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

$$0 \to I_p \to R_p \to (R/I)_p \to 0$$

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 $\mathbb{A}_k^n$ 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

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

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, $J \subset k[X_1, \ldots, X_n]$, then

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

Using this, there is a one to one correspondence

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

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

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

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

Preuve
Let $I \subset k[X_1, \ldots, X_n]$ be any ideal and $P_1, \ldots, P_n \subset V(I)$ distinct.
We can choose (Exercise) $F_1, \ldots, F_r \in K[X_1, \ldots, X_n]$ s.t. $F_i(P_j) = \delta_{ij}$, then we write $f_1, \ldots, f_r$ for the residues of $F_1, \ldots, F_r$ in $K[X_1, \ldots, X_n] / I$.
We claim $f_1, \ldots, f_r$ 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 $\dim_k K[X_1, \ldots, X_n] / I < \infty \implies |V(I)| < \infty$ and in this case $\dim_k K[X_1, \ldots, X_n] / I \geq |V(I)|$.
Now assume $V(I)$ is a finite set $\{P_1, \ldots, P_r\} \subset \mathbb{A}^n$ and write $P_i = (a_{i1}, \ldots, a_{in})$ 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 $K[X_1, \ldots, X_n] / I$, but $f_j^N = (x_j^{Nr}) +$ lower order terms .
This means that X_j^{Nr} is a K-linear combination of $\{1, \ldots, X_j^{Nr-1}\}$.
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 $\{x_1^{m_1}, \ldots, x_n^{m_n}\}$ generates $K[X_1, \ldots, X_n] / I$ □

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 $V = \{x_1, \ldots, x_n\} \subset \mathbb{A}^n$ 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* $F_1 F_2 = I(W_1) \cap I(W_2) = I(V)$. $\square$

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

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

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

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

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

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

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

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

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 $\phi \circ \psi = \mathrm{Id}$ and $\psi \circ \phi = \mathrm{Id}$.

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.*