/—

<u>Rational functions and local rings</u>.

k alg. closed. $V \subset \mathbb{A}^n(k)$ affine var.

$I(V)$ is prime because V irred.

$\Gamma(V) = k[x_1, \dots, x_n]/I(V)$ is integral

$k(V) = \mathrm{Frac}(\Gamma(V)) = \left\{ \frac{f}{g}, f, g \in \Gamma(V), g \neq 0 \right\}$

$k(V)$ is called field of rational functions on V.

<u>Ex</u>: $V = \mathbb{A}^1(k)$. $\Gamma(V) = k[x]$

$k(V) = k(x) = \left\{ \frac{f}{g}, f, g \in k[x], g \neq 0 \right\}$

<u>Def</u>: Let $f \in k(V)$, $P \in V$
f is said to be defined at P if $f = \frac{a}{b}$,
$a, b \in \Gamma(V)$ and $b(P) \neq 0$.

<u>Ex</u>: $V = \mathbb{A}^1(k)$

$$f = \frac{1}{x}$$

f is defined everywhere except when $x = 0$
f is not defined at 0.

Suppose f was defined at 0: $\exists\, a, b \in k[x]$

$$f = \frac{1}{x} = \frac{a}{b} \quad \text{and} \quad b(0) \neq 0.$$

Then $b = xa$.
$\Rightarrow b(0) = (xa)(0) = 0$. contradiction.

f is not defined at 0.

<u>Ex</u>: $k = \mathbb{C}$, $V = \mathbb{A}^1(\mathbb{C})$, $f = \frac{x}{x^2+1}$

f is defined everywhere except $\pm i$
f is not defined at $\pm i$

(excercise)

Ex: $f = \frac{x+1}{x^2-1}$

f defined at $x \neq \pm 1$

$x = -1$. $f = \frac{x+1}{x^2-1} = \frac{x+1}{(x+1)(x-1)} = \frac{1}{x-1}$

f is defined at -1 because you can take:

$$a = 1, \quad b = x-1$$
$$b(-1) = -2 \neq 0.$$

Ex: f is not defined at 1

excersie

12/2/14

Comments from homework 2:

1) $X' \subset \mathbb{A}^n$, $V(I(X'))$

$$X' \subset V(I(X')) \text{ and } V(I(X')) \text{ algebraic}$$

Let V' be algebraic $X' \subset V'$

$$I(X') \subset V(V')$$

$$\underset{\substack{\parallel \\ V'}}{V(I(V'))} \subset V(I(X'))$$

done.

2). $V = \{(t, t^2, t^3)\}$

$$V = V(y - x^2, z - x^3), \; I = (y - x^2, z - x^3)$$

$$F \in I(V)$$

$$\bar{F} \in k[x,y,z]/I \qquad \bar{F} = 0.$$

Equivalently: $F = (y - x^2)\underset{\substack{\cap \\ k[x,y,z]}}{Q} + R^{\in k[x,z]}$

$$R = (z - x^3)Q' + R'$$

$$R' \in k[x].$$

$$F = \underbrace{(y - x^2)Q + (z - x^3)Q'}_{\in I} + R'_{\in k[x]}$$

$F(t, t^2, t^3) = 0 = R'(t)$, $\forall t$.

$\underline{R' = 0}$

$F \in I \Rightarrow I(V) = I$

3) $y^2 - xy - xy^2 + x^3 = (y - x)(y - xy - x^2)$

$V = V(y - x) \cup V(y - xy - x^2)$

$k = \mathbb{R}, \mathbb{C}$

$\left.\begin{array}{l} V(F) \text{ inf} \\ F \text{ irred} \end{array}\right. \Rightarrow V(F)$ irred.

$\underline{\text{irred}} \left\{ \begin{array}{l} V(y - x) \text{ inf} \\ y - x \text{ irred.} \end{array} \right.$

$y - xy - x^2 = 0$.

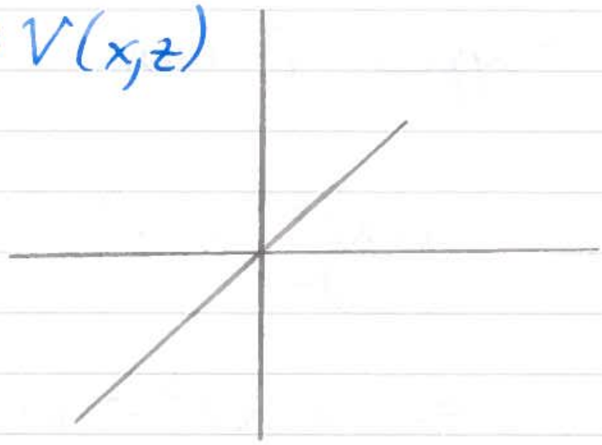
$y(1 - x) - x^2 = 0$. deg 1 in y.

$\left\{ \begin{array}{l} \text{irreducible in } k(x)[y] \\ \text{primitive} \end{array} \right.$ (Gauss lemma and its consequence seen before)

$\Rightarrow$ irred in $k[x, y]$.

4) $V(xy, xz, yz)$

$= V(x,y) \cup V(y,z) \cup V(x,z)$



5) $x^3 + x - x^2y - y = (x-y)(x^2+1)$

$V = V(x-y) \cup V(x^2+1)$

if $k = \mathbb{R}$, $V(x^2+1) = \emptyset$, $V = V(x-y)$ irred.

<u>$k = \mathbb{C}$</u>: $V(x^2+1) = V(x-i) \cup V(x+i)$

3 components.

—/—

$F \in k[x]$, k any field
if $\deg F = 2$ or 3, F irred
$\Rightarrow F$ no root <u>in k</u>

$F = y^3 - x^2 \in k[x,y] = k[x][y]$

F primitive as a polynomial in $k[x][y]$
Then F irred in $k[x,y]$
$\Leftrightarrow F$ irred in $\underbrace{k(x)}_{\text{field.}}[y]$

$\Leftrightarrow$ F has no roots in $k(x)$

Suppose it had a root in $k(x)$, $\dfrac{a(x)}{b(x)}$

$$\frac{a(x)^3}{b(x)^3} = x^2$$

$$\Rightarrow \quad a(x)^3 = b(x)^3 x^2$$

leading term $= 0 \bmod 3$

leading term $2 \bmod 3$

Impossible!

—/—

Back to lectures!

Rational functions and local rings.

$P \in V$ affine variety over k alg. closed

← fixed point

$$k \subset \Gamma(V) \subset \mathcal{O}_P(V) \subset k(V)$$

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

$k(V) = \left\{ \frac{f}{g},\ f, g \in \Gamma(V),\ g \neq 0 \right\}$

$\mathcal{O}_P(V) = \left\{ \frac{f}{g},\ g(P) \neq 0 \right\}$

$z \in k(V)$ is defined at P if $z = f/g$ with $g(P) \neq 0 \Leftrightarrow z = \mathcal{O}_P(V)$

Ex: $V = \mathbb{A}^1$, $P = 0$

$\frac{1}{x}$ not defined at 0.

$f = \frac{x-1}{x^2-1}$ is defined at $P = (1)$

$$f = \frac{1}{x+1}$$

Def: Let $f \in k(V)$
$P \in V$ is called a pole of f if f is not defined at P.

Theorem: Let $f \in k(V)$
1. $\{$Poles of $f\}$ is an algebraic set.
2. $$\Gamma(V) = \bigcap_{P \in V} \mathcal{O}_P(V)$$

Recall

$\forall P$, $\Gamma(V) \subset \mathcal{O}_P(V) \subset k(V)$

$\mathcal{O}_P = \{ f \in k(V) : f$ is defined at $P \}$

ideal

Proof: 1) For $G \in k[x_1, \dots, x_n]$, let $\overline{G}$ be the image of G in $\Gamma(V) = k[x_1, \dots, x_n]/I(V)$
Define $J_f = \{ G \in k[x_1, \dots, x_n], \overline{G} \cdot f \in \Gamma(V) \}$.
$\{$Poles of $f\} = V(J_f)$. algebraic set.

2) First remark:

$$\Gamma(V) \subset \bigcap_{P \in V} \mathcal{O}_P(V)$$

(By definition of $\mathcal{O}_P(V)$ it contains $\Gamma(V)$ for any P).

Let $f \in \bigcap_{P \in V} \mathcal{O}_P(V)$

Then f has no poles $\Rightarrow V(J_f) = \emptyset$.

By unstellensatz, $1 \in J_f$ (Here we use k alg. closed).

By def of J_f, $1 \cdot f = f \in \Gamma(V)$

$\square$.

Rem. Statement (2) is flase if k is not alg. closed

$k = \mathbb{R}$, $V = \mathbb{A}^1(\mathbb{R})$. $\Gamma(V) = \mathbb{R}[x]$

$k(V) = \mathbb{R}$

$f = \frac{1}{x^2+1}$ defined everywhere on V: x^2+1 has no roots

but $f \notin \mathbb{R}[x]$

Ex/excercise.

1) $V = V(y^2 - x^2(x+1))$. $I(V) = (y^2 - x^2(x-1))$

$f = \frac{\bar{y}}{\bar{x}}$

Does f have any pole?

Clearly f is defined at $P = (x, y)$, $x \neq 0$.

The only possible pole is $(0,0)$

Suppose f was defined at $(0,0)$, that means $f = \frac{\bar{a}}{\bar{b}}$, $\bar{a}, \bar{b} \in \Gamma(V)$, $b(0,0) \neq 0$.

In $\Gamma(V)$, $\frac{\bar{y}}{\bar{x}} = \frac{\bar{a}}{\bar{b}}$

$$\bar{b}\bar{y} - \bar{a}\bar{x} = \bar{0} \text{ in } \Gamma(V)$$

Then $by - ax \in I(V)$

$\exists h \in k[x,y]$, $by - ax = h(y^2 - x^2(x+1))$

$$by - hy^2 = ax - hx^2(x+1)$$

$$y(b - hy) = x(a - h\,x(x+1))$$

x and y are coprime, $k[x,y]$ is a UFD

hence $x \mid b - hy$.

$\exists \alpha \in k[x,y]$, $b - hy = \alpha x$

$$b = \alpha x + hy.$$

$b(0,0) = 0$ contradiction

f is not defined at $(0,0)$, $(0,0)$ is the unique pole.

Does $f^2 = \dfrac{\bar{y}^2}{\bar{x}^2}$ have any poles?

We have $f^2 = \dfrac{\bar{y}^2}{\bar{x}^2} = \dfrac{\bar{x}^2(\bar{x}+1)}{\bar{x}^2} = \bar{x} + 1$.

$f^2 \in \Gamma(V)$
f^2 has no poles.

2) $V(y - (x+1))$ $\quad f = \dfrac{\bar{y}}{\bar{x}}$.

Does f have poles?
f is defined whenever $\bar{x} \neq 0$.

The only possible poles are $(0,1)$ and $(0,-1)$

Is f defined at $(0,1)$?

Suppose it was $f = \frac{\bar{y}}{\bar{x}} = \frac{\bar{a}}{\bar{b}}$

$\bar{y}^2 = \bar{x} + 1$

$\bar{x} = \bar{y}^2 - 1$

$f = \dfrac{\bar{y}}{\bar{y}^2 - 1}$

$by - a(y^2 - 1) = h(y^2 - (x+1))$

Evaluate at $(0,1)$

$b(0,1) - 0 = h \times 0.$

$\Rightarrow b(0,1) = 0$

Contradiction

$(0,1)$ is a pole

and similarly $(0,-1)$ is a pole.

$\cdot\ V(y^6 - x^3)$, $f = \dfrac{y}{x^2}$.

Determine whether f has poles,
Same question for f^3.

When $x \neq 0$, f is defined.
The only possible pole is $(0,0)$.

Suppose f was def at $(0,0)$

$$\frac{\bar{y}}{\bar{x}^2} = \frac{a}{b} \quad , b(0,0) \neq 0$$

$$b \cdot y - ax^2 = h(x^6 - x^3)$$

$$by - hy^6 = ax^2 - hx$$

$$y(b - hy^5) = x^2(a - hx)$$

y and x^2 are coprime.

$\Rightarrow x^2 \mid b - hy^5$.

$$b - hy^5 = \alpha \cdot x^2.$$

$\Rightarrow b(0,0) = 0$. contradiction.

$(0,0)$ is the unique pole of f.

$$g = \frac{\bar{x}}{\bar{y}^2}$$

Ex: Determine whether g has any poles. (g has a unique pole at $(0,0)$).

$$g^3 = \frac{\bar{x}^3}{\bar{y}^6} = 1 \in \Gamma(V) \subset k(V)$$

has no poles.

- $V(\underbrace{wz - xy}_{\in k[x,y,z,w]}) \subset \mathbb{A}^4$

$$I(V) = (wz - xy)$$

$$f = \frac{w}{x} \in k(V)$$

Does f have any poles?

f is defined when $x \neq 0$.

The only possible poles are when $x = 0$.

$(x,y,z,w) \in V$ with $x = 0$,

$f = \frac{w}{x} = \frac{y}{z}$ because $wz = xy$.

when $x \neq 0$ or $z \neq 0$ then f is defined.

The only possible poles are when $x = 0$ and $z = 0$.

$\Leftrightarrow$ f is defined outside of the set $S' = \{ (0, y, 0, w), \ y, w \in k \}$.

$$= V(x, z)$$

Let $P \in S'$. Suppose f is defined at P.

$\overset{\parallel}{(0, y_0, 0, w_0)}$

$$\frac{w}{x} = f = \frac{a}{b}, \quad b(P) \neq 0.$$

$$wb - ax \in (wz - xy)$$

$$wb - ax = h(wz - xy)$$

$$w(b - hz) = x(a - hy) \text{ in } k[x, y, z, w]$$

x, w are coprime, $x \mid b - hz$.

$$b - hz = \alpha x$$

$$\Rightarrow b(P) = b(0, y_0, 0, w_0)$$

<u>contradiction</u>

$S = V(x, y)$ is exactly the set of poles of f.

14/2/14

Local properties of algebraic curves

k alg closed.

$V = V(F) \subset \mathbb{A}^2(k)$, $F \in k[x,y]$.

Def: Let $P \in V$, P is called *simple* (or *non-singular*) if

$$\frac{\partial F}{\partial x}(P) \neq 0 \quad \text{or} \quad \frac{\partial F}{\partial y}(P) \neq 0.$$

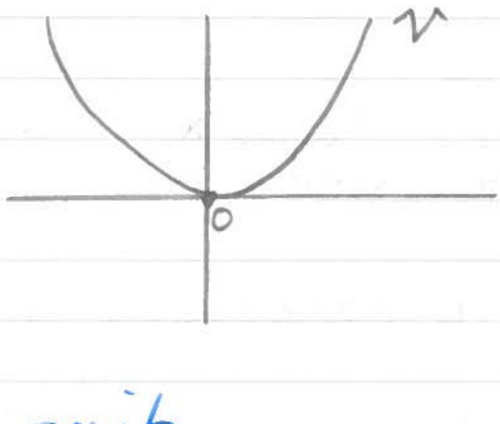
If $P = (a,b) \in V$ is simple, then the *tangent line to V at P* is

$$\left(\frac{\partial F}{\partial x}\right)(P)(x-a) - \left(\frac{\partial F}{\partial y}\right)(P)(y-b) = 0$$

Ex: $V = V(y - x^2)$

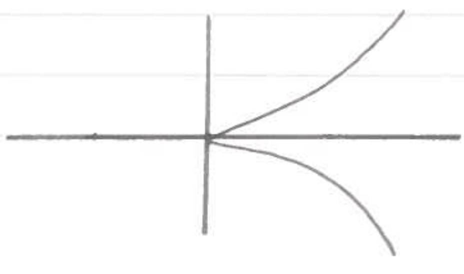
Any point of V is simple. In particular O is simple

Tangent line to V at O is $y = 0$.



Ex $V(y^2 - x^3)$

O is not a simple point.



Def: A point which is not simple is <u>multiple</u> (or <u>singular</u>)

Rem: V has at most finitely many singular points. otherwise:

$$(x,y) \text{ singular } \begin{cases} F(x,y) = 0 \\ \left(\frac{\partial F}{\partial x}\right)(x,y) = 0 \\ \left(\frac{\partial F}{\partial y}\right)(x,y) = 0 \end{cases}$$

$$\{\text{singular point}\} = V\left(F, \frac{\partial F}{\partial x}, \frac{\partial F}{\partial y}\right)$$

finite.

<u>Homogenous polynomials</u>.
$F \in k[x_1, \ldots, x_n]$ is homogenous of degree d if

$$F = \sum_{i_1 + \ldots + i_n = d} a_{i_1 \ldots i_n} x_1^{i_1} \ldots x_n^{i_n}$$

If F is homogenous of degree d, then

$$F(\lambda x_1, \ldots, \lambda x_n) = \lambda^d F(x_1 \ldots x_n)$$

sometimes called form

<u>Ex</u>: · $F(x,y) = x+y$ is homogenous of degree 1.

· $F(x,y) = x+y^2$ is not homogenous

· $F(x,y) = x^2+xy+y^2$ homogenous of degree 2.

· $F(x,y) = x^3+y^3+xy^2+x^2y$ homo of degree 3.

Any polynomial F can be written as

$$F = F_m + \dots + F_d.$$

when F_i is homogenous of degree i.

<u>Ex</u>: $F = \underbrace{x+y}_{=} + \underbrace{x^2}_{=} + \underbrace{y^3x + x^4}_{=}$

$$F = F_1 + F_2 + F_4$$

Look at $V(F)$, $F = F_m + \dots + F_d$.
$(F(0,0) = 0)$

m is called the <u>multiplicity</u> of V at P.
Notation: $m = m_P(V)$

<u>Lemma</u>: $P = (0,0)$ is a simple point of V
$\Leftrightarrow m_P(V) = 1$.

<u>Proof</u>: $F = F_1 + F_2 + \dots$

$$F_1 = ax + by.$$

$F = ax + by + \sum$ monomials of degree > 1

It's immediate that $\begin{cases} \frac{\partial F}{\partial x}(0,0) = a \\ \frac{\partial F}{\partial y}(0,0) = b \end{cases}$

P is simple $\iff a \neq 0$ or $b \neq 0$
$\iff F_1 \neq 0$.

Ex: · $F = y - x^2$ $(0,0)$ is a simple point.
$F_1 = y \neq 0$
$m_{(0,0)}(F) = 1$.

· $F = y^2 - x^2$ $(0,0)$ is a singular point. $F_1 = 0$.

If $P = (x_0, y_0) \neq 0$.
Look at $G = F(x + x_0, y + y_0)$
$(0,0) \in V(G)$.

Def: $m_P(V) = m_{(0,0)}(V(G))$

Lemma: k algebraic closed.
Let $F \in k[x,y]$ be homogenous polynomial of degree d.
Then
$$F = \prod_{i=1}^{d} (a_i x + b_i y)$$
for some $a_i, b_i \in k$.

Proof: F homogenous of deg d.

$$F(x,y) = x^d F\left(1, \frac{y}{x}\right)$$

Let $t = y/x$. $F(1,t)$ is in $k[t]$ and k is algebraic closed hence:

$$F(1,t) = \prod_{i=1}^{d} (a_i + b_i t)$$

So $F(x,y) = x^d F\left(1, \frac{y}{x}\right)$

$$= x^d \prod_{i=1}^{d} \left(a_i + b_i \frac{y}{x}\right) \qquad \square.$$

Ex: $F = x^2 - y^2 = x^2\left(1 - \left(\frac{y}{x}\right)^2\right)$

$$= x^2\left(1 - \frac{y}{x}\right)\left(1 + \frac{y}{x}\right)$$

$$= (x+y)(x-y).$$

Ex: $F = y^3 - x^3 \quad k = \mathbb{C}, \quad \omega = e^{2\pi i/3}$

$$= (y-x)(y-\omega x)(y-\omega^2 x)$$

when $k = \mathbb{R}$ $F = (y-x)\underbrace{(y^2+xy+x^2)}_{\text{irreducible}/\mathbb{R}}$

Def: $P = (0,0) \in V = V(F)$.

$$F = F_m + \dots + F_d.$$

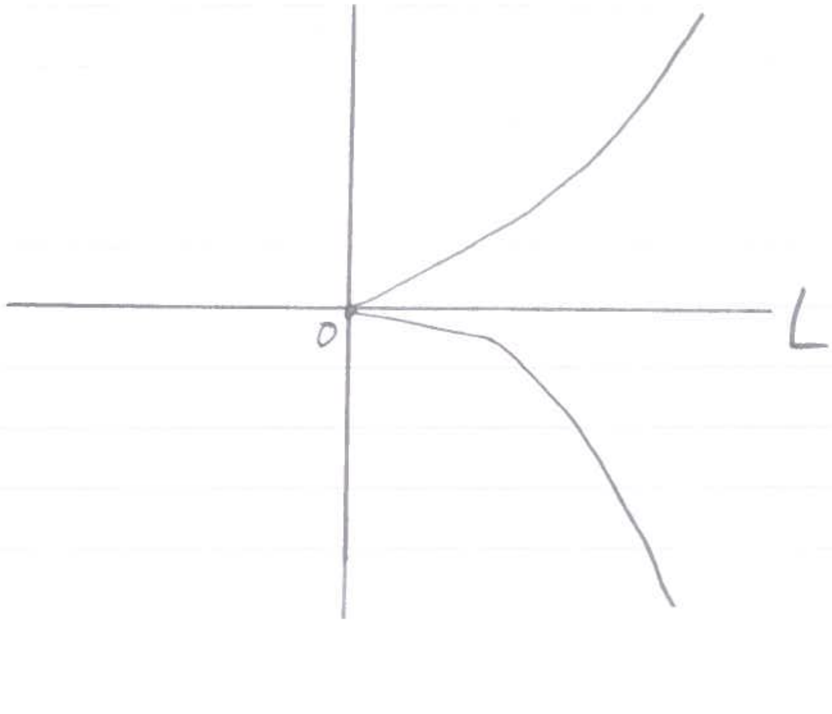
$$F_m = \prod_{i=1}^{m} (a_i x + b_i y)$$

$$= \prod_{i=1}^{m'} \underbrace{(a_i x + b_i y)^{e_i}}_{\text{distinct}}$$

Let L_i be $V(a_i x + b_i y)$, $i = 1, \dots, m$.
L_i's are called tangent lines to V at P.
e_i is called multiplicity of L_i.

Ex: $F = \underbrace{y^2}_{=F_2} - \underbrace{x^3}_{=F_3} \quad P = (0,0)$
$= F_2 + F_3$

$(0,0)$ is a singular point with $m_{(0,0)} V = 2$
One tangent $L = V(y)$ counted with multiplicity 2.



Ex: $F = y^2 - x^2(x+1)$, $P = (0,0)$

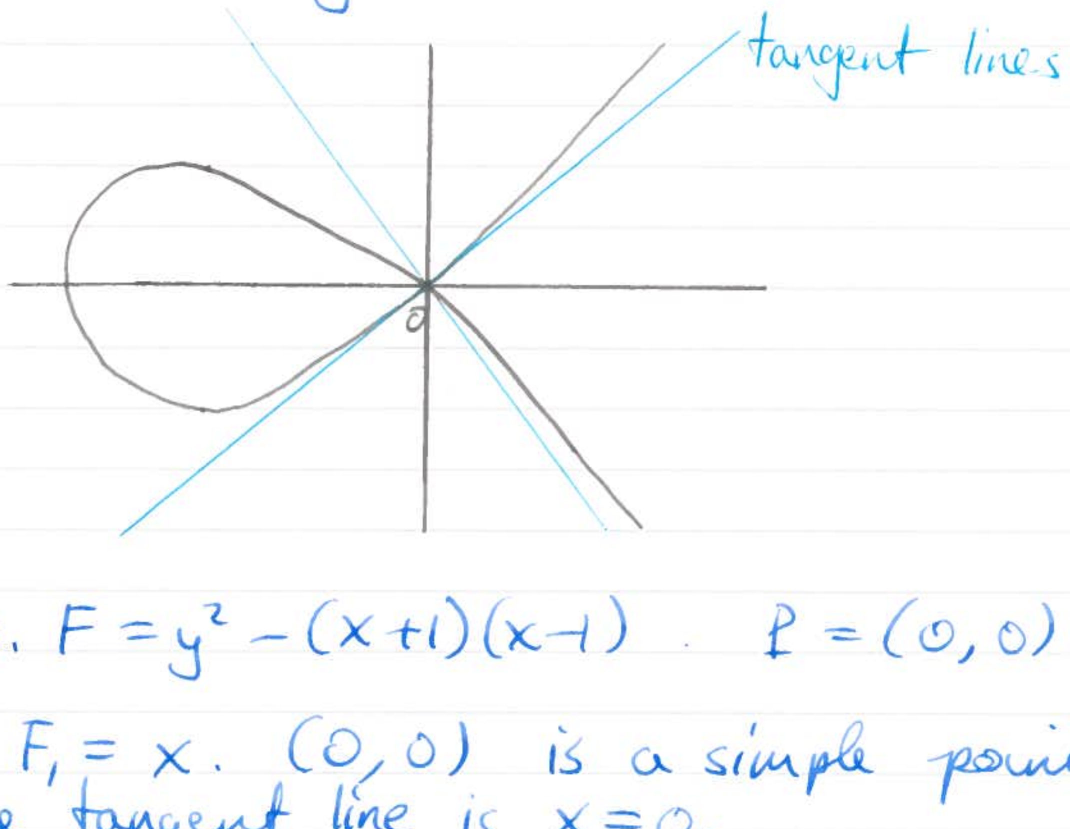
$$= y^2 - x^3 - x^2$$

$$= \underbrace{y^2 - x^2}_{F_2} \underbrace{- x^3}_{F_3}$$

$(0,0)$ is a multiple point with multiplicity 2.

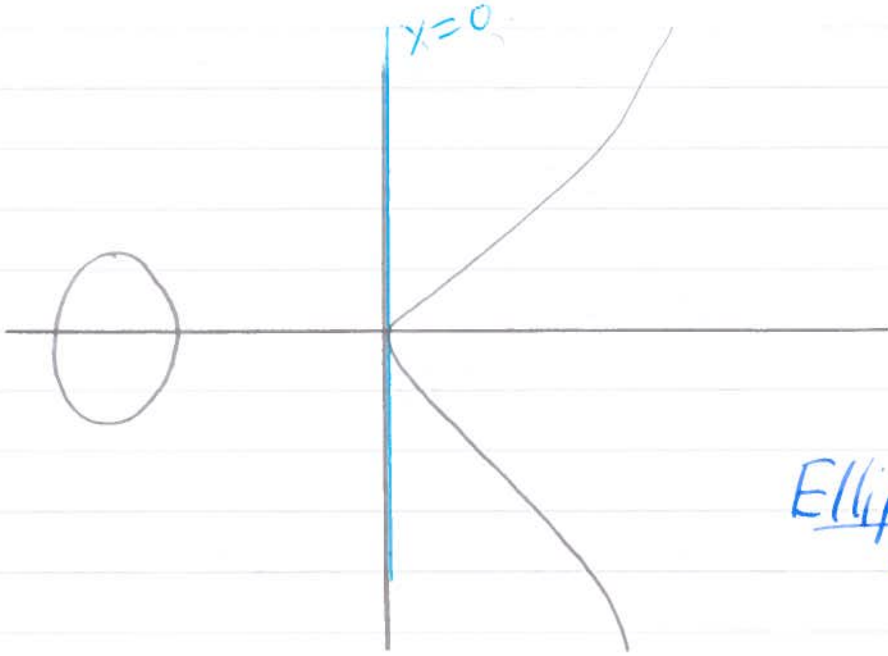
$$F_2 = y^2 - x^2 = (y-x)(y+x)$$

2 tangent lines with multiplicity 1, they are $y = x$ and $y = -x$.



Ex. $F = y^2 - (x+1)(x-1)$. $P = (0,0)$

$F_1 = x$. $(0,0)$ is a simple point and the tangent line is $x = 0$.



Elliptic curve!

26/2/14

Ex: $F = y^2 - 2y + 1 - x^3$.

Find singular points, multiplicities, tangent lines:

$$\begin{cases} F(x,y) = 0 = y^2 - 2y + 1 - x^3 \\ \frac{\partial F}{\partial x}(x,y) = 0 = -3x^2 \Rightarrow x = 0 \\ \frac{\partial F}{\partial y}(x,y) = 0 = 2y - 2 = y = 1 \end{cases}$$

$(0,1) \in V(F)$

This is the only singular point.

$$\begin{cases} x = x' \\ y = y' + 1 \end{cases} \qquad \begin{cases} x = x' \\ y' = y - 1 \end{cases}$$

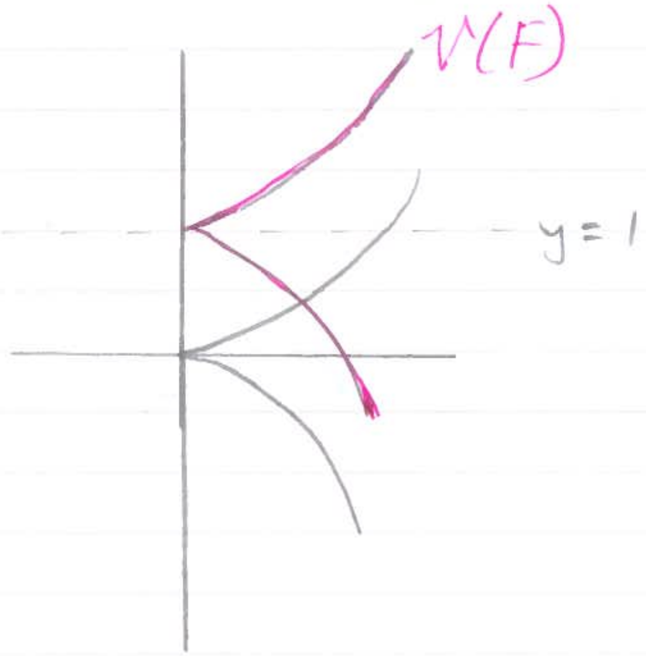
$$(y'+1)^2 - 2(y'+1) + 1 - x'^3$$

$$= y'^2 + 2y' + 1 - 2y' - 2 + 1 - x'^3$$

$$= y'^2 - x'^3$$

One singular point with multiplicity 2. One tangent line $y' = y - 1 = 0$ counted with multiplicity 2.

$P = (0,1)$ is the only singular point.
$m_P(V) = 2$
One tangent line $y=1$ counted with multiplicity 2.



$V \subset \mathbb{A}^k(k)$ affine varity.

$P \in V$. $\mathcal{O}_P(V) = \left\{ \frac{f}{g} \in k(V), \ g(P) \neq 0 \right\}$

= {Rational function defined at P}.

<u>Def</u>: A ring R is called local if R has a unique maximal ideal.

<u>Proposition</u>: R ring the following are equivalent
(1) R is local (has a unique max ideal)
(2) {Non-units in R} is an ideal.

Proof $(2) \Rightarrow (1)$ Let $M = \{\text{All non-units}\}$
By assumption M is an ideal. We need to show that its maximal.

Suppose $M \subsetneq I$ ideal. Then I contains a unit $\Rightarrow I = R$.

$(1) \Rightarrow (2)$ We assume that R has unique max ideal M.

Let $x \in R$ non-unit. Then $x \in m$ maximal
By assumption $m = M$.
$M \supset \{\text{all non-units}\}$ and because M is a maximal ideal, M can't contain a unit.
$M = \{\text{All non-units}\}$.

Examples:

1. Fix p prime.

$$\mathbb{Z}_{(p)} = \{ \tfrac{m}{n} \in \mathbb{Q} \text{ st } p \nmid n \}.$$

This is a local ring?

What is $\mathbb{Z}_{(p)}^*$? A unit in $\mathbb{Z}_{(p)}$ is $\frac{m}{n} \in \mathbb{Z}_{(p)}$ st $p \nmid m$.

It follows that a non-unit is $\frac{pm}{n} \in \mathbb{Z}_{(p)}$

$$\{\text{All non-units}\} = p\mathbb{Z}_{(p)}.$$

This is clearly an ideal $\Rightarrow \mathbb{Z}_{(p)}$ local ring, Its maximal ideal is $p\mathbb{Z}_{(p)}$

What is $\mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)} \simeq \mathbb{Z}/p\mathbb{Z}$.

$$\frac{\overline{n}}{\overline{1}} \leftarrow\!\shortmid \overline{n}$$

2. $R = \left\{ \frac{P}{Q} \in k(x) \, ; \, Q(0) \neq 0 \right\}$

(Notice: $R = \mathcal{O}_{(0)}(\mathbb{A}^1(k))$)

What is R^*? $R^\times = \left\{ \frac{P}{Q} \in R, \ P(0) \neq 0 \right\}$

Non-units: $M = \left\{ \frac{P}{Q} \in R, \ P(0) = 0 \right\}$

This is an ideal $\Rightarrow$ R is local.

$R/_M \simeq k$

$$\frac{P}{Q} \mapsto \left(\frac{P}{Q}\right)(0)$$

Yes

3. $R = \mathbb{Z}/9\mathbb{Z}$. Is this a local ring?

What are ideals of R? $(0), R$

They are images of $m\mathbb{Z}$ where $m|9$.
$m=1$ $I=R$
$m=9$ $I=(0)$
$m=3$ $I=(3)$

$R/I \simeq \mathbb{Z}/3\mathbb{Z}$ I is maximal.

—/—

Back to $\mathcal{O}_P(V) = \left\{ \frac{f}{g} \in k(V), g(P) \neq 0 \right\}$

<u>Lemma</u> $\mathcal{O}_P(V)$ is a local ring.

<u>Proof</u>: Define $m_P = \mathrm{Ker} \begin{pmatrix} \mathcal{O}_P(V) \xrightarrow{\varphi} k \\ z \to z(P) \end{pmatrix}$

φ is surjective because any element of k is the image of a constant function. Therefore $\mathcal{O}_P(V)/m_P \simeq k$ and m_P is a maximal ideal.

Non units in $\mathcal{O}_P(V)$ are exactly $z \in \mathcal{O}_P(V)$ st $z(P) = 0$ which is exactly m_P.

$\mathcal{O}_P(V)$ is a local ring, its maximal ideal is m_P and $\mathcal{O}_P(V)/m_P \simeq k$

—/—

<u>Def</u>: Let R be a local P.I.D
Then R is called a D.V.R = Discrete valuation ring.

$\nearrow$ R is integral

Prop : Let R be a D.V.R
There exist an irreducible element $t \in R$ st any $z \in R$ can be writtern in a unique way as $z = ut^n, n \geq 0$, u is a unit

Proof : Existance of t.

Let m be the maximal ideal of R,
R is a P.I.D $\Rightarrow m$ is principal.
Let t be a generator of m.
Let $z \neq 0$ in R. If z is a unit, then $z \cdot z \cdot t^0$
Take $n = 0$, $u = z$.
If $z \notin R^\times$, then $z \in m = (t)$.
$z = z_1 \cdot t$ for some $z_1 \in R$. if z_1 unit $\rightarrow$ done
$\vdots$ else $z_1 = z_2 t$.
$= z_2 \cdot t^2$
We construct a sequence (z_i) of elements of R st $\begin{cases} z = z_i t^i \\ z_i = z_{i+1} t \end{cases}$

If for some i, z_i is a unit then $n = i$, $z = \underbrace{z_n}_{\in R^\times} t^n$

Assume we have an increasing sequence of ideals.

$(z_1) \subset (z_2) \subset \dots (z_i) \subset (z_{i+1}) \subset \dots$

$\bigcup_{i=1}^{\infty} (z_i)$ is an ideal of R. (because $(z_i) \subset (z_{i+1})$)

R is a P.I.D $\bigcup_{i=1}^{\infty}(z_i) = (x)$ for some $x \in R$.

$$\Rightarrow \begin{cases} \forall i, \ (z_i) \subset (x) \\ \exists x, \ x \in (z_n) \end{cases}$$

$$\Rightarrow x \in (z_{n+1}) \subset (z_{n+2}) \subset \dots$$

$$\Rightarrow \begin{cases} (z_n) = (x) \\ (z_{n+1}) = (x) \end{cases}$$

$$\Rightarrow (z_n) = (z_{n+1})$$

$$\Rightarrow \exists u \in R^{\times}, \ z_{n+1} = u \cdot z_n = u t z_{n+1}$$

$$z_{n+1} \cdot (1 - ut) = 0$$

$z_{n+1} \neq 0$ because $z \neq 0$

$\Rightarrow 1 - tu = 0$ but t is not a unit

$\Rightarrow$ contradiction

<u>Uniqueness of t.</u>

$$z = ut^n = v \cdot t^m, \ n \geq m.$$

$$ut^n - vt^m = 0.$$

$$t^m \underbrace{(ut^{n-m} - v)}_{=0} = 0.$$

$\Rightarrow t^{n-m}$ is a unit

$\Rightarrow \underline{m = n}$

then $u = v$

$\square$

Def: t as in previous statement is called <u>uniformiser</u> of R.

Ex: $R = \left\{ \frac{P}{Q} \in k(x) : Q(0) \neq 0 \right\}$.

R is local maximal ideal $= \left\{ \frac{P}{Q} \in R, P(0) = 0 \right\}$

$$= \left\{ x\frac{P}{Q}, \frac{P}{Q} \in R \right\}$$

$$= (x).$$

R is a D.V.R

Uniformiser is x

If $P/Q \in R$. $\exists\, n$ st $P = xP'$ where $P'(0) = 0$

$$\frac{P}{Q} = x^n \underbrace{\left(\frac{P'}{Q}\right)}_{\text{unit}}$$

In $\mathbb{Z}_{(p)}$, $m = (p)$. D.V.R

Uniformiser $= p$.

—/—

Ex: $V = V(y^2 - x^3)$. $P = (0,0)$

$\mathcal{O}_P(V)$ is a local ring. It's not a D.V.R

It's not even a U.F.D.

x and y are irreducible, not associate,

$z = x^2 = y^3$ are 2 distinct factorisations of z.

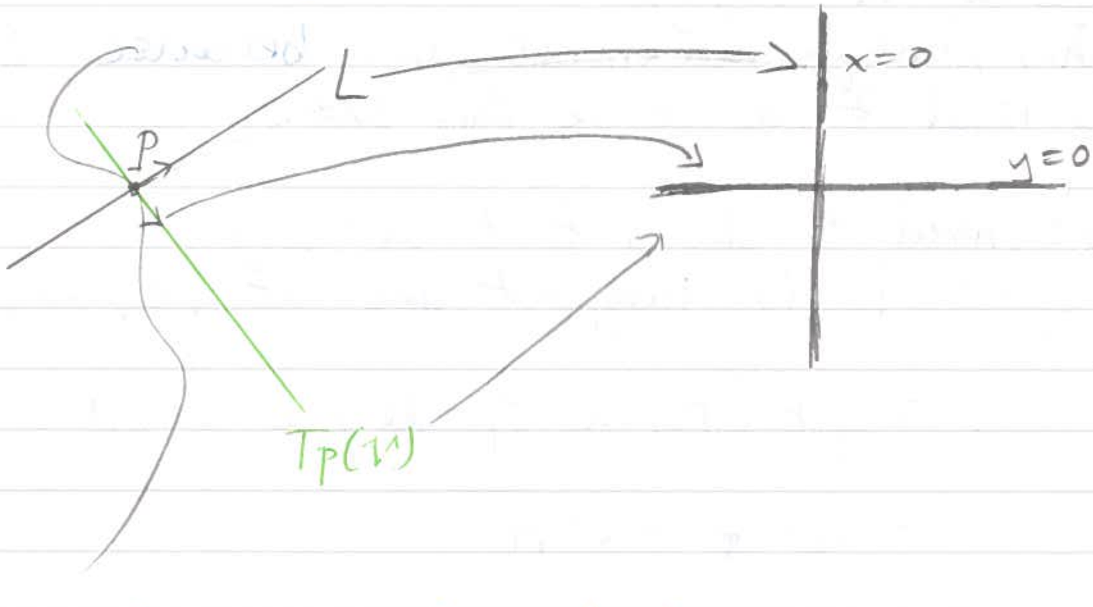
Theorem: $V = V(F)$ irreducible.
$P \in V$

P is a simple point iff $\mathcal{O}_P(V)$ is a DVR

If P is a simple point and L is any line through P which is not tangent to V, then the image of L is a uniformiser of $\mathcal{O}_P(V)$.

($L: ax + by + c = 0$. We can take image of $ax + by + c$ in $\Gamma(V) \hookrightarrow \mathcal{O}_P(V)$)

Proof: We only prove P simple $\Rightarrow \mathcal{O}_P(V)$ DVR.



By applying transformation of the form

$$\begin{pmatrix} x \\ y \end{pmatrix} \mapsto A \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} a \\ b \end{pmatrix}$$

Invertible matrix

we can move P to $\begin{pmatrix} 0 \\ 0 \end{pmatrix}$

L to $(x = 0)$

$T_V(V)$ to $(y = 0)$

$\begin{pmatrix}0\\0\end{pmatrix} = T(P)$ is a simple point on $T(V)$

T induces an isomorphism $\mathcal{O}_P(V) \simeq \mathcal{O}_{(0,0)}(T(V))$
We can assume $P = (0,0)$, $L = (x=0)$,
$T_P(V) = (y=0)$.

—/—

$\mathcal{O}_P(V)$ is a local ring.
We need to show that $m_P = (x)$.

Claim $m = (x,y)$.
This ideal is maximal and because $\mathcal{O}_P(V)$ is local it has to be this one.

We need to show that $m = (x)$.
$y=0$ is the tangent line at $(0,0)$, then

$$F = y + (\text{terms of degree} > 1)$$
$$= y \cdot G + x^2 H.$$

(G collects all terms involving y)

P is a simple point, $G = 1 +$ higher order term.
$$\Rightarrow G(0,0) \neq 0.$$

In $\Gamma(V)$: $0 = \bar{F} = \bar{y} \cdot \bar{G} + \bar{x}^2 \cdot \bar{H}$.
$$\begin{cases} \bar{y} \cdot \bar{G} = -\bar{x}^2 \bar{H} \\ \bar{G}(0,0) \neq 0 \end{cases}$$

In $k(V)$, $\bar{y} = -\bar{x}^2 \dfrac{\bar{H}}{\bar{G}} \in \mathcal{O}_P(V)$
because $\bar{G}(0,0) \neq 0$.

In $\mathcal{O}_P(V)$, $\bar{y} \in (\bar{x}^2) \subset (\bar{x})$

$$\Rightarrow m_P = (\bar{x}, \bar{y}) = (\bar{x})$$

$\square$.

<u>Rem</u>: V, W 2 curves.
Suppose V and W are isomorphic
$\exists \varphi : V \to W$ polynomial s.t.
φ induces an isomorphism $\Gamma(W) \to \Gamma(V)$.
Then φ will induce an isomorphism

$$\mathcal{O}_{\varphi(P)}(W) \simeq \mathcal{O}_P(V).$$

By theorem P is a simple point V iff $\varphi(P)$ is a simple point on W.

<u>Ex</u>: Is $V(y^2 - x^3)$ isomorphic to $\mathbb{A}^1$?

<u>No</u>! Because $V(y^2 - x^3)$ has a singular point at 0 and $\mathbb{A}^1$ has no singular points.

Similarly $V(y^2 - x^3)$ is not isomorphic to $V(y - x^2)$.

28/2/14

Intersection number

$F, G \in k[x,y]$. not necessarily irreducible. $P \in \mathbb{A}^2(k)$

There exists a unique $I(P,F,G) \geq 0$ integer (possibly infinite) which satisfies:

← sometimes called $I(P, F \cap G)$

1) $I(P,F,G) = 0 \iff P \notin V(F) \cap V(G)$

2) $I(P,F,G) = \infty$ if $V(F)$ and $V(G)$ have a common component and $P \in$ this component.

3) If T is an affine transformation

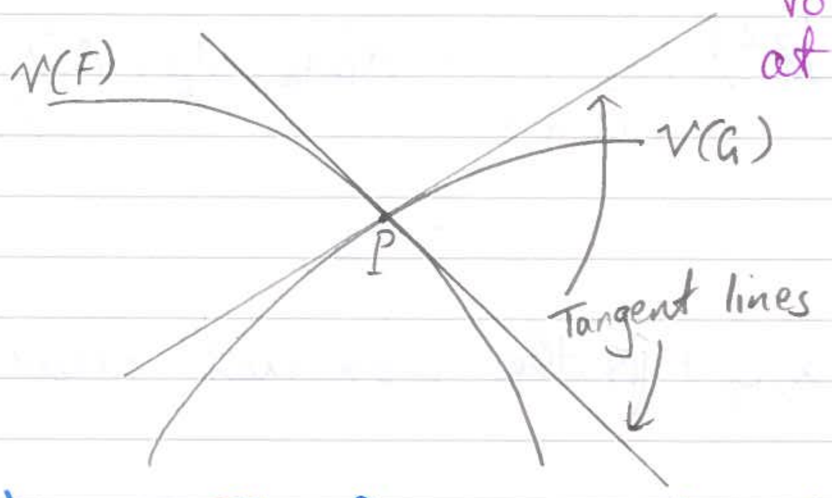
$$\begin{pmatrix} x \\ y \end{pmatrix} \to A \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} a \\ b \end{pmatrix}$$

where A is an invertible 2×2 matrix. Then $I(P,F,G) = I(T(P), T(F), T(G))$

4) $I(P,F,G) = I(P,G,F)$.

5) If $V(F)$ and $V(G)$ intersect transversaly then $I(P,F,G) = m_P(F) \cdot m_P(G)$

All tangent lines to $V(F)$ and $V(G)$ at P are distinct



6) $F = \prod F_i^{r_i}$ F_i irreducible
$G = \prod G_j^{s_j}$ G_j irreducible.
$I(P,F,G) = \sum r_i s_j I(P, F_i, G_j)$

7) $\forall A \in k[x,y]$, $I(P,F,G) = I(P,F,G+A\cdot F)$

Theorem: There exist a unique number $I(P,F,G)$ satisfying (1) – (7).
It is given by $\dim_k \left(\mathcal{O}_P(\mathbb{A}^2) / (F,G) \right)$

If F and G have no common component then

$$\sum_{P \in \mathbb{A}^2} I(P, F, G) = \dim_k \left(k[x,y] / (F,G) \right)$$

— / —

Examples: 1) $F = x$, $G = y$. $P = (0,0)$

$V(F)$ and $V(G)$ intersect transversaly
$m_P(F) = m_P(G) = 1$

By property (4),

$$I(P, F, G) = m_P(F)\, m_P(G) = 1.$$

$$\dim_k \mathcal{O}_P(\mathbb{A}^2) / (F,G) = \dim_k \mathcal{O}_P(\mathbb{A}^2) / (x,y)$$

$$= 1$$

because (x,y) is the maximal ideal of $\mathcal{O}_P(\mathbb{A}^2)$

Also: $\dim_k k[x,y] / (x,y) = 1 = \sum_{P \in \mathbb{A}^2} I(P, x, y)$

(there is only one point of intersection, it is 0)

2) $F = x$, $G = x^2 + y^2$ in $\mathbb{A}^2(\mathbb{C})$
$V(F)$ and $V(G)$ do not intersect transversaly
The line $x = 0$ is a common tangent line.

$$I(P, \underbrace{x}_{F}, \underbrace{x^2+y^2}_{G}) =$$

$$\text{By } \underline{\text{property (7)}},\ I(P, x, x^2+y^2) \overset{(7)}{=} I(P, F, G - xF)$$

$$= I(P, x, y^2)$$

By $\underline{\text{property (6)}}$,
$$= 2\underbrace{I(P, x, y)}_{1}$$

$$= 2$$

Here again $V(F)$ and $V(G)$ intersect at P only,

$$I(P, F, G) = \sum_{P \in \mathbb{A}^2} I(P, F, G)$$

$$= \dim_k k[x,y] / (x, x^2+y^2)$$

Note $\bar{x}, \bar{y}$
$$\begin{cases} \bar{x} = 0, \ \bar{x}^2 + \bar{y}^2 = 0 \\ \bar{y}^2 = 0 \end{cases}$$

A basis for $k[x,y]/(x, x^2+y^2)$ is $\{1, \bar{y}\}$
$$\dim_k k[x,y] / (x, x^2+y^2) = 2.$$

Ex: $F = xy$. $G = x^2+y^2$. $P = (0,0)$

$I(P, xy, x^2+y^2) = ?$

By property (6) $= \underbrace{I(P, x, x^2+y^2)}_{=2} + \underbrace{I(P, y, x^2+y^2)}_{=2}$

$= 2+2 = 4.$

$P=(0,0)$ is the only point in $V(G) \cap V(F)$

$$I(P,F,G) = \dim_k k[x,y] / (xy, x^2+y^2)$$

Note: $\begin{cases} \bar{x}\bar{y} = 0 \\ \bar{x}^2 + \bar{y}^2 = 0 \end{cases}$

$$\bar{P} = \sum a_{ij} \bar{x}^i \bar{y}^j$$

$$= \sum a_{ij} \bar{x}^i + \underbrace{\sum b_j \bar{y}^j}_{b_1 + b_2 \bar{y}}$$

A basis is $1, \bar{x}, \bar{y}, \bar{x}^2$.

$$\dim_k \left(k[x,y] / (xy, x^2+y^2) \right) = 4.$$

—/—

Ex: $F = x^2 + y^3$, $G = x^3 + y^2$, $\quad P = (0,0)$

$$I(P, F, G) = I(P, \underbrace{x^2 + y^3}_{F}, \underbrace{x^3 + y^2}_{G})$$

$$xF = x^3 + xy^3, \quad G = x^3 + y^2$$

$$xF - G = xy^3 - y^2$$

$$= y^2[xy - 1]$$

$$I(P, F, G) = I(P, F, xF - G) \quad \text{(Property 7)}$$

$$= I(P, x^2 + y^3, y^2[xy - 1])$$

$$\overset{(6)}{=} I(P, x^2 + y^3, y^2)$$

$$+ \underbrace{I(P, x^2 + y^3, xy - 1)}_{= 0}$$

$$\overset{(6)}{=} 2\, I(P, x^2 + y^3, y)$$

$$\overset{(7)}{=} 2\, I(P, x^2, y)$$

$$\overset{(6)}{=} 4\, I(P, x, y)$$

$$= 4.$$

For $k[x,y]/(x^2 + y^3, x^3 + y^2)$, $\{1, \bar{x}, \bar{y}, \bar{x}^2\}$ are the basis

Rem In all the above examples, P was the only point intersection, $I(P, F, G) = m_P(F) \cdot m_P(G)$

Ex: $F = y^2 - x^5$

$$G = y^2 x^2 - x^5 - y^5 \quad , \quad P = (0,0)$$

$$\begin{aligned}
I(P, F, G) &= I(P, y^2 - x^5, y^2x^2 - x^5 - y^5) \\
&\overset{(7)}{=} I(P, y^2 - x^5, y^2x^2 - y^2 - y^5) \\
&= I(P, y^2 - x^5, y^2[x^2 - 1 - y^3]) \\
&\overset{(6)+(1)}{=} I(P, y^2 - x^5, y) \\
&\overset{(7)}{=} 2 I(P, x^5, y) \\
&= 10 I(P, x, y) \\
&= 10.
\end{aligned}$$

5/3/14

Hint for excercise sheet.

$V = V(y^2 - x^3)$, $P = (0,0)$

- $\mathcal{O}_P(V)$ not a D.V.R
- $\mathcal{O}_P(V)$ not even a U.F.D

1) $\bar{x}$ any $\bar{y}$ are irreducible in $\mathcal{O}_P(V)$.
2) Not associate
3) $\mathcal{O}_P(V)$ not a UFD.

Show that $\bar{x}$ is irreducible:

$$\bar{x} = f \cdot g \text{ where } f, g \in \mathcal{O}_P(V)$$
$$\Rightarrow f \text{ or } g \text{ is a unit}$$

$$f = \frac{a}{b}, \quad g = \frac{c}{d} \quad \text{where } a,b,c,d \in \Gamma(V), \; b(P) \neq 0, \; d(P) \neq 0$$

Need to show that either $a(P) \neq 0$ (f unit) and $c(P) \neq 0$ (g unit)

Recall that:

$$V = \{(t^2, t^3) : t \in k\}$$

$$x = \frac{a}{b} \cdot \frac{c}{d} \Rightarrow (\bar{b} \cdot \bar{d})\bar{x} = \bar{a} \cdot \bar{c} \text{ in } \Gamma(V)$$

$$\Rightarrow (b \cdot d)x = a \cdot c + (y^2 - x^3) \quad (*)$$

$b(0,0) \neq 0, \quad d(0,0) \neq 0 \quad x, a, b, c, d \in k[x,y]$

$\forall t \quad (b \cdot d)(t^2, t^3) \cdot t^2 = a(t^2, t^3) \cdot c(t^2, t^3)$
in $k[t]$

$(*)$ $t^2 | a(t^2, t^3) c(t^2, t^3)$

Suppose $t^2 | a(t^2, t^3)$, then $a(t^2, t^3) = t^2 \cdot \alpha(t)$

$\Rightarrow (b \cdot d) t^2 = t^2 \cdot \alpha \cdot c$
$\Rightarrow (b \cdot d) = \alpha \cdot c$

$(b \cdot d)(0) \neq 0 \Rightarrow c(0) \neq 0$

$\Rightarrow g = \frac{c}{d}$ is a unit.

$(*)$ if $t^2 | c(t^2, t^3)$ then $a(P) \neq 0$

$\Rightarrow f$ is a unit.

$(*)$ if $t^2 | a(t^2, t^3)$ and $t^2 | b(t^2, t^3)$

$a(P) = 0$.
$a = \alpha_0 t^2 + \beta_0 t^3 + $ (terms involving t^r
$r > 2$)

$= t^2(\alpha_0 + \beta_0 + \text{rest})$

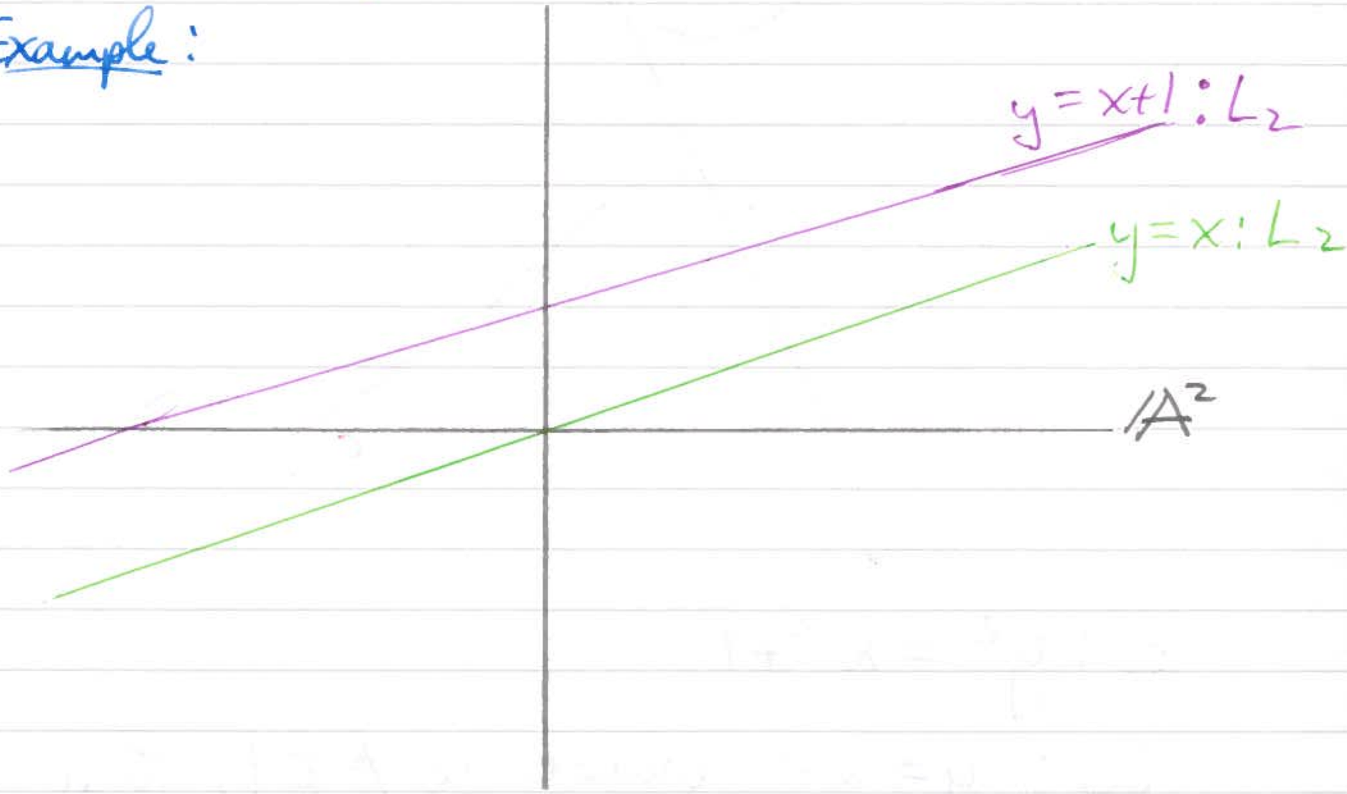
$\Rightarrow t^2 = a(t^2, t^3) \Rightarrow g$ is a unit

This case does not happen

—/— (Back to lectures)

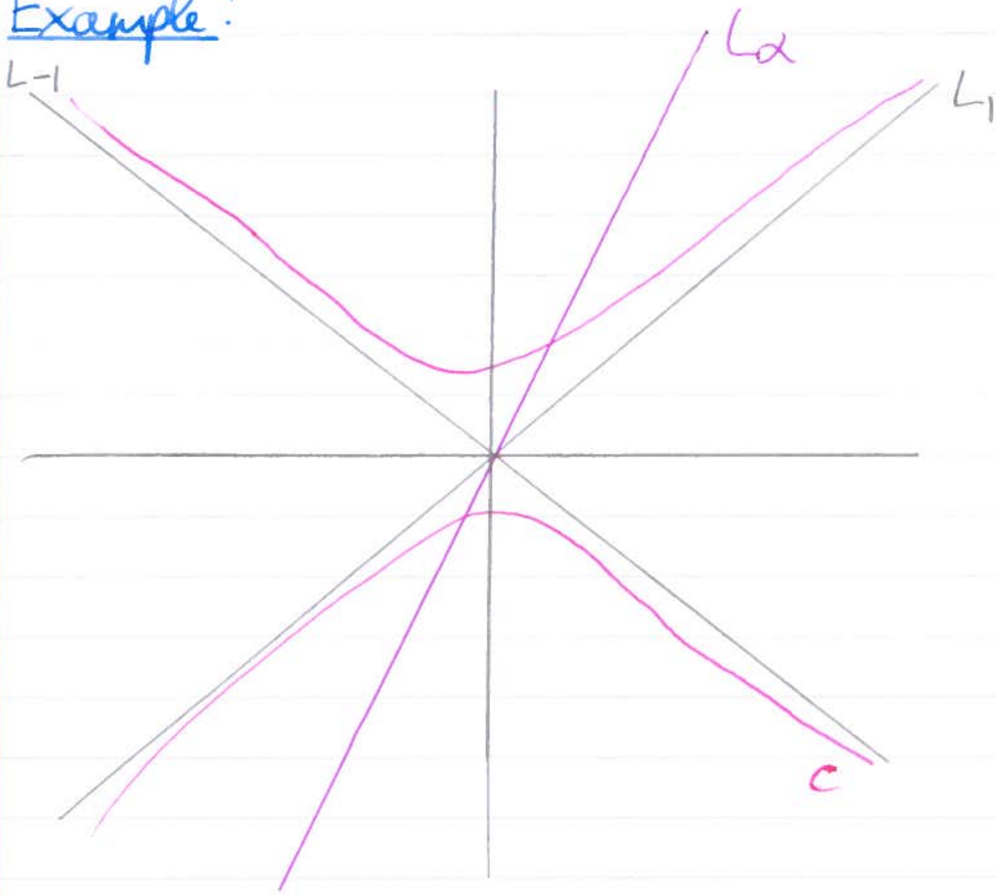
Projective algebraic sets.

Example:



L_1 and L_2 do not intersect in $\mathbb{A}^2$. We want to give meaning to saying that they intersect at ∞.

Example:



$C: y^2 = x^2+1$

$L_\alpha: y = \alpha x$ where $\alpha \neq \pm 1$, then:

$|L_\alpha \cap C| = 2$ with intersection number 1 at each point. If $\alpha = \pm 1$ then $L_{\pm 1} \cap C = \emptyset$ in $\mathbb{A}^2$. But C is asymptotic to $L_{\pm 1}$, we want to say that C intersects $L_{\pm 1}$ at ∞.

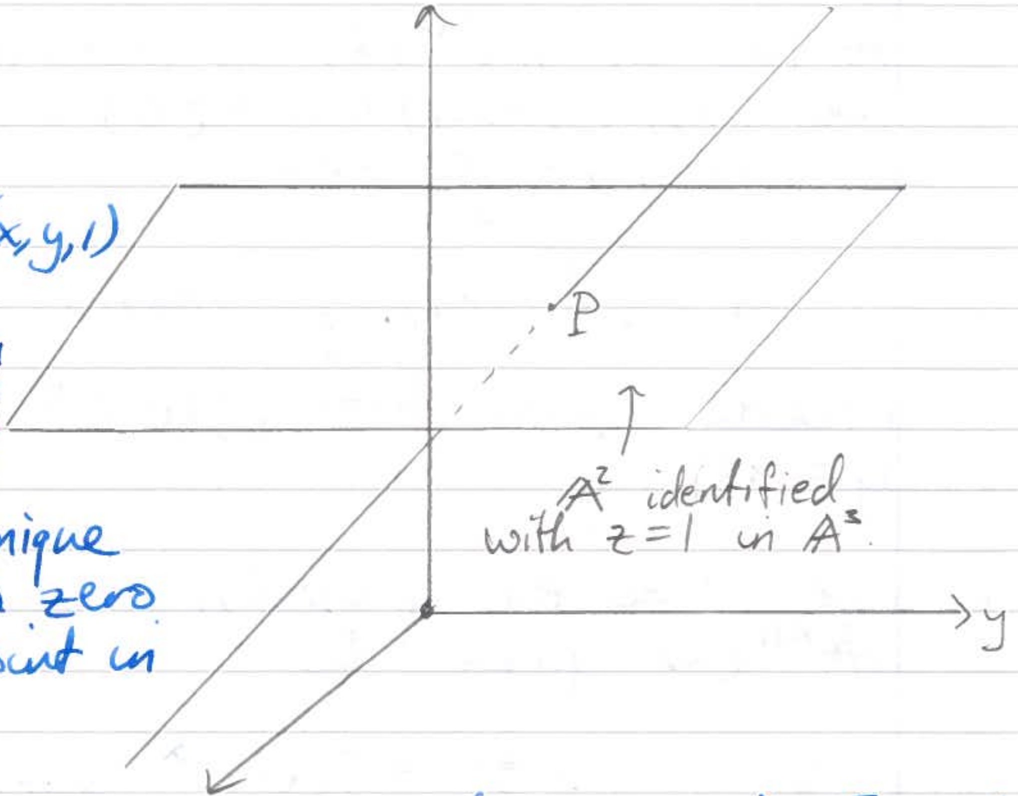
Projective space = enlarge $\mathbb{A}^n$ by adding a number of "points at infinity."

$n=2$:

$\mathbb{A}^2 \subset \mathbb{A}^3$

$(x,y) \mapsto (x,y,1)$

Any point in $\mathbb{A}^2$ (identified with $z=1$) defines a unique line through zero and this point in $\mathbb{A}^3$.



Conversely, any line through zero in $\mathbb{A}^3$ not contained in $z=0$ defines a unique point in $\mathbb{A}^2$ ($z=1$): the unique point where the line intersects $\mathbb{A}^2$ ($z=1$).

Same construction works for $\mathbb{A}^n \subset \mathbb{A}^{n-1}$ identified with $x_{n+1}=1$.

<u>Definition</u>: Let k be a field, $n \geq 0$ an integer, then:

$$\mathbb{P}^n(k) = \{\text{lines in } \mathbb{A}^{n+1}(k) \text{ through } 0\}$$

we called $\mathbb{P}^n(k)$ the projective space of dimension n over k.

A line in $\mathbb{A}^{n+1}(k)$ the projective space of dimension n over k!

A line in $\mathbb{A}^{n+1}(k)$ is determined by any $(x_1, \ldots, x_{n+1}) \in L \setminus \{0\}$ (where the line L goes through zero).

$$L_x = \{(\lambda x_1, \ldots, \lambda x_{n+1}) : \lambda \in k\}.$$

clearly $L_x = L_y \Leftrightarrow \exists \lambda \in k^\times$ such that $y = \lambda x$.

Let $\sim$ be the equivelence relation on $\mathbb{A}^{n+1}(k)$ given by

$$x \sim y \Leftrightarrow \exists \lambda \in k^\times \text{ such that } y = \lambda x.$$

Then an equivalent definition is:

$$\mathbb{P}^n(k) \cong \mathbb{A}^{n+}(k) / \sim$$

An element of $\mathbb{P}^n(k)$ is called a point.

If $P \in \mathbb{P}$ corresponds to $(x_1, \ldots, x_{n+1}) \in \mathbb{A}^{n+1}(k) \setminus \{0\}$ then $(x_1, \ldots, x_{n+1})$ are called projective coordinates of P.

Notation:

$$P = [x_1 : x_2 : \ldots : x_n].$$

Definition

Let $1 \leq i \leq n+1$. Define:

$$U_i = \{[x_1 : \dots : x_{n+1}] \in \mathbb{P}^n(k) : x_i \neq 0\}$$

If $[x_1 : \dots : x_{n+1}] \in U_i$ then

$$[x_1 : \dots : x_{n+1}] =$$

$$[y_1 : \dots : 1 : \dots : y_{n+1}]$$

where $y_k = \frac{x_k}{x_i}$ $\quad$ i^{th} position

Let $\varphi_i : \mathbb{A}^n \longrightarrow U_i$

$$(x_1, \dots, x_n) \longmapsto [x_1 : \dots : 1 : \dots x_n]$$

φ_i is a bijection, one can think of U_i as $\mathbb{A}^n$ viewed as subset of $\mathbb{P}^n$ via φ_i

Then:

$$\mathbb{P}^n = \bigcup_{i=1}^{n+1} U_i$$

One can (and should) think of $\mathbb{P}^n$ as a union of $n+1$ copies of $\mathbb{A}^n$.

Another decomposition of $\mathbb{P}^n$

$$[x_1, \dots, x_{n+1}] \in \mathbb{P}^n$$

By def of proj. coordinates some $x_i \neq 0$.

Suppose : $x_1 \neq 0$

$$\mathbb{P}^n = \underbrace{\{[x_1 \dots x_{n+1}], x_i \neq 0\}}_{\{[1 : x_2 : \dots x_{n+1}]\} \overset{\varphi_1}{=} \mathbb{A}^n} \cup \overbrace{\{[0 : x_2 : \dots : x_{n+1}]\}}^{\mathbb{P}^{n-1}}$$

$$\mathbb{P}^n = \mathbb{A}^n \cup \mathbb{P}^{n-1}$$

$$= \mathbb{A}^n \cup \mathbb{A}^{n-1} \cup \mathbb{P}^{n-2}$$

$$= \dots = \mathbb{A}^n \cup \mathbb{A}^{n-1} \cup \dots \cup \mathbb{A}^1 \cup \mathbb{A}^0$$

This is a decomposition of $\mathbb{P}^n$ as a <u>disjoint</u> union of affine spaces.

<u>Ex</u>: <u>$n=0$</u> $\mathbb{P}^0 = \{\text{lines in } \mathbb{A}^1\}$

There is only one line, $\mathbb{A}^1$ itself,

$$\mathbb{P}^0 = \{1 \text{ point}\}$$

<u>$n=1$</u> $\mathbb{P}^1$ projective line.

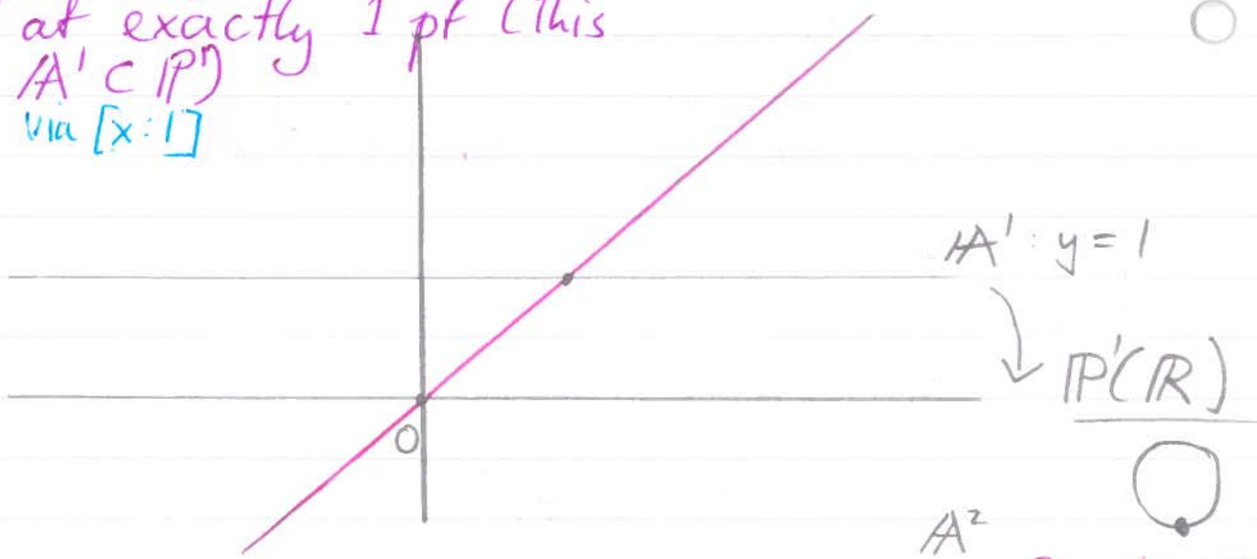
$$\mathbb{P}^1 = \{[x_1 : x_2] : x_1 x_2 \neq 0\}.$$

$$\ldots = \{\underbrace{[x_1 : 1]}_{\mathbb{A}^1}\} \cup \{[1:0]\}$$

$$\mathbb{P}^1 = \mathbb{A}^1 \cup \{\text{A point}\}$$

called "point at infinity"

Any line $\neq (y=0)$ intersects $\mathbb{A}^1$ at exactly 1 pt (This is $\mathbb{A}^1 \subset \mathbb{P}^1$)
via $[x:1]$



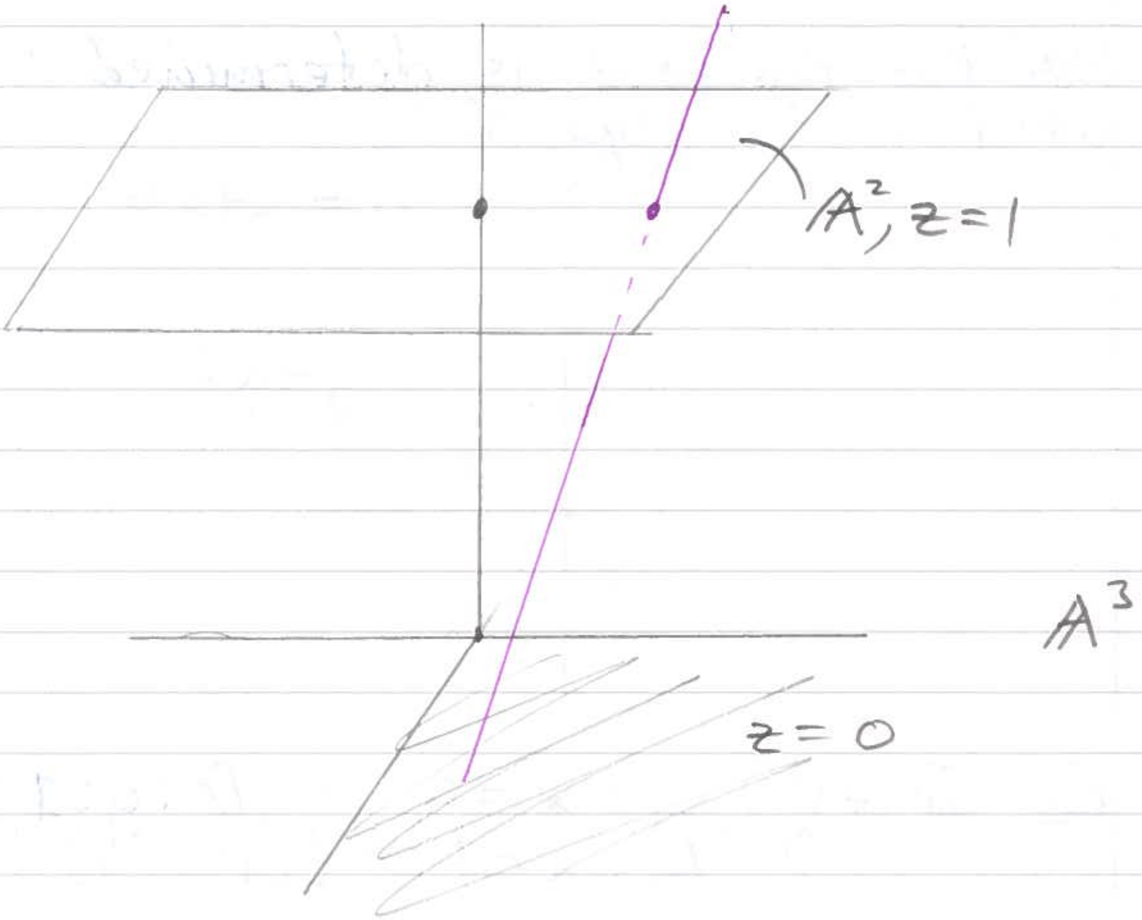
Remark: $\mathbb{P}^1_{\mathbb{C}}$ = sphere in $\mathbb{R}^3$

The line $\underline{y=0}$ defines the point at infinity of $\mathbb{P}$

$\underline{n=2}$ $\mathbb{P}^2 = \{[x:y:z] : xyz \neq 0\}$

$$= \{\underbrace{[x:y:1]}_{=\mathbb{A}^2}\} \cup \{\underbrace{[x:y:0]}_{=\mathbb{P}^1}\}$$

// {lines through O in $\mathbb{A}^3$ contained in the plane $z=0$} = lines at infinity in $\mathbb{P}^2$



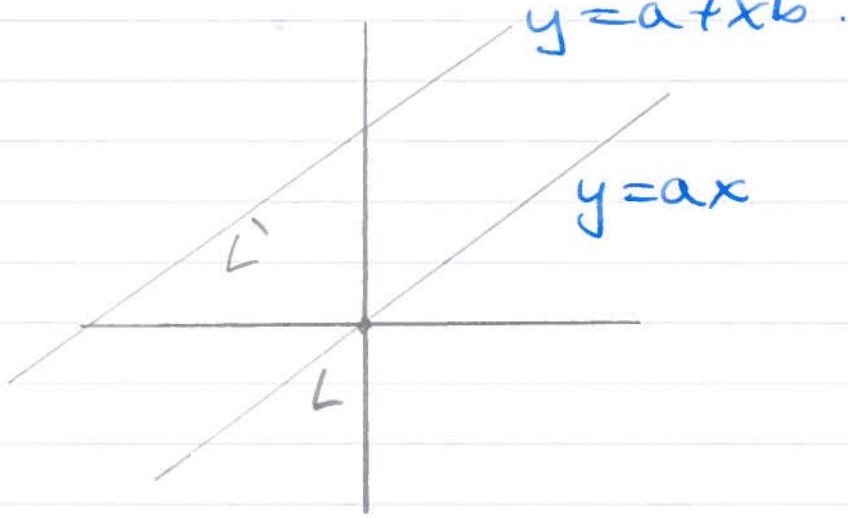
Let $L: y = ax + b$ be a line in $\mathbb{A}^2$. With respect to identification $\mathbb{A}^2 = \{[x:y:1]\}$,
$L = \{[x : ax+b : 1]\} \subset \mathbb{P}^2$
$\bar{L} = \{[x : ax+bz : z]\} \subset \mathbb{P}^2$.
$= \{$Points in $\mathbb{P}^2$ whose intersection with $\mathbb{A}^2$ in $L\}$.

Points on $\bar{L}$ which are not in $\mathbb{A}^2$ are those for which $z=0$.

Exactly one point $[1:a:0]$

$$\bar{L} = L \cup \underbrace{\{[1:a:0]\}}_{\text{Point at infinity of } L}$$

Note that this point is determined by a which is the slope of L.



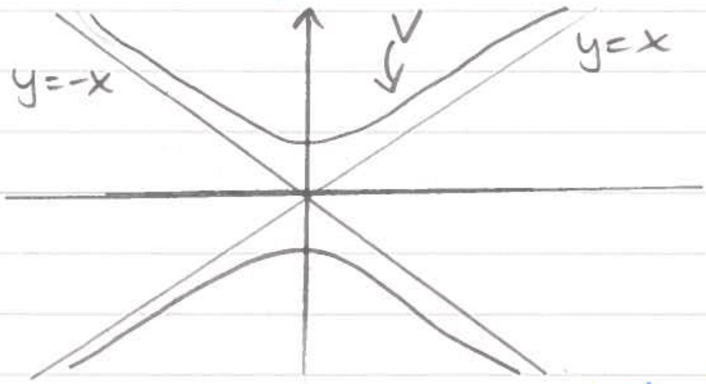
Ex: In $\mathbb{A}^2$: $L_1 : x = 0 \sim \{[0:y:1]\} \subset \mathbb{P}^2$
$(z=1)$ $L_2 : x = 1 \sim \{[1:y:1]\} \subset \mathbb{P}^2$

$$\begin{cases} \bar{L}_1 = \{[0:y:z]\} \subset \mathbb{P}^2 \\ \bar{L}_2 = \{[z:y:z]\} \end{cases}$$

$$\bar{L}_1 \cap \bar{L}_2 = \{[0:1:0]\}.$$

$\bar{L}_1$ and $\bar{L}_2$ ~~inect~~ meet at exactly one point of $\mathbb{P}^2$ which is $[0:1:0]$

$\underline{Ex}$: $V : y^2 \underset{P_1}{=} x^2 + 1 \subset \mathbb{A}^1$



$\overline{V} = \{[x:y:z] \in \mathbb{P}^2 : y^2 = x^2 + z^2\}$

$\overline{V} \cap \underset{(z=1)}{\mathbb{A}^2} = V$

What is $\overline{V} \setminus V$.

$$\overline{V} \setminus V = \{[x:y:0],\ y^2 = x^2\}$$
$$= \{[x:y:0],\ y = \pm x\}$$
$$= \{\underbrace{[1:1:0]}_{P_1}\} \cup \{\underbrace{[1:-1:0]}_{P_2}\}.$$

$L_1 : y = x \sim [x:x:1]$

$\overline{L_1} := \{[x:x:z] \in \mathbb{P}^2\}$

$$\overline{L_1} \setminus L_1 = \{[x:x:0]\} = \{[1:1:0]\}$$
$$= P_1$$

$L_2 : y = -x \sim [x:-x:1]$

$\overline{L_2} = \{[x,-x:z]\}$. $\overline{L_2} \setminus L_2 = \{P_2\}$.

7/3/14

$\mathbb{P}^n = \{[x_1 : \dots : x_{n+1}] \ ; \ (x_1, \dots, x_{n+1}) \neq 0\}$.

$= \bigcup_{i=1}^{n+1} U_i \qquad \phi_i : \mathbb{A}^n \to U_i$

$= \mathbb{A}^n \cup \underbrace{\mathbb{P}^{n+1}}_{\text{points at } \infty}$ disjoint

Algebraic subsets of $\mathbb{P}^n$. k infinite.

$F \in k[x_1, \dots, x_{n+1}]$, $\underset{[a_1 : \dots : a_{n+1}]}{P} \in \mathbb{P}^n$

Does it make sense to talk about $F(P)$?

No. $F(P) = F(a_1, \dots, a_{n+1})$ depends on the choice of $[a : \dots : a_{n+1}]$; and these are defined up to multiplication by $\lambda \in k^*$

Def: $V_p(F) = \{P \in \mathbb{P}^n$ st $F(P) = 0$ for any choice for homogenous coordinates for $P\}$.

Rem: Suppose F homogenous of degree d, which means $F(\lambda x_1, \dots, \lambda x_{n+1}) = \lambda^d F(x_1, \dots x_{n+1})$. Then if $F(P) = 0$ for one choice of hom. coordinates for P then it will be zero for any other choice.

Let $P = [a_1, \dots, a_{n+1}]$
Suppose that $F(a_1, \dots, a_{n+1}) = 0$,

Another choice of homogenous coordinates for P is $[\lambda a_1 : \dots : \lambda a_{n+1}]$ for some $\lambda \in k^\times$

$$F(\lambda a_1, \dots, \lambda a_{n+1}) = \lambda^d \underbrace{F(a_1, \dots, a_{n+1})}_{=0} = 0.$$

Let F be any polynomial

$F = F_m + \dots + F_d$ $\quad F_i$ hom. of degree i.

Suppose $P \in V_P(F)$ where $P = [a_1 : \dots : a_{n+1}]$

By definition, that means that

$$\forall \lambda \in k^\times, \; F(\lambda a_1, \dots, \lambda a_{n+1}) = 0$$
$$= \lambda^m F_m(a_1, \dots, a_{n+1}) + \dots + \lambda^d F_d(a_1, \dots a_{n+1})$$

As k infinite, that implies

$$F_m(a_1, \dots, a_{n+1}) = \dots = F_d(a_1, \dots, a_{n+1}) = 0$$

$$\Rightarrow V_P(F) = V_P(F_m, \dots, F_d)$$

homogenous

$\Rightarrow$ $V_P(F)$ can be defined by homogenous polynomials.

Def: Let S be a subset of $k[x_1 \dots x_n]$
Define $V_P(S) = \bigcap_{F \in S} V_P(F) \subset \mathbb{P}^n$.

By previous remarks we can always choose S' to consist of homogenous polynomials.

<u>Def</u>: A projective algebraic set is a subset of $\mathbb{P}^n$ of the form $V_P(S')$.

<u>Example</u>: $\mathbb{P}^n$ itself is algebraic, it's $V_P(0)$
$\emptyset$ is also algebraic. $\emptyset = V_P(1)$
$V_P(x_1, \ldots, x_{n+1}) = \emptyset$ (because $[0 : \ldots : 0]$ does not exist !!!).

—/—

Algebraic subsets of $\mathbb{P}^1$
Let X be an algebraic subset of $\mathbb{P}^1$. ← There is always $\emptyset$, $\mathbb{P}^1$
$\exists S \subset k[x, y]$ consisting of homogenous polynomials.

$$X = \bigcap_{F \in S'} V_P(F)$$

Enough to consider $V_P(F)$. $F \in k[x, y]$ is homogeneous of deg d.

$$\underset{[a,b]}{\overset{}{P}} \in V_P(F) \Leftrightarrow F(a, b) = 0.$$

Either a or b are $\neq 0$, assume $b \neq 0$.

$$F(a, b) = 0 = b^d F\left(\frac{a}{b}, 1\right)$$

$$\Rightarrow F\left(\frac{a}{b}, 1\right) = 0.$$

a/b is a root of $F(x,1) \in k[x]$

Let $x_1, \ldots, x_r$ be roots of $F(x,1)$

$\frac{a}{b} = x_i \Rightarrow [x_1 b : b], \ldots, [x_r b : b]$

finitely many

$= [x_1 : 1], \ldots, [x_r : 1]$ (as $b \neq 0$)

Remains points st $b = 0$. There is only one $[1:0]$.

If $F(1,0) = 0$, then this is also a point of $V_P(F)$.

In any case $V_P(F)$ is finite.

Algebraic subsets of $\mathbb{P}^1$ ($\neq \mathbb{P}^1$) are finite sets of points.

Conversely, any finite subset of $\mathbb{P}^1$ is algebraic. Enough to check that 1 point is algebraic.

$P = [a;b]$. Find F st $P = V_P(F)$?

$F(x,y) = ay - bx$

$V_P(F) = \{[a:b]\} = P$

More generally: $P=[a_1:\dots:a_{n+1}]\in\mathbb{P}^n$.
Assume $a_i\neq 0$.

$$P=V_p(a_ix_1-a_1x_i,\dots,a_ix_{n+1}-a_{n+1}x_i)$$

Rem: $\mathbb{P}^1=\mathbb{A}^1\cup\{[0,1]\}$
$\mathbb{A}^1$ is not an algebraic subset of $\mathbb{P}^1$.

Def: (Ideal of a projective alg set) in the sense def previously
Let $X\subset\mathbb{P}^n$ be a subset
Let $I_P(X)=\{F\in k[x_1,\dots,x_{n+1}],\ F(P)=0\ \forall P\in X\}$

$I_P(X)$ is an ideal in $k[x_1,\dots x_{n+1}]$

Def: An ideal $I\subset k[x_1\dots x_{n+1}]$ is called homogenous if $I=(F_1,\dots,F_r)$ where $F_1,\dots,F_r$ are homogenous polynomials.

Ex: $(x,\ x^2+y^2)\in k[x,y]$ is homogenous
$(x^3+x)\subset k[x]$ not homogenous. (ex)

Prop: $I_P(X)$ is a homogenous ideal.

Proof: Write $I_P(x)=(F_1,\dots,F_r)$

(Recall that any ideal in $k[x_1,\dots,x_{n+1}]$ is finitely generated).

Write $F_1=\underbrace{F_1^m+\dots+F_1^d}_{\text{homogenous.}}$

$F_1(P) = 0 \Leftrightarrow \forall i \;\; F_1^i(P) = 0$

$\Rightarrow F_1^i \in I_P(X)$

Same for all F_i's

$I_P(X)$ is generated by homo. components of all F_i's.

$I_P(X)$ is homogenous

$\square$.

Let $S \subset k[x_1, \dots, x_{n+1}]$, 12.03.14.

define $V_p(S) = \{P \in \mathbb{P}^n : F(P) = 0 \ \forall P \in S\}$.

$F(a_1, \dots, a_{n+1}) = 0$ for any choice of homogeneous coords. $[a_1 : \dots : a_{n+1}]$ for P.

$V_p(S) = V_p(\langle S \rangle)$

ideal generated by S

In fact, $V_p(S) = V_p(I)$ I is the ideal generated by homogeneous components of $F \in S$.

Recall, an ideal $I \subset k[x_1, \dots, x_{n+1}]$ is called homogeneous if I is generated by homogeneous poly^{ns}.

$X \subset \mathbb{P}^n$, $I_p(X) = \{F \in k[x_1, \dots, x_{n+1}], F(P) = 0, \forall P \in X\}$

$I_p(X)$ is a homogeneous ideal.

Properties of V_p and I_p

1) $I_p(\mathbb{P}^n) = \{0\}$.

$I_p(\emptyset) = (x_1, \dots, x_{n+1})$

$V_p(\{0\}) = \mathbb{P}^n$ $\quad V_p(1) = V_p(x_1, \dots, x_{n+1}) = \emptyset$.

2) $S_1 \subset S_2 \subset k[x_1, \dots, x_{n+1}]$, $\quad V_p(S_2) \subset V_p(S_1)$.

3) (S_i), $S_i \subset k[x_1, \dots, x_{n+1}]$, $\quad V_p(\bigcup S_i) = \bigcap V_p(S_i)$

4) (I_i) homogeneous ideals in $k[x_1, \dots, x_{n+1}]$

$V_p(\sum_i I_i) = \bigcap_i V_p(I_i)$

5) $X_1 \subset X_2 \subset \mathbb{P}^n$ $\quad I_p(X_2) \subset I_p(X_1)$

6) $X \subset \mathbb{P}^n$, $\quad X \subset V_p(I_p(X))$

with equality iff X is a projective algebraic set.

7) $\forall T \subset k[x_1, \dots, x_{n+1}]$, $\quad T \subset I_p(V_p(T))$

and $V_p(T) = V_p(I_p(V_p(T)))$

(all these prop^s are identical to the prop^s in the affine space).

Properties of homogeneous ideals

① If $I \subset k[x_1, \dots, x_{n+1}]$ is a homog. ideal, and $F \in I$.

iff $\Updownarrow$ Write $F = F_m + \dots + F_d$, F_i - homogeneous

Then each $F_i \in I$.

Pf: I is homogeneous, so

$I = (G_1, \dots, G_r)$ $\quad G_i$ - homogeneous.

Let $F \in I$ so

$F = \sum_{i=1}^{r} H_i \cdot G_i$ $\quad H_i \in k[x_1, \dots, x_{n+1}]$

We may assume that each H_i is homogeneous (b/c every poly^n is a sum of homog. polynomials)

Now: each $H_i G_i$ is homogeneous.

Each homogeneous F_i is a sum of some of the $H_i G_i$ and hence belongs to I.

$\blacksquare$

We can take the above property as a def^n of homog. ideal.

② Let $I \subset k[x_1, \dots, x_{n+1}]$ be a homogeneous ideal.
I is prime iff for <u>any homogeneous</u> F and $G \in k[x_1, \dots x_{n+1}]$ s.t. $F \cdot G \in I$, either $F \in I$ or $G \in I$.

($\Longrightarrow$) trivial (def^n of prime ideal).

($\Longleftarrow$) Let F, G be two poly^{ns} s.t. $F \cdot G \in I$.

Suppose $G \notin I$.

$F = F_m + \dots + F_d$

$G = G_n + \dots + G_e$ $\qquad F_i, G_i$ - homogeneous

By property ①, at least one of the $G_i \notin I$.

Let j be the smallest integer s.t. $G_j \notin I$.

Calculate

$$F \cdot \sum_{k=j}^{e} G_k = F\Big(G - \underbrace{\sum_{k=n}^{j-1} G_k}_{\in I}\Big) = \underbrace{FG}_{\in I} - \underbrace{F\Big(\sum_{k=n}^{j-1} G_k\Big)}_{\in I}$$

So $F\left(\sum_{k=j}^{e} G_k\right) \in I$, $\quad F\left(\sum_{k=j}^{e} G_k\right) = F_m G_j$ + higher order terms

$F_m G_j$ is the homogeneous component of lowest degree $F\left(\sum_{k=j}^{e} G_k\right) \in I$.

By property ①, $F_m G_j \in I$.

As F_m and G_j are homogeneous & $G_j \notin I$, $\Rightarrow F_m \in I$.

Now,

$F_m \in I$, hence $(F - F_m) \cdot G \in I$

Repeat the same procedure, with the poly^n starting at F_{m+1}, will find $F_{m+1} \in I$.

In this way, one finds that all $F_i \in I$.

$\Rightarrow F \in I$.

$\blacksquare$

Def^n An algebraic subset $V \subset \mathbb{P}^n$ is irreducible if V is not of the form $V = V_1 \cup V_2$ where V_i algebraic & $V_i \neq V$.

Prop^n V is irreducible $\Longleftrightarrow I_p(V)$ is a prime ideal.

Equivalent to: V - reducible $\Longleftrightarrow I_p(V)$ not prime.

Pf: Suppose V is reducible, $V = V_1 \cup V_2$, and $V_i \neq V$.

$V_1 \subsetneq V \Rightarrow I_p(V) \subsetneq I_p(V_1)$

$\exists F$ homogeneous in $I_p(V_1)$ s.t. $F \notin I_p(V)$.

$V_2 \subsetneq V \Rightarrow I_p(V) \subsetneq I_p(V_2)$

so $\exists$ polynomial G, homogeneous, $G \in I_p(V_2)$, $G \notin I_p(V)$.

Because $V = V_1 \cup V_2$, $F \cdot G \in I_p(V)$.

$\Rightarrow I_p(V)$ not prime by prop. 2.

Conversely assume that $I_p(V)$ is not prime,

$\exists F, G$ - homogeneous, s.t. $FG \in I_p(V)$, but $F \notin I_p(V)$, $G \notin I_p(V)$.

$F \cdot G \in I_p(V)$, so

$$V = \underbrace{(V \cap V_p(F))}_{V_1} \cup \underbrace{(V \cap V_p(G))}_{V_2}$$

As $F \notin I_p(V)$ $\quad V_1 \neq V$

$G \notin I_p(V)$ $\quad V_2 \neq V$ $\quad \rightarrow V$ is reducible ■

Example: $V = \mathbb{P}^n$, $\quad I_p(\mathbb{P}^n) = \{0\}$ prime ideal.

$\mathbb{P}^n$ is irreducible.

Example: $V = V_p(x-y) \subset \mathbb{P}^2 \quad I_p(V) = (x-y) \subset k[x,y,z]$.

$I_p(V)$ is prime $\quad k[x,y,z]/(x-y) \cong k[x,z]$ $\quad$ (Will see a better way soon)

V is irreducible.

Prop^n Let V be an algebraic subset of $\mathbb{P}^n$.

There exists a unique set $\{V_1, \dots, V_r\}$ of irreduc. algebraic subsets of $\mathbb{P}^n$, s.t.

$V_i \not\subseteq V_j$ & $V = V_1 \cup \dots \cup V_r$.

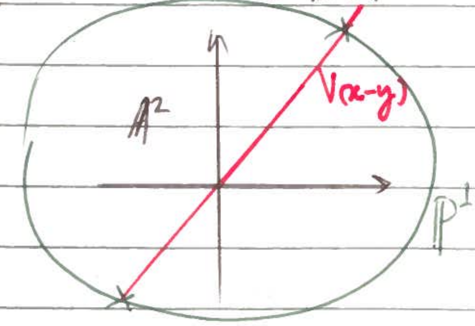
V_i's are called irreducible components of V.

Ex: $V = V_p(z(x-y)) \subset \mathbb{P}^2$

$= V_p(z) \cup V_p(x-y)$ irreduc. components of V.

Remark: $V_p(z)$ is the line at ∞ of $\mathbb{P}^2$. $\quad \mathbb{P}^2 = \mathbb{A}^2 \cup \mathbb{P}^1$

dim = 2 $\quad V_p(x-y) \cap V_p(z) = \{[1:1:0]\}$.



Def^n A **projective variety** V is an irreduc. algebraic subset of $\mathbb{P}^n(k)$ where k is algebraically closed.

Let V be a projective variety.

Define

h-homogeneous

$$\boxed{\Gamma_h(V) = k[x_1,\dots,x_{n+1}]/I_p(V)}$$

$\Gamma_h(V)$ is an integral ring, but unlike in the affine case, elements of $\Gamma_h(V)$ do not define functions on V.
If $F \in k[x_1,\dots,x_{n+1}]$ is a polynomial, even if F is homogeneous, one cannot talk of $F(P)$ for $P \in \mathbb{P}^n$.

it's not a function, can only talk about $F=0$ or not.

Define $k_h(V) = \left\{ \frac{f}{g} : f,g \in \Gamma_h(V),\ g \neq 0 \right\}$ = field of fractions of $\Gamma_h(V)$

Elements of $k_h(V)$ still do not define functions on V.
However, if f and g are homogeneous of same degree, then $\frac{f}{g}$ is a well-defined function on V.

Let $P = [a_1 : \dots : a_{n+1}] \in V$, $\deg f = \deg g = d$
$\frac{f(P)}{g(P)}$ is independent of the choice of $a_1,\dots,a_{n+1}$.

Another choice would be $[\lambda a_1 : \dots : \lambda a_{n+1}]$, $\lambda \in k^\times$.

can't choose projective coords in a unique way

$$\frac{f(\lambda a_1,\dots,\lambda a_{n+1})}{g(\lambda a_1,\dots,\lambda a_{n+1})} = \frac{\lambda^d f(P)}{\lambda^d g(P)} = \frac{f(P)}{g(P)}$$

$$k_h(V) \supset k(V) = \left\{ \frac{f}{g} : f,g \in \Gamma_h(V),\ g \neq 0 ;\ f,g \text{ homogeneous of the same degree} \right\}$$

field of rational functions on V

Let $P \in V$. $\mathcal{O}_P(V) = \left\{ \frac{f}{g} \in k(V),\ g(P) \neq 0 \right\}$ Local ring of V at P

It is a local ring, its maximal ideal is
$$m_P(V) = \left\{ \tfrac{f}{g} \in \mathcal{O}_P(V),\ f(P) = 0 \right\}$$

$$\mathcal{O}_P(V)/m_P(V) \simeq k$$

$$\frac{f}{g} \longmapsto \frac{f(P)}{g(P)} \qquad \Gamma_h(V) \subset \mathcal{O}_P(V) \subset k(V) \subset k_h(V)$$

Example: $V = \mathbb{P}^1$, $I_p(V) = \{0\}$
$\Gamma_h(V) = k[x,y]$ $k_h(V) = k(x,y)$

$k(V) = ?$ $k(V) = \left\{ \frac{f}{g},\ f,g \in k[x,y] \text{ homog. of same degree} \right\}$

$$\frac{f(x,y)}{g(x,y)} = \frac{y^d f(x/y,1)}{y^d g(x/y,1)} = \frac{f(x/y,1)}{g(x/y,1)} = \frac{f(t,1)}{g(t,1)} = \frac{F(t)}{G(t)}$$

$t = x/y$

where $F(t)=f(t,1)$, $G(t)=g(t,1)\in k[t]$,

Conversely, let $F,G\in k[t]$, $G\neq 0$.

Then $\dfrac{F(x/y)}{G(x/y)}$ is of the form $\dfrac{f(x,y)}{g(x,y)}$ f,g - homog. of the same degree.

$$k(\mathbb{P}^1) \xleftarrow{\sim} k(\mathbb{A}^1)=k(t)$$
$$\frac{x}{y} \longleftarrow\!\shortmid\, t$$

Def^n $V\subset\mathbb{P}^n$, any projective variety; $P\in V$, a point.
$f\in k(V)$ is said to be defined at P if $f\in\mathcal{O}_P(V)$.

Def^n If f is not defined at P then we say that P is a pole of f.

Example: $V=\mathbb{P}^1$, $f=\frac{x}{y}\in k(V)$

Does f have any poles?

Let $P=[x:y]\in\mathbb{P}^1$

if $y\neq 0$, f is defined at P.

only need to check whether $[1:0]$ is a pole or not.

Suppose f was defined at $[1:0]$, $\exists\,\alpha,\beta\in k[x,y]$, homog. of degree d.

$\dfrac{x}{y}=\dfrac{\alpha}{\beta}$ $\beta(1,0)\neq 0$.

$x\beta=\alpha y$

Evaluate at $(1,0)$. LHS $\neq 0$; RHS $=0$. Contradiction.

$[1:0]$ is a unique pole of f.

Ex: $V=V(x^2+y^2-z^2)\subset\mathbb{P}^2$ $f=\dfrac{y-z}{x}\in k(V)$.

Does f have any poles?

When $x\neq 0$, f is defined at $[x:y:z]$.

$x=0$, Points $[0:y:z]\in V$ satisfy $y^2=z^2$.

$y=\pm z$.

$P_1=[0:1:1]$, $P_2=[0:1:-1]$.

Assume f defined at P_1, it actually is defined!

Then $\dfrac{y-z}{x}=\dfrac{\alpha}{\beta}$ $\beta(0,1,1)\neq 0$. $\alpha,\beta\in k[x,y,z]$ homog. same degree.

$\beta(y-z)=\alpha x$

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

At P_1:

In $\Gamma_h(V)$ we have $y^2-z^2=-x^2$

$f=\dfrac{y-z}{x}=\dfrac{-x}{y+z}$ f is defined at P_1, $f(P_1)=0$.

At $\overset{[0:1:-1]}{\overset{\shortparallel}{P_2}}$: Suppose f was defined at P_2:

$$\frac{y-z}{x} = \frac{\alpha}{\beta} \qquad \beta(0,1,-1) \neq 0.$$

$$(y-z)\beta = \alpha x$$

$\left.\begin{array}{l} \text{LHS} \neq 0 \\ \text{RHS} = 0 \end{array}\right\} \Rightarrow$ contradiction. P_2 is a unique pole of f.

$[0:1:-1]$
$\overset{\shortparallel}{}$

At P_2: Suppose f was defined at P_2:

$$\frac{y-z}{x} = \frac{\alpha}{\beta} \qquad \beta(0,1,-1) \neq 0.$$

$$(y-z)\beta = \alpha x$$

$\left.\begin{array}{l} LHS \neq 0 \\ RHS = 0 \end{array}\right\} \Rightarrow$ contradiction. P_2 is a unique pole of f.

14.03.14.

Relation betw. affine & projective algebraic sets.

Let $F \in k[x_1, \dots, x_{n+1}]$ be a homogeneous poly^n, $\deg(F) = d$.

$F_* = (x_1, \dots, x_n, 1) \in k[x_1, \dots, x_n]$

eg. $F = xy - z^2 \in k[x,y,z]$

$F_* = xy - 1$

Remark: In general, $\deg F_* \neq \deg F$.

$F = zx + zy \in k[x,y,z]$, $\qquad \deg F = 2$

$F_* = x + y$, $\qquad \deg F_* = 1$

Dual operation: let $F \in k[x_1, \dots, x_{n}]$, $d = \deg(F)$

$$F^* = x_{n+1}^d F\left(\frac{x_1}{x_{n+1}}, \dots, \frac{x_n}{x_{n+1}}\right) \in k[x_1, \dots, x_{n+1}].$$

F^* is homogeneous of deg $= d$.

Remark: F^* is a poly^n b/c $\deg F = d$, therefore powers of x_{n+1} that appear as denominators in $F\left(\frac{x_1}{x_{n+1}}, \dots, \frac{x_n}{x_{n+1}}\right)$ are "killed" by x_{n+1}^d.

It's homogeneous of deg d b/c:

$$F^*(\lambda x_1, \dots, \lambda x_{n+1}) = \lambda^d x_{n+1}^d F\left(\frac{\lambda x_1}{\lambda x_{n+1}}, \dots, \frac{\lambda x_n}{\lambda x_{n+1}}\right) = \lambda^d F^*(x_1, \dots, x_{n+1})$$

Example: • $F = x - y^2 \in k[x,y]$ $\quad \deg(F) = 2$.

$$F^* = z^2 F\left(\frac{x}{z}, \frac{y}{z}\right) = z^2\left(\frac{x}{z} - \left(\frac{y}{z}\right)^2\right) = zx - y^2 \quad \text{is homogeneous}$$

• $F = \underbrace{xy}_{\deg = 2} - 1$, $\qquad F^* = xy - z^2$

• $F = x^2 - y^3$, $\qquad F^* = zx^2 - y^3$

Property: $(F^*)_* = F$

Not true: F-homog. in $k[x_1, \dots, x_{n+1}]$, $\deg = d$, $\cancel{(F_*)^* = d}$

Example: $F = zx + zy$ $\qquad F_* = x+y$, $\quad\|\quad r=1$ $\quad$ using prop ④

$(F_*)^* = x+y \neq F$ $\qquad z(F_*)^* = F$

Properties: ① $(FG)_* = F_* G_*$

② $(FG)^* = F^* G^*$

③ $(F^*)_* = F$

④ $F \in k[x_1, \dots, x_{n+1}]$ homogeneous, deg $= d$.
Let r be the highest power of x_{n+1} dividing F.
Then
$$F = x_{n+1}^r (F_*)^*$$

Proof of ④:
Write $F = x_{n+1}^r G$, $\underline{x_{n+1} \nmid G}$.
then $(G_*)^* = G$ $\quad$ (exercise)
$(F_*)^* = (G_*)^* = G$,
$x_{n+1}^r (F_*)^* = x_{n+1}^r G = F$.

Let $I \subset k[x_1, \dots, x_{n+1}]$ be an ideal, let
I^* be the ideal generated by all F^*, $F \in I$.

I^* is a homogeneous ideal in $k[x_1, \dots, x_{n+1}]$.

Example: $I = (F)$, $\quad F \in k[x_1, \dots, x_{n}]$
$I^* = (F^*) \subset k[x_1, \dots, x_{n+1}]$ $\qquad$ (using rel^n $(FG)^* = F^* G^*$ & from def^{ns})

Let $\varphi_{n+1} : \overset{V_n}{\mathbb{A}^n} \longrightarrow \mathbb{P}^n \supset V^* \supset \varphi_{n+1}(V)$
$(x_1, \dots, x_n) \longmapsto [x_1 : \dots : x_n : 1]$

φ_{n+1} identifies $\mathbb{A}^n$ with $U_{n+1} = \{[x_1 : \dots : x_n : 1] \in \mathbb{P}^n\}$

Let $V = V(I) \subset \mathbb{A}^n$. Define $V^* = V_p(I^*) \subset \mathbb{P}^n$

Prop^n $\underline{\varphi_{n+1}(V) = V^* \cap U_{n+1}}$

Pf: $V^* = \{[x_1 : \dots : x_{n+1}] \in \mathbb{P}^n : F^*(x_1, \dots, x_n, 1) = 0,\ \forall F \in I\}$
$V^* \cap U_{n+1} = \{[x_1 : \dots : x_n : 1] \in \mathbb{P}^n, F^*(x_1, \dots, x_n, 1) = 0\ \forall F \in I\}$
$(F^*)_*(x_1, \dots, x_n) = F(x_1, \dots, x_n), \forall F \in I$
$= \varphi_{n+1}(V)$.

Example: $V = V(\underbrace{y - x^2}_{I}) \subset \mathbb{A}^2$

$V^* = V(yz - x^2)$, $\quad V^* \cap U_3 = \{[x : y : 1] : y - x^2 = 0\} = \varphi_3(V)$

$\mathbb{P}^n = U_{n+1} \cup H_\infty$

$\varphi_{n+1}^{\cong}$ $\mathbb{A}_n$ $\quad \overset{\shortparallel}{\{[x_1:\dots:x_n:0]\}} \cong \mathbb{P}^{n-1}$

$V^* \cap H_\infty$ = components at ∞ of V. (intersection with curve & a line) [V^*, H_∞]

If $V \subset \mathbb{A}^2$ is a curve, $V^* \cap H_\infty$ is called a set of points at ∞ of V.

Example: $V = V(y - x^2)$. $V^* = V(yz - x^2)$

$V^* \cap H_\infty = \{[x:y:0] \in V^*\} = \{[x:y:0],\ x^2 = 0\} = \{[0:1:0]\}$.

Example: $V = V(y^2 - x^3 - x^2 + 1)$

$V^* = V_p(y^2 z - x^3 - x^2 z + z^3)$

(pts at ∞) $V^* \cap H_\infty = \{[0:1:0]\}$.

Example: $V = V(y^2 - x^3)$

$V^* = V_p(y^2 z - x^3)$

$V^* \cap H_\infty = \{[0:1:0]\}$

Def^n Let $I \subset k[x_1, \dots, x_{n+1}]$ be a homogeneous ideal.

Let I_* be the ideal in $k[x_1, \dots, x_n]$ generated by F_*.

Let $V = V_p(I) \subset \mathbb{P}^n$. Define $V_* = V(I_*)$

(In reality $V_* = V \cap U_{n+1}$) $\quad U_{n+1} \overset{\varphi_{n+1}}{\frown} \mathbb{A}^n$

• $V \subset \mathbb{A}^n$, $(V^*)_* = V$ $\quad$ (b/c $(F^*)_* = F$)

• $\underset{\text{irreduc.}}{V \subset \mathbb{A}^n} \Rightarrow V^* \subset \mathbb{P}^n$ irreducible.

Proof: write $V = V(I)$, I is prime ideal.

$V^* = V_p(I^*)$. Need to show that I^* - prime.

Let F, G be homogeneous, s.t. $FG \in I^*$. Apply $(\ )_*$

$(FG)_* = F_* G_* \in (I^*)_* = I$.

I is prime.

$\Rightarrow$ for example, $F_* \in I$, which means

$(F_*)^* \in I^*$

$\Rightarrow \underbrace{x_{n+1}^r (F_*)^*}_{= F} \in I^*$ $\quad$ r = highest power of x_{n+1} dividing F. $\blacksquare$

19/3/14

$F \in k[x_1 \dots x_{n+1}]$ hom of degree d.
$F_* = F(x_1, \dots, x_n, 1) \in k[x_1 \dots x_n]$
$F \in k[x_1, \dots, x_n]$. $\deg F = d$
$F^* = x_{n+1}^d F(x_1/x_{n+1}, \dots x_n/x_{n+1})$
F^* homo polynomial of $\deg = d$.

$(F^*)_* = F$
If x_{n+1}^s is the largest power of x_{n+1} dividing F then

$$x_{n+1}^s (F_*)^* = F$$

$$\begin{array}{ccccc} \mathbb{P}^n & = & U_{n+1} & \cup & H_\infty \\ & & \uparrow{\scriptstyle \varphi_{n+1}} \wr & & \\ & & \mathbb{A} & & \end{array}$$

Let $V \subset \mathbb{A}^n$ algebraic
$I = I(V) \subset k[x_1, \dots, x_n]$
$I^* \subset k[x_1, \dots, x_{n+1}]$ generated by the F^*, $F \in I$

$$V^* = V_p(I^*) \subset \mathbb{P}^n$$

V^* is called projective closure of V. It is the smallest algebraic subset of $\mathbb{P}^n$ containing $\varphi_{n+1}(V)$.

Proof: Let W be an algebraic subset of $\mathbb{P}^n$ containing $\varphi_{n+1}(V)$

Let $F \in I_p(W)$
$F_*(x_1, \dots, x_n, 1) = 0 \ \forall (x_1, \dots, x_n) \in V$
(because $V \subset W$).

$F = x_{n+1}^s (F_*)^* \in I(V)^*$

$I_p(W) \subset I(V)^*$

$V^* = V_p(I(V)^*) \subset V_p(I_p(W)) = W$ $\square$.

<u>Ex</u>: $V = V(\underbrace{y - x^2}_{F}) \subset \mathbb{A}^2$

Find V^* $\quad F^*(x,y,z) = zy - x^2$

$$I(V^*) = (zy - x^2)$$

$$V^* = V(zy - x^2) \subset \mathbb{P}^2.$$

<u>Points at ∞ of V^*</u> $[x, y, 0] \in V^*$

One point: $[0:1:0]$.

Let $V \subset \mathbb{P}^n$ algebraic set.
Let $I = I_p(V)$, let I_* be the ideal of $k[x_1 \ldots x_n]$ generated by F_*, $F \in I$.
Let $V_* \subset \mathbb{A}^n$ be $V_* = V(I_*)$.
In fact V_* is the intersection of V with U_{n+1}

$$(V^*)_* = V \quad (\text{because } (F^*)_* = F)$$

Is it true that $(V_*)^* = V$. <u>NO</u>

Take $V = H_\infty = V_p(x_{n+1})$

$V_* = \emptyset$, $(V_*)^* = \emptyset$.

— / —

Prop: k alg. closed
If $V \subset \mathbb{P}^n$ algebraic and no component of V lies in or contains H_∞, then

$$(V_*)^* = V.$$

$V \subset \mathbb{A}^n$, $V^* \subset \mathbb{P}^n$.

$\Gamma(V) = k[x_1 \dots x_n]/I(V)$, $\Gamma_h(V^*) = k[x_1 \dots x_{n+1}]/I(V)^*$

$k(V) = \left\{ \frac{f}{g}, f,g \in \Gamma(V),\ g \neq 0 \right\} \xrightarrow{\sim} k(V^*) = \left\{ \frac{f}{g},\ f,g \in \Gamma_h(V^*),\ f,g \text{ homo. same degree } g \neq 0 \right\}$

$$\frac{f(x_1, \dots, x_n, 1)}{g(x_1, \dots, x_n, 1)} = \frac{f_*}{g_*} \longleftarrow \frac{f}{g}$$

$$\mathcal{O}_P(V) \xleftarrow{\sim} \mathcal{O}_P(V^*)$$

Ex: $V = V(y - x^2)$. $V^* = V(xz - y^2)$

$P = [1 : 1 : 1]$

$\mathcal{O}_P(V^*) \cong \mathcal{O}_P(V) = \left\{ \frac{f}{g} : f,g \in \Gamma(V)\ \ f,g \in \Gamma(V),\ g(1,1) \neq 0 \right\}$

Projective transformation

Let $T : \mathbb{A}^{n+1} \to \mathbb{A}^{n+1}$ linear invertible map.

As T sends lines through 0 to lines through zero, T induces a bijective map $\tilde{T} : \mathbb{P}^n \to \mathbb{P}^n$

<u>Ex</u>: <u>$n=1$</u> $T = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$

$$\tilde{T} : [x, y] \mapsto [ax+by : cx+dy]$$

If $\tilde{T}$ is a projective transformation $V \subset \mathbb{P}^n$ algebraic set, $V^T = \tilde{T}^{-1}(V)$.

(<u>ex</u>: write $\tilde{T} := [T_1 : \dots : T_{n+1}]$

$$V = V_P(F) \quad F^T = F(T_1, \dots, T_{n+1})$$

$$V^T = V_P(F^T).)$$

$$\left\{ \begin{array}{l} \tilde{T} : \Gamma_h(V) \xrightarrow{\sim} \Gamma_h(V^T) \\ \qquad k(V) \xrightarrow{\sim} k(V^T) \\ \qquad \mathcal{O}_P(V) \to \mathcal{O}_Q(V^T), \; \tilde{T}(Q) = P. \end{array} \right.$$

Projective plane curves and Bézouts theorem.

$C = V_P(F) \subset \mathbb{P}^2$; $F \in k[x, y, z]$ homogenous of degree d.

C is called plane projective algebraic curve of degree d.

$[a,b,c] = P \in C' \subset \mathbb{P}^3$
Without lose of generality, we may assume that $c \neq 0$.

$m_P(C') \overset{def}{=} m_{(\frac{a}{c},\frac{b}{c})}(C'_*)$

$C'_* = V(F(x,y,1))$

P is called simple or nonsingular if $m_P(C) = 1$

Ex: $C' = V_P(yz - x^2)$. $P = [1:1:1]$

$m_P(C') = m_P(C'_*) = m_{(1,1)}(y - x^2) = 1$

$P = [0:1:0]$

w.r.t y

$m_P(C') = m_{(0,0)}(C'_*) = m_{(0,0)}(z - x^2) = 1$

Ex: $C' = V_P(y^2 z - x^3)$, $P = [0:0:1]$

$m_P(C') = m_{(0,0)}(y^2 - x^3) = 2$.

P is a singular point of C.
P_∞ = point at ∞ of $C' = [0:1:0]$

$m_{P_\infty}(C') = m_{(0,0)}(z - x^3) = 1$

P_∞ is a simple point.

Def: C, D 2 plane projective curves
$C = V_P(F)$, $D = V_P(G)$
Let $Q \in \mathbb{P}^2$.
Define
$$I(Q, C, D) = I(Q, F_*, G_*)$$
$$= \dim_R \mathcal{O}_Q(\mathbb{A}^2) / (F_*, G_*)$$

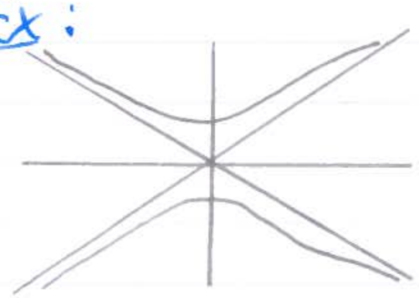
Ex: $F = yz - x^3$ $\quad G = z$ $\quad P = [0:1:0]$

Calculate $I(P, F, G)$

$$I(P, F, G) = I((0,0), z - x^3, z)$$
$$= I((0,0), -x^3, z)$$
$$= 3 \underbrace{I((0,0), -x, z)}_{=1}$$
$$= 3.$$

Note: P is the only point of $V(F) \cap V(G)$
Multiplicity of intersection of $P = 3 = \deg(F) \cdot \deg(G)$

Ex:



$$\begin{cases} F = x^2 - y^2 - z^2 \\ G = x - y \end{cases}$$

$V_P(F) \cap V_P(G) = \{[1:1:0]\}$.

$$I([1:1:0], F, G) = I((1:0) : 1-y^2-z^2, 1-y)$$

$$= I((1:0) : -z, 1-y)$$

$1-y^2-z^2-(1+y)(1-y)$ $$= I((1:0) : -z^2; 1-y)$$

$$= 2I((1:0) : -z : 1-y)$$

$$= 2I((0,0) : z : y')$$

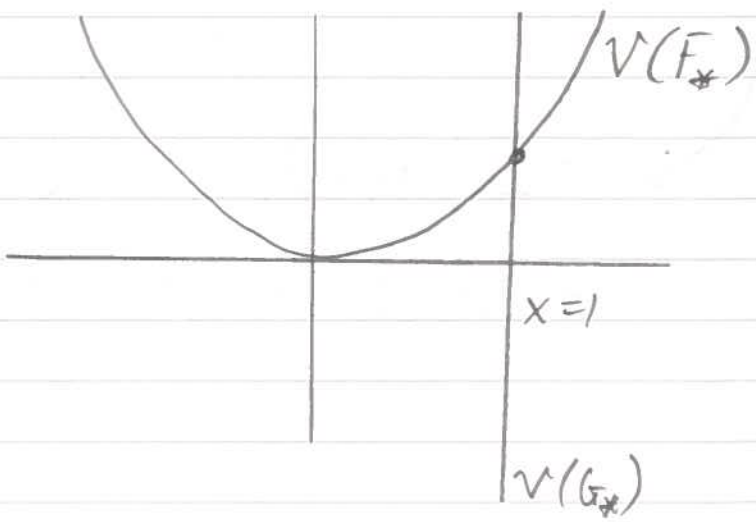
$$= 2.$$

<u>Ex</u>: $\begin{cases} F = zy - x^2 \\ G = x - z \end{cases}$

$\begin{cases} zy - x^2 = 0 \\ x = z \end{cases} \rightarrow z(y-z) = 0.$

$\Rightarrow z = 0$ or $y = z. \rightarrow y = z = x.$

$[0:1:0]$ $\rightarrow [1:1:1]$.



$$I([0:1:0], F, G) = I((0,0), z - x^2, x - z)$$
$$= I((0,0), z - z^2, x - z)$$
$$= I((0,0), z(z-1), x - z)$$
$$= \underset{\substack{\| \\ I((0,0), z, x) \\ \| \\ 1}}{I((0,0), z, x - z)} + \underbrace{I((0,0), z-1, x-z)}_{=0}$$
$$= 1$$
$$I([1:1:1]; zy - x^2, x - z)$$
$$= I([1,1], y - x^2, x - 1)$$
$$\begin{cases} x' = x-1 \\ y' = y-1 \end{cases} \quad \begin{cases} x = x'+1 \\ y = y'+1 \end{cases}$$
$$y - x^2 = y'+1 - (x'+1)^2$$
$$= y' - x'^2 - 2x'$$
$$= I((0,0), y' - x'^2 - 2x'; x')$$
$$= I((0,0), y', x') = 1$$

—/—

Bézout's theorem
Let k be algebraically closed
$\mathbb{P}^2 \supset C = V_P(F)$ curve of degree n
$\mathbb{P}^2 \supset D = V_P(G)$ — " — m
C and D have no component in common

$$\sum_{P \in \mathbb{P}^2} I(P, C, D) = m \cdot n.$$

Rem: $C \cap D$ is finite.

Recall: If C and D are 2 curves in $\mathbb{A}^2$ with no common component then $|C \cap D| < \infty$

—/—

As a projective curve is a union of affine ones, same conclusion holds for curves in $\mathbb{P}^2$.

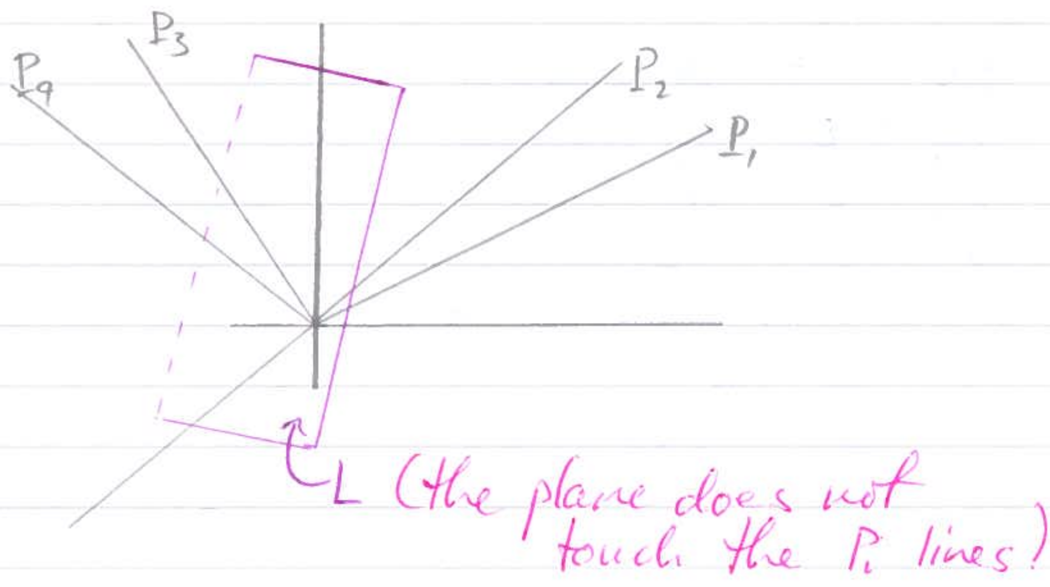
Proof of Bézout's theorem.

Step 1: Reduction to affine case.

$C \cap D = \{P_1 \dots P_n\}$.

We can choose a projective transformation $\tilde{T}$ st $\tilde{T}^{-1}(P_i) \in U_{n+1} \cong \mathbb{A}^n$

Let L be a line in $\mathbb{P}^2$ st $P_i \notin L$, $\forall i$.



Choose $\tilde{T}$ st:

$$\tilde{T}(L) = H_\infty = \{z=0\}.$$

$$L: ax+by+cz=0.$$

$$\tilde{T}: \begin{array}{c} a\neq 0 \\ \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ a & b & c \end{pmatrix} \end{array} : [x:y:z] \to [z:y:ax+by+cz=0]$$

$$(z=0) \to L.$$

21/3/14

Bézout's theorem

k alg. closed field

$\mathbb{P}^2 \supset C = V_p(F)$ of degree m

$D = V_p(G)$ of degree n

C and D have no common component.

$\sum_{P \in \mathbb{P}^2} I(P, C, D) = mn.$

Step 1: Reduction to "affine case".

$$C \cap D = \{P_1, \dots, P_r\}$$

By applying a suitable projective transformation we may assume that all P_i's lies outside $H_\infty = (z = 0)$

$$\Gamma = k[x,y,z] / (F, G) \qquad R = k[x,y,z]$$

$$\Gamma_* = k[x,y,z] / (F_*, G_*)$$

$$\sum_{P \in \mathbb{P}^2} I(P, C, D) = \sum_{P \in \mathbb{A}^2} I(P, C_*, D_*)$$

$$= \dim \Gamma_*$$

This is where "algebraically closed" is used.

otherwise...

Ex: $f = x^2+y^2+1$, $g = x$, $k \in \mathbb{R}$

$$V(f) = \emptyset \quad \sum_{P \in \mathbb{A}^2} I(P,f,g) = 0.$$

But $\dim \mathbb{R}[x,y]/(f,g) = \dim \mathbb{R}[y]/y^2+1 = 2.$

—/—

$R = k[x,y,z]$

$d \geq 0$, $R_d = \{$homogeneous polynomial of deg d in $R\}$

: k-vector space

$\Gamma = R/(F,G)$, $\Gamma_* = k[x,y]/(F_*, G_*)$

$\Gamma_d = \{$homogeneous polynomials in Γ of deg $d\}$

—/—

Step 2 : If $d \geq m+n$, $\dim \Gamma_d = m.n$?

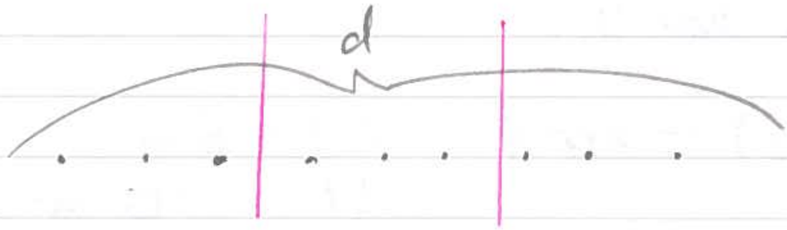
Step 3 : $\varphi : \Gamma_d \xrightarrow{\sim} \Gamma_*$, φ is an isomorph.

$$\overline{H} \longrightarrow \overline{H(x,y,1)} \quad \text{if } d \geq m+n$$

Step 2.

$$\dim R_d = \frac{(d+1)(d+2)}{2}.$$

Basis R_d $\quad x^{i_1} y^{i_2} z^{i_3}$, $i_1 + i_2 + i_3 = d$.
$0 \le i_j \le d$.



$$\binom{d+2}{2} = \frac{(d+1)(d+2)}{2}$$

$\Gamma_d \simeq R_d \big/ (F, G)_d$ isom. of vector spaces.

(here $(F,G)_d = \{$homo. polynomials of deg. d in $(F,G)\}$
its a k-subspace of R_d)

$$\overset{= (F,G) \cap R_d}{(F,G)_d} \to R_d \twoheadrightarrow \Gamma_d$$

$$H(x,y,z) \to H(\bar{x}, \bar{y}, \bar{z})$$

$\dim \Gamma_d = \dim R_d - \dim (F,G)_d$

We need to show that

$\dim (F,G)_d = \dim R_d - m.n.$

—/—

$$R_{d-m} \times R_{d-n} \xrightarrow{\varphi} (F,G)_d$$
$$(A,B) \longrightarrow A\cdot F + B\cdot G.$$

φ is k-linear
φ is surjective (exercise)

<u>Calculate ker φ</u>.

Let $(A,B) \in \ker\varphi$. $A\cdot F + B\cdot G = 0$
$AF = -B\cdot G$.

F, G are coprime $\exists\, C'$ st $\begin{cases} A = G\cdot C' \\ B = -F\cdot C' \end{cases}$

C' homogeneous of degree $d-m-n$.

$\operatorname{Ker}\varphi = \{(G\cdot C', -F\cdot C'),\ C' \in R_{d-m-n}\}$

<u>Concultsion</u>. We have an exact sequence.

$$0 \to R_{d-m-n} \to R_{d-m} \times R_{d-n} \to (F,G)_d \to 0.$$
$$C' \to (G\cdot C', -F\cdot C')$$
$$(A,B) \longrightarrow A\cdot F + BC'.$$

Therefore:

$$\dim (F,G)_d = \dim R_{d-m} + \dim R_{d-n} - \dim R_{d-m-n}$$
$$= \dim R_d - m.n$$

excercise: calculation using $\dim R_k = \frac{(k+2)(k+1)}{2}$

Conclusion if $d \geq m+n$ then

$$\underline{\dim \Gamma_d = mn}$$

Step 3 : $\varphi : \Gamma_d \to \Gamma_*$
$$\overline{H} \longrightarrow \overline{H(x,y,1)}$$

Aim : Show that φ is an isomorphism if $d \geq m+n$

—/—

Lemma $r \geq 1$; $\alpha : \begin{array}{c}\Gamma \to \Gamma \\ \overline{H} \to z^r H\end{array}$ $\left(\Gamma = R/(F,G)\right)$

then α is injective.

Proof : Enough to prove lemma for $r = 1$.

Let $\overline{H} \in \Gamma$ st $\overline{zH} = 0$ in Γ.

Need to show : assume $zH = AF + BG$.
show that $\exists A', B' \in R$, $\underline{H = A'F + B'G}$

As F and G have no common component,
$z \nmid F$ or $z \nmid G \Rightarrow F(x,y,0)$ or $G(x,y,0)$ are not zero.

Evaluate : $zH = A.F + B.G$ at $z = 0$.
$$0 = A(x,y,0)F(x,y,0) + B(x,y,0)G(x,y,0)$$

$$A(x,y,0)F(x,y,0) = -B(x,y,0)G(x,y,0)$$

As F, G are coprime, so are $F(x,y,0)$ and $G(x,y,0)$.

$$\Rightarrow \exists C' \in k[x,y], \begin{cases} A(x,y,0) = -C'G \\ B(x,y,0) = C' \cdot F. \end{cases}$$

Let $\begin{cases} A_1 = A + C'G \\ B_1 = B - C' \cdot F \end{cases} \in k[x,y,z].$

$$\begin{cases} A_1(x,y,0) & \Rightarrow A_1 = z \cdot A' \\ B_1(x,y,0) & \Rightarrow B_1 = z \cdot B' \end{cases}$$

and $A_1F + B_1G = AF + BG = \cancel{z}H = \cancel{z}A'F + \cancel{z}B'G$

$H = A' \cdot F + B' \cdot F \Rightarrow \overline{H} = 0$ in Γ.
α injective.

$\square$

—/—

$\alpha(\overline{H}) = \overline{z^r H}$

$\alpha(\Gamma_d) \subset \Gamma_{d+r}$

if $d \geq m+n$, then by step 2, $\dim \Gamma_d = \dim \Gamma_{d+r} = mn$

α induces an isomorph $\Gamma_d \xrightarrow{\sim} \Gamma_{d+r}$

Hwrk $R = \mathbb{Z}/8\mathbb{Z}$ is local. The only maximal ideal is (2).

R is not of the form $\mathcal{O}_P(V)$, where V - alg. variety$/k$.
V - irred.
$I(V)$ - prime, $\Gamma(V)$ integral.
$\mathcal{O}_P(V)$ - integral.
R is not integral.

Bézout's Theorem k alg. closed. $C = V_p(F) \subset \mathbb{P}^2(k)$, $D = V_p(G) \subset \mathbb{P}^2(k)$
$\deg F = m$, $\deg G = n$.
C, D have no component in common, then

$$\sum_{P \in \mathbb{P}^2} I(P, C, D) = m \cdot n$$

Step 1: Reduce to the affine case.
Apply a projective transformation, so that all $P_i \in C \cap D$ lie in
$\mathbb{A}^2 = \mathbb{P}^2 \setminus H_\infty = (z=0)$

$R = k[x,y,z]$
$\Gamma = k[x,y,z]/(F,G)$ $\Gamma_* = k[x,y]/(F_*,G_*)$
Then

$$\sum_{P \in \mathbb{P}^2} I(P,C,D) = \sum_{P \in \mathbb{A}^2} I(P, C_*, D_*) = \dim_k \Gamma_*.$$

k-alg. closed field!

$d \geq 1$, integer. R_d = k-subspace of homogeneous poly^{ns} of degree d in R
Γ_d = — " — " — " — " — " — in Γ.

Step 2: If $d \geq m+n$, $\dim_k \Gamma_d = m \cdot n$

Step 3: If $d \geq m+n$, then the k-linear map $\varphi : \Gamma_d \longrightarrow \Gamma_*$ is an isom.
$\overline{H} \longmapsto \overline{H(x,y,1)}$

Remark: Step 3 finishes the proof,
$\dim \Gamma_* = \dim \Gamma_d = mn$ - by Step 2.

Lemma: $\alpha : \Gamma \longrightarrow \Gamma$ this map is injective.
$\overline{H} \longmapsto \overline{z^s H}$

Consequence: α induces a map (from) $\Gamma_d \longrightarrow \Gamma_{d+s}$
By Step 2, if $d \geq m+n$,
$\dim \Gamma_d = \dim \Gamma_{d+s}$
α is injective, α induces an isomorphism $\Gamma_d \xrightarrow{\sim} \Gamma_{d+s}$

$\varphi : \Gamma_d \longrightarrow \Gamma_*$
$\overline{H} \longmapsto \overline{H(x,y,1)}$

Let's show: φ is **injective**. Let $\overline{H} \in \Gamma_d$ be s.t. $\varphi(\overline{H}) = 0$.
$\iff \overline{H(x,y,1)} = \overline{0}$ in $\Gamma_* = k[x,y]/(F_*,G_*)$
$\iff H(x,y,1) = A(x,y)F(x,y,1) + B(x,y)G(x,y,1)$
are given this rel^n
some $A, B \in k[x,y]$

We need to prove that $H(x,y,z) = A'F + B'G$ for some $A', B' \in k[x,y,z]$.

H is homogeneous of $\deg = d$,

$$\Longrightarrow z^d H\left(\tfrac{x}{z}, \tfrac{y}{z}, 1\right) = H$$

F - homogeneous of $\deg = m$,

$$z^m F\left(\tfrac{x}{z}, \tfrac{y}{z}, 1\right) = F \qquad (*)$$

$$z^n G\left(\tfrac{x}{z}, \tfrac{y}{z}, 1\right) = G \qquad (**)$$

Let $t \geq d$ be an integer.

$$\begin{aligned} z^{t-d} H(x,y,z) &= z^{t-d}\left(z^d H\left(\tfrac{x}{z}, \tfrac{y}{z}, 1\right)\right) \\ &= z^t H\left(\tfrac{x}{z}, \tfrac{y}{z}, 1\right) \\ &= z^t \left(A\left(\tfrac{x}{z}, \tfrac{y}{z}\right) F\left(\tfrac{x}{z}, \tfrac{y}{z}, 1\right) + B\left(\tfrac{x}{z}, \tfrac{y}{z}\right) G\left(\tfrac{x}{z}, \tfrac{y}{z}, 1\right)\right) \end{aligned}$$

$$\Big\downarrow (*) \qquad\qquad \Big\downarrow (**)$$

Choose $t \geq d \geq mn$

$$= \left[z^{t-m} A\left(\tfrac{x}{z}, \tfrac{y}{z}\right)\right] F + \left[z^{t-n} B\left(\tfrac{x}{z}, \tfrac{y}{z}\right)\right] G$$

If t is large enough,
(for example: $t \geq \max(m + \deg(A), n + \deg(B))$),
then

$$A' = z^{t-m} A\left(\tfrac{x}{z}, \tfrac{y}{z}\right) \in k[x,y,z]$$

$$B' = z^{t-n} B\left(\tfrac{x}{z}, \tfrac{y}{z}\right) \in k[x,y,z]$$

$$z^{t-d} H = A'F + B'G$$

$\overline{z^{t-d} H} = 0$ in Γ.

$\|$

$\alpha(\overline{H})$ So α-injective $\Longrightarrow \overline{H} = 0 \rightarrow \varphi$-injective.

Remains to show: φ-surjective (we will show α-surj.).

Let $\overline{Q} \in \Gamma_*$, $Q \in k[x,y]$.

Let $s = \deg Q$ (d here is fixed, $d \geq mn$).

$t = \max(s, d)$

$q \in k[x,y,z]$, $q = z^t Q\left(\tfrac{x}{z}, \tfrac{y}{z}\right)$

q is homogeneous of degree t.

$\overline{q} \in \Gamma_t$, and $t \geq d$.

$\alpha : \Gamma_d \xrightarrow{\sim} \Gamma_t$ is an isomorphism.

$\overline{H} \longmapsto \overline{z^{t-d} H}$

As α is an isomorphism, there exists $\overline{H}$ s.t. $\overline{q} = \overline{z^{t-d} H}$

$$\varphi(\overline{H}) = \overline{H(x,y,1)} = \overline{q(x,y,1)} = \overline{Q(x,y)} \qquad \blacksquare$$

Whole prf. is not examinable, but MUST KNOW the STEPS

1) Reduce to affine case
2) Calc. dim of Γ_d
3) $\Gamma_* \cong \Gamma_d$ when $d \geq mn$.

Examples: $F = yz^9 + x^{10}$ $G = x^3 + x^2 z$ | field: $\mathbb{C}$

Calculate pts. of intersection, multiplicities; verify conclusion of Bézout's Thm.

(affine patch) $\underline{z=1}$ $\begin{cases} y + x^{10} = 0 \\ x^3 + x^2 = 0 = x^2(x+1) = 0 \end{cases} \begin{cases} x = 0 \\ x = -1 \end{cases}$

if $x=0$, $y=0 \Rightarrow [0:0:1] = P_1$

if $x=-1$, $y=-1 \Rightarrow [-1:-1:1] = P_2$

(should always find some pt. when $z=0$ if field is $\mathbb{C}$) $\underline{z=0}$. $\begin{cases} x^{10} = 0 \\ x^3 = 0 \end{cases}$ $\underline{x=0} \Rightarrow [0:1:0] = P_3$

$$\begin{aligned} I(P_1, F, G) &= I((0,0), y + x^{10}, x^3 + x^2) \\ &= I((0,0), y + x^{10}, x^2) + \underbrace{I((0,0), y + x^{10}, x+1)}_{=0} \quad \text{(as } x+1 \neq 0 \text{ at } (0,0)\text{)!} \\ &= 2 I((0,0), y, x) \\ &= 2 \end{aligned}$$

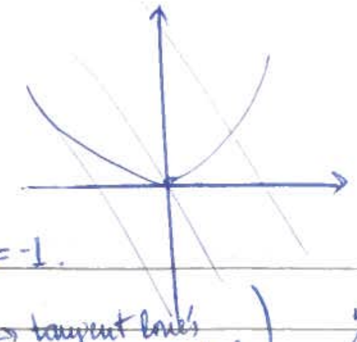
$$\begin{aligned} I(P_2, F, G) &= I((-1,-1), y + x^{10}, x^3 + x^2) \\ &= \underbrace{I((-1,-1), y + x^{10}, x^2)}_{=0} + I((-1,-1), y + x^{10}, x+1) \end{aligned}$$

Change of variables $\begin{cases} x' = x+1 \\ y' = y+1 \end{cases} \begin{cases} x = x'-1 \\ y = y'-1 \end{cases}$

$= I((-1,-1), y' - 1 + (x'-1)^{10}, x')$

not necessary!

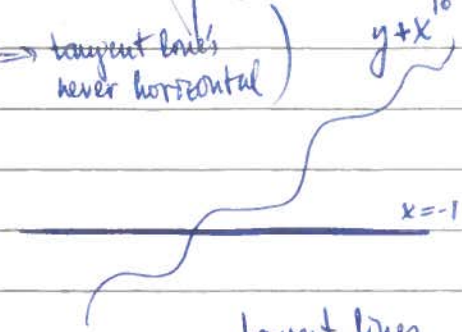
Instead use Property 5) for $I(P, F, G)$.



$(-1,-1)$ is a simple pt. on $y + x^{10} = 0$ and $x = -1$.

Tangent lines are distinct $\left(\frac{\partial}{\partial y}(y + x^{10}) = 1 \Rightarrow \text{tangent lines never horizontal} \right)$

$I((-1,-1), y + x^{10}, x+1) = 1$



tangent lines are distinct.

$\frac{\partial}{\partial y}(y + x^{10}) = 1$

At $P_3 = [0:1:0]$,

$$\begin{aligned} I((0,0), z^9 + x^{10}, x^3 + x^2 z) &= I((0,0), z^9 + x^{10}, x^2) + I((0,0), z^9 + x^{10}, x+z) \\ &= 2 I((0,0), z^9, x) + I((0,0), z^9 + z^{10}, x+z) \quad x = -z,\ x^{10} = z^{10} \\ &= 18 + I((0,0), z^9(1+z), x+z) \\ &= 18 + I((0,0), z^9, x+z) = 18 + 9 = 27. \end{aligned}$$

P_1	P_2	P_3
2	1	27

$2 + 1 + 27 = 30 = \deg F \deg G$.

(k- alg. closed, or not either way works)

Consequence of Bézout's Thm.

If C and D (two curves, $\deg C = m$, $\deg D = n$) intersect at more than $m \cdot n$ points, then C and D have a common component.

Consequence 2

If $C \subset \mathbb{A}^2(k)$, k- algebraically closed, then C has pts at infinity, i.e. $C^* \cap H_\infty \neq \emptyset$.

Follows from Bézout's, b/c $H_\infty = V_p(Z)$.

Not true, if k is not algebraically closed, for example:

$\underline{k = \mathbb{R}}$, $C: x^2+y^2=1$

$C^*: x^2+y^2-z^2=0$.

$\underset{\substack{\| \\ (z=0)}}{C^* \cap H_\infty}: \quad x^2+y^2=0 \Rightarrow x=y=0$

But $[0:0:0]$ doesn't exist in $\mathbb{P}^2$!

$\underline{k = \mathbb{C}}$, have two pts. $[1:i:0]$, $[1:-i:0]$.

Multiplicities $=1$, sum $=2$.

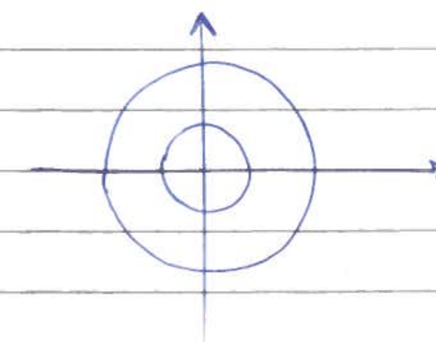
$\underline{\text{Exercise:}}$ $\underline{k = \mathbb{C}}$, $F = x^2+y^2-z^2$ $\quad G = x^2+y^2-2z^2$.

Calculate $V_p(F) \cap V_p(G)$, multiplicities, verify Bézout.

Obviously, intersect at $z=0$.

If $F=G=0 \Rightarrow z=0$.

$\Rightarrow x^2+y^2=0$



2 pts of intersection,

$\begin{cases} P_1 = [1:i:0] \\ P_2 = [1:-i:0] \end{cases}$.

$$I(P_1, x^2+y^2-z^2, x^2+y^2-2z^2) = I(P_1, x^2+y^2-z^2, z^2)$$
$$= I(P_1, x^2+y^2, z^2)$$
$$= 2I(P_1, x^2+y^2, z)$$
$$= 2I((i,0), 1+y^2, z)$$
$1+y^2 = (y-i)(y+i)$
$$= 2I((i,0), y-i, z)$$
$$= 2$$

no need for this:
make $x=1$
$1+y^2, z$ are transverse
$1+y^2=0$, $z=0$ have $\underline{\text{no}}$ tangent in common.

Similarly, $I(P_2, F, G) = 2$.

$4 = \deg F \deg G = I(P_1, F, G) + I(P_2, F, G)$.

Example: $F = z^2y - x^3$ $\quad G = z^4y - x^5$

When $z=1$, $\begin{cases} y - x^3 = 0 \\ y - x^5 = 0 \end{cases}$ $\quad y = x^3 = x^5$

if $x=0$, $y=0$ $\Rightarrow$ $[0:0:1] = P_1$

if $x \neq 0$, $x^2 = 1$, $x = \pm 1$ $\quad$ if $x=1$, $y=1$ $\quad [1:1:1] = P_2$

if $x=-1$, $y=-1$ $\quad [-1:-1:1] = P_3$

When $z=0$, $x=0$, $y=1$

$[0:1:0] = P_4$

$$I(P_1, F, G) = I((0,0), y-x^3, y-x^5) = I((0,0), y-x^3, x^3-x^5)$$
$$= I((0,0), y-x^3, x^3) + \underbrace{I((0,0), y-x^3, 1-x^2)}_{0}$$
$$= 3I((0,0), y, x)$$
$$= 3$$

(make $y=1$)

$$I(P_4, F, G) = I((0,0), z^2-x^3, z^4-x^5) = I((0,0), z^2-x^3, z^4-x^5)$$
$$= I((0,0), z^2-x^3, x^6-x^5)$$
$$= I((0,0), z^2-x^3, x^5(x-1))$$
$$= 5\,I((0,0), z^2, x)$$
$$= 10$$

$I(P_2, F, G) = I((1,1), y-x^3, y-x^5)$ $\quad$ b/c $(1,1)$ is simple pt. on each curve,
$= 1$ $\quad$ and they intersect transversely

$I(P_3, F, G) = 1.$

$1+1+10+3 = \underline{15}.$

Singular points on curves in $\mathbb{P}^2$.

$C = V_p(F) \subset \mathbb{P}^2$

$f = F(x, y, 1)$

$P = [x_0 : y_0 : z_0]$ $\quad z_0 \neq 0$

$$m_P(C) = m_{\left(\frac{x_0}{z_0}, \frac{y_0}{z_0}\right)}(C_*)$$

P is multiple (or singular) if $m_P(C) > 1$.

$P \in C_*$ is singular iff $\begin{cases} \frac{\partial f}{\partial x}(P) = 0 \\ \frac{\partial f}{\partial y}(P) = 0 \\ \cancel{\frac{\partial f}{\partial z}(P) = 0}\ f(P) = 0 \end{cases}$

Euler relation: F - homogeneous of degree d,

$$d \cdot F = x\frac{\partial F}{\partial x} + y\frac{\partial F}{\partial y} + z\frac{\partial F}{\partial z}$$

Pf: $F(\lambda x, \lambda y, \lambda z) = \lambda^d F(x,y,z)$

$$\frac{d}{d\lambda}\left(F(\lambda x, \lambda y, \lambda z)\right) = \frac{d}{d\lambda}\left(\lambda^d F(x,y,z)\right)$$

$$= d \cdot \lambda^{d-1} F(x,y,z)$$

$\|$

$$x\frac{\partial F}{\partial x}(\lambda x, \lambda y, \lambda z) + y\frac{\partial F}{\partial y}(\lambda x, \lambda y, \lambda z) + z\frac{\partial F}{\partial z}(\lambda x, \lambda y, \lambda z)$$

Evaluate at $\lambda = 1$. ■

28/3/14.

P is multiple (or singular) if $m_P(C) > 1$

$P \in C$ is singular iff $\begin{cases} \frac{\partial f}{\partial x}(P) = 0 \\ \frac{\partial f}{\partial y}(P) = 0 \\ f(P) = 0. \end{cases}$

Euler relation : F homogenous of degree d.

$$d \cdot F = x\frac{\partial F}{\partial x} + y\frac{\partial F}{\partial y} + z\frac{\partial F}{\partial z}$$

Proof : $F(\lambda x, \lambda y, \lambda z) = \frac{d}{d\lambda}(\lambda^d F(x,y,z))$

$= d\lambda^{d-1} F(x,y,z)$

$= x\frac{\partial F}{\partial x}(\lambda x, \lambda y, \lambda z) + y\frac{\partial F}{\partial y}(\lambda x, \lambda y, \lambda z)$

$+ z\frac{\partial F}{\partial z}(\lambda x, \lambda y, \lambda z)$

Evaluate at $\lambda = 1$

$\square$.

$P \in C$ is singular iff $\frac{\partial F}{\partial x}(P) = \frac{\partial F}{\partial y}(P) = \frac{\partial F}{\partial z}(P) = 0$

Ex: $F = zx^2 - y^3$

$$\frac{\partial F}{\partial x} = 2xz$$

$$\left.\begin{aligned} \frac{\partial F}{\partial y} &= -3y^2 \Rightarrow y = 0. \\ \frac{\partial F}{\partial z} &= x^2 = 0 \end{aligned}\right\} \Rightarrow z = 1$$

One singular point $[0:0:1]$

$$m_P(F) = m_{(0,0)}(F_*) = 2.$$

Ex: $F_* = y - x^{10}$, $F = yz^9 - x^{10}$

$$\left\{\begin{aligned} \frac{\partial F}{\partial x} &= -10x^9 \rightarrow x = 0 \\ \frac{\partial F}{\partial y} &= z^9 \rightarrow z = 0. \\ \frac{\partial F}{\partial z} &= 9yz^8 \end{aligned}\right.$$

$[0:1:0]$ is the only singular point.

$$m_P(F) = m_{(0,0)}(z^9 - x^{10}) = 9.$$

—/—

Some consequence of Bézout's theorem.

$C = V_p(F)$, $D = V_p(G)$ with no common component.

$$\sum_{P \in \mathbb{P}^2} m_P(C) m_P(D) \leq m.n.$$

By Bézout: $m.n = \sum_P I(P, C, D)$.

By (5) of $I(P,C,D)$, $I(P,C,D) \geq m_P(C) m_P(D)$

—/—

If C and D intersect at exactly $m.n$ points, then these point are simple (or non-singular) i.e. $m_P(C) = m_P(D) = 1$.

Proposition: Any non-singular curve in $\mathbb{P}^2$. is irreducible.

Rem: False in $\mathbb{A}^2$: $V(x(x-1))$ is non-singular but reducible $= V(x) \cup V(x-1)$.

Proof: Let C be a nonsingular projective curve $C = V_p(F)$

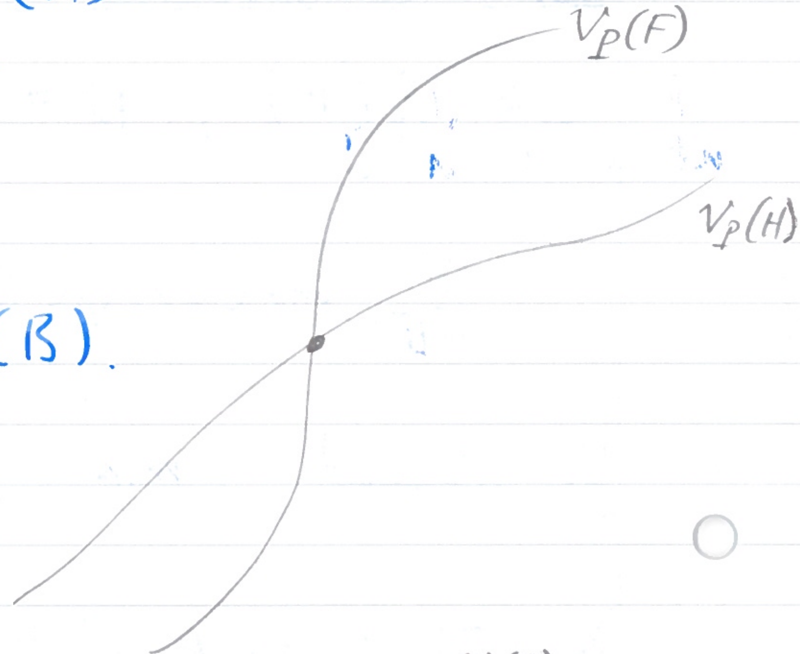
Suppose C is reducible.

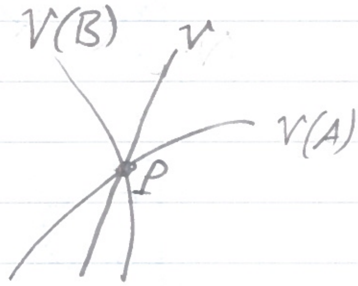
$$F = G \cdot H.$$

Let $P \in V_p(G) \cap V_p(H)$

(P exist by Bezout's theorem).

$$m_P(F) = m_P(A) + m_P(B).$$





Rem: $F = A \cdot B$, $P \in V(F)$

$$m_P(F) = m_P(A) + m_P(B)$$

st L be a line through P st L is not tangent to $V(A)$ and $V(B)$ at P.

$$m_P(F) = I(P, F, C') = I(P, AB, L)$$

$$= \underbrace{I(P, A, L)}_{= m_P(A)} + \underbrace{I(P, B, L)}_{= m_P(B)}$$

$$= m_P(A) + m_P(B).$$

$$m_P(F) = m_P(A) + m_P(B) \geq 2$$

$m_P(F) \geq 2$ contradiction.

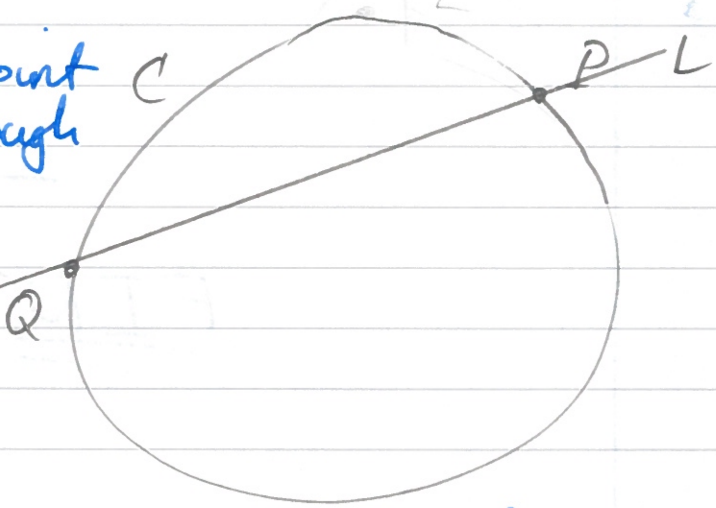
Ex : $F = yz - x^2$

$V_P(F)$ has no singular points, it is irreducible.

Prop : (Partial converse at last one)
Suppose $C = V_P(F)$ has degree 2, irreducible
Then C is non-singular.

Proof : Suppose P is a singular point
$m_P(F) \geq 2$.

Let Q be another point on C, L a line through P and Q.



As C is irreducible, L is not contained in C.

Bézout : $I(P, C, L) + I(Q, C, L) = 2$.

$$\begin{array}{ccc} I(P,C,L) & + & I(Q,C,L) \\ \text{\rotatebox{90}{$\geq$}} & & \\ m_P(C) & + & m_Q(C) \\ \text{\rotatebox{90}{$\geq$}} & & \text{\rotatebox{90}{$\geq$}} \\ 2 & & 1 \end{array}$$

Contradiction.

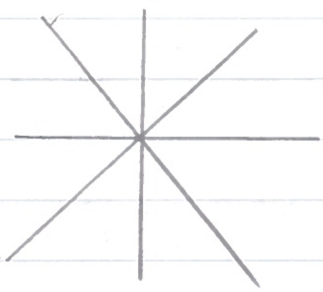
Rem : False if $\deg(C) > 2$.
ex : $zy^2 - x^3$ irreducible
but $[0:0:1]$ is a singular point.

Consequence A singular curve of degree 2 in $\mathbb{P}^2$ is a union of 2 lines.

—/—

Ex:

$$V_{\mathbb{P}}(x^2 - y^2) = V_{\mathbb{P}}(x-y) \cup V_{\mathbb{P}}(x+y)$$



$[0:0:1]$

—/—

FIN

Lin Qun.