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

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

Lemme 10

1. *If $X \subset Y$ then $I(X) \supset I(Y)$*
2. *For $J \subset k[X_1, \dots, X_N]$ 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. $I(V(J)) = \{f \in k[x_1, \dots, x_n] | f(x) = 0 \forall x \in V(J)\} \supset J$
3. *By definition $V(I(X)) \supset X$ for any X.*
   If in addition, if $X = V(J)$ algebraic, then $V(I(X)) = V((I(V(J)))) \subset V(J) = X$ $\square$

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 $f(x) = 0$ $\square$

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

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

Preuve

Let $I \subset k[X_1,\dots,X_n]$ *be any ideal and* $P_1,\dots,P_n \subset V(I)$ *distinct.*

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* ${K[X_1,\dots,X_n]}\big/{I}$.

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 $\dim_k {K[X_1,\dots,X_n]}\big/{I} < \infty \implies |V(I)| < \infty$ *and in this case* $\dim_k {K[X_1,\dots,X_n]}\big/{I} \geq |V(I)|$.

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* ${K[X_1,\dots,X_n]}\big/{I}$, *but* $f_j^N = (x_j^{Nr}) +$ *lower order terms .*

This means that X_j^{Nr} *is a* K*-linear combination of* $\left\{1,\dots,X_j^{Nr-1}\right\}$.

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* ${K[X_1,\dots,X_n]}\big/{I}$ $\square$

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