Courbes algébriques

Alexandre Guillemot

20 septembre 2022

Table des matières

Introduction

ana-maria.castravet@uvsq.fr k un corps, on considère $P_1, \cdots, P_r \in k[x_1, \cdots, x_n]$. $V(P_1, \cdots, P_r) \subseteq \mathbb{A}_k^n$ sont les zéros de $P_1, \cdots, P_r$. Courbe algébrique = variété algébrique de dimension 1. Les courbes elliptiques sont des cas particuliers de courbes algébriques.

Chapitre 1

Ensembles algébriques affines

1.1 Définition

k un corps, $n \in \mathbb{Z}$.

Définition 1.1.1. (Espace affine) $\mathbb{A}_k^n := k^n$ est l'espace affine sur le corps k de dimension n.

Rq 1.1.1. Ce n'est pas vraiment la définition de l'espace affine, c'est la définition de l'ensemble sous-jacent à l'espace affine, sachant que les espaces affines sont des variétés algébriques.

Ex 1.1.1. Si $n = 1$, c'est une "droite". Si $n = 2$, c'est un "plan".

Définition 1.1.2. Soit $S \subseteq k[x_1, \cdots, x_n]$, on définit

$$V(S) := \{a \in \mathbb{A}_k^n \mid \forall P \in S,\, P(a) = 0\}$$

On appelle de tels ensembles des ensembles algébriques affines.

Rq 1.1.2. Si $S = \{P_1, \cdots, P_r\}$, on écrit $V(P_1, \cdots, P_r) := V(S)$.

Ex 1.1.2.

1. $V(\emptyset) = \mathbb{A}_k^n$
2. $V(1) = \emptyset$
3. $P = X^4 - 1 \in k[X]$, si $k = \mathbb{R}$, $V(P) = \{1, -1\}$. Si $k = \mathbb{C}$, $V(P) = \{1, -1, i, -i\}$. Si $k = \mathbb{F}_2$, $V(P) = \{1\}$.
4. $P = X^2 + Y^2 + 1 \in k[X, Y]$, si $k = \mathbb{R}$, $V(P) = \emptyset$. Si $k = \mathbb{C}$, $V(P)$ est isomorphe (en tant que variété algébrique, même si cela n'a pour le moment aucun sens) au cercle complexe (en considérant le changement de variables $a_j = ib_j$).

5. $P_i = \sum a_{ij}x_j - b_i \in k[x_1, \cdots, x_n]$, $i \in [\![1, r]\!]$.

$$V(P_i) = \{x \in k^n \mid (a_{ij})x = b\} \simeq \mathbb{A}_k^n \text{ ou } \emptyset$$

Exercice. Les ensembles algébriques de $\mathbb{A}_k^1$ sont : $\emptyset$, $\mathbb{A}_k^1$, tous les sous-ensembles finis.

Ex 1.1.3. Les sous-ensembles algébriques de $\mathbb{A}_k^2$ sont $\emptyset$, tout le plan, les sous-ensembles finis et des réunions finies des sous-ensembles finis avec des courbes planes, i.e. $V(P) \neq \emptyset$ les zéros d'un seul polynôme non constant. Donnons des exemples de courbes planes :

1. Les droites $V(ax + by + c) \in \mathbb{A}_k^2$, avec $a \neq 0$ ou $b \neq 0$.
2. Les coniques $V(ax^2 + by^2 + cxy + dx + ey + f) \subseteq \mathbb{A}_k^2$ ($a \neq 0$ ou $b \neq 0$ ou $c \neq 0$). Dans $\mathbb{P}_{\mathbb{C}}^2$, toutes les coniques sont de type cercle, droite ou droites qui se croisent.
3. $y^2 = x^3 + ax + b$, $a, b \in k$ définissent ce qu'on appelle des courbes elliptiques.

Rq 1.1.3. $V(S) = V(T)$ n'implique pas que $S = T$. Par exemple $V(x^2+y^2+1) = V(x^4+1) \subseteq \mathbb{A}_{\mathbb{R}}^2$. Plus généralement, sur n'importe quel corps, $V(P^2) = V(P)$ avec $P = k[x_1, \cdots, x_n]$.

Proposition 1.1.1. *1. Si $S \subseteq T \subseteq k[x_1, \cdots, x_n]$, alors $V(T) \subseteq V(S) \subseteq \mathbb{A}_k^n$.*

2. $S \subseteq k[x_1, \cdots, x_n]$, $I = (S)$ idéal engendré par S, alors $V(S) = V(I)$

3. $S \subseteq k[x_1, \cdots, x_n]$, alors

$$V(S) = \bigcap_{p \in S} V(P)$$

4.

$$\bigcap_{j \in J} V(S_j) = V\left(\bigcup_{j \in J} S_j\right),\ S_j \subseteq k[x_1, \cdots, x_n]$$

5. $V(PQ) = V(P) \cup V(Q)$ pour $P, Q \in k[x_1, \cdots, x_n]$

6. Plus généralement, $V(IJ) = V(I) \cup V(J) = V(I \cap J)$ avec $I, J \overset{\text{id}}{\subseteq} k[x_1, \cdots, x_n]$

Démonstration. Prouvons 6 : $IJ \subseteq I \cap J \subseteq I$ donc $V(I) \subseteq V(I \cap J) \subseteq V(IJ)$ et donc par symétrie $V(I) \cup V(J) \subseteq V(I \cap J) \subseteq V(IJ)$. Supposons qu'il existe $x \in V(IJ)$ tq $x \notin V(I) \cup V(J)$. Alors $\exists P \in I$, $Q \in J$ tq $P(x) \neq 0$ et $Q(x) \neq 0$. Mais $PQ \in IJ$ donc $PQ(x) = 0$, contradiction. Les autres points sont en exercice. □

Corollaire 1.1.1. *Les ensembles algébriques de $\mathbb{A}_k^n$ forment les fermés d'une topologie. On appelera cette topologie la topologie de Zariski.*

Définition 1.1.3. Soit $E \subseteq \mathbb{A}_k^n$. On définit

$$I(E) = \{P \in k[x_1, \cdots, x_n] \mid P(a) = 0, \forall a \in E\}$$

Ex 1.1.4.
1. $I(\emptyset) = k[x_1, \cdots, x_n]$
2. $I(a) = (x_1 - a_1, \cdots, x_n - a_n) =: \mathfrak{m}_a$. Remarquons que cet idéal est un idéal maximal.
3. $I(\mathbb{A}_k^n) = \{0\}$ si le corps est infini.

Définition 1.1.4. $I \overset{\text{id}}{\subseteq} A$, alors

$$\sqrt{I} = \{f \in A \mid \exists n > 0,\ f^n \in I\}$$

est le radical de I. I est un idéal radical si $I = \sqrt{I}$

Proposition 1.1.2.
1. *$E \subseteq E' \subseteq \mathbb{A}_k^n$, alors $I(E') \subseteq I(E)$*
2. *$I(E \cup E') = I(E) \cap I(E')$*
3. *$J \subseteq I(V(J))$ pour tout $J \overset{\text{id}}{\subseteq} k[x_1, \cdots, x_n]$.*
4. *$E \subseteq V(I(E))$ pour tout $E \subseteq \mathbb{A}_k^n$.*
5. *$V(I) = V(\sqrt{I}) \subseteq \mathbb{A}_k^n$, pour tout $I \overset{\text{id}}{\subseteq} k[x_1, \cdots, x_n]$*

Démonstration. Exercice □

Lemme 1.1.1. *$E = V(I(E)) \iff E$ est un ensemble algébrique.*

Démonstration. Montrons $V(I(E)) \subseteq E$: Supposons que $E = V(J)$, $J \overset{\text{id}}{\subseteq} k[x_1, \cdots, x_n]$. ALors $J \subseteq I(V(J))$ et ainsi $V(I(E)) \subseteq E$. □

Ex 1.1.5. Le segment ouvert $(0, 1) \subseteq \mathbb{A}_{\mathbb{R}}^1$ n'est pas un ensemble algébrique.

Théorème 1.1.1. *(Nullstellensatz, 1) Si $k = \bar{k}$, alors on a $I(V(J)) = \sqrt{J}$ pour tout $J \overset{\text{id}}{\subseteq} k[x_1, \cdots, x_n]$*

Ex 1.1.6. Si $k = \mathbb{R}$, $P = x^2 + y^2 + 1 \in \mathbb{R}[x, y]$ irréductible. $I = (P)$ est un idéal premier, donc radical, mais $I(V(P)) = I(\emptyset) = \mathbb{R}[x, y] \neq (P)$.

Théorème 1.1.2. *Pour tout $n \geq 1$, $k[x_1, \cdots, x_n]$ est un anneau noéthérien.*

Corollaire 1.1.2. *Chaque ensemble algébrique $V \subseteq \mathbb{A}_k^n$ est de la forme $V = V(P_1, \cdots, P_r)$ avec $P_i \in k[x_1, \cdots, x_n]$*

Ainsi V et I nous donnent des applications entre les idéaux radicaux de $k[x_1, \cdots, x_n]$ et les sous espaces algébriques de $\mathbb{A}_k^n$. Vérifier que $I(E)$ est un idéal radical. De plus, si k est algébriquement clos, d'après le nullstellensatz I et V sont inverses l'une de l'autre. Par cette bijection, les idéaux premiers vont correspondre aux ensembles irréductibles. Les idéaux maximaux vont correspondre à des points.

Définition 1.1.5. $V \subseteq \mathbb{A}_k^n$ ensemble algébrique. V est irréductible si pour toute décomposition $V = V_1 \cup V_2$ avec V_1, V_2 ensembles algébriques, on a $V = V_1$ ou $V = V_2$. On dit sinon que V est réductible.

Proposition 1.1.3. *$V \subseteq \mathbb{A}_k^n$ ensemble algébrique. Alors tfae*

1. *V est irréductible*
2. *$I(V)$ est un idéal premier*
3. *$k[x_1, \cdots, x_n]/I(V)$ est un anneau intègre*

Démonstration. $1 \Rightarrow 2$: Soient $f, g \in k[x_1, \cdots, x_n]$ tq $fg \in I(V)$. Mais $V(fg) = V(f) \cup V(g)$, puis soit $V_1 V \cap V(f)$, $V_2 = V \cap V(g)$, alors $V_1 \cup V_2 = V \cap V(fg) = V$. Ainsi $V_1 = V$ ou $V_2 = V$, donc $f \in V$ ou $g \in V$.
$2 \Rightarrow 1$: Soit $V \subseteq \mathbb{A}_k^n$ ensemble algébrique tq $I(V)$ est un idéal premier. Supposons que V est réductible, alors $V = V_1 \cup V_2$ avec $V \neq V_1, V \neq V_2$. Comme V_1, V_2 sont algébriques, alors $V(I(V)) = V$, $V(I(V_i)) = V_i$, et ainsi $V(I(V)) \neq V(I(V_1))$ et $I(V) \subseteq I(V_1)$. Donc il existe $f_1 \in I(V_1)$ tq $f \notin I(V)$. De même, il existe $f_2 \in I(V_2)$ tq $f_2 \notin I(V)$. Mais $f_1 f_2 \in I(V_1) \cap I(V_2) = I(V)$ et ainsi $I(V)$ n'est pas premier. □

Théorème 1.1.3. *Soit $V \subseteq \mathbb{A}_k^n$ un ensemble algébrique. Alors $\exists V_1, \cdots, V_m \subseteq \mathbb{A}_k^n$ irréductibles tels que*

1. *$V = V_1 \cup V_2 \cup \cdots \cup V_m$*
2. *$\forall i \neq j$, $V_i \not\subseteq V_j$*

Les $\{V_i\}_{i \in [\![1,m]\!]}$ avec ces propriétés sont uniques à ordre près, on les appelle les composantes irréductibles de V.

Ex 1.1.7. Soit $V := V(xy, (x-1)z) \subseteq \mathbb{A}^n_k$, k de caractéristique 0. Sur V, on a

$$\begin{aligned}&(x = 0 \vee z = 0) \wedge (x = 1 \vee y = 0)\\ \iff &(x = 0 \wedge y = 0) \vee (z = 0 \wedge x = 1) \vee (z = 0 \wedge y = 0)\end{aligned}$$

Ainsi $V = V_1 \cup V_2 \cup V_3$ avec $V_1 = V(x, y)$, $V_2 = V(x-1, z)$ et $V_3 = V(y, z)$. On peut alors prouver que ce sont les composantes irréductibles de V.

Démonstration. Soit $V \subseteq \mathbb{A}^n_k$ un ensemble algébrique. Si V est irréductible, on a terminé. Sinon il existe des sous-ensembles algébriques propres de $V_1, V_2 \nsubseteq V$ tels que $V = V_1 \cup V_2$. Si V_1, V_2 sont irréductibles, alors on a finit. Sinon on itère le procédé sur V_1 et V_2. Alors supposons que le procédé ne termine pas, il va exister une suite strictement décroissante $\cdots \nsubseteq W_2 \nsubseteq W_1 \nsubseteq V$ d'ensembles algébriques. Ainsi on obtiens une suite croissante

$$I(W) \subseteq I(W_1) \subseteq I(W_2) \subseteq \cdots$$

Remarquons alors qu'elle es strictement croissante puisque $V(I(W_i)) = W_i$ et la suite des W_i est strictement décroissante. Ainsi on obtiens une contradiction avec le fait que $k[x_1, \cdots, x_n]$ est noéthérien.
Occupons nous maintenant de l'unicité : Supposons que

$$V = \bigcup_{i=1}^{s} V_i = \bigcup_{i=1}^{t} W_i$$

On veut montrer que l'ensemble $\{V_i\}_{i\in[\![1,s]\!]}$ est égal à l'ensemble $\{W_i\}_{i\in[\![1,t]\!]}$. On va montrer une inclusion : montrons qu'il existe $j \in [\![1, t]\!]$ tel que $V_i = W_j$, avec $i \in [\![1, s]\!]$. Comme $V_i \subseteq \bigcup_{j\in[\![1,t]\!]} W_j$, on a

$$V_i \subseteq \bigcup_{j\in[\![1,t]\!]} W_j \cap V_i$$

Mais V_i est irréductible, donc $\exists j \in [\![1, t]\!]$ tel que $V_i = W_j \cap V_j$, et en particulier $V_i \subseteq W_j$. Maintenant de la même manière on peut prouver qu'il existe $i' \in [\![1, s]\!]$ tel que $W_i \subseteq V_{i'}$. Mais alors $V_i \subseteq W_j \subseteq V_{i'}$ et donc $i = i'$, d'où $V_i = W_j$. □

Donnons 2 reformulations du Nullstellensatz

Proposition 1.1.4. *(Nullstellensatz 2,3) Considérons l'anneau $k[x_1, \cdots, x_n]$. Tfae :*

1. *Pour tout $J \overset{\text{id}}{\subseteq} k[x_1, \cdots, x_n]$, $I(V(J)) = \sqrt{J}$*
2. *Pour tout $J \overset{\text{id}}{\subseteq} k[x_1, \cdots, x_n]$, J propre implique que $V(J) \neq \emptyset$*

3. Les idéaux maximaux de $k[x_1, \cdots, x_n]$ sont exactement les idéaux

$$\mathfrak{m}_a = (x_1 - a_1, \cdots, x_n - a_n)$$

Démonstration. $2 \Rightarrow 3$: Soit $\mathfrak{m} \overset{\max}{\subseteq} k[x_1, \cdots, x_n]$. C'est un idéal propre, donc $V(\mathfrak{m}) \neq \emptyset$. Alors soit $a \in V(\mathfrak{m})$, remarquons que pour tout $f \in \mathfrak{m}$, $f(a) = 0$ donc $f \in \mathfrak{m}_a$ (vu que l'on peut écrire $f = Q_1(x_1 - a_1) + \cdots + Q_i(x_i - a_i) + c$). Ainsi $\mathfrak{m} \subseteq \mathfrak{m}_a$ mais $\mathfrak{m}$ est maximal donc $\mathfrak{m} = \mathfrak{m}_a$ ce qui prouve simultanément que $(x_1 - a_1, \cdots, x_n - a_n)$ est un idéal maximal et que $\mathfrak{m}$ est cet idéal.
$1 \Rightarrow 2$: Soit $J \overset{\text{id}}{\subseteq} k[x_1, \cdots, x_n]$ idéal propre. On a $\sqrt{J} = I(V(J))$. Supposons que $V(J) = \emptyset$, alors $\sqrt{J} = I(V(J)) = k[x_1, \cdots, x_n]$ et donc $J = k[x_1, \cdots, x_n]$, contradiction.
$3 \Rightarrow 1$: Soit $I \overset{\text{id}}{\subseteq} k[x_1, \cdots, x_n]$, on veut mq $\sqrt{I} = I(V(I))$. Comme $I \subseteq I(V(I))$, on a directement le première inclusion du fait que $\sqrt{I(V(I))} = I(V(I))$. Dans l'autre sens, si $I = k[x_1, \cdots, x_n]$, l'égalité est claire. Sinon soit $f \in I(V(I))$, écrivons $I = (P_1, \cdots, P_r)$. Maintenant considérons l'anneau $k[x_1, \cdots, x_n, x_{n+1}]$, puis l'idéal

$$(P_1, \cdots, P_r, 1 - x_{n+1}f) =: J \overset{\text{id}}{\subseteq} k[x_1, \cdots, x_{n+1}]$$

Si J est un idéal propre, alors d'après le théorème de Krull il existe $\mathfrak{m} \overset{\max}{\subseteq} k[x_1, \cdots, x_{n+1}]$ tel que $J \subseteq \mathfrak{m}$. Maintenant par hypothèse il existe $(a_1, \cdots, a_n, b) \in \mathbb{A}_k^{n+1}$ tel que

$$\mathfrak{m} = (x_1 - a_1, \cdots, x_n - a_n, x_{n+1} - b)$$

Mais alors pour tout $i \in [\![1, r]\!]$, $P_i(a) = 0$ et $1 - bf(a) = 0$. Mais alors la première série d'égalités nous indique que $a \in V(I)$, et comme $f \in I(V(I))$, $f(a) = 0$, ce qui est absurde. Ainsi J est $k[x_1, \cdots, x_{n+1}]$ tout entier, donc en particulier il existe $Q_1, \cdots, Q_n, Q \in k[x_1, \cdots, x_{n+1}]$ tels que

$$1 = P_1Q_1 + \cdots + P_rQ_r + Q(1 + x_{n+1}f) \tag{1.1}$$

Maintenant le morphisme de localisation $k[x_1, \cdots, x_n] \to k[x_1, \cdots, x_n, 1/f]$ et le choix de l'élément $1/f$ induit un morphisme d'évaluation

$$\begin{array}{ccccc} k[x_1, \cdots, x_n] & \longrightarrow & k[x_1, \cdots, x_n, 1/f] & \hookrightarrow & k(x_1, \cdots, x_n) \\ \downarrow & \nearrow_{\exists!} & & & \\ k[x_1, \cdots, x_n][x_{n+1}] & & & & \end{array}$$

Ainsi au travers de ce morphisme l'égalité 1.1 deviens

$$1 = P_1(x_1, \cdots, x_n)Q_1(x_1, \cdots, x_n, 1/f) + \cdots + P_r(x_1, \cdots, x_n)Q_r(x_1, \cdots, x_n, 1/f)$$

Alors écrivons les Q_i comme des éléments de $k[x_1, \cdots, x_n][x_{n+1}]$,

$$Q_i = \sum_{l=0}^{d_i} R_{i,l}(x_1, \cdots, x_n) x_{n+1}^l$$

En les passant au travers du morphisme d'évaluation précédent on peut les réécrire

$$Q_i = \frac{R_i(x_1, \cdots, x_n)}{f^{d_i}}$$

et alors 1.1 deviens

$$1 = \sum_{i=1}^{r} \frac{P_i R_i}{f^{d_i}}$$

et ainsi en notant $d = \max\{d_i\}$

$$f^d = \sum_{i=1}^{r} P_i R_i f^{d-d_i}$$

dans $k(x_1, \cdots, x_n)$ donc dans $k[x_1, \cdots, x_n]$. Finalement si $d = 0$, alors $1 \in I$ absurde puisque l'on avait supposé I propre. Sinon, $f^d \in I$ et donc $f \in \sqrt{I}$. □