Algebraic Curves

David Wiedemann

Table des matières

List of Theorems

Lecture 1: Introduction

Fri 25 Feb

Let K be a field, given a set of polynomials $S = \{f_1, \ldots\}$, we can consider $V(S) = \{(x_1, \ldots) \in K^n | f_i(x_1, \ldots) = 0 \forall i\}$.
Notice that if $a_1, \ldots \in K[x_1, \ldots]$ then also $\sum_i a_i(x) f_i(x) = 0$ only depends on the ideal generated by S.
If $I(S)$ happens to be prime, we call V an algebraic variety.

1 Affine algebraic sets

1.1 Recollection on commutative algebra

All rings are commutative and with unit.
Let R be a ring.

— R is an integral domain, or just domain if there are no zero divisors, ie, $\forall a, b \in R$ s.t.

$$a.b = 0 \implies a = 0 \text{ or } b = 0$$

— Any domain can be embedded into it's quotient ring.

— A proper ideal I is maximal if it's not contained in any other proper ideal
— A proper ideal I is prime if

$$\forall a, b \in R, ab \in I \implies a \in I \text{ or } b \in I$$

— A proper ideal I is radiccal if

$$a^n \in I \implies a \in I$$

— For any ideal $I \subset R$, the radical $\sqrt{I}$ is the smallest radical ideal containing I

Lemme 1
— *$I \subset R$ is maximal $\iff$ R/I is a field*

Lemme 2
— *$I \subset R$ is prime $\iff$ R/I is a domain*

Lemme 3
— *radical $\iff$ R/I has no nilpotent elements.*

Given a subset $S \subset R$ we can consider the ideal generated by S

$$I(S) = \left\{ \sum_i a_i s_i \right\}$$

I is finitely generated if $I = I(S)$ with S finite.

— We say that R is Noetherian $\not\exists$ a chain of strictly increasing ideals. Equivalently, every ideal is finitely generated.

> **Theorème 4**
> — *In fact, hilbert's basis theorem says that, if R is Noetherian, then $R[x]$ is noetherian.*

In particular $K[x_1, \ldots, x_n]$ is Noetherian

— I is in principal if it is generated by one element.

— A domain is called a principal ideal domain (PID) if every ideal is principal.

— $a \in R$ is irreducible if a is not a unit, nor zero and if

$$a = b.c$$

then either b or c are units.

— A pid $(a) \subset R$ is prime $\iff$ a is irreducible.

— R is a UFD if R is a domain and elements in R can be factored uniquely up to units and reordering into irreducible elements.

> **Theorème 5**
> *R is a UFD $\implies$ $R[x]$ is a UFD*

And, if R is a PID, then R is a UFD

> **Theorème 6 (Gauss Lemmma)**
> — *R is a UFD and $a \in R[X]$ irreducible, then also $a \in Q(R)[X]$ is irreducible.*

— Localization

Let R be a domain, if $S \subset R$ is a multiplicative subset, then the localization of R at S is defined as

$$S^{-1}R = \left\{ x \in Q(R) | x = \frac{a}{b}, b \in S \right\}$$

If M is an $R-$module, we have similarly

$$S^{-1}M = \left\{ \frac{m}{s} | m \in M, s \in M \right\} / \left\{ \frac{m}{s} = \frac{m'}{s'} \iff ms' = sm' \right\}$$

If $p \subset R$ is a prime ideal, then it's complement is a multiplicative subset and we define

$$R_p = (R \setminus p)^{-1} R$$

— There is a 1-1 correspondence between $p \subset R$ prime and ideals of R_p, furthermore R_p is a local ring
— Localization is exact, in particular, given $I \subset p$ the short exact sequence

$$o \to I \to R \to R/I \to 0$$

gets sent to

$$0 \to I_p \to R_p \to (R/I)_p \to 0 \tag{1}$$

ie. localization commutes with taking quotients.

1.2 Polynomial rings

For $a \in \mathbb{N}^n$, we set

$$X^a = X_1^{a_1} \ldots \in k[X_1, \ldots]$$

Thus for any $F \in k[X_1, \ldots, X_n]$, we can write it as

$$F = \sum_{a \in \mathbb{N}^n} \lambda_a X^a$$

F is homogeneous or a form of degree d if the coefficients $\lambda_a = 0$ unless $a_1 + \ldots + a_n = d$.
Any F can be written uniquely as $F = F_0 + \ldots + F_d$ where F_i is a form of degree i.
The derivative of $F = \sum_{a \in \mathbb{N}^n} \lambda_a X^a$ with repsect to X_i is $F_{X_i} = \frac{\partial F}{\partial X_i}$.
If F is a form of degree d we have

Theorème 7 (Euler's theorem)

$$\sum_{i=1}^{n} \frac{\partial F}{\partial X_i} X_i = dF$$

Lecture 2: Affine space and algebraic sets

Wed 02 Mar

1.3 Affine spaces and algebraic sets

Let k be a field.

Definition 1
For every $n \geq 0$ the affine n -space $\mathbb{A}_k^n$ is the set k^n .

In particular $\mathbb{A}^0$ is a point, $\mathbb{A}^1$ is a line, $\mathbb{A}^2$ the affine plane.
Given a subset $S \subset k[X_1, \ldots, X_n]$ of polynomials, we set

$$V(S) = \{x = (x_1, \ldots, x_n) \in \mathbb{A}^n | f(x_1, \ldots, x_n) = 0 \forall f \in S\}$$

If S is finite, we write $V(f_1, \ldots, f_k)$ for $V(S)$.
If the set S is a singleton, then we call $V(S)$ a hyperplane.
Any subset of $\mathbb{A}^n$ V algebraic if $V = V(S)$ for some subset of polynomials.

Lemme 8

- *Let $S \subset k[X_1, \ldots, X_n]$ and I the ideal generated by S, then $V(S) = V(I)$.*
- *Let $\{I_\alpha\}$ be a collection of ideals, then*

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

- *If $I \subset J$ then $V(J) \subset V(I)$*
- *For polynomials $f, g \in k[x_1, \ldots, x_n]$, then $V(f) \cup V(g) = V(f \cdot g)$ For ideals I, J ideals, then $V(I) \cup V(J) = V(I \cdot J)$ where $IJ = \{fg | f \in I, g \in J\}$*
- *For $a = (a_1, \ldots, a_n) \in \mathbb{A}^n, v(\{x_1 - a_1, \ldots\}) = \{a\}$*

Preuve

1. *Let $h \in \sum_i f_i g_i \subset I$ with $f_i \in S$ and $x \in V(S)$, then $f_i(x) = 0 \forall i$ hence $h(x) = 0 \implies x \in V(I) \implies V(S) \subset V(I)$.*
   Furthermore, if $x \in V(I)$, then in particular $f(x) = 0 \forall f \in S \subset I$, hence $x \in V(S)$ and $V(S) \supset V(I)$
2. *Let $x \in V(\cup I_\alpha)$, then for any α and $f \in I_\alpha$, we must have $f(x) = 0$, hence $x \in V(I_\alpha) \implies x \in \bigcap_\alpha V(I_\alpha)$.*
   Conversely, if $x \in \bigcap_\alpha V(I_\alpha)$ and $f \in \bigcup_\alpha I_\alpha$, then $f \in I_\alpha$ for some α, then $f(x) = 0$ hence $x \in V(\bigcup_\alpha I_\alpha)$ □

By Hilbert's basis theorem $k[x_1, \ldots, x_n]$ is Noetherian hence every ideal is finitely generated.

Corollaire 9
Every algebraic set $V \subset \mathbb{A}^n$ is of the form

$$V = V(f_1, \ldots, f_k) = V(f_1) \cap \ldots \cap V(f_k)$$

1.4 Ideals of a set of points and the nullstellensatz

Using the previous section, we have a map

$$V : \{ \text{ Ideals in } k[X_1, \ldots, X_N]\} \mapsto \{ \text{ algebraic sets in } \mathbb{A}^n\}$$

Conversely, for any subset $X \subset \mathbb{A}^n$ we define

$$I(X) \coloneqq \{f \in k[X_1, \ldots, X_N] | f(x) = 0 \forall x \in X\} \subset k[X_1, \ldots, X_N]$$

Lemme 10

1. *If $X \subset Y$ then $I(X) \supset I(Y)$*
2. *For $J \subset k[X_1, \ldots, X_N]$ an ideal $I(V(J)) \supset J$*
3. *For $W \subset \mathbb{A}^n$ algebraic, $V(I(W)) = W$*

Preuve

1. *Let $f \in I(Y)$, then f vanishes on X and hence f in $I(X)$*
2. *$I(V(J)) = \{f \in k[x_1, \ldots, x_n] | f(x) = 0 \forall x \in V(J)\} \supset J$*
3. *By definition $V(I(X)) \supset X$ for any X.*
   If in addition, if $X = V(J)$ algebraic, then $V(I(X)) = V((I(V(J)))) \subset V(J) = X$ □

There are essentially two reasons why $I(V(J)) \supsetneq J$ in general

1. $J = (x^n) \subset k[x] \implies V(x^n) = \{0\}$ and $I(\{0\}) = (x)$
2. $(x^2 + 1) \subset \mathbb{R}[x]$ and $I(\emptyset) = \mathbb{R}[X]$

Lemme 11
For any $X \subset \mathbb{A}^n$, $I(X)$ is a radical ideal

Preuve
If $f^n \in I(X)$ for some n, then $f(x)^n = 0$ and hence $f(x) = 0$ □

So the first phenomenon is related to the fact that J is not radical, the second is related to the fact that $\mathbb{R}$ is not algebraically closed.

Theorème 12 (Hilbert's Nullstellensatz)
Let K be algebraically closed, $J \subset k[X_1, \dots, X_n]$, then

$$I(V(J)) = \sqrt{J}$$

Using this, there is a one to one correspondence

$$\{ \text{ radical ideals in } k[X_1, \dots, X_n] \} \leftrightarrow \{ \text{ algebraic subsets of } \mathbb{A}^n \}$$

Theorème 13 (Weak Nullstellensatz)
Let K be algebraically closed, every maximal ideal $I \subset K[X_1, \dots, X_n]$ is of the form $I = \{x_1 - a_1, \dots, x_n - a_n\}$ with $a = (a_i) \in \mathbb{A}^n$

Corollaire 14
Let $I \subset K[X_1, \dots, X_n]$ be any ideal, then $V(I)$ is a finite set $\iff$ $k[X_1, \dots, X_n]/I$ is a finite dimensional K- vector space.
In this case

$$|V(I)| \leq \dim_k k[X_1, \dots, X_n]/I$$

Preuve
First, we show that if $k[x_1, \dots, x_n]/I$ is finite dimensional, then $V(I)$ is finite.
Let $I \subset k[X_1, \dots, X_n]$ be any ideal and $P_1, \dots, P_r \subset V(I)$ be distinct points, we want to show that $r \leq \dim_k k[x_1, \dots, x_n]/I$.
We can choose (Exercise) $F_1, \dots, F_r \in K[X_1, \dots, X_n]$ s.t. $F_i(P_j) = \delta_{ij}$, then we write $f_1, \dots, f_r$ for the residues of $F_1, \dots, F_r$ in $K[X_1, \dots, X_n]/I$.
We claim $f_1, \dots, f_r$ are linearly independent.
Indeed suppose $\sum_i \lambda_i f_i = 0$, this implies $\sum_i \lambda_i F_i \in I$ hence $0 = \sum \lambda_i F_i(P_j)$ which implies $\lambda_j = 0$, hence the f_i are linearly independent.
It follows that $\dim_k K[X_1, \dots, X_n]/I < \infty \implies |V(I)| < \infty$ and in this case $\dim_k K[X_1, \dots, X_n]/I \geq |V(I)|$.
Now assume $V(I)$ is a finite set $\{P_1, \dots, P_r\} \subset \mathbb{A}^n$ and write $P_i = (a_{i1}, \dots, a_{in})$ and define $F_j = \prod_{i=1}^{r} (X_j - a_{ij})$.
By construction $F_j \in I(V(I)) = \sqrt{I}$
$\exists N > 0$ such that $F_j^N \in I$.
Hence $f_j^N = 0$ in $K[X_1, \dots, X_n]/I$, but $f_j^N = (x_j^{Nr}) +$ lower order terms .
This means that X_j^{Nr} is a K-linear combination of $\{1, \dots, X_j^{Nr-1}\}$.
This means that X_j^s is a linear combination for any $s > 0$.
Hence taking products for different j's, we see that the set $\{x_1^{m_1}, \dots, x_n^{m_n}\}$ generates $K[X_1, \dots, X_n]/I$ □

Due to these theorems, we'll always suppose K is algebraically closed.

Lecture 3: Irreducible sets

Fri 11 Mar

1.5 Irreducible sets

Definition 2 (Irreducible set)
An algebraic set $V \subset \mathbb{A}^n$ is irreducible if $\forall W_1, W_2 \subset \mathbb{A}^n$ algebraic s.t. $V = W_1 \cup W_2$, then either $W_1 = V$ or $W_2 = V$

Exemple

- *Let $V = \{x_1, \dots, x_n\} \subset \mathbb{A}^n$ is irreducible iff $n = 1$*
- *Let $f(X, Y) = Y(X^2 - Y), V = V(f) \subset \mathbb{A}^2$ is not irreducible by taking $W_1 = V(Y), W_2 = V(X^2 - Y)$*

Proposition 16
An algebraic set V is irreducible iff $I(V)$ is prime.

Preuve
If $I(V)$ is not prime, let $F_1, F_2 \notin I(V)$ s.t. $F_1, F_2 \in I(V)$, then we can write $V = (V \cap V(F_1)) \cup (V \cap V(F_2))$.
Conversely, if $V = W_1 \cup W_2$ and $W_i \neq V$, then $I(W_i) \supsetneq I(V)$, pick $F_i \in I(W_i) \setminus I(V)$, then $F_1 F_2 = I(W_1) \cap I(W_2) = I(V)$. □

If $V \subset \mathbb{A}^n$ is irreducible, we can decompose it into a union of irreducible sets. The union is always finite as the polynomial ring is noetherian.

Theorème 17 (Theorem name)
Every $V \subset \mathbb{A}^n$ algebraic can be written uniquely (up to ordering) as a union of irreducible sets.

$$V = V_1 \cup \ldots \cup V_k$$

where the V_i's are irreducible and $V_i \not\subset V_j \forall i \neq j$

Definition 3 (Irreducible Components)
The $V_1 \ldots V_k$ are irreducible components of V.

Remarque
Applying I in theorem 1.9, we get

$$I(V) = I(V_1) \cap \ldots \cap I(V_k)$$

and $I(V_i)$ is the primary decomposition of $I(V)$

In general, it is quite difficult to find this decomposition.
For hypersurfaces, it's easy, for $I(F)$, write $F = F_1^{\alpha_1} \cdot \ldots F_k^{\alpha_k}$, then $V(F) = V(F_1) \cup \ldots \cup V(F_k)$.

1.6 Algebraic subsets of $\mathbb{A}^2$

Lemme 19
Let $F, G \in k[X, Y]$ with no common factors, then $V(F) \cap V(G)$ is a finite set of points.

Preuve
By Gauss's lemma, F, G have no common factors in $k(X)[Y]$. Since $k(x)[Y]$ is a PID $\exists A, B \in k(X)$ such that

$$AF + BG = 1$$

Now there exists $C \in k[X]$ such that $AC, BC \in k[X]$.
Let $(x, y) \in V(F, G)$, then $C(x) = 0$ and hence there are only finitely many x's possible.
By symmetry, the same is true for the Y coordinate, hence $|V(F, G)| < \infty \square$

Using this, we can now classify all algebraic subsets of $\mathbb{A}^2$.

Corollaire 20
The irreducible algebraic subsets of $\mathbb{A}^2$ are $\mathbb{A}^2, V(F)$ with F irreducible or singletons.

2 Affine algebraic varieties

Definition 4 (Affine algebraic variety)
An affine algebraic variety is an irreducible affine algebraic set.

2.1 Zariski topology

Definition 5 (Zariski topology)
The Zariksi-topology on $\mathbb{A}^n$ is the topology whose open sets are complements of algebraic sets.

Lemme 21
This indeed defines a topology on $\mathbb{A}^n$

Preuve
Certainly $\emptyset, \mathbb{A}^n$ are algebraic, hence their complements are open.
Let $\{U_i\}$ be a family of open sets, ie. such that

$$U_i = \mathbb{A}^2 \setminus V(I)$$

Then

$$\bigcup U_i = \bigcup \mathbb{A}^n \setminus V(I_i) = \mathbb{A}^n \setminus \bigcap_i V(I_i) = \mathbb{A}^n \setminus V(\bigcup I)$$

Similarly, if U_1, U_2 are open, then

$$U_1 \cap U_2 = \mathbb{A}^n \setminus I(V_1 V_2)$$ □

is again open.

Exemple
If $n = 1$, then algebraically closed sets are either $\mathbb{A}^n, \emptyset$ are finite union of points so the Zariski topology is the cofinite topology. Hence the open sets are huge.

Definition 6
For $V \subset \mathbb{A}^n$ an algebraic variety or set, the Zariski topology on V is just the subspace topology.

Definition 7 (New definition of irreducibility)
A non-empty subset V of a topological space X is irreducible if it cannot be expressed as $V = W_1 \cup W_2$ where $W_1, W_2 \subsetneq V$ are closed subsets.

Lemme 23
A non-empty open subset of an irreducible topological space is again irreducible and dense.
Furthermore, if $V \subset X$ is irreducible, then so is $\overline{V}$

The proof is an exercise.

Definition 8 (Quasi-affine algebraic variety)
A quasi-affine variety is an open subset of an affine variety.

Remarque
By the lemma above, quasi-affine variety are also irreducible.

2.2 Regular functions and coordinate rings

Regular functions are the natural "continuous" functions on algebraic varieties.

2.2.1 Affine case

Definition 9
Let $V \subset \mathbb{A}^n$ be an affine algebraic variety.
A map

$$f : V \to K = \mathbb{A}^1$$

is regular if $\exists F \in k[X_1, \ldots, X_n]$ such that

$$f(X) = F(X) \forall X \in V$$

The set $\Gamma(V)$ of regular functions on V is a ring with the usual pointwise multiplication and addition. and is called the coordinate ring of V.

Lemme 25
If $I = I(V)$ for some prime, then

$$\Gamma(V) \simeq {}^{k[X_1, \ldots, X_n]}\!/_{I(V)}$$

In particular, $\Gamma(V)$ is a domain.

Preuve
By definition, we have a surjective morphism

$$k[X_1, \ldots, X_n] \to \Gamma(V)$$

Now note that $F \in \ker \phi \iff F(X) = 0 \forall x \in V \iff F \in I(V)$ □

Definition 10 (Subobjects)
An affine subvariety of V is an affine variety contained in V.

Lemme 26
There is a one-to-one correspondence between V and $\Gamma(V)$ where

$$\{ \text{ algebraic subsets of } V \} \leftrightarrow \{ \text{ radical ideals of } \Gamma(V) \}$$

$$\{ \textit{ algebraic subvarieties of } V \} \leftrightarrow \{ \textit{ prime ideals of } \Gamma(V) \}$$

$$\{ \textit{ points of } V \} \leftrightarrow \{ \textit{ maximal ideals of } \Gamma(V) \}$$

The proof is again an exercise.

Definition 11 (Morphism)
A morphism $\phi : V \to W$ between affine algebraic varieties $V \subset \mathbb{A}^n, W \subset \mathbb{A}^m$ is a map such that $\exists$ polynomials $T_1, \ldots, T_m \in k[X_1, \ldots, X_n]$ such that

$$\phi(X) = (T_1(X), \ldots, T_m(X))$$

Then ϕ is an isomorphism if there exists a morphism ψ such that $\phi \circ \psi =$ Id and $\psi \circ \phi =$ Id.

Exemple
Take $V(X^2 - Y) \subset \mathbb{A}^2$ the the projection $p : V(X^2 - Y) \to \mathbb{A}^1$ on the first coordinate is an isomorphism with inverse $\psi(X) = (X, X^2)$.
A non-example of a bijective map which is not an isomorphism :
$\phi : \mathbb{A}^1 \to V(Y^2 - X^3)$, $\phi(t) = (t^2, t^3)$.
One can check that ϕ is bijective but not an isomorphism.

Lecture 4: Morphisms of Affine Varieties

Fri 18 Mar

In general any morphism $\phi : V \to W$ induces a morphism of rings (of k-algebras) $\tilde{\phi} : \Gamma(W) \to \Gamma(V)$ by composition, ie.

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

Proposition 28
This defines a one to one correspondence

$$\{ \textit{ Morphisms } \phi : V \to W \} \leftrightarrow \left\{ \textit{ k-algebra homomorphisms } \tilde{\phi} : \Gamma(W) \to \Gamma(V) \right\}$$

In particular ϕ is an isomorphism iff $\tilde{\phi}$ is an isomorphism.

Preuve
Need to construct for any $\alpha : \Gamma(W) \to \Gamma(V)$ a morphism $\overline{\alpha} : V \to W$ s.t.

$$\tilde{\overline{\alpha}} = \alpha$$

Suppose $V \subset \mathbb{A}^n, W \subset \mathbb{A}^m$ and write

$$\Gamma(V) = {}^{k[x_1, \ldots, x_n]}\!/_{I(V)} \text{ and } \Gamma(W) = {}^{k[y_1, \ldots, y_m]}\!/_{I(W)}$$

Choose lifts T_i of $\alpha([Y_i])$ in $k[x_1, \ldots, x_n]$.

In particular $\forall f \in \Gamma(W)$ *and* F *a lift,then*

$$\alpha(f) = F(T_1, \ldots, T_m) \mod I(V)$$

Then define $T : \mathbb{A}^n \to \mathbb{A}^m : x \mapsto (T_1(x) \ldots T_m(x))$.
We claim that $T(V) \subset W$.
From the diagram, we see that for any $G \in I(W)$, $G(T_1, \ldots, T_m) \in I(V)$, *hence for any* $v \in V$, $0 = G(T_1, \ldots, T_m)(v) = G(T(v))$ *which means that* $T(v) \in W$.
Now

$$\tilde{\overline{\alpha}} : \Gamma(W) \to \Gamma(V)$$

satisfies $\forall v \in V \forall f \in \Gamma(W)$

$$\tilde{\overline{\alpha}}(v) = f(\overline{\alpha}(v)) = f(T(v)) = \alpha(f(v)) \implies \tilde{\overline{\alpha}} = \alpha \qquad \square$$

Definition 12
The quotient field $K(V)$ *of* $\Gamma(V)$ *is called the field of rational function on* V.

Let $f \in K(V)$ is defined at a point $p \in V$ if we can write f as the quotient $f = \frac{a}{b}$ and $b(p) \neq 0$.
The pole set of $f \in K(V)$ is the set of points where f is not defined.

Remarque
$\Gamma(V)$ *is not a UFD in general, and so the presentation* $f = \frac{a}{b}$ *is not unique.*

Exemple
$V = (xy - zw) \subset \mathbb{A}^4$ *and let* $\overline{x}, \overline{y}, \overline{z}, \overline{w} \in \Gamma(V)$ *be the respective images.*
Then $f = \frac{\overline{x}}{\overline{y}} = \frac{\overline{z}}{\overline{w}}$.
Hence f *is defined whenever* $Y \neq 0$ *or* $w \neq 0$
Hence the pole set of f *is* $\{Y = 0\} \cap \{W = 0\}$

Definition 13 (Local Ring)
The local ring of V *at a point* $p \in V$ *is a subring* $K(V)$ *defined by*

$$\mathcal{O}_p(V) = \{f \in K(V) | f \text{ defined at } p \}$$

We have natural inclusions $\Gamma(V) \subset \mathcal{O}_p(V) \subset K(V)$

Remarque
$\Gamma(V), \mathcal{O}_p(V)$ *and* $K(V)$ *are intrinsic to* V, *ie. if* $V \simeq W$ *then* $\Gamma(V) \simeq \Gamma(W)$ *and* $\mathcal{O}_p(V) \simeq \mathcal{O}_{p'}(W)$

Proposition 32
Let $p \in V$ and $m_p \subset \Gamma(V)$ be the corresponding maximal ideal, then

$$\mathcal{O}_p(V) \simeq \Gamma(V)_{m_p}$$

In particular $\mathcal{O}_p(V)$ is a noetherian local domain and we have that

$$\Gamma(V) = \bigcap_{p \in V} \mathcal{O}_p(V) \subset K(V)$$

Preuve
Recall that $m_p = \{f \in \Gamma(V) | f(p) = 0\}$, then

$$\begin{aligned} \Gamma(V)_{m_p} &= \left\{ f \in K(V) | f = \frac{a}{b}, b \notin m_p \right\} \\ &= \mathcal{O}_p(V) \end{aligned}$$

The rest follows from standard properties of localization.
In particular for any domain R we have that

$$R = \bigcap_{m \in R, m \text{ maximal}} R_m$$

□

Notice that the notions of regular functions is sufficient to define morphisms of local rings etc.
How can we extend this to quasi-affine varieties ?

Exemple
Consider $V(XY-1) \subset \mathbb{A}^2$.
There is a natural projection $\phi : V(XY-1) \to x \in \mathbb{A}^1$.
The image of ϕ is $\mathbb{A}^n \setminus \{0\}$ quasi-affine and we'd like ϕ to be an isomorphism, ie.

$$\phi^{-1}(x) = (x, \frac{1}{x})$$

Ie. the map $x \to \frac{1}{x}$ should be a regular function on $\mathbb{A}^1 \setminus \{0\}$.

Definition 14
Let $V \subset \mathbb{A}^n$ be quasi-affine.
A map $f : V \to \mathbb{A}^1 = k$ is called regular if $\forall v \in V$ there exists an open neighbourhood $v \in U \subset V$ and $g, h \in k[x_1, \ldots, x_n]$ s.t. $h(V) \neq 0 \forall x \in U$ and $f(x) = \frac{g(x)}{h(x)}$

Why do we need the U ?

Exemple
Consider again $V = V(XY - ZW) \setminus V(Y, W)$ and consider $f = \frac{x}{w} = \frac{z}{y}$ on V.
None of the two presentations works on V

Definition 15
Let $\mathcal{O}(V)$ be the ring of regular functions on V

Remarque
$f : V\mathbb{A}^1 \setminus \{0\} \to \mathbb{A}^1 : x \mapsto \frac{1}{x}$ *is regular.*
Then we may take $U = V$, it is not hard to see that

$$\mathcal{O}(V) = k[x][\frac{1}{x}, \frac{1}{x^2}, \ldots]$$

In particular $\mathcal{O}(V) \supsetneq \Gamma(\mathbb{A}^1)$

If $V \subset \mathbb{A}^n$ is affine, then we have $k[x_1, \ldots, x_n] \to \mathcal{O}(V) : F \mapsto (v \mapsto F(v))$.

Proposition 36
For V affine, we have that $\Gamma(V) \simeq \mathcal{O}(V)$.

Preuve
We have $O(V) \subset O_p(V)$ $\forall p \in V$ hence $\Gamma(V) \hookrightarrow O(V) \hookrightarrow \bigcap_{p\in V} O_p(V) = \Gamma(V)$ □

Lemme 37
Let V be a quasi-affine subset and $f : V \to \mathbb{A}^1$ regular, then f is continuous (with respect to the Zariski topology)

Preuve
It is enough to show that $f^{-1}(X)$ is closed for any closed X .
Without loss of generality $X = \{x\}$.
Let $V = \cup_i U_i i$ a cover such that $f|_{U_i} = \frac{g_i}{h_i}$ and $h_i \neq 0$ on U_i.
Then $f^{-1}(X) \cap U_i = \left\{v \in U_i | f(v) = \frac{g_i(v)}{h_i(v)}\right\} = \{v \in U_i | x \cdot h_i(v) - g_i(v) = 0\}$ which is an algebraic set.
Hence $f^{-1}(X) \cap U_i$ is closed which implies $f^{-1}(X)$ is closed. □

Corollaire 38
Let $f, g \in O(V)$ and $U \subset V$ non empty and open s.t. $f|_U = g|_U$ then $f = g$

Preuve
Using an exercise, open subsets are dense, since f, g are continuous

$$f|_U = g|_U \implies f|_{\mathrm{cl}\, U} = f|_{\mathrm{cl}\, V}$$ □

Remarque
Let $U \subset V$ open, then the restriction of functions induces $\mathcal{O}(V) \to \mathcal{O}(U)$.
i.e. $\mathcal{O}(-)$ defines a sheaf of k-algebras on V.
Using this one can define a general algebraic as a topological space X with some sheaf $\mathcal{O}_X$ which locally looks like a quasi-affine variety V with $\mathcal{O}(-)$.
We'll define $\mathcal{O}_p(V)$ and $K(V)$ for V quasi-affine, but these depend only on "local structure".
We can guess $\mathcal{O}_p(V) = \mathcal{O}_p(\operatorname{cl} V)$ and similarly for the quotient field.

3 (Quasi-)Projective and general algebraic varieties

Affine varieties usually "go to infinity" when we draw them.
This leads to complications in the theory

Exemple
Two distinct lines in $\mathbb{A}^2$ they will intersect in 1 point unless they're parallel

3.1 Projective space

Definition 16 (Projective n-space)
$\mathbb{P}^n$ is the set

$$\mathbb{P}^n = K^{n+1} \setminus \{0\}/\sim$$

Where we identify

$$(x_1, \dots, x_{n+1}) \sim (y_1, \dots, y_{n+1}) \text{ if } \exists \lambda \in K^* \text{ s.t. } x_i = \lambda y_i$$

Elements in $\mathbb{P}^n$ are called points.

If $p \in \mathbb{P}^n$ is the equivalence classe of $(x_1, \dots, x_{n+1}) \in \mathbb{A}^{n+1}$ we write

$$p = [x_1 : \dots : x_n]$$

$x_1, \dots, x_n$ are the homogenuous coordinates of p.

Remarque
Any point in $\mathbb{A}^n \setminus \{0\}$ defines a line through the origin and $x, y \in \mathbb{A}^n \setminus \{0\}$ define the same line iff $x = \lambda y$

Lecture 5: Projective varieties

Fri 25 Mar

While the i-th coordinate x_i of a point $[x_1 : \dots : x_{n+1}] \in \mathbb{P}^n$ is not well defined, the equation $x_i = 0$ or $x_i \neq 0$ is well defined.

Hence we can write

$$U_i = \{[x_1 : \ldots : x_n] | x_i \neq 0\}$$

Clearly $\mathbb{P}^n = \cup_i U_i$.
Furthermore for all i, we have a bijection

$$\phi_i : \mathbb{A}^n \to U_i$$
$$(x_1, \ldots, x_n) \mapsto [x_1 : \ldots : x_{i-1} : 1 : x_{i+1} : \ldots : x_{n+1}]$$

And this is clearly a bijection.
We'll see in a bit, that the ϕ_i's provide an open cover of $\mathbb{P}^n$ by $\mathbb{A}^n$

Definition 17
The set

$$H_\infty \coloneqq \mathbb{P}^n \setminus U_{n+1} = \{x \in \mathbb{P}^n | x_{n+1} = 0\}$$

is called the hyperplane at infinity.

One can identify $H_\infty = \mathbb{P}^{n-1}$
Thus

$$\mathbb{P}^n = U_{n+1} \coprod H_\infty = \mathbb{A}^n \coprod \mathbb{P}^{n-1}$$

Exemple
$\mathbb{P}^0 =$ *point*
$\mathbb{P}^1 = \mathbb{A}^1 \coprod$ *point is called the projective line.*
Similarly $\mathbb{P}^2$ *is called the projective plane.*

3.2 Projective algebraic sets

For a general $F \in k[x_1, \ldots, x_n]$, the equation $F(x) = 0, x \in \mathbb{P}^n$ doesn't make sense.
But it does if F is homogeneous, say of degree d, since then

$$F(\lambda x) = \lambda^d F(x) = 0 \forall x \in \mathbb{A}^{n+1}, \lambda \in k^*$$

Definition 18 (Projective set)
For any set $S \subset k[x_1, \ldots, x_n]$ *of homogeneous polynomials we set*

$$V(S) = \{[x_1 : \ldots : x_n] \in \mathbb{P}^n | F(x_1, \ldots, x_n) = 0 \forall F \in S\}$$

A subset of $\mathbb{P}^n$ *is algebraic if it is of the form* $V(S)$ *as above.*

Exemple
Take $V(X^2 - YZ) \subset \mathbb{P}^2$*, how to draw it ?*
We draw the intersections $V \cap U_i$

Definition 19 (Homogeneous ideal)
An ideal $I \subset k[x_1, \dots, x_n]$ is homogeneous if it is generated by homogeneous elements.
The for I a homogeneous ideal we set

$$V(I) = V(T) \subset \mathbb{P}^n$$

where T is the set of forms in I.

Remarque
Since the ring is noetherian, we can always find a finite number of homogeneous generators.
For $I = (x_1, \dots, x_{n+1})$ we have $V(I) = \emptyset$, we denote this ideal by I_+, it's called the irrelevant ideal.

Exemple
(x, y^2) is homogeneous, $(x + y^2, y^2)$ is also homogeneous but $(x + y^2)$ is not.

Lemme 46
I is a homogeneous ideal if and only if for every $F \in I$, if we write $F = \sum_{i \geq 0} F_i$ with F_i homogeneous of degree i.

Preuve
Let $G^{(1)}, \dots, G^{(k)}$ be a set of homogeneous generators of I with degrees $d_1, \dots, d_k$.
Any $F = \sum F_i$ can be written as $F = \sum A^{(i)} G^{(i)}$ for some $A^{(i)}$.
Since the degree is additive we get $F_j = \sum A^{(i)}_{j-d_i} G^{(i)}$
For the other direction, let $G^{(1),\dots,G^{(k)}}$ any set of generators, then $G^{(i)}_j \in I$ and then the set of $G^{(i)}_j$ is a set of generators. □

Furthermore, the sum, the product, the intersection and the radical of homogeneous ideals are homogeneous.
A homogeneous ideal is prime if for any homogeneous $f, g \in k[x_1, \dots, x_n]$

$$fg \in I \implies f \in I \text{ or } g \in I$$

Definition 20 (Zariski topology)
We define the Zariski topology on $\mathbb{P}^n$ by taking the open sets to be the complements of algebraic sets.

This defines a topology using the properties above.

Definition 21
An algebraic set $V \subset \mathbb{P}^n$ is irreduciable if it is irreducible as a topological space.

As in the affine case, there is a correspondence

$$\{ \text{ Algebraic subsets in} \mathbb{P}^n \} \leftrightarrow \{ \text{ Homogeneous ideals in } k[x_1, \dots, x_{n+1}] \}$$

Where $I(V)$ is the ideal generated by $\{F \in k[x_1, \dots, x_n] | F \text{ homogeneous }, F(v) = 0 \forall v \in V\}$

Remarque
If we need to distinguish between the affine and projective correspondence we'll write V_a, I_a and V_p, I_p respectively.

Definition 22 (Cone)
For $V \subset \mathbb{P}^n$ algebraic, we define the conve over V as

$$C(V) = \left\{(x_1, \dots, x_{n+1}) \in \mathbb{A}^{n+1} | [x_1, \dots, x_{n+1}] \in V\right\} \cup \{(0, \dots, 0)\}$$

Lemme 48

1. *For $V \neq \emptyset$, then*
$$I_p(V) = I_a(C(V))$$
2. *If $I \subsetneq k[x_1, \dots, x_n]$ homogeneous, then*
$$C(V_p(I)) = V_a(I)$$

Preuve

1. *$G \in I_p(V)$ homogeneous and $(x_1, \dots, x_{n+1}) \in C(V)$, then $G(x_1, \dots, x_{n+1}) = 0$*
Conversely, if $G \in I_a(C(V))$ write
$$G = \sum_i G_i, \quad G_i \text{ homogeneous}$$
Then, for every $x \in C(V)$ and $\lambda \in k^*$ we have $\lambda x \in C(V)$ hence
$$0 = G(\lambda x) = \sum_i \lambda^i G_i(x)$$
Let $\tilde{G}(y) = \sum_i y^i G_i(x) \in K[Y]$, this has infinitely many 0's.
Which in turn implies $G_i \in I_p(V)$
2. *Notice for G homogeneous non-constant, then*
$$C(V_p(G)) = V_a(G)$$

Since I is generated by homogeneous polynoials, the satement holds. □

Proposition 49 (Projective nullstellensatz)
Let I be a homogeneous ideal, then
- *If $V_p(I) = \emptyset$, then $\sqrt{I} = k[x_1, \dots, x_{n+1}]$ or $\sqrt{I} = I_+$*
- *If $V_p(I) \neq \emptyset$ then $I_p(V_p(I)) = \sqrt{I}$*

Preuve
- *If $V_p(I) = \emptyset \iff V_a(I) \subset \{(0, \dots, 0)\}$ which implies $\sqrt{I} \supset (x_1, \dots, x_{n+1})$.*
- $I_p(V_p(I)) = I_a(C(V_p(I))) = I_a(V_a(I)) = \sqrt{I}$ □

Corollaire 50
There is a one-to-one correspondence between radical homogeneous ideals and projective algebraic sets.
Furthermore $V_p(I)$ is irreducible $\iff$ I is prime.

Remarque
Points in $\mathbb{P}^n$ do not correspond to maximal ideals.

We can also relate affine and projective algebraic sets through the charts

$$\phi_i : \mathbb{A}^n \to U_i$$

We'll focus on $\phi \coloneqq \phi_{n+1} : \mathbb{A}^n \to U \coloneqq U_{n+1}$
For $F \in k[x_1, \dots, x_n]$ homogeneous, we define

$$F_*(x_1, \dots, x_n) = F(x_1, \dots, x_n, 1)$$

Conversely, for $G \in k[x_1, \dots, x_n]$, we write

$$G = \sum_{i=0}^{d} G_i \text{ and define } G^*(x_1, \dots, x_{n+1}) = x_{n+1}^d G_0 + \dots + G_d = X_{n+1}^d G(\frac{x_1}{x_{n+1}}, \dots, \frac{x_n}{x_{n+1}})$$

Definition 23 (Homogenization)
$(\cdot)_*$ and $(\cdot)^*$ are called dehomogenisation and homogenization.

For I an ideal, we denote by I^* be the homogeneous ideal generated by $\{F^* | F \in I\}$.
Conversely, if $V = V_a(I)$, we write

$$V^* = V_p(I^*)$$

V^* is called the projective closudre of V in $\mathbb{P}^n$.
Similarly if I is homogeneous, then

$$I_* = \{F_* | F \in I\}$$

and if $V = V_p(I)$, we set $V_* = V_a(I_*)$

Exemple
Let $F = X_1^2 - X_2$, *then*

$$F^* = X_1^2 - X_2 X_3$$

Lemme 53
If $V \subset \mathbb{A}^n$ *is closed, then* $\phi(V) = V^* \cap U$
Conversely, if $V \subset \mathbb{P}^n$ *is closed then* $\phi^{-1}(V \cap U) = V_*$
In particular ϕ *is a homeomorphism*

Preuve
Recall that $\phi(x_1, \ldots, x_n) = [x_1 : \ldots : x_n : 1]$.
For $V \subset \mathbb{A}^n$ *write* $V = V_a(F_1, \ldots, F_k)$ *then*

$$V^* = V_p(F_1^*, \ldots, F_k^*)$$

But $F_i^* = X_{n+1}^d F_i(\frac{x_1}{x_{n+1}, \ldots, \frac{x_n}{x_{n+1}}})$ $F_i(v) = 0 \iff F_i^*(\phi(v)) = 0 \implies \phi(V) = V^* \cap U$ □

Lecture 6: Algebraic varieties

Fri 01 Apr

3.3 Quasi-projective and general varieties

Definition 24
A projective variety is a closed irreducible subset of $\mathbb{P}^n$.
A quasi-projective variety is an open subset of a projective variety.
An algebraic variety is one of the four types we've seen : affine, quasi-affine, projective or quasi-projective.

Remarque
In order to define morphisms between varieties, we need regular functions, ie. $\mathcal{O}(V)$ *for* V *quasi-projective.*

Definition 25
Let $V \subset \mathbb{P}^n$ *be quasi-projective, a map* $f : V \to k$ *is regular at* $p \in V$ *if* $\exists$ *an open neighbourhood* $p \in U \subset V$ *and* $g, h \in k[x_1, \ldots, x_{n+1}]$ *formes of the same degree such that* $h(U) \neq 0$ *and such that* $f(u) = \frac{g(u)}{h(u)}$

Exemple
Set $V = \mathbb{P}^n$ and take also $U = V$ in the definition, then $h(u) \neq 0 \forall u \in \mathbb{P}^n$ is only possible if h is constant.
In fact, constants are the only regular functions on $\mathbb{P}^n$ and in fact on any projective variety.

Definition 26
We again, define $\mathcal{O}(V)$ the ring of regular functions on V.

Remarque
As in the quasi-affine case, regular functions are continuous for the Zariski topology.

3.4 Morphisms

Definition 27 (Morphism)
A morphism between two algebraic varieties V, W is a continuous map $\phi : V \to W$ such that for every open $U \subset W$ and every $f \in \mathcal{O}(U)$ the map $\phi \circ f : \phi^{-1}(U) \to k$ is regular.

ϕ is an isomorphism if $\exists \psi : W \to V$ such that $\phi \circ \psi$ and $\psi \circ \phi$ is the identity.

Remarque
In particular any $\phi : V \to W$ induces a map $\tilde{\phi} : \mathcal{O}(W) \to \mathcal{O}(V)$ a k-algebra homomorphism.
The converse is only true if W is affine.

Proposition 58
The maps $\phi_i : \mathbb{A}^n \to U_i \subset \mathbb{P}^n$ are isomorphisms.
In fact, for every $V \subset \mathbb{A}^n$ quasi-affine, $\phi_i|_V$ is an isomorphism onto it's image $\phi_i(V) \subset \mathbb{P}^n$ which is quasi-projective.

Preuve
We may take $i = n + 1$ and write $\phi = \phi_{n+1} : \mathbb{A}^n \to U$
We know that ϕ is a homeomorphism, hence $\phi(V)$ is quasi projective since

$$\phi(V) \subset \phi(\overline{V}) = \overline{\phi(V)} = \overline{\phi(V)}^* \cap U \subset \overline{\phi(V)}^*$$

Let F be some regular function on some open $W \subset \phi(V)$.
By shrinking if necessary we can write $F = \frac{G}{H}$ where G and H are forms of the same degree and $H(w) \neq 0 \forall w \in W$.

Then

$$F \circ \phi = \frac{G \circ \phi}{H \circ \phi} = \frac{G_*}{H_*}$$

and since G_* and H_* don't vanish on $\phi^{-1}(W)$, $F \circ \phi$ is regular.
Thus $\phi|_V$ is a morphism of algebraic varieties.
Conversely, we have $\phi^{-1} : U \to \mathbb{A}^n$, let $W \subset V$, take $F \in \mathcal{O}(W)$, up to shrinking.
Then $F \circ \phi^{-1}([x_1 : \ldots : x_{n+1}]) = \frac{G(\frac{x_1}{x_{n+1}},\ldots)}{H(\frac{x_1}{x_{n+1}},\ldots)} = x_{n+1}^{\alpha} \frac{G^*([x_1:\ldots:x_{n+1}])}{H^*[x_1:\ldots:x_{n+1}]}$.
Now, if $\alpha \geq 0$ then x_{n+1}^{α} then $x_{n+1}^{\alpha} G^*$ and H^* are of the same degree.
If $\alpha < 0$, then G^* and $x_{n+1}^{-\alpha} H^*$.
Hence $F \circ \phi^{-1} \in \mathcal{O}(\phi(V))$ and hence ϕ^{-1} is a morphism. □

Definition 28
A variety is (quasi-) affine or quasi-projective if V is isomorphic to a quasi-affine or quasi-projective variety.

Corollaire 59
Any variety is quasi-projective.
Every quasi-projective variety admits a finite open cover by quasi-affine varieties namely $V = \bigcup_i V \cap U_i$

Preuve
projective implies quasi-projective and affine implies quasi-affine and the theorem above gives quasi-affine implies quasi-projective.
Furthermore, since $\mathbb{P}^n = \bigcup_i U_i \implies V = \bigcup V \cap U_i$.
If V is projective,$V \cap U_i \subset U_i \simeq \mathbb{A}^n$ is closed and irreducible, hence $V \cap U_i$.
Finally, if $V \subset \overline{V} \subset \mathbb{P}^n$ quasi-projective, then $V \cap U_i \subset \overline{V} \cap U_i$ is quasi-affine. □

Exemple
For any polynomial $f \in k[x_1, \ldots, x_n]$, $\mathbb{A}^n \setminus V(f)$ is affine, but $\mathbb{A}^2 \setminus \{0\}$ is not affine.

Remarque
The above also shows that if V is quasi-affine, then $\mathcal{O}(V) \simeq \mathcal{O}(\phi(V))$, hence all our definitions of $\mathcal{O}(-)$ are compatible.

The definition of a morphism is clean, but difficult to check in practice.
It becomes easier if at least the target is affine :

Lemme 62
Let $\phi : V \to W$ be a map, suppose $W \subset \mathbb{A}^n$ affine, and $x_i : \mathbb{A}^n \to \mathbb{A}^1$

coordinate functions, then ϕ is a morphism $\iff$ $x_i \circ \phi : V \to \mathbb{A}^1$ is regular.

Preuve

If ϕ is a morphism, then $x_i \circ \phi$ is regular by definition.
Conversely, if $x_i \circ \phi$ is regular for all $1 \leq i \leq n$, then

$$f \circ \phi$$

is also regular for any $f \in k[x_1, \ldots, x_n]$.
Since regular functions form a ring.
Hence

$$\begin{aligned} \phi^{-1}(V(f_1, \ldots, f_k) \cap W) &= \bigcap \phi^{-1}(V(f_i) \cap W) \\ &= \bigcap (f \circ \phi)^{-1}(0) \end{aligned}$$

Thus ϕ is continuous.
Now let $U \subset W$ be open and $f \in \mathcal{O}(U)$, after shrinking, we may suppose $f = \frac{g}{h}$ where $g, h \in k[x_1, \ldots, x_n], h(u) \neq 0 \forall u \in U$.
Then

$$f \circ \phi = \frac{g \circ \phi}{h \circ \phi}$$

where $g \circ \phi, h \circ \phi$ are regular and $h \circ \phi(v) \neq 0 \forall v \in V$.
Thus $\frac{1}{h \circ \phi}$ is regular, therefore $\frac{g \circ \phi}{h \circ \phi}$ is regular. □

Exemple

Now, the map $\mathbb{A}^1 \setminus \{0\} \to V(XY - 1) \subset \mathbb{A}^2$ is a morphism.

Corollaire 64

Let V, W be two varieties and W affine, then there is a bijection

$$\hom_{Var}(V, W) \simeq \hom_{k- \ alg}(\mathcal{O}(W), \mathcal{O}(V))$$

sending $\phi \to \tilde{\phi}$

Remarque

If V is projective, we claim that $\mathcal{O}(V) \simeq k$

3.5 General rational functions an local rings

Let V be an algebraic variety and $p \in V$.

Definition 29 (Local ring)
The local ring of V at p : $\mathcal{O}_p(V)$ is the set of pairs $\langle U, f\rangle$, where $U \subset V$ is open containing p and f is a regular function on U, modulo the relation

$$[U, f] \sim [U', f'] \iff f = f' \text{ on } U \cap U'$$

Lemme 66
$\sim$ is an equivalence relation and $\mathcal{O}_p(V)$ is a ring with the operations

$$[U, f] + [U', f'] = [U \cap U', f + f']$$

and similarly for the product

$$[U, f] \cdot [U', f'] = [U \cap U', f \cdot f']$$

Furthermore $\mathcal{O}_p(V)$ is a local ring with maximal ideal

$$m = \{[U, f] | f(p) = 0\}$$

Preuve
Reflexivity and identity is obvious, we need to check transitivity, suppose $[U, f] \sim [U', f']$ and $[U'', f''] \sim [U', f']$ then clearly $F = f''$ on $U \cap U' \cap U''$ but

$$U \cap U' \cap U'' \subset U \cap U''$$

is open and dense and since f, f'' are continuous, $f = f''$ on $U \cap U''$.
To show the ring is local, notice that there is an evaluation morphism

$$\mathcal{O}_p(V) \to k$$
$$[U, f] \to f(p)$$

This map is surjective since we have constant functions.
Hence m_p is a maximal ideal.
Finally $\mathcal{O}_p(V)$ is local since $[U, f] \notin m_p$ hence $f(p) \neq 0$.
Thus $\frac{1}{f}$ is regular in some neighbourhood of p.
Thus f is a unit. □

Lecture 7: rational functions and dimension

Fri 08 Apr

3.6 The field of rational functions

Definition 30 (Field of rational functions)
$K(V)$ is the set of pairs (U, f) with $U \subset V$ open and non-empty and f a regular function on U modulo the equivalence relation $(U, f) \sim (U', f')$ iff $f = f'$ on $U \cap U'$.

Remarque
Since V is irreducible, any non-empty open is dense, hence $U \cap U'$ is non-empty and open as well.

Furthermore, note that $[U, f]$ has $\frac{1}{f}$ as an inverse.
As in the affine case, we have inclusions

$$\mathcal{O}(V) \hookrightarrow \mathcal{O}_p(V) \hookrightarrow K(V)$$

Proposition 68

1. *Let V be an algebraic variety and $U \subset V$ open and non-emtpy.*
   Then $K(V) = K(U)$ and $\mathcal{O}_p(V) = \mathcal{O}_p(U)$ for any $p \in U$
2. *For any algebraic variety V and any $p \in V, K(V)$ is the quotient field of $\mathcal{O}_p(V)$.*
3. *If V is affine, then $\mathcal{O}_p(V) = \Gamma(V)_{m_p}$ for anu $p \in V$ and $K(V)$ is the quotient field at $\Gamma(V)$.*
   In particular all definitions of $K(V)$ and $\mathcal{O}_p(V)$ agree for affine varieties.

Remarque

1. *For $V \subset \mathbb{P}^n$ quasi-projective and $P \in V \cap U_i$ for some i, then $\mathcal{O}_p(V) = \mathcal{O}_p(\overline{V}) = \mathcal{O}_p(\overline{V} \cap U_i)$.*
   Since $U_i = \mathbb{A}^n, \overline{V} \cap U_i$ is affine and $\mathcal{O}_p(\overline{V} \cap U_i) = \Gamma(\overline{V} \cap U_i)_{m_p}$.
   Thus $\mathcal{O}_p(V)$ is always an explicit localization(as any variety is quasi-projective).

Preuve

1. *Immediate from the definition : $[W, f] \in \mathcal{O}_p(V)$.*
   We know that $[W, f] \sim [W \cap U, f] \in \mathcal{O}_p(U)$ so there is a bijection between the equivalence classes.
2. *As in the remark, we can reduce to the affine case and then it follows from the third part of the proposition.*
3. *We have a map $\Gamma(V)_{\mathfrak{m}_p} \to \mathcal{O}_p(V)$ sending $\frac{f}{g} \to [V, \frac{f}{g}]$.*
   It is injective by continuity (as V is open hence dense.).

And also surjective by definition of $\mathcal{O}_p(V)$.
Indeed, any $[U,h] \in \mathcal{O}_p(V)$ is of the form $h = \frac{f}{g}$ with $g(u) \neq 0$ on U.
Since U is quasi-affine , f and g are both quotients of regular functions on $V = \overline{U}$.
Similarly, we have an inclusion $Q(\Gamma(V)) \hookrightarrow K(V)$ sending $\frac{f}{g} \to [V, \frac{f}{g}]$.
But any $[U,h] \in K(V)$ is contained in $\mathcal{O}_p(V) \subset Q(\Gamma(V))$ for any $p \in U$ so we also have a reverse inclusion. □

3.7 Dimension of a Variety

Should be a basic invariant, in fact it isn't.

Definition 31 (Dimension of a topological space)
The dimension of a topological space X is the largest integer n such that there exists a chain $Z_n \supset \ldots \supset Z_1 \supset Z_0$ of distinct irreducible closed subsets of X .
Then, the dimension of an algebraic set is it's dimension as a topological space.

So now we'd like to relate this definition with the dimension theory for rings.
Recall that in any ring A, the height $ht(p)$ of a prime ideal $P \subset A$ is the supremum of all integers n such that $\exists$ a chain $p_0 \subset \ldots \subset p_n = p$ of distinct prime ideals.
The krull dimension of A is defined as

$$\dim A = \sup \{ht(p) | p \subset A \text{ prime } \}$$

Proposition 70
If $V \subset \mathbb{A}^n$ is an affine algebraic variety, then

$$\dim V = \dim \mathcal{O}(V)$$

Preuve
If $V_0 \subset V_1 \ldots \subset V_d = V$ is a maximal chain of irreducible closed subsets of V, then ($d < \infty$ by Noetherianity), applying I gives

$$I(V_1) \supset \ldots \supset I(V_d) = I(V)$$

is a chain of distinct prime ideals containing $I(V)$, so in the quotient we get a chain

$$p_0 \supset \ldots p_d = (0) \text{ in } \mathcal{O}(V)$$ □

So $\dim \mathcal{O}(V) \geq \dim V$*, we can of course go the other way to find* $\dim \mathcal{O}(V) \leq \dim V$

Computing dimensions is hard, the main tool is the following theorem

Theorème 71
Let K *be a field and* B *a domain, which is a finitely generated* K*-algebra, then*

$$\dim B = \text{ transcendence degree of } {}^{Q(B)}\!/_{K}$$

— *For any prime ideal* $p \subset B$ *we have*

$$ht(p) + \dim {}^{B}\!/_{p} = \dim B$$

Corollaire 72
$\dim \mathbb{A}^n = n$

Preuve
We have that

$$\dim \mathbb{A}^n = \dim K[x_1, \ldots, x_n] = trdegK(x_1, \ldots, x_n) = n$$ □

Corollaire 73
If $V \subset \mathbb{P}^n$ *is a quasi-projective variety, then*

$$\dim \overline{V} = \dim V$$

To prove this, we need the following lemma

Lemme 74
If X *is a topological space and* $\{U_i\}$ *a family of open subsets covering* X*, then*

$$\dim X = \sup_i \dim U_i$$

Preuve (Of the Corrolary)
Let $U_1, \ldots, U_{n+1}$ *be the open charts of* $\mathbb{P}^n$*, then* $V_i = V \cap U_i$ *gives an open cover of* V *by quasi-affine varieties and* $\overline{V} \cap U_i = \overline{V_i}$ *where the second closure is taken in* $\mathbb{U}_i \simeq \mathbb{A}^n$*.*

If we know the corollary for quasi-affine varieties, we get that

$$\dim \overline{V} = \sup \dim \overline{V_i} = \sup \dim V_i = \dim V$$

Therefore, assume $V \subset \mathbb{A}^n$ is quasi-affine of dimension d and let $Z_0 \subset \ldots \subset Z_d$ be a maximal chain of irreducibles in V .
Hence $Z_d = V$ and $Z_0 = \{x\}$.
Let $m \subset \mathcal{O}(\overline{V})$ be the maximal ideal corresponding to x, we claim that $ht(m) = d$.
If this is true, then we have

$$\dim \overline{V} = \dim \mathcal{O}(\overline{V}) = \dim {}^{\mathcal{O}(\overline{V})}\!/_{m} + ht(m) = d$$

So now we have to prove the claim.
Clearly $ht(m) \geq d$.
Let $p_0 \subset \ldots \subset p_r = m$ be a longer chain of distinct prime ideals in $\mathcal{O}(\overline{V})$.
Set $W_i = V(p_i) \to \overline{V} = W_0 \supset \ldots \supset W_r = \{x\}$.
Intersecting with V gives

$$V = W_0 \cap V \supset \ldots \supset W_r \cap V = \{x\}$$

Since $W_i \cap V \subset W_i$ are open and non-empty, $W_i \cap V$ is irreducible.
By maximality of the initial sequence $\exists i$ such that

$$W_i \cap V = W_{i+1} \cap V$$

But then $W_i = \overline{W_i \cap V} = \overline{W_{i+1} \cap V} = W_{i+1}$ which is a contradiction. □

From linear algebra, we would expect that if V is given by r "independent" equations should have dimension $n - r$.

Proposition 75

— *Let V be an affine variety of $\dim d$ and $H = V(F) \subset \mathbb{A}^n$ a hypersurface such that $V \subsetneq H$. Then every irreducible component of $V \cap H$ has dimension $d - 1$.*

— *Let $I \subset K[x_1, \ldots, x_n]$ be an ideal that can be generated by r polynomials, then every irreducible component of $V(I)$ has dimension $\geq n - r$*

Note that it is <u>not</u> true that if we choose the minimal number of generators, we get equality

Exemple
If $I = (XY, YZ) \subset K[x, y, z]$, then

$$V(I) = V(Y) \cup V(X, Z)$$

Lecture 8: Dimension

Fri 29 Apr

We'll use the following without proof :

Theorème 77 (Krull's Hauptidealsatz)
Let A be a noetherian ring, $f \in A$ neither a 0-divisor nor a unit.
Then any minimal ideal containing f has height 1.

We can now prove the above proposition.

Preuve
$V \not\subset H = V(f)$ which means $f \neq 0$ in $\mathcal{O}(V)$.
Hence, f is not a zero-divisor.
If f is a unit in $\mathcal{O}(V)$, then $V \cap H = \emptyset$ and there is nothing to prove.
Otherwise every irreducible component of $V \cap H \subset V$ corresponds to a prime ideal p in $\mathcal{O}(V)$ and p is minimal .
Hence $ht(p) = 1$ and thus $\dim V(p) = \dim(\mathcal{O}(V)/p) = \dim(\mathcal{O}(V)) - ht(p) = d - 1$

To prove the second statement we argue by induction.
For $r = 0$, this is trivially true.
Let $I = (f_1, \dots, f_r)$ with $r \geq 1$ and W an irreducible component of $V(I)$.
By induction any irreducible component W' of $V(f_1, \dots, f_{r-1})$ has dimension $n - (r-1)$.
By a every irreducible component of $W' \cap V(f_r)$ has dimension $\geq n - r$.
W is a union of irreducible components of $W' \cap V(f_r)$. □

4 Local Properties of plane curves

Definition 32 (Plane curve)
Let $F, G \in K[x, y]$ are equivalent if $\exists \lambda \in K^\times$ such that $F = \lambda G$.

An affine plane curve is an equivalence class of non constant polynomials in $K[x, y]$.
If $F = \prod F_i e^i$ with F_i irreducible.
We call F_i the components of F ad e_i the multiplicities. Note that we can recover the F_i from $V(F)$ but not the e_i's.
The degree of an affine plane curve is the degree of F as a polynomial.
A line is a curve of degree 1.
If F is irreducible, we write $\Gamma(F), \mathcal{O}_p(F)$ for $\Gamma(V(F))$ etc.

Definition 33 (Singular point)
Let F be a plane curve and $P = (a, b) \in F$.
Then P is called a simple point if either

$$\frac{\partial F}{\partial X}(p) = F_X(p) \neq 0 \text{ or } \frac{\partial F}{\partial Y}(p) \neq 0$$

Ie., if the jacobian of F has full rank. In this case, the line $L(x, y) = F_x(p)(X - a) + F_y(p)(Y - b)$ is the tangent line to F at p .
A point which is not simple is called singular or multiple.
A curve with only simple points is called non-singular or smooth.

We'll usually arrange things such that $p = (0, 0)$ is a singular point of F.
Writing $F = F_m + \ldots + F_n$ for F_i forms of degree i, $(0, 0) \in F \iff m \geq 1$

Definition 34
The integer $m = m_p(F)$ is called the multiplicity of F at $p = (0, 0)$

We have that $p = (0, 0)$ is simple iff $m = 1$.
And in this case F_1 is the tangent line to F at $(0, 0)$.
If $m = 2$ then $p = (0, 0)$ is called a double point.
Since F_m is homogeneous and in two variables we can factor it as

$$F = \prod L_i^{r_i}$$

where L_i are distinct lines through the origin.
To see this, notice that the dehomonigenization $(F_m)_* = F_m(X, 1)$ factors into linear terms.

Definition 35
The L_i are called the tangent lines to F at $(0, 0)$.

L_i is a simple (double, triple,...) tangent if $r_i = 1(2, 3)$.
A point P is an ordinary multiple point of F , if F has m distinct tangents at p.
An ordinary double point is called a node. It is in many ways the simplest example of a singular point.

Exemple
Let $F = Y^2 - X^3 - X^2 = F_2 + F_3$.
We can write $F_2 = (Y - X)(Y + X)$

If $F = \prod F_i^{e_i}$ then $m_p(F) = \sum_i e_i m_p(F_i)$.
And if L is a tangent to F_i with multiplicity r_i, then L is a tangent to F with

multiplicity $\sum e_i r_i$.
For $p = (a, b)$ let $T(x, y) = (x + a, y + b)$ and set $F^T(x, y) = F(T(x, y))$.
We then define $m_p(F) = m_{(0,0)}(F^T)$ and similarly for tangent lines, multiple points etc.

Theorème 79
Let P be a point on an irreducible plane curve F and $\mathfrak{m}_p(F) \subset \mathcal{O}_p(F)$ the corresponding maximal ideal.
Then for sufficiently large n, we have that

$$m_p(F) = \dim_K \left({\mathfrak{m}_p(F)^n}/{\mathfrak{m}_p(F)^{n+1}} \right)$$

Exemple
Let $F = X$ and $p = (0, 0)$, then

$$\mathfrak{m}_P(F) = (Y, X) \subset \left({k[x, y]}/{(x)} \right)_{(x,y)}$$

and

$$\mathfrak{m}_p(F)^n = (Y^n)$$

and thus ${(Y^n)}/{(Y^{n+1})}$ is generated by Y^n

We'll need the following lemma

Lemme 81
Let $I \subset K[X_1, \ldots, X_n]$ be an ideal such that $V(I) = \{P_1, \ldots, P_n\}$ is finite.
Let $\mathcal{O}_i = \mathcal{O}_{P_i}(\mathbb{A}^n)$.
Then there is an isomorphism

$$\Phi : {K[x_1, \ldots, x_n]}/{I} \to \prod {\mathcal{O}_i}/{I \cdot \mathcal{O}_i}$$

We'll prove the theorem assuming this.
Let's write $\mathcal{O}, \mathfrak{m}$ and m for $\mathcal{O}_p(F), \mathfrak{m}_p(F)$ and $m_p(F)$.
We have the exact sequence

$$0 \to {\mathfrak{m}^n}/{\mathfrak{m}^{n+1}} \to {\mathcal{O}}/{\mathfrak{m}^{n+1}} \to {\mathcal{O}}/{\mathfrak{m}^n} \to 0$$

The theorem follows if $\dim({\mathcal{O}}/{\mathfrak{m}^n}) = n \cdot m + s$ and all $n \geq m$ Without loss of generality $P = (0, 0)$ and hence $\mathfrak{m}^n = I^n \mathcal{O}$.
Then

$${\mathcal{O}}/{\mathfrak{m}^n} = {\mathcal{O}}/{I^n \mathcal{O}} = {\mathcal{O}_p(\mathbb{A}^2)}/{(F, I^n)} = {K[x, y]}/{(F, I^n)}$$

Notice $\forall G \in I^{n-m}\ GF \in I^n$.

We get a short exact sequence

$$K[x,y]/I^{n-m} \xrightarrow{F} k[x,y]/I^n \to K[x,y]/(F,I^n) \to 0$$

Since $\dim_k K[x,y]/I^n = \frac{n(n+1)}{2}$ we have

$$\dim K[x,y]/(F,I^n) = \frac{n(n+1)}{2} - \frac{(n-m)(n-m+1)}{2} = mn - \frac{m(m-1)}{2}$$

Lecture 9: stuff

Fri 06 May

We now show the lemma above.

Preuve
Let $\mathfrak{m}_i = \mathfrak{m}_{p_i}$ *and* $R = k[x_1,\dots,x_n]/I$ *and* $R_i = \mathcal{O}_i/I\mathcal{O}_i$.
For each i *we have the localisation map*

$$\phi_i : K[x_1,\dots,x_n]/I \to \mathcal{O}_i/I\mathcal{O}_i$$

And we define ϕ *as the product of the* ϕ_i .
To show that ϕ *is an isomorphism, we construct idempotents :* $e_1,\dots,e_n \in R$ *such that*

$$e_i^2 = e_i, e_ie_j = 0 \text{ and } \sum_i e_i = 1$$

Further, we'll want $e_i(P_i) = 1$ *and* $\forall G \in k[x_1,\dots,x_n]$ *with* $G(P_i) \neq 0$, $\exists t \in R$ *such that* $tg = e_i$ $(g = \overline{G})$.
Let's suppose we have such e_i*'s, then*

1. ϕ *is injective.*
   Indeed, if $f \in \ker\phi_i \iff \exists G$ *with* $G(P_i) \neq 0$ *and* $GF \in I$ *Thus,* $f \in \ker\phi \implies \forall i \exists G_i$ *with* $G_i(P_i) \neq 0$ *and* $G_iF = 0$

   $$f = \sum_i e_if = \sum_i t_ig_if$$

2. ϕ *is surjective.*
   Let $z = (\frac{a_1}{g_1},\dots,\frac{a_n}{g_n}) \in \prod R_i$ *where* $g_i(P_i) \neq 0$.
   Let $t_i \in R$ *be such that* $t_ig_i = e_i$, *since* $e_i(P_i) = 1$, $\phi_i(e_i) \in R^*$.
   $\phi_i(e_j) = \phi_i(e_je_i)\phi(e_i)^{-1} = 0$
   Thus

   $$\phi_i(e_i) = \phi_i(\sum_i e)i) = \phi_i(1) = 1$$

   Hence $\phi_i(t_ig_i) = 1$ *and*

   $$\frac{a_i}{g_i} = \phi_i(a_it_i)$$

Let's construct $e_1,\dots,e_n$ *:*
By the nullstellensatz, we have that $\sqrt{I} = I(P_1,\dots,P_n) = \bigcap_{i=1}^N \mathfrak{m}_i$

Thus there exists d such that $(\bigcap_i \mathfrak{m}_i)^d \subset I$.
Choose F_i such that $F_i(P_j) = \delta_{ij}$ and set $E_i = 1 - (1 - F_i^d)^d$.
Then the residues $e_i \in R$ of E satisfy 1 and 2.
We have $E_i = F_i^d D_i$ thus $E_i \in \mathfrak{m}_j^d \forall j \neq i$.
Then $i \neq j$ implies $E_i E_j \in \bigcap_k \mathfrak{m}_k^d = (\bigcap \mathfrak{m}_k)^d \subset I$.
Then

$$1 - \sum_i E_i = 1 - E_j = \sum_{i \neq j} E_i \in \bigcap_k \mathfrak{m}_k^d \subset I$$

Further

$$E_i - E_i^2 = E_i(1 - F_i^d)^d \in \bigcap \mathfrak{m}_j^d \mathfrak{m}_i^d \subset I$$

Let $G \in k[x_1, \ldots, x_n], G(P_i) \neq 0$, say $G(P_i) = 1$, $H = 1 - G \in \mathfrak{m}_i$.
Then $H^d E_i \in \mathfrak{m}_i \bigcap_{j \neq i} \mathfrak{m}_j^d \in I$.
Then

$$g(e_i + he_i + \ldots + h^{d-1}e_i) = e_i - h^d e_i = e_i$$ □

4.1 Curves and DVR's

Proposition 82

Let R be a domain that is not a field, then the two following things are equivalent

1. *R is a noetherian, local and the maximal ideal is principal.*
2. *There exists an irreducible element $t \in R$ such that every non zero element $z \in R$ can be written uniquely as $z = U \cdot t^n$, where $U \in R^\times$ and $n \in \mathbb{Z}_{\geq 0}$.*

Definition 36 (Discrete valuation ring)
A ring satisfying these properties is called a discrete valuation ring.

Exemple

1. *$K[[t]]$, with maximal ideal (t)*
2. *$k[x]_{(x)} = \left\{ \frac{f}{g} | g(0) \neq 0 \right\}$*
3. *$\mathbb{Z}_{(p)}$.*

We prove the equivalence above.

Preuve
$1 \implies 2$
Let $\mathfrak{m} \subset R$, let $t \in \mathfrak{m}$ be a generator.
Since $(t) = \mathfrak{m}$, t is irreducible.
Assume $ut^m = vt^n$ with $n \geq m$.

Then

$$u = vt^{n-m} \in R \setminus \mathfrak{m}$$

Assume $\exists z \in R \setminus \{0\}$ *which is not of the form* ut^n .
Since z *is not a unit,* $z \in (t)$.
Thus there exists z_1 *such that* $z = tz_1$.
If z_1 *is a unit, we're done, otherwise we get* $z_1, \ldots,$ *with* $z_i = tz_{i+1}$.
Since R *is noetherian, the chain*

$$(z) \subset (z_1) \subset \ldots$$

stabilizes.
Thus, there exists a $v \in R$ *such that* $z_{n+1} = vz_n = vtz_{n+1}$.
$2 \implies 1$
Clearly $\mathfrak{m} = (t)$ *is the set of non-units, thus* R *is local with maximal ideal* (t).
It's enough to show that every ideal of R *is finitely generated.*
Let $I \subset R$ *be an ideal, then* $I \subset \mathfrak{m}$.
Let $n = \min\{n | \exists n \in R^\times$ *such that* $ut^n \in I\}$.
Then $t^n \in I$, *but any* $z \in I$ *is of the form* ut^m *and thus* I *is finitely generated.*
The proof also shows that any ideal in R *is of the form* (t^n), *thus DVR* $\implies$ *PID.* □

Definition 37 (uniformizer)
A generator t *of* $\mathfrak{m}$ *in DVR is a uniformizer.*

If $K = Q(R)$ denotes the quotient field, then any $z \in K$ can be written uniquely as $z = ut^n$ with $u \in R^\times$ and $n \in \mathbb{Z}$.
The integer n is called the order of z and is denoted $ord(z)$.

Corollaire 84
Let F *be an irreducible plane curve and* $p \in F$, *then* p *is simple iff* $\mathcal{O}_p(V)$ *is a DVR.*

In this case, if $L = aX + bY + c$ is any line through P that is not tangent to F, then it's image in $\mathcal{O}_p(F)$ is a uniformizer.

Definition 38
If $p \in F$ *is simple,* F *irreducible, we write* ord_p^F *for the order on* $K(F)$.

We have $ord_p^F(g) = \dim_K(\mathcal{O}_p(F)/(g))$ for any $g \in \mathcal{O}_p(F)$.

Preuve
If $\mathcal{O}_p(F)$ is a DVR, let $\mathfrak{m}_p(F) = (x)$, then

$$\mathfrak{m}_p(F)^n = (x^n) \to \mathcal{O}_p(F) \to k$$

Where we send λx^n to λ.
This map is surjective with kernel (X^{n+1}), thus

$$m_P(F) = \dim_K({}^{(X^n)}\!/_{X^{n+1}}) = 1 \qquad \square$$

Conversely, let P be a simple point, say $P = (0,0)$.
Let T be the unique tangent and $L \neq T$ a line as in the statement.
$\exists A \in GL_2(K)$ such that $AT = \{y = 0\}$ and $AL = \{X = 0\}$.
Since $FA \simeq F$ as varieties, we may assume that $T = Y, L = X$.
Then $F = Y +$ terms of higher order.
We need to show $\mathfrak{m}_p(F) = (x, y) \subset \mathcal{O}_p(F)$ is principal with generator X.
Write $F =$ (All monomial containing Y) + Rest $= Y(1 + H(x,y)) + X^2G(x)$.
The image of $1 + H$ is a unit in $\mathcal{O}_p(F)$.
Thus $Y = x^2G(x)(1 + H)^{-1} \in \mathcal{O}_pF$.
Thus $(x, y) = (x)$ is principal, thus $\mathcal{O}_p(F)$ is a DVR.

Lecture 10: Intersection numbers

Fri 13 May

4.2 Intersection Numbers

Definition 39 (Intersection Number)
Let $p \in \mathbb{A}^2$, F, G two plane curves, then the intersection number of F and G at p $I(p, F \cap G) = \dim_k \mathcal{O}_p(\mathbb{A}^2)/(F, G) \in \mathbb{N} \cup \infty$

Definition 40 (Transversal intersection)
Two plane curves F, G intersect transversally at $p \in F \cap G$ if p is a simple point of F and G and the tangent of F at p is different from the tangent of G at p.

In fact

Proposition 85
Two plane curves intersect transversally iff $I(p, F \cap G) = 1$

Preuve
Suppose F irreducible.

$$\mathcal{O}_p(\mathbb{A}^2)/_{(F,G)} = ({}^{k[x,y]}\!/_{(F,G)})_{m_p} = ({}^{\Gamma(F)}\!/_{G})_{m_p} = \mathcal{O}_p(F)/_{(g)}$$

where g is the image of G at $\mathcal{O}_p$.
Note that since $G(p) = 0, g \in m_p$.
Further, recall that the tangent of G at p is a uniformizer of $\mathcal{O}_p(F)$.
Thus

$$\mathcal{O}_p(F)/(g) = \mathcal{O}_p(F)/(L) \simeq k$$

□

Exemple
Let $G = x^2 - y$ and $F = y$
Then

$$\mathcal{O}_p(\mathbb{A}^2)/(F,G) \simeq (k[x,y]/(x^2 - y, y))_{m_p} = k[x]/(x^2)$$

We now move on to axiomatic properties of intersection numbers

Theorème 87 (Axiomatic properties)

1. *$I(p, F \cap G) = \infty$ iff p lies on a common component of F and G*
2. *$I(p, F \cap G) = 0$ iff $p \notin F \cap G$*
3. *(locality) $I(p, F \cap G)$ only depends on the components of F and G passing through p.*
4. *$I(p, F \cap G) = I(p, G \cap F)$*
5. *(lower bound) $I(p, F \cap G) \geq m_p(f)m_p(G)$ and we have equality iff F and G have no common tangent line at P .*
6. *(compatibility with products) If $F = \prod F_i^{r_i}$ and $G = \prod G_i^{s_j}$, then*

$$I(p, F \cap G) = \sum_{i,j} r_i s_j$$

7. *$I(p, F \cap G) = I(p, F \cap (G + FA))\forall a \in k[x, y]$*
8. *If p is a simple point of F*

$$I(p, F \cap G) = ord_p^F(G)$$

9. *(local-global) if F, G have no common component, then $\sum_{p \in F \cap G} I(p, F \cap G) = \dim_k(k[x,y]/(F,G))$*

Preuve
Lets first prove 1 and 9 .
If F, G have no common component, then $|V(F,G)| < \infty$ and by some lemma

$$k[x,y]/(F,G) = \prod_{p \in F \cap G} \mathcal{O}_p(\mathbb{A}^2)/(F,G)$$

Thus, $\forall p \in F \cap G, I(p, F \cap G) < \infty$, taking dimensions yields

$$\dim_k {k[x,y]}/{(F,G)} = \sum_{p \in F \cap G} I(p, F \cap G)$$

If H is a common irreducible component of F, G.
The slogan is that ${\mathcal{O}_p(\mathbb{A}^2)}/{(F,G)}$ is "bigger than" $\Gamma(H)$.
Indeed, we have a surjective map (just a quotient)

$${\mathcal{O}_p(\mathbb{A}^2)}/{(F,G)} \to {\mathcal{O}_p(\mathbb{A}^2)}/{(H)}$$

Since $\dim \Gamma(H) = \infty$, we have that $I(p, F \cap G) = \infty$.
Now we prove 2.
Note that $p \in F \cap G \iff m_p \supset (F,G) \iff (F,G) \subsetneq \mathcal{O}_p(\mathbb{A}^2) \iff I(p, F \cap G) \neq 0$.
To show 3, write $F = F_1 F_2$, if $F_2(P) \neq 0$, thus $F_2(P)$ is a unit in $\mathcal{O}_p(\mathbb{A}^2)$ thus $(F,G) = (F_1, G)$, hence we get equality. To show 6, note that it is sufficient to show that $\forall F, G, H \in k[x,y]$

$$I(p, F \cap GH) = I(P, F \cap G) + I(P, F \cap H)$$

We may also assume that F, GH have no common irreducible components, otherwise the equality is trivial.
We'll decompose the ring ${\mathcal{O}_p(\mathbb{A}^2)}/{(F,GH)}$.
We'll write $\mathcal{O} \coloneqq \mathcal{O}_p(\mathbb{A}^2)$.
Then we have a short exact sequence

$$0 \to {\mathcal{O}}/{(F,H)} \xrightarrow{\xi} {\mathcal{O}}/{(F,GH)} \xrightarrow{\phi} {\mathcal{O}}/{(F,G)} \to 0$$

Where ϕ is the quotient map $(F,G) \supset (F,GH)$ and ξ is the multiplication by G.
Showing that this is exact will imply the claim, it is in fact enough to show that

$$0 \to {k[x,y]}/{(F,H)} \xrightarrow{\xi} {k[x,y]}/{(F,G)} \to {k[x,y]}/{(F,G)} \to 0$$

Note that ϕ is surjective since it is a quotient.
ψ is injective :
Let $z \in k[x,y]$, we want to prove that if $Gz \in (F,GH)$ then $z \in (F,H)$.
Assume that $Gz = AF + BGH \iff AF = G(z - BH)$, since F, G have no common components $F | z - BH$ thus there exists C such that $z = BH + CF \in (F,H)$
To show 7, simply notice that $(F,G) = (F, G + AF)$.
Finally, wlog, suppose F is irreducible (if it isn't split into irreducible components), then

$${\mathcal{O}(\mathbb{A}^2)}/{(F,G)} = {\mathcal{O}_p(F)}/{(g)}$$

Finally, taking dimensions we get the desired equality.
We now go on to prove part 5.
Write $m = m_p(F), n = m_p(G)$ *and assume* $p = (0,0)$*, then* $m_p = I = (X,Y)$.
Consider the resolution

$$k[x,y]/I^n \times k[x,y]/I^m \to k[x,y]/I^{n+m} \to k[x,y]/(I^{n+m}, F, G)$$

where the first map is given by $\psi(A,B) = FA + BG$.
Since $k[x,y]/(I^{n+m}, F, G) \simeq \mathcal{O}_p(\mathbb{A}^2)/(I^{n+m}, F, G)$ ·
Since $\mathcal{O}_p(\mathbb{A}^2)/(F,G)$ *surjects onto this ring,* $(I(p, F \cap G)) \geq \dim_k k[x,y]/(I^{n+m}, F, G) \geq \dim k[x,y]/I^{m+n} - \dim_k k[x,y]/I^n - \dim_k k[x,y]/I^m = mn$.
Thus $I(p, F \cap G) \geq mn$ *with equality iff* $\alpha : \mathcal{O}_p(\mathbb{A}^2)/(F,G) \to \mathcal{O}_p(\mathbb{A}^2)/(I^{m+n}, F, G)$ *is an isomorphism and* ψ *is injective.*
Thus the proposition follows if can show that if F, G *have no common tangents at* P*, then* $I^t \subset (F,G) \cdot \mathcal{O}_p(\mathbb{A}^2)$ *for* $t \geq m + n - 1$.
Further we have to show that ψ *is injective iff* F, G *have no common tangents.*
First we show that $I^t \subset (F,G) \cdot \mathcal{O}_p(\mathbb{A}^2)$ *for larget* t *:*
Let $V(F,G) = \{P, Q_1, \ldots, Q_s\}$ *and choose* H *such that* $H(p) \neq 0$ *and* $H(Q_i) = 0$.
Thus $\exists N$ *such that* $(HX)^N$ *and* $(HY)^N \in (F,G)$.
But H^N *is a unit, thus* $X^N, Y^N \in (F,G) \cdot \mathcal{O}_p(\mathbb{A}^2)$.
Thus $I^{2N} \subset (F,G) \cdot \mathcal{O}_p(\mathbb{A}^2)$.
Now let $L_1, \ldots, L_m$ *be the tangents of* F *at* P *and* $M_1, \ldots, M_n$ *the tangents of* G *at* P.
Set $A_{i,j} = L_1 \ldots L_i M_1 \ldots M_j$ *where we set* $L_i = L_m$ *if* $i \geq m+1$ *and* $M_j = M_n \forall j > n$.
Using an exercise, the set $\{A_{i,j} | i + j = t\}$ *is a basis for* I^t/I^{t-1}.
Hence we need to show that $A_{i,j} \subset (F,G) \cdot \mathcal{O}_p(\mathbb{A}^2)$ *if* $i + j \geq m + n - 1$.
Wlog $i \geq m$ *then* $A_{i,j} = A_{m,0}B$ *with* $B \in I^{i+j-m}$ *and we can write* $F = A_{m,0} + F'$ *with* $F' \in I^{m+1}$ *and we can write* $A_{i,j} - BF = BF' \in I^{i+j+1}$.
We can now repeat this with elements in $I^{i+j+1}, I^{i+j+2}, \ldots$.

Let's show the second point.
Let $A, B \in k[x,y]$ *with* $\psi(A,B) = AF + BG = 0$.
Write $A = A_r + \ldots + A_d$ *and* $B = B_s + \ldots + B_{d'}$.
We need to show $r \geq n$ *and* $s \geq m$*, assume not, then write*

$$A_r F_m + B_s G_n + \text{ higher order } \in I^{m+n} \qquad \square$$

Thus $A_r F_m = -B_s G_n$*, since by assymption* F_m, G_n *have no common factors, thus* $F_m | B_s, G_n | A_r$ *thus* $m \leq s$ *and* $n \leq r$.

For the other direction, assume L is a common tangent, then $F_m = LF'_{m-1}$ and $G_n = LG'_{n-1}$, then $\psi(G'_{n-1}, -F'_{n-1}) = G_{n-1'}F - F'_{m-1}G = 0$

4.3 Algorithm for $I(p, F \cap G)$

The main idea is to notice that it is easy to compute $\forall G$

$$I(p, Y \cap G)$$

So let's suppose $p = (0,0)$ (wlog) and $F, G \ni p$.
Let $r = \deg(F(x,0)), j = \deg(G(x,0))$ and wlog $r \leq s$.
Now, if $r = 0$, then $Y|F$ hence by 6

$$I(p, F \cap G) = \underbrace{I(p, Y \cap G)}_{\text{easy}} + \underbrace{I(p, H \cap G)}_{\text{compute recursively}}$$

So write $G(X,0) = X^m(a_0 + a_1X \ldots)$ where $m > 0$ because $p \in G$.
Then $I(p, Y \cap G) = m$
Now for the second case, assume $F(X,0)$ are monic, then let $H = G = X^{s-r}F$ then $I(p, F \cap G) = I(p, F \cap G) = I(p, F \cap H)$ and $\deg(H(x,0)) < r$ and we repeat until r or s is $= 0$.

Lecture 11: Projective Plane Curves

Fri 20 May

5 Projective Plane Curves

Definition 41 (Plane Curves)
Two non constant forms $F, G \in k[x,y,z]$ are equivalentif $\exists \lambda \in K^*$ such that $F = \lambda G$.
A projective plane curve is an equivalence class of forms.
The degree of a projective plane curve is the degree of a form representing it.
As before we'll write $F \subset \mathbb{P}^2$ instead of $V(F)$.

Curves of degrees $1, 2, 3, 4$ are called lines, conics, cubics and quartics.
Components and multiplicities are defined as in th affine case.
If $p = [x : y : 1]$, then $\mathcal{O}_p(F) = \mathcal{O}_{(x,y)}(F_*)$.
The multiplicity $m_p(F)$ of F at $p \in \mathbb{P}^2$ is defined as (for F irreducible)

$$m_p(F) = \dim_k {m_p^n(F)}/{m_p^{n+1}(F)}$$

for n big enough.
If $p \in F$ is a simple point ($\iff m_p(F) = 1$) and F is irreducible then $\mathcal{O}_p(F)$

is a DVR.
We write ord_p^F for the corresponding order function on $K(F)$.
Finally, if $P = [x, y, 1]$ and F, G projective plane curves, we set $I(p, F \cap G) = I((x, y), F_* \cap G_*) = \dim_k {}^{\mathcal{O}_{(x,y)}(\mathbb{A}^2)}\!/_{(F_*, G_*)}$.
Where we always choose a "practical" dehomogenization.

Remarque
We'd like to define

$$I(p, F \cap G) = \dim_k({}^{\mathcal{O}_p(\mathbb{P}^2)}\!/_{(F,G)})$$

but F, G are not functions defined in a neighbourhood of p.

However if L is any line in $\mathbb{P}^2$ not containing p, then $\frac{F}{L^{\deg F}} \in \mathcal{O}_p(\mathbb{P}^2)$, if L' is another line, then $\frac{F}{L^{\deg F}}, \frac{F}{L'^{\deg F}}$ differ by $(\frac{L'}{L})^{\deg F}$ which is a unit in $\mathcal{O}_p(\mathbb{P}^2)$.
By abuse of notation we may write $F \in \mathcal{O}_p(\mathbb{P}^2)$ for $\frac{F}{L^{\deg F}}$ which is well defined up to a unit.
And then

$$I(p, F \cap G) = \dim_k \left({}^{\mathcal{O}_p(\mathbb{P}^2)}\!/_{(F,G)} \right)$$

In particular, $I(p, F \cap G)$ does not depend on the dehomogenization we choose.

Definition 42
A line L is tangent to F at p if

$$I(p, L \cap F) > m_p(F)$$

P is an ordinary multiple point of F if there are $m_p(F)$ distinct tangents.

5.1 Bezout's Theorem

Theorème 89 (Bezout)
Let F, G be projective plane curves of degree m and n and suppose F and G have no common component.
Then,

$$\sum_{p \in F \cap G} I(p, F \cap G) = mn$$

We defer the proof until next week.

Corollaire 90
If F, G have no common components, then

$$\sum_{p \in F \cap G} m_p(F) m_p(G) \leq \deg F \deg G$$

Preuve
Immediate using the theorem about general properties of intersection numbers. □

Corollaire 91
If F and G meet in $\deg F \deg G$ points, then all these points are simple.

Corollaire 92
If two curves of degree m and n have more than mn points in common, then they must have a common component.

Lecture 12: Bezout's Theorem

Fri 27 May

Preuve (Bezout's Theorem)
First, notice that F and G having no common components implies that $|F \cap G| < \infty$.
After a projective change of coordinates, we may assume that none of these points lie at ∞.
Then,

$$\sum_{p \in F \cap G} I(p, F \cap G) = \sum_{p \in F_* \cap G_*} I(p, F_* \cap G_*) = \dim_k {}^{k[x,y]}\!/_{(F_*, G_*)}$$

Now, let $\Gamma = {}^{k[x,y,z]}\!/_{(F,G)}, \Gamma_* = {}^{k[x,y]}\!/_{(F_*, G_*)}$ and $R = k[x, y, z]$.
Consider $h : \Gamma \to \Gamma_*$ sending $\overline{H} \to \overline{H}_*$.
Set $\Gamma_d = \left\{\overline{H} \in \Gamma | \deg H = d\right\} \cup \{0\}$, note that Γ_d is a vector space.
We claim that $\dim_k \Gamma_d = mn$ for $d \geq m + n$.
Since F, G have no common components, we have an exact sequence

$$0 \to R \xrightarrow{\psi} R \times R \xrightarrow{\phi} R \to \Gamma \to 0$$

where $\psi(c) = (cG, -cF)$ and $\phi(A, B) = (AF + BG)$.
Restricting this to a given degree, we get

$$0 \to R_{d-m-b} \to R_{d-m} \times R_{d-n} \to R_d \to \Gamma_d \to 0$$

Since $\dim R_k = \frac{(k+1)(k+2)}{2}$ we get $\Gamma_d = mn$.

Now, we claim that the map $\alpha : \Gamma \to \Gamma$ *sending* $\overline{H} \to \overline{zH}$ *is injective.*
In particular, $\alpha|_{\Gamma_d} : \Gamma_d \to \Gamma_{d+1}$ *is an isomorphism for* $d \geq m + n$.
Assume $\overline{zH} = 0 \iff zH = AF + BG$.
Let $A_0, B_0, F_0, G_0 \in k[x, y]$ *be* $A(x, y, 0), \ldots$.
As $F \cap G \cap \{z = 0\} = \emptyset$, F_0 *and* G_0 *have no common components, since any such component would be homogeneous and it's* 0*-set would be contained in* $F \cap G \cap \{z = 0\}$.
Thus $B_0 = F_0 c$ *and* $A_0 = -G_0 C$.
Set $A' = A + GC$ *and* $B' = B - FC$.
Then $A'_0 = A_0 + G_0 c = 0 = B'_0$, *thus* $z|A', z|B'$.
Thus $zH = AF + BG = (A + GC)F + (B - FC)G$, *thus* $\overline{H} = 0$.

Finally, we claim that $H|_{\Gamma_d} : \Gamma_d \to \Gamma_*$ *is an isomorphism of* k*-vector spaces.*
Let $\overline{A}_1, \ldots, \overline{A}_{mn}$ *be a basis of* Γ_d.
The image of this basis generates Γ_* *:*
Let $H_* \in \Gamma_*$ *and* $N > 0$ *such that*

$$z^N H^* = z^{N'} H(\frac{x}{z}, \frac{y}{z})$$

is a form of degree $N' = d + r \geq d$,, *thus* $\overline{z^{N'} H^*} \in \Gamma_{d+r} \simeq \Gamma_d$.
Thus

$$\overline{z^{N'} H} = \sum_i \lambda_i \overline{z^r A_i}$$

$$\overline{H} = \overline{(z^{N'} H)_*} = \sum_i \lambda_i \overline{A_i}_* r$$

Finally, we have to show they are linearly independent :
Assume $\sum_i \lambda_i \overline{A}_{i,*} = 0 \iff \sum_i \lambda_i A_{i,*} = AF_* + BG_*$.
Then, homogenizing gives

$$z^a \sum_i \lambda_i A_i = z^b A^* F + z^c B^* G$$

Thus, $\sum_i \lambda_i \overline{z^a A_i} = 0$ *in* Γ_{d+a} *and thus, by the second claim,* $\lambda_i = 0$. □

5.2 Applications to Incidence Geometry

Theorème 93 (Cayley-Bacharch)
Let F_1, F_2 *be two projective cubics intersecting in* 9 *different points* $A_1, \ldots, A_9 \in \mathbb{P}^2$.
If G *is another cubic such that* $A_1, \ldots, A_8 \in G$, *then* G *is a linear combination of* F_1, F_2.

Preuve

1. *No 4 points of $F_1 \cap F_2$ are colinear, otherwise, this line L containing these points would be a component of F_1 and F_2.*
2. *By the same argument, no seven points lie on a quadric.*
3. *Any 5 points in $F_1 \cap F_2$ define a unique quadric.*
   Existence :
   A genenral quadric Q in $\mathbb{P}^2$ has the following form

   $$a_1X^2 + a_2Y^2 + \ldots + a_6XZ$$

   The 5 points will give 5 linear conditions for $a_1, \ldots, a_6$, thus there exists anon trivial solution.
   Uniqueness :
   Assume Q_1, Q_2 are two quadrics containing the 5 points, then they share a component, thus they must share a line L_1 (otherwise $Q_1 = Q_2$).
   By the first part, this line contains at most 3 of the 5 points.
   Let L_2 be the line passing through the other two, then $\frac{Q_1}{L_1} = L_2 = \frac{Q_2}{L_1} \implies Q_1 = Q_2$
4. *No 3 points in $A_1, \ldots, A_8$ are colinear :*
   Assume A_1, A_2, A_3 lie on a line L, then $A_4, \ldots, A_8$ don't lie on L (using the first part) and $\exists!$ quadric Q passing through $A_4, \ldots, A_8$.
   Let $B \in L \setminus \{A_1, A_2, A_3\}$ and $C \in \mathbb{P}^2 \setminus \{L, Q\}$.
   By linear algebra $\exists \alpha, \beta, \gamma \in K$ not all 0 such that

   $$H \coloneqq \alpha F_1 + \beta F_2 + \gamma G$$

   vanishes on B and C and $H \neq 0$ (otherwise we're done).
   Then H vanishes on A_1, A_2, A_3, B, thus $L|H$ and the quadric $\frac{H}{L}$ vanishes on $A_4, \ldots, A_8$.
   Using 3, $\frac{H}{L} = Q \implies H = LQ$ but $L(C)Q(C) \neq 0$
5. *No 6 points on $\{A_1, \ldots, A_8\}$ lie on a quadric (Exercise)*
6. *Finally, let L be the line through A_1, A_2 and Q the unique quadric through $A_3, \ldots, A_7$.*
   Pick $B, C \in L \setminus \{A_1, A_2\}$ and let $H = \alpha F_1 + \beta F_2 + \gamma G$ such that $B, C \in H$ and assume $H \neq 0$.
   Then $A_1, A_2, B, C \in L \cap H \implies L|H$ and $A_3, \ldots, A_7 \in \frac{H}{L}$, thus $\frac{H}{L} = Q$.
   However $A_8 \notin QL = H$, thus $H = 0$ □

Corollaire 94 (Pappus theorem)
Let $L_1, L_2 \in \mathbb{P}^2$ be two distinct lines. Let $A_1, A_2, A_3 \in L_2 \setminus L_2$ and $B_1, B_2, B_3 \in L_2 \setminus L_1$.
Let c_{ij} be the intersection of the lines $\overline{A_iB_j}$ and $\overline{A_jB_i}$ for $ij = 12, 23, 31$, then C_{12}, C_{23}, C_{31} are colinear.

Preuve
Let G the line through C_{12}, C_{23} with $|F_1 \cap F_2| = 9$.
As G contains 8 of them, $C_{31} \in G$.
However $C_{31} \notin L_1L_2 \implies C_{31} \in \overline{C_{12}C_{23}}$. □

Remarque
Typically this theorem is stated in $\mathbb{R}^2$, but we may just consider the equations of the real lines in $\mathbb{C}^2$, homogenize and then apply the actual corolarry.

5.3 Elliptic Curves

We have seen in an exercise that $F \subset \mathbb{P}^2$ of degree 2 and irreducible is isomorphic to $\mathbb{P}^1$.
Elliptic curvesare the next "simplest" case, ie. $\deg F = 3$.

Definition 43 (Elliptic Curve)
An elliptic curve $(E, 0)$ is a non-singular cubic $E \subset \mathbb{P}^2$ together with a point $0 \in E$.
$(E, 0)$ comes with a commutative group structure.

Define a map $\phi : E \times E \to E$ by $\phi(A, B) \in E$ is the unique third intersection point of the line $\overline{AB}$ with E if $A \neq B$.
Or of the tangent of A with E if $A = B$.
Finally, we define $A + B = \phi(0, \phi(A, B))$

Lecture 13: Elliptic Curves

Fri 03 Jun

Theorème 96
$(E, 0, +)$ is a commutative group.

Preuve
We saw that 0 is a neutral element in the exercises and that $\forall A \in E$, $-A \coloneqq \phi(A, \phi(0, 0))$ is an additive inverse.
So it suffices to show associativity. We want to show that $(P + Q) + R = P + (Q + R)$, let $S' = \phi(P, q), S = P + Q, U' = \phi(Q, R), Q + R = U$.
We want to show that $S + R = P + U$, it is sufficient to show that $\phi(S, R) =$

$\phi(P,U)$.
Assume that none of the points are the same.
Let F be the product of $\overline{QP}, \overline{U,U'}, \overline{RS}$ and G the product of $\overline{QR}, \overline{SS'}, \overline{PU}$.
$F \cap E$ intersect in 9 different points and G contains 8 of them (all but $\phi(P,U)$ a priori).
By Cayley-Bacharach, G also contains $\phi(P,U) \in G$ but $|G \cap E| = 9$. □

(Up to here for exam)

Lemme 97
Any elliptic curve is isomorphic to a curve with equation

$$Y^2Z - X^3 - aXZ^2 - bZ^3$$

where $a, b \in K$ such that $4a^3 + 27b^2 \neq 0$

Preuve (Sketch)
To get the equation, one has to do a series of coordinate changes.
The condition $4a^3 + 27b^2 \neq 0$ is equivalent to the curve being non-singular.
Note that 0 is the only point of the curve at ∞ and it is a simple point.
If $z = 1$, we get $Y^2 - X^3 - aX - b$.
Taking the derivatives, we get $\frac{\partial E}{\partial Y} = 2Y$ and $\frac{\partial E}{\partial X} = 3X^2 - a$.
Thus, $Y = 0$ implies $X^3 + aX + b = 0$ and $3X^2 - a$. solving this gives the criteria. □

If we add the point 0, we get something compact.
Topologically, all elliptic curves are Tori, ie. $E \simeq S^1 \times S^1$.
The fact that E has a group structure is reflected by the fact that $S^1 \times S^1$ has many automorphisms.
If $\deg(F) > 3$, $F(\mathbb{C})$ is a torus with many holes, which has few automorphisms and so putting a group structure on it is difficult.
The fact that elliptic curves have a group structure is useful :

Lenstra's Algorithm for integer factorization

Given $n \in \mathbb{Z}$, is it prime ? If not, find the factorization.
The basic idea is to compute $\gcd(a, n)$ for a variying in some finite subset of $\mathbb{Z}$

Pollard's $(p-1)$-method

Choose $a \in {}^{\mathbb{Z}}\!/_{n\mathbb{Z}}$ random and fix $k \in \mathbb{N}$ with many small prime factors.
Then, compute $a^k \mod (n)$ and $\gcd(a^k = 1, n)$.
This works well if n has a prime divisor p such that $p-1$ is a product of small primes and $p-1|k$.
If further $p \not| a$ then by Fermat $p|a^k - 1 \implies p|\gcd(a^k - 1, n)$.

If we believe that everything we learned about elliptic curves over an algebraically closed field K can be extended to $\mathbb{Z}/n\mathbb{Z}$, we can describe Lenstra's algorithm.
Choose a random elliptic curve over $\mathbb{Z}/n\mathbb{Z}$ i.e. an equation of the form $Y^2Z - X^3 - aZ^2 - bZ^3$.
Choose K with many small prime divisors and a random point $e \in E$ satisfying the Weierstrass equation.
Now compute $Ke = e + \ldots + e$ k-times and then $\gcd(n, z - \text{ coordinate })$.
If this gcd is > 1 we're done.
Why does this work ?
If n has a prime divisor p s.t. $|E(\mathbb{Z}/p\mathbb{Z})||K$ then $Ke = 0$ in $\mathbb{Z}/p\mathbb{Z}$.

Remarque (Weil bound)
$p + 1 - 2\sqrt{p}|E(\mathbb{Z}/p\mathbb{Z})| \leq p + 1 + 2\sqrt{p}$