Université de Rennes 1

ACGA

ALGÈBRE COMMUTATIVE & GÉOMÉTRIE ALGÉBRIQUE

Auteur
Bernard Le Stum

Notes de cours
Victor Lecerf

2021–2022

Table des matières

Introduction

Soit $F \in \mathbb{R}[X]$. La première étape de l'étude d'un polynôme est celui de ses racines réelles $V(F) = \{a \in \mathbb{R} \mid F(a) = 0\}$. Première question : son cardinal N est-il fini ? La réponse est que N est fini *si et seulement si* $F \neq 0$. Deuxième question : a-t-on $N \leq \deg F$ lorsque $F \neq 0$? La réponse est toujours positive. De plus, quand a-t-on égalité ? C'est le cas pour $X^2 - 1$, mais l'on doit se poser des questions de multiplicité pour des polynômes telles que $X^2 - 2X + 1$, ou de l'existence de racines complexes comme avec $X^2 + 1$.

Intéressons nous maintenant à deux polynômes $F, G \in \mathbb{R}[X, Y]$, et soit $V(F, G) = \{(a, b) \in \mathbb{R}^2 \mid F(a, b) = G(a, b) = 0\}$, et soit N le cardinal de cet ensemble. On a $N < \infty$ *si et seulement si* F et G sont premiers entre eux (dans l'anneau $\mathbb{C}[X, Y]$) et les deux ont chacun une infinité de points d'annulation. Peut-on majorer N en fonction de paramètres de F et G ? En fait, $N \leq \deg F \cdot \deg G$ et le cas d'égalité peut se produire et revient encore une fois à étudier des notions de multiplicités (que nous définirons tardivement, ce n'est pas trivial) et des solutions complexes, mais aussi des solutions à l'infini (deux droites parallèles doivent avoir un point d'intersection à l'infini dans un plan projectif).

L'algèbre commutative ici sera l'étude de l'idéal $(F, G) \subset \mathbb{R}[X, Y]$, tandis que la géométrie algébrique sera l'étude de $V = V(F, G) \subset \mathbb{A}^2 = \mathbb{R}^2$.

Chapitre 1

Polynômes

1.1 Définitions

Soit R un anneau commutatif unitaire. Bien évidemment – comme dans tout court d'algèbre commutative, le terme "anneau" désigne toujours un anneau commutatif unitaire. Nous préciserons lorsque nous travaillerons avec un anneau qui n'est pas de cette nature.

Définition 1.1.1 (R-algèbre)**.** *Le quadruplet* $(A, +, \times, \cdot)$ *est une* R*-algèbre si*

(i) $(A, +, \times)$ *est un anneau ;*

(ii) $(A, +, \cdot)$ *est un* R*-module ;*

(iii) pour tout $c \in R$ *et* $f, g \in A$, $(c \cdot f) \times g = c \cdot (f \times g)$.

Remarques.

— Une application $u : A \longrightarrow B$ entre deux R-algèbres est un (homo)morphisme de R-algèbre si c'est un morphisme d'anneaux et un morphisme de R-modules.

— Une partie $B \subset A$ est dite être une sous-R-algèbre si B est un sous-anneau de A et un sous-R-module de A. En fait, B est une sous-R-algèbre si $B \hookrightarrow A$ est un morphisme de R-algèbres.

Exemples. R est une R-algèbre. Tout anneau est une $\mathbb{Z}$-algèbre.

Exercice.

1. Soit A une R-algèbre, et $u : R \to A$, $c \mapsto c1_A$. Montrer que u est un morphisme d'anneaux.
2. Soit A un anneau, et $u : R \longrightarrow A$ un morphisme d'anneaux. Montrer que u muni A d'une structure de R-algèbre [1] avec $c \cdot f = u(c) \times f$ pour tout $c \in R$ et $f \in A$.
3. Soit A une R-algèbre et E un ensemble (quelconque). Montrer que l'ensemble $\mathcal{F}(E, A)$ des applications de E dans A est une A-algèbre pour des lois évidentes.
4. Montrer que $\mathcal{F}_0(E, A)$ l'ensemble des applications de E dans A à support fini est une sous-algèbre de $\mathcal{F}(E, A)$.

1. Dans beaucoup de livres, une algèbre est définie comme un anneau muni d'un morphisme d'anneaux (généralement injectif).

Digression (propriété universelle).

— L'objet $(\mathbb{C}, i)$ est dit *universel* pour les couples (K, α) avec K un corps contenant $\mathbb{R}$ et $\alpha^2 = -1$. Cela signifie qu'il existe un unique morphisme de corps $\varphi : \mathbb{C} \longrightarrow K$ tel que $\varphi(i) = \alpha$ (K est en fait un corps de rupture).

— R est universel pour les corps complets contenant $\mathbb{Q}$.

Lemme 1.1.1. *Il existe une R-algèbre $R[X_1, \ldots, X_n]$ avec $X_1, \ldots, X_n \in R[X_1, \ldots, X_n]$ universelle pour les R-algèbres A munie de $f_1, \ldots, f_n \in A$. C'est-à-dire qu'il existe un unique morphisme de R-algèbres*

$$\begin{array}{rcl} R[X_1, \ldots, X_n] & \longrightarrow & A \\ X_i & \longmapsto & f_i. \end{array}$$

Notation. On note $F(f_1, \ldots, f_n)$ l'image de $F \in R[X_1, \ldots, X_n]$.

Remarque. Tout $F \in R[X_1, \ldots, X_n]$ s'écrit de manière unique

$$F = \sum_{0 \leq d_1, \ldots, d_n \leq m} c_{d_1, \ldots, d_n} X_1^{d_1} \cdots X_n^{d_n}$$

avec $c_{d_1, \ldots, d_n} \in R$ (cela revient à dire que $(X_1^{d_1} \cdots X_n^{d_n})_{0 \leq d_1, \ldots, d_n \leq m}$ est une base). On pose

$$F(f_1, \ldots, f_n) = \sum_{0 \leq d_1, \ldots, d_n \leq m} c_{d_1, \ldots, d_n} f_1^{d_1} \cdots f_n^{d_n}.$$

Démonstration. On a $R[X_1, \ldots, X_n] = \mathcal{F}_0(N^n, R)$.

□

Alternatives. On peut construire récursivement $R[X_1, \ldots, X_n] = R[X_1, \ldots, X_{n-1}][X_n]$, ou encore poser

$$R[X_1, \ldots, X_n] = \underbrace{R[X] \otimes_R \cdots \otimes_R R[X]}_{n \text{ fois}}.$$

Exercice.

1. Si $R[Y_1, \ldots, Y_n]$ avec $Y_1, \ldots, Y_n$ est une autre solution au problème, montrer qu'il existe un unique isomorphisme de R-algèbres

$$\begin{array}{rcl} R[X_1, \ldots, X_n] & \longrightarrow & R[Y_1, \ldots, Y_n] \\ X_i & \longmapsto & Y_i. \end{array}$$

2. Montrer que $R[X_1, \ldots, X_{n+1}] \cong R[X_1, \ldots, X_n][X_{n+1}]$.
3. Montrer que si A est une R-algèbre, l'application

$$\begin{array}{rcl} R[X_1, \ldots, X_n] & \longrightarrow & \mathcal{F}(A^n, A) \\ F & \longmapsto & \left| \begin{array}{rcl} A^n & \longrightarrow & A \\ (f_1, \ldots, f_n) & \longmapsto & F(f_1, \ldots, f_n) \end{array} \right. \end{array}$$

est un morphisme de R-algèbres.

Définition 1.1.2. *$R[X_1, \dots, X_n]$ est l'algèbre des polynômes en n variables. Un élément de la forme $X_1^{d_1} \cdots X_n^{d_n}$ est appelé monôme de degré $d = d_1 + \cdots + d_n$. Si $c \in R$, $cX_1^{d_1} \cdots X_n^{d_n}$ est un terme de degré d et c est son coefficient.*

Exercice.

1. Soit k un corps *infini* et $F \in k[X_1, \dots, X_n]$. Montrer que $F = 0$ *si et seulement si* pour tout $a_1, \dots, a_n \in k$, $F(a_1, \dots, a_n) = 0$.
2. En déduire que l'application $k[X_1, \dots, X_n] \longrightarrow \mathcal{F}(k^n, k)$ est injective.
3. Trouver un contre-exemple si k est fini [2].

Définition 1.1.3. *Soit $F \in R[X_1, \dots, X_n]$. On appelle* degré *de F le plus grand degré des termes non nuls de F noté* $\deg F$. *On appelle* valuation *de F le plus petit degré des termes non nuls de F noté* $\operatorname{val} F$. *Le polynôme F est dit* homogène *si* $\operatorname{val} F = \deg F$. *La partie homogène de F de degré d est la somme des termes de degré d de F.*

Exemple. Si $F = XYZ + X^3 - 2X$, on a $\deg F = 3$, $\operatorname{val} F = 1$, et ses parties homogènes sont $XYZ + Y^3$ et $-2X$.

Remarque. En général, $\operatorname{val} F \leq \deg F$ (lorsque $F \neq 0$).

Exercice.

1. — Montrer que $\deg F = -\infty$ *si et seulement si* $F = 0$, et que $\deg F = 0$ *si et seulement si* $F \in R \backslash \{0\}$.
   — Montrer que $\deg(F + G) \leq \max(\deg F, \deg G)$ avec égalité si $\deg F \neq \deg G$.
   — Montrer que $\deg(FG) \leq \deg F + \deg G$ avec égalité si R est intègre.
   — Montrer que $\deg F = \infty$ *si et seulement si* $F = 0$, et que $\operatorname{val} F = 0$ *si et seulement si* $F(0, \dots, 0) \neq 0$.
   — Montrer que $\operatorname{val}(F + G) \geq \min(\operatorname{val} F, \operatorname{val} G)$ avec égalité si $\operatorname{val} F \neq \operatorname{val} G$.
   — Montrer que $\operatorname{val}(FG) \geq \operatorname{val} F + \operatorname{val} G$ avec égalité si R est intègre.

   Si $F \in R[X_1, \dots, X_{n+1}]$ est homogène, on pose

   $$F_*(X_1, \dots, X_n, 1) \in R[X_1, \dots, X_n].$$

   Si $F \in R[X_1, \dots, X_n]$, on pose

   $$F^* = X_{n+1}^{\deg F} F\left(\frac{X_1}{X_{n+1}}, \dots, \frac{X_n}{X_{n+1}}\right) \in R[X_1, \dots, X_{n+1}].$$

2. Montrer que $(FG)_* = F_* G_*$, $(FG)^* = F^* G^*$, $(F^*)_* = F$, et $X_{n+1}^m (F_*)^* = F$ avec $m = \operatorname{val}_{X_{n+1}}(F)$.

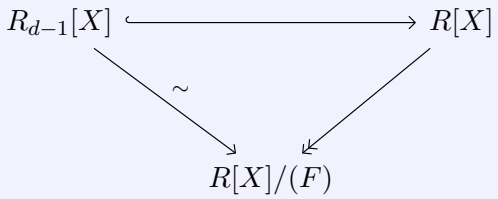
Exemple. Soit $F = X^2 + XY + Y^2$. On a $F_* = X^2 + X + 1 = (X - j)(X - j^2)$ et donc $(F_*)^* = (X - j)^*(X - j^2)^* = (X - jY)(X - j^2 Y)$. Puisque $\operatorname{val}_Y(F) = 0$, on en déduit que $X^2 + XY + Y^2 = (X - jY)(X - j^2 Y)$.

2. On peut en fait en trouver dans tous les corps finis.

1.2 Anneaux factoriels

Soit R un anneau (commutatif unitaire) *intègre*.

Proposition 1.2.1 (division euclidienne)**.** *Soit $F \in R[X]$ un polynôme de degré d de coefficient dominant inversible. Alors, l'application composée*



est bijective.

Démonstration. On veut montrer que pour tout $G \in R[X]$, il existe un unique $H \in R_{d-1}[X]$ tel que $H \equiv G \mod F$. Que $G - H \equiv 0 \mod F$ est équivalent à montrer qu'il existe $Q \in R[X]$ avec $G = QF + H$ (avec G unique de degré $\deg H < d$).

□

Définition 1.2.1. *Soit A un anneau intègre. Un idéal $I \subset A$ dit* principal *s'il existe $f \in A$ tel que $I = (f) = fA$. L'anneau A est dit principal si tous ses idéaux sont principaux.*

Exercice. Soit k un corps. Montrer que les anneaux k, $\mathbb{Z}$, et $\mathbb{Z}[X]$ sont principaux[3]. Montrer que $\mathbb{Z}[X]$ et $k[X, Y]$ ne sont pas principaux.

Définition 1.2.2. *Soit A un anneau intègre et $f, g \in A$. On dit que f divise g (noté $f|g$) si $(g) \subset (f)$.*

On dit aussi que f est un facteur de g, ou que g est un multiple de f.

Exercice.

1. Soit A un anneau intègre. Si $f, g \in A$, alors f divise g *si et seulement s'*il existe $h \in A$ tel que $g = hf$. Montrer que f divise g et g divise f *si et seulement s'*il existe $h \in A^\times$ tel que $g = hf$.
2. Soit R un anneau intègre. Montrer que pour tout $F \in R[X]$ et pour tout $\alpha \in R$, il existe un unique $Q \in R[X]$ tel que $F = (X - \alpha)Q + F(\alpha)$. En déduire que $X - \alpha$ divise F *si et seulement si* $F(\alpha) = 0$ (*i.e* que α est une racine de F).

Définition 1.2.3. *Deux éléments $f, g \in A$ sont dits étrangers si pour tout idéal I de A contenant f et g, $I = A$. Les éléments f et g sont dits premiers entre eux si pour tout idéal principal I de A contenant f et g, $I = A$.*

Remarque. Deux éléments étrangers sont premiers entre eux. Il y a équivalence entre les deux notions sur les anneaux principaux. $\mathbb{R}[X, Y]$ est un contre-exemple de la réciproque dans le cas général : X et Y sont premiers entre eux mais pas étrangers.

3. En fait, ils sont euclidiens, et donc principaux.

Exercice.

1. Montrer que f et g sont étrangers *si et seulement s'*il existe $u, v \in A$ tels que $uf + vg = 1$ (Bézout).
2. Montrer que f et g sont premiers entre eux *si et seulement si* pour tout $h \in A$ tel que h divise f et h divise h, alors h est inversible.
3. Soient $F, G \in R[X]$. Montrer que si F et G sont premiers entre eux, alors ils n'ont pas de racine commune. Montrer que la réciproque est vrai si R est un corps algébriquement clos et trouver un contre-exemple sur $\mathbb{R}$.

Définition 1.2.4 (élément irréductible, premier)**.** *Un élément $p \in A$ est non nul dit* irréductible *(resp.* premier*) si l'idéal (p) est maximal parmi les idéaux principaux différents de A (resp. si (p) est premier).*

Définition 1.2.5. *Un anneau est dit factoriel s'il existe $\mathcal{P} \subset A$ tel que tout $f \in A\backslash\{0_A\}$ s'écrive de manière unique sous la forme*

$$f = u \prod_{p \in \mathcal{P}} p^{v_p}$$

avec $u \in A^\times$ et $v_p \in \mathbb{N}$, où le produit est fini.

Remarque. Formellement, il existe $\mathcal{P} \subset A$ tel que l'application

$$\begin{array}{rcl} \mathbb{N}^{(\mathcal{P})} & \longrightarrow & (A\backslash\{0\})/A^\times \\ (v_p)_{p \in P} & \longmapsto & \overline{\prod_{p \in \mathcal{P}} p^{v_p}} \end{array}$$

est injective.

Exercice.

1. Montrer que p est irréductible *si et seulement si* p est non nul, non inversible et que pour tout $f, g \in A$, $p = fg$ implique que $f \in A^\times$ ou $g \in A^\times$. De même, montrer que p est premier *si et seulement si* p est non nul, non inversible, et pour tout $f, g \in A$, p divise fg implique que p divise f ou p divise g.
2. Montrer qu'un élément premier est irréductible. Montrer que la réciproque est vraie dans un anneau factoriel. Toujours lorsque A est factoriel, montrer qu'un élément $p \in A$ (*i.e* irréductible ici) *si et seulement s'*il existe $u \in A^\times$ tel que $up \in \mathcal{P}$, *i.e* que $\mathcal{P}$ est système de représentants des irréductibles modulo les inversibles.
3. Montrer que si A est factoriel et que $f, g \in A$ sont premiers entre eux, alors pour tout $h \in A$, f divise gh *si et seulement si* f divise h (lemme de Gauss).

Exercice (plus concret).

1. Soit K un corps et $F \in K[X]$.
   (a) Montrer que si $\deg F = 1$, alors F est irréductible.
   (b) Si $\deg F > 1$ et F est irréductible, montrer que F n'a pas de racine dans K.
   (c) Si $\deg F \in \{2, 3\}$, montrer que F est irréductible si et seulement s'il n'a pas de racine dans K.

2. Soient $F_d, F_{d-1} \in K[X_1, \ldots, X_n]$ des polynômes homogènes de degrés respectifs d et $d-1$. Montrer que $F_d + F_{d-1}$ est irréductible *si et seulement si* F_d et F_{d-1} sont premiers entre eux.

Remarque. $R[X_1, \ldots, X_n]^\times = R^\times$. Ce n'est pas toujours vrai lorsque R n'est pas intègre (un contre-exemple est $R = \mathbb{R}[T]/T^2$ avec $1 + \overline{T}X \in R[X]$).

Exemples.

— Le polynôme $X^4 + 2X^2 + 1 \in \mathbb{R}[X]$ n'est pas irréductible car $X^4 + 2X^2 + 1 = (X^2 + 1)^2$ et n'a pas de racine.

— Soit $F_4 = X^4 + Y^4$, $F_3 = X^3 - 2X^2Y + XY^2$, et $F = F_4 + F_3$ (en tant qu'éléments de $\mathbb{R}[X, Y]$). F est irréductible car F_4 et F_3 sont premiers entre eux ($\mathbb{R}[X, Y]$ est factoriel). En effet, $F_3 = X(X - Y)^2$ mais X ne divise pas F_4 et $X - Y$ ne divise pas F_4. Une autre façon de montrer qu'ils sont premiers entre est d'observer que sinon (en prenant $Y = 1$), X divise $X^4 + 1$ ou $X - 1$ divise $X^4 + 1$ ce qui n'est pas possible.

Définition 1.2.6. *Un élément $d \in A$ est dit être un* pgcd *(resp.* ppcm*) de $f, g \in A$ si (d) est le plus petit (resp. plus grand) idéal principal contenant f et g (resp. contenu dans (f, g)).*

Remarque. À priori, d n'existe pas toujours. S'il existe, il n'est pas non plus nécessairement unique.

Exercice.

1. Montrer que f et g sont premiers entre eux *si et seulement si* 1_A est un pgcd de f et g.
2. Si A est principal, alors pour tout $f, g \in A$, il existe un pgcd d de f et g tel que $(f, g) = (d)$.
3. Si A est factoriel, alors pour tout $f, g \in A$ avec

$$f = u \prod_{p \in \mathcal{P}} p^{v_p} \quad \text{et} \quad g = v \prod_{p \in \mathcal{P}} p^{w_p},$$

alors

$$d = \prod_{p \in \mathcal{P}} p^{\min(v_p, w_p)}$$

est un pgcd de f et g. Les résultats sont les mêmes pour le ppcm en remplaçant le minimum par un maximum.

Définition 1.2.7. *Un polynôme $F \in R[X]$ est dit primitif si ses coefficients sont premiers entre eux.*

Remarque. SI $F \in K[X]$ est non nul avec $K = \mathrm{Frac}(R)$, on peut trouver $c \in K$ de sorte que $\frac{1}{c}F$ soit primitif.

Théorème 1.2.1. *Si R est un anneau factoriel, $R[X_1, \ldots, X_n]$ l'est aussi.*

Démonstration. Remarquons d'abord que $R[X_1, \dots, X_n]$ est isomorphe à $R[X_1, \dots, X_{n-1}][X_n]$, il suffit donc de montrer le résultat pour $n = 1$ et une récurrence donnera le résultat complet. Soit $K = \mathrm{Frac}(R)$. $K[X]$ est principal (car euclidien) donc factoriel. Il existe donc un système Q de représentants d'irréductibles modulo les inversibles. Sans perte de généralité, on peut supposer que les éléments de $\mathcal{Q}$ sont primitifs. Soit $F \in K[X]$ écrit de manière unique

$$F = a \prod_{P \in \mathcal{Q}} p^{v_P}$$

avec $a \in K^\times$. Or, puisque $F \in R[X]$ et les p sont primitifs, a est élément de R (exercice). R est factoriel donc $a = u \prod_{p \in \mathcal{P}} p^{w_p}$ avec $\mathcal{P}$ un système d'irréductibles pour R. On a donc

$$F = u \prod_{p \in \mathcal{P}} p^{w_p} \prod_{P \in \mathcal{Q}} P^{v_P}.$$

□

Remarque. $\mathcal{P} \cup \mathcal{Q}$ est un système de représentants d'irréductibles pour $R[X]$. En conséquence, les irréductibles de $R[X]$ sont les irréductibles de R et les polynômes primitifs irréductibles dans $K[X]$ avec $K = \mathrm{Frac}(R)$.

Exercice. Soit R un anneau factoriel.

1. Soient $F, G \in R[X]$. Montrer que si F et G sont premiers dans $K[X]$, alors ils sont premiers entre eux dans $R[X]$. Montrer que la réciproque est vrai lorsque F et G sont primitifs.
2. Soit $F \in R[X]$. Montrer que F est non constant et irréductible dans $R[X]$ *si seulement s'*il est primitif et irréductible dans $K[X]$.
3. *Critère d'*Eisenstein. Soit R un anneau factoriel, $F = \sum_{k=0}^{d} a_k X^k \in F[X]$ un polynôme primitif. Supposons qu'il existe $\mathfrak{P} \subset R$ un idéal premier tel que $a_d \notin \mathfrak{P}$, $a_{d-1}, \dots, a_0 \in \mathfrak{P}$, et $a_0 \notin \mathfrak{P}^2$ (où $\mathfrak{P}^2$ est l'idéal engendré par les carrés des éléments de $\mathfrak{P}$). Alors, F est irréductible.

Exemples.

— Soit $F = X^2Y^2 - X^2 + Y^2 + 1 \in \mathbb{R}[X, Y]$. On a $F = (X^2 + 1)Y^2 - (X^2 - 1) \in \mathbb{R}[X][Y]$. Ce polynôme est primitif en tant qu'élément de $\mathbb{R}[X][Y]$. F est de degré 2 et peut être vu comme élément de $\mathbb{R}(X)[Y]$ (puisque $\mathrm{Frac}(\mathbb{R}[X]) = \mathbb{R}(X)$). Puisque $\mathbb{R}(X)$ est un corps, il suffit de montrer que F n'a pas de racine dans $\mathbb{R}[X]$, c'est-à-dire que $\frac{X^2-1}{X^2+1}$ n'est pas un carré dans $\mathbb{R}(X)$. En effet, si R est un anneau factoriel, $K = \mathrm{Frac}(R)$ et $a, b \in R$ avec $b \neq 0_R$ sont premiers entre eux, alors a/b est un carré dans K *si et seulement si* a et b sont des carrés dans R.

Remarquons qu'on peut montrer le résultat avec le critère d'Eisenstein en prenant $\mathfrak{P} = (X - 1)$ dans $\mathbb{R}[X][Y]$.

— Le polynôme $X^7 + X^4Y^2 + Y$ est irréductible. Pour montrer cela, on peut utiliser le critère d'Eisenstein avec $\mathfrak{P} = (Y)$. On peut aussi écrire que $X^4Y^2 + Y + X^7 \in \mathbb{R}[X][Y]$ est primitif de degré 2 sans racine. Si ce n'est pas le cas, alors si $F \in \mathbb{R}(X)$ en est une racine, on a $X^4F^2 + F + X^7 = 0$ donc $(X^4F + 1)F = -X^7$. On a donc $4 + 2 \deg F = 7$, ce qui est impossible.

1.3 Résultant

Soit R un anneau intègre, et soit K son corps de fraction. Soient $F, G \in R[X]$ de degrés respectifs d et e avec $d + e > 0$.

Définition 1.3.1. *Le résultant de F et G est le déterminant de l'application de* Sylvester

$$\mathscr{S}\left|\begin{array}{ccc} R[X]_{<e}\times R[X]_{<d} & \longrightarrow & R_{<d+e}[X] \\ (U,V) & \longmapsto & UF+VG \end{array}\right.$$

dans les bases $(X^{e-1},\dots,1)$, $(X^{d-1},\dots,1)$ et $(X^{d+e-1},\dots,1)$, noté $\operatorname{Res}(F,G)$.

Remarque. Cette application a pour matrice

$$\begin{pmatrix} a_d & 0 & \cdots & 0 & b_e & 0 & \cdots & 0 \\ a_{d-1} & a_d & \ddots & \vdots & \vdots & b_e & \ddots & \vdots \\ \vdots & a_{d-1} & \ddots & 0 & \vdots & & \ddots & 0 \\ \vdots & \vdots & \ddots & a_d & b_1 & & & b_e \\ a_0 & & & a_{d-1} & b_0 & \ddots & \vdots & \vdots \\ 0 & \ddots & & \vdots & 0 & \ddots & b_1 & \vdots \\ \vdots & \ddots & a_0 & \vdots & \vdots & \ddots & b_0 & b_1 \\ 0 & \cdots & 0 & a_0 & 0 & \cdots & 0 & b_0 \end{pmatrix} \in \mathcal{M}_{e+d}(R),$$

qui a e colonnes de a_i et d colonnes de b_j.

Exercice.

1. Montrer que $\operatorname{Res}(G,F) = (-1)^{de}\operatorname{Res}(F,G)$.
2. Montrer que pour tout $c\in R$, $\operatorname{Res}(cF,G) = c^e\operatorname{Res}(F,G)$ et $\operatorname{Res}(F,cG) = c^d\operatorname{Res}(F,G)$.
3. Montrer que pour tout $\alpha\in R$, $\operatorname{Res}(F(X-\alpha),G(X-\alpha)) = \operatorname{Res}(F,G)$.

Exemples.

— Si $b\in R$,

$$\operatorname{Res}(F,b) = \begin{vmatrix} b & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & b \end{vmatrix} = b^d.$$

De même, $\operatorname{Res}(a,G) = a^e$ pour tout $a\in R$.

— Pour tout $G\in R[X]$ de degré e,

$$\operatorname{Res}(X,G) = \begin{vmatrix} 1 & 0 & \cdots & \cdots & 0 \\ 0 & \ddots & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & 1 & 0 \\ b_e & b_{e-1} & \cdots & \cdots & b_0 \end{vmatrix} = b_0.$$

De même, $\operatorname{Res}(F,X) = (-1)^d a_0$.

— On a

$$\mathrm{Res}(X^2-1, X^3-1) = \begin{vmatrix} 1 & 0 & -1 & 0 & 0 \\ 0 & 1 & 0 & -1 & 0 \\ 0 & 0 & 1 & 0 & -1 \\ 1 & 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 & -1 \end{vmatrix} \overset{L_4 \leftarrow L_4 - L_1}{=} \begin{vmatrix} 1 & 0 & -1 & 0 & 0 \\ 0 & 1 & 0 & -1 & 0 \\ 0 & 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & -1 & 0 \\ 0 & 1 & 0 & 1 & -1 \end{vmatrix} = 1 - 1 = 0.$$

Proposition 1.3.1. *Il existe $U \in \mathbb{R}[X]_{<e}$ et $V \in R[X]_{<d}$ tels que $\mathrm{Res}(F,G) = UF + VG$ (en tant que polynôme constant).*

Démonstration. On rappelle la formule de Laplace : pour tout $M \in \mathcal{M}_n(R)$, il existe $M^* \in \mathcal{M}_n(R)$ tel que $MM^* = M^*M = \det(M)I_n$. En conséquence, pour tout $M \in \mathcal{M}_n(R)$ et $w \in R^n$, il existe $v \in \mathbb{R}^n$ tel que $Mv = \det(M)w$ (en fait, $v = M^*w$). On l'applique ici avec $w = 1 \in R[X]_{d+e}$ (dans les bases canoniques). Il existe $(U,V) \in R[X]_{<e} \times R[X]_{<d}$ tel que $\mathscr{S}(U,V) = \det \mathscr{S}$.

□

Exercice.

1. Montrer que $\mathrm{Res}(F,G) \in R \cap (F,G)$.
2. Montrer que s'il existe $\alpha \in R$ tel que $F(\alpha) = G(\alpha) = 0$, alors $\mathrm{Res}(F,G) = 0$.

Proposition 1.3.2. *On a $\mathrm{Res}(F,G) = 0$ si et seulement s'il existe $U \in R[X]_{<e}\backslash\{0\}$ et $V \in R[X]_{<d}\backslash\{0\}$ tels que $UF + VG = 0$.*

Démonstration. On a les équivalences suivantes.

$$\begin{aligned} \mathrm{Res}(F,G) = 0 &\iff \det \mathscr{S} = 0 \\ &\iff \mathscr{S} \text{ n'est pas injective} \\ &\iff \ker \mathscr{S} \neq \{0\} \\ &\iff \exists (U,V) \in (R[X]_{<e} \times R[X]_{<d})\backslash\{(0,0)\}, \mathscr{S}(U,V) = 0 \\ &\iff \exists (U,V) \in (R[X]_{<e} \times R[X]_{<d})\backslash\{(0,0)\}, UF + VG = 0 \\ &\iff \exists U \in R[X]_{<e}\backslash\{0\}, \exists V \in R[X]_{<d}\backslash\{0\}, UF + VG = 0. \end{aligned}$$

□

Corollaire 1.3.1. *Si R est factoriel, alors $\mathrm{Res}(F,G) \neq 0$ si et seulement si $F \wedge G = 1$ dans $K[X]$ où $K = \mathrm{Frac}(R)$.*

Démonstration. $\boxed{\Longrightarrow}$ On a $F \wedge G \neq 1$ dans $R[X]$ *si et seulement s'*il existe $H \in R[X]$ avec $\deg H > 0$, $H|F$ et $H|G$, et $c \in R$ tel que $c \notin R^\times$ tel que $c|F$ et $c|G$. Ainsi, $F \wedge G \neq 1$ dans $R[X]$ *si et seulement s'*il existe $H \in R[X]$ avec $\deg H > 0$, $H|F$ et $H|G$. Si $F \wedge G \neq 1$ dans $K[X]$, il existe $H \in R[X]$ avec $\deg H > 0$ tel que $F = -VH$ et $G = UH$ avec $U \in R[X]_{<e}$ et $V \in R[X]_{<d}$. Alors, $UF + VG = -UVH + VUH$. Ainsi, $\mathrm{Res}(F,G) = 0$.

$\boxed{\Longleftarrow}$ Supposons que F et G soient premier entre eux, et que $\mathrm{Res}(F,G) = 0$. Selon la proposition précédente, il existe $U \in R[X]_{<e}\backslash\{0\}$ et $V \in R[X]_{<d}\backslash\{0\}$ tels que $UF + VG = 0$. On a donc $-UF = VG$ donc F divise VG. Par le lemme de GAUSS, F divise V dans $K[X]$ et nécessairement $V = 0$ car $\deg F > \deg V$, ce qui est contradictoire.

□

Lemme 1.3.1. *Pour tout $\alpha \in R$, $\mathrm{Res}((X-\alpha)F, G) = G(\alpha)\,\mathrm{Res}(F,G)$.*

Démonstration. Quitte à translater, on peut supposer que $\alpha = 0$ (puisque que le résultant est invariant par translation). On a

$$\mathrm{Res}(XF,G) = \begin{vmatrix} & & (\mathrm{mat}\,\mathscr{S}) & & 0 \\ & & & & \vdots \\ & & & & 0 \\ 0 & \cdots & 0 \quad b_e & b_{e-1} \quad \cdots & b_0 \end{vmatrix} = b_0\,\mathrm{Res}(F,G).$$

En effet, $XF = \sum_{k=1}^{d+1} a_{k-1}X^k$ et $b_0 = G(0)$.

□

Exercice.

(*i*) Montrer que si $F = a_d \prod_{i=1}^{d}(X-\alpha_i)$, alors $\mathrm{Res}(F,G) = a_d^e \prod_{i=1}^{d} G(\alpha_i)$.

(*ii*) Montrer que si $G = b_e \prod_{j=1}^{e}(X-\beta_j)$, alors $\mathrm{Res}(F,G) = a_d^e b_e^d \prod_{i,j}(\alpha_i - \beta_j)$.

Proposition 1.3.3. *On a les propriétés suivantes.*

— $\mathrm{Res}(F, G_1G_2) = \mathrm{Res}(F,G_1)\,\mathrm{Res}(F,G_2)$.

— *Si $G = QF + H$, alors* $\mathrm{Res}(F,G) = a_d^{e-f}\,\mathrm{Res}(F,H)$ *avec* $f = \deg H$.

Démonstration. On a $R \subset K \subset K^{\mathrm{alg}}$ où K^{alg} est la clôture algébrique de K. On peut donc supposer que R est un corps algébriquement clos. Montrons uniquement le second point (le premier est en exercice). On a $F = a_d\prod_{i=1}^{d}(X-\alpha_i)$ avec $\alpha_i \in R$, donc $\mathrm{Res}(F,G) = a_d^e\prod_{i=1}^{d}G(\alpha_i) = a_d^{e-f}a_d^f\prod_{i=1}^{d}H(\alpha_i) = a_d^{e-f}\,\mathrm{Res}(F,H)$, car $G(\alpha_i) = Q(\alpha_i)F(\alpha_i) + H(\alpha_i) = H(\alpha_i)$ pour tout $i \in [\![1,d]\!]$.

□

Exercice. Calculer $\mathrm{Res}(X^n+1, X^{n+1}+1)$. *Indication : traiter le cas $n=1$ et remarquer que $X^{n+1}+1 = (X^n+1)X + (-X+1)$.*

1.4 Base de GRÖBNER

Dans la théorie des polynômes en une variable, on peut écrire $R[X]_{<d} \cong R[X]/F$. Cela est permis par l'existence d'une division euclidienne sur l'anneau $R[X]$ car le degré définit un ordre total sur les monômes, et est additif. Cet argument fonctionne en une variable, mais comment généraliser en plusieurs variables ? Il est clair (avec l'ordre du degré) que "$X^7 \geq X^5$", mais a-t-on "$X^2Y \leq XZ^2$". Les bases de GRÖBNER sont la réponse à ce problème et vont permettre de généraliser dans la théorie en plusieurs variables.

Dans cette section, k désignera un corps. On note $i = (i_1,\ldots,i_n) \in \mathbb{N}^n$, et $|i| = i_1 + \cdots + i_n$. De même, on notera $X^i = X_1^{i_1}\cdots X_n^{i_n}$.

Définition 1.4.1. *Un ordre total additif (ou admissible) sur $\mathbb{N}^n$ est une relation $\leq$ sur $\mathbb{N}^n$ telle que*

- *(total) pour tout $i, j \in \mathbb{N}^n$, $i \leq j$ ou $j \leq i$;*
- *(antisymétrie) pour tout $i, j \in \mathbb{N}^n$, si $i \leq j$ et $j \leq i$, alors $i = j$;*
- *(transitivité) pour tout $i, j, k \in \mathbb{N}^n$, si $i \leq j$ et $j \leq k$, alors $i \leq k$;*
- *pour tout $i, j, k \in \mathbb{N}^n$, si $i \leq j$, alors $i + k \leq j + k$;*
- *Pour tout $i \in \mathbb{N}^n$, $0 \leq i$.*

Remarques.

- Les trois premières conditions sont celles d'un ordre total, tandis que les deux dernières correspondent à l'additivité.
- On inclut toujours la condition de réflexivité dans la définition d'un ordre. Il n'est pas nécessaire ici de l'imposer puisqu'elle est une conséquence de la totalité de l'ordre.

Exercice.

1. Montrer qu'il existe un unique ordre total additif sur $\mathbb{N}$ (cas $n = 1$).
2. Montrer que la relation définie par "$(i_1, i_2) \leq (j_1, j_2)$ *si et seulement si* $i_1 \leq j_1$ et $i_2 \leq j_2$" n'est pas un ordre total additif sur $\mathbb{N}^2$. Montrer qu'il en est de même pour la relation définie par "$(i_1, i_2) \leq (j_1, j_2)$ *si et seulement si* $i_1 + j_1 \leq i_2 + j_2$".
3. Montrer qu'un ordre total additif est un bon ordre, *i.e* que toute partie minorée possède un minimum.

Définition 1.4.2. *On définit un ordre total additif sur $\mathbb{N}^n$ en posant $i \leq j$ lorsque*

- *(ordre lexicographique – lex) le premier terme non nul de $j - i$ non nul est strictement positif ;*
- *(ordre lexicographique inversé – invlex) le dernier terme non nul de $j - i$ non nul est strictement positif ;*
- *(ordre lexicographique gradué – deglex) $|i| < |j|$, ou $|i| = |j|$ et le premier terme non nul de $j - i$ non nul est strictement positif ;*
- *(ordre lexicographique inverse gradué – degrevlex) $|i| < |j|$, ou $|i| = |j|$ et le dernier terme non nul de $j - i$ est strictement négatif.*

Remarques.

- L'ordre lexicographique inverse gradué est l'ordre permettant des calculs par ordinateur les plus optimisés dans le cadre de la théorie de cette section.
- On notera $X^i \leq X^j$ lorsque $i \leq j$ (en fonction de l'ordre $\leq$ choisi).

Exemple. On étudie les monômes XZ, X, Y^2, et Y.

- (*lex*) $XZ > X > Y^2 > Y$;
- (*invlex*) $XZ > Y^2 > Y > X$;
- (*deglex*) $XZ > Y^2 > X > Y$;
- (*degrevlex*) $Y^2 > XZ > X > Y$.

On fixe un ordre total additif sur $\mathbb{N}^n$ (ce qui nous donne un ordre admissible sur les monômes).

Définition 1.4.3. *Soit $F \in k[X_1, \ldots, X_n]$. On appelle monôme dominant (resp. terme dominant) de F le monôme (resp. le terme) maximal de F. On appelle coefficient dominant de F le coefficient apparaissant dans son terme dominant.*

Remarque. On note $M(F)$ le monôme dominant, $T(F)$ le derme dominant, et $c(F)$ le coefficient dominant. On choisit les conventions $M(0) = T(0) = c(0) = 0$.

Exemple. Si $F = 3X^2Y + 3Y^2 - 2X^2 - 11Y$ et on utilise l'ordre lexicographique (et ce pour toute cette section). On a alors $M(F) = X^2Y$, $T(F) = 2X^Y$ et $c(F) = 3$.

Exercice.

1. Montrer que $M(F) = 0$ *si et seulement si* $F = 0$, et que $M(F) = 1$ *si et seulement si* F est constant.
2. Montrer que pour tout $F, G \in k[X_1, \ldots, X_n]$, $M(FG) = M(F)M(G)$.
3. Montrer que pour tout $F, G \in k[X_1, \ldots, X_n]$, $M(F+G) \leq \max(M(F), M(G))$ avec égalité si $M(F) \neq M(G)$.

Définition 1.4.4. *Soit $F, G, H \in k[X_1, \ldots, X_n]$, et S une partie de $k[X_1, \ldots, X_n]$.*

— *On dit que F se réduit en H modulo G en une étape, noté $F \xrightarrow{G} H$, si $F = GQ + H$ et $T(G)Q$ est un terme de F, où Q est un terme.*

— *On dit que F se réduit en H modulo S, noté $F \xrightarrow{S}_+ H$ s'il existe $G_1, \ldots, G_r$ tels que*

$$F \xrightarrow{G_1} \cdots \xrightarrow{G_2} \cdots \xrightarrow{G_r} H.$$

— *On dit que F est une forme normale modulo S si aucun terme de F n'est multiple d'un $M(G)$ avec $G \in S$ (i.e que F n'est pas réductible modulo S).*

Exemples.

— *Réduction en un étape.* Soit $F = X^2Y + XY^2 + Y^2$ et $G = (XY - 1)$. On a $F = XG + XY^2 + X + Y^2$.

— *Réduction selon une partie.* Soit $F = X^2 + XY^2 + Y^2$, et $S = \{XY - 1, Y^2 - 1\}$. On a

$$F \xrightarrow{XY-1} XY^2 + X + Y^2 \xrightarrow{XY-1} X + Y^2 + Y \xrightarrow{Y^2-1} X + Y + 1.$$

En effet, $XY^2+X+Y^2 = (XY-1)Y+X+Y^2+Y$, et $X+Y^2+Y = (Y^2-1)\times 1+X+Y+1$.

Exercice.

1. Montrer que les formes normales modulo S forment un sous-espace vectoriel (noté E) de $k[X_1, \ldots, X_n]$. Montrer que les monômes qui sont pas multiples de $M(G)$ avec $G \in S$ forment une base[4] de E.
2. Montrer que tout polynôme $F \in k[X_1, \ldots, X_n]$ se réduit modulo S une forme normale H. Montrer de plus que $F \equiv H \mod S$ (*i.e* que $F - H \in (S)$).

4. Dans l'exemple précédent, cette base est $\{1, X, Y, X^2, X^3, \ldots\}$.

Remarques.

— Dans le cas d'une variable donc dans $k[X]$, si $F = GQ+R$ avec $\deg R < \deg G$, alors $F \equiv R \mod G$. La définition précédente permet de se rapprocher d'une division euclidienne sur $k[X_1, \ldots, X_n]$.

— Si $F \xrightarrow[S]{}_+ H$, H n'est généralement *pas unique.*

Notations. Si $S \subset k[X_1, \ldots, X_n]$, on note $\mathcal{I} = (S)$ l'idéal engendré par S. On note $M(S)$ l'image de S par l'application M (*i.e* que $M(S)$ est l'ensembles des monômes dominants de S). Généralement, $(M(S)) \neq (M(\mathcal{I}))$. Par exemple, si $S = \{XY-1, Y^2-1\}$, on a $\mathcal{I} = (XY-1, Y^2-1)$, $M(S) = \{XY, Y^2\}$, $(M(S)) = (XY, Y^2)$, et $(M(\mathcal{I})) = (X, Y^2)$. On a donc $(M(S)) \neq (M(\mathcal{I}))$.

Définition 1.4.5. *Une partie $S \subset k[X_1, \ldots, X_n]$ est dite être une* base de Gröbner *pour un idéal $\mathcal{I}$ si $(M(S)) = (M(\mathcal{I}))$.*

Attention. S n'est pas nécessairement fini.

Exercice.

(*i*) Montrer qu'une partie $S \subset k[X_1, \ldots, X_n]$ est une base de Gröbner pour $\mathcal{I}$ *si et seulement si* pour tout $F \in \mathcal{I}$, il existe $G \in S$ tel que $M(G)$ divise $M(F)$.

(*ii*) Montrer que $\mathcal{I}$ est une base de Gröbner pour $\mathcal{I}$.

(*iii*) Montrer que si $S \subset S' \subset \mathcal{I}$ sont des parties de $\mathcal{I}$ et S est une base de Gröbner pour $\mathcal{I}$, alors S' l'est aussi.

(*iv*) Montrer que toute base de Gröbner contient une base de Gröbner finie.

Lemme 1.4.1. *Si S est une base de* Gröbner *pour $\mathcal{I}$, alors $\mathcal{I} = (S)$.*

Démonstration. Soit $F \in \mathcal{I}$. On a $F = T(F) + (F - T(F))$. On a $F = T(G)Q + (F - T(F)) = GQ + (T(G) - G)Q + (F - T(F))$ où $G \in S$ est tel que $M(G)$ divise $M(F)$. On a donc $F = GQ + H$ avec $G \in S$ et $M(H) < M(F)$ où $H = (T(G) - G)Q + (F - T(F))$. On a donc $H = F - GQ \in \mathcal{I}$. On conclut par récurrence.

□

Théorème 1.4.1. *Si $S \subset k[X_1, \ldots, X_n]$ est une base de* Gröbner*, alors tout $F \in k[X_1, \ldots X_n]$ se réduit de manière unique en une forme normale H modulo S. De plus, H ne dépend que de F modulo S.*

Démonstration. Soit $F_1, F_2 \in k[X_1, \ldots, X_n]$ se réduisant chacun en une forme normale H_1 et H_2 modulo S, et telles que $F_1 \equiv F_2 \mod S$. Alors, on a $H := H_2 - H_1 \equiv F_2 - F_1 \equiv 0 \mod S$, donc H est élément de (S). Mais comme les formes normales forment un sous espace vectoriel, H est une forme normale. Puisque $H \in (S)$, il existe $G \in S$ tel que $M(G)$ divise $M(H)$. Or, H étant une forme normale, il est nécessaire que $H = 0$. On a donc $H_1 = H_2$.

□

Remarque. On peut donc dire que H est *le* reste de F modulo S.

Rappel. Si $\mathcal{I}, \mathcal{J} \subset A$ sont des idéaux de l'anneau A, $\mathcal{I}+\mathcal{J} = \{f+g \,|\, (f,g) \in \mathcal{I}\times\mathcal{J}\}$ et $\mathcal{I}\mathcal{J} = (\{fg \,|\, (f,g) \in \mathcal{I}\times\mathcal{J})\}$ sont des idéaux . On définit récursivement $\mathcal{I}^n = \mathcal{I}^{n-1}\mathcal{I} = (\{f_1\cdots f_n \,|\, f_1,\ldots,f_n \in \mathcal{I}\})$. Par exemple, on a

$$(X_1,\ldots,X_n)^N = \{X_1^{N_1}\cdots X_n^{N_n} \,|\, N_1+\cdots+N_n = N\}.$$

Exercice.

1. Montrer que si S est une base de GRÖBNER pour $\mathcal{I}$, alors le reste de F modulo S ne dépend que $\mathcal{I} = (S)$.
2. Montrer que si S est une base de GRÖBNER pour $\mathcal{I}$, on a un isomorphisme

   $$E \cong k[X_1,\ldots,X_n]/\mathcal{I}$$

   où E l'ensemble des formes normales modulo S.
3. Montrer que les assertions suivantes sont équivalentes.

   (*i*) $k[X_1,\ldots,X_n]/\mathcal{I}$ est de k-dimension finie.

   (*ii*) Il existe $N \in \mathbb{N}$ tel que $(X_1,\ldots,X_n)^N \subset (M(\mathcal{I}))$.

   (*iii*) Pour tout $i \in [\![1,n]\!]$, il existe $N_i \in \mathbb{N}$ tel que $X_i^{N_i} \in M(\mathcal{I})$.

   (*iv*) Si S est une base de GRÖBNER pour $\mathcal{I}$, alors pour tout $i \in [\![1,n]\!]$, il existe $N_i \in \mathbb{N}$ et $G_i \in S$ tel que $M(G_i) = X_i^{N_i}$.

Exemple. Si $\mathcal{I} = (XY-1, Y^2-1) = (X-Y, Y^2-1)$, alors $\{X-Y, Y^2-1\}$ est une base de GRÖBNER.

Définition 1.4.6. *Le S-polynôme de G et H, éléments de $k[X_1,\ldots,X_n]$, est le polynôme*

$$S(G,H) = \frac{M(G)\vee M(H)}{T(G)}G - \frac{M(G)\vee M(H)}{T(H)}H.$$

Exemple. Si $G = XY-1$ et $H = Y^2-1$, alors $S(G,H) = Y(XY-1) - X(Y^2-1) = X-Y$.

Théorème 1.4.2 (BUCHBERGER)**.** *Soit $S \subset k[X_1,\ldots,X_n]$. S est une base de* GRÖBNER si et seulement si *pour tout $G,H \in S$, $S(G,H) \xrightarrow{S}_+ 0$.*

Démonstration. Laborieux. Pas le temps. On s'en dispense.

□

Exercice.

1. Montrer la correction de l'algorithme de BUCHBERGER. L'algorithme de BUCHBERGER permet de transformer une partie finie S quelconque en une base de GRÖBNER. Notons $S = \{G_1,\ldots,G_r\}$. Le principe est le suivant : on vérifie si $S(G_i,G_j) \xrightarrow{S}_+ 0$ pour tout $i,j \in [\![1,r]\!]$. Si c'est le cas, alors S est une base de GRÖBNER. Sinon, on rajoute à S les formes normales de $S(G_i,G_j)$ pour tout les couples $(i,j) \in [\![1,r]\!]^2$ qui ont mis le test en défaut. On recommence jusqu'à atteindre la condition d'arrêt. L'algorithme se termine bien en vertu du théorème de la base de NOETHER.
2. Montrer que tout idéal possède une unique base de GRÖBNER réduite, *i.e* que pour tout $G \in S$, $c(G) = 1$ et G et une forme normale modulo $S\backslash\{G\}$.

Exemple. Soit $S = \{XY - 1, Y^2 - 1\}$. On a $S(XY - 1, Y^2 - 1) = X - Y$, qui est une forme normale modulo S. Soit $S' = \{XY - 1, Y^2 - 1, X - Y\}$. On a $S(XY - 1, Y^2 - 1) \xrightarrow{S'}_+ 0$ et $S(XY - 1, X - Y) = (XY - 1) - Y(X - Y) = Y^2 - 1 \xrightarrow{S'} 0$. On a $S(Y^2 - 1, X - Y) = X(Y^2 - 1) - Y^2(X - Y) = -X + Y^3 = -X + Y(Y^2 - 1) + Y \xrightarrow{S'}_+ -X + Y \xrightarrow{S'} 0$. Enfin, on a $XY - 1 = Y(X - Y) + Y^2 - 1 \xrightarrow{X-Y} Y - 1$, qui n'est pas une forme réduite : il suffit de l'enlever. Ainsi, $\{Y^2 - 1, X - Y\}$ est une base de GRÖBNER.

Application. La dimension de $k[X, Y]/(XY - 1, Y^2 - 1)$ est 2, car $\{Y^2 - 1, X - Y\}$ est une base de GRÖBNER et $E = \langle 1, Y \rangle$.

Principe de l'élimination...

— *... via les résultants.* Si $F, G \in k[X_1, \ldots, X_n]$ et $\mathcal{I} = (F, G)$, alors $\mathrm{Res}_{X_n}(F, G)$ est élément de $\mathcal{I} \cap k[X_1, \ldots, X_{n-1}]$.

— *... via les bases de* GRÖBNER. Soit $S \subset k[X_1, \ldots, X_n]$ une base de GRÖBNER pour l'ordre invlex et $\mathcal{I} = (S)$. Alors, $S \cap k[X_1, \ldots, X_n]$ est une base de GRÖBNEZR pour $\mathcal{I} \cap k[X_1, \ldots, X_m]$ avec $m \leq n$.

Chapitre 2

Ensembles algébriques

2.1 Lieux de zéros

Soit k un corps infini [1].

Définition 2.1.1. *L'ensemble $\mathbb{A}^n(k) = k^n$ est l'espace affine sur k.*

Remarques.

— On introduit cette notation redondante pour différencier l'espace vectoriel k^n en tant qu'espace de vecteurs et l'espace affine $\mathbb{A}^n(k)$ en tant qu'espace de points.

— $\mathbb{A}^1(k)$ est la droite affine et $\mathbb{A}^2(k)$ le plan affine. L'utilisation d'articles définies ne sous-entend pas qu'ils sont uniques. Elle sert seulement à les différencier avec les autres "plans" et "droites" affines que l'on pourra rencontrer et qui porteront le même nom (sans articles définis).

Définition 2.1.2. *Si $S \subset k[X_1, \dots, X_n]$, on appelle lieu des zéros de S l'ensemble*

$$\mathcal{V}(S) = \{p \in \mathbb{A}^n(k) \,|\, \forall F \in S,\, F(p) = 0\}.$$

Remarque. On le note $\mathcal{V}(s)$ si $S = \{s\}$ est un singleton.

Proposition 2.1.1. *On a les propriétés suivantes.*

(i) On a $\mathcal{V}(1) = \varnothing$ et $\mathcal{V}(0) = \mathbb{A}^n(k)$.

(ii) Pour toute famille $(S_\alpha)_{\alpha\in\Lambda}$ de parties de $k[X_1, \dots, X_n]$, on a

$$\bigcap_{\alpha\in\Lambda} \mathcal{V}(S_\alpha) = \mathcal{V}\left(\bigcup_{\alpha\in\Lambda} S_\alpha\right).$$

(iii) Soient $S, T \subset k[X_1, \dots, X_n]$. Alors, $\mathcal{V}(S) \cup \mathcal{V}(T) = \mathcal{V}(ST)$, où $ST = \{FG \,|\, F \in S, G \in T\}$.

(iv) Si $S \subset T \subset k[X_1, \dots, X_n]$, alors $\mathcal{V}(T) \subset \mathcal{V}(S)$.

1. Les premières définitions sont valables pour tous les corps, peu importe leur cardinaux. Cependant, seul l'étude des corps finis dans ce chapitre sera pertinente.

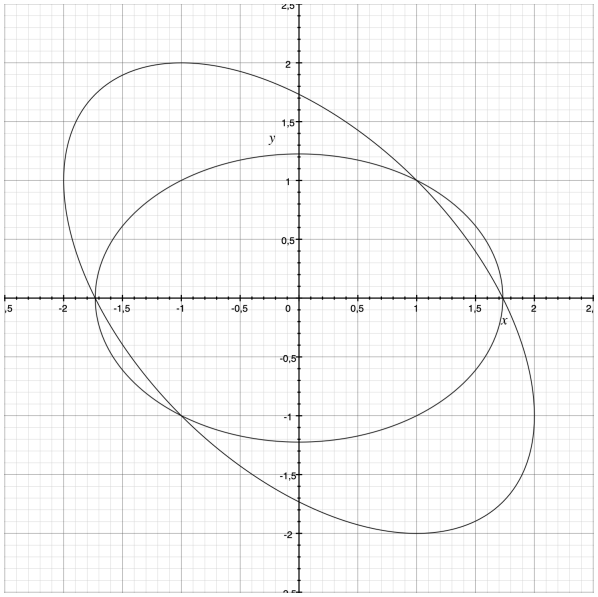


FIGURE 2.1 – Coniques définissant le système (E).

Démonstration. Clair.

□

Exercice. Si $F \in k[X_1, \ldots, X_n]$ et k est infini, alors $\mathcal{V}(F) = \mathbb{A}^n(k)$ *si et seulement si* $F = 0$. On pourra le démontrer par récurrence. Ce résultat n'est plus vrai lorsque k est fini : un polynôme sur un corps $\mathbb{F}_q$ peut être analytiquement nul sans nécessairement être formellement nul. Par exemple, $X(X-1)(X-2) \in \mathbb{F}_3$ est analytiquement nul mais n'est pas formellement nul.

Proposition 2.1.2. *Si $F, G \in k[X, Y]$ sont premiers entre eux, alors $\mathcal{V}(F, G)$ est fini.*

Démonstration. Puisque F et G sont premiers entre eux, $R_X = \mathrm{Res}_X(F, G) \neq 0$. De même, $R_Y = \mathrm{Res}_Y(F, G) \neq 0$. Les polynômes $R_X \in k[Y]$ et $R_Y \in k[X]$ sont non nuls et ont donc un nombre fini de racines, mais $\mathcal{V}(F, G) \subset \mathcal{V}(R_Y) \times \mathcal{V}(R_X)$. On conclut alors.

□

Remarque. On a en fait montrer dans la démonstration que $\operatorname{card} \mathcal{V}(F, G) \leq \deg R_X \deg R_Y$. En fait, cette majoration est très loin d'être optimale puisque le degré d'un résultant peut monter très vite en fonction des degrés de F et G. Une meilleure majoration (que l'on démontrera après une quantité non négligeable de travail) est $\operatorname{card} \mathcal{V}(F, G) \leq \deg F \deg G$.

Exemple. On étudie le système (E)

$$\left\{ \begin{array}{rcl} x^2 + 2y^2 & = & 3, \\ x^2 + xy + y^2 & = & 3. \end{array} \right.$$

On a alors $y(y - x) = 0$. Si $y = 0$, le système d'équations est vérifié *si et seulement si* $x^2 = 3$, *i.e* $x = \pm\sqrt{3}$. Si $y = x$, le système est vérifié *si et seulement si* $3x^2 = 3$, *i.e* $x = \pm 1$. L'ensemble des solutions est donc

$$\{(\sqrt{3}, 0), (-\sqrt{3}, 0), (-1, 1), (1, -1)\}.$$

Exercice. Montrer que si $f, g \in k[T]$ sont des polynômes non constants et

$$\mathcal{C} = \{(f(t), g(t)) \,|\, t \in k\}.$$

Si $R_T = \mathrm{Res}_T(f(T)-X, g(T)-Y) \in k[X,Y]$, alors $\mathcal{C} \subset \mathcal{V}(R_T)$ avec égalité si k est algébriquement clos.

Remarque. Si $\mathcal{I} = (S)$, alors $\mathcal{V}(\mathcal{I}) = \mathcal{V}(S)$.

Proposition 2.1.3. *Soit $\mathcal{I} \subset k[X_1, \ldots, X_n]$ un idéal tel que $d = \dim k[X_1, \ldots, X_n]/\mathcal{I} < \infty$. Alors, $\mathcal{V}(\mathcal{I})$ est fini et $\operatorname{card} \mathcal{V}(\mathcal{I}) \leq nd$.*

Démonstration. Les monômes $X_i^d, X_i^{d-1}, \ldots, X_i, 1$ sont linéaires dépendants modulo $\mathcal{I}$ (*i.e* dans $k[X_1, \ldots, X_n]/\mathcal{I} < \infty$). Il existe donc $(a_0, \ldots, a_d) \in k^{d+1}$ non nul tel que $F_i := a_d X_i^d + \cdots + a_1 X_i + a_0 \neq 0$ et $F_i \equiv 0 \mod \mathcal{I}$, *i.e* que $F_i \in \mathcal{I}$. Cela signifie que $\mathcal{V}(\mathcal{I}) \subset \mathcal{V}(F_1) \times \cdots \times \mathcal{V}(F_n)$ est fini.

□

2.2 Ensembles algébriques

Définition 2.2.1. *Un ensemble $V \subset \mathbb{A}^n(k)$ est dit être un* ensemble algébrique *s'il existe $S \subset k[X_1, \ldots, X_n]$ tel que $V = \mathcal{V}(S)$. On dit que $H \subset \mathbb{A}^n(k)$ est une* hypersurface *de degré $d > 0$ s'il existe $F \in k[X_1, \ldots, X_n]$ de degré d tel que $H = \mathcal{V}(F)$.*

Remarque. On parle de *courbe* si $n = 2$ et de *surface* si $n = 3$. Dans le cas $n = 2$ et $d = 2$, ces courbes sont appelées les coniques.

Exercices.

1. Montrer que $\varnothing$ et $\mathbb{A}^n(k)$ sont algébriques.
2. Montrer que les ensembles algébriques sont stables par intersection quelconque et par union finie.
3. Montrer que les ensembles finis sont algébriques.
4. Montrer que tout ensemble algébrique non vide est une intersection d'hypersurfaces.
5. Montrer que $V \subset \mathbb{A}^1(k)$ est algébrique *si et seulement si* $V = \mathbb{A}^1(k)$ et V est fini.

Proposition 2.2.1. *Si $V \subset \mathbb{A}^n(k)$ et $W \subset \mathbb{A}^m(k)$ sont algébriques, alors $V \times W \subset \mathbb{A}^{n+m}(k)$ l'est aussi.*

Démonstration. Soient $S \subset k[X_1, \ldots, X_n]$ tel que $V = \mathcal{V}(S)$ et $T \subset k[X_1, \ldots, X_m]$ tel que $V = \mathcal{V}(T)$. si $F \in S$, on note $\tilde{F} = F(X_1, \ldots, X_n)$ le polynôme élément de $k[X_1, \ldots, X_{n+m}]$ (et de même pour $G \in T$). On pose

$$\tilde{S} = \{\tilde{F}(X_1, \ldots, X_n) \,|\, F \in S\} \subset k[X_1, \ldots, X_{n+m}]$$

et

$$\tilde{T} = \{\tilde{G}(X_1, \ldots, X_n) \,|\, G \in T\} \subset k[X_1, \ldots, X_{n+m}].$$

Alors, $\mathcal{V}(S) \times \mathcal{V}(T) = \mathcal{V}(\tilde{S} \cup \tilde{T})$. Soit $\mathcal{P} \in \mathbb{A}^n(k)$ et $\mathcal{Q} \in \mathbb{A}^m(k)$. Alors,

$$\begin{aligned}(\mathcal{P}, \mathcal{Q}) \in \mathcal{V}(S) \times \mathcal{V}(T) &\iff \forall F \in S, \forall G \in T, (F(\mathcal{P}), G(\mathcal{Q})) = 0 \\ &\iff \forall \tilde{F} \in \tilde{S}, \forall \tilde{G} \in \tilde{T}, \tilde{F}(\mathcal{P}, \mathcal{Q}) = \tilde{G}(\mathcal{P}, \mathcal{Q}) = 0 \\ &\iff \forall H \in \tilde{S} \cup \tilde{T}, H(\mathcal{P}, \mathcal{Q}) = 0 \\ &\iff (\mathcal{P}, \mathcal{Q}) \in \mathcal{V}(\tilde{S} \cup \tilde{T}).\end{aligned}$$

□

Exercices.

1. Montrer que $H \subset \mathbb{A}^n(k)$ est un hyperplan affine *si et seulement si* H est une hypersurface de degré 1.
2. Montrer que $E \subset \mathbb{A}^n(k)$ est un sous-espace affine *si et seulement s'* il existe $F_1, \ldots, F_r \in k[X_1, \ldots, X_n]$ tels que $E = \mathcal{V}(F_1, \ldots, F_r)$ avec $\deg F_i = 1$ pour tout $i \in [\![1, r]\!]$ et $E \neq \varnothing$.

Proposition 2.2.2. *On a les propriétés suivantes.*

(i) Soit $V \subset \mathbb{A}^n(k)$ une courbe algébrique, et soit $L \subset \mathbb{A}^n(k)$ une droite. Si $L \not\subset V$, alors $L \cap V$ est fini.

(ii) Soient $V \subset \mathbb{A}^2(k)$ une courbe algébrique et $\mathcal{C} = \mathcal{V}(F) \subset \mathbb{A}^2(k)$ avec F un polynôme irréductible. Si $\mathcal{C} \not\subset V$, alors $\mathcal{C} \cap V$ est fini.

Démonstration. La première propriété est laissée en exercice. On montre donc la seconde. On peut supposer que $V = \mathcal{V}(G)$ avec $G \in k[X, Y]$. Puisque F est irréductible on a l'alternative suivante.

— Ou bien F divise G, donc $(G) \subset (F)$ et donc $\mathcal{V}(F) \subset \mathcal{V}(G)$ ($i.e$ $\mathcal{C} \subset V$) ;

— ou bien F et G sont premiers entre eux et alors $\mathcal{C} \cap V = \mathcal{V}(F) \cap \mathcal{V}(G) = \mathcal{V}(F, G)$.

□

Exercice. Soit $V, W \subset \mathbb{A}^n(k)$ des ensembles algébriques et $L \subset \mathbb{A}^n(k)$ une droite. Si $L \subset V \cup W$, alors $L \subset V$ ou $L \subset W$.

2.3 Fonctions polynomiales

Définition 2.3.1. *Soit $V \subset \mathbb{A}^n(k)$ un ensemble algébrique.*

— *Une application $f : V \longrightarrow k$ est dite* polynomiale *s'il existe $F \in k[X_1, \ldots, X_n]$ tel que pour tout $\mathcal{P} \in V$, $f(\mathcal{P}) = F(\mathcal{P})$.*

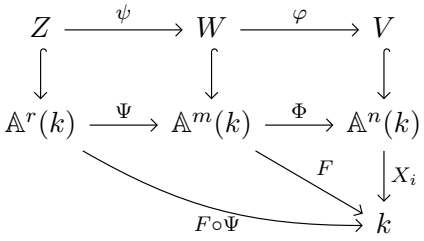
— *Soit $W \subset \mathbb{A}^n(k)$ et $V \subset \mathbb{A}^n(k)$ deux ensembles algébriques. Une application $\varphi : W \longrightarrow V$ est dite* polynomiale *si ses fonctions coordonnées sont des fonctions polynomiales.*

Exercice.

1. Montrer que si $V \subset \mathbb{A}^n(k)$, les fonctions coordonnées
$$x_i : \left| \begin{array}{rcl} V & \longrightarrow & k \\ \mathcal{P} = (a_1, \ldots, a_n) & \longmapsto & a_i \end{array} \right.$$
(pour tout $i \in [\![1, n]\!]$) sont polynomiales (prendre $F = X_i$).
2. Montrer que si $W \subset V \subset \mathbb{A}^n(k)$ sont des ensembles algébriques, alors l'application d'injection $W \longrightarrow V$ est polynomiale (ses composantes sont les x_i). En particulier l'identité $\mathrm{id}_V : V \longrightarrow V$ est une application polynomiale.
3. Montrer que si $V \subset \mathbb{A}^n(k)$ et $W \subset \mathbb{A}^m(k)$ sont algébriquement clos, les projections $P_1 : V \times W \longrightarrow V$ et $P_2 : V \times W \longrightarrow W$ sont polynomiales (de composantes x_i).
4. Soit $V \subset \mathbb{A}^n(k)$ et $W \subset \mathbb{A}^m(k)$ des ensembles algébriques, et soit $\varphi : W \longrightarrow V$. Montrer que φ est polynomiale *si et seulement si* elle se prolonge en une application polynomiale $\Phi : \mathbb{A}^m(k) \longrightarrow \mathbb{A}^n(k)$.
5. Montrer que les applications
$$\begin{array}{rcl} \mathcal{V}(XY-1) & \longrightarrow & \mathbb{R} \\ (a,b) & \longmapsto & b/a \end{array} \quad \text{et} \quad \begin{array}{rcl} \mathcal{V}(Y^4 - X) & \longrightarrow & \mathbb{R} \\ (a,b) & \longmapsto & \sqrt{a} \end{array}$$
sont polynomiales.

Proposition 2.3.1. *La composée de deux applications polynomiales est polynomiale.*

Démonstration. Soit $\psi : Z \longrightarrow W$ et $\varphi : W \longrightarrow V$ des applications polynomiales avec $Z \subset \mathbb{A}^r(k)$, $W \subset \mathbb{A}^m(k)$, et $V \subset \mathbb{A}^n(k)$. Les applications ψ et φ se prolongent en des applications $\Psi : \mathbb{A}^r(k) \longrightarrow \mathbb{A}^m(k)$ et $\Phi : \mathbb{A}^m(k) \longrightarrow \mathbb{A}^n(k)$. Notons X_i la projection en la i-ième coordonnée.



□

Exercice.

1. Montrer que si Φ :

Définition 2.3.2. *Soit W et V des ensembles algébriques. Un isomorphisme $\varphi : W \longrightarrow V$ est une application polynomiale bijective telle que φ^{-1} est polynomiale.*

Exemples.

— L'application $\mathcal{V}(Y - X^2) \subset \mathbb{A}^2(k) \to \mathcal{V}(Y)$, $(a, a^2) \mapsto (a, 0)$ (projection de la parabole sur l'abscisse) est un isomorphisme. Remarquons par ailleurs qu'un isomorphisme ne préserve pas nécessairement le degré.

— L'application $\mathcal{V}(Y^2 - X^3) \to \mathcal{V}(X)$, $(a, b) \mapsto (0, b)$ est polynomiale, bijective, mais n'est pas un isomorphisme.

Exercice.

1. Montrer que si $E \subset \mathbb{A}^m(k)$ et $F \subset \mathbb{A}^n(k)$ sont des sous-espaces affines, alors $\varphi : E \longrightarrow F$ est affine *si et seulement si* elle est polynomiale et ses composantes sont de degré 1.
2. Si $\varphi : E \longrightarrow F$ est une application affine bijective, alors φ est un isomorphisme.

2.4 Topologie de Zariski

Définition 2.4.1. *La topologie de* Zariski *sur un ensemble algébrique V est la topologie pour laquelle les fermés sont les sous-ensembles algébriques de V. On appelle* fermeture algébrique *d'une partie $A \subset V$ son adhérence dans V pour la topologie de* Zariski.

Exemples.

— Si $A = \mathbb{N}$ et $V = A^1(\mathbb{R})$, alors $\bar{A} = \mathbb{A}^1(\mathbb{R})$ (donc $\mathbb{N}$ est dense dans $\mathbb{R}$ pour la topologie de Zariski). En fait, la topologie de Zariski sur $\mathbb{A}^1(k)$ est la topologie cofinie.

— Si $A = \{(t^2, t^4) \,|\, t \in \mathbb{R}\}$ et $V = \mathbb{A}^2(\mathbb{R})$, alors $\bar{A} = \mathcal{V}(Y - X^2)$ (la fermeture géométrique d'une branche est la courbe tout entière).

Exercice.

1. Montrer que si W est un sous-ensemble algébrique de V, alors la topologie de Zariski sur W est la topologie induite par la topologie de Zariski de V.
2. Montrer qu'une application polynomiale est continue.
3. Montrer que si C est une droite, ou bien une courbe plane d'équation $F = 0$ où F est irréductible, alors la topologie de C est la topologie cofinie.
4. Montrer que les seuls fermés propres de $\mathbb{A}^2(k)$ pour la topologie produit sont les unions finies de droites horizontales, de droites verticales et de points. Cela signifie qu'un produit de topologies de Zariski n'est pas une topologie de Zariski.
5. Montrer que si V et W sont deux ensembles algébriques infinis, alors la topologie de Zariski sur $V \times W$ est strictement plus fine que la topologie produit des topologies de Zariski (et donc qu'une application $Z \longrightarrow V \times W$ dont les composantes sont continues n'est pas nécessairement continue).

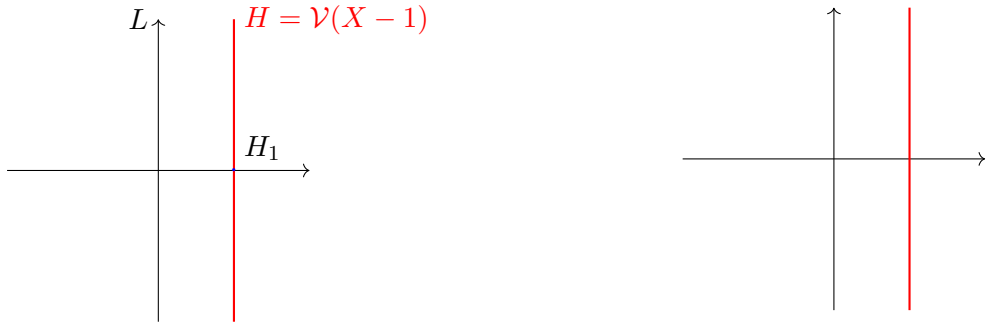
Proposition 2.4.1. *Si V et W sont deux ensembles algébriques, alors les projections $V \times W \longrightarrow V$ et $V \times W \longrightarrow W$ sont ouvertes pour les topologies de* Zariski.

Démonstration. Par symétrie des rôles, on montre uniquement un résultat. On a $V \subset \mathbb{A}^n(k)$ et $\subset \mathbb{A}^m(k)$, donc $V \times W \subset \mathbb{A}^{n+m}(k)$. Si $Q = (b_1, \ldots, b_m) \in \mathbb{A}^m(k)$ et $F \in k[X_1, \ldots, X_{n+m}]$, on pose

$$F_Q = F(X_1, \ldots, X_n, b_1, \ldots, b_m) \in k[X_1, \ldots, X_n].$$

Soit $U \subset V \times W$ un ouvert. Si $Z = (V \times W) \backslash U$, on peut écrire $Z = \mathcal{V}(S)$ avec $S \subset k[X_1, \ldots, X_{n+m}]$. On va montrer que le complémentaire de $p(U)$ est un sous-ensemble algébrique de V. Soit donc $P \in V$. On a les équivalences suivantes.

$$\begin{aligned} P \notin p(U) &\iff \forall Q \in W,\ (P, Q) \notin U \\ &\iff \forall Q \in W, (P, Q) \in Z \\ &\iff \forall Q \in W, \forall F \in S, F_Q(P) = F(P, Q) = 0. \end{aligned}$$



Il est donc clair que le complémentaire de $p(U)$ est l'ensemble algébrique $V \cap \mathcal{V}(T)$ avec

$$T = \{F_Q \mid \ F \in S, Q \in W\} \subset k[X_1, \ldots, X_n].$$

□

Corollaire 2.4.1. *Si $n \geq 1$, alors tout ouvert non vide de $\mathbb{A}^n(k)$ est infini.*

Démonstration. En utilisant la projection de $\mathbb{A}^n(k)$ sur $\mathbb{A}^1(k)$, on se ramène au cas $n = 1$ (puisque la projection $\mathbb{A}^1(k) \times \mathbb{A}^{n-1}(k) \longrightarrow \mathbb{A}^1(k)$ est ouverte). Or, la topologie de Zariski sur $\mathbb{A}^1(k)$ est la topologie cofinie (puisqu'un polynôme non nul en une variable a un nombre fini de zéros).

□

Proposition 2.4.2. *On suppose k algébriquement clos. Soit $H \subset \mathbb{A}^n(k)$ une hypersurface, et $\mathbb{A}^n(k) \longrightarrow \mathbb{A}^{n-1}(k)$ la projection et $L = \mathcal{V}(X_1, \ldots, X_{n-1})$ l'axe de X_n. On se trouve alors dans l'un des deux cas suivants.*

(i) Ou bien il existe une hypersurface $H_1 \subset \mathbb{A}^{n-1}(k)$ telle que $H = H_1 \times L$,

(ii) ou bien $p(H)$ contient un ouvert non vide de $\mathbb{A}^{n-1}(k)$.

Démonstration. Soit $H = \mathcal{V}(F)$ avec $F = F_d X_n^d + \cdots + F_1 X_n + F_0 \in k[X_1, \ldots, X_{n-1}][X_n]$ avec $F_d \neq 0$. Soit $H_1 = \mathcal{V}(F_d)$. Si $d = 0$, alors $H = H_1 \times L$. Sinon, on pose $U = \mathbb{A}^{n-1}(k) \backslash H_1$ qui est ouvert. Puisque F_d est non nul, $H_1 \neq \mathbb{A}^{n-1}(k)$ donc U est non vide. On va montrer que $U \subset p(H)$. Soit $(a_1, \ldots, a_{n-1}) \in U$. On a $F_d(a_1, \ldots, a_{n-1}) \neq 0$, donc $F(a_1, \ldots, a_{n-1}, X) \in k[X]$ est un polynôme non cnostant sur le corps algébriquement clos k. Ainsi, il existe $a_n \in k$ tel que $F(a_1, \ldots, a_n) = 0$ donc $(a_1, \ldots, a_n) \in H$, et donc $(a_1, \ldots, a_{n-1}) \in p(H)$.

□

Contre-exemple. Si k n'est pas algébriquement clos, le résultat est faux. Par exemple si $k = \mathbb{R}$ et $H = \mathcal{V}(X^2 + Y^2 - 1)$, $H = \mathbb{S}^1$. Le projeté du cercle sur l'axe des abscisses est le segment $[-1, 1]$ qui ne contient aucun ouvert non vide de la topologie de Zariski.

Corollaire 2.4.2. *Supposons k algébriquement clos. Soit H une hypersurface de $\mathbb{A}^n(k)$. Alors, H est non vide et H est infini si $n \geq 2$.*

Rappel (théorème d'élimination). Soient $F, G \in k[X_1, \ldots, X_n]$ et $R = \mathrm{Res}_{X_n}(F, G)$, et $p : \mathbb{A}^n(k) \longrightarrow \mathbb{A}^{n-1}(k)$ la projection en les $n-1$ premières coordonnées. Alors, $p(\mathcal{V}(F, G)) \subset \mathcal{V}(R)$ (en remarquant que $R \in (F, G) \cap k[X_1, \ldots, X_{n-1}]$).

Théorème 2.4.1 (d'extension)**.** *Soient F_d et G_e les coefficients de F et G (éléments de $k[X_1, \ldots, X_{n-1}][X_n]$). Si $P \in \mathcal{V}(F_d, G_e)$, alors $P \in p(\mathcal{V}(F, G))$* si et seulement si *$P \in \mathcal{V}(R)$.*

Concrètement. Si $(a_1, \ldots, a_{n-1})$ est solution de $R = 0$ mais pas de $F_d = G_e = 0$, alors il existe $a_n \in k$ tel que $(a_1, \ldots, a_n)$ est solution de $F = G = 0$.

Exemple. Soit $k = \mathbb{C}$. Si $F = X^2Y - 1$ et $G = XY^2 - 1$, on a $F_1 = X^2$ et $G_2 = X$. Alors, $\mathcal{V}(F_1, G_2) = \mathcal{V}(X) = \{0\} \subset \mathbb{A}^1(k)$. On a $R = \mathrm{Res}_Y(X^2Y - 1, XY^2 - 1) = X^4 - X$ et $\mathcal{V}(R) = \{0, 1, j, j^2\}$. Si $F(a, b) = G(a, b) = 0$, alors $a \in \{0, 1, j, j^2\}$ (par élimination). Si $a \in \{1, j, j^2\}$, il existe $b \in \mathbb{C}$ tel que $F(a, b) = G(a, b) = 0$.

2.5 Ensembles algébriques irréductibles

Définition 2.5.1. *Un espace topologique est* irréductible *s'il est non vide et vérifie l'une des deux propriétés équivalentes suivantes.*

(i) L'espace ne peut être écrit comme l'union de deux fermés propres.

(ii) L'intersection de deux ouverts non vides est non vide.

(iii) Tout ouvert non vide est dense.

Définition 2.5.2. *Un ensemble algébrique est* irréductible *s'il est irréductible pour la topologie de* Zariski.

Exemple. $\mathcal{V}(XY) \subset \mathbb{A}^2(k)$ n'est pas irréductible, mais $\mathcal{V}(XY - 1)$ l'est.

Proposition 2.5.1. *Si V et W sont deux ensembles algébriques affines irréductibles, alors $V \times W$ est aussi irréductible.*

Démonstration. Il s'agît de montrer que si pour $i \in \{1, 2\}$, si U_i est un ouvert non vide de $V \times W$, alors $U_1 \cap U_2$ est non vide. Si $p : V \times W \longrightarrow V$ désigne la première projection, on a $p(U_i) \neq \varnothing$. D'autre, $p(U_i)$ est un ouvert car p est ouverte. Par irréductibilité de V, $p(U_1) \cap p(U_2)$ est non vide et il existe alors $P \in p(U_1) \cap p(U_2)$. Quitte à remplacer U_i par $U_i \cap (\{P\} \times W)$, on peut supposer que $V = \{P\}$. Par symétrie, on peut supposer que $W = \{Q\}$, et le problème est alors trivial.

□

Corollaire 2.5.1. *Un sous-espace affine $E \subset \mathbb{A}^n(k)$ est toujours irréductible. En particulier, $\mathbb{A}^n(k)$ est irréductible.*

Démonstration. On sait que E est isomorphe à un produit fini de copies de $\mathbb{A}^1(k)$. Grâce à la proposition précédente, on peut supposer que $E = \mathbb{A}^1(k)$. Or, $\mathbb{A}^1(k)$ est muni de la topologie cofinie, donc ne peut être écrit comme union de deux fermés propres puisque les fermés propres sont finis.

□

Chapitre 3

Anneaux

3.1 Anneaux

Vous voulez vraiment un rappel sur les anneaux ?

3.2 Anneaux locaux

Proposition 3.2.1. *Soit A un anneau et $S \subset A$ une partie. Il existe alors un anneau noté $S^{-1}A$ et un morphisme d'anneau $A \to S^{-1}A$, $a \mapsto \frac{a}{1}$ tel que pour tout $s \in S$, $\frac{s}{1} \in (S^{-1}A)^\times$ et tout morphisme d'anneaux $u : A \longrightarrow B$ tel que $u(S) \subset B^\times$ se prolonge de manière unique en un morphisme $u' : S^{-1}A \longrightarrow B$.*

Remarque. La A-algèbre $S^{-1}A$ est essentiellement définie par cette propriété. En effet, si elle existe, elle unique à isomorphisme près. Si $f, g \in A$ et $\frac{g}{1} \in (S^{-1}A)^\times$, on note $\frac{f}{g} = \frac{f}{1} \times \left(\frac{g}{1}\right)^{-1}$.

Démonstration. On utilise successivement la propriété universelle de l'anneau des polynômes (en une infinité de variables) et celle du quotient. Il suffit de considérer l'anneau

$$A[(X_s)_{s\in S}]/((sX_s - 1)_{s\in S}).$$

□

Exemples.

- On a par exemple $\{1\}^{-1}A = A$ (et plus généralement $(A^\times)^{-1}A = A$), $\{0\}^{-1}A = \{0\}$ (et $0 = 1$ dans cet anneau). Enfin, $S^{-1}A = \{0\}$ si $0 \in S$.
- Supposons A intègre (le cas en pratique dans ce cours). Alors, A s'injecte dans $S^{-1}A$. L'anneau $K := (A\backslash\{0\})^{-1}A$ est le *corps des fractions* de A. Enfin, pour toute partie $S \subset A$, $S^{-1}A$ s'injecte dans K.
- Si $g \in A$, on note $A_g = \{g\}^{-1}A$. On a donc $A_g = \{f/g^n \,|\, g \in A, n \in \mathbb{N}\}$. Remarquons que si $\varphi_g : A \longrightarrow A_g$ désigne le morphisme canonique, le noyau

  $$\ker \varphi_g = \{f \in A \,|\, \exists n \in \mathbb{N}, g^n f = 0\}$$

  est généralement non trivial.

Exercice. On suppose A intègre.

1. Montrer que si $\mathcal{I} \subset A$, alors $S^{-1}I := \{f/s \,|\, f \in \mathcal{I}, s \in \langle S \rangle\}$ ont un idéal de $S^{-1}A$.
2. Montrer que $\mathcal{J} \subset S^{-1}A$ est un idéal, alors $\mathcal{J} = S^{-1}\mathcal{I}$ avec $\mathcal{I} = \{f \in A \,|\, f/1 \in \mathcal{J}\}$ est un idéal de A.

Définition 3.2.1. *Un anneau A est* local *s'il satisfait les propriétés équivalentes suivantes.*

(i) A possède un unique idéal maximal $\mathfrak{m}_A$.

(ii) $A \backslash A^\times$ est un idéal de A.

On dit alors que $k(A) := A/\mathfrak{m}_A$ est le corps résiduel *de A. Un morphisme d'anneaux locaux $\varphi : A \longrightarrow B$ est* local *si $\varphi(\mathfrak{m}_A) \subset \mathfrak{m}_B$.*

Remarque. Si $\varphi : A \longrightarrow B$ est un morphisme d'anneaux locaux, alors φ se transmet aux quotients *via* un unique morphisme $\bar{\varphi} : k(A) \longrightarrow k(B)$.

Exercice.

1. Soit A un anneau intègre et $\mathfrak{P}$ un idéal premier de A (donc en particulier, vrai pour les idéaux maximaux), montrer que

$$A_{\mathfrak{P}} = (A \backslash \mathfrak{P})^{-1} A = \{f/g \,|\, f \in A, g \in A \backslash \mathfrak{P}\}$$

   est un anneau local d'idéal maximal $\mathfrak{m} = \{f/g \,|\, f \in \mathfrak{P}, g \in A \backslash \mathfrak{P}\}$ et de corps résiduel $k(\mathfrak{P}) = \mathrm{Frac}(A/\mathfrak{P})$ (égal à $A/\mathfrak{P}$ si $\mathfrak{P}$ est maximal).
2. Soit $u : A \longrightarrow B$ un morphisme d'anneau et $\mathfrak{Q} \subset B$ un idéal premier. Montrer que $\mathfrak{P} := u^{-1}(\mathfrak{Q})$ est un idéal premier [1], et que u induit un morphisme $u_{\mathfrak{Q}} : A_{\mathfrak{P}} \longrightarrow B_{\mathfrak{Q}}$. Montrer que si u est injectif (*resp.* surjective, *resp.* bijective), alors $u_{\mathfrak{Q}}$ est injective (*resp.* surjective, *resp.* bijective).

Définition 3.2.2 (valuation discrète)**.** *Soit K un corps. Une valuation discrète sur K est une application $v : K \longrightarrow \mathbb{Z} \cup \{\infty\}$ surjective telle que*

- *pour tout $f \in K$, $v(f) = \infty$* si et seulement si *$f = 0$;*
- *pour tout $f, g \in K$, $v(fg) = v(f) + v(g)$;*
- *pour tout $f, g \in K$, $v(f+g) \geq \min(v(f), v(g))$.*

*On dit que $A := \{f \in K \,|\, v(f) \geq 0\}$ est l'*anneau de valuation *de v.*

Remarques.

- L'inégalité vérifiée par une valuation discrète est appelée *inégalité triangulaire ultramétrique.*
- Si $v(\ell) = 1$, on dit que ℓ est une uniformisante.
- Il n'est pas nécessaire de demander que v soit surjective (si ce n'est pas le cas, on peut toujours s'y ramener).

Exercice. Montrer que A est un anneau local (principal).

1. Attention, c'est faux lorsque l'on remplace "premier" par "maximal".

Exemples.

— Si f est une fonction méromorphe sur $\mathbb{C}$ et $x \in \mathbb{C}$, on pose

$$v_x(f) = \begin{cases} n & \text{si } x \text{ est un zéro d'ordre } n, \\ -n & \text{si } x \text{ est un pôle d'ordre } n, \\ 0 & \text{sinon.} \end{cases}$$

Alors, $v_x : \mathcal{M}(\mathbb{C}) \longrightarrow \mathbb{Z} \cup \{\infty\}$ est une valuation discrète.

— L'application val : $k(x) \to \mathbb{Z} \cup \{\infty\}$, $F/G \mapsto \text{val}(F) - \text{val}(G)$ est une valuation discrète. L'application $-\deg : k(X) \longrightarrow \mathbb{Z} \cup \{\infty\}$ est une valuation.

— Soit p un nombre premier. La valuation p-adique $v_p : \mathbb{Q} \longrightarrow \mathbb{Z} \cup \{\infty\}$ (*i.e* définie par $v_p(r) = k$ *si et seulement si* $r = \frac{m}{n}p^k$ où p ne divise pas m et n).

3.3 Anneaux noethériens

Soit R un anneau (commutatif unitaire).

Définition 3.3.1. *Soit A une R-algèbre.*

— *A est* finie *s'il existe $f_1, \ldots, f_r \in A$ tel que pour tout $f \in A$ s'écrive $f = a_1 f_1 + \cdots + a_r f_r$ avec $a_1, \ldots, a_r \in R$ (*i.e *que A est un R-module de type fini).*

— *A est de type fini s'il existe $f_1, \ldots, f_n \in A$ tels que tout $f \in A$ s'écrive $f = F(f_1, \ldots, f_n)$ avec $F \in R[X_1, \ldots, X_n]$.*

— *Un morphisme d'anneau $u : A \longrightarrow B$ est fini (*resp. *de type fini) s'il fait de B un A-algèbre finie (*resp. *de type fini).*

Exemples.

— $\mathbb{Q}$ n'est pas de type fini sur $\mathbb{Z}$.

— $\mathbb{R}$ n'est pas de type fini sur $\mathbb{Q}$.

— $\mathbb{C}$ est de type fini sur $\mathbb{R}$.

— $R[(X_n)_{n\in\mathbb{N}}]$ n'est pas de type fini sur $\mathbb{R}$.

— $R[X]$ est de type fini, mais n'est pas fini.

Exercice.

1. Montrer que A est de type fini sur R *si et seulement s'*il existe un isomorphisme de A-algèbres entre A et un $R[X_1, \ldots, X_n]/\mathcal{I}$.
2. Soit $u : A \longrightarrow B$ et $v : B \longrightarrow C$ des morphismes d'anneaux. Montrer que si u et v sont finis (*resp.* de types finis), alors $v \circ u$ est fini (*resp.* de type fini). Montrer que si $v \circ u$ est fini (*resp.* de type fini), alors, v est fini (*resp.* de type fini).
3. Soit R un anneau intègre, et $F \in R[X]$ à coefficient dominant inversible. Alors, $R[X]/(F)$ est une R-algèbre finie.

Lemme 3.3.1. *Si A est une R-algèbre finie et $f \in A$, alors f est entier sur R,* i.e *qu'il existe $a_1, \ldots, a_r \in R$ tels que $f^r + a_1 f^{r-1} + \cdots + a_r = 0$.*

Démonstration. Il existe $f_1, \dots, f_r \in A$ tels que tout $f \in A$ s'écrit $a_1 f_1 + \cdots + a_r f_r$ avec $a_1, \dots, a_r \in R$. On écrit

$$f f_i = \sum_{j=1}^{r} a_{i,j} f_j.$$

Alors, f est valeur propre de la matrice $M = (a_{i,j})_{i,j}$ de vecteur propre $(f_1, \dots, f_r)$. Donc, si χ est le polynôme caractéristique de M, alors $\chi(f) f_i = 0$ pour tout $i \in [\![1, r]\!]$. On peut donc écrire $1 = c_1 f_1 + \cdots + c_r f_r$ où $c_1, \dots, c_r$. On a donc $\chi(f) = \chi(f) \cdot 1 = \sum_{i=1}^{r} c_i \chi(f) f_i = 0$. La démonstration est terminée puisque χ est unitaire de degré r.

□

Définition 3.3.2. *Un anneau A est noethérien s'il satisfait l'un des propriétés suivantes équivalentes.*

(i) Toute famille non vide d'idéaux contient un élément maximal.

(ii) Toute suite croissante d'idéaux est stationnaire.

(iii) Tout idéal est de type fini.

Exercices.

— Démontrer les équivalences.

— Montrer qu'un anneau principal est noethérien. Montrer qu'il existe des anneaux factoriels non noethériens et des anneau noethériens non factoriels [2].

— Montrer que si A est noethérien et $S \subset A$, alors A/S et $S^{-1}A$ sont noethériens.

— Montrer que l'anneau des éléments de $\mathbb{C}$ sur $\mathbb{Z}$ n'est pas noethérien.

Théorème 3.3.1. *Toute algèbre de type fini sur un anneau noethérien est un anneau noethérien.*

Démonstration. Il suffit de montrer que si R est noethérien, alors $R[X]$ aussi. Soit $\mathcal{I} \subset R[X]$ et $d \in \mathbb{N}$. On note $c_d(\mathcal{I}) \subset R$ l'ensemble des coefficients dominants des polynômes de degrés d de $\mathcal{I}$. Si $\mathcal{I}$ est un idéal, alors $(c_d(\mathcal{I}))_{d \in \mathbb{N}}$ est une suite croissante d'idéaux de R. De plus, si $\mathcal{J}$ est un autre idéal et contenant $\mathcal{I}$, alors $c_d(\mathcal{I}) \subset c_d(\mathcal{J})$, et on a l'équivalence suivante : $\mathcal{I} = \mathcal{J}$ *si et seulement si* $c_d(\mathcal{I}) = c_d(\mathcal{J})$ pour tout $d \in \mathbb{N}$ (qui se montre par récurrence sur le degré d).

Soit $(\mathcal{I}_k)_{k \in \mathbb{N}}$ une suite croissante d'idéaux de $R[X]$. On considère la famille $(c_d(\mathcal{I}_k))_{d,k \in \mathbb{N}}$ d'idéaux de R. Puisque R est noethérien, il existe D et $K \in \mathbb{N}$ des entiers tels que $c_D(\mathcal{I}_K)$ soit maximal, *i.e* que $C_D(\mathcal{I}_k) = c_d(\mathcal{I}_k)$ pour tout $d \geq D$ et $k \geq K$. D'autre part, pour tout $i \in \mathbb{N}$, $N_i \in \mathbb{N}$ tel que $c_i(\mathcal{I}_{N_i}) = c_i(\mathcal{I}_k)$ pour tout $k \geq N_i$. On pose $N = \max(K, \max_{i \leq D} N_i)$. Alors, on a $c_i(\mathcal{I}_N) = c_i(\mathcal{I}_k)$ pour tout $i \in \mathbb{N}$ et $k \geq N$. Ainsi, $\mathcal{I}_N = \mathcal{I}_k$ pour tout $k \geq N$.

□

Lemme 3.3.2 (Artin-Rees)**.** *Soit A un anneau noethérien et $\mathcal{I}, \mathcal{J} \subset A$ deux idéaux. Alors, il existe $n \in \mathbb{N}$ tel que pour tout $k \in \mathbb{N}$,*

$$\mathcal{I}^{n+k} \cap \mathcal{J} = \mathcal{I}^n (\mathcal{I}^k \cap \mathcal{J}).$$

2. Prendre $\mathbb{Q}[(X_n)_{n \in \mathbb{N}}]$.

Démonstration. Soit $A_X = \sum_{n\geq 0} \mathcal{I}^n X^n \subset A[X]$ et $\mathcal{J}_X = \sum_{n\geq 0} \mathcal{J} X^n \subset A[X]$. A_X est un sous-anneau de $A[X]$ tandis que $\mathcal{J}_X$ est un idéal de $A[X]$. Puisque A est noethérien, $\mathcal{I}$ est un idéal de type fini, et donc A_X est une A-algèbre de type fini. En effet, si $f_1, \dots, f_r$ sont des générateurs de $\mathcal{I}$, on a alors un morphisme d'anneaux surjectif

$$\begin{array}{rcl} A[X_1, \dots, X_r] & \longrightarrow & A_X, \\ X_i & \longmapsto & f_i X. \end{array}$$

□

L'anneau A_X est donc noethérien, et on en déduit que

$$A_X \cap \mathcal{J}_X = \sum_{n\geq 0} (\mathcal{I}^n \cap \mathcal{J}) X^n$$

est un idéal de type fini de A_X. Soit $F_1, \dots, F_m \in A[X]$ des générateurs de cet idéal et soit $k = \max_{i=1}^m \deg F_i$. Ainsi, $F_i \in \sum_{\ell=0}^k (\mathcal{I}^\ell \cap \mathcal{J}) X^\ell$. Ainsi,

$$A_X \cap \mathcal{J}_X = \sum_{i=1}^m A_X F_i = \sum_{n\geq 0} \mathcal{I}^n X^n \sum_{\ell=0}^k (\mathcal{I}^\ell \cap \mathcal{J}) X^\ell = \sum_{n\geq 0} \sum_{\ell=0}^k \mathcal{I}^n (\mathcal{I}^\ell \cap \mathcal{J}) X^{n+\ell}.$$

En observant les coefficients de X^{n+k}, on a

$$\mathcal{I}^{n+k} \cap \mathcal{J} = \sum_{\ell=0}^k \mathcal{I}^{n+k-\ell} (\mathcal{I}^k \cap \mathcal{J}) = \sum_{n\geq 0} \mathcal{I}^n (\mathcal{I}^k \cap \mathcal{J}).$$

Lemme 3.3.3 (Nakayama)**.** *Soit A un anneau local noethérien et $\mathcal{J} \subset A$. Si $\mathfrak{m}_A \mathcal{J} = \mathcal{J}$, alors $\mathcal{J} = \{0\}$.*

Démonstration. Soit $g_1, \dots, g_r \in \mathcal{J}$ des générateurs de $\mathcal{J}$. Pour tout $i \in [\![1, r]\!]$, on peut écrire $g_i = \sum_{i=1}^r f_{i,j} g_i$ avec $f_{i,j} \in m_A$ (car $\mathfrak{m}_A \mathcal{J} = \mathcal{J}$). Soit $F = (f_{i,j})_{i,j}$. Or, $\det(I_r - F)$ est de la forme $1 - f$ avec un certain $f \in \mathfrak{m}_A$. Si g_i est non nul, alors il est vecteur propre de F et donc $1 - f = 0$. C'est impossible car $1 - f$ est inversible [3], donc les g_i sont tous nuls.

□

Théorème 3.3.2 (d'intersection de Krull)**.** *Soit A un anneau local noethérien. Alors,*

$$\bigcap_{n=0}^{\infty} \mathfrak{m}_A^n = \{0\}.$$

Remarque. Géométriquement, ce théorème signifie (entre autres) qu'une fonction méromorphe n'a que des zéros d'ordres finis.

Démonstration. Selon le lemme d'Artin-Rees avec $\mathcal{I} = \mathfrak{m}_A$ et $\mathcal{J} = \bigcap_{n=0}^\infty \mathfrak{m}_A^n$, il existe $k \in \mathbb{N}$ tel que $\mathcal{I}^{k+1} \cap \mathcal{J} = \mathcal{I}(\mathcal{I}^k \cap \mathcal{J})$, *i.e* $\mathcal{J} = \mathfrak{m}_A \mathcal{J}$. Ainsi, $\mathcal{J} = \{0\}$.

□

3. autrement, $1 = 1 - f + f$ serait élément de $\mathfrak{m}_A$.

Lemme 3.3.4 (de normalisation de NOETHER). *Soit $F \in R[X_0, \dots, X_d]$. Il existe $e_1, \dots, e_d \in \mathbb{N}$ tels que l'application*

$$\Phi : \left| \begin{array}{rcl} R[X_0, \dots, X_d] & \longrightarrow & R[X_0, \dots, X_d], \\ X_0 & \longmapsto & X_0, \\ X_i & \longmapsto & X_i + X_0^{e_i} \end{array} \right.$$

est telle que $\Phi(F)$ a pour un coefficient dominant en X_0 constant. De plus, Φ est bijective.

Remarque. L'application Φ est bijective.

Démonstration. Soit $e = \max_{i=0}^{d}(\deg_{X_i} F)+1$ et $e_i = e^i$ pour tout $i \in [\![0, d]\!]$. Si $M = X_0^{n_0} \cdots X_d^{n_d}$ un monôme de F. On pose $n(M) = \sum_{i=0}^{d} n_i e^i$. Par définition de e, on a $n(M) \neq n(M')$ pour tout monôme $M' \neq M$ de F. De plus, on peut écrire

$$\Phi(M) = X_0^{n_0} \prod_{i=1}^{d} (X_i + X_0^{e_i})^{n_i} = G + X_0 + n(M)$$

avec G tel que $\deg_{X_0}(G) < n(M)$. On a donc $\deg_{X_0}(\Phi(F)) = \max_M(n(M))$.

□

Théorème 3.3.3 (de normalisation). *Si A est de type fini sur un corps k, il existe un morphisme de k-algèbres $k[X_1, \dots, X_d] \longrightarrow A$ injectif fini.*

Remarque. La réciproque est vraie.

Démonstration. Il existe (par définition) un morphisme de k-algèbre surjectif (et donc fini) $k[X_1, \dots, X_d] \longrightarrow A$. S'il n'est pas injectif, et que $F \neq 0$ est élément de son noyau, on peut supposer grâce au lemme de normalisation que le coefficient dominant de X_d est constant. Le morphisme composé

$$k[X_1, \dots, X_{d-1}] \longrightarrow k[X_1, \dots, X_d]/(F) \longrightarrow A.$$

Ce morphisme est fini (comme composée de morphismes finis), et on conclut par récurrence sur d. □

Théorème 3.3.4 (des zéros de HILBERT). *Toute extension de corps $k \subset K$ de type finie est finie.*

Chapitre 4

Anneaux de fonctions

Soit k un corps infini, et $n \in \mathbb{N}$.

4.1 Idéal de définition

Définition 4.1.1. *Soit $A \subset \mathbb{A}^n(k)$. L'idéal de* définition *de A est l'ensemble*

$$\mathrm{I}(A) = \{F \in k[X_1, \ldots, X_n] \,|\, \forall p \in A, F(p) = 0\}.$$

Exercice. Montrer que $\mathrm{I}(A)$ est un idéal radiciel.

Proposition 4.1.1. *On a les propriétés suivantes.*

(i) $\mathrm{I}(\varnothing) = k[X_1, \ldots, X_n]$ *et* $\mathrm{I}(\mathbb{A}^n(k)) = (0)$.

(ii) Si $(A_\alpha)_\alpha$ est une famille de parties de $\mathbb{A}^n(k)$, alors

$$\bigcap_\alpha \mathrm{I}(A_\alpha) = \mathrm{I}\left(\bigcup_\alpha A_\alpha\right).$$

(iii) Si $A \subset B \subset \mathbb{A}^n(k)$, alors $\mathrm{I}(B) \subset \mathrm{I}(A)$.

(iv) $A \subset \mathcal{V}(\mathrm{I}(A))$ et $S \subset \mathrm{I}(\mathcal{V}(S))$ pour tout $A \subset \mathbb{A}^n(k)$ et $S \subset k[X_1, \ldots, X_n]$.

Exemple. En général, $\sum_\alpha \mathrm{I}(A_\alpha) \neq \mathrm{I}\left(\bigcap_\alpha A_\alpha\right)$.

Exercice.

1. Montrer que si $p \in \mathbb{A}^n(k)$, $\mathrm{I}(p) := \mathrm{I}(\{p\})$ est un idéal maximal. Montrer que si $p = (a_1, \ldots, a_n)$, alors $\mathrm{I}(p) = (X_1 - a_1, \ldots, X_n - a_n)$.
2. Montrer que $V \subset \mathbb{A}^n(k)$ est algébrique *si et seulement si* $V = \mathcal{V}(\mathrm{I}(V))$.
3. Montrer que si $V, W \subset \mathbb{A}^n(k)$ sont algébriques, alors

$$V = W \iff \mathrm{I}(V) = \mathrm{I}(W).$$

4. Montrer que si $A \subset \mathbb{A}^n(k)$, alors $\overline{A} = \mathcal{V}(\mathrm{I}(A))$ (où $\overline{A}$ est l'adhérence de A pour la topologie de Zariski, *i.e* la fermeture algébrique).

5. Montrer que $\mathrm{I} \circ \mathcal{V}$ et $\mathcal{V} \circ \mathrm{I}$ sont des *opérateurs de saturation*. On rappelle qu'un opérateur de saturation est une application $e : (X, \leq) \longrightarrow (X, \leq)$ où $\leq$ est un ordre sur X et e est telle que $e^2 = e$ (idempotence), croissante pour $\leq$, et $x \leq e(x)$ pour tout $x \in X$.

Proposition 4.1.2 (cas des sous-espaces affines)**.** *Si $V = \mathcal{V}(F_1, \ldots, F_r)$ avec $F_1, \ldots, F_r \in k[X_1, \ldots, X_n]$ des polynômes de degré 1. Alors, $\mathrm{I}(V) = (F_1, \ldots, F_r)$.*

Démonstration. Exercice.

□

Exercice. Si $C = \mathcal{V}(F)$. Si F est irréductible et C est infini, $\mathrm{I}(C) = (F)$.

4.2 Anneau de coordonnées

Soit V un sous-ensemble algébrique de $\mathbb{A}^n(k)$. On note $k[V]$ l'ensemble des fonctions polynomiales sur V, appelé *anneau de coordonnées* de V.

Proposition 4.2.1. *L'application*

$$\pi_V : \left| \begin{array}{ccc} k[X_1, \ldots, X_n] & \longrightarrow & \mathcal{F}(V, k) \\ F & \longmapsto & F|_V \end{array} \right.$$

induit un isomorphisme de k-algèbres

$$k[X_1, \ldots, X_n]/\mathrm{I}(V) \cong k[V].$$

Démonstration. On a le diagramme commutatif suivant.

$$\begin{array}{ccc} k[X_1, \ldots, X_n] & \xrightarrow{\pi_V} & \mathcal{F}(V, k) \\ \downarrow & & \uparrow \\ k[X_1, \ldots, X_n]/\ker \pi_V & \xrightarrow{\cong} & \mathrm{Im}(\pi_V) \end{array}$$

Or, $\ker \pi_V = \mathrm{I}(V)$ et $\mathrm{Im}\, \pi_V = k[V]$.

□

Exercice. Montrer que si l'on pose $x_i = X_i|_V \in k[V]$ pour tout $i \in [\![1, n]\!]$, alors pour tout $F \in k[X_1, \ldots, X_n]$, $F_{|V} = F(x_1, \ldots, x_n) \in k[V]$.

Remarque. Si $p \in V$, alors $p = (x_1(p), \ldots, x_n(p))$.

Exemples.

— $k[\varnothing] = \{0\}$, $k[p] = k$, $k[\mathbb{A}^n(k)] \cong k[X_1, \ldots, X_n]$ (ce dernier exemple est faux si k n'est pas supposé infini).

— Soit C la courbe d'équation $Y = X^2$. On a l'isomorphisme $k[X, Y]/(Y - X^2) \cong k[C]$. Or, la division euclidienne donne un isomorphisme $k[X] \cong k[X, Y]/(Y - X^2)$. Ainsi, $k[C] \cong k[X]$ et

$$k[C] = \{F(x) \mid F \in k[X]\}$$

où $x = X_{|C}$ (et une telle écriture d'un élément de $k[C]$ est unique).

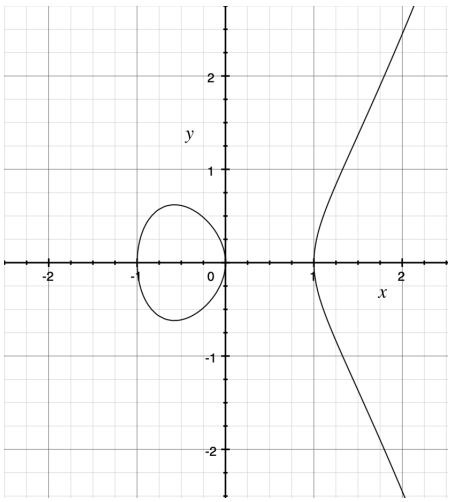


FIGURE 4.1 – Courbe elliptique d'équation $Y^2 = X^3 - X$.

— Soit C la courbe elliptique d'équation $Y^2 = X^3 - X$. Alors, $k[X][Y]_{<2} \cong k[X,Y]/(Y^2 - X^3 + X) \cong k[C]$. On a donc

$$k[C] = \{F(x) + G(x)y \,|\, F, G \in k[X]\}$$

où $x = X_{|C}$ et $y = Y_{|C}$ (et une telle écriture d'un élément de $k[C]$ est unique).

Remarques. Si $A \subset V$, on définit $\mathrm{I}_V(A) = \{f \in k[V] \,|\, \forall p \in A, f(p) = 0\}$. De même, si $S \subset k[V]$, on pose $\mathcal{V}(S) = \{p \in V \,|\, \forall f \in S, f(p) = 0\}$. Ce qui a été vu pour $\mathbb{A}^n(k)$ et $k[X_1, \ldots, X_n]$ se généralise, par exemple comme avec l'exercice précédent.

Exercice. Si $W \subset V$ est algébrique, alors

$$k[V]/\mathrm{I}_V(W) \cong k[W].$$

4.3 Applications polynomiales et morphismes d'anneaux

Si $\varphi : W \longrightarrow V$ est une application polynomiale, on pose

$$\varphi^* : \left| \begin{array}{ccc} k[V] & \longrightarrow & k[W], \\ f & \longmapsto & f \circ \varphi. \end{array} \right.$$

Exercice.

1. Montrer que si $i : W \longrightarrow V$ est l'inclusion d'un sous-ensemble algébrique, alors

$$i^* : \left| \begin{array}{ccc} k[V] & \longrightarrow & k[W] \\ f & \longmapsto & f|_W \end{array} \right.$$

   est l'application de restriction. En particulier, $\mathrm{id}_V^* = \mathrm{id}_{k[V]}$.
2. Montrer que si $\varphi : W \longrightarrow V$ et $\psi : Z \longrightarrow W$ sont polynomiales, alors $(\varphi \circ \psi)^* = \psi^* \circ \varphi^*$ ($\varphi \longmapsto \varphi^*$ est un foncteur contravariant).
3. Soit $W \subset \mathbb{A}^m(k)$, $V \subset \mathbb{A}^n(k)$, et $\Phi : \mathbb{A}^m(k) \longrightarrow \mathbb{A}^n(k)$ une application polynomiale. Soit $\varphi : W \longrightarrow V$ telle que

$$\begin{array}{ccc} \mathbb{A}^m(k) & \xrightarrow{\Phi} & \mathbb{A}^n(k) \\ \uparrow & & \uparrow \\ W & \xrightarrow{\varphi} & V \end{array}$$

commute. Alors, pour tout $f \in k[V]$, $f = F|_V$ implique que $\varphi^*(f) = \Phi^*(F)|_W$.

4. Montrer que si $\varphi : W \longrightarrow V$ est une application polynomiale, et $f \in k[V]$, alors

$$\varphi^{-1}(\mathcal{V}(f)) = \mathcal{V}(\varphi^*(f)).$$

5. Montrer que si φ est polynomiale, alors φ^* est un morphisme de k-algèbres.

Notation. On note $\mathrm{Hom}(W, V)$ l'ensemble des applications polynomiales de W vers V, et $\mathrm{Hom}(k[V], k[W])$ l'ensemble des morphismes de k-algèbres de $k[V]$ vers $k[W]$.

Théorème 4.3.1. *Si V et W sont des ensembles algébriques, alors*

$$* : \left| \begin{array}{ccc} \mathrm{Hom}(W, V) & \longrightarrow & \mathrm{Hom}(k[V], k[W]) \\ \varphi & \longmapsto & \varphi^* \end{array} \right.$$

est une bijection.

Démonstration. Soit $x_1, \ldots, x_n$ les coordonnées sur V. Si $\varphi : W \longrightarrow V$ est polynomiale et $q \in W$, alors

$$\begin{aligned} \varphi(q) &= (x_1(\varphi(q)), \ldots, x_n(\varphi(q))) \\ &= (\varphi^*(x_1)(q), \ldots, \varphi^*(x_n)(q)). \end{aligned}$$

Ainsi, φ est uniquement déterminé par φ^* et donc $*$ est injective. Soit maintenant $u : k[V] \longrightarrow k[W]$ un morphisme de k-algèbres. On pose $\varphi(q) = (u(x_1)(q), \ldots, u(x_n)(q))$ pour tout $q \in W$. Soit $F \in \mathrm{I}(V)$, on a

$$\begin{aligned} F(\varphi(q)) &= F(u(x_1)(q), \ldots, u(x_n)(q)) \\ &= F(u(x_1), \ldots, u(x_n))(q) \\ &= u(F(x_1, \ldots, x_n))(q) \\ &= u(F|_V)(q) \\ &= u(0)(q) \\ &= 0. \end{aligned}$$

On en déduit que φ est bien à valeurs dans V. Enfin, il est clair que $\varphi^* = u$ car $\varphi^*(x_i) = u(x_i)$. □

Corollaire 4.3.1. *Si $\varphi : W \longrightarrow V$ est une application polynomiale, φ est un isomorphisme* si et seulement si *φ^* est bijective (*si et seulement si *φ^* est un isomorphisme de k-algèbre).*

Démonstration. Exercice.

□

Corollaire 4.3.2. *Si V et W sont des ensembles algébriques, alors*

$$V \cong W \iff k[V] \cong k[W].$$

Exemples.

— Soit C la parabole d'équation $Y = X^2$. On a $k[C] \cong k[X] = k[\mathbb{A}^1(k)]$, donc $C \cong \mathbb{A}^1(k)$.

— Soit C l'hyperbole d'équation $XY = 1$. Alors, $C \ncong \mathbb{A}^1(k)$. En effet,

$$k[C] \cong k[X,Y]/(XY-1) \cong X^{-1}k[X]$$

(où $X^{-1}k[X]$ est le localisé). Ainsi, $k[C]^\times \backslash k^\times \neq \varnothing$ mais $k[\mathbb{A}^1(k)]^\times \backslash k^\times = \varnothing$.

— Soit C la courbe paramétrée définie par $(x(t), y(t), z(t)) = (t, t^2, t^3)$ pour tout $t \in k$. On a un isomorphisme $C \cong \mathbb{A}^1(k)$. En effet, on a $\mathrm{I}(C) = (Y - X^2, Z - X^3)$ donc

$$k[C] \cong k[X,Y,Z]/(Y-X^2, Z-X^3) \cong k[X,Y]/(Y-X^2) \cong k[X].$$

— Soit C la courbe d'équation $Y^2 = X^3$. On a $C \ncong \mathbb{A}^1(k)$. En effet,

$$k[C] \cong k[X,Y]/(Y^2 - X^3) \cong A = \left\{ \sum a_i T^i \;\middle|\; a_1 = 0 \right\}.$$

Or, A n'est pas factoriel.

Proposition 4.3.1. *Soit $\varphi : W \longrightarrow V$ une application polynomiale. On a les propriétés suivantes.*

(i) $\ker \varphi^* = \mathrm{I}_V(\mathrm{Im}\, \varphi)$.

(ii) φ^* *est injective* si et seulement si φ *est dominante (*i.e *à image dense).*

(iii) φ^* *est surjective* si et seulement si φ *est une immersion fermée,* i.e *qu'il existe $V' \subset V$ un ensemble algébrique et $\psi : W \longrightarrow V'$ une application polynomiale telle que le diagramme suivant commute.*

$$\begin{array}{ccc} W & \xrightarrow{\varphi} & V \\ & \searrow^{\psi} & \cong \uparrow \\ & & V' \end{array}$$

Démonstration. (i) Soit $f \in k[V]$. Alors,

$$\begin{aligned} f \in \ker \varphi^* &\iff \varphi^*(f) = 0_W \\ &\iff f \circ \varphi = 0 \\ &\iff f \in \mathrm{I}_V(\mathrm{Im}\, \varphi). \end{aligned}$$

(ii) $\boxed{\Longrightarrow}$ Si $\ker \varphi^* = \{0_V\}$ (donc $\mathrm{I}_V(\mathrm{Im}\, \varphi) = \{0_V\}$), on a $\mathcal{V}(\mathrm{I}_V(\mathrm{Im}\, \varphi)) = \mathcal{V}(0_V)$ donc $V = \overline{\mathrm{Im}\, \varphi}$.
$\boxed{\Longleftarrow}$ Si $\overline{\mathrm{Im}\, \varphi} = V$,

□

Corollaire 4.3.3. *Soit $\mathcal{I} \subset k[V]$ un idéal. On a l'équivalence suivante.*

$$\exists P \in V, \mathcal{I} = \mathrm{I}_V(P) \iff k[V]/\mathcal{I} \cong_{k-\mathrm{alg}} k.$$

Démonstration. $\boxed{\Longleftarrow}$ Si $P \in V$, alors $k[V]/\mathrm{I}_V(P) \cong k[P] \cong k$. Soit maintenant $\mathcal{I}$ un tel idéal. On a le diagramme commutatif

$$\begin{array}{ccc} k[V] & \twoheadrightarrow & k[V]/\mathcal{I} \\ & \searrow^{i_*} & \downarrow \cong \\ & & k[\{0\}] \end{array}$$

où l'on a posé $i : \{0\} \to V, 0 \mapsto P$. On a alors $\mathcal{I} = \ker i_* = \mathrm{I}_V(\operatorname{Im} i) = \mathrm{I}_V(P)$.

□

Interlude topologique

Définition 4.3.1. *Une composante irréductible d'un espace topologique V est une partie maximale pour l'irréductibilité.*

Exemples.

- Si V est un espace métrique, les composantes irréductibles sont les points.
- Si V est infini et est muni de la topologie cofinie, sa seule composante irréductible est V.

Exercice.

1. Montrer q'un composante irréductible est fermée.
2. Montrer que toute partie irréductible est contenu dans une composante irréductible. *Indication : si A est une composante irréductible, appliquer le lemme de* Zorn *à $\mathcal{F}$ l'ensemble des irréductibles W contenant A.*
3. Montrer que V est réunion de ses composantes irréductibles.
4. Montrer que si $V = V_1 \cup \cdots \cup V_r$ avec V_i fermé irréductible pour tout $i \in [\![1, r]\!]$, et $V_i \not\subset V_j$ si $i \neq j$, alors les V_i sont les composantes irréductibles de V.

Définition 4.3.2. *Un espace topologique est* noethérien *s'il vérifie l'une des conditions équivalentes suivantes.*

(i) Toute famille non vide de fermés possède un élément minimal.

(ii) Toute famille non vide d'ouverts possède un élément maximal.

(iii) Toute suite décroissante de fermés est stationnaire.

(iv) Toute suite croissante d'ouverts est stationnaire.

Exercice.

1. Montrer que les quatre propriétés sont équivalentes.
2. Montrer qu'un sous-espace d'un espace noethérien est noethérien.

Proposition 4.3.2. *Un espace noethérien possède un nombre fini de composantes irréductibles.*

Démonstration. On présente seulement l'idée de la démonstration. On applique $\mathcal{F}$ l'ensemble des sous-espaces $W \subset V$ qui ne sont pas union finie d'irréductibles. S'il était non vide, on pourrait alors y trouver un élément minimal et donc une contradiction.

□

4.4 Composantes irréductibles

Proposition 4.4.1. *Soit V un ensemble algébrique. Les conditions suivantes sont équivalentes.*

(i) V *est irréductible.*

(ii) $\mathrm{I}(V)$ *est un idéal premier.*

(iii) $k[V]$ *est intègre.*

Démonstration.

— $(i) \implies (ii)$. Soit F, G deux polynômes tels que $FG \in \mathrm{I}(V)$. On a $\mathcal{V}(FG) = \mathcal{V}(F) \cup \mathcal{V}(G)$. Or, $V = \mathcal{V}(\mathrm{I}(V)) \subset \mathcal{V}(FG)$. Or, $\mathcal{V}(F)$ et $\mathcal{V}(G)$ sont fermés. Par irréductibilité $V \subset \mathcal{V}(F)$ ou $V \subset \mathcal{V}(G)$. Si on suppose que $G \notin \mathrm{I}(V)$, alors $F \in \mathrm{I}(\mathcal{V}(F)) \subset \mathrm{I}(V)$.

— $(ii) \iff (iii)$. On a $k[V] \cong k[X_1, \ldots, X_n]/\mathrm{I}(V)$. Or, le quotient est intègre *si et seulement si* $\mathrm{I}(V)$ est premier.

— $(iii) \implies (i)$. On écrit $V = V_1 \cup V_2$ avec V_1, V_2 deux fermés de V. On a

$$\{0\} = \mathrm{I}_V(V) = \mathrm{I}_V(V_1 \cup V_2) = \mathrm{I}_V(V_1) \cap \mathrm{I}_V(V_2) \supset \mathrm{I}_V(V_1) \cdot \mathrm{I}_V(V_2),$$

mais $k[V]$ étant intègre, ou bien $\mathrm{I}_V(V_1) = \{0\}$, ou bien $\mathrm{I}_V(V_2) = \{0\}$. Dans le premier cas par exemple, on a

$$V_1 = \mathcal{V}(\mathrm{I}_V(V_1)) = \mathcal{V}(0) = V.$$

□

Proposition 4.4.2. *Les sous-ensembles algébriques irréductibles de $\mathbb{A}^2(k)$ sont*

— *les points ;*

— *les courbes infinies d'équations $F = 0$ avec F un polynôme irréductible ;*

— *le plan.*

Démonstration. Soit V un sous-ensemble algébrique de $\mathbb{A}^2(k)$. On va monter que V est irréductible *si et seulement si* c'est une courbe infini d'équation $F = 0$ où F est irréductible. La condition "$\Leftarrow$" a déjà été vue. On montre le sens direct : soit $V \subset \mathbb{A}^2(k)$ un ensemble algébrique irréductible qui n'est pas un singleton, ni le plan tout entier. Puisque $V \neq \mathbb{A}^2(k)$, $\mathrm{I}(V) \neq \{0\}$, et puisque V n'est pas réduit à un point, V est infini car il est irréductible. Soit $F \in \mathrm{I}(V)$ un

polynôme non nul. On peut supposer F irréductible. En effet, si $F = F_1 \cdots F_k$ où les F_i sont irréductibles, puisque $F \in \mathrm{I}(V)$, on a $V = \mathcal{V}(\mathrm{I}(V)) \subset \mathcal{V}(F) = \mathcal{V}(F_1) \cap \cdots \cap \mathcal{V}(F_k)$. Puisque V est irréductible, V est nécessairement contenu dans un des $\mathcal{V}(F_i)$. Ainsi, $F_i \in \mathrm{I}(V)$ et F_i est irréductible.

Soit donc $F \in \mathrm{I}(V)$ supposé irréductible. On a $(F) \subset \mathrm{I}(V)$. Si $G \in \mathrm{I}(V)$, alors puisque $V \subset \mathcal{V}(F) \cap \mathcal{V}(G)$ et V est infini, $\mathcal{V}(F) \cap \mathcal{V}(G)$ est infini et donc F et G ne sont *pas* premiers entre eux. Ainsi, F divise G et donc $G \in (F)$.

□

Théorème 4.4.1. *Un ensemble algébrique est noethérien. Soit $(V_\lambda)_\lambda$ une suite décroissante de fermés de V. La suite $(\mathrm{I}_V(V_\lambda))_\lambda$ est une famille croissante d'idéaux de $k[V]$. Puisque $k[V]$ est noethérien (car de type fini sur corp), $(\mathrm{I}_V(V_\lambda))_\lambda$ est stationnaire. Ainsi, $(V_\lambda)_\lambda = (\mathcal{V}(\mathrm{I}_V(V_\lambda)))_\lambda$ est stationnaire.*

4.5 Fonctions rationnelles

Soit V un ensemble algébrique irréductible.

Définition 4.5.1. *On appelle* corps des fonctions rationnelles *sur V le corps de fraction de $k[V]$,* i.e

$$k(V) = \mathrm{Frac}(k[V]).$$

Si $f \in k(V)$ et $f = g/h$ avec $g, h \in k[V]$, et $P \in V$ est tel que $h(P) \neq 0$, on dit que f est régulière *en P. On pose alors $f(P) = g(P)/h(P)$. On dit alors que f a un* zéro *en P si $f(P) = 0$. Si f n'est pas régulière en P, on dit que f a un* pôle *en P.*

Exemples.

- Soit $C : Y = X^2$. On a $k(X) \cong k(C) \cong k(x) = \{F(x)/G(x) \,|\, F, G \in k[X], G \neq 0\}$, où $x \in k[C]$ est la fonction coordonnée en la première variable $C \to k$, $(a, b) \mapsto a$.
- Soit $C : Y^2 = X^3 - X$. On a $k(C) = k(X)[Y]/(Y^2 - X^3 + X)$. Remarquons que $k(X)[Y]/(Y^2 - X^3 + X)$ est bien un corps car $Y^2 - X^3 + X$ est un polynôme irréductible à coefficient dans le corps $k(X)$.
- Soit $V : XT = YZ \subset \mathbb{A}^4(k)$. Soit $f = x/y \in k(V)$, où x et y sont la première et la deuxième fonction coordonnée. L'application f a un pôle en $0_{\mathbb{A}^4(k)} = (0, 0, 0, 0)$. Elle est régulière en $P = (0, 0, 1, 1)$, et $f(P) = 1$. Enfin, elle a un zéro en $Q = (0, 0, 0, 1)$ (car $f = x/y = z/y$ dans $k(V)$).

Exercice.

1. Montrer dans la définition que f est bien définie en les points où elle est régulière (*i.e* que $f(P)$ ne dépend du choix de g et h avec $h(P) \neq 0$).
2. Soit $I_f = \{h \in k[V] \,|\, fh \in k[V]\} \cup \{0\}$ l'ensemble des dénominateurs de f auquel on rajoute 0. Montrer que I_f est idéal de $k[V]$, et que $\mathcal{V}(I_f)$ est l'ensemble des pôles de f.
3. Montrer que I_f est principal si $k[V]$ est factoriel.
4. Montrer que $f \in k[V]$ *si et seulement si* $I_f = k[V]$.
5. Si f n'est pas identiquement nulle et est régulière en P, alors P est un zéro de f *si et seulement si* f est un pôle de $1/f$.

6. Montrer que l'ensemble des points de V où f est régulière est un ouvert de V. De même, l'ensemble des points $P \in V$ telle que f est régulière en V et $f(P) \neq 0$ est un ouvert de V.

Soit V un ensemble algébrique et $P \in V$. On note $\mathcal{O}_{V,P}$ l'ensemble des fonctions rationnelles sur V régulières en P. De même, on note $\mathfrak{m}_{V,P}$ l'ensemble des fonctions rationnelles sur V régulières en P, et qui s'annule en P. On appelle $\mathcal{O}_{V,P}$ est appelé *anneau local en P*.

Proposition 4.5.1. *$\mathcal{O}_{V,P}$ est un anneau local intègre noethérien d'idéal maximal $\mathfrak{m}_{V,P}$.*

Démonstration. □

Proposition 4.5.2. *Si $V \subset \mathbb{A}^n(k)$ est irréductible et $P \in V$, alors*

$$\mathcal{O}_{\mathbb{A}^n(k),P} / \mathrm{I}(V)\, \mathcal{O}_{\mathbb{A}^n(k),P} \cong \mathcal{O}_{V,P}\,.$$

Remarque. Plus généralement, si $\mathcal{J} \subset k[X_1, \ldots, X_n]$ est un idéal, alors

$$\mathcal{O}_{\mathbb{A}^n(k),P} / (\mathcal{J} + \mathrm{I}(V))\, \mathcal{O}_{\mathbb{A}^n(k),P} \cong \mathcal{O}_{V,P} / \mathcal{J}\, \mathcal{O}_{V,P}\,.$$

Exercice.

1. Si $\varphi : W \longrightarrow V$ est polynomiale dominante, alors φ^* se prolonge en $\varphi^* : k(V) \longrightarrow k(W)$ qui est injective et donc est une extension de corps.
2. Soit $\varphi : W \longrightarrow V$ une application polynomiale, $Q \in W$, et $P = \varphi(Q)$. Alors, φ^* se prolonge en

$$\varphi_Q^* : \left| \begin{array}{ccc} \mathcal{O}_{V,P} & \longrightarrow & \mathcal{O}_{W,Q}, \\ f = \frac{g}{h} & \longmapsto & f \circ \varphi = \frac{\varphi^* g}{\varphi^* h}. \end{array} \right.$$

3. Montrer que si f est dominante (*resp.* une immersion fermée, *resp.* un isomorphisme), alors φ_Q^* est injective (*resp.* surjective, *resp.* bijective et donc un isomorphisme).
4. Montrer que si U est un ouvert de V, alors $\Gamma(U)$ l'ensemble des $f \in k(V)$ régulières sur U est une k-algèbre (et un sous-anneau de $k(V)$), et

$$\Gamma(U) = \bigcap_{P \in U} \mathcal{O}_{V,P}\,.$$

Remarque. Si k est algébriquement clos, $\Gamma(V) = k[V]$. Ce résultat est faux sur $\mathbb{R}$: $\frac{1}{1+X^2}$ est élément de $\Gamma(\mathbb{A}^1(\mathbb{R}))$.

Définition 4.5.2. *Soit V et W deux ensembles algébriques. On suppose V irréductible. Une application (injective) polynomiale est une* immersion ouverte *si*

- *j induit un homéomoprhisme $W \longrightarrow U$ où U est un ouvert de V ;*
- *pour tout $Q \in W$, j_Q^* est bijective.*

Remarque. U n'est pas un ensemble algébrique. On dit que U est un *ouvert affine*. En guise de contre-exemple, $\mathbb{A}^2(k) \backslash \{0\}$ n'est pas un ouvert affine.

Chapitre 5

Courbes algébriques

Soit k un corps algébriquement clos.

5.1 Théorème des zéros de Hilbert

Soit V un ensemble algébrique (contenu dans un $\mathbb{A}^n(k)$).

Proposition 5.1.1 (caractérisation des idéaux maximaux)**.** *Soit $\mathcal{I} \subset k[V]$. $\mathcal{I}$ est un idéal maximal* si et seulement s'*il existe $P \in V$ tel que $\mathcal{I} = \mathrm{I}_V(P)$.*

Démonstration. On sait que $\mathcal{I} = \mathrm{I}_V(P)$ *si et seulement si* $k[V]/\mathcal{I} \cong k$. Le sens direct a déjà été vu. Pour le sens réciproque, soit $\mathcal{I}$ un idéal maximal. Le corps $k[V]/\mathcal{I}$ constitue une extension de k. Mais puisque k est supposée algébriquement clos et que le théorème des zéros de Hilbert permet d'affirmer que l'extension est finie, on a $k \cong k[V]/\mathcal{I}$.

□

Remarques.

- On note $\mathrm{Spm}(k[V])$ l'ensemble des idéaux maximaux de $k[V]$. Alors, l'application $V \to \mathrm{Spm}(k[V])$, $P \mapsto \mathrm{I}_V(P)$ est une bijection.
- Soit K un compact. Alors, $\mathrm{Spm}(\mathcal{C}^0(K, \mathbb{R}))$ et K sont en bijection.

Corollaire 5.1.1. *Soit $\mathcal{I} \subset k[V]$. Alors,*

$$\mathcal{I} = k[V] \iff V(\mathcal{I}) = \varnothing.$$

Démonstration. Le sens direct est clair. Soit $\mathcal{I} \subsetneq k[V]$. Il existe $\mathfrak{m}$ un idéal maximal tel que $\mathcal{I} \subset \mathfrak{m}$. Alors, $\mathfrak{m} = \mathrm{I}_V(P)$ avec $P \in V$. On a $\mathcal{I} \subset \mathrm{I}_V(P)$ donc $\{P\} \subset \mathcal{V}(\mathrm{I}_V(P)) \subset V(\mathcal{I})$, et $V(\mathcal{I})$ est donc non non vide.

□

Corollaire 5.1.2. *On a $\Gamma(V) = k[V]$. Toute fonction rationnelle sur un ensemble algébrique irréductible V dans un corps k algébriquement clos est régulière.*

Démonstration. Si $f \in \Gamma(V)$, alors $I_f = \{h \in k[V] \mid fh \in k[V]\}$ l'idéal des dénominateurs de f. Alors, $\mathcal{V}(I_f) = \varnothing$ (c'est l'ensemble des pôles de f), donc $1 \ \in I_f$ et alors $f \in k[V]$.

□

Exercice. Soit $g \in k[V]$.

1. Montrer que si $W = \mathcal{V}(gX - 1) \subset V \times \mathbb{A}^1(k)$, alors $\mathrm{I}_{V\times\mathbb{A}^1(k)}(W) = (gX - 1)$.
2. En déduire que $k[W] \cong k[V]_g$, où

$$k[V]_g = g^{-1}k[V] = \{f/g^n \mid f \in k[V], n \in \mathbb{N}\}.$$

3. En déduire que $\Gamma(D(g)) = k[V]_g$.

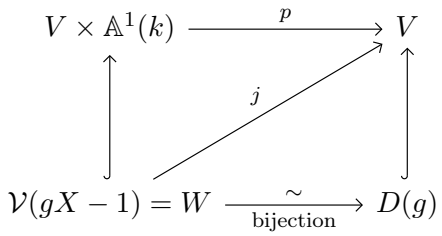
Théorème 5.1.1 (des zéros de Hilbert)**.** *Soit $\mathcal{I} \subset k[V]$ un idéal. Alors,*

$$\mathrm{I}_V(V(\mathcal{I})) = \sqrt{\mathcal{I}}.$$

Démonstration. On cherche l'équivalence suivante :

$$g \in \mathrm{I}_V(V(\mathcal{I})) \iff \exists n \in \mathbb{N}, g^n \in \mathcal{I}.$$

Le sens réciproque est clair. Pour le sens direct, soit $g \in \mathrm{I}_V(V(\mathcal{I}))$. Alors, $V(\mathcal{I}) \subset V(g)$ et donc $V(\mathcal{I}) \cap D(g) = \varnothing$. On considère l'immersion ouverte suivante.



On a donc $V(\mathcal{I}k[W]) = j^{-1}(V(\mathcal{I})) = j^{-1}(\varnothing) = \varnothing$. Ainsi, $\mathcal{I}k[W] = k[W]$. Or, d'une part on a $\mathcal{I}k[W] \cong \mathcal{I}k[V]_g$, et d'une autre $k[W] \cong k[V]_g$. Or, $1 \in k[V]_g$. Donc on peut écrire $1 = f/g^n$ avec un certain $n \in \mathbb{N}$.

□

Corollaire 5.1.3. *À ajouter.*

Corollaire 5.1.4. *Si $F = F_1^{e_1} \cdots F_r^{e_r} \in k[X_1, \ldots, X_n]$ est la décomposition en irréductibles de F, alors*

$$\mathcal{V}(F) = \mathcal{V}(F_1) \cup \cdots \cup \mathcal{V}(F_r)$$

est la décomposition en composantes irréductibles de $\mathcal{V}(F)$.

5.2 Courbe généralisée (diviseur)

Définition 5.2.1. *Une courbe plane généralisée est une combinaison linéaire non nulle*

$$C = \sum_{i=1}^{r} e_i C_i$$

(somme formelle) où les C_i sont des courbes algébriques planes irréductibles, et $e_i \in \mathbb{N}$ pour tout $i \in [\![1, r]\!]$. Si $e_i \neq 0$, la composante C_i est dite simple *si $e_i = 1$, et* multiple *si $e_i > 1$.*

Notation alternative. On note aussi $C = \bigcup_{i=1}^{r} C_i$ lorsque $e_i = 1$ pour tout $i \in [\![1, r]\!]$.

Remarque. Soit $\Phi : \mathbb{A}^n(k) \longrightarrow \mathbb{A}^n(k)$ une application bijective affine (donc un changement de coordonnées). On a

$$\Phi^{-1}\left(\sum_{i=1}^{r} e_i C_i\right) = \sum_{i=1}^{r} e_i \Phi^{-1}(C_i).$$

Définition 5.2.2. *Si C est irréductible et $\mathrm{I}(C) = (F)$, alors le degré de C est la quantité $\deg(C) = \deg(F)$. On étend cette définition en notant*

$$\deg\left(\sum_{i=1}^{r} e_i C_i\right) = \sum_{i=1}^{r} e_i \deg(C_i).$$

Exercice.

1. Montrer que si C et D sont deux courbes généralisées, alors

$$\deg(C + D) = \deg C + \deg D.$$

2. Si C est une courbe généralisée et $\Phi : \mathbb{A}^n(k) \longrightarrow \mathbb{A}^n(k)$ est une application bijective affine, alors $\deg(\Phi^{-1}(C)) = \deg C$.

Définition 5.2.3. *Si $F = F_1^{e_1} \cdots F_r^{e_r} \in k[X, Y]$ est une décomposition en irréductibles, alors le* diviseur *de F est la courbe généralisée*

$$[F] = \sum_{i=1}^{r} e_i \mathcal{V}(F_i).$$

Exercice.

1. Montrer que $[FG] = [F] + [G]$ pour tout $F, G \in k[X, Y]$.
2. Montrer que $\Phi^{-1}([F]) = [\Phi^*(F)]$ pour tout $F \in k[X, Y]$.
3. Montrer que $\deg[F] = \deg F$ pour tout $F \in k[X, Y]$.

Proposition 5.2.1. *Soit C une courbe irréductible et $P \in C$. Alors, il existe un unique $m \in \mathbb{N}$ tel que*

$$\dim_k \mathfrak{m}_{C,P}^n / \mathfrak{m}_{C,P}^{n+1} = \begin{cases} n+1 & si\ n < m, \\ m & si\ n \geq m. \end{cases}$$

Si $P = 0$ et $C = [F]$, alors $m = \mathrm{val}(F)$ (où $\mathcal{I}(C) = (F)$).

Notation. On note $m = m_P(C)$.

Démonstration. Admis.

□

Définition 5.2.4. *On dit que $m = m_P(C)$ est la multiplicité de C en P. Si $C = \sum_{i=1}^r e_i C_i$ est une courbe généralisée, on pose*

$$m_P(C) = \sum_{i=1}^r e_i m_P(C_i).$$

Convention. Si $P \notin C$, on pose $m_P(C) = 0$.

Exercice.

1. Montrer que $m_P(C + D) = m_P(C) + m_P(D)$.
2. Montrer que $m_{\Phi(P)}(C) = m_P(\Phi^{-1}(C))$.
3. $m_0([F]) = \mathrm{val}(F)$.

Exemple. Soit C la courbe d'équation $Y^2 - 2Y = X^3 - 1$ et $P = (0, 1)$. Soit $\Phi(X, Y) = (X, Y + 1)$. On a $P = \Phi(0)$ et $m_P(C) = m_0(\Phi^{-1}(C))$. Si on note $F = 0$ le polynôme irréductible définissant C, alors $\Phi^{-1}(C)$ est la courbe d'équation $\Phi^*(F) = 0$. Le calcul permet de montrer que $\Phi^{-1}(C)$ a pour équation $Y^2 = X^3$ et donc $m_P(C) = 0$.

Définition 5.2.5. *Soit C une courbe généralisée. Alors, on note $P \in C$ si $m_P(C) \neq 0$. Le point P est dit singulier si $m_P(C) > 1$. La courbe C est non-singulière si tous ses points ne sont pas singulier.*

Exercice.

1. Si $C = [F]$, alors $P \in C$ *si et seulement si* $F(P) = 0$.
2. Montrer que $\Phi(P) \in C$ *si et seulement si* $P \in \Phi^{-1}(C)$. Dans ce cas, montrer que $\Phi(P)$ est singulier *si et seulement si* P l'est.
3. Monter que $0 \in [F]$ *si et seulement si* $\mathrm{val}(F) > 0$, et que 0 est singulier *si et seulement si* $\mathrm{val}(F) > 1$.

Exemples.

— La courbe $[Y^2 - X^3 + X]$ est non singulière.

— La courbe d'équation $[Y^2 - X^3 + X^2]$ est telle que 0 est un point double : $m_0(C) = 2$ (c'est son seul point non singulier).

— $[Y^2 - X^3]$ a aussi 0 pour point double.

— La courbe $[Y^2 - X^3 + X] + [X^2 + Y^2 - 1]$ possède deux points doubles.

— La courbe $2[Y]$ est entièrement singulières.

Remarques.

— Une courbe non-singulière n'a que des composantes simples qui ne se rencontrent pas. En effet, si $C = \sum_{i=1}^{r} e_i C_i$ et $1 = m_P(C) = \sum_{i=1}^{r} e_i m_P(C_i)$, alors $e_i = 0$ pour tout $i \in [\![1, r]\!]$ sauf pour un certain $i_0 \in [\![1, r]\!]$ qui est tel que $m_p(C_{i_0}) = 1$ et $e_{i_0} = 1$.

— Une conique irréductible est non singulière. En effet, si P est un point singulier de $C = \mathcal{V}(F)$ (avec F irréductible) et $\deg F = 2$, on peut supposer quitte à translater que $P = 0$. On a donc $\mathrm{val}(F) \geq 2$ mais puisque $\deg(F) = 2$, F est nécessairement homogène. Puisque le corps est algébriquement clos, F est réductible.

Proposition 5.2.2. *Soit $P \in C = [F]$. Alors, P est singulier* si et seulement si $F'(P) = 0$. *C'est encore équivalent à dire que*

$$\frac{\partial F}{\partial X}(P) = \frac{\partial F}{\partial Y}(P) = 0.$$

Démonstration. On présente seulement l'idée de la démonstration. Tout d'abord, on peut se ramener *via* un changement de variable au cas $P = 0$. Ensuite, on écrit

$$F = F(0) + \frac{\partial F}{\partial X}(0)X + \frac{\partial F}{\partial Y}(0)Y \mod (X, Y)^2.$$

On remarque aussi que $\mathrm{val}\, F \geq 2$ *si et seulement si* $F \in (X, Y)^2$.

□

Exemple. On suppose $\mathrm{car}\, k \in \{2, 3\}$. On cherche les points singuliers de $F = (X^2 + Y^2)^2 - 3X^2Y + Y^3 = 0$ (équation du trèfle à trois feuilles). Le calcul des dérivées partielles de F montre que 0 est un point singulier (de multiplicité 3). C'est aussi le seul.