CHAPITRE
III

Polynômes, ensembles algébriques affines et idéaux

Sommaire

§ 1 Les polynômes à plusieurs indéterminées

Nous avons vu dans le premier chapitre la notion de polynôme à une indéterminée., dans cette section, nous introduisons les polynômes à plusieurs indéterminées à coefficients dans un corps.

III.1.1. Les monômes.— Un *monôme* en les indéterminées $x_1, x_2, \ldots, x_n$ est un produit de la forme

$$x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n},$$

où $\alpha_1, \ldots, \alpha_n$ sont des entiers naturels. On appelle *degré total* d'un tel monôme, la somme

$$\alpha_1 + \alpha_2 + \ldots + \alpha_n.$$

Par exemple, les monômes

$$x_1^4 x_2^3 x_3^2, \quad x_1^2 x_3^2, \quad x_3^5$$

sont des monômes de degré total 9, 4 et 5 respectivement.

III.1.2. Notations.— En notant α un n-uplet $(\alpha_1, \alpha_2, \ldots, \alpha_n)$ d'entiers naturels, on notera

$$x^\alpha = x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n}.$$

En particulier, on pose $x^{(0,0,\ldots,0)} = 1$. Le degré total du monôme x^α sera noté

$$|\alpha| = \alpha_1 + \alpha_2 + \ldots + \alpha_n.$$

III.1.3. Les polynômes.— Un *polynôme* f d'indéterminées $x_1, \ldots, x_n$ à coefficients dans un corps $\mathbb{K}$ est une combinaison linéaire (finie) à coefficients dans $\mathbb{K}$ de monômes d'indéterminées $x_1, \ldots, x_n$. Avec les notations précédentes, un polynôme f s'écrit sous la forme

$$f = \sum_\alpha a_\alpha x^\alpha,$$

où a_α est un scalaire dans $\mathbb{K}$ et la somme est indexée par un nombre fini de n-uplets $\alpha = (\alpha_1, \ldots, \alpha_n)$.

La somme et le produit de deux polynômes d'indéterminés $x_1, \ldots, x_n$ est encore un polynôme d'indéterminées $x_1, \ldots, x_n$. On a

III.1 Proposition.— L'ensemble des polynômes d'indéterminées $x_1, \ldots, x_n$, muni de l'addition et de la multiplication forme un anneau commutatif, noté $\mathbb{K}[x_1, \ldots, x_n]$.

III.1.4. Notation.— Lorsque l'on considérera des polynômes avec un petit nombre d'indéterminées, on utilisera les lettres sans indice x, y, z, ..., pour désigner les indéterminées. Les anneaux des polynômes d'une, deux et trois indéterminées seront ainsi notés $\mathbb{K}[x]$, $\mathbb{K}[x,y]$ et $\mathbb{K}[x,y,z]$ respectivement. Par exemple, le polynôme

$$f = \frac{1}{2} x^4 y^3 z^2 + 2x^2 z^2 - \frac{1}{5} xyz + z^5$$

est un polynôme de $\mathbb{Q}[x,y,z]$.

III.1.5. Définitions.— Soit $f = \sum_\alpha a_\alpha x^\alpha$ un polynôme de $\mathbb{K}[x_1, \ldots, x_n]$,

- **i)** le scalaire a_α est appelé le *coefficient* du monôme x^α,
- **ii)** si $a_\alpha \neq 0$, $a_\alpha x^\alpha$ est un *terme* du polynôme f,
- **iii)** le *degré total* du polynôme f, noté $\deg(f)$, est le degré total maximun $|\alpha|$, tel que le coefficient a_α soit non nul.

Par exemple, le polynôme

$$f = 2xy^2z^2 + 3x^2z^2 - 5xyz^3 + z^5$$

possède 4 termes de degrés 5, 4, 5 et 5 respectivement, il est de degré total 5. Notons que trois termes sont de même degré total maximal 5 avec des monômes différents. Cette situation n'est pas possible avec des polynômes d'une seule indéterminée. Dans la suite de ce cours, nous expliciterons les méthodes permettant d'ordonner les termes dans un polynôme à plusieurs indéterminées.

III.1.6. Remarque sur la construction de l'anneau des polynômes à plusieurs indéterminées.— De la même façon que nous avons construit l'anneau $\mathbb{K}[x]$ des polynômes à une indéterminée à coefficients dans $\mathbb{K}$, on peut construire l'anneau $A[x]$ des polynômes à coefficients dans un anneau commutatif A. Étant donné un anneau de polynômes $A[x_1]$, on peut construire l'anneau des polynômes à une indéterminée x_2 à coefficients dans $A[x_1]$, que l'on note $(A[x_1])[x_2]$. De la même façon, on peut construire l'anneau $(A[x_2])[x_1]$. Ces deux anneaux sont canoniquement isomorphes par l'isomorphisme [1] suivant :

$$\begin{aligned} (A[x_1])[x_2] &\longrightarrow (A[x_2])[x_1] \\ \sum_{\alpha_2}\left(\sum_{\alpha_1} a_{\alpha_1,\alpha_2}\, x_1^{\alpha_1}\right) x_2^{\alpha_2} &\longmapsto \sum_{\alpha_1}\left(\sum_{\alpha_2} a_{\alpha_1,\alpha_2}\, x_2^{\alpha_2}\right) x_1^{\alpha_1} \end{aligned}$$

On note cet anneau $A[x_1,x_2]$ et ses éléments sont notés

$$\sum_{\alpha_1,\alpha_2} a_{\alpha_1,\alpha_2}\, x_1^{\alpha_1} x_2^{\alpha_2}.$$

Par itération, on peut construire l'anneau des polynômes à n indéterminées à coefficients dans A, noté

$$A[x_1,\ldots,x_n] = (A[x_1,\ldots,x_{n-1}])[x_n],$$

ses éléments sont les sommes finies

$$\sum_{\alpha_1,\ldots,\alpha_n} a_{\alpha_1,\ldots,\alpha_n}\, x_1^{\alpha_1}\ldots x_n^{\alpha_n}.$$

§ 2 Les ensembles algébriques affines

III.2.1. Fonction polynomiale.— Étant donné un polynôme $f = \sum_{\alpha} a_\alpha x^\alpha$ de $\mathbb{K}[x_1,\ldots,x_n]$, on définit la *fonction polynomiale* associée comme l'application

$$\widetilde{f} : \mathbb{K}^n \longrightarrow \mathbb{K},$$

1. Soient A et B deux anneaux. Un *morphisme d'anneaux* de A dans B est une application $f : A \longrightarrow B$ vérifiant les assertions suivantes

i) $f(a+b) = f(a)+f(b)$, pour tous $a,b \in A$,

ii) $f(ab) = f(a)f(b)$, pour tous $a,b \in A$,

iii) $f(1) = 1$.

Un *isomorphisme* d'anneaux est un morphisme d'anneaux bijectif.

qui à tout $(a_1,\dots,a_n) \in \mathbb{K}^n$ associe le scalaire $f(a_1,\dots,a_n) \in \mathbb{K}$, obtenu en remplaçant dans l'expression de f l'indéterminée x_i par a_i, pour tout i.

Nous avons déjà vu en I.4.1 que les notions de polynôme et de fonction polynomiale ne coïncident pas lorsque $\mathbb{K}$ est un corps fini. Pour les corps infinis, tels que $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$, on a cependant

III.2 Proposition.— Soit $\mathbb{K}$ un corps infini et soit f un polynôme de $\mathbb{K}[x_1,\dots,x_n]$. Alors f est le polynôme nul de $\mathbb{K}[x_1,\dots,x_n]$ si, et seulement si, la fonction polynomiale associée $\widetilde{f} : \mathbb{K}^n \longrightarrow \mathbb{K}$ est la fonction nulle.

Exercice 1.— L'objectif est de montrer la proposition III.2.

1. Montrer que la fonction polynomiale du polynôme nul est la fonction nulle.
2. Montrer la réciproque dans le cas où $n = 1$: si $f \in \mathbb{K}[x]$ possède une fonction polynomiale nulle, alors f est nul.
3. Montrer la réciproque dans le cas général, par récurrence sur l'entier n.

Exercice 2.— On suppose que $\mathbb{K}$ est le corps $\mathbb{Z}/2\mathbb{Z}$.

1. Considérons le polynômes $f = x^2y + y^2x$ de $\mathbb{K}[x,y]$. Montrer que la fonction polynomiale $\widetilde{f}$ est nulle.
2. Trouver un polynôme non nul de $\mathbb{K}[x,y,z]$ à trois indéterminées, dont la fonction polynomiale est nulle.

On déduit de la proposition III.2, le résultat suivant

III.3 Proposition.— Soit $\mathbb{K}$ un corps infini et soient f,g deux polynômes de $\mathbb{K}[x_1,\dots,x_n]$. Alors les polynômes f et g sont égaux si, et seulement si, les fonctions polynomiales $\widetilde{f} : \mathbb{K}^n \longrightarrow \mathbb{K}$ et $\widetilde{g} : \mathbb{K}^n \longrightarrow \mathbb{K}$ sont égales.

Exercice 3.— Montrer la proposition III.3.

III.2.2. Espaces affines de dimension *n*.— Étant donné un corps $\mathbb{K}$ et $n \geq 1$ un entier naturel, on appelle *espace affine* de dimension n sur $\mathbb{K}$ l'ensemble

$$\mathbb{K}^n = \{(a_1,\dots,a_n) \mid a_1,\dots,a_n \in \mathbb{K}\}.$$

L'espace $\mathbb{K}^1$ est appelé la *droite affine*, l'espace $\mathbb{K}^2$ est appelé le *plan affine* .

III.2.3. Ensembles algébriques affines.— Soit $\mathbb{K}$ un corps et soient $f_1,\dots,f_s$ des polynômes de $\mathbb{K}[x_1,\dots,x_n]$. On note

$$\mathbf{V}(f_1,\dots,f_s) = \{(a_1,\dots,a_n) \in \mathbb{K}^n \mid f_i(a_1,\dots,a_n) = 0, \quad \text{pour tout } i \in [\![1,s]\!]\}$$

Le sous-ensemble $\mathbf{V}(f_1,\ldots,f_s)$ de $\mathbb{K}^n$ est appelé l'*ensemble algébrique affine*, ou *variété algébrique affine*, définie par les polynômes $f_1,\ldots,f_s$. L'ensemble algébrique affine $\mathbf{V}(f_1,\ldots,f_s)$ est ainsi le sous-ensemble de $\mathbb{K}^n$ formé des solutions du système d'équations

$$\left\{\begin{array}{c} f_1(a_1,\ldots,a_n)=0 \\ f_2(a_1,\ldots,a_n)=0 \\ \vdots \\ f_s(a_1,\ldots,a_n)=0 \end{array}\right.$$

Exercice 4.— Montrer que l'ensemble vide et l'espace affine $\mathbb{K}^n$ sont des ensembles algébriques affines.

Exercice 5.— Montrer qu'un point de $\mathbb{K}^n$ est un ensemble algébrique affine.

Exercice 6.— On suppose que $n=1$. Si f n'est pas le polynôme nul de $\mathbb{K}[x]$, montrer que $\mathbf{V}(f)$ est un ensemble fini. Ainsi, les ensembles algébriques affines de la droite affine sont la droite elle-même et les ensembles finis.

Exercice 7.— Montrer que deux polynômes différents peuvent définir le même ensemble algébrique affine.

III.2.4. Exemples dans $\mathbb{R}^2$.— Pour les exemples suivants, on considère que $\mathbb{K}$ est le corps des réels. Dans le plan $\mathbb{R}^2$, l'ensemble algébrique affine $\mathbf{V}(x^2+y^2-1)$ est le cercle centré sur l'origine et de rayon 1.

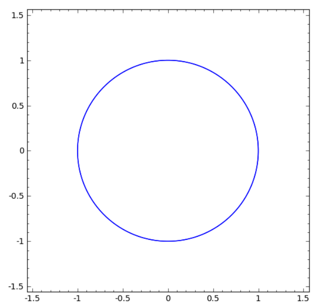


FIGURE III.1.: Cercle $\mathbf{V}(1-x^2-y^2)$

Les commandes Sage pour tracer la figure III.1 sont

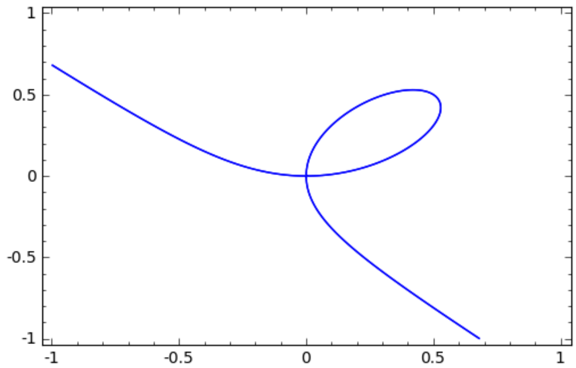
```
sage: R.<x, y> = RR[]
sage: C = Curve(x^2 + y^2 -1)
sage: C.plot((x,-1.5,1.5), (y,-1.5,1.5))
```

L'ensemble algébrique affine réel $\mathbf{V}(x^2+y^2+1)$ est l'ensemble vide, car l'équation $x^2+y^2=-1$ ne possède pas de solution réelle

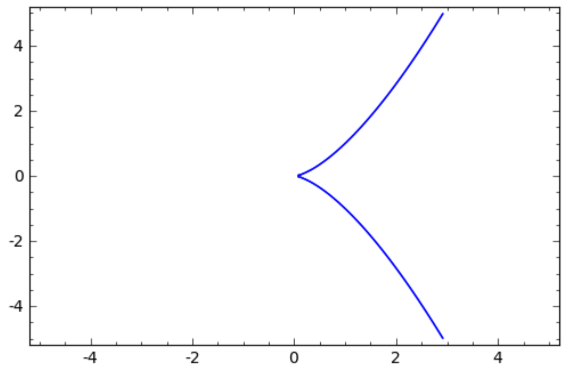
Exercice 8.— Montrer qu'un ensemble algébrique affine $\mathbf{V}(f)$ défini par un polynôme f de $\mathbb{R}[x,y]$ n'est pas toujours une partie connexe de $\mathbb{R}^2$.

Exercice 9.— Tracer les ensembles algébriques suivants dans $\mathbb{R}^2$:

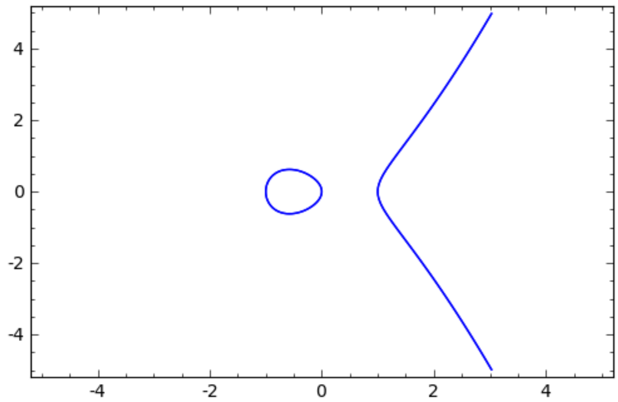
1. $\mathbf{V}(x^2+4y^2+2x-16y+1)$,
2. $\mathbf{V}(x^2-y^2)$,
3. $\mathbf{V}(2x+y-1, 3x-y+2)$,
4. $\mathbf{V}(y^2-x(x-1)(x-2))$.



(a) Cubique nodale $\mathbf{V}(x^3+y^3-xy)$

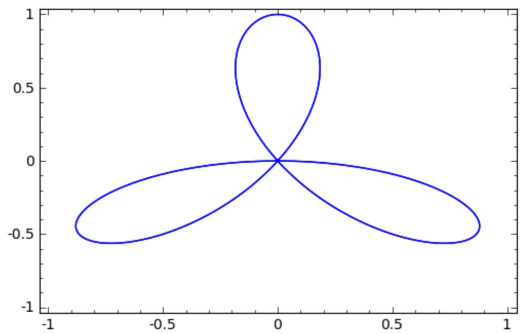


(b) Cubique cuspidale $\mathbf{V}(y^2-x^3)$

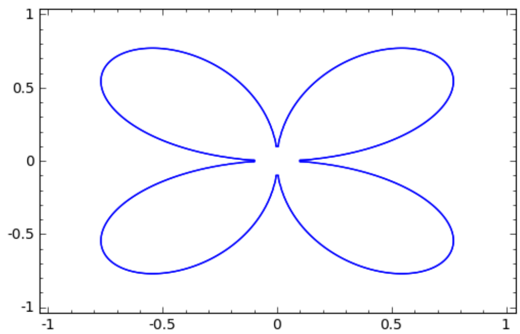


(c) Une cubique non singulière $\mathbf{V}(y^2-x(x-1)(x+1))$

FIGURE III.2.: Des cubiques $\mathbf{V}(f)$ (f de degré 3).

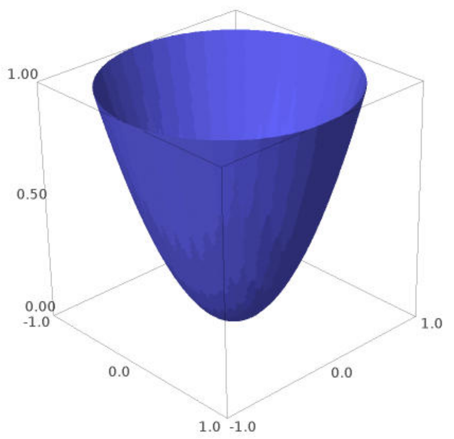


(a) Trifolium $\mathbf{V}((x^2+y^2)^2+3x^2y-y^3)$

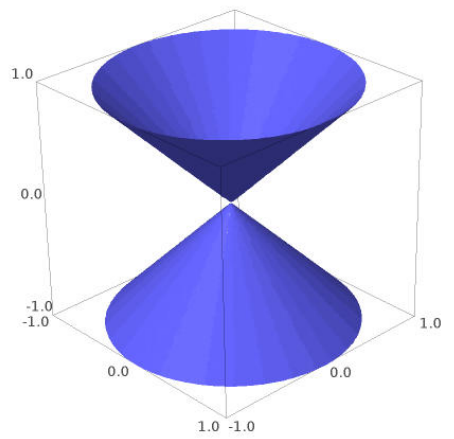


(b) Quadrifolium $\mathbf{V}((x^2+y^2)^3-4x^2y^2)$

III.2.5. Exemples dans $\mathbb{R}^3$.— Le paraboloïde de révolution, obtenu par rotation d'une parabole $z = x^2$ autour de l'axe Oz.



(c) Paraboloïde de révolution $\mathbf{V}(z - x^2 - y^2)$



(d) Cône de révolution $\mathbf{V}(z^2 - x^2 - y^2)$

Les commandes Sage pour le tracé du paraboloïde :

```
sage: var('x,y,z')
sage: h = lambda x,y,z:z-x^2-y^2
sage: f = implicit_plot3d(h,(x,-1,1),(y,-1,1),(z,0,1),\
....:                   plot_points=100, smooth=True, adaptative=True)
sage: f
```

Exercice 10. — Tracer les ensembles algébriques suivants dans $\mathbb{R}^3$:

1. $\mathbf{V}(x^2 + y^2 + z^2 - 1)$,
2. $\mathbf{V}(x^2 + y^2 - 1)$,
3. $\mathbf{V}(x + 2, y - 3/2, z)$,
4. $\mathbf{V}(xz^2 - xy)$,
5. $\mathbf{V}(x^2 + y^2 + z^2 - 1, x^2 + y^2 + (z-1)^2 - 1)$.

Exercice 11. — Décrire l'équation de l'ensemble algébrique affine constitué du cylindre de rayon 1 centré sur l'axe des y.

Exercice 12. — On considère l'ensemble

$$X = \{(x,x) \mid x \in \mathbb{R} - \{1\}\} \subset \mathbb{R}^2.$$

1. Montrer que si f est un polynôme de $\mathbb{R}[x,y]$, tel que la fonction polynomiale $\widetilde{f}$ s'annule sur X, alors $f(1,1) = 0$.
2. En déduire que X n'est pas un ensemble algébrique affine de $\mathbb{R}^2$.

III.2.6. Un exemple en robotique.— En conclusion de ce cours, nous développerons un exemple d'application de l'étude des ensembles algébriques affines à la robotique. L'idée est la suivante. Considérons un bras de robot articulé dont les mouvements sont dans un plan ; le bras est constitué de deux segments

- un segment de longueur 2 est fixé à l'origine par une rotule,
- un deuxième segment de longueur 1 est fixé à l'extrémité du premier segment par une autre rotule.

Les états du bras sont déterminés par deux couples de coordonnées (x,y) et (z,w) qui correspondent à l'extrémité de chaque segment. Une configuration du bras du robot peut ainsi être vue come un 4-uplet
$$(x,y,z,w) \in \mathbb{R}^4.$$
Notons que, si l'on considère le problème en dimension 3, le système admettra 6 indéterminées. Tous les points de $\mathbb{R}^4$ ne sont pas une configuration du bras du robot. En particulier, des points du plan ne seront pas atteignables par le bras. L'ensemble des configurations du robot est défini par les équations

$$\left\{ \begin{array}{rl} x^2+y^2 & = 4, \\ (x-z)^2+(y-w)^2 & = 1. \end{array} \right.$$

Par exemple, l'origine $(z,w) = (0,0)$ n'est pas atteignable par l'extrémité du bras du robot. En effet, le système
$$\left\{ \begin{array}{rl} x^2+y^2 & = 4, \\ x^2+y^2 & = 1. \end{array} \right.$$
ne possède pas de solution. Par contre, le point $(z,w) = (1,0)$ est atteignable, car le système
$$\left\{ \begin{array}{rl} x^2+y^2 & = 4, \\ (x-1)^2+y^2 & = 1. \end{array} \right.$$
est équivalent au système
$$\left\{ \begin{array}{rl} x^2+y^2 & = 4, \\ -2x & = -4. \end{array} \right.$$
Il admet donc pour solution $(x,y) = (2,0)$. Le point du plan de coordonnées $(z,w) = (4,0)$ n'est pas atteignable par le bras du robot, car le système

$$\left\{ \begin{array}{rl} x^2+y^2 & = 4, \\ x^2+(y-4)^2 & = 1. \end{array} \right.$$

ne possède pas de solution. La seconde équation s'écrit $x^2+y^2-8y+16 = 1$, or, d'après la première équation, on a $-8y = -19$, soit $y = 19/8 > 2$. Le système n'a donc pas de solution.

III.2.7. Opérations sur les ensembles algébriques affines.— L'intersection et la réunion d'ensembles algébriques affines sont encore des ensembles algébriques affines.

III.4 Proposition. — Si $\mathbf{V}$ et $\mathbf{W}$ sont deux ensembles algébriques affines, alors il en est de même pour $\mathbf{V} \cup \mathbf{W}$ et $\mathbf{V} \cap \mathbf{W}$.

Preuve. Supposons que

$$\mathbf{V} = \mathbf{V}(f_1, \ldots, f_s), \quad \mathbf{W} = \mathbf{V}(g_1, \ldots, g_t).$$

On a

$$\mathbf{V} \cap \mathbf{W} = \mathbf{V}(f_1, \ldots, f_s, g_1, \ldots, g_t),$$

car un élément de $\mathbf{V} \cap \mathbf{W}$ annule à la fois les polynômes $f_1, \ldots, f_s$ et les polynômes $g_1, \ldots, g_t$. Ainsi $\mathbf{V} \cap \mathbf{W}$ est un ensemble algébrique affine.

Par ailleurs, on a

$$\mathbf{V} \cup \mathbf{W} = \mathbf{V}(f_i g_j \mid i \in [\![1, s]\!],\ j \in [\![1, t]\!]).$$

Un élément de $\mathbf{V}$ annule tous les polynômes f_i, il annulent donc tous les polynômes $f_i g_j$. Ainsi $\mathbf{V}$ est un sous-ensemble de $\mathbf{V}(f_i g_j)$. On montre de la même façon, que $\mathbf{W}$ est un sous-ensemble de $\mathbf{V}(f_i g_j)$, ainsi, $\mathbf{V} \cup \mathbf{W} \subset \mathbf{V}(f_i g_j)$. Montrons l'inclusion réciproque. Considérons $(a_1, \ldots, a_n) \in \mathbf{V}(f_i g_j)$, on a soit $(a_1, \ldots, a_n) \in \mathbf{V}$ qui termine le raisonnement, soit $f_{i_0}(a_1, \ldots, a_n) \neq 0$, pour au moins un $i_0 \in [\![1, s]\!]$. Comme $f_{i_0} g_j(a_1, \ldots, a_n) = 0$, pour tout j, alors $g_j(a_1, \ldots, a_n) = 0$, pour tout j, ainsi $(a_1, \ldots, a_n) \in \mathbf{W}$. Par suite, $\mathbf{V}(f_i g_j) \subset \mathbf{V} \cup \mathbf{W}$. □

De ce résultat, on déduit

III.5 Proposition. — Toute intersection finie et toute réunion finie d'ensembles algébriques affines est un ensemble algébrique affine.

III.2.8. Exemples.— L'ensemble algébrique affine suivant

$$\mathbf{V}(x^2 + z^2 - 1, x^2 + y^2 + (z-1)^2 - 1)$$

est l'intersection de la sphère de rayon 1 centrée en $(0, 0, 1)$ et du cylindre de rayon 1 centré sur l'axe des y.

L'ensemble algébrique affine

$$\mathbf{V}((x^2 + z^2 - 1)(x^2 + y^2 + (z-1)^2 - 1))$$

est la réunion des mêmes sphère et cylindre.

Exercice 13. — Montrer que tout sous-ensemble fini de $\mathbb{K}^n$ est un ensemble algébrique affine.

Exercice 14. — Décrire et tracer l'ensemble algébrique affine défini par

$$\mathbf{V}(x^2 + z^2 - 1, x^2 + y^2 + z^2 - 1).$$

§ 3 Les idéaux

Définition III.6. — Un sous-ensemble I de $\mathbb{K}[x_1,\ldots,x_n]$ est un *idéal* s'il satisfait aux assertions suivantes :

i) $0 \in I$,

ii) si $f,g \in I$, alors $f+g \in I$,

iii) si $f \in I$ and $h \in \mathbb{K}[x_1,\ldots,x_n]$, alors $hf \in I$.

III.3.1. Idéal engendré par une famille de polynômes.— Soient $f_1,\ldots,f_s$ des polynômes de $\mathbb{K}[x_1,\ldots,x_n]$. On notera

$$\langle f_1,\ldots,f_s\rangle = \left\{ \sum_{i=1}^{s} h_i f_i \;\middle|\; h_i \in \mathbb{K}[x_1,\ldots,x_n] \right\}$$

III.7 Proposition. — L'ensemble $\langle f_1,\ldots,f_s\rangle$ forme un idéal de $\mathbb{K}[x_1,\ldots,x_n]$.

Preuve. L'idéal $\langle f_1,\ldots,f_s\rangle$ contient le polynôme nul, car

$$0 = 0f_1 + 0f_2 + \ldots + 0f_s.$$

Soient $f = \sum_{i=1}^{s} h_i f_i$ et $g = \sum_{i=1}^{s} k_i f_i$, alors

$$f+g = \sum_{i=1}^{s} (h_i+k_i) f_i \in I,$$

et si en outre $h \in \mathbb{K}[x_1,\ldots,x_n]$, on a

$$hf = \sum_{i=1}^{s} hh_i f_i \in I.$$

Ainsi, $\langle f_1,\ldots,f_s\rangle$ est un idéal. □

Définition III.8. — L'idéal $\langle f_1,\ldots,f_s\rangle$ est appelé l'*idéal engendré* par $f_1,\ldots,f_s$.

III.3.2. Idéal de type fini.— On dit qu'un idéal I de $\mathbb{K}[x_1,\ldots,x_n]$ est *finiment engendré*, ou de *type fini*, s'il existe des polynômes $f_1,\ldots,f_s \in \mathbb{K}[x_1,\ldots,x_n]$, tels que $I = \langle f_1,\ldots,f_s\rangle$. On dit alors que les polynômes $f_1,\ldots,f_s$ forment une *base* de l'idéal I. Nous verrons plus loin, que tout idéal de $\mathbb{K}[x_1,\ldots,x_n]$ est finiment engendré, ce résultat est appelé le théorème de la base de Hilbert.

III.9 Proposition.— Soient $f_1, \ldots, f_s$ et $g_1, \ldots, g_t$ des polynômes de $\mathbb{K}[x_1, \ldots, x_n]$ tels que

$$\langle f_1, \ldots, f_s \rangle = \langle g_1, \ldots, g_t \rangle ,$$

alors $\mathbf{V}(f_1, \ldots, f_s) = \mathbf{V}(g_1, \ldots, g_t)$.

Preuve. Supposons que $\langle f_1, \ldots, f_s \rangle = \langle g_1, \ldots, g_t \rangle$. Soit $(a_1, \ldots, a_n) \in \mathbf{V}(f_1, \ldots, f_s)$, comme pour tout $j \in [\![1, t]\!]$, il existe une décomposition

$$g_j = h_1 f_1 + \ldots + h_s f_s,$$

on a $g_j(a_1, \ldots, a_n) = 0$. On montre ainsi que $\mathbf{V}(f_1, \ldots, f_s) \subset \mathbf{V}(g_1, \ldots, g_t)$. L'inclusion réciproque se montre de la même façon. □

Exercice 15.— Soit I un idéal de $\mathbb{K}[x_1, \ldots, x_n]$ et soient $f_1, \ldots, f_s$ des polynômes de $\mathbb{K}[x_1, \ldots, x_n]$. Montrer que les deux assertions suivantes sont équivalentes

i) $f_1, \ldots, f_s \in I$,

ii) $\langle f_1, \ldots, f_s \rangle \subset I$.

Exercice 16.— Montrer les égalités des idéaux suivants de $\mathbb{Q}[x, y]$,

1. $\langle x + y, x - y \rangle = \langle x, y \rangle$,

2. $\left\langle x + xy, y + xy, x^2, y^2 \right\rangle = \langle x, y \rangle$,

3. $\left\langle 2x^2 + 3y^2 - 11, x^2 - y^2 - 3 \right\rangle = \left\langle x^2 - 4, y^2 - 1 \right\rangle$.

III.3.3. Idéal d'un ensemble algébrique affine.— Soit $\mathbf{V}$ un ensemble algébrique affine de $\mathbb{K}^n$. On pose

$$I(\mathbf{V}) = \{ f \in \mathbb{K}[x_1, \ldots, x_n] \mid f(a_1, \ldots, a_n) = 0 \text{ pour tout } (a_1, \ldots, a_n) \in \mathbf{V} \} .$$

III.10 Proposition.— Ainsi défini, l'ensemble $I(\mathbf{V})$ est un idéal.

Preuve. L'ensemble $I(\mathbf{V})$ contient le polynôme nul, car il s'annule sur tous les points de $\mathbb{K}^n$, donc en particulier sur tous les points de $\mathbf{V}$. Soient f et g deux polynômes de $I(\mathbf{V})$, pour tout point $(a_1, \ldots, a_n)$ de $\mathbf{V}$, on a

$$(f + g)(a_1, \ldots, a_n) = f(a_1, \ldots, a_n) + g(a_1, \ldots, a_n) = 0 + 0 = 0.$$

Ainsi $f + g$ est un polynôme de $I(\mathbf{V})$. Si de plus $h \in \mathbb{K}[x_1, \ldots, x_n]$, on a

$$(hf)(a_1, \ldots, a_n) = h(a_1, \ldots, a_n) f(a_1, \ldots, a_n) = 0.$$

D'où $hf \in I(\mathbf{V})$. Ainsi $I(\mathbf{V})$ est un idéal. □

Définition III.11.— L'idéal $I(\mathbf{V})$ est appelé l'*idéal de l'ensemble algébrique affine* $\mathbf{V}$.

L'idée avec cette notion est d'associer à l'ensemble algébrique affine $\mathbf{V}$, objet de nature géométrique, un objet algébrique $I(\mathbf{V})$ afin de traduire les propriétés géométriques sous forme algébrique.

Exercice 17.— Montrer que $I(\mathbf{V}(x^n, y^m)) = \langle x, y\rangle$.

III.3.4. Relation entre idéaux et ensembles algébriques affines.— Considérons une famille de polynômes de $\mathbb{K}[x_1, \ldots, x_n]$:

$$f_1, \ldots, f_s.$$

On peut construire l'ensemble algébrique affine engendré par ces polynômes

$$\mathbf{V}(f_1, \ldots, f_s),$$

puis l'idéal de l'ensemble algébrique affine

$$I(\mathbf{V}(f_1, \ldots, f_s)).$$

Une question naturelle est : a-t-on

$$I(\mathbf{V}(f_1, \ldots, f_s)) = \langle f_1, \ldots, f_s\rangle ?$$

La réponse est négative en général :

III.12 Proposition.— Si $f_1, \ldots, f_s$ sont des polynômes de $\mathbb{K}[x_1, \ldots, x_n]$, alors

$$\langle f_1, \ldots, f_s\rangle \subset I(\mathbf{V}(f_1, \ldots, f_s)), \tag{III.1}$$

de plus, cette inclusion est stricte en général.

Preuve. Soit $f \in \langle f_1, \ldots, f_s\rangle$, alors il existe une décomposition

$$f = h_1 f_1 + \ldots + h_s f_s,$$

où les h_i sont des polynômes de $\mathbb{K}[x_1, \ldots, x_n]$. Pour tout $(a_1, \ldots, a_n) \in \mathbf{V}(f_1, \ldots, f_s)$, on a $f_i(a_1, \ldots, a_n) = 0$, pour tout $i \in [\![1, s]\!]$, par suite $f(a_1, \ldots, a_n) = 0$. Ainsi f s'annule sur tous les points de $\mathbf{V}(f_1, \ldots, f_s)$, ce qui entraîne que $f \in I(\mathbf{V}(f_1, \ldots, f_s))$.

Pour montrer que l'inclusion est stricte, il suffit de considérer l'exemple suivant

$$\left\langle x^2, y^2 \right\rangle \subset I(\mathbf{V}(x^2, y^2)).$$

Or $\mathbf{V}(x^2, y^2) = \{(0,0)\}$, car c'est l'ensemble des (x, y) tels que $x^2 = y^2 = 0$. Ainsi $I(\mathbf{V}(x^2, y^2)) = \langle x, y\rangle$. L'inclusion est stricte, car le polynôme x ne peut pas s'écrire sous

la forme
$$x = h_1(x,y)x^2 + h_2(x,y)y^2.$$

□

Exercice 18.— Montrer que l'inclusion (III.1) est stricte en considérant le polynôme $x^2 + y^2 + 1$ de $\mathbb{R}[x,y]$.

Exercice 19.— Soient $\mathbf{V}$ et $\mathbf{W}$ des ensembles algébriques affines de $\mathbb{K}^n$.

1. Montrer que $\mathbf{V} \subset \mathbf{W}$ si, et seulement si, $I(\mathbf{W}) \subset I(\mathbf{V})$.
2. Montrer que $\mathbf{V} = \mathbf{W}$ si, et seulement si, $I(\mathbf{V}) = I(\mathbf{W})$.

III.3.5. Problèmes.— Voici des problèmes que nous allons aborder dans la suite de ce cours.

a) Problème de la description d'un idéal :

- est-ce que tout idéal I de $\mathbb{K}[x_1,\ldots,x_n]$ possède un nombre fini de générateurs ? Autrement dit, existe-t-il une famille de polynômes $f_1,\ldots,f_s$ tels que $I = \langle f_1,\ldots,f_s\rangle$?
- si oui, comment déterminer une telle famille génératrice ?
- existe-t-il une famille génératrice « plus intéressante » que les autres ?

b) Problème de l'appartenance à un idéal :

étant donné un idéal $I = \langle f_1,\ldots,f_s\rangle$ et un polynôme f de $\mathbb{K}[x_1,\ldots,x_n]$, déterminer si $f \in I$.

c) Problème de la résolution d'équations polynomiales :

étant donnés des polynômes $f_1,\ldots,f_s$ de $\mathbb{K}[x_1,\ldots,x_s]$, trouver les solutions dans $\mathbb{K}^n$ du système d'équations polynomiales

$$\begin{cases} f_1(x_1,\ldots,x_n) = 0 \\ \qquad \vdots \\ f_s(x_1,\ldots,x_n) = 0 \end{cases}$$

d) Problème d'impliciter une présentation paramétrée : *étant donné un paramétrage*
$$x_i = g_i(t_1,\ldots,t_m), \quad i \in [\![1,n]\!], \quad g_i \in \mathbb{K}[x_1,\ldots,x_m],$$
d'un ensemble algébrique affine $\mathbf{V}$ de $\mathbb{K}^n$, déterminer des polynômes $f_1,\ldots,f_s$ de $\mathbb{K}[x_1,\ldots,x_n]$, tels que
$$\mathbf{V} = \mathbf{V}(f_1,\ldots,f_s).$$