Algèbre commutative et géométrie algébrique

Bernard Le Stum

Master 1 de mathématiques fondamentales · Université de Rennes 1
Notes prises par Téofil Adamski (version du 16 mars 2021)

Chapitre 1

Polynômes

1.1 Anneaux de polynômes

Tous les anneaux considérés sont commutatifs et unitaire. Dans tout le chapitre, on fixe un tel anneau R. On fixe également un entier $n \in \mathbf{N}$.

Définition 1.1. Une *R-algèbre* est un anneau A muni d'une loi externe $(c, f) \in R \times A \longmapsto cf \in A$ vérifiant les points suivants :

1. pour tout $f \in A$, on a $1_R f = f$;
2. pour tous $c_1, c_2 \in R$ et $f \in A$, on a $(c_1 + c_2)f = c_1 f + c_2 f$;
3. pour tous $c_1, c_2 \in R$ et $f_1, f_2 \in A$, on a $(c_1 c_2)(f_1 f_2) = (c_1 f_1)(c_2 f_2)$.

Un *morphisme* de R-algèbres entre deux R-algèbres A et B est un morphisme d'anneaux $u\colon A \longrightarrow B$ tel que

$$\forall c \in R,\ \forall f \in A, \quad u(cf) = cu(f).$$

◇ Remarques. – Pour toute R-algèbre A, l'application $c \in A \longmapsto c1_A$ est un morphisme d'anneaux. Réciproquement, pour tout morphisme d'anneaux $u\colon A \longrightarrow B$, l'application $(f, g) \longmapsto u(f)g$ munit l'anneau B d'une structure de A-algèbre.

– Une algèbre sur un corps k est un espace vectoriel où la multiplication est bilinéaire. Réciproquement, pour tout k-espace vectoriel A et toute application bilinéaire $b\colon A \times A \longrightarrow A$, cet espace vectoriel A est une k-algèbre muni de la loi externe b.

– Pour tout ensemble E et toute R-algèbre A, l'ensemble A^E est une R-algèbre muni de l'évaluation.

Lemme 1.2. Il existe une R-algèbre $R[X_1, \ldots, X_n]$ muni de n éléments X_1, …, X_n vérifiant la propriété suivante : étant donnés une R-algèbre A et $f_1, \ldots, f_n \in A$, il existe un unique morphisme de R-algèbres de $R[X_1, \ldots, X_n]$ dans A envoyant chaque élément X_i sur chaque élément f_i.

Preuve Il suffit de procéder par récurrence sur l'entier n et de se rappeler la propriété universelle de l'algèbre $R[X]$. □

◇ Remarques. – On peut montrer l'unicité de la R-algèbre $R[X_1, \ldots, X_n]$ à isomorphisme près. Cette anneau est appelé l'*anneau des polynômes* à n variables sur R. Un *monôme de degré $d \in \mathbf{N}$* est un élément de la forme $X_1^{d_1} \cdots X_n^{d_n}$ avec $d = d_1 + \cdots + d_n$. Les monôme forment alors une base du R-module $R[X_1, \ldots, X_n]$.

– De plus, pour un corps infini k, l'application canonique $k[X_1, \ldots, X_n] \longrightarrow \mathscr{F}(k^n, k)$ est un morphisme injectif de k-algèbres.

Définition 1.3. 1. Le *degré* (respectivement la *valuation*) d'un polynôme $F \in R[X_1, \ldots, X_n]$ est le plus grand (respectivement le plus petit) degré des termes non nuls apparaissant dans son écriture. On les notes respectivement $\deg F$ et $\operatorname{val} F$.

2. Un polynôme $F \in R[X_1, \ldots, X_n]$ est *homogène* si $\deg F = \operatorname{val} F$.

◇ Remarques. – Le degré et la valuation vérifient des propriétés similaires au degré défini pour un polynôme de $R[X]$.

– Pour tout polynôme homogène $F \in R[X_1, \ldots, X_{n+1}]$, on pose $F_* \coloneqq F(X_1, \ldots, X_n, 1)$. Pour tout polynôme $F \in R[X_1, \ldots, X_n]$ de degré $d \in \mathbf{N}$, on pose

$$F^* \coloneqq X_{n+1}^d F(X_1/X_{n+1}, \ldots, X_n/X_{n+1})$$

qui est un polynôme homogène de $R[X_1, \dots, X_{n+1}]$. Alors en considérant les bons polynômes, on a

$$(FG)_* = F_* G_*, \quad (FG)^* = F^* G^*, \quad F = (F^*)_* \quad \text{et} \quad F = X^m (F_*)^*$$

où l'entier $m \in \mathbf{N}$ est la valuation de F en X^{n+1}.

▷ Exemples. Illustrons ces notations. On considère le polynôme $P \coloneqq X^2 + XY + Y^2 \in \mathbf{R}[X, Y]$. Alors on obtient

$$P_* = X^2 + X + 1 = (X - j)(X - j^2) \quad \text{avec} \quad j \coloneqq e^{2i\pi/3}$$

ce qui, avec la dernière propriété, permet d'écrire

$$P = (P_*)^* = (X - j)^*(X - j^2)^* = (X - jY)(X - j^2 Y).$$

Définition 1.4. Le *polynôme dérivé* d'un polynôme $F \coloneqq a_0 + \cdots + a_d X^d \in R[X]$ est le polynôme

$$F' \coloneqq \sum_{k=1}^{d} k a_k X^{k-1} \in R[X].$$

On peut également le noter $\mathrm{d}F/\,\mathrm{d}X$.

◇ Remarques. – Soit A une R-algèbre. Pour tous $F \in R[X_1, \dots, X_n]$ et $G_1, \dots, G_2 \in A[X]$, on a

$$\frac{\mathrm{d}F(G_1, \dots, G_n)}{\mathrm{d}X} = \sum_{i=1}^{n} \frac{\mathrm{d}F}{\mathrm{d}X_i}(G_1, \dots, G_n) \frac{\mathrm{d}G_i}{\mathrm{d}X}.$$

– Pour tout $F \in R[X, Y]$, on dispose de la relation de Schwarz

$$\frac{\mathrm{d}^2 F}{\mathrm{d}X\,\mathrm{d}Y} = \frac{\mathrm{d}^2 F}{\mathrm{d}Y\,\mathrm{d}X}.$$

– Soit k un corps de caractéristique $p \in \mathbf{N}$. Pour tout $F \in k[X, Y]$, tout $N \in \mathbf{N}^*$ et tout $a, b \in k$, on dispose de la formule de Taylor

$$F \equiv \sum_{k<N} \frac{1}{k!} \sum_{i+j=k} \binom{k}{i} \frac{\mathrm{d}^k F}{\mathrm{d}X^i\,\mathrm{d}Y^j}(a, b)(X - a)^i (Y - b)^j \mod \langle X - a, X - b \rangle^N$$

avec la condition $N \leqslant p$ lorsque $p > 0$.

1.2 Anneaux factoriels

On suppose maintenant que l'anneau R est intègre.

Proposition 1.5 *(division euclidienne).* Soit $F \in R[X]$ un polynôme non nul de degré $d \in \mathbf{N}^*$ tel que son coefficient dominant $a \in R$ soit inversible. Alors l'application composée

$$R[X]_{<d} \hookrightarrow R[X] \twoheadrightarrow R[X]/\langle F \rangle$$

est bijective.

Preuve L'injectivité de cette application est évidente. Montrons sa surjectivité. Soit $G \in R[X]$ Tout d'abord, remarquons qu'il existe deux polynômes $Q, H \in R[X]$ tels que $G = FQ + H$: il suffit de prendre $Q = 0$ et $H = G$. Pour conclure, choisissons un tel polynôme $H \in R[X]$ de plus petit degré $r \in \mathbf{N}$ et montrer que $r < d$. Dans le cas contraire, en notant $c \in R$ son coefficient dominant et en posant $H_1 \coloneqq H - \frac{c}{a} X^{d-r} F$, on obtient $\deg H_1 < r$ et $G = FQ_1 + H_1$ avec $Q \coloneqq Q + cX^{d-r}$ ce qui est impossible. □

Corollaire 1.6. On reprend les mêmes notations. Pour tout $G \in R[X]$, il existe un unique couple de polynômes $(Q, H) \in R[X]^2$ tel que

$$G = FQ + H \quad \text{et} \quad \deg H < d.$$

◇ Remarque. Soient k un corps et $a_1, \dots, a_n \in k$. Alors on peut montrer, par récurrence, que l'idéal $\langle X_1 - a_1, \dots, X_n - a_n \rangle$ de $k[X_1, \dots, X_n]$ est maximal et qu'il existe un isomorphisme

$$k[X_1, \dots, X_n]/\langle X_1 - a_1, \dots, X_n - a_n \rangle \simeq k.$$

Définition 1.7. Soit A un anneau intègre. Deux éléments $f, g \in A$ sont *étrangers* (respectivement *premiers entre eux*) si, pour tout idéal (respectivement principal) I de A, on a $f, g \in I \Rightarrow I = A$.

◇ Remarques. – Deux éléments $f, g \in A$ sont étrangers si et seulement s'ils satisfont l'identité de Bézout, *i. e.* il existe $u, v \in A$ tels que $fu + gv = 1$.

– Deux éléments sont premiers entre eux si et seulement si tout facteur commun est inversible.

– Deux polynômes de $R[X]$ premiers entre eux n'ont aucune racine commune. La réciproque est vrai sur un corps algébriquement clos.

Définition 1.8. Soit A un anneau intègre.

1. Un élément $p \in A \setminus \{0\}$ est *irréductible* (respectivement *premier*) si l'idéal $\langle p \rangle$ de A est maximal (respectivement premier).
2. L'anneau A est *factoriel* s'il existe une partie $\mathbb{P} \subset A$ telle que l'application

$$\left| \begin{array}{l} \mathbf{N}^{(\mathbb{P})} \longrightarrow (A \setminus \{0\})/A^\times, \\ (v_p)_{p \in \mathbb{P}} \longmapsto \overline{\displaystyle\prod_{p \in \mathbb{P}} p^{v_p}} \end{array} \right.$$

soit bijective. Une telle partie $\mathbb{P}$ est appelée un *système de représentant d'irréductibles*.

◇ Remarque. On rappel que le lemme de Gauss est vérifié dans un anneau factoriel et que tout anneau principal est factoriel.

Définition 1.9. Un polynôme de $R[X]$ est *primitif* si ses coefficients sont premiers entre eux.

◇ Remarques. – Tout polynôme irréductible sur un corps k est irréductible sur un sous-corps de k.

– Un polynôme $F \in k[X_1, \dots, X_n]$ est irréductible si et seulement si le polynôme irréductible F^* l'est. Le même est énoncé reste valable avec le polynôme F_* pour un polynôme $F \in k[X_1, \dots, X_{n+1}]$ qui n'est pas un multiple du monôme X_{n+1}.

Définition 1.10. Soit A un anneau intègre.

1. Un *plus grand commun diviseurs* (ou pgcd) de deux éléments $f, g \in R$ est un éléments $d \in R$ tel que l'idéal $\langle d \rangle$ soit le plus petit idéal principal contenant l'idéal $\langle f, g \rangle$.
2. Un *plus petit commun multiple* (ou ppcm) de deux éléments $f, g \in R$ est un éléments $d \in R$ tel que l'idéal $\langle d \rangle$ soit le plus grand idéal principal contenu l'idéal $\langle f, g \rangle$.

Théorème 1.11. Soit R un anneau factoriel. Alors l'anneau $R[X]$ est factoriel. De plus, les irréductibles de $R[X]$ sont les irréductibles de R et les polynômes irréductible de $(\operatorname{Frac} R)[X]$.

Preuve Notons $K \coloneqq \operatorname{Frac} R$ le corps des fractions de R. Soient $\mathbb{P}$ et $\mathscr{Q}$ des systèmes de représentations d'irréductibles dans anneaux R et $K[X]$. On dispose alors de deux bijections

$$\mathbf{N}^{(\mathbb{P})} \simeq (R \setminus \{0\})/R^\times \quad \text{et} \quad \mathbf{N}^{(\mathscr{Q})} \simeq (K[X] \setminus \{0\})/K[X]^\times.$$

Quitte à multiplier tout polynôme $F \in \mathbf{Q}$ par un élément bien choisi de R, on peut toujours supposer que ce polynôme F est un polynôme primitif de $R[X]$. On obtient alors

$$\mathbf{N}^{(\mathbb{P} \cup \mathscr{Q})} \simeq (R[X] \setminus \{0\})/R[X]^\times.$$

En effet, soit $F \in R[X]$. Alors on peut l'écrire de manière unique sous la forme $a \prod F_i^{n_i}$ avec $F_i \in \mathscr{Q}$ et $a \in K^\times$. On peut supposer que les polynôme F_i sont primitifs. Dans ce cas, il vient que $a \in R$. Il suffit d'alors de décomposé l'élément a en produit d'éléments irréductibles de $\mathscr{Q}$ et on a fini. □

◇ Remarque. Soit R un anneau factoriel.

– L'anneau $R[X_1, \dots, X_n]$ est factoriel.

– Deux polynômes de $R[X]$ premiers entre eux le sont dans $(\operatorname{Frac} R)[X]$. La réciproque est vrai pour deux polynômes primitifs de $R[X]$.
– Un polynôme de $R[X]$ est non constant et irréductible sur R si et seulement s'il est primitif et irréductible sur $\operatorname{Frac} R$.
– On rappel le critère d'Eisenstein : un polynôme primitif $a_d X^d + \cdots + a_0 \in R[X]$ est irréductible si et seulement s'il existe un idéal premier $\mathfrak{p}$ de R tel que

$$a_d \notin \mathfrak{p}, \quad a_{d-1}, \dots, a_0 \in \mathfrak{p} \quad \text{et} \quad a_0 \notin \mathfrak{p}^2.$$

Par exemple, ce critère assure que le polynôme $X^7 + X^4Y^2 + Y \in \mathbf{R}[X,Y]$ est irréductible sur $\mathbf{R}$ en prenant $R \coloneqq \mathbf{R}[Y]$ et $\mathfrak{p} \coloneqq \langle Y \rangle$.

1.3 Résultant

On fixe un anneau intègre R dont on note $K \coloneqq \operatorname{Frac} R$ le corps des fractions. Soient $F, G \in R[X]$ deux polynômes de degrés respectifs $d, e \in \mathbf{N}$ tels que $d + e > 0$.

Définition 1.12. Le *résultant* des polynômes F et G est le déterminant dans les bases canoniques, noté $\operatorname{Res}(F,G)$, de l'application de Sylvester

$$\begin{vmatrix} R[X]_{<e} \oplus R[X]_{<d} & \longrightarrow & R[X]_{<e+d}, \\ (U,V) & \longmapsto & UF + VG. \end{vmatrix}$$

En écrivant $F = \sum_{k=0}^{d} a_k X^k$ et $G = \sum_{k=0}^{e} b_k X^k$, en évaluant l'application de Sylvester sur la base canonique, ce déterminant vaut simplement

$$\operatorname{Res}(F,G) = \begin{vmatrix} a_d & \cdots & \cdots & a_0 & 0 & \cdots & 0 \\ 0 & \ddots & & & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & & & \ddots & 0 \\ 0 & \cdots & 0 & a_d & \cdots & \cdots & a_0 \\ b_e & \cdots & \cdots & b_0 & 0 & \cdots & 0 \\ 0 & \ddots & & & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & & & \ddots & 0 \\ 0 & \cdots & 0 & b_e & \cdots & \cdots & b_0 \end{vmatrix}.$$

Proposition 1.13. Il existe deux polynômes $U \in R[X]_{<e}$ et $V \in R[X]_{<d}$ tels que

$$\operatorname{Res}(F,G) = UF + VG.$$

Preuve Ceci est une conséquence de la formule de Laplace. Notons $M \in \mathscr{M}_{e+d}(R)$ la matrice de l'application de Sylvester. Alors il existe une matrice $M^* \in \mathscr{M}_{e+d}(R)$ tel que $MM^* = (\det M) I_{e+d}$. Par conséquent, pour tout $w \in R^{e+d}$, il existe un vecteur $v \in R^{e+d}$ tel que $Mv = (\det M)w$: il suffit de prendre $v = M^*v$. Le cas $w = 1$ donne le résultat. □

◇ Remarque. Le résultant $\operatorname{Res}(F,G)$ est alors un élément de l'intersection $\langle F, G \rangle \cap R$.

Proposition 1.14. Le résultant $\operatorname{Res}(F,G)$ est nul si et seulement s'il existe deux polynômes non nuls $U \in R[X]_{<e}$ et $V \in R[X]_{<d}$ tels que

$$UF + VG = 0.$$

Preuve Remarquons que le résultant est nul si et seulement si l'application de Sylvester n'est pas injective, *i. e.* il existe deux polynômes non tous nuls $U \in R[X]_{<e}$ et $V \in R[X]_{<d}$ tels que $UF + VG = 0$. Si on avait $V = 0$, alors on aurait $UF = 0$, donc $F = 0$ ce qui est impossible. □

Corollaire 1.15. On suppose que l'anneau R est factoriel. Alors le résultant $\operatorname{Res}(F,G)$ n'est pas nul si et seulement si les polynômes F et G sont premiers entre eux dans $K[X]$.

Preuve On montre la contraposée dans les deux sens.

$\Rightarrow$ On suppose qu'ils ne sont pas premiers entre eux dans $K[X]$. Alors on peut les écrire sous la forme $F = -VH$ et $G = UH$ dans $R[X]$ avec $\deg H > 0$. Alors $0 \leqslant \deg U < e$ et $0 \leqslant \deg V < d$. De plus, comme $(UF + VG)H = GF - FG = 0$ et $H \neq 0$, on obtient $UF + VG = 0$ où les polynômes U et V ne sont pas tous les deux nuls. On en déduit que l'application de Sylvester n'est pas injective. En particulier, elle n'est pas bijective et son déterminant $\operatorname{Res}(F, G)$ est nul.

$\Leftarrow$ Réciproquement, on suppose que $\operatorname{Res}(F, G) = 0$. Alors il existe deux polynômes $U \in R[X]_{<e}$ et $V \in R[X]_{<d}$ non tous nuls tels que $UF + VG = 0$. Alors $-UF = VG$, donc $F \mid VG$. Si les polynômes F et G sont premiers entre eux dans $K[X]$, alors le lemme de Gauss assure $F \mid V$ dans $K[X]$, donc $d \leqslant \deg V$ ce qui est impossible. Donc ils ne sont pas premiers entre eux dans $K[X]$. □

LEMME 1.16. Soit $\alpha \in R$. Alors

$$\operatorname{Res}((X - \alpha)F, G) = G(a) \operatorname{Res}(F, G).$$

Preuve On remarque que $\operatorname{Res}(XF, G) = G(0) \operatorname{Res}(F, G)$ et il suffit de faire une translation. □

◇ REMARQUE. On écrit $F = a \prod_{i=1}^{d} (X - \alpha_i)$. Une simple récurrence montre alors

$$\operatorname{Res}(F, G) = a^e \prod_{i=1}^{d} G(\alpha_i).$$

De plus, on écrit $G = b \prod_{j=1}^{e} (X - \beta_j)$. De la relation précédente, on en déduit

$$\operatorname{Res}(F, G) = a^e b^d \prod_{i=1}^{d} \prod_{j=1}^{e} (\alpha_i - \beta_j).$$

PROPOSITION 1.17. Soient $G_1, G_2, Q, H \in R[X]$ quatre polynômes tels que $G = G_1 G_2 = FQ + H$. On note $f \coloneqq \deg H$ et $a \in R$ le coefficient dominant de F. Alors

$$\operatorname{Res}(F, G) = \operatorname{Res}(F, G_1) \operatorname{Res}(F, G_2) \quad \text{et} \quad \operatorname{Res}(F, G) = a^{e-f} \operatorname{Res}(F, H).$$

Preuve Quitte se placer dans une extension algébriquement clos de R, on peut écrire

$$F = a \prod_{i=1}^{d} (X - \alpha_i).$$

On note $e_1 \coloneqq \deg G_1$ et $e_2 \coloneqq \deg G_2$. D'après la remarque précédente, on obtient

$$\operatorname{Res}(F, G) = a^e \prod_{i=1}^{d} G(\alpha_i) = a^{e_1} \prod_{i=1}^{d} G_1(\alpha_i) \times a^{e_2} \prod_{i=1}^{d} G_2(\alpha_i) = \operatorname{Res}(F, G_1) \operatorname{Res}(F, G_2)$$

et

$$\operatorname{Res}(F, G) = a^e \prod_{i=1}^{d} G(\alpha_i) = a^{e-f} a^f \prod_{i=1}^{d} H(\alpha_i) = a^{e-f} \operatorname{Res}(F, H).$$ □

1.4 Bases de Gröbner

On fixe un corps k et un entier $n \in \mathbf{N}^*$. Pour un n-uplet $i \coloneqq (i_1, \ldots, i_n) \in \mathbf{N}^n$, on notera

$$X^i \coloneqq X_1^{i_1} \cdots X_n^{i_n} \in k[X_1, \ldots, X_n] \quad \text{et} \quad |i| \coloneqq i_1 + \cdots + i_n.$$

L'élément neutre du groupe additif $\mathbf{N}^n$ sera également noté 0.

DÉFINITION 1.18. Un *ordre total additif* sur $\mathbf{N}^n$ est une relation $\leqslant$ vérifiant

1. pour tous $i, j \in \mathbf{N}^n$, on a $i \leqslant j$ ou $j \leqslant i$;
2. pour tous $i, j \in \mathbf{N}^n$, si $i \leqslant j$ et $j \leqslant i$, alors $i = j$;
3. pour tous $i, j, j \in \mathbf{N}^n$, si $i \leqslant j$ et $j \leqslant k$, alors $i \leqslant k$;
4. pour tous $i, j, k \in \mathbf{N}^n$, si $i \leqslant j$, alors $i + k \leqslant j + k$;

5. pour tout $i \in \mathbf{N}^n$, on a $0 \leqslant i$.

Une telle relation induit un *ordre total multiplicatif* sur les mônomes de $k[X_1, \dots, X_n]$ en posant

$$X^i \leqslant X^j \iff i \leqslant j, \qquad i, j \in \mathbf{N}^n.$$

◇ Remarque. On peut montre qu'un ordre total additif est un bon ordre : toute partie non vide possède un plus petit élément. On pourra alors procéder par récurrence.

Définition 1.19. On considère les ordres sur $\mathbf{N}^n$ déclarant $i \leqslant j$ pour deux éléments $i, j \in \mathbf{N}^n$ si

– *ordre lexicographique* ou lex : le premier terme non nul de $j - i$ est positif ;
– *ordre lexicographique inverse* ou invlex : le dernier terme non nul de $j - i$ est positif ;
– *ordre lexicographique gradué* ou deglex : $|i| < |j|$ ou, si $|i| = |j|$, alors le premier terme non nul de $j - i$ est positif ;
– *ordre lexicographique inverse gradué* ou degrevlex : $|i| < |j|$ ou, si $|i| = |j|$, alors le dernier terme non nul de $j - i$ est négatif.

▷ Exemple. Rangons les mônomes X, XZ, Y et Y^2 dans $k[X, Y, Z]$ pour ces quatre ordres :

– lex : $XZ > X > Y^2 > Y$;
– invlex : $XZ > Y^2 > Y > X$;
– deglex : $XZ > Y^2 > X > Y$;
– degrevlex : $Y^2 > XZ > X > Z$.

On fixe maintenant un ordre total additif sur $\mathbf{N}^n$.

Définition 1.20. Pour un polynôme $F \in k[X_1, \dots, X_n]$ non nuls, on pose

– $\mathrm{M}(F) \in k[X_1, \dots, X_n]$ le monôme d'ordre maximal de F, appelé le *monôme dominant* ;
– $\mathrm{T}(F) \in k[X_1, \dots, X_n]$ le terme d'ordre maximal de F, appelé le *terme dominant* ;
– $\mathrm{c}(F) \in k$ le coefficient d'ordre maximal de F, appelé le *coefficient dominant*.

Par convention, on pose $\mathrm{M}(0) = \mathrm{T}(0) = \mathrm{c}(0) = 0$.

◇ Remarque. Pour tous polynômes $F, G \in k[X_1, \dots, X_n]$, on a

$$\begin{aligned} \mathrm{M}(F) = 0 &\iff F = 0, \\ \mathrm{M}(F) = 1 &\iff \deg F = 0, \\ \mathrm{M}(FG) &= \mathrm{M}(F)\,\mathrm{M}(G), \\ \mathrm{M}(F+G) &\leqslant \max(\mathrm{M}(F), \mathrm{M}(G)) \end{aligned}$$

où la dernière inégalité est une égalité lorsque $\mathrm{M}(F) = \mathrm{M}(G)$.

Définition 1.21. Soient $F, G, H \in k[X_1, \dots, X_n]$. On dit que le polynôme F se *réduit en une étape* en H modulo G s'il existe $Q \in k[X_1, \dots, X_n]$ tel que $F = CQ + H$. On note alors $F \xrightarrow{G} H$.

Soit $S \coloneqq \{G_1, \dots, G_r\}$ une partie finie de $k[X_1, \dots, X_n]$. On dit que le polynôme F se réduit en H modulo S s'ils existe $H_1, \dots, H_{r-1} \in k[X_1, \dots, X_n]$ tels que

$$F \xrightarrow{G_1} H_1 \xrightarrow{G_2} \cdots \xrightarrow{G_{r-1}} H_{r-1} \xrightarrow{G_r} H.$$

On note alors $F \xrightarrow{S}{}_+ H$.

On dit que le polynôme H est une *forme normal* de F modulo S si $F \xrightarrow{S}{}_+ H$ et il n'est pas réductible en une étape modulo un élément de S.

◇ Remarque. – Le polynôme H est une forme normale modulo S si et seulement si aucun terme non nul n'est multiple d'un terme $\mathrm{M}(G)$ avec $G \in S$. Ainsi les formes normales module S forment un sous-espace vectoriel de $k[X_1, \dots, X_n]$.
– Il existe toujours une forme normal H pour un polynôme F et on peut écrire ce dernier sous la forme

$$F = \sum_{i=1}^{r} G_i Q_i + H$$

pour des éléments $G_i \in S$ et $Q_i \in k[X_1, \dots, X_n]$ vérifiant $\mathrm{M}(G_i Q_i) \leqslant \mathrm{M}(F)$.
– Dans le cas particulier $n = 1$, la forme normale du polynôme F par rapport à un singleton $\{G\}$ avec $G \in k[X_1, \dots, X_n]$ est le reste de la division euclidien de F par G.

▷ Exemple. On considère l'ensemble $S \coloneqq \{Y^2 - 1, XY - 1\}$ et l'ordre lex. Trouvons une forme normale du polynôme $P \coloneqq X^2Y + XY^2 + Y^2$ modulo S. On obtient

$$\begin{aligned} P &= X(XY-1) + XY^2 + X + Y^2 \\ &= X(XY-1) + Y(XY-1) + X + Y^2 + Y \\ &= X(XY-1) + Y(XY-1) + (Y^2-1) + X + Y + 1 \end{aligned}$$

ce qui montre $P \xrightarrow{s}_+ X + Y + 1$.

Notation. Pour une partie $S \subset k[X_1, \dots, X_n]$, on note

$$\mathrm{M}(S) \coloneqq \{\mathrm{M}(F) \mid F \in S\}.$$

Définition 1.22. Une *base* (respectivement *base de Gröbner*) pour un idéal I de $k[X_1, \dots, X_n]$ est une partie $S \subset I$ telle que

$$\langle S \rangle = I \qquad (\text{respectivement } \langle \mathrm{M}(S) \rangle = \langle \mathrm{M}(I) \rangle).$$

◇ Remarques. – Une partie $S \subset I$ est une base de Gröbner pour I si et seulement si

$$\forall F \in I,\ \exists G \in S, \quad \mathrm{M}(G) \mid \mathrm{M}(F).$$

– On peut montrer que toute partie d'un idéal I contenant une base est elle même une base pour I et que tout base pour I contient une base finie pour I. Ainsi il existe des bases finies pour I. Les mêmes énoncés sont également vérifiés pour des bases de Gröbner.

Lemme 1.23. Soit S une base de Gröbner pour un idéal I. Alors c'est une base pour I.

◇ Remarque. On peut donc parler d'une base de Gröbner sans mentionner l'idéal.

Preuve L'inclusion $\langle S \rangle \subset I$ est évidente. Réciproquement, soit $F \in I$ un polynôme non nul. Grâce à la remarque précédente, il existe un polynôme $G \in S$ tel que $\mathrm{M}(G) \mid \mathrm{M}(F)$. On peut donc trouver un polynôme $M \in k[X_1, \dots, X_n]$ tel que $\mathrm{T}(F) = M\,\mathrm{T}(G)$. On obtient alors

$$\begin{aligned} F &= M\,\mathrm{T}(G) + (F - \mathrm{T}(F)) \\ &= MG + H \quad \text{avec} \quad H \coloneqq -M(G - \mathrm{T}(G)) + (F - \mathrm{T}(F)) \end{aligned}$$

avec $\mathrm{M}(H) < \mathrm{M}(F)$. On peut raisonner par récurrence et, puisque $H = F - MG \in I$, on a $H \in \langle S \rangle$ et donc $F \in \langle S \rangle$. Cela termine la preuve. □

Théorème 1.24. Soit S une base de Gröbner. Alors tout polynôme $F \in k[X_1, \dots, X_n]$ admet une unique forme normale H modulo S et celle-ci ne dépend que de F modulo S. Ce polynôme H est appelée le *reste* de F modulo S.

Preuve Soient $F_1, F_2 \in k[X_1, \dots, X_n]$ deux polynômes tels que $F_1 \equiv F_2 \mod S$. Soient H_1 et H_2 deux formes normales pour F_1 et F_2. Alors

$$F_1 \equiv H_1 \mod S \quad \text{et} \quad F_2 \equiv H_2 \mod S,$$

donc $H \coloneqq H_1 - H_2 \equiv 0 \mod S$. Ceci implique $H \in \langle S \rangle$. Comme S est une base de Gröbner, il existe $G \in S$ tel que $\mathrm{M}(G) \mid \mathrm{M}(H)$. Alors H est nécessairement une forme normale modulo S puisque celles-ci forment un espace vectoriel. Cela implique $H = 0$, donc $H_1 = H_2$ □

◇ Remarques. – Pour toute base de Gröbner S, le reste d'un polynôme modulo S ne dépend que de l'idéal $\langle S \rangle$.
– Pour un idéal I, l'application quotient induit un isomorphisme entre le sous-espace vectoriel des formes normales et le quotient $k[X_1, \dots, X_n]/I$.
– Pour un idéal I, les conditions suivantes sont équivalentes :

(i) on a $\dim k[X_1,\dots,X_n]/I < +\infty$;
(ii) il existe un entier $N \in \mathbf{N}$ tel que $\langle X_1,\dots,X_n\rangle^N \subset \langle \mathrm{M}(I)\rangle$;
(iii) pour tout $i \in [\![1,n]\!]$, il existe un entier $N_i \in \mathbf{N}$ tel que $X_i^{N_i} \subset \langle \mathrm{M}(I)\rangle$;
(iv) pour tout $i \in [\![1,n]\!]$ et toute base de Gröbner S pour I, il existe un polynôme $G_i \in S$ et un entier $N_i \in \mathbf{N}$ tel que $\mathrm{M}(G_i) = X_i^{N_i}$.

Définition 1.25. Le *S-polynôme* de deux polynômes $G, H \in k[X_1,\dots,X_n]$ est le polynôme

$$\mathrm{S}(G,H) \coloneqq \frac{\mathrm{M}(G)\vee\mathrm{M}(H)}{\mathrm{T}(G)}G - \frac{\mathrm{M}(G)\vee\mathrm{M}(H)}{\mathrm{T}(H)}H \in k[X_1,\dots,X_n].$$

◇ Remarque. On a $\mathrm{M}(\mathrm{S}(G,H)) < \mathrm{M}(G)\vee\mathrm{M}(H)$.

Théorème 1.26 *(Buschberger).* Une partie $S \subset k[X_1,\dots,X_n]$ est une base de Gröbner si et seulement si

$$\forall G,H \in S, \quad \mathrm{S}(G,H) \xrightarrow{S}{}_+ 0.$$

Preuve Le sens direct résulte du théorème précédent puisque puisque $\mathrm{S}(G,H) \equiv 0 \mod S$ pour tous $G, H \in S$. Réciproquement, on suppose

$$\forall G,H \in S, \quad \mathrm{S}(G,H) \xrightarrow{S}{}_+ 0.$$

Montrons que, si $F = \sum_{k=1}^d H_k G_k$ avec $G_k \in S$, alors $\mathrm{M}(F) \in \langle \mathrm{M}(S)\rangle$. Il suffit de montrer qu'il existe une telle écriture de F et d'un entier $k \in [\![1,d]\!]$ tels que $M_k \coloneqq \mathrm{M}(H_kG_k) = \mathrm{M}(F)$. En effet, on aura alors $\mathrm{M}(F) \in \langle \mathrm{M}(S)\rangle$. Pour cela, on va même montrer que l'on peut trouver une telle écriture avec $\mathrm{M}(F) = M \coloneqq \max(M_1,\dots,M_d)$ ce qui conclura la preuve. Puisque

$$F = \sum_{M_k=M} \mathrm{T}(H_k)G_k - \sum_{M_k=M}(H_k - \mathrm{T}(H_k))G_k + \sum_{M_k<M} H_kG_k,$$

il suffit, par récurrence, de considérer la première somme. On peut donc supposer que

(i) les polynômes H_k se réduisent à un seul terme,
(ii) la quantité $\mathrm{M}(H_k)\,\mathrm{M}(G_k) = M$ ne dépend pas de l'entier $k \in [\![1,d]\!]$.

On suppose $\mathrm{M}(F) < M$. Montrons que

$$F = \sum_{j=1}^{d-1}\Big(\sum_{i=1}^{j}\mathrm{c}(H_iG_i)\Big)\frac{M}{\mathrm{M}(G_j)\vee\mathrm{M}(G_{j+1})}\mathrm{S}(G_j,G_{j+1}).$$

Puisque $\mathrm{M}(F) < M = \mathrm{M}(H_kG_k)$ pour $k \in [\![1,d]\!]$ et $F = \sum_{k=1}^d H_kG_k$, on a $\sum_{k=1}^d \mathrm{c}(H_kG_k) = 0$. Pour tout $k \in [\![1,d]\!]$, on écrit $G_k = \mathrm{c}(G_k)G'_k$ et $H_k = \mathrm{c}(H_k)H'_k$. On obtient alors

$$\begin{aligned}\sum_{j=1}^{d-1}\Big(\sum_{i=1}^{j}\mathrm{c}(H_iG_i)\Big)(H'_jG'_j - H'_{j+1}G'_{j+1}) &= \sum_{i=1}^{d-1}\mathrm{c}(H_iG_i)\sum_{j=i}^{d-1}(H'_jG'_j - H'_{j+1}G'_{j+1})\\ &= \sum_{i=1}^{d-1}\mathrm{c}(H_iG_i)(H'_iG'_i - H'_dG'_d)\\ &= \sum_{i=1}^{d-1}\mathrm{c}(H_iG_i)H'_iG'_i + \mathrm{c}(H_dG_d)H'_dG'_d = F.\end{aligned}$$

Identifions les termes du membre de gauche. Pour tout $j \in [\![1,d]\!]$, l'hypothèse (ii) assure

$$H'_jG'_j = \mathrm{M}(H_j)G'_j = \frac{M}{\mathrm{M}(G_j)}G'_j = \frac{M}{\mathrm{T}(G_j)}G_j.$$

Utilisons notre hypothèse de départ. Pour tout $j \in [\![1,d-1]\!]$, on a $\mathrm{S}(G_j,G_{j+1}) \xrightarrow{S}{}_+ 0$, donc on peut écrire le S-polynôme sous la forme

$$\mathrm{S}(G_j,G_{j+1}) = \sum_{k=1}^{d} Q_{j,k}G_k \quad \text{avec} \quad \mathrm{M}(Q_{j,k}G_k) \leqslant \mathrm{M}(\mathrm{S}(G_j,G_{j+1})) < \mathrm{M}(G_j)\vee\mathrm{M}(G_{j+1}).$$

Alors en posant

$$K_k \coloneqq \sum_{j=1}^{d-1}\Big(\sum_{i=1}^{j}\mathrm{c}(H_iG_i)\Big)\frac{MQ_{j,k}}{\mathrm{M}(G_j)\vee\mathrm{M}(G_{j+1})},\quad k\in[\![1,d]\!],$$

on obtient

$$\begin{aligned}\sum_{k=1}^{d}K_kG_k &= \sum_{k=1}^{d}\sum_{j=1}^{d-1}\Big(\sum_{i=1}^{j}\mathrm{c}(H_iG_i)\Big)\frac{MQ_{j,k}}{\mathrm{M}(G_j)\vee\mathrm{M}(G_{j+1})}G_k\\ &= \sum_{j=1}^{d-1}\Big(\sum_{i=1}^{j}\mathrm{c}(H_iG_i)\Big)\frac{M\mathrm{S}(G_j,G_{j+1})}{\mathrm{M}(G_j)\vee\mathrm{M}(G_{j+1})}\\ &= \sum_{j=1}^{d-1}\Big(\sum_{i=1}^{j}\mathrm{c}(H_iG_i)\Big)M\left(\frac{G_j}{\mathrm{T}(G_j)}-\frac{G_{j+1}}{\mathrm{T}(G_{j+1})}\right)\\ &= \sum_{j=1}^{d-1}\Big(\sum_{i=1}^{j}\mathrm{c}(H_iG_i)\Big)(H'_jG'_j-H'_{j+1}G'_{j+1}) = F.\end{aligned}$$

Comme $\mathrm{M}(K_kG_k)<M$ pour tout $k\in[\![1,d]\!]$, on conclut par récurrence sur le monôme M. □

Algorithme de Buschberger. Avec le théorème, on peut en déduire un algorithme simple pour construire une base de Gröbner pour un idéal $I\subset k[X_1,\dots,X_n]$. Le voici.

Entrée : un idéal $I\subset k[X_1,\dots,X_n]$
Sortie : une base de Gröbner S pour l'idéal I

```
S ⟵ F
Répéter
    S' ⟵ S
    Pour tous éléments distincts F, G ∈ S'
        Calculer le reste H de S(F, G) modulo G
        Si H ≠ 0
            S ⟵ S ∪ {H}
Tant que S = S'
Retourner S
```

▷ Exemple. Cherche une base de Gröbner pour l'idéal $I\coloneqq\langle XY-1,Y^2-1\rangle$ pour l'ordre lexicographique. On calcule le S-polynôme

$$\mathrm{S}(XY-1,Y^2-1)=Y(XY-1)-X(Y^2-1)=X-Y.$$

Puisque $X-Y$ est une forme normal, la partie $\{XY-1,Y^2-1\}$ n'est pas une base de Gröbner. On calcule alors les deux autres S-polynômes

$$\begin{aligned}\mathrm{S}(XY-1,X-Y)&=(XY-1)-Y(X-Y)=Y^2-1\longrightarrow_+0,\\ \mathrm{S}(Y^2-1,X-Y)&=X(Y^2-1)+Y^2(X-Y)=Y^3-X=X(Y^2-1)\longrightarrow_+0.\end{aligned}$$

On voit ainsi que le partie $\{XY-1,Y^2-1,X-Y\}$ est une base de Gröbner. Enfin, puisque

$$XY-1=Y(X-Y)+Y^2-1\longrightarrow Y^2-1\longrightarrow 0$$

et qu'on ne peut pas faire mieux, la partie $\{Y^2-1,X-Y\}$ est une base de Gröbner réduite.

Proposition 1.27. Soient S un base de Gröber pour idéal $I\subset k[X_1,\dots,X_n]$ pour l'ordre lexicographique inverse. Soit $m\leqslant n$ un entier. Alors la partie $S\cap k[X_1,\dots,X_m]$ est une base de Gröbner pour l'idéal $I\cap k[X_1,\dots,X_m]$.

Preuve Soit $F\in I\cap k[X_1,\dots,X_m]$. Puisque $F\in I$ et que S est une base de Gröber pour I, il existe $G\in S$ tel que $\mathrm{M}(G)\mid\mathrm{M}(F)$. Or $\mathrm{M}(F)\in k[X_1,\dots,X_m]$, donc $\mathrm{M}(G)\in k[X_1,\dots,X_m]$. Pour l'ordre lexicographique inverse, cela implique $G\in S\cap k[X_1,\dots,X_m]$. On obtient alors $F=\mathrm{M}(G)Q+H$ dans $k[X_1,\dots,X_m]$ avec $\mathrm{M}(H)<\mathrm{M}(H)$ et on conclut par récurrence. □

◇ Remarque. La partie $S\cap k[X_1,\dots,X_m]$ est même une base pour l'idéal $I\cap k[X_1,\dots,X_n]$.

Chapitre 2

Ensembles algébriques

Dans tout ce chapitre, on fixe un corps infini k et deux entiers naturels m et n.

2.1 Zéros de polynôme

Définition 2.1. L'*espace affine* de dimension n sur k est l'ensemble $\mathbb{A}^n(k) \coloneqq k^n$. Le *lieu d'annulation* d'une partie $S \subset k[X_1, \dots, X_n]$ est l'ensemble

$$\mathrm{V}(S) \coloneqq \{P \in \mathbb{A}^n(k) \mid \forall F \in S,\ F(P) = 0\}.$$

On écrira $\mathrm{V}(F_1, \dots, F_r) \coloneqq \mathrm{V}(\{F_1, \dots, F_r\})$ pour des éléments $F_1, \dots, F_k \in k[X_1, \dots, X_n]$. La notation $\mathbb{A}^n(k)$ a plusieurs avantages par rapport à k^n : d'une part, cela permet d'oublier la structure algébrique ou topologique de k^n ; d'autre part, tout ce qu'on va développer va fonction pour l'espace projectif $\mathbb{P}^n(k)$.

Proposition 2.2. 1. On a $\mathrm{V}(1) = \emptyset$ et $\mathrm{V}(0) = \mathbb{A}^n(k)$.
2. Soit $(S_\lambda)_{\lambda\in\Lambda}$ une famille de parties de $k[X_1, \dots, X_n]$. Alors $\bigcap_{\lambda\in\Lambda} \mathrm{V}(S_\lambda) = \mathrm{V}(\bigcup_{\lambda\in\Lambda} S_\lambda)$.
3. Soient $S, T \subset k[X_1, \dots, X_n]$. Alors $\mathrm{V}(S) \cup \mathrm{V}(T) = \mathrm{V}(ST)$. Si $S \subset T$, alors $\mathrm{V}(T) \subset \mathrm{V}(S)$.

Preuve Les démonstrations de ces énoncés sont assez faciles. □

◇ Remarque. On peut même montrer que, pour tout polynôme $F \in k[X_1, \dots, X_n]$, on a

$$\mathrm{V}(F) = \mathbb{A}^n(k) \quad \Longleftrightarrow \quad F = 0$$

Proposition 2.3. Soient $F, G \in k[X, Y]$ deux polynômes premiers entre eux. Alors leur lieu d'annulation $\mathrm{V}(F, G)$ est fini.

Preuve Notons $V \coloneqq \mathrm{V}(F, G)$. Puisque les polynômes F et G sont premiers entre eux dans $k[X, Y]$, ils le sont dans l'anneau principal $k(X)[Y]$. On peut donc appliquer le théorème de Bézout : il existe deux éléments $A, B \in k(X)[Y]$ tels que $AF + BG = 1$. Autrement dit, on peut trouver un polynôme non nul $R \in k[X]$ et deux polynômes $A, B \in k[X, Y]$ tels que $AF + BG = R$. Soit $P \coloneqq (a, b) \in V$. L'égalité précédente permet d'écrire $R(a) = A(P)F(P) + B(P)G(P) = 0$, donc $a \in \mathrm{V}(R)$. Ceci montre l'inclusion $V \subset \mathrm{V}(R) \times \mathbb{A}^1(k)$ où l'ensemble $\mathrm{V}(R)$ est fini puisque $R \neq 0$. De même, on peut trouver un polynôme non nul $S \in k[Y]$ vérifiant $V \subset \mathbb{A}^1(k) \times \mathrm{V}(S)$. Tout cela permet de conclure que l'ensemble $V \subset \mathrm{V}(R) \times \mathrm{V}(S)$ est fini. □

▷ Exemple. Cherchons l'intersection de deux coniques d'équations

$$X^2 + 2Y^2 - 3 = 0 \quad \text{et} \quad X^2 + XY + Y^2 - 3 = 0$$

dans le plan réel. En retranchant une égalité à l'autre, on peut la remplacer par $Y(X - Y) = 0$ et on trouve

$$\begin{cases} Y = 0, \\ X^2 - 3 = 0 \end{cases} \quad \text{ou} \quad \begin{cases} X - Y = 0, \\ 3(X^2 - 1) = 0. \end{cases}$$

Les deux coniques s'intersectent alors en quatre points qui sont $(\pm\sqrt{3}, 0)$ et $(\pm 1, \pm 1)$.

Exercice 2.1. Soient $f, g \in k[T]$. On pose

$$S \coloneqq \{(f(t), g(t)) \mid t \in k\} \subset \mathbb{A}^2(k) \quad \text{et} \quad F \coloneqq \mathrm{Res}_T(f(T) - X, g(T) - Y) \in k[X, Y].$$

Montrer que $S \subset \mathrm{V}(F)$ avec égalité si le corps k est algébriquement clos et la partie S n'est pas réduite à un point.

▷ Soit $t \in k$. Montrons que $(f(t), g(t)) \in \mathrm{V}(F)$. Les polynômes $f(T) - f(t)$ et $g(T) - f(t)$ de $k[T]$ ont une racine commune t et la remarque de la page 5 assure que leur résultant $F(f(t), g(t))$ est nul, donc $(f(t), g(t)) \in \mathrm{V}(F)$. On peut alors conclure l'inclusion $S \subset \mathrm{V}(F)$.

Supposons maintenant que le corps k est algébriquement clos et la partie S n'est pas réduite à un point. Soit $(x, y) \in \mathrm{V}(F)$. Alors $F(x, y) = \mathrm{Res}_T(f(T) - x, g(T) - y) = 0$.

On suppose que les polynômes f et g ne sont pas constants. L'hypothèse de clôture algébrique combinée à cette même remarque nous assure alors que les polynômes $f(T) - x$ et $g(T) - y$ ont une racine commune $t \in k$. On obtient donc $(x, y) = (f(t), g(t)) \in S$.

On suppose désormais que le polynôme f est constant, l'autre cas se traitant de la même manière. On écrit $f = f_0 \in k$ Alors $F(x, y) = (f_0 - x)^e$ avec $e \coloneqq \deg G$. Comme $F(x, y) = 0$, on a $x = f_0$. Par ailleurs, la partie $S = \{(f_0, g(t)) \mid t \in k\}$ n'est pas réduite à un point, donc le polynôme $g(T)$ n'est pas constant et il en va de même pour le polynôme $g(T) - y$. En réutilisant l'hypothèse de clôture, ce dernier admet une racine $t \in k$. Alors $x = f_0 = f(t)$ et cela donne $(x, y) = (f(t), g(t)) \in k$.

Proposition 2.4. Soit $I \subset k[X_1, \ldots, X_n]$ un idéal tel que le quotient $k[X_1, \ldots, X_n]/I$ soit (de dimension) fini. Alors l'ensemble $\mathrm{V}(I)$ est fini.

Preuve On suppose que le quotient est de dimension $d \in \mathbf{N}$. Pour chaque indice $i \in [\![1, n]\!]$, cela signifie que la famille $(1, X_i, \ldots, X_i^d)$ est linéairement dépendantes modulo I, c'est-à-dire qu'il existe un polynôme nono nul $F_i \in k[X_i]$ tel que $F \in I$. Comme chaque polynôme F_i n'est pas nul, l'ensemble $\mathrm{V}(I) \subset \mathrm{V}(F_1, \ldots, F_n) = \mathrm{V}(F_1) \times \cdots \times \mathrm{V}(F_n)$ est fini. □

2.2 Ensembles algébrique affine

Définition 2.5. Une partie $V \subset \mathbb{A}^n(k)$ est *algébrique* s'il existe une partie $S \subset k[X_1, \ldots, X_n]$ tel que $V = \mathrm{V}(S)$. De plus, une partie $V \subset \mathbb{A}^n(k)$ est une *hypersurface* de degré $d \in \mathbf{N}^*$ s'il existe un polynôme $F \in k[X_1, \ldots, X_n]$ de degré d tel que $V = \mathrm{V}(F)$.

Vocabulaire. Lorsque $V = \mathrm{V}(F)$, on dit que la partie V a pour équation $F = 0$.

◇ Remarques. – Les ensembles $\mathbb{A}^n(k)$ et $\emptyset$ sont algébriques, toute partie finie est algébriques.
– D'après la proposition 2.2, toute intersection et toute union finie de sous-ensembles algébrique sont encore des sous-ensembles algébriques.
– Les sous-ensembles algébriques de $\mathbb{A}^1(k)$ sont les ensembles finis ou la droite elle-même.

Proposition 2.6. Soient $V \subset \mathbb{A}^n(k)$ et $W \subset \mathbb{A}^m(k)$ deux sous-ensembles algébriques. Alors leur produit $V \times W \subset \mathbb{A}^{n+m}(k)$ est encore un sous-ensemble algébrique.

Preuve Il suffit de « décaler » les variables des polynômes. □

◇ Remarque. – Une partie $H \subset \mathbb{A}^n(k)$ est un hyperplan de du k-espace vectoriel k^n si et seulement si c'est une hypersurface de degré un.
– Par conséquent, on peut en déduire qu'une partie non vide $E \subset \mathbb{A}^n(k)$ est un sous-espace affine si et seulement si on peut l'écrire sous la forme $E = \mathrm{V}(S)$ pour une partie S de polynômes de degré un.

Proposition 2.7. 1. Soit $L \subset \mathbb{A}^n(k)$ une droite affine et $V \subset \mathbb{A}^n(k)$ un sous-ensemble algébrique ne contenant pas L. Alors l'intersection $L \cap V$ est finie ou égale à L.
2. Soit C une courbe affine plane d'équation $F = 0$ pour un polynôme irréductible $F \in k[X, Y]$.

Soit $V \subset \mathbb{A}^2(k)$ un sous-ensemble algébrique du plan ne contenant pas C. Alors l'intersection $C \cap V$ est fini.

Preuve 1. Comme le sous-ensemble V est une intersection d'hypersurface, on peut supposer que c'est une hypersurface d'équation $F = 0$. De plus, on peut écrire la droite L comme l'image d'une application affine

$$\Phi : \left| \begin{array}{l} \mathbb{A}^1(k) \longrightarrow \mathbb{A}^n(k), \\ \qquad t \longmapsto (\alpha_1 t + \beta_1, \ldots, \alpha_n t + \beta_n). \end{array} \right.$$

Posons

$$G \coloneqq F(\alpha_1 T + \beta_1, \ldots, \alpha_n T + \beta_n) \in k[T].$$

Alors $L \cap V = \Phi(\mathrm{V}(G))$. Comme le polynôme n'a qu'une seule variable, le partie $\mathrm{V}(G) \subset \mathbb{A}^1(k)$ est soit fini, soit égal à $\mathbb{A}^1(k)$. On en déduit que l'intersection $L \cap V$ est finie ou égale à L.
2. De même, on peut supposer que le sous-ensemble V est une courbe affine plane d'équation $G = 0$. Avec la proposition 2.2, on obtient alors $C \cap V = \mathrm{V}(F, G)$. Raisonnons par l'absurde et supposons que cette intersection soit infini. Dans ce cas, la proposition 2.3 assure que les polynômes F et G ne sont pas premiers entre eux. Comme F est irréductible, cela signifie $F \mid G$ conduisant à avoir

$$C = \mathrm{V}(F) \subset \mathrm{V}(G) = V$$

ce qui est exclu par notre hypothèse. Ainsi l'intersection $C \cap V$ est finie. □

Exercice 2.2. Soient $V, W \in \mathbb{A}^n(k)$ deux sous-ensembles algébriques et $L \subset \mathbb{A}^n(k)$ une droite. On suppose $L \subset V \cap W$. Alors $L \subset V$ ou $L \subset W$.

2.3 Fonctions polynomiales

Définition 2.8. Soit $V \subset \mathbb{A}^n(k)$ un ensemble algébrique. Une fonction $f : V \longrightarrow V$ s'il existe un polynôme $F \in k[X_1, \ldots, X_n]$ tel que, pour tout point $P \in V$, on ait $f(P) = F(P)$. On note $k[V]$ l'ensemble des fonctions polynomiales sur V.

Plus généralement, une application entre deux sous-ensembles algébriques W et V est polynomiale si ses composantes le sont. On note $\mathrm{Hom}(W, V)$ l'ensemble des fonctions polynomiales de W dans V.

◇ Remarques. – Soit $V \subset \mathbb{A}^n(k)$ un ensemble algébrique. Les fonctions coordonnées

$$x_i : (a_1, \ldots, a_n) \in V \longmapsto a_i \in k$$

sont polynomiales.
– Soit $W, V \subset \mathbb{A}^n(k)$ deux ensembles algébriques tels que $W \subset V$. L'inclusion $W \hookrightarrow V$ est polynomiale. En particulier, l'identité Id_V est une application polynomiale.
– Soient V et W deux ensembles algébriques. Les projections $V \times W \longrightarrow V$ et $V \times W \longrightarrow W$ sont polynomiales.
– On peut montrer qu'une application $W \longrightarrow V$ est polynomiale si et seulement si elle se prolonge en une application polynomiale $\mathbb{A}^m(k) \longrightarrow \mathbb{A}^n(k)$. En effet, la réciproque est évidente puisque la restriction d'une application polynomiale est encore polynomiale. Directement, il suffit de prolonger l'application à tout $\mathbb{A}^m(k)$ et on peut le faire car les composantes $F_i \in k[X_1, \ldots, X_m]$ de l'application considérée $W \longrightarrow V$ peuvent se prolonger en des fonctions $\mathbb{A}^m(k) \longrightarrow k$.
– Pour tout point $P \in \mathbb{A}^n(k)$, on a $k[\{P\}] = k$.

Proposition 2.9. Le composée de deux applications polynomiales est polynomiale.

Preuve Considérons deux applications polynomiales $\psi : Z \longrightarrow W$ et $\phi : W \longrightarrow V$. Montrons que la composée $\phi \circ \psi$ est polynomiale. D'après la remarque précédente, ces deux applications se prolongent en des applications polynomiales $\Psi : \mathbb{A}^r(k) \longrightarrow \mathbb{A}^m(k)$ et $\Phi : \mathbb{A}^m(k) \longrightarrow \mathbb{A}^n(k)$. Comme $\Phi \circ \Psi$ prolonge $\phi \circ \psi$, il suffit de montrer qu'elle est polynomiale. Comme cette dernière propriété se vérifie sur les composantes, il suffit de vérifier que, pour tout $F \in k[X_1, \ldots, X_m]$, la composée $F \circ \Psi$ est polynomiale. En notant $G_1, \ldots, G_m \in k[X_1, \ldots, X_n]$ les composantes de Ψ, on a

$$F \circ \Psi = F(G_1, \ldots, G_m),$$

donc la composée $F \circ \Psi$ est bien polynomiale. □

◇ Remarque. L'image réciproque d'une hypersurface pour une application polynomiale est soit vide, soit une hypersurface. Ainsi l'image réciproque d'un ensemble algébrique par une application polynomiale est algébrique.

Définition 2.10. Une application polynomiale est un *isomorphisme* si elle est bijective et sa réciproque est polynomiale. Deux ensembles algébriques sont *isomorphes* s'il existe un isomorphisme entre eux. Une application entre deux ensembles algébriques est une *immersion fermée* si c'est las composée d'un isomorphisme et d'une inclusion d'un sous-ensemble algébrique.

▷ Exemples. – Deux courbes isomorphes n'ont pas nécessairement le même degré : on pensera aux courbes d'équation $Y = 0$ et $Y = X^2$ sur $\mathbf{R}$. En effet, les applications

$$\begin{vmatrix} \mathrm{V}(Y=0) \longrightarrow \mathrm{V}(Y=X^2), \\ (x,y) \longmapsto (x,x^2) \end{vmatrix} \quad \text{et} \quad \begin{vmatrix} \mathrm{V}(Y=X^2) \longrightarrow \mathrm{V}(Y=0), \\ (x,y) \longmapsto (x,0) \end{vmatrix}$$

sont polynomiales et réciproques l'une de l'autre.

– Une application polynomiale bijective n'est pas nécessairement un isomorphisme. On pourra considérer la projection sur l'axe des abscisses de la courbe d'équation $Y^2 = X^3$.

Proposition 2.11. Soient V et W deux ensembles algébriques et $\Gamma \subset V \times W$. Soit $\pi\colon \Gamma \longrightarrow V$ la composée de l'inclusion $\Gamma \hookrightarrow V \times W$ et de la première projection $V \times W \longrightarrow\!\!\!\!\rightarrow V$. Alors les propositions suivantes sont équivalentes :

(i) l'ensemble Γ est un le graphe d'une application polynomiale ;

(ii) il est algébrique et l'application π est un isomorphisme.

Preuve Par définition, l'ensemble Γ est le graphe d'une application $\varphi\colon V \longrightarrow W$ si et seulement si l'application π est bijective. Dans ce cas, l'application φ est la composée de la réciproque π^{-1}, de l'inclusion $\Gamma \hookrightarrow V \times W$ et de la projectif $V \times W \longrightarrow\!\!\!\!\rightarrow W$ de telle sorte que le diagramme suivant commute.

$$\begin{array}{ccc} \Gamma & \hookrightarrow & V \times W \\ \downarrow{\scriptstyle \pi} & & \downarrow \\ V & \xrightarrow{\varphi} & W \end{array}$$

En particulier, si π est un isomorphes d'ensemble algébriques, alors φ est polynomiale comme la composée d'applications polynomiales. Réciproquement, on suppose que l'application φ est polynomiale dont les composantes sont induites pour des polynômes $F_1, \ldots, F_m \in k[X_1, \ldots, X_n]$. Alors Γ est algébrique puisque

$$\Gamma = (V \times W) \cap \mathrm{V}(X_{n+1} - F_1, \ldots, X_{n+m} - F_m).$$

Les composantes de l'application π^{-1} sont induites par les polynômes X_1, …, X_n, F_1, …, F_m, donc elle est polynomiale. Finalement, l'application π est un isomorphisme ce qui conclut la preuve. □

2.4 Topologie de Zariski

Définition 2.12. La *topologie de Zariski* sur un ensemble algébrique V est la topologie pour laquelle les fermés sont les sous-ensembles algébriques de V. L'adhérence d'une partie $A \subset V$ pour cette topologie est appelée la *fermeture algébrique* de A dans V.

Dans la suite, on considérera toujours la topologie de Zariski. Ainsi une fonction continue, par exemple, sera continue pour les topologies de Zariski.

Proposition 2.13. Soient $V \subset \mathbb{A}^n(k)$ et $W \subset \mathbb{A}^m(k)$ deux sous-ensembles algébriques. Alors les projections $V \times W \to V$ et $V \times W \to W$ sont ouvertes.

Preuve Par symétrie, il suffit de la montrer pour la première projection $p\colon V\times W \to V$. Remarquons qu'on a $V \times W \subset \mathbb{A}^{n+m}(k)$. Pour $Q \coloneqq (b_1, \dots, b_m) \in \mathbb{A}^m(k)$ et $F \in k[X_1, \dots, X_{n+m}]$, on pose

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

Soit $U \subset V \times W$ un ouvert. Son complémentaire Z dans $V \times W$ est un fermé, donc il existe une partie $S \subset k[X_1, \dots, X_{n+m}]$ telle que $Z = \mathrm{V}(S)$. Montrons que le complémentaire de $p(U)$ dans W est un sous-ensemble algébrique ce qui terminera la preuve. Pour tout point $P \in V$, on a

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

Ainsi le complémentaire de $p(U)$ dans W est l'ensemble algébrique $V \cap \mathrm{V}(T)$ où l'on a définie T comme l'ensemble des polynômes $F_Q \in k[X_1, \dots, X_n]$ avec $F \in S$ et $Q \in W$. □

Corollaire 2.14. Si $n \geqslant 1$, alors tout ouvert non vide de $\mathbb{A}^n(k)$ est infini.

Preuve Il suffit de procéder par récurrence : on utilise la proposition précédente et le fait que les ensembles algébriques de $\mathbb{A}^1(k)$ sont finis ou $\mathbb{A}^1(k)$. □

Lemme 2.15. On suppose que le corps k est algébriquement clos. Soient $H \subset \mathbb{A}^n(k)$ une hypersurface, $p\colon \mathbb{A}^n(k) \to \mathbb{A}^{n-1}(k)$ la projection sur les $n-1$ premières coordonnées et $L \subset \mathbb{A}^n(k)$ le sous-ensemble algébrique d'équation $X_n = 0$. Alors on se trouvé dans l'un des deux cas suivant :

- soit il existe une hypersurface $H_1 \subset \mathbb{A}^{n-1}(k)$ telle que $H = H_1 \times L$;
- soit l'image $p(H)$ contient un ouvert non vide de $\mathbb{A}^{n-1}(k)$.

Preuve On peut écrire $H = \mathrm{V}(F)$ pour un certain polynôme

$$F \coloneqq F_d X_n^d + \cdots + F_0 \in k[X_1, \dots, X_{n-1}][X_n].$$

tel que $F_d \neq 0$. Posons $H_1 \coloneqq \mathrm{V}(F_d) \subset \mathbb{A}^{n-1}(k)$. Si $d = 0$, alors $F = F_d \in k[X_1, \dots, X_{n-1}]$ et il vient $H = H_1 \times L$. On suppose désormais $d > 0$. Le complémentaire U de H_1 dans $\mathbb{A}^{n-1}(k)$ est un ouvert et il n'est pas vide car sinon on aurait $\mathrm{V}(F_d) = \mathbb{A}^{n-1}(k)$ ce qui impliquerait $F_d = 0$. Pour conclure, il suffit donc de montrer l'inclusion $U \subset p(H)$. Soit $(a_1, \dots, a_{n-1}) \in U$ un point de U. Alors $F_d(a_1, \dots, a_{n-1}) \neq 0$, donc le polynôme $F(a_1, \dots, a_{n-1}, T) \in k[T]$ est de degré $d > 0$. Comme le corps k est algébriquement clos, il admet une racine $a_n \in k$. Ceci donne $(a_1, \dots, a_n) \in H$, donc $(a_1, \dots, a_{n-1}) \in p(H)$. Ceci conclut. □

Théorème 2.16. On suppose que le corps k est algébriquement clos. Soit $H \subset \mathbb{A}^n(k)$ une hypersurface. Alors ce sous-ensemble algébrique H est non vide si $n \geqslant 1$ et infini si $n \geqslant 2$.

Preuve On procède par récurrence et on utilise le lemme et le corollaire précédents. □

Proposition 2.17. On suppose que le corps k est algébriquement clos. Soient $p\colon \mathbb{A}^n(k) \twoheadrightarrow \mathbb{A}^{n-1}(k)$ la projection sur les $n-1$ premières coordonnées. Soient $F, G \in k[X_1, \dots, X_n]$ deux polynômes de coefficients dominants F_d et G_e et de résultant R en X_n. Si $P \notin \mathrm{V}(F_d, G_e)$, alors

$$P \in \mathrm{V}(R) \iff P \in p(\mathrm{V}(F, G)).$$

Preuve On pose

$$\begin{aligned} F_P &\coloneqq F(P, X) & G_P &\coloneqq G(P, X), \\ f_d &\coloneqq F_d(P) & g_e &\coloneqq G_e(P), & r &\coloneqq R(P). \end{aligned}$$

Alors

$$P \in \mathrm{V}(R) \iff r = 0 \qquad \text{et} \qquad P \in p(\mathrm{V}(F, G)) \iff f_d = g_e = 0.$$

Par symétrie, on peut supposer $f_d \neq 0$. En notant $e_P \coloneqq \deg G_p$, on trouve $r = f_d^{e-e_P} \operatorname{Res}(F_P, G_P)$. Par conséquent, on a $r = 0$ si et seulement si les polynômes F_P et G_P ne sont pas premiers entre eux. Puisque k est algébriquement clos, cela signifie que ces deux polynômes possèdent une racine commune $a \in k$, *i. e.* un élément $a \in k$ vérifiant $F(P, a) = G(P, a) = 0$, *i. e.* $P \in p(\mathrm{V}(F, G))$. Ceci conclut notre équivalence. □

2.5 Ensembles algébriques irréductibles

Définition 2.18. Un espace topologique est *irréductible* s'il est non vide et possède l'une des propriétés équivalentes suivantes :

– on ne peut pas l'écrire comme une union de deux fermés propres ;
– tout ouvert non vide est dense.

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

▷ Exemples. L'ensemble algébrique $\mathrm{V}(XY) \subset \mathbb{A}^2(k)$ n'est pas irréductible, mais l'ensemble algébrique $\mathrm{V}(XY-1) \subset \mathbb{A}^2(k)$ est irréductible.

◇ Remarques. – L'image d'un ensemble algébrique irréductible par une application polynomiale est irréductible. De même pour l'image réciproque par un isomorphisme.
– Soit $\varphi\colon V \to W$ une application polynomiale. Alors son graphe $\Gamma \subset V \times W$ est irréductible si et seulement si l'ensemble algébrique V l'est.

Proposition 2.19. Soient V et W deux ensembles algébriques irréductibles. Alors leur produit $V \times W$ est irréductible.

Preuve Cela revient à montrer que, pour tous ouverts U_1 et U_2 de $V \times W$, on a $U_1 \cap U_2 \neq \emptyset$. On note $p\colon V \times W \to V$ la première projection. Alors $p(U_i) \neq \emptyset$ pour $i = 1, 2$. La proposition 2.13 nous assure que les images $p(U_i)$ sont ouvertes. Puisque V est irréductible, l'intersection $p(U_1) \cap p(U_2)$ n'est pas vide. Soit $P \in p(U_1) \cap p(U_2)$. Quitte à remplacer l'ouvert U_i par la partie $U_i \cap (\{P\} \times W)$, on peut supposer $V = \{P\}$. Par symétrique, on peut faire la même chose pour Q et le résultat devient trivial. □

Corollaire 2.20. Un sous-espace affine $E \subset \mathbb{A}^n(k)$ est irréductible.

Preuve L'espace E est isomorphe à produit fini de copies de l'espace $\mathbb{A}^1(k)$. Avec la proposition précédente, on peut donc supposer $E = \mathbb{A}^1(k)$ et le résultat est immédiat. □

Chapitre 3

Anneaux

3.1 Rappels et nouvelles définitions

Définition 3.1. Un anneau est *réduit* si son neutre 0 est son seul élément nilpotent. Un idéal I d'un anneau A est *radiciel* s'il est égal à son *radical*

$$\sqrt{I} \coloneqq \{f \in A \mid \exists n \in \mathbf{N}, f^n \in I\}.$$

◇ Remarque. Le radical d'un idéal est le plus petit idéal radiciel contenant dans cet idéal.

Définition 3.2. Les idéaux d'un anneau A d'une famille $(I_\lambda)_{\lambda\in\Lambda}$ sont *étrangers* si

$$\sum_{\lambda\in\Lambda} I_\lambda = A.$$

Théorème 3.3 *(des restes chinois).* Soient $I_1, \ldots, I_k$ des idéaux d'un anneau A qui sont étrangers deux à deux. Alors

$$I \coloneqq \prod_{k=1}^{n} = \bigcap_{k=1}^{n} I_k$$

et il existe un isomorphisme canonique $A/I \simeq \prod_{k=1}^{n} A/I_k$ qui fait correspond une classe modulo I a la famille des classes modulo I_k.

Preuve En raisonnant par récurrence, il suffit de considérer le cas $n = 2$. Comme I_1 et I_2 sont étrangers, on peut trouver deux éléments $e_1 \in I_1$ et $e_2 \in I_2$ tels que $e_1 + e_2 = 1$. Montrons la surjectivité de l'application considérée. Pour tous éléments $f_1, f_2 \in E$, en notant $f \coloneqq f_1e_2 + f_2e_1$, on a $f \equiv f_1 \mod I_1$ et $f \equiv f_2 \mod I_2$ ce qui montre la surjectivité. Montrons l'injectivité. Soit $f \in A$ un élément tel que $f \equiv 0 \mod I_1$ et $f \equiv 0 \mod I_2$. Alors $f \in I_1 \cap I_2$, donc $f = fe_2 + fe_1 \in I_1I_2 = I$, donc $f \equiv 0 \mod I$ ce qui montre l'injectivité. □

Corollaire 3.4. Soient $I_1, \ldots, I_k$ des idéaux d'un anneau A qui sont étrangers deux à deux et I un idéal de A contenant $\prod_{k=1}^{n} I_k$. Alors

$$A/I \simeq \prod_{k=1}^{n} A/(I + I_k).$$

Preuve Il suffit d'appliquer le théorème des restes chinois à la famille d'idéaux $(I + I_k)_{k\in[\![1,n]\!]}$ et d'utiliser le fait

$$I \subset \prod_{k=1}^{n}(I + I_k) = \bigcap_{k=1}^{n}(I + I_k) \subset I + \prod_{k=1}^{n} I_k \subset I.$$ □

3.2 Anneaux locaux

Proposition 3.5. Soient A un anneau et $S \subset A$ une partie quelconque de ce dernier. Alors il existe un anneau $S^{-1}A$ et un morphisme d'anneaux $A \to S^{-1}A$ ayant la propriété universelle :

> *tout morphisme d'anneaux $u\colon A \to B$ tel que $u(S) \subset B^\times$ se prolonge en un unique morphisme $u'\colon S^{-1}A \to B$.*

Preuve En utilisant successivement la propriété universelle de l'anneau des polynômes à une

infinité de variables et celle de l'anneau quotient, l'anneau

$$A[\{X_s\}_{s\in S}]/\langle sX_s - 1\rangle_{s\in S}$$

convient. □

◇ Remarques. – On peut montrer que l'anneau construit $S^{-1}A$ ne dépend que de l'ensemble $\overline{S}$ des produits d'éléments de S. On peut donc supposer que la partie S est multiplicative.
– Pour voir un peu mieux les choses, l'anneau localisé est juste isomorphe au quotient

$$(A \times \overline{S})/\mathscr{R}$$

où la relation d'équivalence $\mathscr{R}$ est définie par la relation

$$(f,s)\,\mathscr{R}\,(g,t) \quad\Longleftrightarrow\quad \exists u \in \overline{S},\quad u(tf - sg) = 0$$

et où les lois sont induites par les lois sur A

$$(f,s) + (g,t) = (tf, st) \quad\text{et}\quad (f,s) \times (g,t) = (fg, st).$$

et l'application $A \to S^{-1}A$ est induit par l'application $f \longmapsto (f,1)$.
– Pour un anneau A, on notera $\operatorname{Frac} A \coloneqq (A \setminus \{0\})^{-1}A$ son corps des fractions. Par exemple, le corps des fractions de $\mathbf{Z}$ est $\mathbf{Q}$ et celui de $k[X]$ est $k(X)$.

Définition 3.6. Un anneau A est *local* s'il satisfait les propriétés équivalentes suivantes :
– il possède un unique idéal maximal $\mathfrak{m}_A$;
– la partie $A \setminus A^\times$ est un idéal de A.

Dans le cas, le *corps résiduel* de l'anneau A est le quotient

$$k(A) \coloneqq A/\mathfrak{m}_A.$$

Un morphisme d'anneaux locaux $\varphi\colon A \to B$ est local si $\varphi(\mathfrak{m}_A) \subset \mathfrak{m}_B$.

Preuve Justifions l'équivalence des deux propriétés. On suppose d'abord qu'il possède un unique idéal maximal $\mathfrak{m}_A$. Soient $a \in A \setminus A^\times$ et $b \in A$. Alors $ab \in A \setminus A^\times$ car sinon il existerait $c \in A$ tel que $abc = 1$, donc l'élément a serait inversible ce qui est impossible. Soient $a, b \in A \setminus A^\times$. Alors $a + b \in A \setminus A^\times$ car sinon il existerait $c \in A$ tel que $c(a+b) = 1$, donc $ca + cb = 1$ impliquant $\langle a\rangle + \langle b\rangle = A \subset \mathfrak{m}_A$ car $\langle a\rangle \subset \mathfrak{m}_A$ et $\langle b\rangle \subset \mathfrak{m}_A$ car $a, b \notin A^\times$ ce qui est impossible. Ceci montre que la partie $A \setminus A^\times$ est un idéal.

Réciproquement, on suppose que la partie $A \setminus A^\times$ est un idéal. C'est un idéal propre, donc le théorème de Krull assure qu'il existe un idéal $\mathfrak{m}$ de A tel que $\mathfrak{m} \supset A \setminus A^\times$. L'inclusion réciproque est évidente puisque, si $\mathfrak{m}$ contient un inversible, alors $\mathfrak{m} = A$. Ainsi l'idéal $\mathfrak{m}$ ne contient pas d'inversible ce qui montre $\mathfrak{m} = A \setminus A^\times$. Par le même argument, c'est l'unique idéal maximal. □

◇ Remarques. – Soit φ un idéal premier de A. Alors l'anneau $A_\varphi \coloneqq (A \setminus \varphi)^{-1}A$ est local d'idéal maximal $(A \setminus \varphi)^{-1}\varphi$. Son corps résiduel est le corps des fractions de A/φ.
– Soient $u\colon A \to B$ un morphisme d'anneaux et $\mathfrak{q}$ un idéal premier de B. Alors $\varphi \coloneqq u^{-1}(\mathfrak{q})$ est un idéal premier de A et le morphisme u se prolonge en un unique morphisme local $u_\mathfrak{q}\colon A_\varphi \to B_\mathfrak{q}$.

Définition 3.7. Soit k un corps. Une *valuation discrète* sur k est une application surjective

$$v\colon k \to \mathbf{Z} \cup \{\infty\}$$

vérifiant les trois propriétés suivantes :
– pour tout $f \in k$, on a $v(f) = \infty \Leftrightarrow f = 0$;
– pour tous $f, g \in k$, on a $v(fg) = v(f) + v(g)$;
– pour tous $f, g \in k$, on a $v(f+g) \geqslant \min(v(f), v(g))$.

Un élément de k est *uniformisant* si sa valuation est égale à 1. L'*anneau de valuation* de k est l'anneau

$$\{f \in k \mid v(f) \geqslant 0\}.$$

▷ Exemples. – Soit $x \in \mathbf{C}$. La fonction qui a une fonction méromorphe non nulle f sur $\mathbf{C}$ associe l'ordre de x pour f est une valuation.

– La valuation p-adique est une valuation sur $\mathbf{Q}$.

Exercice 3.1. Montrons qu'un anneau A de valuation discrète v est un anneau local d'idéal maximal $\mathfrak{m}_A = \{f \in A \mid v(f) > 0\}$.

Proposition 3.8. Soit A un anneau. Alors les propositions suivantes sont équivalentes :

(i) l'anneau A admet une valuation discrète ;

(ii) il est factoriel et admet, à multiplication près par un inversible, un unique élément irréductible ;

(iii) il est local et principal ;

(iv) il est local, intègre et noethérien et $\dim_{k(A)} \mathfrak{m}_A/\mathfrak{m}_A^2 = 1$.

Preuve Remarquons d'abord que, dans les quatre cas, l'anneau est local et intègre. De plus, on peut se donner un élément $\ell \in A$ qui vérifie, selon les cas, une condition :

(i) $v(\ell) = 1$;

(ii) ℓ est irréductible ;

(iii) $\mathfrak{m}_A = \langle \ell \rangle$;

(iv) $\overline{\ell} \neq 0$ où $\overline{\ell}$ est la classe de $\ell \in \mathfrak{m}_A$ modulo $\mathfrak{m}_A^2$.

• *(i) ⇒ (ii).* Soit $f \in A$ un élément s'écrivant sous la forme $f = u\ell^n$ avec $a \in A^\times$ et $n \in \mathbf{N}$. Montrons que cette écriture est unique. Alors $v(f) = v(u) + nv(\ell)$. Comme $v(\ell) = 1$ et $v(u) = 0$, on obtient $n = v(f)$ puis $u = f(\ell^n)^{-1}$ ce qui montre l'unicité. Réciproquement, soit $f \in A \setminus \{0\}$ un élément de valuation $n \in \mathbf{N}$. On pose $u \coloneqq f(\ell^n)^{-1} \in A$. Alors $v(u) = 0$, donc $u \in A \setminus \mathfrak{m}_A = A^\times$.

• *(ii) ⇒ (iii).* Il suffit de remarquer que les seuls idéaux de A sont les idéaux $\langle \ell^n \rangle$ avec $n \in \mathbf{N}$ d'après notre hypothèse.

• *(iii) ⇒ (iv).* Un anneau principal est bien noethérien. Vérifions que $\overline{\ell}$ est une base de $\mathfrak{m}_A/\mathfrak{m}_A^2$. Comme $\ell \notin \mathfrak{m}_A^2$, on a $\overline{\ell} \neq 0$ et, si $f \in A$, on peut l'écrire sous la forme $f = g\ell$ avec $g \in A$ et on a $\overline{f} = \overline{g}\overline{\ell}$. Cela montre la liberté et le caractère générateur du vecteur $\overline{\ell}$.

• *(iv) ⇒ (i).* En effectuant une récurrence, on vérifie que, pour tout entier $n \in \mathbf{N}$, le $k(A)$-espace vectoriel $\mathfrak{m}_A^n/\mathfrak{m}_A^{n+1}$ est engendré par la classe $\overline{\ell^n}$, c'est-à-dire $\mathfrak{m}_A^n = \langle \ell^n \rangle + \mathfrak{m}_A^{n+1}$. En effet, le cas initial $n = 1$ est donné par notre hypothèse. Si c'est vrai pour un rang $n \in \mathbf{N}$, on obtient alors

$$\mathfrak{m}_A^{n+1} = \mathfrak{m}_A^n \mathfrak{m}_A = (\langle \ell^n \rangle + \mathfrak{m}_A^{n+1})(\langle \ell \rangle + \mathfrak{m}_A^{n+2}) = \langle \ell^{n+1} \rangle + \mathfrak{m}_A^{n+1}.$$

Ensuite, on voit que cette classe $\overline{\ell^n}$ est non nulle car sinon on aurait $\mathfrak{m}_A^n = \mathfrak{m}_A^{n+1}$ ce qui contredirait le théorème de Krull (voir ci-dessous).

On construit maintenant une valuation sur A : pour un élément $f \in A$, on pose

$$v(f) \coloneqq \sup \{n \in \mathbf{N} \mid f \in \mathfrak{m}_A^n\} \in \mathbf{N} \cup \{\infty\}.$$

Montrons qu'il s'agit bien d'une valuation. La première condition résulte du théorème de Krull. La deuxième condition est réalisée puisque l'application

$$\mathfrak{m}_A^n/\mathfrak{m}_A^{n+1} \times \mathfrak{m}_A^m/\mathfrak{m}_A^{m+1} \to \mathfrak{m}_A^{m+n}/\mathfrak{m}_A^{m+n+1}$$

induit par la multiplication est bilinéaire et intègre : cela vient du fait que ces trois espaces vectoriels sont des droites. La troisième condition vient du fait que, si $n \leqslant m$, on a $\mathfrak{m}_A^n + \mathfrak{m}_A^m = \mathfrak{m}_A^n$. En effet, cette application v est bien surjective puisque, pour tout $n \in \mathbf{N}$, on a $v(\ell^n) = n$. On la prolonge naturellement en une application sur le corps $K \coloneqq \operatorname{Frac} A$ en posant $v(f/g) = v(f) - v(g)$ pour tous éléments $f, g \in A$ avec $g \neq 0$. Cette application est bien définie et donne une valuation sur K ce qui termine la preuve. □

3.3 Anneaux noethériens

Définition 3.9. Une R-algèbre A est de *type fini* si elle est isomorphe à un quotient d'un anneau de polynôme sur R. Elle est finie s'il existe des éléments $f_1, \ldots, f_r \in A$ tels que tout élément $f \in A$ puisse s'écrire sous la forme $f = \sum_{i=1}^r a_i f_i$ avec $a_1, \ldots, a_r \in R$. Un morphisme d'anneaux $u \colon A \to B$ est de type fini (respectivement fini) s'il munit l'anneau B d'une structure de A-algèbre de type fini (respectivement fini).

LEMME 3.10. Soient A une R-algèbre finie et $f \in A$. Alors il existe $a_1, \dots, a_r \in R$ tels que

$$f^r + a_1 f^{r-1} + \cdots + a_{r-1} f + a_r = 0.$$

On dit alors que l'élément f est *entier* sur R.

Preuve Par définition, il existe des éléments $g_1, \dots, g_r \in A$ tels que tout élément $g \in A$ puisse s'écrire sous la forme $g = \sum_{j=1}^r b_j g_j$ avec $b_1, \dots, b_r \in R$. En particulier, pour tout $i \in [\![1, r]\!]$, on peut écrire $f g_i = \sum_{j=1}^r a_{i,j} g_j$. On peut aussi écrire

$$d \coloneqq \det(f\delta_{i,j} - a_{i,j})_{1 \leqslant i,j \leqslant r} = f^r + a_1 f^{r-1} + \cdots + a_{r-1} f + a_r.$$

Par ailleurs, la formule de Laplace nous assure $d g_i = 0$ pour tout $i \in [\![1, r]\!]$, donc $dg = 0$ pour tout $g \in A$. En particulier, on a $d = 0$. □

DÉFINITION 3.11. Un anneau est *noethérien* s'il satisfait les propriétés équivalentes suivantes :

- toute famille non vide d'idéaux contient un élément maximal ;
- toute suite croissante d'idéaux est stationnaire ;
- tout idéal est de type fini.

THÉORÈME 3.12 *(de la base de Noether).* Toute algèbre de type fini sur un anneau noethérien est un anneau noethérien.

Preuve Soit R un anneau noethérien. Avec la définition d'une R-algèbre de type fini, il suffit de montrer que l'anneau $R[X]$ est noethérien.

Pour $I \subset R[X]$ et $d \in \mathbf{N}$, on note $c_d(I) \subset R$ l'ensemble des coefficients dominants des polynômes de degré d de I. Soient I et J deux idéaux de $R[X]$. Alors la suite $(c_d(I))_{d \in \mathbf{N}}$ est croissante et l'on dispose de l'équivalence

$$I = J \quad \Longleftrightarrow \quad \forall d \in \mathbf{N},\ c_d(I) = c_d(J). \tag{$*$}$$

qui se démontre par récurrence sur le degré.

Montrons maintenant ce qu'on veut. Soit $(I_k)_{k \in \mathbf{N}}$ une suite croissante d'idéaux de $R[X]$. Alors la famille $(c_d(I_k))_{d,k \in \mathbf{N}}$ est une famille d'idéaux de l'anneau noethérien R. On peut alors trouver deux entiers $D, K \in \mathbf{N}$ tels que

$$c_D(I_K) = c_d(I_k), \quad k \geqslant K,\ d \geqslant D.$$

Par ailleurs, pour tout entier $i \in \mathbf{N}$, la suite $(c_i(I_k))_{k \in \mathbf{N}}$ étant constituée d'idéaux de R, il existe un entier $N_i \in \mathbf{N}$ tel que

$$c_i(I_{N_i}) = c_i(I_k), \quad k \geqslant N_i.$$

On pose $N \coloneqq \max(K, N_0, \dots, N_D)$. Alors pour tous $k \geqslant N$ et $i \in \mathbf{N}$, on a $c_i(I_N) = c_i(I_k)$. Avec l'équivalence $(*)$, on trouve finalement $I_N = I_k$ dès que $k \geqslant N$. Donc l'anneau $R[X]$ est noethérien et la preuve est conclue. □

LEMME 3.13 *(Artin-Rees).* Soient A un anneau noethérien et I et J deux idéaux de A. Alors il existe un entier $n \in \mathbf{N}$ tel que

$$\forall k \in \mathbf{N}, \quad I^{n+k} \cap J = I^n (I^k \cap J).$$

Preuve On considère respectivement le sous-anneau et l'idéal de $A[X]$

$$A_X \coloneqq \sum_{n \in \mathbf{N}} I^n X^n \subset A[X] \quad \text{et} \quad J_X \coloneqq \sum_{n \in \mathbf{N}} J X^n \subset A[X].$$

Comme A est noethérien, l'idéal I est de type fini, donc la A-algèbre A_X est de type fini. D'après le théorème de la base de Noether, cette A-algèbre A_X est un anneau noethérien. Ainsi l'idéal de A_X

$$A_X \cap J_X = \sum_{n \in \mathbf{N}} (I^n \cap J) X^n$$

est une A_X-algèbre de type fini. On en choisit des générateurs $F_1, \dots, F_m \in A[X]$. Maintenant, en notant $k \coloneqq \max(\deg F_1, \dots, \deg F_k)$, on a immédiatement

$$F_i \in \sum_{\ell=0}^{k} (I^\ell \cap J) X^\ell, \quad i \in [\![1, m]\!]$$

et on en déduit

$$A_X \cap J_X = \sum_{i=1}^{m} A_X F_i = \sum_{n\in\mathbf{N}} I^n X^n \sum_{\ell=0}^{k} (I^\ell \cap J) X^\ell = \sum_{n\in\mathbf{N}} \sum_{\ell=0}^{k} I^n (I^\ell \cap J) X^{n+\ell}$$

si bien que

$$I^{n+k} \cap J = \sum_{\ell=0}^{k} I^{n+k-\ell}(I_k \cap J) = \sum_{n\in\mathbf{N}} I^n (I^k \cap J). \qquad \square$$

LEMME 3.14 *(Nakayama).* Soient A un anneau local noethérien et J un idéal de A. On suppose $\mathfrak{m}_A J = J$. Alors $J = 0$

Preuve Soient $g_1, \dots, g_r \in I$ des générateurs de J. Pour tout $i \in [\![1, r]\!]$, on peut écrire

$$g_i = \sum f_{i,j} g_j \quad \text{avec} \quad f_{i,j} \in \mathfrak{m}_A.$$

Alors $\det(\delta_{i,j} - f_{i,j})_{1\leqslant i,j\leqslant r} = 1 - f$ avec $f \in \mathfrak{m}_A$. Avec la formule de Laplace, on obtient $(1-f)g_i = 0$ pour tout $i \in [\![1, r]\!]$. Comme $f \in \mathfrak{m}_A$, on a $1 - f \in A^\times$ ce qui force $g_i = 0$ pour tout $i \in [\![1, r]\!]$. En conclusion, on a $J = 0$. $\square$

THÉORÈME 3.15 *(d'intersection de Krull).* Soit A un anneau local noethérien. Alors

$$\bigcap_{n\in\mathbf{N}} \mathfrak{m}_A^n = \{0\}.$$

Preuve On applique le lemme d'Artin-Rees pour les idéaux $I \coloneqq \mathfrak{m}_A$ et $J \coloneqq \bigcap_{n\in\mathbf{N}} \mathfrak{m}_A^n$. On obtient

$$J = \mathfrak{m}_A^{k+1} \cap J = \mathfrak{m}_A(\mathfrak{m}_A^k \cap J) = \mathfrak{m}_A J$$

et on utilise le lemme de Nakayama. $\square$

LEMME 3.16 *(de normalisation de Noether).* Soient $F \in R[X_0, \dots, X_d]$ et $e > \max_{i\in[\![0,d]\!]} \deg_{X_i}(F)$. On considère l'application $\Phi\colon R[X_0, \dots, X_d] \to R[X_0, \dots, X_d]$ telle que

$$\Phi(X_0) = X_0 \quad \text{et} \quad \Phi(X_i) = X_i + X_0^{e^i}, \quad i \geqslant 0.$$

Alors le coefficient dominants de $\Phi(F)$ en X_0 est constant.

Preuve Pour un monôme $M \coloneqq X_0^{n_0} \cdots X_d^{n_d}$ de F, on pose

$$n(M) \coloneqq \sum_{i=0}^{d} n_i e^i \in \mathbf{N}.$$

On remarque que l'application n est injective des monômes de F vers $\mathbf{N}$. Maintenant, pour tout monôme $M \coloneqq X_0^{n_0} \cdots X_d^{n_d}$ de F, la quantité

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

peut s'écrire sous la forme $G + X_0^{n(M)}$ avec $\deg_{X_0} G < n(M)$. On en déduit

$$\deg_{X_0} \Phi(F) = \max_M n(M)$$

ce qui assure la conclusion. $\square$

THÉORÈME 3.17 *(de normalisation de Noether).* Soit A une k-algèbre de type fini. Alors il existe une unique morphisme de k-algèbres injectif et fini $\iota\colon k[X_1, \dots, X_d] \hookrightarrow A$.

Preuve Par définition, il existe une morphisme de k-algèbres surjectif $k[X_1, \dots, X_d] \to A$. Il est donc fini. S'il est injectif, la preuve est terminée. Mais on peut ne pas avoir de chance. Dans ce cas, on peut trouver un élément non nul F dans son noyau. Grâce au lemme de normalisation, on peut supposer que le coefficient dominant de F en X_d est constant. Alors le morphisme composé

$$k[X_1, \dots, X_{d-1}] \to k[X_1, \dots, X_d]/\langle F\rangle \to A$$

est fini et on peut alors procéder par récurrence sur l'entier $d \in \mathbf{N}$. $\square$

THÉORÈME 3.18 *(des zéros de Hilbert, version algébrique).* Soit K/k une extension de corps, *i. e.* une k-algèbre K qui est un corps. On suppose qu'elle est de type fini. Alors elle est finie.

Preuve Avec le théorème de normalisation, il existe une morphisme d'anneaux injectif et fini

$$\iota\colon k[X_1,\dots,X_d] \hookrightarrow K.$$

Soit $F \in k[X_1,\dots,X_d]$ un polynôme non nul. Comme ι est injective, l'élément $\iota(F)$ n'est pas nul et il possède donc un inverse $g \in K$. Comme K est fini sur k, elle est finie sur $k[X_1,\dots,X_d]$. Le lemme 3.10 nous assure alors l'existence d'éléments $F_1,\dots,F_r \in k[X_1,\dots,X_d]$ tels que

$$g^r + F_1 g^{r-1} + \cdots + F_{r-1} g + F_r = 0.$$

En multipliant par l'élément $\iota(F)^{r-1}$ cette dernière égalité, on obtient

$$g^r \iota(F)^{r-1} + F_1 g^{r-1} \iota(F)^{r-1} + \cdots + F_{r-1} g \iota(F)^{r-1} + F_r \iota(F)^{r-1} = 0,$$

donc

$$g = -(F_1 + \cdots + F_{r-1} F^{r-2} + F_r F^{r-1}) \in k[X_1,\dots,X_d].$$

Ainsi l'élément F est inversible dans $k[X_1,\dots,X_d]$, donc il est constant. Cela montre que $d = 0$. On a donc obtenu un morphisme d'anneaux injectif et fini $\iota\colon k \longrightarrow K$. La k-algèbre k étant finie, la k-algèbre K est finie. □

Chapitre 4

Anneaux de fonctions

Dans tout le chapitre, on considère un corps infini k et un entier naturel $n \in \mathbf{N}^*$.

4.1 Idéal de définition

DÉFINITION 4.1. L'*idéal de définition* d'une partie $A \subset \mathbb{A}^n(k)$ est l'ensemble

$$\mathrm{I}(A) \coloneqq \{F \in k[X_1, \dots, X_n] \mid \forall P \in A,\ F(P) = 0\}.$$

◇ REMARQUE. Il s'agit bien d'un idéal de l'anneau $k[X_1, \dots, X_n]$ et il est radiciel.

PROPOSITION 4.2. 1. On a $\mathrm{I}(\emptyset) = k[X_1, \dots, X_n]$ et $\mathrm{I}(\mathbb{A}^n(k)) = \{0\}$.
2. Soit $(A_\alpha)_{\alpha\in\Lambda}$ une famille de parties de $\mathbb{A}^n(k)$. Alors

$$\bigcap_{\alpha\in\Lambda} \mathrm{I}(A_\alpha) = \mathrm{I}\Big(\bigcup_{\alpha\in\Lambda} A_\alpha\Big).$$

3. Soient $A, B \subset \mathbb{A}^n(k)$ deux parties telles que $A \subset B$. Alors $\mathrm{I}(B) \subset \mathrm{I}(A)$.
4. Soient $S \subset k[X_1, \dots, X_n]$ et $A \subset \mathbb{A}^n(k)$ deux parties. Alors $S \subset \mathrm{I}(\mathrm{V}(S))$ et $A \subset \mathrm{V}(\mathrm{I}(A))$.

◇ REMARQUES. – Pour tout point $P \in \mathbb{A}^n(k)$, l'idéal $\mathrm{I}(P)$ est maximal.
– Une partie $V \subset \mathbb{A}^n(k)$ est algébrique si et seulement si $V = \mathrm{V}(\mathrm{I}(V))$.
– Deux ensembles algébriques de $\mathbb{A}^n(k)$ sont égaux si et seulement s'ils le même idéal de définition.
– La fermeture algébrique d'une partie $A \subset \mathbb{A}^n(k)$ est $V \coloneqq \mathrm{V}(\mathrm{I}(A))$ et on a $\mathrm{I}(A) = \mathrm{I}(V)$.

PROPOSITION 4.3. Soient $F_1, \dots, F_r \in k[X_1, \dots, X_n]$ des polynômes de degré au plus un. En notant $V \coloneqq \mathrm{V}(F_1, \dots, F_r)$, on a $\mathrm{I}(V) = \langle F_1, \dots, F_r\rangle$.

Preuve On peut déjà supposer que les formes affines F_i sont linéairement indépendantes. De plus, quitte à faire un changement de variables, on peut alors supposer

$$F_1 = X_{m+1}, \quad \dots, \quad F_r = X_n.$$

Alors $V = \mathbb{A}^m(k)$. Dans ce cas, on obtient alors

$$\begin{aligned} F \in \mathrm{I}(V) &\iff \forall a_1, \dots, a_m \in k, \quad F(a_1, \dots, a_m, 0, \dots, 0) = 0 \\ &\iff F(X_1, \dots, X_m, 0, \dots, 0) \\ &\iff F \in \langle X_{m+1}, \dots, X_n\rangle \end{aligned}$$

ce qui conclut. □

4.2 Anneau de coordonnées

Dans cette section, on considère un sous-ensemble algébrique $V \subset \mathbb{A}^n(k)$.

PROPOSITION 4.4. L'application de restriction

$$\pi_V : \left| \begin{aligned} k[X_1, \dots, X_n] &\longrightarrow k^V, \\ F &\longmapsto F|_V \end{aligned} \right.$$

induit un isomorphisme de k-algèbre

$$k[X_1, \dots, X_n]/\operatorname{I}(V) \simeq \operatorname{Im} \pi_V.$$

Preuve L'application π_V est bien un morphisme de k-algèbres de noyau $\operatorname{I}(V)$. On obtient l'isomorphisme en la passant au quotient. □

▷ Exemples. – Considérons la parabole $C \coloneqq \operatorname{V}(Y - X^2)$. Alors $\operatorname{I}(C) = \langle Y - X^2 \rangle$. Avec la proposition précédente et une division euclidienne, on obtient un isomorphisme composé

$$\mathbf{R}[C] \simeq \mathbf{R}[X, Y]/\langle Y - X^2 \rangle \simeq \mathbf{R}[X].$$

Définition 4.5. L'*anneau des coordonnées* de V est l'image $\operatorname{Im} \pi_V$, notée $k[V]$.

On étend la notation $\operatorname{V}(S)$ pour une partie $S \subset k[V]$, c'est-à-dire que l'on pose

$$\operatorname{V}(S) \coloneqq \{P \in V \mid \forall f \in S,\ f(P) = 0\}.$$

Proposition 4.6. Soit $S \subset k[V]$ une partie. Alors le sous-ensemble $\operatorname{V}(S) \subset V$ est algébrique. Plus précisément, soit $\tilde{S} \subset k[X_1, \dots, X_n]$ une partie telle que $\pi_V(\tilde{S}) = S$. Alors $\operatorname{V}(S) = \operatorname{V}(\tilde{S}) \cap V$.

Preuve Pour tout point $P \in \mathbb{A}^n(k)$, il suffit d'écrire la suite d'équivalences

$$\begin{aligned} P \in \operatorname{V}(S) &\iff P \in V \quad \text{et} \quad \forall f \in S,\ f(P) = 0 \\ &\iff P \in V \quad \text{et} \quad \forall F \in \tilde{S},\ \pi_V(F)(P) = 0 \\ &\iff P \in V \quad \text{et} \quad \forall F \in \tilde{S},\ F(P) = 0 \\ &\iff P \in V \cap \operatorname{V}(\tilde{S}). \end{aligned}$$

□

◇ Remarque. Pour une partie $S \subset k[V]$, on peut même montrer l'égalité $\operatorname{V}(S) = \operatorname{V}(\pi_V^{-1}(S)) \cap V$ avec la proposition précédente.

Proposition 4.7. 1. On a $\operatorname{V}(1_V) = \emptyset$ et $\operatorname{V}(0_V) = \emptyset$.
2. Soit $(S_\alpha)_{\alpha \in \Lambda}$ une famille de parties de $k[V]$. Alors

$$\bigcap_{\alpha \in \Lambda} \operatorname{V}(S_\alpha) = \operatorname{V}\Big(\bigcup_{\alpha \in \Lambda} S_\alpha\Big).$$

3. Soient $S, T \in k[V]$ deux parties. Alors $\operatorname{V}(S) \cap \operatorname{V}(T) = \operatorname{V}(ST)$.
4. Si $S \subset T$, alors $\operatorname{V}(T) \subset \operatorname{V}(S)$.

Preuve On va utiliser en masse la proposition précédente.
1. On a $\operatorname{V}(1_V) = \operatorname{V}(1) \cap V = \emptyset$ et $\operatorname{V}(0_V) = \operatorname{V}(0) \cap V = V$.
2. Pour tout indice $\alpha \in \Lambda$, la partie $\tilde{S}_\alpha \coloneqq \pi_V^{-1}(S_\alpha)$ vérifie $\pi_V(\tilde{S}_\alpha) = S_\alpha$. Ces parties $\tilde{S}_\alpha$ satisfont

$$\pi_V\Big(\bigcup_{\alpha \in \Lambda} \tilde{S}_\alpha\Big) = \bigcup_{\alpha \in \Lambda} S_\alpha.$$

Alors on obtient

$$\begin{aligned} \operatorname{V}\Big(\bigcup_{\alpha \in \Lambda} S_\alpha\Big) &= \operatorname{V}\Big(\bigcup_{\alpha \in \Lambda} \tilde{S}_\alpha\Big) \cap V \\ &= \Big(\bigcap_{\alpha \in \Lambda} \operatorname{V}(\tilde{S}_\alpha)\Big) \cap V \\ &= \bigcap_{\alpha \in \Lambda} (\operatorname{V}(\tilde{S}_\alpha) \cap V) \\ &= \bigcap_{\alpha \in \Lambda} \operatorname{V}(S_\alpha). \end{aligned}$$

3. En posant $\tilde{S} \coloneqq \pi_V^{-1}(S)$ et $\tilde{T} \coloneqq \pi_V^{-1}(T)$, on a $\pi_V(\tilde{S}\tilde{T}) = ST$ en on procède comme précédemment.
4. En remarquant l'inclusion $\tilde{S} \subset \tilde{T}$, on obtient bien $\operatorname{V}(T) = \operatorname{V}(\tilde{T}) \cap V \subset \operatorname{V}(\tilde{S}) \cap V = \operatorname{V}(S)$. □

PROPOSITION 4.8. Soit $A \subset V$ une partie. Alors la partie

$$\mathrm{I}_V(A) \coloneqq \{f \in k[V] \mid \forall P \in A,\ f(P) = 0\}$$

est un idéal de $k[V]$. Plus précisément, on a

$$\pi_V^{-1}(\mathrm{I}_V(A)) = \mathrm{I}(A) \quad \text{et} \quad \pi_V(\mathrm{I}(A)) = \mathrm{I}_V(A).$$

Preuve Pour tout polynôme $F \in k[X_1, \dots, X_n]$, on a

$$\begin{aligned} F \in \pi_V^{-1}(\mathrm{I}_V(A)) &\iff F|_V \in \mathrm{I}_V(A) \\ &\iff \forall P \in A,\ F(P) = 0 \\ &\iff F \in \mathrm{I}(A) \end{aligned}$$

ce qui montre l'égalité $\pi_V^{-1}(\mathrm{I}_V(A)) = \mathrm{I}(A)$. La second résulte de la surjectivité du morphisme π_V. □

PROPOSITION 4.9. 1. On a $\mathrm{I}_V(\emptyset) = k[V]$ et $\mathrm{I}_V(V) = \{0_V\}$.
2. Soit $(A_\alpha)_{\alpha\in\Lambda}$ une famille de parties de V. Alors

$$\bigcap_{\alpha\in\Lambda} \mathrm{I}_V(A_\alpha) = \mathrm{I}_V\Big(\bigcup_{\alpha\in\Lambda} A_\alpha\Big).$$

3. Soient $A, B \subset V$ deux parties telles que $A \subset B$. Alors $\mathrm{I}_V(B) \subset \mathrm{I}_V(A)$.
4. Soient $S \subset k[V]$ et $A \subset V$ deux parties. Alors $S \subset \mathrm{I}_V(\mathrm{V}(S))$ et $A \subset \mathrm{V}(\mathrm{I}_V(A))$.

Preuve Comme pour la preuve de la proposition 4.7, on utilise les propositions 4.2 et 4.8. □

◇ REMARQUES. – Pour une partie $A \subset V$, on a $\mathrm{V}(\mathrm{I}_V(A)) = \mathrm{V}(\mathrm{I}(A))$.
– Une partie $W \subset V$ est algébrique si et seulement si $W = \mathrm{V}(\mathrm{I}_V(W))$. Dans ce cas, L'application de restriction induit un isomorphisme

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

– La fermeture algébrique d'une partie $A \subset V$ dans V est $W \coloneqq \mathrm{V}(\mathrm{I}_V(A))$ et on a $\mathrm{I}_V(A) = \mathrm{I}_V(W)$.

4.3 Applications polynomiales et homomorphismes d'anneaux

DÉFINITION 4.10. Soit $\varphi\colon W \to V$ une application polynomiale. On définit l'application

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

◇ REMARQUES. – Si $i\colon W \to V$ est une application d'inclusion, alors $i^*\colon k[V] \to k[W]$ est l'application de restriction $f \longmapsto f|_W$.
– Pour deux applications polynomiales $\varphi\colon W \to V$ et $\psi\colon Z \to W$, on a $(\psi \circ \varphi)^* = \varphi^* \circ \psi^*$.
– Pour une application polynomiale $\varphi\colon W \to V$ et $f \in k[V]$, on a $\varphi^{-1}(\mathrm{V}(f)) = \mathrm{V}(\varphi^*(f))$.

THÉORÈME 4.11. Soient V et W deux sous-ensembles algébriques affines. Alors l'application

$$\left|\begin{array}{l} \mathrm{Hom}(W, V) \longrightarrow \mathrm{Hom}_{k\text{-alg}}(k[V], k[W]), \\ \qquad \varphi \longmapsto \varphi^* \end{array}\right.$$

est une bijection.

Preuve Notons $x_1, \dots, x_n\colon V \to k$ les applications coordonnées sur V. Montrons l'injectivité. Soient $\varphi \in \mathrm{Hom}(W, V)$ et $Q \in W$. Pour tout $i \in [\![1, n]\!]$, remarquons que $\varphi^*(x_i)(Q) = x_i(\varphi(Q))$ de sorte qu'on puisse écrire

$$\varphi(Q) = (\varphi^*(x_1)(Q), \dots, \varphi^*(x_n)(Q)).$$

Ceci implique l'injectivité.

Montrons la surjectivité. Soit $u \in \mathrm{Hom}_{k\text{-alg}}(k[V], k[W])$. Pour tout point $Q \in W$, on pose

$$\varphi(Q) \coloneqq (u(x_1)(Q), \dots, u(x_n)(Q)) \in \mathbb{A}^n(k).$$

Montrons que $u = \varphi^*$. Soit $Q \in W$. Procédons d'abord à deux petites remarques :

– pour tout polynôme $F \in k[X_1, \dots, X_n]$ et toutes applications $g_1, \dots, g_n \colon V \to k$, on a

$$F(g_1(Q), \dots, g_n(Q)) = F(g_1, \dots, g_n)(Q) \ ;$$

– comme u est un morphisme d'algèbres, on a $F(u(x_1), \dots, u(x_n)) = u(F(x_1, \dots, x_n))$.

Établissons d'abord que $\mathrm{Im}\,\varphi \subset V$. Soit $F \in \mathrm{I}(V)$. Avec le second point, on trouve alors

$$F(u(x_1), \dots, u(x_n)) = 0.$$

Avec le premier point, on en déduit

$$F(\varphi(Q)) = F(u(x_1)(Q), \dots, u(x_n)(Q)) = 0.$$

Ceci étant vrai pour tout polynôme $F \in \mathrm{I}(V)$, on obtient $\varphi(Q) \in V$. D'où $\mathrm{Im}\,\varphi \subset V$. Par ailleurs, cette application φ est polynomiale d'après sa construction. Enfin, pour tout $i \in [\![1, n]\!]$, on a

$$u(x_i) = x_i \circ \varphi = \varphi^*(x_i).$$

Comme $k[V]$ est un quotient de $k[X_1, \dots, X_n]$, le morphisme de k-algèbres u est uniquement déterminé par les images $u(x_i)$. D'où $u = \varphi^*$ et cela conclut la surjectivité. □

Corollaire 4.12. Une application polynomiale $\varphi \colon W \to V$ est un isomorphisme si et seulement si l'application φ^* est bijective.

Preuve $\Rightarrow$ On suppose que l'application φ est un isomorphisme. Elle admet un inverse polynomiale ψ. Dans ce cas, l'application φ^* est bien une bijection d'inverse ψ^*.

$\Leftarrow$ On suppose que l'application φ^* est bijective. Alors c'est un isomorphisme de k-algèbres, donc elle admet un inverse u qui est un morphisme de k-algèbres. Par le théorème, on peut trouver une application polynomiale ψ telle que $\psi^* = u$. Cette dernière application ψ va bien être l'inverse de l'application φ. □

Corollaire 4.13. Deux ensembles algébriques affines sont isomorphes si et seulement si leurs anneaux de coordonnées sont isomorphes.

Preuve Soient V et W deux ensembles algébriques. Si $\varphi \colon W \to V$ est un isomorphisme, alors φ^* en est aussi un. Réciproquement, si $u \colon k[V] \to k[W]$ est un isomorphisme, alors on peut l'écrire sous la forme $u = \varphi^*$ et l'application $\varphi \colon W \to V$ est nécessairement un isomorphisme par le corollaire précédent. □

▷ Exemple. La courbe $C \coloneqq \mathrm{V}(Y - X^2)$ est isomorphe à la droite $\mathrm{V}(X)$ puisqu'on a $k[C] \simeq k[X]$.

Proposition 4.14. Soit $\varphi \colon W \to V$ une application polynomiale. Alors

1. on a $\mathrm{Ker}\,\varphi^* = \mathrm{I}_V(\mathrm{Im}\,\varphi)$;
2. l'application φ^* est injective si et seulement si l'application φ est dominante, *i. e.* la fermeture algébrique de son image dans V est égale à V ;
3. l'application φ^* est surjective si et seulement si l'application φ est une immersion fermée.

Preuve 1. Pour tout $f \in k[V]$, on a

$$f \in \mathrm{Ker}\,\varphi^* \iff f \circ \varphi = 0 \iff f|_{\mathrm{Im}\,\varphi} = 0 \iff f \in \mathrm{I}_V(\mathrm{Im}\,\varphi)$$

ce qui conclut.

2. On suppose que l'application φ est dominante. Comme $\mathrm{V}(\mathrm{I}_V(\mathrm{Im}\,\varphi))$ est la fermeture algébrique de $\mathrm{Im}\,\varphi$ dans V, on a $\mathrm{V}(\mathrm{I}_V(\mathrm{Im}\,\varphi)) = V$. Avec le point précédent, on obtient

$$\mathrm{Ker}\,\varphi^* = \mathrm{I}_V(\mathrm{Im}\,\varphi) = \mathrm{I}_V(\mathrm{V}(\mathrm{I}_V(\mathrm{Im}\,\varphi))) = \mathrm{I}_V(V) = \{0_V\}$$

de telle sorte que l'application φ^* est injective. Réciproquement, si cette dernière est injective, on obtient $\mathrm{V}(\mathrm{I}_V(\mathrm{Im}\,\varphi)) = \mathrm{V}(\mathrm{Ker}\,\varphi^*) = \mathrm{V}(0_V) = V$ ce qui montre la dominance de l'application φ.

3. Notons V' la fermeture algébrique de $\operatorname{Im}\varphi$ dans V. Alors l'application φ se factorise en une application dominante $\varphi\colon W \to V'$ suivie de l'inclusion $i\colon V' \to V$. Dans ce cas, l'application φ est une immersion fermée si et seulement si l'application ψ est un isomorphisme, *i. e.* l'application ψ^* est bijective. Comme ψ est dominante, l'application ψ^* est injective. Comme i^* est surjective, l'application ψ^* est surjective si et seulement si l'application φ^* l'est. En regroupant tous ces arguments, on obtient l'énoncé souhaité. □

Corollaire 4.15. Soient V un ensemble algébrique et $\mathfrak{m} \subset k[V]$ est un idéal. Alors

$$\exists P \in V,\ \mathfrak{m} = \mathrm{I}_V(P) \quad \Longleftrightarrow \quad k[V]/\mathfrak{m} \simeq k.$$

Preuve $\Rightarrow$ On écrit $\mathfrak{m} = \mathrm{I}_V(P)$. D'après la remarque page 24, on a alors $k[V]/\mathfrak{m} \simeq k[P] \simeq k$.

$\Leftarrow$ Réciproquement, on suppose qu'on a un isomorphisme $k[V]/\mathfrak{m} \simeq k$. Alors il existe un immersion fermée $i\colon \mathbb{A}^0(k) = \{0\} \to V$ telle que l'application $i^*\colon k[V] \to k$ soit la composée de la projection $k[V] \to k[V]/\mathfrak{m}$ et de l'isomorphisme $k[V]/\mathfrak{m} \to k$. Posons alors $P \coloneqq i(0) \in V$. On obtient $\mathfrak{m} = \mathrm{I}_V(P)$ puisque, pour tout $f \in k[V]$, on a

$$f \in \mathfrak{m} \quad \Longleftrightarrow \quad i^*(f) = 0 \quad \Longleftrightarrow \quad f(P) = i^*(f)(0) = 0 \quad \Longleftrightarrow \quad f \in \mathrm{I}_V(P). \qquad \square$$

4.4 Composantes irréductibles

Définition 4.16. – Une *composante irréductible* d'un espace topologique V est une partie maximale pour l'irréductibilité.

– Un espace topologique est *noethérien* si toute famille non vide de fermés (respectivement d'ouverts) contient un élément minimal (respectivement maximal), *i. e.* si toute suite décroissante de fermés (respectivement croissante d'ouverts) est stationnaires.

Proposition 4.17. Un espace topologique noethérien V possède un nombre fini de composantes irréductibles.

Preuve On suppose $V \neq \emptyset$. Considérons la famille des fermés non vides de V qui ne sont pas une réunion finie de fermés irréductibles. Raisonnons par l'absurde et supposons que cette famille est non vide. Comme l'espace V est noethérien, elle admet un plus petit élément W. Par construction, cet élément W est non vide et irréductibles : on peut donc écrire $W = W_1 \cup W_2$ pour deux fermés propres W_1 et W_2. Par minimalité de W, on peut écrire les fermés W_1 et W_2 comme des réunions finies de fermés irréductibles. Dès lors, il en va de même pour le fermé W ce qui est impossible. Finalement, cette famille est vide.

Ainsi tout fermé non vide de V est une réunion finie d'irréductibles. En particulier, on peut écrire $V = \bigcup_{i=1}^{r} V_i$ pour des irréductibles V_i. Maintenant, pour une composante irréductible A, elle sera incluse dans un irréductible V_i et, par maximalité des composantes, on aura $A = V_i$. On en déduit que l'espace possède un nombre fini de composantes irréductibles. □

Proposition 4.18. Soit V un ensemble algébrique. Alors les propositions suivantes sont équivalentes :

(i) l'espace V est irréductible ;

(ii) l'idéal $\mathrm{I}(V)$ est premier ;

(iii) l'anneau $k[V]$ est intègre.

Preuve Remarquons d'abord que, si on peut trouver deux polynômes $F, G \in k[X_1, \ldots, X_n]$ tels que $FG \in \mathrm{I}(V)$, alors on obtient $V = \mathrm{V}(\mathrm{I}(V)) \subset \mathrm{V}(FG) = \mathrm{V}(F) \cap \mathrm{V}(G)$.

On suppose que l'espace V est irréductible. Soient $F, G \in k[X_1, \ldots, X_n]$ tels que $FG \in \mathrm{I}(V)$. Quitte à échanger les rôles de ces deux polynômes, la remarque précédente et l'irréductibilité conduisant à avoir l'inclusion $V \subset \mathrm{V}(F)$. Comme $F \in \mathrm{I}(\mathrm{V}(F))$, on obtient $F \in \mathrm{I}(V)$. Ceci montre que l'idéal $\mathrm{I}(V)$ est premier.

On sait déjà que $k[X_1, \ldots, X_n]/\mathrm{I}(V) \simeq k[V]$, donc l'idéal $\mathrm{I}(V)$ est premier si et seulement si l'anneau $k[V]$ est intègre.

Enfin, on suppose que l'anneau $k[V]$ est intègre. Montrons que l'espace V est irréductible. Pour cela, soient V_1 et V_2 deux sous ensembles algébriques de V. Alors

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

Comme $k[V]$ est intègre, un des deux derniers idéaux est nul. Supposons $\mathrm{I}_V(V_1) = \{0_V\}$. Dans ce cas, on obtient $V_1 = \mathrm{V}(\mathrm{I}_V(V_1)) = \mathrm{V}(0_V) = V$. Ceci montre l'irréductibilité de l'espace V. □

THÉORÈME 4.19. Outre les points et le plan tout entier, les sous-ensembles algébriques irréductibles du plan sont les courbes infinies d'équation $F = 0$ où le polynôme $F \in k[X, Y]$ est irréductible.

Preuve On a déjà vu que la condition est suffisante. Maintenant, on se donne un sous-ensemble algébrique V qui n'est pas le plan et réduit à un point. Alors $\mathrm{I}(V) \neq \{0\}$. On peut donc trouver un polynôme non constant $F \in \mathrm{I}(V)$ qu'on suppose irréductible. Montrons que $V = \mathrm{V}(F)$. Si V était fini, alors V serait réduit à un unique point par son irréductibilité ce qui est exclut. Donc V est infini. Par ailleurs, soit $G \in \mathrm{I}(V)$. Alors $V \subset \mathrm{V}(F, G)$ est infini, donc les polynômes F et G ne sont pas premiers entre eux. Comme F est irréductible, on trouve donc $F \mid G$ si bien que $G \in \langle F \rangle$. Comme l'inclusion réciproque est évidente, on trouve $\mathrm{I}(V) = \langle F \rangle$ ce qui implique $V = \mathrm{V}(F)$. □

◇ REMARQUE. Si V est un ensemble algébrique, alors $k[V]$ est noethérien. En effet, il suffit de remarquer que l'anneau $k[V]$ est une k-algèbre de type fini sur un corps et d'appliquer le théorème de la base de Noether.

THÉORÈME 4.20. Un ensemble algébrique V est un espace topologique noethérien.

Preuve Soit $(V_i)_{i\in\mathbf{N}}$ une suite décroissante de sous-ensembles algébriques de V. La suite $(\mathrm{I}(V_i))_{i\in\mathbf{N}}$ d'idéaux de $k[V]$ est croissante. Comme V est noethérien, l'anneau $k[V]$ l'est, donc cette suite est stationnaire. Comme $V_i = \mathrm{V}(\mathrm{I}(V_i))$, la suite $(V_i)_{i\in\mathbf{N}}$ est aussi stationnaire ce qui conclut. □

4.5 Fonctions rationnelles

DÉFINITION 4.21. Soit V un ensemble algébrique irréductible. Une *fonction rationnelle* sur V est un élément du corps des fractions $k(V) \coloneqq \operatorname{Frac} k[V]$. Une fonction $f \in k(V)$ est *régulière* en un point $P \in V$ si on peut l'écrire sous la forme $f = g/h$ avec $g, h \in k[V]$ et $h(P) \neq 0$. Dans ce cas, l'élément h est le *dénominateur* de la fonction f et on pose $f(P) \coloneqq g(P)/h(P) \in k$. Le point P est

- un *zéro* de la fonction f si $f(P) = 0$;
- un *pôle* de la fonction f si cette dernière n'est pas régulière au point P.

◇ REMARQUES. – Soit $f \in k(V)$. L'ensemble $I_f \subset k[V]$ des dénominateurs de la fonction f est un idéal et l'ensemble de ces pôles est l'ensemble algébrique $\mathrm{V}(I_f)$. La fonction f est polynomiale si et seulement si $I_f = k[V]$. Si l'anneau $k[V]$ est factoriel, alors l'idéal I_f est principal.

– Soit $f \in k(V)$ une fonction rationnelle non nulle et régulière en un point $P \in V$. Alors elle admet un zéro au point P si et seulement si son inverse $1/f$ admet un pôle au point P.

– L'ensemble des points où une fonction rationnelle sur V est régulière est un ouvert de V.

NOTATIONS. Pour un ensemble algébrique irréductible V et un point $P \in V$, on note $\mathscr{O}_{V,P} \subset k(V)$ (respectivement $\mathfrak{m}_{V,P} \subset k(V)$) l'ensemble des fonctions rationnelles sur V qui sont régulières au point P (respectivement et qui s'annulent au point P).

PROPOSITION 4.22. Soient V un ensemble algébrique irréductible et $P \in V$. L'ensemble $\mathscr{O}_{V,P}$ est un anneau local intègre noethérien d'idéal maximal $\mathfrak{m}_{V,P}$. Plus précisément, en notant $\mathfrak{m} \coloneqq \mathrm{I}_V(P)$,

- l'anneau $\mathscr{O}_{V,P} = k[V]_{\mathfrak{m}}$ est le localisé de $k[V]$ en $\mathfrak{m}$;
- son idéal maximal est $\mathfrak{m}_{V,P} = \mathfrak{m}k[V]_{\mathfrak{m}}$.

Preuve D'abord, l'égalité $\mathscr{O}_{V,P} = k[V]_{\mathfrak{m}}$ est vraie puisque, pour toute fonction $f \in k(V)$, on a

$$f \in \mathscr{O}_{V,P} \quad \Longleftrightarrow \quad \exists g, h \in k[V], \quad f = g/h \quad \text{et} \quad h(P) \neq 0$$

$$\begin{aligned} &\iff \quad \exists g, h \in k[V], \quad f = g/h \quad \text{et} \quad h \notin \mathfrak{m} \\ &\iff \quad f \in k[V]_{\mathfrak{m}}. \end{aligned}$$

En particulier, l'anneau $\mathscr{O}_{V,P}$ est un anneau local intègre noethérien d'idéal $\mathfrak{m}k[V]_{\mathfrak{m}}$. Maintenant, l'égalité $\mathfrak{m}_{V,P} = \mathfrak{m}k[V]_{\mathfrak{m}}$ est bien vérifié puisque, pour toute fonction $f \in k(V)$, on a

$$\begin{aligned} f \in \mathfrak{m}_{V,P} \quad &\iff \quad \exists g, h \in k[V], \quad f = g/h \quad \text{et} \quad g(P) = 0 \quad \text{et} \quad h(P) \neq 0, \\ &\iff \quad \exists g, h \in k[V], \quad f = g/h \quad \text{et} \quad g \in \mathfrak{m} \quad \text{et} \quad h \notin \mathfrak{m}, \\ &\iff \quad f \in \mathfrak{m}k[V]_{\mathfrak{m}}. \end{aligned}$$

□

▷ Exemples. On a

$$\frac{X+1}{X-1} \in \mathscr{O}_{\mathbb{A}^n(k),0} \quad \text{et} \quad \frac{X}{X-1} \in \mathfrak{m}_{\mathbb{A}^n(k),0}.$$

Notation. Lorsque un morphisme d'anneaux de A dans B est fixé, pour un idéal I de A, on notera IB l'idéal de B engendré par l'image de I par ce morphisme.

Proposition 4.23. Soient V un ensemble algébrique irréductible et $P \in V$. Alors il existe un isomorphisme

$$\mathscr{O}_{\mathbb{A}^n(k),P}/\operatorname{I}(V)\mathscr{O}_{\mathbb{A}^n(k),P} \simeq \mathscr{O}_{V,P}.$$

Plus généralement, pour tout idéal I de $k[X_1, \ldots, X_n]$, on a

$$\mathscr{O}_{\mathbb{A}^n(k),P}/(J + \operatorname{I}(V))\mathscr{O}_{\mathbb{A}^n(k),P} \simeq \mathscr{O}_{V,P}/J\mathscr{O}_{V,P}.$$

Preuve Le premier isomorphisme est une conséquence de la commutation de la localisation et des quotients : en posant

$$A \coloneqq k[X_1, \ldots, X_n], \quad \mathfrak{m} \coloneqq \operatorname{I}(P), \quad I \coloneqq \operatorname{I}(V), \quad \overline{A} \coloneqq k[V] \quad \text{et} \quad \overline{\mathfrak{m}} \coloneqq \operatorname{I}_V(P),$$

on obtient un isomorphisme

$$A_{\mathfrak{m}}/IA_{\mathfrak{m}} \simeq \overline{A}/\overline{A}_{\overline{\mathfrak{m}}}.$$

Le second résulte d'un corollaire du théorème d'isomorphisme. □

◇ Remarques. – Soit $\varphi\colon W \to V$ une application polynomiale entre deux ensembles algébriques irréductibles. L'application φ^* se prolonge en une unique extension de corps $k(W) \to k(V)$. Pour voir cela, il suffit d'utiliser la propriété universelle du corps des fractions.

– Soient $Q \in W$ et $P \in \varphi(Q)$. L'application φ^* se prolonge de manière unique en un morphisme d'anneaux $\varphi_Q^*\colon \mathscr{O}_{V,P} \to \mathscr{O}_{W,Q}$. En effet, en posant $\mathfrak{m} \coloneqq \operatorname{I}_V(P)$ et $\mathfrak{n} \coloneqq \operatorname{I}_W(Q)$, on a $(\varphi^*)^{-1}(\mathfrak{n}) = \mathfrak{m}$ et l'application φ^* se prolonge alors en un morphisme d'anneaux $k[V]_{\mathfrak{m}} \to k[W]_{\mathfrak{n}}$.

– Soit U un ouvert non vide de V. L'ensemble $\Gamma(U)$ des fonctions régulières sur U est une k-algèbre intègre et il vérifie $\Gamma(U) = \bigcap_{P \in U} \mathscr{O}_{V,P}$.

Définition 4.24. Soient V et W deux ensembles algébrique tel que l'ensemble V soit irréductible. Une application (injective) polynomiale $j\colon W \to V$ est une *immersion ouverte* si

(i) elle induit un homéomorphisme entre W et un ouvert U de V ;

(ii) pour tout $Q \in W$, l'application j_Q^* est un isomorphisme.

Dans ce cas, on dit que l'ensemble U est un *ouvert affine* de V.

◇ Remarques. – On peut remplacer les deux points de la définition par les deux suivants, *a priori* plus fortes :

(i′) elle induit un bijection entre W et un ouvert U de V ;

(ii′) l'application j^* se prolonge en un isomorphisme entre $\Gamma(U)$ et $\Gamma(W)$.

En effet, supposons que ces deux derniers points (i′) et (ii′) sont vérifiées. Montrons d'abord que l'application j induit un homomorphisme de W dans U. Il suffit de montrer que l'image d'un fermé est bien un fermé. Soit $f \in k[V]$ une fonction non nulle. Avec le point (i′), on peut écrire $f = j^*(\varphi)$ avec $\varphi \in \Gamma(U)$. Alors l'image

$$j(\operatorname{V}(f)) = \{P \in U \mid \varphi(P) = 0\} = \operatorname{V}(I_{1/\varphi}) \cap U$$

est fermée dans U. Ceci conclut le point (i). Montrons le point (ii). Soient $Q \in W$ et $h \in \mathscr{O}_{W,Q}$. On peut écrire $h = f/g$ avec $f, g \in k[W]$ et $g(Q) \neq 0$. Avec le point (i′), on peut aussi écrire $f = j^*(\varphi)$ et $g = j^*(\psi)$ avec $\varphi, \psi \in \Gamma(U)$. Comme $g(Q) \neq 0$, on a $\psi(j(Q)) = j^*(\psi)(Q) = g(Q) \neq 0$. Ceci nous montre que $\psi \in \mathscr{O}^\times_{V,j(Q)}$ et $j^*(\psi^{-1}\varphi) = h$. Ceci conclut à la surjectivité de l'application j^*_Q. De plus, elle est injective puisque l'application j est dominante. D'où le point (ii).

– Un *ouvert principal* de V une partie de la forme $\mathrm{D}(g) \coloneqq \{P \in V \mid g(V) = 0\}$ avec $g \in k[V]$. C'est un ouvert affine de V. Plus précisément, la projection $p\colon V \times \mathbb{A}^1(k) \to V$ induit une immersion ouverte entre $W \coloneqq \mathrm{V}(gX_{n+1} - 1)$ dans V dont l'image vaut $\mathrm{D}(g)$.

▷ Exemple. L'ensemble $\mathbb{A}^1(k) \setminus \{0\}$ est un ouvert affine de $\mathbb{A}^1(k)$. Cela ne marche plus avec $\mathbb{A}^2(k)$.

Chapitre 5

Courbes algébriques planes

Dans tout le chapitre, on considère un corps algébriquement clos k.

5.1 Le théorème des zéros de Hilbert

PROPOSITION 5.1. Soit V un ensemble algébrique. Alors les idéaux maximaux de $k[V]$ sont exactement les idéaux de la forme $\mathrm{I}_V(P)$ avec $P \in V$.

Preuve Soit $P \in V$. On considère l'idéal $\mathfrak{m} \coloneqq \mathrm{I}_V(P)$. Par le corollaire 4.15 du chapitre précédent, il existe un isomorphisme $k[V]/\mathfrak{m} \simeq k$ si bien qu'il est maximal.

Réciproquement, soit $\mathfrak{m}$ un idéal maximal de $k[V]$. Alors l'extension $k[V]/\mathfrak{m}$ est une k-algèbre de type fini qui s'avère être un corps. La version algébrique du théorème des zéros de Hilbert nous assure alors qu'il s'agit d'une extension finie du corps k. Mais puisque que ce dernier est algébriquement clos, on obtient un isomorphisme $k[V]/\mathfrak{m} \simeq k$. En appliquant le corollaire 4.15, l'idéal maximal est bien de la forme $\mathrm{I}_V(P)$. □

◇ REMARQUE. Autrement dit, en notant $\mathrm{Spm}(A)$ l'ensemble des idéaux maximaux d'un anneau A, on obtient une bijection $V \simeq \mathrm{Spm}(k[V])$, celle qui associe un point $P \in V$ à l'idéal $\mathrm{I}_V(P) \in \mathrm{Spm}(k[V])$.

COROLLAIRE 5.2. Soit I un idéal de $k[V]$. Alors $I = k[V]$ si et seulement si $\mathrm{V}(I) = \emptyset$.

Preuve Il suffit de montrer le sens réciproque. Par cela, on va raisonner par contraposée et supposer $I \neq k[V]$. Alors l'idéal I est contenu dans un idéal maximal qui, par la proposition, est nécessairement de la forme $\mathrm{I}_V(P)$ avec $P \in V$. On peut alors écrire $\{P\} = \mathrm{V}(\mathrm{I}_V(P)) \subset \mathrm{V}(I)$ ce qui montre $\mathrm{V}(I) \neq \emptyset$. □

COROLLAIRE 5.3. Soit V un ensemble algébrique irréductible. Alors $\Gamma(V) = k[V]$.

Preuve Pour toute fonction $f \in \Gamma(V)$, on a $\mathrm{V}(I_f) = \emptyset$ impliquant $I_f = k[V]$, donc la fonction f est polynomiale. Ceci montre l'inclusion $\Gamma(V) \subset k[V]$. L'inclusion réciproque étant évidente, on obtient l'égalité. □

THÉORÈME 5.4 *(des zéros de Hilbert).* Soient V un ensemble algébrique et I un idéal de $k[V]$. Alors

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

Preuve Seule l'inclusion directe est à montrer. Comme on peut se ramener au cas $V = \mathbb{A}^n(k)$, on peut suppose que l'ensemble algébrique V est irréductible. Soit $g \in \mathrm{I}_V(\mathrm{V}(I))$. Considérons l'immersion ouvert $j\colon W \to V$ avec $W \coloneqq \mathrm{V}(gX_{n+1} - 1)$ dont l'image vaut $\mathrm{D}(g)$. On a

$$\mathrm{V}(I) = \mathrm{V}(\mathrm{I}_V(\mathrm{V}(I))) \subset \mathrm{V}(g)$$

de telle sorte qu'on ait $\mathrm{V}(I) \cap \mathrm{D}(g) = \emptyset$. On en déduit alors $\mathrm{V}(Ik[W]) = j^{-1}(\mathrm{V}(I)) = \emptyset$. Par notre premier corollaire, on en déduit $Ik[W] = k[W]$ ce qui se réécrit $Ik[V]_g = k[V]_g$. Cela implique l'existence d'une fonction $f \in I$ et d'un entier $n \in \mathbf{N}$ vérifiant $f/g^n = 1$, c'est-à-dire $g^n = f \in I$. D'où $g \in \sqrt{I}$. Finalement, on a montré l'inclusion directe. □

COROLLAIRE 5.5. Les applications $S \longmapsto \mathrm{V}(S)$ et $A \longmapsto \mathrm{I}_V(A)$ sont des bijections réciproques l'une de l'autre entre les idéaux radicaux (respectivement les idéaux premiers ou les idéaux maximaux) de $k[V]$ et les sous-ensembles algébriques (respectivement les sous-ensembles algébriques irréductibles ou les points) de V.

Preuve Si $W \subset V$ est un sous-ensemble algébrique, alors $I \coloneqq \mathrm{I}_V(W)$ est un idéal radiciel de $k[V]$ vérifiant $W = \mathrm{V}(I)$. Réciproquement, si I est un idéal radiciel de $k[V]$, alors $W \coloneqq \mathrm{V}(I)$ est un sous-ensemble algébrique de V et, avec le théorème des zéros de Hilbert, on a $\mathrm{I}_V(\mathrm{V}(I)) = \sqrt{I} = I$. Enfin, on sait que l'ensemble algébrique W est irréductible (respectivement réduit à un point) si et seulement si l'idéal I est premier (respectivement maximal). □

COROLLAIRE 5.6. Soit $V \subset \mathbb{A}^n(k)$ une hypersurface d'équation $F = 0$. Alors les composantes irréductibles de V sont les hypersurfaces définies par les facteurs irréductibles de F.

Preuve On décompose le polynôme F en produit $F_1^{r_1} \cdots F_m^{r_m}$ de facteurs irréductibles. Alors

$$V = \mathrm{V}(F_1) \cup \cdots \cup \mathrm{V}(F_m).$$

De plus, comme les polynômes F_i sont irréductibles, les idéaux principaux $\langle F_i \rangle$ sont premiers et ils ne peuvent pas être contenu les uns dans les autres puisque les polynômes F_i sont premiers entre eux. Par conséquent, l'écriture précédente correspond à la décomposition en composantes irréductibles de V. □