

Courbes algébriques

Alexandre Guillemot

27 novembre 2022

Table des matières

1	Ensembles algébriques affines	3
1.1	Définition	3
1.2	Topologie de Zariski	4
1.3	Nullstellensatz de Hilbert	5
1.4	Sous-ensembles irréductibles	10
2	Catégorie des ensembles algébriques et foncteur $k[-]$	13
2.1	Catégorie des ensembles algébriques sur k	13
2.2	Foncteur $k[-]$	15
2.3	Cas des corps algébriquement clos	18
3	Dimension, espace tangent	19
3.1	Topologie induite sur les ensembles algébriques	19
3.2	Variétés affines, dimension	20
3.2.1	Dimension d'une variété affine	20
3.2.2	Dimension de krull	23
3.3	Singularités	24
3.4	Espace tangent	25
3.4.1	Anneau des fonctions régulières en un point	25
3.4.2	Anneaux locaux	26
3.4.3	Espace tangent de Zariski	28
3.4.4	Espace tangent géométrique	28
4	Courbes algébriques affines	33
4.1	Rappels d'algèbre commutative	33
4.2	Régularité des courbes algébriques	34
5	Géométrie projective	37
5.1	Ensembles algébriques projectifs	37
5.2	Topologie de Zariski sur \mathbb{P}^n et ses sous-ensembles algébriques projectifs . . .	39
5.3	Lien entre géométrie affine et géométrie projective	41

5.3.1	Ensembles quasi-projectifs	41
5.3.2	Variétés	44
5.4	Courbes projectives	46
5.4.1	Définition, première propriétés	46
5.4.2	Pôles et zéros	48
5.4.3	Diviseurs sur une courbe	49
A		57
A.1	Localisation d'un anneau	57
A.2	Théorie des corps	57

Introduction

ana-maria.castravet@uvsq.fr k un corps, on considère $P_1, \dots, P_r \in k[x_1, \dots, x_n]$. $V(P_1, \dots, P_r) \subseteq \mathbb{A}_k^n$ sont les zéros de P_1, \dots, 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.

lorsque $n = 1$, on parlera de droite affine. Lorsque $n = 2$, on parlera de plan affine.

|| **Définition 1.1.2.** Soit $S \subseteq k[X_1, \dots, X_n]$, 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 $S = \{P_1, \dots, P_r\}$, on écrit $V(P_1, \dots, P_r) := V(S)$.

Ex 1.1.1. 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. $P_i = \sum a_{ij}X_j - b_i \in k[X_1, \dots, X_n]$, $i \in \llbracket 1, r \rrbracket$.

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

pour un certain $0 \leq m \leq n$.

Exercice. Les ensembles algébriques de \mathbb{A}_k^1 sont : \emptyset , \mathbb{A}_k^1 , tous les sous-ensembles finis (cf Td1 Exercice 1).

Ex 1.1.2. 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 $P = k[X_1, \dots, X_n]$.

|| **Théorème 1.1.1.** (Théorème de la base de Hilbert) Pour tout $n \geq 1$, $k[X_1, \dots, X_n]$ est un anneau noethérien.

Rq 1.1.4. Pour tout $S \subseteq k[X_1, \dots, X_n]$, on a $V(S) = V((S))$. Ainsi tout ensemble algébrique peut s'écrire $V(I)$ avec $I \subseteq k[X_1, \dots, X_n]$.

La remarque précédente combinée au théorème de la base de Hilbert nous permet de donner le corollaire suivant :

|| **Corollaire 1.1.1.** Chaque ensemble algébrique $V \subseteq \mathbb{A}_k^n$ est de la forme $V = V(P_1, \dots, P_r)$ avec $P_i \in k[X_1, \dots, X_n]$

1.2 Topologie de Zariski

|| **Proposition 1.2.1.** 1. Si $S \subseteq T \subseteq k[X_1, \dots, X_n]$, alors $V(T) \subseteq V(S) \subseteq \mathbb{A}_k^n$.
2. $S \subseteq k[X_1, \dots, X_n]$, alors

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

3.

$$\bigcap_{j \in J} V(S_j) = V \left(\bigcup_{j \in J} S_j \right), \quad S_j \subseteq k[X_1, \dots, X_n]$$

 4. $V(PQ) = V(P) \cup V(Q)$ pour $P, Q \in k[X_1, \dots, X_n]$

 5. Plus généralement, $V(IJ) = V(I) \cup V(J) = V(I \cap J)$ avec $I, J \stackrel{\text{id}}{\subseteq} k[X_1, \dots, X_n]$

Démonstration. 1. Soit $x \in V(T)$. Alors soit $P \in S$, $P \in T$ comme $S \subseteq T$ et donc $P(x) = 0$, d'où $x \in V(S)$.

2. Pour tout $P \in S$, $V(S) \subseteq V(P)$ d'après (1). Ainsi $V(S) \subseteq \bigcap_{P \in S} V(P)$. Réciproquement, si $x \in \bigcap_{P \in S} V(P)$, alors $P(x) = 0$ pour tout $P \in S$ et ainsi $x \in V(S)$.

3. $S_i \subseteq \bigcup_{j \in J} S_j$, \supseteq est claire. Maintenant soit $x \in \bigcap_{j \in J} V(S_j)$, soit $P \in \bigcup_{j \in J} S_j$, il existe $j \in J$ tel que $P \in S_j$. Mais en particulier $x \in V(S_j)$, et donc $P(x) = 0$, ce qui prouve \subseteq .

4. D'après (1), $V(P), V(Q) \subseteq V(PQ)$ et ainsi $V(P) \cup V(Q) \subseteq V(PQ)$. Réciproquement, si $x \in V(PQ)$, alors $PQ(x) = 0$ et ainsi $P(x) = 0$ ou $Q(x) = 0$ par intégrité de k , et donc $x \in V(P) \cup V(Q)$.

$IJ \subseteq I \cap J \subseteq I$ 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.

□

Corollaire 1.2.1. Les ensembles algébriques de \mathbb{A}_k^n forment les fermés d'une topologie. On appelle cette topologie la topologie de Zariski.

1.3 Nullstellensatz de Hilbert

Définition 1.3.1. Soit $E \subseteq \mathbb{A}_k^n$. On définit

$$I(E) = \{P \in k[X_1, \dots, X_n] \mid P(a) = 0, \forall a \in E\}$$

Ex 1.3.1. 1. $I(\emptyset) = k[X_1, \dots, X_n]$

2. $I(a) = (X_1 - a_1, \dots, X_n - a_n) =: \mathfrak{m}_a$. Cet idéal est maximal, vu que c'est le noyau de l'application surjective

$$\begin{aligned} \text{ev}_a : k[X_1, \dots, X_n] &\rightarrow k \\ X_i &\mapsto a_i \end{aligned}$$

et donc $k[X_1, \dots, X_n]/\mathfrak{m}_a \simeq k$.

3. $I(\mathbb{A}_k^n) = \{0\}$ si le corps est infini.

Définition 1.3.2. $I \subseteq A$, 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 1.3.1. 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 $J \subseteq k[X_1, \dots, X_n]$.

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 $I \subseteq k[X_1, \dots, X_n]$

6. $I(V) = \sqrt{I(V)}$, pour tout $V \subseteq \mathbb{A}_k^n$ ensemble algébrique affine.

Démonstration. 1. Soit $P \in I(E')$. Alors pour tout $x \in E$, $x \in E'$ et donc $P(x) = 0$, ce qui prouve que $P \in I(E)$.

2. $E, E' \subseteq E \cup E'$, donc $I(E \cup E') \subseteq I(E), I(E')$ et donc $I(E \cup E') \subseteq I(E) \cap I(E')$. Réciproquement, soit $P \in I(E) \cap I(E')$, alors pour tout $x \in E \cup E'$, $x \in E$ ou $x \in E'$ et donc $P(x) = 0$.

3. Soit $P \in J$, alors pour tout $x \in V(J)$, $P(x) = 0$ et ainsi $P \in I(V(J))$.

4. Soit $x \in E$, alors pour tout $P \in I(E)$, $P(x) = 0$ et ainsi $x \in V(I(E))$.

5. Comme $I \subseteq \sqrt{I}$, $V(\sqrt{I}) \subseteq V(I)$. Maintenant soit $x \in V(I)$, alors pour tout $P \in \sqrt{I}$, il existe $n \geq 1$ tel que $P^n \in I$, et ainsi $P^n(x) = 0$. Mais par intégrité de k , $P(x) = 0$ et ainsi $x \in V(\sqrt{I})$.

6. On a toujours $I(V) \subseteq \sqrt{I(V)}$. Maintenant soit $P \in \sqrt{I(V)}$, alors $\exists n \geq 1$ tel que $P^n \in I(V)$. Ainsi, pour tout $x \in V$, $P^n(x) = 0$ et donc $P(x) = 0$ par intégrité de k . Finalement, $P \in I(V)$. □

Lemme 1.3.1. $E = V(I(E)) \iff E$ est un ensemble algébrique.

Démonstration. Il suffit de montrer que si E est un ensemble algébrique affine, alors $V(I(E)) \subseteq E$: supposons que $E = V(J)$, $J \subseteq k[X_1, \dots, X_n]$. Alors $J \subseteq I(V(J))$ et ainsi $V(I(E)) = V(I(V(J))) \subseteq V(J) = E$. □

Ex 1.3.2. Le segment $[0, 1] \subseteq \mathbb{A}_{\mathbb{R}}^1$ n'est pas un ensemble algébrique.

Fixons $k \in \mathbf{Fld}$, $n \geq 1$. Définissons deux applications :

$$\begin{array}{ccc} I : \{V \subseteq \mathbb{A}_k^n \text{ ensemble algébrique}\} & \xrightarrow{\text{id}} & \{I \subseteq k[X_1, \dots, X_n] \mid I = \sqrt{I}\} \\ V & \mapsto & I(V) \end{array}$$

Remarquons que cette application est bien définie d'après 1.3.1. De même, on définit

$$\begin{array}{ccc} V : \{I \subseteq k[X_1, \dots, X_n] \mid I = \sqrt{I}\} & \xrightarrow{\text{id}} & \{V \subseteq \mathbb{A}_k^n \text{ ensemble algébrique}\} \\ I & \mapsto & V(I) \end{array}$$

|| **Théorème 1.3.1.** (*Nullstellensatz, 1*) Si $k = \bar{k}$, alors on a $I(V(J)) = \sqrt{J}$ pour tout $J \subseteq k[X_1, \dots, X_n]$

Ex 1.3.3. 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 $I(V(P)) = I(\emptyset) = \mathbb{R}[X, Y] \neq (P)$.

|| **Corollaire 1.3.1.** Si $k = \bar{k}$, alors V et I sont inverses l'une de l'autre.

Démonstration. Soit $J \subseteq k[X_1, \dots, X_n]$ un idéal radical. Alors $I(V(J)) = \sqrt{J} = J$ et donc $I \circ V = \text{id}$. Soit $V = V(J) \subseteq \mathbb{A}_k^n$ un ensemble algébrique affine. Alors $I(V(J)) = \sqrt{J}$ et donc $V(I(V)) = V(\sqrt{J}) = V(J) = V$, donc $V \circ I = \text{id}$. \square

Donnons 2 reformulations du Nullstellensatz

|| **Proposition 1.3.2.** (*Nullstellensatz 2,3*) Considérons l'anneau $k[X_1, \dots, X_n]$. Tfae :

1. Pour tout $J \subseteq k[X_1, \dots, X_n]$, $I(V(J)) = \sqrt{J}$
2. Pour tout $J \subseteq k[X_1, \dots, X_n]$, J propre implique que $V(J) \neq \emptyset$
3. Les idéaux maximaux de $k[X_1, \dots, X_n]$ sont exactement les idéaux

$$\mathfrak{m}_a = (X_1 - a_1, \dots, X_n - a_n)$$

Démonstration. $2 \Rightarrow 3$: Soit $\mathfrak{m} \subseteq k[X_1, \dots, X_n]$. 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 $f = Q_1(X_1 - a_1) + \dots + Q_i(X_i - a_i) + c$). Ainsi $\mathfrak{m} \subseteq \mathfrak{m}_a$ mais \mathfrak{m} est maximal donc $\mathfrak{m} = \mathfrak{m}_a$.

$1 \Rightarrow 2$: Soit $J \subseteq k[X_1, \dots, X_n]$ idéal propre. On a $\sqrt{J} = I(V(J))$. Supposons que $V(J) = \emptyset$,

alors $\sqrt{J} = I(V(J)) = k[X_1, \dots, X_n]$ et donc $J = k[X_1, \dots, X_n]$, contradiction.

$3 \Rightarrow 1$: Soit $I \stackrel{\text{id}}{\subseteq} k[X_1, \dots, X_n]$, on veut mq $\sqrt{I} = I(V(I))$. Comme $I \subseteq I(V(I))$, on a directement la première inclusion du fait que $\sqrt{I(V(I))} = I(V(I))$. Dans l'autre sens, si $I = k[X_1, \dots, X_n]$, l'égalité est claire. Sinon soit $f \in I(V(I))$, écrivons $I = (P_1, \dots, P_r)$. Maintenant considérons l'anneau $k[X_1, \dots, X_n, X_{n+1}]$, puis l'idéal

$$(P_1, \dots, P_r, 1 - X_{n+1}f) =: J \stackrel{\text{id}}{\subseteq} k[X_1, \dots, X_{n+1}]$$

Si J est un idéal propre, alors d'après le théorème de Krull il existe $\mathfrak{m} \stackrel{\text{max}}{\subseteq} k[X_1, \dots, X_{n+1}]$ tel que $J \subseteq \mathfrak{m}$. Maintenant par hypothèse il existe $(a_1, \dots, a_n, b) \in \mathbb{A}_k^{n+1}$ tel que

$$\mathfrak{m} = (X_1 - a_1, \dots, X_n - a_n, X_{n+1} - b)$$

Mais alors pour tout $i \in \llbracket 1, r \rrbracket$, $P_i(a) = 0$ 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 $k[X_1, \dots, X_{n+1}]$ tout entier, donc en particulier il existe $Q_1, \dots, Q_r, Q \in k[X_1, \dots, X_{n+1}]$ tels que

$$1 = P_1 Q_1 + \dots + P_r Q_r + Q(1 - X_{n+1}f) \quad (1.1)$$

Maintenant le morphisme de localisation $k[X_1, \dots, X_n] \rightarrow k[X_1, \dots, X_n, 1/f]$ et le choix de l'élément $1/f$ induit un morphisme d'évaluation

$$\begin{array}{ccccc} k[X_1, \dots, X_n] & \longrightarrow & k[X_1, \dots, X_n, 1/f] & \hookrightarrow & k(X_1, \dots, X_n) \\ \downarrow & & \nearrow \text{!}\exists & & \\ k[X_1, \dots, X_n][X_{n+1}] & & & & \end{array}$$

Ainsi au travers de ce morphisme l'égalité 1.1 devient

$$1 = P_1(X_1, \dots, X_n)Q_1(X_1, \dots, X_n, 1/f) + \dots + P_r(X_1, \dots, X_n)Q_r(X_1, \dots, X_n, 1/f)$$

Alors écrivons les Q_i comme des éléments de $k[X_1, \dots, X_n][X_{n+1}]$,

$$Q_i = \sum_{l=0}^{d_i} R_{i,l}(X_1, \dots, X_n) X_{n+1}^l$$

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

$$Q_i = \frac{R_i(X_1, \dots, X_n)}{f^{d_i}}$$

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 $k(X_1, \dots, X_n)$ donc dans $k[X_1, \dots, X_n]$. Finalement si $d = 0$, alors $1 \in I$ absurde puisque l'on avait supposé I propre. Sinon, $f^d \in I$ et donc $f \in \sqrt{I}$. \square

Citons finalement une version plus générale du Nullstellensatz. Montrons qu'elle implique la version 3, et ainsi tous les énoncés équivalents prouvés précédemment.

|| **Théorème 1.3.2.** (*Nullstellensatz, 0*) Soit une extension de corps $K \hookrightarrow L$, avec L une k -algèbre de type fini. Alors $[L : K] < \infty$.

Rq 1.3.1. L K -algèbre de type fini ssi $L \simeq k[X_1, \dots, X_n]/I$.

Montrons que 1.3.2 implique 3 :

Démonstration. Soit k un corps algébriquement clos. Soit $\mathfrak{m} \subseteq^{\max} k[X_1, \dots, X_n]$. Soit $L := k[X_1, \dots, X_n]/\mathfrak{m}$ (qui est un corps et une k -algèbre de type fini). Considérons les morphismes $i : k \hookrightarrow k[X_1, \dots, X_n]$, $\pi : k[X_1, \dots, X_n] \twoheadrightarrow L$. On note $\varphi = \pi \circ i$. $k \rightarrow L$ est un morphisme de k -algèbres, donc de corps et donc d'après 1.3.2, $[L : K] < \infty$. Mais comme k est algébriquement clos, on doit avoir $k \simeq L$ (car $K \hookrightarrow L$ est alors une extension algébrique de k). Soit $a_i := \pi(X_i) \in L \simeq k$. Maintenant $\pi(X_i - i(\varphi^{-1}(a_i))) = \pi(X_i) - a_i = a_i - a_i = 0$, donc

$$(X_1 - i(\varphi^{-1}(a_1)), \dots, X_n - i(\varphi^{-1}(a_n))) =: \mathfrak{m}_a \subseteq \mathfrak{m}$$

et comme \mathfrak{m}_a est maximal, $\mathfrak{m} = \mathfrak{m}_a$. \square

Prouvons 1.3.2 dans le cas où k est non dénombrable :

Démonstration. (Nullstellensatz 0, corps K non dénombrable) Soit $K \hookrightarrow L$ une extension de corps, avec L une k -algèbre de type fini. Écrivons $L \simeq k[X_1, \dots, X_n]/I = K[a_1, \dots, a_n]$. Il suffit de montrer que $K \hookrightarrow L$ est algébrique, car dans ce cas a_1, \dots, a_n sont des éléments algébriques sur K et donc $K \hookrightarrow K(a_1) \hookrightarrow \dots \hookrightarrow K(a_1, a_2, \dots, a_n) = L$ est finie et chaque extension de cette suite d'extension est finie. Pour prouver que $K \hookrightarrow L$ est algébrique, supposons le contraire. Alors soit $z \in L$ un élément transcendant, puis considérons $K \hookrightarrow K(z) \hookrightarrow L$, et $K(z) \simeq K(T)$ le corps des fractions de $k[T]$. Maintenant

$L \simeq K[a_1, \dots, a_n]$ est un isom de K -algèbres, L admet une base dénombrable comme K -espace vectoriel. Mais $K(T)$ comme K -ev admet une famille libre non dénombrable

$$\left\{ \frac{1}{T - \lambda} \right\}_{\lambda \in k}$$

car K est non dénombrable. Vérifions que cette famille est bien libre : écrivons

$$\sum_{\text{finie}} a_i \frac{1}{T - \lambda_i} = 0$$

dans $K(T) \hookrightarrow L$. Ainsi

$$\sum_{\text{finie}} a_i (T - \lambda_i) \cdots (\widehat{T - \lambda_i}) \cdots (T - \lambda_l) = 0$$

dans $k[T]$, puis on évalue en λ_i et on obtiens $a_i = 0$ pour tout i . □

1.4 Sous-ensembles irréductibles

|| **Définition 1.4.1.** $V \subseteq \mathbb{A}_k^n$ 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 1.4.1.** $V \subseteq \mathbb{A}_k^n$ ensemble algébrique. Alors tfae

1. V est irréductible
2. $I(V)$ est un idéal premier
3. $k[X_1, \dots, X_n]/I(V)$ est un anneau intègre

Démonstration.

$1 \Rightarrow 2$: Soient $f, g \in k[X_1, \dots, X_n]$ 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 $f_1 \notin I(V)$. 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.

$2 \iff 3$: viens du fait que $J \xrightarrow{\text{id}} A$ est premier si et seulement si A/J est intègre. □

Rq 1.4.1. Supposons que $k = \bar{k}$. Alors I et V sont inverses l'une de l'autre et donnent une correspondance entre les idéaux radicaux de $k[X_1, \dots, X_n]$ et les ensembles algébriques affines de \mathbb{A}_k^n . Alors au travers de cette bijection, les ensembles irréductibles correspondent aux idéaux premiers, et les points aux idéaux maximaux.

Théorème 1.4.1. Soit $V \subseteq \mathbb{A}_k^n$ un ensemble algébrique. Alors $\exists V_1, \dots, V_m \subseteq \mathbb{A}_k^n$ irréductibles tels que

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

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

Ex 1.4.1. Soit $V := V(XY, (X-1)Z) \subseteq \mathbb{A}_k^n$, 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 $V \subseteq \mathbb{A}_k^n$ un ensemble algébrique. Si V est irréductible, on a terminé. Sinon il existe des sous-ensembles algébriques propres de V , $V_1, V_2 \subsetneq V$ tels que $V = V_1 \cup V_2$. Si V_1, V_2 sont irréductibles, alors on a fini. 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 $\dots \subsetneq W_2 \subsetneq W_1 \subsetneq V$ d'ensembles algébriques. Ainsi on obtiens une suite croissante

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

Remarquons alors qu'elle est 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 $k[X_1, \dots, X_n]$ est noethérien.

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

$$V_i \subseteq \bigcup_{j \in \llbracket 1, t \rrbracket} W_j \cap V_i$$

Mais V_i est irréductible, donc $\exists j \in \llbracket 1, t \rrbracket$ 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 $i' \in \llbracket 1, s \rrbracket$ tel que $W_i \subseteq V_{i'}$. Mais alors $V_i \subseteq W_j \subseteq V_{i'}$ et donc $i = i'$, d'où $V_i = W_j$. \square

Chapitre 2

Catégorie des ensembles algébriques et foncteur $k[-]$

Fixons un $k \in \mathbf{Fld}$.

2.1 Catégorie des ensembles algébriques sur k

Pour définir une catégorie des ensembles algébriques, nous avons besoin de définir une notion de morphisme entre ensembles algébriques.

Définition 2.1.1. (Morphisme d'ensembles algébriques) Soit $V, W \subseteq \mathbb{A}^n, \mathbb{A}^m$ des ensembles algébriques affines. $\varphi = (\varphi_1, \dots, \varphi_m) : V \rightarrow W$ est une fonction régulière, ou morphisme (d'ensembles algébriques affines) si pour tout $i \in \llbracket 1, l \rrbracket$, $\exists P_i \in k[X_1, \dots, X_n]$ tel que $\varphi_i(a) = P_i(a)$ pour tout $a \in V$.

Ex 2.1.1. 1. Soit $V \subseteq W \subseteq \mathbb{A}^n$ un ensemble algébrique. Alors l'injection associée à cette inclusion $i : V \rightarrow W$ est un morphisme.
2. $\pi_i : \mathbb{A}_k^n \rightarrow \mathbb{A}_k^1$ la projection sur la i -ème coordonnée est un morphisme.

Proposition 2.1.1. Soit $\varphi^1 : V_1 \rightarrow V_2$, $\varphi^2 : V_2 \rightarrow V_3$ des morphismes d'ensembles algébriques, où $V_i \subseteq \mathbb{A}_k^{n_i}$. Alors $\varphi^2 \circ \varphi^1 : V_1 \rightarrow V_3$ est un morphisme d'ensembles algébriques.

Démonstration. Notons $\varphi^1 = (\varphi_1^1, \dots, \varphi_{n_2}^1)$ et $\varphi^2 = (\varphi_1^2, \dots, \varphi_{n_3}^2)$, puis $f_i^1, g_j^2 \in k[X_1, \dots, X_{n_1}], k[Y_1, \dots, Y_{n_2}]$ les polynômes associés à φ_i^1, φ_j^2 . Maintenant considérons les polynômes $h_i \in k[X_1, \dots, X_{n_1}]$ obtenus en évaluant les g_i en f_1, \dots, f_{n_2} , alors

on a

$$\begin{aligned} (\varphi^2 \circ \varphi^1)(a) &= (g_1(f_1(a), \dots, f_{n_2}(a)), \dots, g_{n_3}(f_1(a), \dots, f_{n_2}(a))) \\ &= (h_1(a), \dots, h_{n_3}(a)) \end{aligned}$$

et donc $\varphi^2 \circ \varphi^1$ est un morphisme. \square

Proposition 2.1.2. *Soient $V, W \subseteq \mathbb{A}_k^n, \mathbb{A}_k^l$ des ensembles algébriques. Une application $\varphi : V \rightarrow W$ est un morphisme si et seulement si pour tout morphisme $f : W \rightarrow \mathbb{A}^1$, $f \circ \varphi : V \rightarrow \mathbb{A}^1$ est un morphisme.*

Démonstration.

\Rightarrow : La composition de morphismes est un morphisme.

\Leftarrow : Soit $p_i : W \hookrightarrow \mathbb{A}^l \rightarrow \mathbb{A}^1$ la projection sur la i -ème coordonnée, c'est un morphisme car composition de morphismes. Maintenant $\pi \circ \varphi = \varphi_i$ est un morphisme donc il existe $P_i \in k[X_1, \dots, X_n]$ tel que $\varphi_i(a) = P_i(a)$ pour tout $a \in V$, et ainsi φ est un morphisme. \square

On peut ainsi définir une catégorie des ensembles algébriques affines sur k , notée $k\text{-}\mathbf{EnsAlg}$, ou encore seulement \mathbf{EnsAlg} si le contexte est clair, dont

1. Les objets sont les ensembles algébriques affines $V \subseteq \mathbb{A}_k^n$,
2. $\mathbf{Hom}_{\mathbf{EnsAlg}}(V, W)$ est la classe des morphismes de V dans W au sens de 2.1.1
3. La composition de morphismes correspond à la composition des applications sous-jacentes.

Remarquons que cette catégorie est bien définie du fait que id_V est un morphisme et que les morphismes sont stables par composition.

Proposition 2.1.3. $\varphi : V \rightarrow W \subseteq \mathbb{A}^l$ est un morphisme ssi $V \rightarrow \mathbb{A}^l$ est un morphisme.

Démonstration.

\Rightarrow : $V \rightarrow W \hookrightarrow \mathbb{A}^l$ est une composition de morphismes, donc est un morphisme.

\Leftarrow : Par hypothèse, $i \circ \varphi : V \rightarrow \mathbb{A}^l$ est un morphisme ($i : W \rightarrow \mathbb{A}^l$ est le morphisme associé à l'inclusion $W \subseteq \mathbb{A}^l$). Ainsi il existe $P_i \in k[X_1, \dots, X_n]$ tels que

$$(P_1(a), \dots, P_l(a)) = (i \circ \varphi)(a) = \varphi(a)$$

pour tout $a \in V$, et donc φ est un morphisme. \square

- Ex 2.1.2.**
1. $\varphi : \mathbb{A}^n \rightarrow \mathbb{A}^l$ définie par $\varphi(X_1, \dots, X_n) = (P_1(x), \dots, P_l(x))$ avec les $P_i \in k[X_1, \dots, X_n]$ est un morphisme, par définition.
 2. $\varphi : \mathbb{A}^1 \rightarrow V := \{(x, y) \mid y = x^2\} \subseteq \mathbb{A}^2$ donné par $\varphi(t) = (t, t^2)$ est un morphisme.
 3. $\varphi : \mathbb{A}^1 \rightarrow V := \{(x, y) \mid y^2 = x^3\} \subseteq \mathbb{A}^2$ donné par $\varphi(t) = (t^2, t^3)$ est un morphisme.

2.2 Foncteur $k[-]$

Donnons maintenant un foncteur entre **EnsAlg** et $k - \mathbf{CAlg}_{\text{tf,red}}$ la catégorie des k -algèbres de type fini réduites sur k .

Définition 2.2.1. $V \subseteq \mathbb{A}_k^n$ ensemble algébrique. L'algèbre des fonctions régulières sur V est

$$k[V] := k[X_1, \dots, X_n]/I(V)$$

Rq 2.2.1. Comme $I(V) = \sqrt{I(V)}$, $k[V]$ est une k -algèbre de type fini et réduite ($\sqrt{\{0\}} = \{0\}$). En effet, pour tout anneau A et $I \subseteq A$, A/I est réduit si et seulement si $I = \sqrt{I}$.

Remarquons que l'ensemble des fonctions régulières sur un ensemble algébrique $V \subseteq \mathbb{A}_k^n$ est munie d'une structure naturelle de k -algèbre. Alors

Lemme 2.2.1. *L'application*

$$\begin{aligned} \chi : k[V] &\rightarrow \mathbf{Hom}_{\mathbf{EnsAlg}}(V, \mathbb{A}^1) \\ [P] &\mapsto (f_P : a \mapsto P(a)) \end{aligned}$$

est bien définie et est un isomorphisme de k -algèbres.

Démonstration. Considérons l'application

$$\begin{aligned} \tilde{\chi} : k[X_1, \dots, X_n] &\rightarrow \mathbf{Hom}_{\mathbf{EnsAlg}}(V, \mathbb{A}^1) \\ P &\mapsto f_P \end{aligned}$$

C'est un morphisme de k -algèbres, vérifions que son noyau est exactement $I(V)$:

$$\tilde{\chi}(P) = 0 \iff \forall a \in V, P(a) = 0 \iff P \in I(V)$$

Finalement, cette application est surjective par définition de $\mathbf{Hom}_{\mathbf{EnsAlg}}(V, \mathbb{A}^1)$, et donc $\tilde{\chi}$ se factorise en un isomorphisme au travers du quotient $k[V]$ (cet isomorphisme est χ et donc χ est un isomorphisme). \square

Maintenant, soit $\varphi : V \subseteq \mathbb{A}_k^n \rightarrow W \subseteq \mathbb{A}_k^l$ un morphisme, alors ce morphisme induit un morphisme de k -algèbres entre $k[W]$ et $k[V]$, définit formellement comme

$$\begin{aligned} k[\varphi] = \varphi^* : k[W] &\rightarrow k[V] \\ [P] &\mapsto \chi^{-1}(\chi([P]) \circ \varphi) \end{aligned}$$

Ainsi au travers de χ il envoie f_P sur $f_P \circ \varphi$. De plus, si on note $\varphi_i \in k[X_1, \dots, X_n]$ des polynômes tels que $\varphi(a) = (\varphi_i(a))$ pour tout $a \in V$, alors

$$\varphi^*([Y_i]) = \chi^{-1}(\chi([Y_i]) \circ \varphi) = \varphi_i$$

CHAPITRE 2. CATÉGORIE DES ENSEMBLES ALGÈBRIQUES ET FONCTEUR $K[-]$

Ainsi φ^* correspond au morphisme d'évaluation en les φ_i . Finalement, pour tout $x \in V$,

$$\varphi^*([P])(x) = (f_P \circ \varphi)(x) = f_P(\varphi(x)) = [P](\varphi(x))$$

|| **Proposition 2.2.1.** *Soient $\varphi_1 : V_1 \rightarrow V_2$, $\varphi_2 : V_2 \rightarrow V_3$. Alors $\varphi_1^* \circ \varphi_2^* = (\varphi_2 \circ \varphi_1)^*$. De plus, $(\text{id}_V)^* = \text{id}_{k[V]}$.*

Démonstration. 1. $k[\text{id}_V]([P]) = \chi^{-1}(\chi([P]) \circ \text{id}_V) = [P] = \text{id}_{k[V]}([P])$ donc $k[\text{id}_V] = \text{id}_{k[V]}$.
2.

$$\begin{aligned} (k[\varphi_1] \circ k[\varphi_2])[P] &= \chi^{-1}(\chi(\chi^{-1}(\chi([P]) \circ \varphi_2)) \circ \varphi_1) \\ &= \chi^{-1}(\chi([P]) \circ \varphi_2 \circ \varphi_1) \\ &= k[\varphi_2 \circ \varphi_1]([P]) \end{aligned}$$

□

|| **Définition 2.2.2.** (Foncteur $k[-]$) On définit

$$\begin{array}{ccc} k[-] : \mathbf{EnsAlg}^{\text{op}} & \rightarrow & k - \mathbf{CAlg}_{\text{tf,red}} \\ V & \mapsto & k[V] \\ \varphi : V \rightarrow W & \mapsto & k[\varphi] : k[W] \rightarrow k[V] \end{array}$$

Ce foncteur est bien défini au vu de 2.2.1.

|| **Théorème 2.2.1.** $k[-]$ est pleinement fidèle.

|| **Corollaire 2.2.1.** *Soit $\varphi : V \rightarrow W$ morphisme. C'est un isomorphisme ssi $\varphi^* : k[W] \rightarrow k[V]$ est un isomorphisme. En particulier V non isomorphe à W ssi $k[V]$ non isomorphe à $k[W]$.*

Démonstration. (2.2.1) Les foncteurs pleinement fidèles préservent et réfléchissent les isomorphismes. □

Démonstration. (2.2.1) Soit $\varphi : V \rightarrow W \subseteq \mathbb{A}^l$, écrivons $\varphi = (\varphi_1, \dots, \varphi_l)$, avec $\varphi_i : V \rightarrow k$. φ morphisme, donc

$$\begin{array}{ccc} \varphi^* : k[W] \simeq k[Y_1, \dots, Y_l]/I(W) & \rightarrow & k[V] \\ [Y_i] & \mapsto & \varphi_i \end{array}$$

CHAPITRE 2. CATÉGORIE DES ENSEMBLES ALGÈBRIQUES ET FONCTEUR $K[-]$

Montrons que F est injective : soient φ, ψ telles que $\varphi^* = \psi^*$. Alors $\varphi_i = \psi_i$ et donc $\varphi = \psi$. Montrons que F est surjective : soit $\alpha : k[W] \rightarrow k[V]$ un morphisme de k -algèbres. Alors notons $\varphi_i := \alpha([Y_i]) \in k[V]$, ainsi $\varphi_i : V \rightarrow k$ est une fonction régulière. Posons alors $\varphi = (\varphi_1, \dots, \varphi_l)$. Il suffit de montrer que l'image de φ est contenue dans W . En effet, si c'est le cas, on peut définir $\tilde{\varphi} : V \rightarrow W$ qui fait commuter

$$\begin{array}{ccc} V & \xrightarrow{\varphi} & \mathbb{A}^l \\ & \searrow \tilde{\varphi} & \uparrow \\ & & W \end{array}$$

et ainsi $\tilde{\varphi}^* = \alpha$. Soit $W = V(P_1, \dots, P_r) \subseteq \mathbb{A}^l$, $P_i \in k[Y_1, \dots, Y_l]$. En particulier, $P_i \in I(W)$ pour tout i . On doit vérifier que $P_i(\varphi_1(a), \dots, \varphi_l(a)) = 0$ pour tout i et $a \in V$. Comme $P_i \in I(W)$, $\alpha([P_i]) = 0$. Mais $\alpha([Y_i]) = \varphi_i$, donc

$$0 = \alpha([P_i]) = P_i(\alpha([Y_1]), \dots, \alpha([Y_l])) = P_i(\varphi_1, \dots, \varphi_l) \in k[V]$$

□

|| **Proposition 2.2.2.** $\varphi : V \rightarrow W$ est un isomorphisme si et seulement si l'application sous-jacente à φ est bijective, et son inverse $\varphi^{-1} : W \rightarrow V$ est un morphisme.

Démonstration. Clair du fait que le foncteur d'oubli **EnsAlg** \rightarrow **Sets** est fidèle. □

Ex 2.2.1. Reprenons les points 2 et 3 de 2.1.2 :

3. C'est un isomorphisme puisque $\varphi^{-1} : V \rightarrow \mathbb{A}^1$ donné par $\varphi^{-1}(x, y) = x$ est un morphisme et est une inverse de φ dans **Sets**.
4. Forcément, une inverse de φ est une inverse dans **Sets** au travers du foncteur d'oubli qui envoie un ensemble algébrique sur son ensemble sous-jacent. Ainsi $\varphi^{-1} : V \rightarrow \mathbb{A}^1$ doit forcément être définie comme

$$\varphi^{-1}(x, y) = \begin{cases} y/x & \text{si } (x, y) \neq 0 \\ 0 & \text{sinon} \end{cases}$$

Mais φ^{-1} n'est pas un morphisme : supposons qu'il existe $P \in k[X, Y]$ tq $P(x, y) = \varphi^{-1}(x, y)$, alors $P(x, y) = y/x$ pour tout $(x, y) \in V$ et $V = \{(t^2, t^3) \mid t \in k\}$, et ainsi $P(t^2, t^3) = t$ pour tout $t \in k \setminus \{0\}$, ce qui est clairement impossible. On peut aussi vérifier que le morphisme induit sur les algèbres de fonctions régulières n'est pas un isomorphisme.

2.3 Cas des corps algébriquement clos

Supposons désormais que $k = \bar{k}$. Alors

|| **Proposition 2.3.1.** $k[-] : \mathbf{EnsAlg}^{\text{op}} \rightarrow k - \mathbf{CAlg}_{\text{tf,red}}$ est essentiellement surjectif.
 Ainsi les catégories $\mathbf{EnsAlg}^{\text{op}}$ et $k - \mathbf{CAlg}_{\text{tf,red}}$ sont équivalentes.

Démonstration. Soit $L = k[X_1, \dots, X_n]/J \in k - \mathbf{CAlg}_{\text{td,red}}$. Alors

$$k[V(J)] = k[X_1, \dots, X_n]/I(V(J)) = k[X_1, \dots, X_n]/\sqrt{J} = L$$

d'après le Nullstellensatz. □

Chapitre 3

Dimension, espace tangent

3.1 Topologie induite sur les ensembles algébriques

\mathbb{A}_k^n est muni d'une topologie, dont les fermés sont les $V(I)$ pour I un idéal de $k[X_1, \dots, X_n]$. Ainsi on définit la topologie de Zariski sur $V \subseteq \mathbb{A}_k^n$ un ensemble algébrique comme la topologie induite sur V . Plus concrètement, les fermés de V sont les $V(I) \cap V$, pour I un idéal de $k[X_1, \dots, X_n]$ (i.e. les ensembles algébriques $W \subseteq V$).

Exercice. Les ouverts distingués $D(f)$ forment une base pour la topologie de Zariski de \mathbb{A}^n .

Ainsi $\{D(f) \cap V\}_f$ est une base des ouverts pour la topologie de Zariski sur V un ensemble algébrique fixé.

|| **Proposition 3.1.1.** Soient $V, W \subseteq \mathbb{A}^n, \mathbb{A}^l$. Tout morphisme $\varphi : V \rightarrow W$ est continu pour la topologie de Zariski induite sur V et W .

Démonstration. Dans un premier temps, soit $f_i \in k[X_1, \dots, X_n]$ tels que $\varphi(a) = (f_1(a), \dots, f_i(a))$. Alors montrer que φ est continue revient à montrer que $\tilde{\varphi} : \mathbb{A}^n \rightarrow \mathbb{A}^l$ définie par $\tilde{\varphi}(a) = (f_1(a), \dots, f_i(a))$ pour tout $a \in \mathbb{A}^n$ est continue. En effet, soit Z un fermé de W , alors $Z = Z' \cap W$ pour Z' un fermé de \mathbb{A}^l . Maintenant $\varphi^{-1}(Z) = \tilde{\varphi}^{-1}(Z') \cap V$ et est donc un fermé si et seulement si $\tilde{\varphi}^{-1}(Z')$ est un fermé. On peut donc se ramener au cas $\varphi : \mathbb{A}^n \rightarrow \mathbb{A}^l$. Ainsi considérons un fermé $V(J) \stackrel{\text{ferm}}{\subseteq} \mathbb{A}^l$, posons $I := k[\varphi](J)$, et montrons que $\varphi^{-1}(V(J)) = V(I)$.
 \subseteq : soit $x \in \varphi^{-1}(V(J))$, alors pour tout $P \in I$, il existe $Q \in J$ tel que $P = k[\varphi](Q)$. Maintenant

$$P(x) = k[\varphi](Q)(x) = Q(\varphi(x)) = 0$$

puisque $Q \in J$ et $\varphi(x) \in V(J)$.

\supseteq : Soit $x \in V(I)$, alors pour tout $Q \in J$, $k[\varphi](Q) \in I$ et donc

$$Q(\varphi(x)) = k[\varphi](Q)(x) = 0$$

et donc $\varphi(x) \in V(J)$. □

Exercice. Soit $f : X \rightarrow Y$ un morphisme dans **Top**, si X est irréductible, alors $\overline{f(X)}$ est irréductible.

Ex 3.1.1. ($k = \bar{k}$)

$$\begin{array}{ccc} f : \mathbb{A}^1 & \rightarrow & V = \{(x, y) \in \mathbb{A}^2 \mid y^2 = x^3\} \\ t & \mapsto & (t^2, t^3) \end{array}$$

est surjectif, donc V est irréductible.

Ex 3.1.2. $V = \{(x, y) \mid xy = 1\} \subseteq \mathbb{A}^2$. Notons $f : V \rightarrow \mathbb{A}^1$ la projection sur la première coordonnée, alors $f(V) = \mathbb{A}^1 \setminus \{0\}$ n'est pas fermé (si $|k| = \infty$) et donc ne peut pas être un ensemble algébrique.

Exercice. $E \subseteq \mathbb{A}_k^n$ ensemble quelconque, alors $\bar{E} = V(I(E))$. Soit $E \subseteq V(J)$ un fermé. Alors $J \subseteq I(V(J)) \subseteq I(E)$ et donc $V(I(E)) \subseteq V(J)$, ce qui prouve que $V(I(E)) = \bar{E}$.

3.2 Variétés affines, dimension

|| **Définition 3.2.1.** (Variété affine) Une variété affine est un ensemble algébrique affine irréductible.

Ainsi si V est une variété affine, alors $k[V] = k[X_1, \dots, X_n]/I(V)$ est intègre (vu que $I(V)$ est un idéal premier).

3.2.1 Dimension d'une variété affine

Dans un premier temps, rappelons quelques notions de théorie des extensions de corps :

|| **Définition 3.2.2.** $k \hookrightarrow K$ extension de corps.

1. Une partie $S \subseteq K$ est algébriquement indépendante si pour tout $m \geq 1$, tout $s_1, \dots, s_m \in S$, si $P \in k[X_1, \dots, X_m]$ est tel que $P(s_1, \dots, s_m) = 0$, alors $P = 0$.
2. $S \subseteq K$ est une base de transcendance de K (sur k) si S est algébriquement indépendante et $k(S) \hookrightarrow K$ est algébrique.
3. On dit que $k \hookrightarrow K$ est purement transcendante s'il existe S une base de transcen-

|| dance telle que $k \hookrightarrow k(S) \simeq K$.

|| **Proposition 3.2.1.** *Si $|S| = n$, alors $k(S) \simeq k(X_1, \dots, X_n)$. Si S_1, S_2 sont deux bases de transcendance de K/k , alors $|S_1| = |S_2|$.*

Démonstration. Tag 030D □

|| **Définition 3.2.3.** Soit $k \hookrightarrow K$ une extension de corps. On définit le degré de transcendance de K sur k par $\text{trdeg}_k(K) = |S|$, où S est une base de transcendance de K/k .

|| **Définition 3.2.4.** (Corps des fonctions rationnelles) Soit V une variété affine. On appelle corps des fonctions rationnelles sur V le corps des fractions de $k[V]$, noté $k(V)$.

|| **Définition 3.2.5.** ($k = \bar{k}$) V variété affine. On définit la dimension de V par

$$\dim V := \text{trdeg}_k k(V)$$

Rq 3.2.1. $\dim V \leq n$ pour toute variété algébrique dans \mathbb{A}^n .

Ex 3.2.1. 1. $\dim \mathbb{A}_k^n = n$: $V = \mathbb{A}_k^n$, $k[V] = k[X_1, \dots, X_n]$. $I(V) = \{0\}$. Ainsi $k(V) = k(X_1, \dots, X_n)$. Et $\{X_1, \dots, X_n\}$ est une base de transcendance de $k(V)$, donc $\dim V = n$.

2. $V = \{(x, y) \mid xy = 1\} \subseteq \mathbb{A}^1$. Alors $V = V(XY - 1)$ est irréductible ; Ainsi V est une variété affine. $k[V] = k[X, Y]/(XY - 1) = k[x, y]$ où $x = [X]$, $y = [Y]$ (et $xy = 1$). $k(V) = \text{Frac}(k[x, y]) =: k(x, y)$. Maintenant $k(x, y) = k(x)$ vu que $y = 1/x$. Ainsi $\{x\}$ est une base de transcendance de $k(x)$: sinon il existe $P \in k[X]$ non nul tel que $P(x) = 0 \in k(x)$, et en particulier dans $k[x] \subseteq k[V]$. Ainsi $P \in I(V)$ donc $P(X) = (XY - 1)Q(X, Y)$ dans $k[X, Y]$ avec $Q \in k[X, Y]$, ce qui est absurde puisque $\deg_Y P = 0$. Ainsi $\dim V = 1$

|| **Lemme 3.2.1.** ($k = \bar{k}$) Soit $f \in k[X_1, \dots, X_n]$ irréductible. Alors $V := V(f) \subseteq \mathbb{A}_k^n$ est une variété affine de dimension $n - 1$.

Démonstration. Comme f est non constant, quitte à réindexer ops que $\deg_{X_n}(f) > 0$. Notons $k[V] = k[x_1, \dots, x_n]$. Ainsi $f(x_1, \dots, x_n) = 0$ vu que $I(V) = (f)$. . Maintenant $k \subseteq k(x_1, \dots, x_{n-1}) \subseteq k(x_1, \dots, x_{n-1})(x_n)$ est algébrique car $f(x_1, \dots, x_n) = 0$. Montrons que $\{x_1, \dots, x_{n-1}\}$ sont algébriquement indépendants sur k : si $g \in k[X_1, \dots, X_{n-1}]$ tel que $g(x_1, \dots, x_{n-1}) = 0$ dans $k(V)$ (donc dans $k[V]$). Alors $g(x_1, \dots, x_{n-1}) \in I(V) = (f)$ mais $\deg_{X_n} g = 0$, donc g est nul. □

Rq 3.2.2. Soient $f_1, \dots, f_r \in k[X_1, \dots, X_n]$, $V := V(f_1, \dots, f_r) \subseteq \mathbb{A}_k^n$. Supposons que V est irréductible, alors $\dim V \geq n - r$. **Preuve en exercice**

Ex 3.2.2. $V := V(Y - X^2, Z - X^3, XZ - Y^2) \subseteq \mathbb{A}_k^3$. Alors $V = \{(t, t^2, t^3) \mid t \in k\}$ est une variété affine de dimension 1 (on parle de courbe affine). En effet, V est irréductible, puis $k[V] \simeq k[T]$ donc $\text{Frack}[V] \simeq k(T)$ est de degré de transcendance 1 sur k . Comme V est définie par 3 équations, $XZ - Y^2$ peut s'exprimer en fonction des deux autres polynômes et est donc superflue.

Rq 3.2.3. Si V, W sont des variétés affines isomorphes, alors $k[V] \simeq k[W]$ (morphisme de k -algèbres) et ainsi $k(V) \simeq k(W)$ (morphisme d'extensions de corps) donc $\dim V = \dim W$. Dans l'exemple précédent, on peut directement conclure que V est de dimension 1 avec cette remarque.

Ex 3.2.3. $V = V(XZ - Y^2, XW - YZ, YW - Z^2) = V(f_1, f_2, f_3) \subseteq \mathbb{A}^4$. On sait que $\dim V \geq 1$ d'après la remarque 3.2.2. En fait, $\dim V = 2$, et $f_i \notin (f_j, f_l)$ pour tout i, j, l différents deux à deux. Montrons par exemple que $f_3 \notin (f_1, f_2)$: Soit $W = V(f_1, f_2)$, si $f_3 \in (f_1, f_2)$, alors $V = W$. Mais $V \cap \{x = 0\} \neq W \cap \{x = 0\}$:

$$\begin{aligned} V \cap \{x = 0\} &= \{(0, 0, 0, w) \mid w \in k\} \\ W \cap \{x = 0\} &= \{(0, 0, z, w) \mid z, w \in k\} \end{aligned}$$

On peut montrer les autres de manière similaire, ainsi on ne peut pas éliminer d'équation, mais pourtant $\dim V = 2$: Soit $V' = V(f_1)$, $V'' = V(f_1, f_2)$ ($V \subseteq V'' \subseteq V'$). Calculons la dimension de ces différentes variétés :

$$k[V'] = k[X, Y, Z, W]/(XZ - Y^2) = k[x, y, z, w]$$

où $xz = y^2$. Alors $k(V') = k(x, y, z, w) = k(x, y, w)$ puisque $z = y^2/x$ dans $k(V')$. Enfin on peut prouver que x, y, z sont algébriquement indépendants, et donc $\dim V' = 3$.

$k[V''] = k[x, y, z, w]$ avec $xz = y^2$, $sw = yz$. Ainsi $k(V'') = k(x, y)$ puisque $z = y^2/x$, $w = yz/x$, et on peut prouver que x, y sont algébriquement indépendants, i.e. $\dim V'' = 2$.

$k(V) = k(x, y, z, w)$, mais $z = y^2/x$, $w = yz/x$, mais la 3ème équation ne nous donne pas d'autre relation (c'est la même que celle donnée par la première équation). Il est donc possible de prouver que x, y sont algébriquement indépendants et alors $\dim V = 2$.

3.2.2 Dimension de krull

Soit $A \in \mathbf{CRings}$.

Définition 3.2.6. (Dimension de Krull) La dimension de Krull d'un anneau est définie comme

$$\dim A := \sup\{l \geq 0 \mid \mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_l \subseteq A\}$$

- Ex 3.2.4.**
1. $A = k[X_1, \dots, X_n]$. Alors considérons $\mathfrak{p}_i = (X_1, \dots, X_i)$ pour $0 \leq i \leq n$, on a donc $\dim A \geq n$. On peut en fait montrer que $\dim A = n$.
 2. La dimension d'un corps vaut 0,
 3. $\dim \mathbb{Z} = 1$.

Rq 3.2.4. $\mathfrak{p} \subseteq A$ idéal premier, alors

$$\dim(A/\mathfrak{p}) = \sup\{l \geq 0 \mid \mathfrak{p} = \mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_l\}$$

Définition 3.2.7. (Hauteur) Soit $\mathfrak{p} \overset{\text{pr}}{\subseteq} A$, alors

$$ht(\mathfrak{p}) = \sup\{s \geq 0 \mid \mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_s = \mathfrak{p}\}$$

- Ex 3.2.5.**
1. $A = \mathbb{Z}$, alors $ht(p\mathbb{Z}) = 1$.
 2. $A = k[T]$, alors $ht((f)) = 1$.
 3. $A = k[X_1, \dots, X_n]$, $\mathfrak{p} = (X_1, \dots, X_s)$. Alors $ht\mathfrak{p} = s$.

Théorème 3.2.1. k corps, A k -algèbre de type fini. Soit \mathfrak{p} idéal premier, alors

$$ht\mathfrak{p} + \dim A/\mathfrak{p} = \dim A$$

Démonstration. **Référence**

□

- Ex 3.2.6.**
1. $A = \mathbb{Z}$, $\mathfrak{p} = p\mathbb{Z}$ avec p premier ; Alors $ht\mathfrak{p} = 1$, $A/\mathfrak{p} = \mathbb{F}_p$ est de dimension 0.
 2. $A = k[X_1, \dots, X_n]$, $\mathfrak{p} = (X_1, \dots, X_s)$ avec $s \in \llbracket 1, n \rrbracket$. $ht\mathfrak{p} = s$, $A/\mathfrak{p} \simeq k[X_{s+1}, \dots, X_n]$, $\dim A/\mathfrak{p} = n - s$.
 3. La dimension peut être infinie : par exemple $A = k[\mathbb{N}]$ est de dimension infinie.

Théorème 3.2.2. *Soit V une variété affine. Alors*

$$\dim k[V] = \dim V$$

Démonstration. **Référence**

□

3.3 Singularités

Soit $V \subseteq \mathbb{A}_k^n$ une variété affine. Notons $d = \dim V$, et soit $I(V) = (P_1, \dots, P_r) \subseteq k[X_1, \dots, X_n]$. On a $d \geq n - r$. Considérons le morphisme

$$\begin{aligned} \varphi : \mathbb{A}^n &\rightarrow \mathbb{A}^r \\ x &\mapsto (P_1(x), \dots, P_r(x)) \end{aligned}$$

En particulier, $\varphi|_V = 0$.

Notation. On note

$$d\varphi(x) = \begin{bmatrix} \frac{\partial P_1}{\partial X_1}(x) & \cdots & \frac{\partial P_1}{\partial X_n}(x) \\ \vdots & & \vdots \\ \frac{\partial P_r}{\partial X_1}(x) & \cdots & \frac{\partial P_r}{\partial X_n}(x) \end{bmatrix} \in M_{r,n}(k)$$

la matrice jacobienne de φ en x .

Proposition 3.3.1. *Pour tout $a \in V$, le rang de $d\varphi(a)$ ne dépend pas du choix des P_i , et on a $\text{rk} d\varphi(a) \leq n - d$.*

Démonstration. **A faire**

□

Définition 3.3.1. $a \in V$ est un point régulier (ou encore non singulier) de V si

$$\text{rk}(d\varphi(a)) = n - d$$

Si $\text{rk}(d\varphi(a)) < n - d$, on dit que a est un point singulier de V . Enfin, si pour tout $a \in V$, a est un point régulier, alors on dira que V est lisse.

Ex 3.3.1. 1. \mathbb{A}^n est lisse.

2. $V = V(f) \subseteq \mathbb{A}^n$ pour $f \in k[X_1, \dots, X_n]$ irréductible est une variété affine de dimension $n - 1$. Alors

$$d\varphi = \left[\frac{\partial f}{\partial X_1}, \dots, \frac{\partial f}{\partial X_n} \right]$$

Ainsi $a \in V(f)$ est singulier ssi $\text{rk}(d\varphi(a)) = 0$ ssi $\frac{\partial f}{\partial X_1}(a) = \dots = \frac{\partial f}{\partial X_n}(a) = 0$.

3. Si $f = XY - 1$, $V = V(f) \subseteq \mathbb{A}^2$. Alors $\frac{\partial f}{\partial X} = Y$ et $\frac{\partial f}{\partial Y} = X$, alors $a \in V$ singulier si $a_2 = a_1 = 0$, mais $a \in V \iff a_1 a_2 = 1$, donc tout point de V est régulier et V est donc lisse.
4. $f = Y^2 - X^3$, $V := V(f) \subseteq \mathbb{A}^2$. Si $\text{char } k \neq 2, 3$, alors $a \in V$ singulier ssi $a = (0, 0)$.
5. $f = Y^2 - X(X-1)(X-\lambda)$, $\lambda \in k$ ("courbe elliptique" si $\lambda \neq 0, 1$). $f = Y^2 - X^3 + (\lambda+1)X^2 - \lambda X$.
Alors

$$\begin{aligned}\frac{\partial f}{\partial X} &= -3X^2 + 2(\lambda+1)X - \lambda \\ \frac{\partial f}{\partial Y} &= 2Y\end{aligned}$$

et donc $(a, b) \in V(f)$ singulier ssi

$$\begin{cases} -3x^2 + 2(\lambda+1)x - \lambda = 0 \\ 2y = 0 \\ y^2 = x(x-1)(x-\lambda) \end{cases} \iff \begin{cases} y = 0 \\ x = 0, 1, \lambda \\ -3x^2 + 2(\lambda+1)x - \lambda = 0 \end{cases}$$

Alors

- (a) Si $x = 0$, $\lambda = 0$ et $(0, 0)$ est le seul point singulier.
 - (b) Si $x = 1$, alors $\lambda = 1$ et $(1, 0)$ est le seul point singulier.
 - (c) Si $x = \lambda$, alors $\lambda = 0, 1$ et donc c'est les cas précédents.
- Ainsi si $\lambda \neq 0, 1$, alors $V(f)$ est lisse.

3.4 Espace tangent

3.4.1 Anneau des fonctions régulières en un point

Soit $V \subseteq \mathbb{A}_k^n$ une variété affine, $a \in V$. Par définition,

$$k[V] = \frac{k[X_1, \dots, X_n]}{I(V)}$$

puis $k(V) = \text{Frack}[V]$.

|| **Définition 3.4.1.** $\alpha \in k(V)$ est bien définie au point $a \in V$ si $\exists f, g \in k[V]$ telles que $\alpha = f/g \in k(V)$ et $g(a) \neq 0$. Dans ce cas, la valeur de α en a est définie comme $\alpha(a) := f(a)/g(a) \in k$.

Rq 3.4.1. En général, pour $\alpha \in k(V)$, on peut toujours écrire $\alpha = f/g$ mais f et g ne sont pas uniques.

Ex 3.4.1. $V = V(Y^2 - X^3) \subseteq \mathbb{A}^2$; Alors $k[V] = k[x, y]$ avec $y^2 = x^3$. Alors

$$\frac{y}{x} = \frac{x^2}{y} \in k(V)$$

|| **Proposition 3.4.1.** Soit $\alpha \in k(V)$ bien définie en $a \in V$. Alors $\alpha(a)$ est bien définie.

Démonstration. Si $\alpha = f/g = f'/g'$ avec $f, g, f', g' \in k[V]$ et $g(a), g'(a) \neq 0$. Alors $fg' - f'g = 0 \in k[V]$ et donc $f(a)g'(a) - f'(a)g(a) = 0$, ce qui implique que

$$\frac{f(a)}{g(a)} = \frac{f'(a)}{g'(a)} \in k$$

□

Notation.

$$k[V]_a := \{\alpha \in k(V) \mid \alpha \text{ est définie en } a\}$$

C'est un sous anneau de $k(V)$, dit anneau local de fonctions régulières autour de a .

Rq 3.4.2. 1. $k \subseteq k[V] \subseteq k[V]_a \subseteq k(V)$

2. $a \in V \iff I(V) \subseteq \mathfrak{m}_a$. Si $g \in k[V]$, $g(a) = 0 \iff g \in \mathfrak{m}_a/I(V) \subseteq^{\max} k[V]$.

3. $k[V]_a$ est la localisation de $k[V]$ en $S = k[V] \setminus \mathfrak{p}$, où $\mathfrak{p} = \mathfrak{m}_a/I(V)$. En effet,

$$(k[V] \setminus \mathfrak{p})k[V] = \left\{ \frac{p}{q} \in k(V) \mid q \in k[V] \setminus \mathfrak{p} \right\}$$

$$\text{puis } q(a) = 0 \iff q \in \mathfrak{p}.$$

3.4.2 Anneaux locaux

Avant de parler d'espace tangent de Zariski, faisons quelques rappels sur les anneaux locaux. Si A est un anneau, $S = A \setminus \mathfrak{p}$, l'image $S^{-1}\mathfrak{p}$ de \mathfrak{p} par le morphisme canonique $A \rightarrow S^{-1}A$ est l'unique idéal maximal de $S^{-1}A$. En effet, $S^{-1}A \setminus S^{-1}\mathfrak{p}$ sont des inversibles de $S^{-1}A$. Ainsi $S^{-1}A$ est un anneau local.

Notation. On notera (A, \mathfrak{m}) les anneaux locaux, avec \mathfrak{m} leur unique idéal maximal. A/\mathfrak{m} est le corps résiduel de A .

|| **Proposition 3.4.2.** *Soit A un anneau noethérien intègre, $S \subseteq A$ un ensemble multiplicatif. Alors $S^{-1}A$ est noethérien.*

Démonstration. Soit $I \subseteq S^{-1}A$, Comme A est intègre, le morphisme $\varphi : A \rightarrow S^{-1}A$ est injectif. alors $J := \varphi^{-1}(I)$ est un idéal de A , qui est de type fini. Ainsi il existe $P_1, \dots, P_r \in J$ tel que $J = (P_1, \dots, P_r)$. Montrons que $I = (\varphi(P_1), \dots, \varphi(P_r)) = (P_1/1, \dots, P_r/1)$. Soit $a/s \in I$, alors

$$\varphi(a) = \frac{a}{1} = \frac{a}{s} \frac{s}{1}$$

donc il existe $f_1, \dots, f_r \in A$ tq $a = \sum f_i P_i \in A$. Et donc

$$\frac{a}{s} = \sum \frac{f_i}{s} \frac{P_i}{1}$$

et donc $a/s \in (P_1/1, \dots, P_r/1)$. □

|| **Corollaire 3.4.1.** *Soit V une variété algébrique. Alors $k[V]_a$ est un anneau noethérien.*

Démonstration. $k[V]$ est noethérien, donc $k[V]_a$ est noethérien comme localisation de $k[V]$. □

|| **Lemme 3.4.1.** (Nakayama) *(A, \mathfrak{m}) anneau local noethérien, et M un A -module de type fini. Si $\mathfrak{m}M = M$, alors $M = 0$.*

Démonstration. Référence □

|| **Corollaire 3.4.2.** $\mathfrak{m}^i/\mathfrak{m}^{i+1} = 0 \iff \mathfrak{m}^i = 0$. En particulier, $\mathfrak{m}/\mathfrak{m}^2 = 0 \iff \mathfrak{m} = 0 \iff A$ est un corps.

Démonstration. Comme $\mathfrak{m}^i/\mathfrak{m}^{i+1} = 0$, on a $\mathfrak{m}\mathfrak{m}^i = \mathfrak{m}^{i+1} = \mathfrak{m}^i$ et donc $\mathfrak{m}^i = 0$ d'après le lemme de Nakayama. □

Rq 3.4.3. Soit (A, \mathfrak{m}) un anneau local noethérien. $\mathfrak{m}/\mathfrak{m}^2$ est un A -module, mais aussi un k -ev où $k = A/\mathfrak{m}$ de type fini (en tant que A -module et en tant que k -ev)

|| **Théorème 3.4.1.** *(A, \mathfrak{m}) anneau local noethérien, $k = A/\mathfrak{m}$. Alors*

$$\dim_k \mathfrak{m}/\mathfrak{m}^2 \geq \dim A$$

où $\dim A$ est la dimension de krull de A . De plus, si on a égalité (on note $d = \dim A$),

|| alors $\mathfrak{m} = (x_1, \dots, x_d)$ avec $x_i \in A$, et on dit que (A, \mathfrak{m}) est un anneau régulier.

Démonstration. **Référence**

□

3.4.3 Espace tangent de Zariski

Soit V une variété affine, $a \in V$. Comme $k[V]_a$ est la localisation de $k[V]$ en l'idéal maximal $\mathfrak{m}_a/I(V)$. C'est donc un anneau local d'idéal maximal noté \mathfrak{m} .

Exercice. Considérons le morphisme

$$\begin{aligned} ev_a : k[V]_a &\rightarrow k \\ \alpha &\mapsto ev_a(\alpha) = \alpha(a) \end{aligned}$$

Alors $\ker(ev) = \mathfrak{m}$ est l'unique idéal maximal de $k[V]_a$, et $k[V]_a/\mathfrak{m} \simeq k$. Notons \mathfrak{n} l'idéal maximal de $k[V]_a$. Alors soit $p/q \in \mathfrak{n}$, alors $p(a)/q(a) = 0$ puisque $p \in \mathfrak{m}_a/I(V) =: \mathfrak{p}$. Réciproquement, si $p/q \in \ker ev_a$, alors $p(a)/q(a) = 0$, et donc $p(a) = 0$, ce qui veut dire que $p \in \mathfrak{m}_a/I(V)$ et donc $p/s \in \mathfrak{n}$. Finalement $k \simeq k[V]_a/\ker ev_a \simeq k[V]_a/\mathfrak{m}$

Définition 3.4.2. $V \subseteq \mathbb{A}^n$ variété affine, $a \in V$. Soit $A = k[V]_a$ l'anneau local associé à a . L'espace tangent de V en a est le k -ev

$$T_a V := (\mathfrak{m}/\mathfrak{m}^2)^\vee := \mathbf{Hom}_k(\mathfrak{m}/\mathfrak{m}^2, k)$$

l'espace tangent à V en a .

Rq 3.4.4. $\mathfrak{m}_a/\mathfrak{m}_a^2 \simeq M_a/M_a^2$ (isomorphisme de k -espaces vectoriels), où $M_a = \ker(ev_a : k[V] \rightarrow k) \stackrel{\text{id}}{\subseteq} k[V]$.
Pas si facile ...

|| **Théorème 3.4.2.** $\dim k[V] = \dim k[V]_a$

Donc (A, \mathfrak{m}) est régulier ssi $\dim V = \dim A = \dim_k \mathfrak{m}/\mathfrak{m}^2 = \dim_k T_a V$. On va montrer que (A, \mathfrak{m}) est régulier si et seulement si $a \in V$ est régulier.

|| **Théorème 3.4.3.** $\dim_k T_a V \geq \dim V$ avec égalité si et seulement si $a \in V$ est un point régulier.

Pour montrer ce théorème, nous devons parler d'espace tangent géométrique.

3.4.4 Espace tangent géométrique

Soit $V = V(P_1, \dots, P_r) \subseteq \mathbb{A}^n$, avec $P_1, \dots, P_r \in k[X_1, \dots, X_n]$, et $a \in V$.

Définition 3.4.3. (Espace tangent géométrique) L'espace tangent géométrique de V en a est défini comme

$$T_a^{\text{geom}}V = V(P_1^1, \dots, P_r^1) \subseteq \mathbb{A}^n$$

où

$$P_i^1 = \sum_{j=1}^n \frac{\partial P_i}{\partial X_j}(a)(X_j - a_j)$$

Rq 3.4.5. Soit $P \in k[X_1, \dots, X_n]$, on peut décomposer P en $P = \sum_{i=0}^d P^i$ où les P^i sont des polynômes homogènes de degré i (tous les monômes sont de la forme X^α avec $|\alpha| = i$) en réalisant l'expansion de Taylor de P en 0. Ainsi,

$$P^1 = \sum_{j=1}^n \frac{\partial P}{\partial X_j}(0)X_j$$

Maintenant si $a \in \mathbb{A}^n$, alors on peut réaliser l'expansion de Taylor de P en a , $P = \sum P^i$, et alors

$$P^1 = \sum_{j=1}^n \frac{\partial P}{\partial X_j}(a)(X_j - a_j)$$

Ex 3.4.2. 1. Soit $V = \{(x, y) \mid y^2 = x\} \subseteq \mathbb{A}^2$. Alors $V = V(P)$ avec $P = Y^2 - X$. Alors soit $a = (a_1, \dots, a_2) \in V$ (donc $a_2^2 = a_1$), on a

$$\begin{aligned} \frac{\partial P}{\partial X} &= -1 \\ \frac{\partial P}{\partial Y} &= 2Y \end{aligned}$$

On a donc

$$T_a^{\text{geom}} = V(-(X - a_1) + 2a_2(Y - a_2))$$

est la droite tangente au point (a_1, a_2) , qui est isomorphe à k . En effet, $\dim T_a^{\text{geom}} = 1$ (c'est le translaté d'un sous-espace de k^2 de dimension 1). De même, $\dim V = 1$ vu que $k[V] = k[Y]$, puis V est lisse donc tout point est régulier.

2. Cas particulier : $a = (0, 0)$, alors $T_a^{\text{geom}}V = V(x)$. Maintenant $k[V] \simeq k[X]$, et $k[V]_a = k[x, y]_{(x, y)} \simeq k[x]/(x)$. Finalement, $\mathfrak{m} = (X/1)$ et donc $\dim_k \mathfrak{m}/\mathfrak{m}^2 = 1$ ($X/1$ est une base de ce k -ev). Ainsi $\dim T_a V = 1$ en 0.

Soit $a \in V$, considérons l'application

$$\begin{aligned} \tau_a : \mathbb{A}^n &\rightarrow \mathbb{A}^n \\ x &\mapsto x - a \end{aligned}$$

C'est un isomorphisme, et alors on peut considérer l'image par τ_a de $T_a^{\text{geom}}V$. Elle est alors munie d'une structure canonique d'espace vectoriel. Alors on a les deux résultats suivants :

|| **Théorème 3.4.4.** *Pour tout $a \in V$,*

$$\tau_a(T_a^{\text{geom}}V) \simeq T_aV$$

|| **Théorème 3.4.5.** *Pour tout $a \in V$,*

$$\dim T_a^{\text{geom}}V = n - \text{rk} d\varphi(a)$$

Ces deux théorèmes permettent de faire le lien entre les deux notions d'espace tangent, ainsi qu'entre leur dimension et la notion de point régulier. Nous résumons cela dans le corollaire suivant :

|| **Corollaire 3.4.3.** *Soit $a \in V$. Alors $\dim T_aV = \dim T_a^{\text{geom}}V \geq d$, avec égalité si et seulement si a est un point régulier.*

Démonstration. (3.4.3) Ce résultat découle directement du fait que $\text{rk} d\varphi(a) \leq n - d$, avec égalité si et seulement si a est régulier, par définition. \square

Avant de prouver les deux théorèmes précédents, vérifions les sur un exemple :

Ex 3.4.3. $k = \bar{k}$, $\text{char} k = 0$. Soit $V = V(Y^2 - X^3) \subseteq \mathbb{A}^2$, on a $\dim V = 1$. Ainsi

$$\begin{aligned} \frac{\partial P}{\partial X} &= -3X^2 \\ \frac{\partial P}{\partial Y} &= 2Y \end{aligned}$$

Alors $(a, b) \in V$ est singulier si et seulement si $(a, b) = 0$. Maintenant soit $(a, b) \in V$, alors

$$T_a^{\text{geom}}V = \{(x, y) \in \mathbb{A}^2 \mid -3a^2(x - a) + 2b(Y - b) = 0\}$$

droite dans \mathbb{A}^2 si $(a, b) \neq 0$. Si $(a, b) = 0$, alors $T_0^{\text{geom}}V = \mathbb{A}^2$ est de dimension 2. On peut aussi calculer l'espace tangent de Zariski :

$$\begin{aligned} K[V]_{(a,b)} &= (k[X, Y]/(Y^2 - X^3))_{(X-a, Y-b)} \\ &= k[x, y]_{(x-a, y-b)} \\ &= \left\{ \frac{P}{Q} \mid P, Q \in k[x, y], Q(a, b) \neq 0 \right\} \end{aligned}$$

Alors on peut voir que $\mathfrak{m}_{(a,b)} = (x-a, y-b) \subseteq K[V]_{(a,b)}$. Maintenant $(x-a, y-b)$ engendre $\mathfrak{m}/\mathfrak{m}^2$ en tant que k -ev, donc $\dim_k \mathfrak{m}/\mathfrak{m}^2 \leq 2$. Maintenant si $(a, b) \neq 0$, alors $\{x-a, y-b\}$ n'est pas libre modulo \mathfrak{m}^2 : en effet, dans $k[x, y]$,

$$3a^2(x-a) - 2b(y-b) = (y-b)^2 - 3a(x-a)^2 - (x-a)^3 \in \mathfrak{m}^2$$

et $3a, 2b \neq 0, 0$. Maintenant, si $(a, b) = 0$, alors $\mathfrak{m} := \mathfrak{m}_0 = (x, y)$, montrons que $\{x, y\}$ est libre sur k modulo \mathfrak{m}^2 . Soient $\alpha, \beta \in k$ tels que $\alpha x + \beta y = 0 \pmod{\mathfrak{m}^2}$. Ainsi $\alpha x + \beta y \in \mathfrak{m}^2 \subseteq k[V]_0$, et donc il existe $P_i/Q_i \in k[V]_0$ avec

$$\alpha x + \beta y = \frac{P_1}{Q_1}x^2 + \frac{P_2}{Q_2}xy + \frac{P_3}{Q_3}y^2$$

dans $k[V]_0$. Maintenant $Q_i(0) \neq 0$, donc $\exists Q \in k[x, y]$ tel que $Q(0) \neq 0$ et $Q(\alpha x + \beta y) \in (x^2, xy, y^2)$ dans $k[x, y]$ cette fois. Ainsi $\exists R_i \in k[x, y]$ tels que

$$Q(X, Y)(\alpha X + \beta Y) - R_1X^2 - R_2XY - R_3Y^2 \in I(V) = (Y^2 - X^3)$$

dans $k[X, Y]$. Ainsi $Q(X, Y)(\alpha X + \beta Y) \in (X^2, XY, Y^2)$ car $Y^2 - X^3 \in (X^2, XY, Y^2)$. Remarquons qu'en général, si $P \in k[X_1, \dots, X_n]$, alors $P^0 = 0 \iff P \in (X_1, \dots, X_n)$, $P^0 = P^1 = 0 \iff P \in (X_1, \dots, X_n)^2$. Mais alors Q a un terme constant car $Q(0) = 0$, et donc le terme linéaire de $Q(\alpha X + \beta Y)$ doit être $Q^0(\alpha X + \beta Y)$ et doit être 0 car $Q(\alpha X + \beta Y) \in (X, Y)^2$. Ainsi $Q^0\alpha, Q^0\beta = 0 \in k$ et donc $\alpha, \beta = 0$ ce qui prouve la liberté de $\{x, y\}$.

Soit $a \in V$, notons

$$H_a := \{x \in \mathbb{A}^n \mid \sum \alpha^j(x_j - a_j) = 0\} \subseteq \mathbb{A}^2$$

Remarquons alors que $a \in H_a$. Alors on a

$$\tau_a(H_a) = \{z \in \mathbb{A}^n \mid \sum \alpha^j z_j = 0\} \subseteq \mathbb{A}^n$$

et c'est un sev de k^n . Ainsi

$$\tau_a(T_a^{\text{geom}}V) = \{z \in k^n \mid \forall i \in \llbracket 1, r \rrbracket, \sum_j \frac{\partial P_i}{\partial X_j}(a) z_j = 0\}$$

Si $V = V(P_1, \dots, P_r)$. C'est le noyau de l'application $k^n \rightarrow k^r$ correspondant à la matrice jacobienne $d\varphi(a)$, et ainsi $\dim T_a^{\text{geom}} V = n - rk d\varphi(a)$.

Montrons maintenant que $\tau_a(T_a^{\text{geom}} V) \simeq T_a V$ en tant que k -ev. On peut supposer que $a = 0 \in \mathbb{A}_k^n$, montrons que

$$\mathbf{Hom}_k(T_a^{\text{geom}} V, k) \simeq \mathfrak{m}/\mathfrak{m}^2$$

On note $x_i = [X_i] \in k[V]$, $M = (x_1, \dots, x_n)$. D'après la remarque 3.4.4, prouver le point précédent revient à prouver qu'il existe un isomorphisme

$$M/M^2 \simeq \mathbf{Hom}_k(T_a^{\text{geom}} V, k)$$

(rappelons que la remarque prouve que $M/M^2 \simeq \mathfrak{m}/\mathfrak{m}^2$) Notons ainsi $V = V(P_1, \dots, P_r)$, $W := T_a^{\text{geom}} V$. Comme $a = 0 \in V$, alors $P_i(0) = 0$ pour tout i . Alors soit

$$\begin{aligned} \varphi : M &\rightarrow \mathbf{Hom}_k(W, k) \\ [P] &\mapsto P|_W : x \in W \mapsto P^1(x) \in k \end{aligned}$$

1. Montrons que φ est bien définie : soient $P, Q \in k[X_1, \dots, X_n]$ tels que $[P] = [Q]$, alors $P - Q \in I(V)$. Mais écrivons $P, Q = P^1, Q^1 + \dots + P^d, Q^e$ avec P^i, Q^j homogènes. Alors $P - Q = (P^1 - Q^1) + \dots$ et $(P - Q)^1 = P^1 - Q^1$. Maintenant $P - Q \in I(V) \Rightarrow P^1 - Q^1 \in I(W)$ et donc $P^1 - Q^1$ est nul sur W . Précisons l'implication précédente : si $R \in I(V)$, alors $R^1 \in I(W)$. EN effet, écrivons $R = \sum P_i Q_i$, puis écrivons $P_i = P_i^1 + P_i^2 + \dots$, $Q_i = Q_i^0 + Q_i^1 + \dots$. Mais alors $(P_i Q_i)^1 = P_i^1 Q_i^0$ donc $R^1 = \sum P_i^1 Q_i^0 \in I(W)$.
2. Montrons que φ est surjective. Soit $f : W \rightarrow k$ k -linéaire. Alors $\exists \tilde{f} : k^n \rightarrow k$ k -linéaire telle que $\tilde{f}|_W = f$, puis

$$\tilde{f}(x) = \sum \alpha_i x_i$$

Ainsi $\varphi([\sum \alpha_i X_i]) = \tilde{f}|_W = f$.

3. Montrons que $\ker \varphi = M^2$: **flemme**

Chapitre 4

Courbes algébriques affines

4.1 Rappels d'algèbre commutative

Soit k corps algébriquement clos. Une courbe est une variété affine de dimension 1. $a \in C$ dans une courbe est régulier ssi $\dim \mathfrak{m}_a / \mathfrak{m}_a^2 = 1$.

|| **Définition 4.1.1.** Un anneau de valuation discrète (DVR, Discrete Valuation Ring) est un anneau local (A, \mathfrak{m}) tel que A intègre et principal, mais n'est pas un corps.

En particulier, un tel anneau est

1. Noethérien, car principal,
2. $\mathfrak{m} = (t)$ (on appelle $t \in A$ une uniformisante). Un tel t est irréductible (car \mathfrak{m} est un idéal premier et A un anneau principal).
3. Factoriel, car principal,
4. $\dim A = 1$, car principal.

|| **Proposition 4.1.1.** Soit (A, \mathfrak{m}) un DVR, notons $K = \text{Frac} A$ et $\mathfrak{m} = (t)$, $t \in A$.

1. Les idéaux non nuls de A sont les $\mathfrak{m}^i = (t^i)$, $i \in \mathbb{N}$.
2. $\bigcap_{i \geq 0} \mathfrak{m}^i = \{0\}$
3. $\forall x \in K \setminus \{0\}$, $\exists ! n \in \mathbb{Z}$ tel que $x = t^n u$, $u \in A^\times$ et l'application

$$\begin{aligned} v : K \setminus \{0\} &\rightarrow \mathbb{Z} \\ x &\mapsto v(x) = n \end{aligned}$$

satisfait

$$\begin{cases} v(xy) = v(x) + v(y) \\ v(x+y) \geq \min\{v(x), v(y)\} \end{cases}$$

(v est une valuation sur K)

De plus,

$$\begin{aligned} A &= \{x \in K \setminus \{0\} \mid v(x) \geq 0\} \cup \{0\} \\ \mathfrak{m} &= \{x \in K \setminus \{0\} \mid v(x) > 0\} \cup \{0\} \end{aligned}$$

Exercice. Si $v : K \setminus 0 \rightarrow \mathbb{Z}$ est une valuation d'un corps K , alors $A = \{x \in K \setminus 0 \mid v(x) \geq 0\} \cup \{0\}$ est un DVR d'idéal maximal $\mathfrak{m} = \{x \in K \setminus 0 \mid v(x) > 0\} \cup \{0\}$. **Pas fait**

Démonstration. 1. A factoriel, t irréductible. Pour tout $x \in A \setminus 0$, $\exists N \geq 0$ maximal avec la propriété que $t^N \mid x$ dans A . Alors $x = t^N y$, $y \in A^\times$ (vu que A est local donc $A^\times = A \setminus \mathfrak{m}$, et N est maximal). Maintenant soit $I \subseteq A$ idéal, alors $\exists x \in A$ non nul tq $I = (x)$; Alors on a que $x = t^N y$ avec $y \in A^\times$, et donc $I = (t^N)$.

2. On a $0 \subseteq \mathfrak{m}^i \not\subseteq \mathfrak{m}^{i-1} \subseteq A$. Alors soit $x \in \bigcap_{\mathbb{N}} \mathfrak{m}^i$ non nul, on a $x = t^N y$ pour un N maximal, $y \in A^\times$. Mais $x \in \mathfrak{m}^{N+1}$ donc $t^{N+1} \mid t^N y$ absurde.

3. Soit $x \in K \setminus 0$. Alors $x = y/z$, $y, z \in A$ et $z \neq 0$. Alors $\exists N, M \in \mathbb{N}$ t.q. $y = t^N u$, $z = t^M v$ avec $u, v \in A^\times$. Ainsi $x = t^{N-M} (uv^{-1})$. Maintenant vérifions que la valuation est bien définie : si $x = t^i u = t^j v$, alors ops $i > j$ et alors $t^{i-j} \in A^\times$, absurde. Anis $i = j$ et $u = v$. Il est finalement facile de voir que v est une valuation. \square

4.2 Régularité des courbes algébriques

Dans l'objectif de caractériser les points réguliers d'une courbe, ainsi que la propriété d'être lisse, faisons quelques rappels d'algèbre commutative :

Définition 4.2.1. (Entiers sur un anneau, anneau intégralement clos dans son corps des fractions) A anneau intègre, $K = \text{Frac} A$. Alors

1. $x \in K$ est entier sur A s'il existe $P \in A[X]$ unitaire tel que $P(x) = 0$ (dans K).
2. A intégralement clos dans K si $x \in K$ entier sur A implique que $x \in A$.

Ex 4.2.1. 1. \mathbb{Z} est intégralement clos dans \mathbb{Q} .
2. $\mathbb{Z}[i]$ est intégralement clos dans \mathbb{Q} .

3. $A = k[X, Y]/(Y^2 - X^3) = k[x, y]$ n'est pas intégralement clos. Par exemple, y/x est entier sur A car $(y/x)^2 - x = 0$ mais pas dans A .

|| **Théorème 4.2.1.** *Soit A un anneau intègre. Alors A est intégralement clos si et seulement si $A_{\mathfrak{p}}$ est intégralement clos, pour tout $\mathfrak{p} \subseteq A$.*

Démonstration. **Reference** □

|| **Théorème 4.2.2.** *Soit A un anneau local intègre, tel que $\dim A = 1$. Alors A est intégralement clos si et seulement si A est un DVR.*

Démonstration. **Référence** □

|| **Définition 4.2.2.** *Un anneau de Dedekind est intègre, noeth, intégralement clos, de dimension 1.*

Ex 4.2.2. $\mathbb{Z}, \mathbb{Z}[i], k[C]$ pour C une courbe lisse.

Maintenant remarquons que

|| **Théorème 4.2.3.** *C courbe, $a \in C$. Alors $a \in C$ est un point régulier ssi $k[C]_a$ est un DVR.*

Démonstration. **A voir** □

|| **Théorème 4.2.4.** *C courbe affine. C est lisse si et seulement si $k[C]$ est intégralement clos dans $k(C)$.*

Démonstration. C lisse $\iff \forall a \in C, k[C]_a$ est un DVR $\iff \forall a \in C, k[C]_a$ est intégralement clos. Maintenant, si $k[C]$ est intégralement clos, alors toutes les localisations de $k[C]$ en un idéal premier sont des anneaux intégralement clos, et en particulier les localisations $k[C]_a$, pour tout $a \in C$. Réciproquement, **Je sais pas haha.** □

|| **Théorème 4.2.5.** *C courbe affine.*

$$\text{Sing}(C) = \{a \in C \mid a \text{ singulier}\}$$

|| *est un ensemble propre de C*

Démonstration. **A voir** □

Exercice. $\text{Sing}(C)$ est un sous-ensemble algébrique.

|| **Proposition 4.2.1.** *Soit C une courbe affine. Les sous-ensembles propres de C sont finis.*

Démonstration. Soit $V \subseteq C \subseteq \mathbb{A}^n$ ensemble algébrique propre. Ops V irréductible (sinon on considère une composante de V). Alors $V \subsetneq C$ implique que $I(C) \subsetneq I(V) \subseteq k[X_1, \dots, X_n]$. Montrons que $I(V) = \mathfrak{m}_a$, $a \in \mathbb{A}^n$. Maintenant

$$0 \subseteq I(V)/I(C) \subseteq k[C]$$

est un idéal premier. Mais $\dim k[C] = 1$, donc $I(V)/I(C)$ est maximal, donc $I(V)$ maximal. Ainsi $I(V) = \mathfrak{m}_a$ car $k = \bar{k}$, donc V doit être un point. \square

|| **Corollaire 4.2.1.** *Soit C une courbe algébrique, alors $|\text{Sing}(C)| < \infty$*

Chapitre 5

Géométrie projective

5.1 Ensembles algébriques projectifs

Soit k un corps, V un k espace vectoriel tel que $1 \leq \dim V < \infty$.

|| **Définition 5.1.1.** L'espace projectif de V est donné par

$$\mathbb{P}(V) := \{L \subseteq V \mid \dim L = 1\}$$

Il est possible de représenter $\mathbb{P}(k^{n+1}) := \mathbb{P}_k^n$ de manière un peu plus explicite : considérons la relation d'équivalence sur $k^{n+1} \setminus \{0\}$ suivante :

$$x \sim y \iff \exists \lambda \in k \setminus \{0\} \mid x = \lambda y$$

Alors $\mathbb{P}_k^n \simeq k^{n+1} \setminus \{0\} / \sim$ (en tant qu'ensembles), via l'application

$$\begin{aligned} k^{n+1} / \sim &\rightarrow \mathbb{P}_k^n \\ [x_0, \dots, x_n] &\mapsto \text{vect}((x_0, \dots, x_n)) \end{aligned}$$

Ex 5.1.1. 1. Si $n = 1$, alors on $\mathbb{P}_k^1 = \{[x_0, x_1] \mid x_0 \neq 0 \text{ ou } x_1 \neq 0\}$. Remarquons alors que l'on dispose d'une application

$$\begin{aligned} \mathbb{A}^1 &\rightarrow \mathbb{P}^1 \\ x &\mapsto [1, 0] \end{aligned}$$

qui est injective et d'image $\mathbb{P}^1 \setminus \{[0, 1]\}$. On appelle souvent $[1, 0]$ le point à l'infini de \mathbb{P}^1 , noté $[1, 0] = \infty$, du fait que $\mathbb{P}^1 = \mathbb{A}^1 \cup \{\infty\}$ si on identifie \mathbb{A}^1 et l'image de l'application précédemment définie. On a en quelque sorte rajouté un point à \mathbb{A}^1 pour construire \mathbb{P}^1 .

2. Si $n = 2$, $\mathbb{P}_k^2 = \{[x, y, z] \mid x \neq 0 \vee y \neq 0 \vee z \neq 0\}$. Comme précédemment, on dispose d'une application injective

$$\begin{aligned} \mathbb{A}^2 &\rightarrow \mathbb{P}^2 \\ (x, y) &\mapsto [x, y, 1] \end{aligned}$$

et si on identifie l'image de cette application avec \mathbb{A}^2 , alors

$$\mathbb{P}^2 = \mathbb{A}^2 \cup \{[x, y, 0] \mid x \neq 0 \vee y \neq 0\} = \mathbb{A}^2 \cup \mathcal{D}$$

où \mathcal{D} est appelée droite à l'infini.

3. Plus généralement, on dispose pour tout $i \in \llbracket 0, n \rrbracket$ d'une application injective

$$\begin{aligned} u_i : \mathbb{A}^n &\rightarrow \mathbb{P}^n \\ (x_1, \dots, x_n) &\mapsto [x_1, \dots, x_{i-1}, 1, x_i, \dots, x_n] \end{aligned}$$

et alors $\mathbb{P}^n \setminus u_i(\mathbb{A}^n) = \{[x_1, \dots, x_i, 0, x_{i+1}, \dots, x_n]\}$. Si $i = 0$, on appelle cet ensemble hyperplan à l'infini.

Rq 5.1.1. Pour tout $F \in k[X_0, \dots, X_n]$, on peut décomposer F comme $F = \sum F^i$ où les F^i sont homogènes de degré i . Alors dans ce cas soit $[a] \in \mathbb{P}^n$, on a $F(\lambda a) = 0$ pour tout $\lambda \in k^\times$ si et seulement si $F^i(a) = 0$ pour tout i . On écrit cette condition $F([a]) = 0$. **Vrai que si le corps est infini ? Si le corps est infini, ça paraît vrai au vu de la gueule qu'un déterminant de vandermonde a**

Définition 5.1.2. (Ensemble algébrique projectif) Soit $S \subseteq k[X_0, \dots, X_n]$. On définit

$$\begin{aligned} V(S) &:= \{[a] \in \mathbb{P}^n \mid \forall F \in S, F([a]) = 0\} \\ &= \{[a] \in \mathbb{P}^n \mid \forall F = \sum F^i \in S, F^i(a) = 0 \forall i\} \end{aligned}$$

Rq 5.1.2. Si $\tilde{S} = \{F^i \mid F \in S, F = \sum F^i\}$, alors $V(S) = V(\tilde{S})$. Remarquons que \tilde{S} ne contient que des polynômes homogènes, ainsi on peut toujours considérer des ensembles de polynômes homogènes pour définir un $V(S)$.

Ex 5.1.2. Soit $F \in k[X_0, \dots, X_n]$ un polynôme homogène de degré $d > 0$. Alors dans ce cas

$$V(F) = \{[a] \in \mathbb{P}^n \mid F(a) = 0\}$$

On appelle un tel ensemble algébrique projectif une hypersurface de degré d . En particulier, si $d = 1$, en notant $F = \sum c_i X_i$, on obtiens que $V(F) = \{[a] \in \mathbb{P}^n \mid \sum c_i a_i = 0\}$. On appelle un tel ensemble un hyperplan. Si $n = 2$, ça correspond à de "droites".

Exercice. Pour tous $L_1, L_2 \subseteq \mathbb{P}^2$ droites telles que $L_1 \neq L_2$, alors $L_1 \cap L_2$ est un point.

Rq 5.1.3. Soit $f \in k[X_1, \dots, X_n]$ que l'on décompose en homogènes $f = f_0 + \dots + f_d$. Alors $F = X_0^d f_0 + \dots + X_0 f_{d-1} + f_d \in k[X_0, \dots, X_n]$ (dit homogénéisation de f en X_0) est un polynôme homogène de degré d , et alors $F(1, X_1, \dots, X_n) = f(X_1, \dots, X_n)$.

Notation. 1. $\mathcal{U}_i = \{[x_0, \dots, x_n] \mid x_i \neq 0\} \subseteq \mathbb{P}^n$. Ainsi on a $\mathbb{P}^n = \bigcup_{i=0}^n \mathcal{U}_i$.

2. L'image du morphisme $u_i : \mathbb{A}^n \rightarrow \mathbb{P}^n$ définit précédemment est exactement \mathcal{U}_i . En effet, si $[x_0, \dots, x_n] \in \mathcal{U}_i$, alors $x_i \neq 0$, et ainsi

$$[x_0, \dots, x_n] = [x_0/x_i, \dots, x_{i-1}/x_i, 1, x_{i+1}/x_i, \dots, x_n/x_i]$$

qui est bien dans l'image de u_i .

Observons que si $F \in k[X_0, \dots, X_n]$ est homogène de degré d , alors u_0 induit une bijection entre $V(f)$ et $V(F) \cap \mathcal{U}_0$, où $f(X_1, \dots, X_n) = F(1, X_1, \dots, X_n) \in k[X_1, \dots, X_n]$. En effet,

$$\begin{aligned} V(F) \cap \mathcal{U}_0 &= \{[a] \in \mathbb{P}^n \mid F(a) = 0 \wedge a_0 \neq 0\} \\ &= \{[1, b_1, \dots, b_n] \in \mathbb{P}^n \mid F(1, b_1, \dots, b_n) = 0\} \\ &= \{[1, b_1, \dots, b_n] \in \mathbb{P}^n \mid f(b_1, \dots, b_n) = 0\} \\ &= u_0(V(f)) \end{aligned}$$

Plus généralement, si $S \subseteq k[X_1, \dots, X_n]$, notons $\tilde{S} = \{X_0^d f_0 + \dots + f_d \in k[X_0, \dots, X_n] \mid f \in S\}$. Alors on a $V(\tilde{S}) \cap \mathcal{U}_0 = u_0(V(S))$.

5.2 Topologie de Zariski sur \mathbb{P}^n et ses sous-ensembles algébriques projectifs

|| **Définition 5.2.1.** Les fermés de la topologie de Zariski sur \mathbb{P}^n sont les $V(S)$, $S \subseteq k[X_0, \dots, X_n]$. Soit $T \subseteq k[X_0, \dots, X_n]$, les fermés de la topologie de Zariski sur $V(T)$ sont les $V(S) \cap V(T)$, pour $S \subseteq k[X_0, \dots, X_n]$ (topologie induite).

Rq 5.2.1. Une manière équivalente de définir la topologie de Zariski sur $V(T)$, pour $T \subseteq k[X_0, \dots, X_n]$ est de prendre les $V(E)$, $E \subseteq k[X_0, \dots, X_n]$ tels que $V(E) \subseteq V(T)$.

|| **Proposition 5.2.1.** Soit $T \subseteq k[X_0, \dots, X_n]$ un ensemble de polynômes homogènes. Alors $V(T) = V((T))$

|| **Définition 5.2.2.** (Idéal homogène) Soit $I \subseteq k[X_0, \dots, X_n]$. I est un idéal homogène si pour tout $F \in I$ décomposé de manière unique en homogènes comme $F = \sum F^i$, alors $F^i \in I$.

Ex 5.2.1. 1. L'idéal $(Y^2 - X^3) \subseteq k[X, Y]$ n'est pas homogène. En effet, $X^3 \notin I$.
 2. L'idéal $(Y^2 + X^2, Y^3 - XZ^2)$ est homogène, d'après le point suivant :
 3. Si $T \subseteq k[X_0, \dots, X_n]$ est un ensemble de polynômes homogènes, alors (T) est un idéal homogène. En effet, soit $P \in (T)$, alors on peut écrire $P = \sum Q_i T_i$ où $Q_i \in k[X_0, \dots, X_n]$ et $T_i \in T$. Mais si on décompose les $Q_i = \sum a_\alpha X^\alpha$, et alors $P = \sum \sum a_\alpha^i T_i X^\alpha$. Les P^k sont donc des sommes de $a_\alpha^i T_i X^\alpha$ où $|\alpha| + \deg T_i = k$, et sont donc des éléments de (T) .

|| **Proposition 5.2.2.** 1. $V(\emptyset) = \mathbb{P}^n$,
 2. $V(1) = \emptyset$,
 3. $V(I) \cup V(J) = V(IJ)$, $\forall I, J \subseteq k[X_0, \dots, X_n]$ idéaux homogènes,
 4.

$$\bigcap_{i \in I} V(I_i) = V\left(\bigcup_{i \in I} I_i\right)$$

|| **Définition 5.2.3.** (Variété projective) On appelle variété projective un ensemble algébrique projectif.

|| **Définition 5.2.4.** Soit $E \subseteq \mathbb{P}^n$. On définit

$$I(E) := (\{F \in k[X_0, \dots, X_n] \text{ homogène} \mid F(a) = 0, \forall a \in E\})$$

Exercice. $I(E)$ est un idéal homogène radical. $I(\emptyset) = k[X_0, \dots, X_n]$, et si $E \neq \emptyset$, alors $I(E) \subseteq (X_0, \dots, X_n)$.

|| **Proposition 5.2.3.** Soit $V \subseteq \mathbb{P}^n$ un ensemble algébrique projectif, alors $V(I(V)) = V$.

Démonstration. **Exercice** □

|| **Proposition 5.2.4.** Soit $V \subseteq \mathbb{P}^n$ un ensemble algébrique projectif, V est irréductible si et seulement si $I(V)$ est un idéal premier.

Démonstration.

$1 \Rightarrow 2$: Soient $f, g \in k[X_0, \dots, X_n]$ 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 $f \in I(V)$ ou $g \in I(V)$.

$2 \Rightarrow 1$: Soit $V \subseteq \mathbb{P}_k^n$ ensemble algébrique projectif 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 projectifs, 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 $f_1 \notin I(V)$. 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. \square

Théorème 5.2.1. (*Nullstellensatz projectif*) Soit $I \subseteq k[X_0, \dots, X_n]$ un idéal homogène, supposons que $k = \bar{k}$. Alors

- Si $V(I) \neq \emptyset$, alors $I(V(I)) = \sqrt{I}$,
- Sinon,

$$\begin{aligned} V(I) = \emptyset &\iff (X_0, \dots, X_n) \subseteq I \\ &\iff \sqrt{I} = (X_0, \dots, X_n) \vee \sqrt{I} = k[X_0, \dots, X_n] \end{aligned}$$

Exercice. Montrer que $I(\mathbb{P}^n) = 0$. Comme $\mathbb{P}^n = V(0)$, on a $I(\mathbb{P}^n) = I(V(0)) = \sqrt{(0)} = (0)$.

Corollaire 5.2.1. Supposons que k est algébriquement clos. Alors I et V induisent une correspondance bijective entre le ensemble projectifs de \mathbb{P}^n non vides et les idéaux homogènes radicaux $I \not\subseteq k[X_0, \dots, X_n]$ et $I \neq (X_0, \dots, X_n)$.

5.3 Lien entre géométrie affine et géométrie projective

5.3.1 Ensembles quasi-projectifs

Lemme 5.3.1. La bijection $u_i : \mathbb{A}^n \rightarrow \mathcal{U}_i \subseteq \mathbb{P}^n$ est un homéomorphisme pour la topologie de Zariski sur \mathbb{A}^n et la topologie de Zariski induite par \mathbb{P}^n induite sur \mathcal{U}_i .

Démonstration. Sans perte de généralité, supposons que $i = 0$. On a déjà montré que si $S \subseteq k[X_1, \dots, X_n]$, alors $u_0(V(S)) = V(\tilde{S}) \cap \mathcal{U}_0$, où \tilde{S} est l'ensemble des homogénéisés des éléments de S , puis pour tout $T \subseteq k[X_0, \dots, X_n]$, il existe $S \subseteq k[X_1, \dots, X_n]$ tel que $V(T) = V(\tilde{S})$, donc cette égalité prouve la continuité de l'application et de sa réciproque. \square

|| **Définition 5.3.1.** On appelle ensemble quasi-projectif un (ensemble homéomorphe à un) ouvert d'un ensemble algébrique projectif.

Rq 5.3.1. Les ensembles algébriques projectifs sont des ensembles quasi-projectifs. Les ensembles algébriques affines sont des ensembles quasi-projectifs, d'après le lemme 5.3.1.

|| **Définition 5.3.2.** Soient $U_1 \subseteq \mathbb{P}^n, U_2 \subseteq \mathbb{P}^l$ des ensembles quasi-projectifs. Une application $\varphi : U_1 \rightarrow U_2$ est un morphisme si pour tout $a \in \mathcal{U}_1$, $\exists \Omega_a \overset{\text{op}}{\subseteq} \mathcal{U}_1$ tel que $a \in \Omega_a$, et $\exists G_i, H_i \in k[X_0, \dots, X_n]$ des polynômes homogènes tels que $G_i(a) \neq 0$ et $\deg G_i = \deg H_i$ pour tout $0 \leq i \leq l$, et

$$\varphi(x) = \left[\frac{H_0}{G_0}, \dots, \frac{H_l}{G_l} \right]$$

|| pour tout $x \in \Omega_a$.

Exercice. 1. $u_0 : \mathbb{A}^n \rightarrow \mathcal{U}_0 \subset \mathbb{P}^n$ est un isomorphisme.
 2. $\varphi : \mathcal{U}_1 \rightarrow \mathcal{U}_2$ est un morphisme si et seulement si $\exists \{W_\alpha\}$ recouvrement ouvert de \mathcal{U}_2 tel que $\varphi|_{\varphi^{-1}(W_\alpha)} : \varphi^{-1}(W_\alpha) \rightarrow W_\alpha$ est un morphisme.

Ex 5.3.1. Considérons l'application

$$\begin{aligned} \varphi : \mathbb{P}^1 &\rightarrow \mathbb{P}^n \\ [u, v] &\mapsto [u^n, u^{n-1}v, \dots, uv^{n-1}, v^n] \end{aligned}$$

Alors φ est bien définie et est un morphisme. Considérons le recouvrement ouvert canonique $\mathcal{U}_0 \cup \mathcal{U}_1 = \mathbb{P}^1$. Alors pour tout $[u, v] \in \mathcal{U}_0$, $u \neq 0$ et ainsi

$$\varphi([u, v]) = \left[1, \frac{v}{u}, \frac{v^2}{u^2}, \dots, \frac{v^n}{u^n} \right]$$

et si $[u, v] \in \mathcal{U}_1$, $v \neq 0$ et alors

$$\varphi([u, v]) = \left[\frac{u^n}{v^n}, \dots, \frac{u^2}{v^2}, \frac{u}{v}, 1 \right]$$

ainsi φ est un morphisme.

Rq 5.3.2. Si $U_2 = k = \mathbb{A}^1 \subseteq \mathbb{P}^1$, alors un morphisme $f : U_1 \rightarrow k$ est appelé fonction régulière (projective). Alors par définition, une application $f : U_1 \rightarrow k$ est régulière si et seulement si pour tout $a \in \mathcal{U}$, $\exists \Omega_a \overset{\text{op}}{\subseteq} \mathcal{U}$ qui contient a , et $G, H \in k[X_0, \dots, X_n]$ homogènes de degré d tels que $f = H/G$ sur Ω_a et $G(a) \neq 0$.

|| **Proposition 5.3.1.** *Les morphismes sont continus pour la topologie de Zariski.*

Démonstration. Piéton (probablement ?) □

|| **Proposition 5.3.2.** *Soit $\varphi : U_1 \rightarrow U_2$ une application continue. Alors φ est un morphisme si et seulement si pour tout $W \subseteq U_2$ ouvert, et pour toute fonction régulière $f : W \rightarrow k$, alors $f \circ \varphi : \varphi^{-1}(W) \rightarrow k$ est une fonction régulière.*

Démonstration. Piéton □

|| **Proposition 5.3.3.** *Les morphismes sont stables par composition.*

Démonstration. Se déduit facilement de la proposition précédente. □

Il nous faut maintenant vérifier que si U_1 et U_2 sont homéomorphes à des ensembles algébriques affines, alors la notion de morphisme en tant qu'ensembles quasi-projectifs coïncide avec la notion de morphismes d'ensembles algébriques. Pour cela, on utilise le résultat suivant :

|| **Proposition 5.3.4.** *Soit $V \subseteq \mathbb{A}^n$ un ensemble algébrique affine, supposons que k est algébriquement clos. Alors $f : V \rightarrow k$ est régulière si et seulement si pour tout $a \in V$, $\exists \Omega_a \overset{\text{op}}{\subseteq} V$ tel que $a \in \Omega_a$ et $\exists g, h \in k[V]$, $g \neq 0$ sur Ω_a , tels que $f = h/g$ sur Ω_a (nous appelons cette dernière condition la condition (*)).*

Démonstration.

\Rightarrow : Par définition, il existe $P \in k[X_1, \dots, X_n]$ tel que $f(a) = P(a)$ sur V , donc pour $a \in V$, on prend $\Omega_a = V$ et $h = [P]$, $g = 1$.

\Leftarrow : Supposons dans un premier temps que V est irréductible, et que $f : V \rightarrow k$ vérifie (*). Considérons l'idéal $\mathcal{J} := \{g \in k[V] \mid gf \in k[V]\}$ de $k[V]$. Il suffit de montrer que $1 \in \mathcal{J}$ (en effet, si $1 \in \mathcal{J}$, alors $f \in k[V]$). Supposons le contraire, alors $\mathcal{J} \not\subseteq k[V]$ et donc d'après le théorème de Krull il existe un idéal maximal $M \subseteq k[V]$ contenant \mathcal{J} . Et d'après le Nullstellensatz ($k = \bar{k}$), $\exists a = (a_1, \dots, a_n) \in \mathbb{A}^n$ tel que

$$M = (x_1 - a_1, \dots, x_n - a_n) = (X_1 - a_1, \dots, X_n - a_n)/I(V)$$

On a donc $I(V) \subseteq (X_1 - a_1, \dots, X_n - a_n)$ et donc $a \in V(I(V)) = V$. Et comme $\mathcal{J} \subseteq (x_1 - a_1, \dots, x_n - a_n)$, pour tout $g \in \mathcal{J}$, $g(a) = 0$. Maintenant utilisons la condition : il existe $\Omega_a \subseteq V$ un ouvert tel que $a \in \Omega_a$ et $\exists P, Q \in k[X_1, \dots, X_n]$ avec $Q(a) \neq 0$ tels que $P(a) \neq 0$ et $f = [P]/[Q]$ sur Ω_a . Alors $[Q]f = [P]$ sur Ω_a , mais comme V est irréductible, Ω_a est dense et ainsi $[Q]f = [P]$ sur V , donc $[Q] \in \mathcal{J}$, absurde puisque $Q(a) \neq 0$.

Pour passer au cas réductible, remarquons que si $f : V \rightarrow k$ vérifie (*), alors f est continue (Exercice). Maintenant si V est réductible, notons $V = V_1 \cup V_2$, où les V_i sont des fermés de V . Par récurrence (sur le nombre de composantes irréductibles) et par le point précédent, on peut trouver $P, Q \in k[X_1, \dots, X_n]$ tels que pour tout $a \in V_1$, $f(a) = P(a)$ et pour tout $b \in V_2$, $f(a) = Q(a)$. Mais alors considérons $I_i = I(V_i)$, $i = 1, 2$, on a

$$I(V_1 \cap V_2) = \sqrt{I(V_1) + I(V_2)} = \sqrt{I(V_1)} + \sqrt{I(V_2)} = I(V_1) + I(V_2)$$

Maintenant $P = Q$ sur $V_1 \cap V_2$, donc $P - Q \in I_1 + I_2$, et ainsi il existe $R_1, R_2 \in I_1, I_2$ tels que $P - Q = R_1 + R_2$ dans $k[X_1, \dots, X_n]$. Définissons alors $R := P - R_1 = Q + R_2$, on a $R = P$ sur V_1 et $R = Q$ sur V_2 , donc finalement $f(a) = R(a)$ pour tout $a \in V$ et donc f est une fonction régulière. \square

On peut finalement prouver que

Proposition 5.3.5. *Soit $V, W \subseteq \mathbb{P}^n, \mathbb{P}^l$ des ensembles quasi-projectifs isomorphes à des ensembles algébriques affines, et $\varphi : V \rightarrow W$ une application. Alors φ est un morphisme d'ensembles algébriques affines si et seulement si c'est un morphisme d'ensembles quasi-projectifs (vus comme sous-ensembles de $\mathbb{P}^n, \mathbb{P}^l$).*

Démonstration. D'après le point précédent, une application $f : W \rightarrow k$ est régulière affine si et seulement si elle est régulière projective. Ainsi φ est un morphisme d'ensembles algébriques si et seulement si pour tout fonction régulière affine $f : W \rightarrow k$, $f \circ \varphi$ est régulière affine si et seulement si pour toute fonction régulière projective $f : W \rightarrow k$, $f \circ \varphi$ est régulière projective si et seulement si φ est un morphisme d'ensembles projectifs. \square

Cela nous permet finalement de définir une catégorie des ensembles quasi-projectifs, dont les objets sont les ensembles quasi-projectifs et les morphismes sont les morphismes d'ensembles quasi-projectifs. Remarquons que la dernière vérification que nous avons faite nous permet de voir la catégorie des ensembles algébriques affines comme une sous-catégorie pleine de cette nouvelle catégorie.

5.3.2 Variétés

Définition 5.3.3. Une variété est un ensemble algébrique quasi-projectif irréductible. Si V est une variété, on définit le corps des fractions rationnelles de V comme

$$k(V) = \{(U, f) \mid U \overset{\text{ouv}}{\subseteq} V, f : U \rightarrow k \text{ fonction régulière}\} / \sim$$

Où $(U, f) \sim (U', f') \iff f = f'$ sur $U \cap U'$ (c'est une relation d'équivalence).

Rq 5.3.3. $k(V)$ est muni d'une structure canonique de corps : les opérations sont

$$\begin{aligned} (U, f) + (U', f') &= (U \cap U', f + f') \\ (U, f)(U', f') &= (U \cap U', ff') \\ (V, 0) &= 0 \\ (V, 1) &= 1 \\ (U, f)^{-1} &= (U \cap D(f), 1/f) \text{ si } (U, f) \neq (V, 0) \end{aligned}$$

Rq 5.3.4. Si V est une variété, et $W \subseteq V$ un ouvert non vide, alors

$$\begin{aligned} k(V) &\rightarrow k(W) \\ (U, f) &\mapsto (U \cap W, f|_{U \cap W}) \end{aligned}$$

est un isomorphisme de corps (en partie car W est irréductible, donc les ouverts non-vides sont denses)

|| **Lemme 5.3.2.** Soit $V \subseteq \mathbb{A}^n$ une variété algébrique. Alors $k(V) \simeq \text{Frac } k[V]$.

Démonstration. Notons $A = k[V]$, $K = \text{Frac}(A)$. Considérons le morphisme d'anneaux

$$\begin{aligned} \chi : K &\rightarrow k(V) \\ \frac{f}{g} &\mapsto (D(g), \frac{f|_{D(g)}}{g|_{D(g)}}) \end{aligned}$$

Alors χ est surjective (et cela suffit à prouver que c'est un isomorphisme) : en effet, soit $(U, f) \in k(V)$, avec $U \stackrel{\text{op}}{\subseteq} V$ et $f : U \rightarrow k$ une fonction régulière. Alors par définition soit $a \in U$, il existe $a \in \Omega_a \subseteq U$ un ouvert et $g, h \in k[V]$ telles que $g \neq 0$ sur Ω_a et $f = h/g$. Mais alors $(U, f) = (\Omega_a, h/g) = (D(g), h/g) = \chi(h/g)$. \square

|| **Définition 5.3.4.** Soient V, W des variétés. Une application rationnelle entre V et W est la classe d'équivalence d'un morphisme $\varphi : U_V \rightarrow W$ avec $U_V \stackrel{\text{op}}{\subseteq} V$, pour la relation d'équivalence

$$\varphi_1 : U_1 \rightarrow W \sim \varphi_2 : U_2 \rightarrow W \iff \varphi_1 = \varphi_2 \text{ sur un ouvert } \emptyset \neq D \subseteq U_1 \cap U_2$$

|| On note $V \dashrightarrow W$.

Rq 5.3.5. Un morphisme $V \rightarrow \mathbb{A}^1$ est une fonction régulière $V \rightarrow k$. Une application rationnelle $V \dashrightarrow \mathbb{A}^1$ est une fonction rationnelle $V \rightarrow k$.

|| **Définition 5.3.5.** (Dimension) Soit V une variété. Alors $\dim(V) := \text{tr deg}_k k(V)$.

Ex 5.3.2. $k(\mathbb{P}^n) = k(\mathbb{A}^n)$, $\dim \mathbb{P}^n = \dim \mathbb{A}^n$.

Rq 5.3.6. Soit V une variété et U un ouvert de V . Alors $\dim U = \dim V$.

|| **Définition 5.3.6.** Soit V une variété, $x \in V$. On définit

$$\mathcal{O}_x = \{(U, f) \in k(V) \mid x \in U \stackrel{\text{op}}{\subseteq} V\} / \sim$$

|| On appelle cet anneau l'anneau des fonctions régulières en x .

|| **Définition 5.3.7.** Soit V une variété, $x \in v$. On définit $\mathfrak{m}_x := \{(U, f) \in \mathcal{O}_x \mid f(x) = 0\}$

Exercice. 1. \mathfrak{m}_x est un idéal maximal,

2. \mathcal{O}_x est un anneau local,

3. Si V est une variété affine, alors $\mathcal{O}_x \simeq k[V]_x$,

4. \mathcal{O}_x dépend seulement d'un voisinage de x (i.e. si V, W sont des variétés avec $x \in U_V \stackrel{\text{op}}{\subseteq} V$, $y \in U_W \stackrel{\text{op}}{\subseteq} W$, et $U_V \simeq U_W$ qui fait correspondre x avec y , alors $\mathcal{O}_{V,x} \simeq \mathcal{O}_{W,y}$)

|| **Définition 5.3.8.** Soit V une variété, $x \in V$. On définit l'espace tangent de V en x comme

$$T_x V = (\mathfrak{m}_x / \mathfrak{m}_x^2)^\vee$$

|| C'est un k -ev. On dit que x est régulier si $\dim V = \dim T_x V$, que x est singulier sinon.

5.4 Courbes projectives

5.4.1 Définition, première propriétés

|| **Définition 5.4.1.** Une courbe projective est une variété projective de dimension 1.

Ex 5.4.1. $C \subseteq \mathbb{A}^n$ courbe affine, alors $\overline{C} \subseteq \mathbb{P}^n$ est une courbe projective.

|| **Proposition 5.4.1.** *C courbe projective, $x \in C$ point régulier. Si $\varphi : C \rightarrow \mathbb{P}^n$ application rationnelle, alors φ est défini en x , i.e. il existe $\varphi' : U \rightarrow \mathbb{P}^n$ morphisme, $x \in U$ et $\varphi' \sim \varphi$.*

Ex 5.4.2. Soit $E_\lambda = V(Y^2 - X(X-1)(X-\lambda)) \subseteq \mathbb{A}_{(X,Y)}^2 \subseteq \mathbb{P}_{(X,Y,Z)}^2$. Alors

$$\overline{E_\lambda} = V(Y^2Z - X(X-Z)(X-\lambda Z))$$

est irréductible. E_λ est régulière si $\lambda \neq 0, 1$. Considérons l'application rationnelle

$$\begin{aligned} \pi : \quad \mathbb{P}^2 &\rightarrow \mathbb{P}^1 \\ [X, Y, Z] &\mapsto [X, Y] \end{aligned}$$

π n'est pas défini en $[0, 0, 1]$. Soit $\varphi = \pi_{\overline{E_\lambda}} : \overline{E_\lambda} \rightarrow \mathbb{P}^1$, supposons que $\lambda \neq 0, 1$ (donc $[0, 0, 1]$ est un point régulier de $\overline{E_\lambda}$). Soit $\varphi([x, y, z]) = [X, Y] = [YZ, (X-Z)(X-\lambda Z)]$ (car $X(X-Z)(X-\lambda Z) = Y^2Z$). A $z = 1$, $\varphi([x, y, 1]) = [Y, (X-1)(X-\lambda)]$.

1. Si $\lambda = 0$: on voit $[x, y, 1]$ comme un point de \mathbb{A}^2 , alors $\varphi : \mathbb{A}^2 \rightarrow \mathbb{P}^1$. Mais il n'existe pas de $\psi : U \rightarrow \mathbb{P}^1$ morphisme, $(0, 0) \in U \subseteq \overset{\text{ouv}}{\mathbb{A}^2}$. Supposons que ψ existe, alors

$$\psi = \left[\frac{H_0}{G_0}, \frac{H_1}{G_1} \right]$$

sur $0 \in U' \subseteq \overset{\text{ouv}}{U}$, avec $H_i, G_i \in k[X, Y, Z]$ homogènes tq $\deg H_i = \deg G_i$ et $G_i([0, 0, 1]) \neq 0$. Rq : On peut supposer $U \subseteq U_z = \{z = 1\} \simeq \mathbb{A}^2$. Ainsi il existe $U' \subseteq \mathbb{A}_{x,y}^2$, $0 \in U$, $\exists h_i, g_i \in k[X, Y]$, $g_i(0, 0) \neq 0$. Dans \mathbb{P}^1 ,

$$[X, Y] = \left[\frac{h_0}{g_0}, \frac{h_1}{g_1} \right]$$

sur U' . Ainsi $Xh_1/g_1 = Yh_0/g_0$ sur $0 \in U' \subseteq \overset{\text{ouv}}{E_\lambda}$, donc $xh_1g_0 = yh_0g_1$ et $x, y \in k[E_\lambda]$. Maintenant U' est dense dans E_λ donc $xh_1g_0 - yh_0g_1 \in (Y^2, X^2(X-1))$
— $g_0(0, 0) \neq 0 \Rightarrow g_0 = g_0^0 + \dots$ et $g_0^0 \neq 0$
— $g_1(0, 0) \neq 0 \Rightarrow g_1 = g_1^0 + \dots$ et $g_1^0 \neq 0$
 ψ défini en 0 ssi $h_0(0, 0) \neq 0$ ou $h_1(0, 0) \neq 0$. Supposons $h_0(0, 0) \neq 0$, on a $h_0 = h_0^1 + \dots$ avec $h_0^1 \neq 0$. La partie linéaire de $Xh_1g_0 - Yh_0g_1$ est $Xh_1^0g_0^0 - Yh_0^1g_1^0$. Les éléments de $(Y^2 - X(X-1))$ ont 0 comme partie linéaire donc $Xh_1^0g_0^0 - Yh_0^1g_1^0 = 0$ donc $h_1^0g_0^0 = 0 = h_0^0g_0^0$ absurde.

|| **Corollaire 5.4.1.** *C courbe projective lisse. Alors toute application rationnelle $\varphi : C \dashrightarrow \mathbb{P}^n$ est régulière.*

Corollaire 5.4.2. *C, C' courbes lisses projectives, toute application birationnelle (application rationnelle $C \dashrightarrow C'$ telle que $\exists \emptyset \neq U \subseteq^{\text{ouv}} C, \exists \emptyset \neq U' \subseteq^{\text{ouv}} C'$, telle que $\varphi : U \rightarrow U'$ isom) est un isomorphisme.*

Démonstration. $x \in U \subseteq^{\text{ouv}} C, \varphi : U \setminus \{x\} \rightarrow \mathbb{P}^n$ morphisme. On peut supposer que $x = [x_0, \dots, c_n]$ avec $x_0 \neq 0$. Soit $C' = C \cap U_0 \subseteq U_0 \simeq \mathbb{A}^n$. On peut supposer que $U \subseteq^{\text{ouv}} C'$. Soit $\varphi = [f_0, \dots, f_n], f_i = H_i/G_i$ sur $U \setminus \{x\}, H_i, G_i \in k[X_0, \dots, X_n]$ homogènes, $\deg G_i = \deg H_i, G_i(x) \neq 0$. Soient $h_i = H_i(1, X_1, \dots, X_n), g_i = G_i(1, X_1, \dots, X_n), f_i = h_i/g_i$ sur $U \setminus \{x\}, g_i, h_i \in k[C']$. x point régulier $\iff \mathcal{O}_x \simeq k[C']_x$ est un DVR. Ainsi $\mathfrak{m}_x = (t)$, notons $v_x : k(C') \setminus \{0\} \rightarrow \mathbb{Z}$. Soit $r_i = v_x(f_i) \in \mathbb{Z}$. (ops $f_0, \dots, f_n \neq 0$, sinon si $f_0 = 0$, on considère $C \dashrightarrow \mathbb{P}^{n-1}$). Soit $r = \min\{r_0, \dots, r_n\}$, soit $\varphi' = [t^{-r}f_0, \dots, t^{-r}f_n]$. Alors $\varphi = \varphi'$ sur $U \setminus \{x\}$ et φ' est défini en x , car si $r_i = r$, alors $v_x(t^{-r}f_i) = 0$, i.e. $t^{-r}f_i \in \mathcal{O}_x^\times$ n'est pas 0 en x . \square

5.4.2 Pôles et zéros

C courbe projective lisse, $x \in C, C \subseteq \mathbb{P}_{X_0, \dots, X_n}^n, \exists U \subseteq^{\text{ouv}} C, x \in U, U$ est une courbe affine ($U = C \cap \{X_i \neq 0\}$). $\mathcal{O}_C = k[U]_x$ DVR, $\mathfrak{m}_x = (t)$, on dispose d'une valuation v_x . Alors

$$\begin{aligned}\mathcal{O}_x &= \{f \in k(C) \mid v_x(f) \geq 0\} \\ \mathfrak{m}_x &= \{f \in k(C) \mid v_x(f) > 0\}\end{aligned}$$

Définition 5.4.2. $f \in k(C)$ non nul.

1. Si $v_x(f) > 0$, on dit que x est un zéro de f .
2. Si $v_x(f) < 0$, on dit que x est un pôle de f .

Ex 5.4.3. $C = \mathbb{P}^1, f = \frac{X(2X-Y)}{(X-3Y)^2} \in k(\mathbb{P}^1)$ Trouver les zéros et les pôles de $f : U_0 = \{[1, t] \mid t \in k\}, U_1 = \{[s, 1] \mid s \in k\}, k(\mathbb{P}^1) = k(U_0) = k(t)$. A travers cette égalité on a

$$f = \frac{2-t}{(1-3t)^2} \in k(t)$$

Sur $U_0 : t = 2$ est un zéro, $t = 1/3$ est un pôle. Soit $t_0 \in \mathbb{A}^1 = U_0, k[\mathbb{A}^1]_{t_0} = k[t]_{(t-t_0)} = \{P/Q \mid P, Q \in k[t], Q(t_0) \neq 0\}$. Ainsi si $t \neq 2, 1/3, f = P/Q \in \mathcal{O}_{t_0}^\times$ (car $P(t_0) \neq 0, Q(t_0) \neq 0$). Et si $t_0 = 2, \mathfrak{m}_{t_0} = (t-2)$ et alors $v_{t_0}(f) = 1$ donc 2 est zéro d'ordre 1. Si $t_0 = 1/3$, alors $\mathfrak{m}_{1/3} = (t-1/3) = (3t-1)$, et alors $v_{1/3}(f) = -2$ donc $1/3$ est un pôle d'ordre 2. On fait pareil avec l'autre recouvrement si x est le point à l'infini, et on remarque que c'est un zéro d'ordre 1.

|| **Théorème 5.4.1.** $V \subseteq \mathbb{P}^n$ variété projective. Si $f : V \rightarrow k$ est une fonction régulière, alors f est une constante.

Ex 5.4.4. $V = \mathbb{P}^1$, soit $f : \mathbb{P}^1 \rightarrow k$ une fonction régulière. Ainsi on obtiens deux restrictions $f|_{U_0} \in k[\mathbb{A}^1]$, $f|_{U_1} \in k[\mathbb{A}^1]$ qui sont des fonctions régulières. Ainsi $\exists P \in k[t]$ tq $f([1, t]) = P(t)$ pour tout $t \in k$, et il existe $Q \in k[s]$ tel que $f([s, 1]) = Q(s)$ pour tout $s \in k$. Si $t \neq 0$, alors $P(t) = f([1, t]) = f([1/t, 1]) = Q(1/t)$. Mais alors soient $P = \sum^n a_i t^i$, $Q = \sum^l b_i t^i$, on obtiens donc l'égalité

$$\sum^n a_i t^i = \sum^l b_i \frac{1}{t^i} \Rightarrow a_n t^{l+n} + \dots + a_0 t^l = b_l + \dots + b_0 t^l$$

donc $n = l = 0$ et donc $P, Q \in k$ i.e. $f \in k$.

|| **Corollaire 5.4.3.** Soit C une courbe projective lisse, alors $\forall f \in k(C)$, f non constante a au moins un pôle et au moins un zéro.

Démonstration. (coro) On a, pour tout $f \in k(C)$ non nulle, $x \in X$, que

$$v_x(f) = -v_x(1/f)$$

Ainsi x est un zéro de $f \iff x$ est un pôle de $1/f$. Ainsi il suffit de montrer que $\forall f \in k(C)$ non constante, f a au moins un pôle. Supposons le contraire, soit $f \in k(C)$, f non constante mais qui n'a pas de pôle. Alors $v_x(f) \geq 0$ pour tout $x \in X$. Alors $f : C \rightarrow k$ est une fonction régulière globale, ce qui est contradictoire avec le théorème. \square

|| **Proposition 5.4.2.** C courbe projective lisse, $f \in k(C)$, $f \neq 0$. Alors il y a un nombre fini de zéros et de pôles.

Démonstration. Soit $\emptyset \neq C' \stackrel{\text{ouv}}{\subseteq} C$ ouvert avec C' courbe affine. On a montré que si V est une courbe affine, les sous-ensembles algébriques propres sont finis. C'est aussi vrai pour une courbe projective (**Exercice**) : les sous-ensembles projectifs propres sont finis (on applique le résultat précédent plusieurs fois). Maintenant $C \setminus C'$ est fini (c'est un sous-ensemble algébrique propre). Vérifions que f a un nombre fini de pôles et de zéros sur cette courbe affine. Soit $f = g/h$, avec $g, h \in k[C']$ et $h \neq 0$. Alors $\{\text{zéros de } f\} \subseteq \{\text{zéros de } g\} = V(g) \cap C'$, et idem pour les pôles : $\{\text{pôles de } f\} \subseteq \{\text{zéros de } h\} = V(h) \cap C'$. Mais $V(g) \cap C'$ est un sous-ensemble algébrique propre de C' , car sinon on aurait $g = 0$ sur C' , i.e. $g \in k[C']$ donc $f = 0$. De manière similaire, $V(h) \cap C'$ est un sous-ensemble algébrique propre de C' . \square

5.4.3 Diviseurs sur une courbe

Définition 5.4.3. C courbe projective lisse, un diviseur sur C est une somme finie formelle

$$D = \sum_{x \in C} n_x x$$

avec $n_x = 0$ sauf pour un ensemble fini de points $x \in C$.

Notation. On note $\text{Div}(C) = \{\text{diviseurs de } C\}$ (c'est le groupe abélien libre engendré par C vue comme un ensemble)

Notation. On défini

$$\begin{aligned} \deg : \quad \text{Div}(C) &\rightarrow \mathbb{Z} \\ \sum_{x \in C} n_x x &\mapsto \sum_{x \in C} n_x \end{aligned}$$

C'est un morphisme de groupes, et on notera $\text{Div}^0(C) = \ker \deg$

Définition 5.4.4. Un diviseur principal est un diviseur associé à $f \in k(C)$, $f \neq 0$ est

$$\text{div } f = \sum_{x \in C} v_x(f) x$$

Notation.

$$\begin{aligned} \text{div}_0(f) &= \sum_{\substack{p \in C \\ p \text{ zéro de } f}} v_p(f) p \\ \text{div}_\infty(f) &= \sum_{\substack{g \in C \\ g \text{ pôle de } f}} -v_p(f) g \end{aligned}$$

Rq 5.4.1.

$$\text{div } f = \text{div}_0(f) - \text{div}_\infty(f)$$

Ex 5.4.5. $C = \mathbb{P}^1$, $f = \frac{X(2X-Y)}{(X-3Y)^2}$.

1. zéros : $\infty = [0, 1]$, $p = [1, 2]$ (d'ordre 1)
2. pôles : $q = [3, 1]$ d'ordre 2.

Ainsi $\text{div } f = \infty + p - 2q$, diviseur principal de degré 0.

|| **Théorème 5.4.2.** $f \in k(C)$ non nulle, alors $\text{div } f$ est de degré 0.

|| **Proposition 5.4.3.** 1. $\text{div}(fg) = \text{div } f + \text{div } g$ pour tous $f, g \in k(C)$ non nuls.
 2. $\text{div } 1/f = -\text{div } f \ \forall f \in k(C), f \neq 0$.

Démonstration. **Exercice** □

|| **Définition 5.4.5.** $\text{Pr}(C) := \{\text{div } f \mid f \in k(C)^\times\}$

|| **Proposition 5.4.4.** 1. $\text{Pr}(C) \subseteq \text{Div}(C)$ est un sous-groupe.
 2.

$$\begin{array}{ccc} \text{div} : & k(C)^\times & \rightarrow \text{Pr}(C) \\ & f & \mapsto \text{div } f \end{array}$$

est un morphisme de groupes surjectif, de noyau k^\times .

Démonstration. soit $f \in k(C)^\times$ dans le noyau de div . Si f n'est pas constante, alors f a au moins un pôle et un zéro, et ainsi $\text{div } f \neq 0$. □

|| **Définition 5.4.6.** On définit le groupe de Picard de C comme

$$\text{Pic}(C) = \text{Div}(C) / \text{Pr}(C) = \text{Div}(C) / \sim$$

Notation. Soient $D, D' \in \text{Div}(C)$, alors

$$D \sim D' \iff D - D' = \div(f) \in \text{Pr}(C)$$

où $f \in k(C)^\times$. Cette relation d'équivalence est nommée "linéairement équivalents". On note $[D]$ la classe de D dans $\text{Pic}(C)$.

|| **Théorème 5.4.3.** $\text{Pr}(C) \subseteq \text{Div}^0(C)$, i.e. pour tout $f \in k(C)^\times$, $\text{div}(f)$ est de degré 0, i.e. $\deg(\text{div}_0(f)) = \deg(\text{div}_\infty(f))$.

Rq 5.4.2. $f \in k(C)$ non constante. Alors $\bar{k} = k \subseteq k(f)$ est purement transcendante, mais $\dim C = 1$, i.e. $\text{tr deg}_k k(C) = 1$, donc $k(f) \subseteq k(C)$ est algébrique (et de type fini), i.e. $[k(C) : k(f)] < \infty$.

Théorème 5.4.4. $f \in k(C)^\times$ non constante. Alors

$$\deg(\operatorname{div}_0(f)) = \deg(\operatorname{div}_\infty(f)) = [k(C) : k(f)]$$

Rq 5.4.3. $f \in k(C)^\times$ non constante, alors on peut définir

$$\begin{aligned} F : C &\dashrightarrow \mathbb{P}^1 \\ x &\mapsto [1, f(x)] \end{aligned}$$

et on a prouvé que si C est lisse, alors F est en réalité un morphisme (est bien défini).

Théorème 5.4.5.

$$[k(C), k(f)] = \deg F$$

où $\deg F$ est le nombre de points dans $F^{-1}(y)$ pour un $y \in \mathbb{P}^1$ point général.

Rq 5.4.4. Si $[k(C), k(f)] = 1$, alors F est en réalité un isomorphisme.

Rq 5.4.5. V, W variétés, et $V \dashrightarrow W$ birationnelle ($\exists \emptyset \neq U_V \subseteq V, \emptyset \neq U_W \subseteq W$ ouverts, $U_V \simeq U_W$), alors $k(V) \simeq k(W)$. La réciproque est aussi vraie. Ainsi si C est une courbe projective, $f \in k(C)^\times$ non constante, si $k(C) = k(f) \simeq k(\mathbb{P}^1)$, alors il existe une application birationnelle $C \dashrightarrow \mathbb{P}^1$.

Exercice. C, C' courbes lisses, alors il existe une application birationnelle $C \dashrightarrow C'$ si et seulement si $C \simeq C'$.

Une conséquence du théorème 5.4.3 est que le morphisme \deg passe au quotient par $Pr(C)$, i.e. le morphisme

$$\begin{aligned} \deg : \operatorname{Pic}(C) &\rightarrow \mathbb{Z} \\ [D] &\mapsto \deg D \end{aligned}$$

est bien défini (et il est surjectif). Autrement dit, si $D \sim D'$, alors $\deg D = \deg D'$.

Exercice. $C = \mathbb{P}^1$, alors pour tout $D \in \operatorname{Div}^0(C)$, on a que D est principal ($D = \operatorname{div} f$ pour un $f \in k(\mathbb{P}^1)^\times$)

Définition 5.4.7. On définit la variété de Picard comme

$$\operatorname{Pic}^0(C) = \operatorname{Div}^0 / Pr(C)$$

C'est un sous groupe de $\operatorname{Pic}(C)$.

Rq 5.4.6. Considérons le morphisme $\deg : \text{Pic}(C) \rightarrow \mathbb{Z}$. Alors $\ker(\deg) = \text{Div}^0(C)$. Ainsi si $C = \mathbb{P}^1$, $\text{Pic}^0(\mathbb{P}^1) = 0$ et ainsi $\text{Pic}(\mathbb{P}^1) \simeq \mathbb{Z}$.

|| **Définition 5.4.8.** Un diviseur $D = \sum n_p p$ sur C est effectif si $n_p \geq 0$ pour tout $p \in C$.

Notation. On note $D \geq 0$ si D est effectif, et $D' \geq D$ si $D - D' \geq 0$.

Notation. $D \in \text{Div}(C)$, considérons

$$\mathcal{L}(D) = \{0\} \cup \{f \in k(C)^\times \mid \text{div}(f) + D \geq 0\}$$

Plus explicitement, $D = \sum n_p p$, alors $f \in k(C)^\times$ est dans $\mathcal{L}(D)$ si et seulement si $n_p + v_p(f) \geq 0$.

|| **Lemme 5.4.1.** ($D = 0$)

$$\mathcal{L}(0) = k$$

Démonstration. $\mathcal{L}(0) = \{0\} \cup \{f \in k(C)^\times \mid \text{div}(f) \geq 0\}$, or $\text{div}(f) = \text{div}_0(f) - \text{div}_\infty(f)$, et si $f \notin k$, alors $\text{div}_\infty(f) \neq 0$ donc $f \notin \mathcal{L}(0)$, et si $f \in k^\times$, alors on a bien $\text{div}(f) = 0$. \square

Ex 5.4.6. $C = \mathbb{P}^1$, $p = [0, 1] \in \mathbb{P}^1$, $n > 0$ entier. Notons $D = np$, alors

$$\mathcal{L}(D) = \{0\} \cup \{f \in k(C)^\times \mid \text{div}(f) + np \geq 0\}$$

Ainsi $f \in \mathcal{L}(D) \iff \forall g \neq p, v_p(f) \geq 0$ et $v_p(f) + n \geq 0$. Essayons de caractériser cela : $p \in \mathbb{A}^1 \subseteq \mathbb{P}^1$ où on identifie \mathbb{A}^1 avec l'ouvert $\{[x, 1] \mid x \in \mathbb{A}^1\}$, et $k(\mathbb{P}^1) \simeq \mathbb{A}^1 = k(t)$. Ainsi $\mathcal{O}_p = k[\mathbb{A}^1]_0$ correspond donc aux fractions rationnelles dont le dénominateur ne s'annule pas en 0. Remarquons alors que si $f = P/Q$, $P, Q \in k[t]$. Alors écrivons $P = t^n P'$, $Q = t^m Q'$, avec $P'(0) \neq 0$, $Q'(0) \neq 0$. Alors $f = t^{n-m}(P'/Q')$, et $v_p(f) = n - m$. On voudrait alors montrer que

$$\mathcal{L}(np) = \left\{ \frac{P(t)}{t^n} \mid P \in k[t], \deg P \leq n \right\}$$

Il faut d'abord montrer que $1/t^i \in \mathcal{L}(np)$ si $0 \leq i \leq n$ pour prouver \supseteq . Mais si $p = 0$, alors $v_p(1/t^i) = -i$, et donc $v_p(1/t^i) + n \geq 0$. Et si $g \neq 0$, alors $v_g(1/t^i) = 0$ (**Exercice**). Maintenant si $g = \infty = [1, 0]$, on doit changer de carte pour calculer \mathcal{O}_g : on prend $y \in \mathbb{A}^1 \mapsto [1, y] \in \mathbb{P}^1$. Et par ce changement de carte $k(t) \simeq k(s)$ via $t \mapsto 1/s$, et alors $1/t^i \mapsto s^i$ qui est de g -valuation positive, et ainsi ∞ n'est pas un pôle de $1/t^i$. **Le sens réciproque est laissé en exercice**

- Proposition 5.4.5.** 1. $\mathcal{L}(D) \neq 0$ si et seulement si $\exists E \geq 0$ diviseur effectif tel que $D \sim E$.
2. $\mathcal{L}(D) \subseteq k(C)$ est un k -sev.
3. Si $D \geq D'$, alors $\mathcal{L}(D) \subseteq \mathcal{L}(D')$ et $\dim_k \mathcal{L}(D')/\mathcal{L}(D) \leq \deg D' - \deg D$.
4. Si $D' \sim D$, alors $\mathcal{L}(D) \simeq \mathcal{L}(D')$ dans \mathbf{Vect}_k .
5. Si $D \geq 0$, alors $\dim_k \mathcal{L}(D) \leq \deg(D) + 1$ (et en particulier $\mathcal{L}(D)$ est un k -ev de dimension finie)

Démonstration. 1. $\mathcal{L}(D) \neq 0 \iff f \in k(C)^\times$ tel que $\text{div}(f) + D \geq 0$. Ainsi posons $E := \text{div}(f) + D \geq 0$, alors $E \sim D$ car $E - D = \text{div}(f)$. Pour le sens réciproque, si $E \geq 0$ et $E \sim D$, alors $\exists f \in k(C)^\times$ tel que $E - D = \text{div}(f)$, donc $0 \leq E = D + \text{div}(f)$ et ainsi $f \in \mathcal{L}(D) \setminus \{0\}$.

2. Si $f, g \in \mathcal{L}(D)$, alors $f + g \in \mathcal{L}(D)$: notons $D = \sum_{p \in C} n_p p$, $p_i \in C$, $n_i \in \mathbb{Z}$. Alors $f \in \mathcal{L}(D) \iff v_p(f) + n_p \geq 0$ pour tout $p \in C$. Soit $f, g \in \mathcal{L}(D)$, il faut montrer que $v_p(f+g) + n_p \geq 0$ pour tout $p \in C$. Mais on sait que $v_p(f+g) \geq \min\{v_p(f), v_p(g)\} \geq -n_p$ comme $f, g \in \mathcal{L}(D)$, et ainsi $f + g \in \mathcal{L}(D)$. Il faut ensuite montrer que si $f \in \mathcal{L}(D)$, $\lambda \in k$, alors $\lambda f \in \mathcal{L}(D)$: si $\lambda = 0$, ok. Sinon, $v_p(\lambda f) = v_p(f) \geq -n_p$ si $f \in \mathcal{L}(D)$.

3. Comme $D \geq D'$, alors $D' = D + E$ où $E \geq 0$. Maintenant si $f \in \mathcal{L}(D)$, alors $D' + \text{div}(f) = E + D + \text{div}(f)$ et $E, D + \text{div}(f) \geq 0$ donc $f \in \mathcal{L}(D')$. Pour le deuxième point, notons $D' = D + \sum_{i=1}^l n_i y_i$, $n_i \geq 0$. D'après le point précédent, on a $\mathcal{L}(D) \subseteq \mathcal{L}(D + y_1) \subseteq \mathcal{L}(D + 2y_1) \subseteq \dots \subseteq \mathcal{L}(D)(D + n_1 y_1) \subseteq \mathcal{L}(D)(D + n_1 y_1 + y_2) + \dots$. Comme $\deg D' - \deg D = \sum n_i$, il suffit de montrer que $\dim_k \mathcal{L}(D + y)/\mathcal{L}(D) \leq 1$ pour $y \in C$. Pour cela, considérons

$$\begin{aligned} \varphi : \mathcal{L}(D + y) &\rightarrow k \\ f &\mapsto (t^{n_y+1}f)(y) \end{aligned}$$

où $D = n_y y + \sum_{p \neq y} n_p p$, $m_y = (t) \subseteq \mathcal{O}_y$. φ est bien défini : si $f \in \mathcal{L}(D + y)$ est non nul, $v_y(f) + n_y + 1 \geq 0$ et donc $v_y(t^{n_y+1}f) \geq 0$ et ainsi $t^{n_y+1}f \in k(C)^\times$ est bien défini en y . Maintenant $f \in \ker \varphi \iff v_y(t^{n_y+1}f) > 0 \iff n_y + v_y(f) \geq 0$. Il faut donc vérifier que si $f \in \ker \varphi$, alors $f \in \mathcal{L}(D)$. En y , $v_y(f) + n_y \geq 0$, et sinon si $x \neq y$, $f \in \mathcal{L}(D + y) \Rightarrow v_x(f) + n_x \geq 0$ et ainsi au final $\text{div}(f) + D \geq 0$.

4. $D \sim D' \iff D' = D + \text{div}(f)$, où $f \in k(C)^\times$. Soit

$$\begin{aligned} \varphi : \mathcal{L}(D) &\rightarrow \mathcal{L}(D') \\ g &\mapsto \frac{1}{f}g \end{aligned}$$

alors φ est bien défini : soit $g \in \mathcal{L}(D)$, alors $D + \text{div}(g) \geq 0$. Mais

$$\text{div}(g/f) + D' = \text{div}(g) - \text{div}(f) + D' = \text{div}(g) + D \geq 0$$

puis φ est k -linéaire. Par le même argument, l'application

$$\begin{array}{ccc} \psi : \mathcal{L}(D') & \rightarrow & \mathcal{L}(D) \\ g & \mapsto & fg \end{array}$$

est bien définie et k -linéaire, et est l'inverse de φ .

5. C'est un cas particulier du point (3) : on a que $\dim_k \mathcal{L}(D)/\mathcal{L}(0) \leq \deg D$, puis $\mathcal{L}(0) \simeq k$ donc $\dim \mathcal{L}(D) - 1 \leq \deg D$.

□

Ainsi on peut énoncer un corollaire du théorème 5.4.3 :

- || **Corollaire 5.4.4.** 1. Si $D \sim D'$, alors $\deg D = \deg D'$.
 2. Si $\mathcal{L}(D) \neq 0$, alors $\deg D \geq 0$ (donc si $\deg D < 0$, alors $\mathcal{L}(D) = 0$)
 3. Si $\deg D \geq -1$, alors $\dim \mathcal{L}(D) \leq \deg D + 1$.

Démonstration. 1. Ok

2. $\mathcal{L}(D) \neq 0 \iff \exists E \geq 0$ tel que $E \sim D$. Mais alors $\deg E = \deg D \geq 0$ car $E \geq 0$.

3. Si $\mathcal{L}(D) = 0$, alors $0 \leq \deg D + 1$ si $\deg D \geq -1$. Ainsi on peut supposer que $\mathcal{L}(D) \neq 0$. Alors $\exists E \geq 0$ tel que $E \sim D$, donc $\deg E = \deg D$, et $\dim \mathcal{L}(D) = \dim \mathcal{L}(E)$. On a donc que $\dim \mathcal{L}(E) \leq \deg E + 1$ par le point (5) du lemme précédent, et ainsi $\dim \mathcal{L}(D) \leq \deg D + 1$.

□

Notation. $\dim D := \dim_k \mathcal{L}(D)$

|| **Théorème 5.4.6.** (Riemann-Roch) C courbe projective lisse, $k = \bar{k}$. Alors il existe un entier $g \geq 0$ (le genre de C) tel que

1. Pour tout diviseur D sur C , on a $\dim(D) \geq \deg(D) + 1 - g$
 2. Si $\deg D \geq 2g - 1$, alors $\dim(D) = \deg(D) + 1 - g$

|| **Théorème 5.4.7.** (dualité de Serre) \exists diviseur K_C (diviseur canonique) tel que $\deg(K_C) = 2g - 2$, et $\dim(D) - \dim(K_C - D) = \deg D + 1 - g$.

|| **Théorème 5.4.8.** C courbe projective lisse sur $k = \bar{k}$. On a $g = 0 \iff C \simeq \mathbb{P}^1$

Démonstration.

\Leftarrow : Montrer que $\dim(D) \geq \deg(D) + 1$ pour tout diviseur D , et $\sim(D) = \deg D + 1$ si $\deg D \geq -1$. On sait déjà que si $\deg D \geq -1$, alors $\dim(D) \leq \deg(D) + 1$ (vrai pour tout C !). Il suffit donc de montrer $\dim D = \deg D + 1$ si $\deg D \geq -1$. Si $\deg D = -1$, alors $\mathcal{L}(D) = 0$ et donc $0 = -1 + 1$ ok. Ainsi on peut supposer que $\deg(D) = n \geq 0$. On a vu (exercice) que sur \mathbb{P}^1 , si $\deg D = \deg D'$, alors $D \sim D'$. Ainsi si $\deg D = n$, alors $D \sim np$ avec $p \in \mathbb{P}^1$. Et ainsi $\dim(D) = \dim(np)$ mais on a aussi vu en exercice que $\mathcal{L}(np) = k + k1/t + \dots + k1/t^n$ dont une base est les $1/t^i$, donc de dimension $n + 1$. On a donc $\dim D = \dim np = n + 1 = \deg D + 1$.

\Rightarrow : Supposons que le genre g de C est 0. Donc pour tout diviseur D sur C on a que $\dim D \geq \deg D + 1$ et $\dim D = \deg D + 1$ si $\deg D \geq -1$. Soit $D = p$, $p \in C$. Alors $\deg D = 1$, et $\dim(D) = \deg(D) + 1 = 2$. Et donc $\mathcal{L}(0) \not\subseteq \mathcal{L}(D)$ et donc il existe $f \in \mathcal{L}(D)$ non constante, et donc $\div_{\infty}(f) \neq 0$, mais comme $f \in \mathcal{L}(D)$, $\div(f) + p \geq 0$, $\div_{\infty} = p$. Mais d'après le théorème 5.4.4, $\deg(\div_{\infty}(f)) = \deg(\div_0(f)) = [k(C) : k(f)] = 1$ et donc $k(C) = k(f)$, mais $k(f) \simeq k(\mathbb{P}^1)$ et ainsi $C \simeq \mathbb{P}^1$ (du fait que si C, C' sont des courbes lisses, alors $k(C) \simeq k(C') \iff C \simeq C'$) \square

|| **Définition 5.4.9.** C courbe elliptique est une courbe projective lisse de genre $g = 1$.

|| **Théorème 5.4.9.** C courbe elliptique, $o \in C$ point. Soit

$$\begin{aligned} \varphi : C &\rightarrow \text{Pic}^0(C) \\ p &\mapsto [p - o] \end{aligned}$$

|| Alors φ est bijectif.

Démonstration.

Injective : supposons que $\varphi(p) = \varphi(g)$, $p, g \in C$ et $p \neq g$. Alors $[p - o] = [g - o]$, et ainsi $p - o \sim g - o$ et donc $p \sim g$, i.e. $p - g = \text{div}(f)$, pour un $f \in k(C)^{\times}$. Maintenant $\text{div}_0(f) = p$, $\text{div}_{\infty}(f) = g$ est de degré 1 donc $k(f) = k(C)$ (d'après 5.4.4). Ainsi $k(\mathbb{P}^1) \simeq k(C)$ et donc $\mathbb{P}^1 \simeq C$, absurde puisque \mathbb{P}^1 est de genre 0.

Surjective : Soit $D \in \text{Div}^0(C)$, soit $D' = D + o$. Alors D' est un diviseur de degré 1 : d'après le théorème de Riemann-Roch, $\dim(D') = \deg(D') + 1 - 1 = 1$. Alors $\mathcal{L}(D') \neq 0$, et ainsi il existe $E \geq 0$ tel que $D' \sim E$. Mais $\deg E = \deg D' = 1$ donc $E = p$, $p \in C$. Et alors $D' \sim E = p$ d'où $D + o \sim p$ et donc $[D] = [p - o]$. \square

Annexe A

A.1 Localisation d'un anneau

Soit $A \in \mathbf{CRings}$, et $S \subseteq A$ une partie multiplicative de A ($1 \in S$, $x, y \in S \Rightarrow xy \in S$).

Définition A.1.1. La localisation de A en S , notée $S^{-1}A$, est défini par la propriété universelle

$$\mathbf{Hom}_{\mathbf{CRings}}(S^{-1}A, B) \simeq \{\varphi : A \rightarrow B \mid \varphi(S) \subseteq B^\times\}$$

On construit la localisation comme un quotient de $A \times S$ par la relation d'équivalence $(a, s) \sim (a', s') \iff as' = a's \in A$, et on note $\frac{a}{s}$ les classes d'équivalence pour cette relation. La somme et le produit fonctionnent comme sur \mathbb{Q} .

- Ex A.1.1.** 1. Soit A un anneau commutatif, $\mathfrak{p} \overset{\text{prm}}{\subseteq} A$. Alors $A \setminus \mathfrak{p}$ est une partie multiplicative, du fait que \mathfrak{p} ne peut pas être A tout entier, donc $1 \notin \mathfrak{p}$, puis si $xy \in \mathfrak{p}$, alors $x \in \mathfrak{p}$ ou $y \in \mathfrak{p}$. On note $A_{\mathfrak{p}} := (A \setminus \mathfrak{p})^{-1}A$.
2. Prenons toujours A un anneau commutatif, et $f \in A$. Alors considérons $S := \{f^n \in A \mid n \in \mathbb{N}\}$. Alors c'est une partie multiplicative, et on note $A_f := S^{-1}A$. Remarquons que si (f) est un idéal premier, alors A_f n'est pas la même chose que $A_{(f)}$.

A.2 Théorie des corps

Définition A.2.1. (Corps des fractions) Soit A un anneau. Le corps des fractions de A , noté $\text{Frac}A$, est défini par la propriété universelle

$$\mathbf{Hom}_{\mathbf{Fld}}(\text{Frac}A, k) \simeq \{A \hookrightarrow k \in \mathbf{CRings}\}$$

Rq A.2.1. C'est un cas particulier de localisation, où la partie multiplicative choisie est $A \setminus \{0\}$. Ainsi, on peut le construire comme

$$\text{Frac}A = \left\{ \frac{P}{Q} \mid (P, Q) \in A \times A \setminus \{0\} \right\}$$