

Préliminaires algébriques

Sommaire

1.	Ensembles et applications	3
2.	Les corps	4
3.	Les anneaux	6
4.	Les polynômes à une indéterminée	10
5.	Arithmétique des polynômes	13
6.	Les relations d'ordre	19

Ce chapitre contient peu de démonstrations, son rôle est de fixer les notations et de rappeler les structures algébriques fondamentales, ainsi que les principaux résultats algébriques que nous utiliserons dans ce cours. Nous renvoyons le lecteur au cours de première année pour tout approfondissement.

§ 1 Ensembles et applications

I.1.1. Applications.— Soient A et B deux ensembles. Une *application* f de A dans B est un procédé qui à tout élément x de A associe un élément unique de B , noté $f(x)$. On note $f : A \longrightarrow B$, ou $A \xrightarrow{f} B$, ou encore

$$\begin{aligned} f : A &\longrightarrow B \\ x &\longrightarrow f(x). \end{aligned}$$

On note $f(A)$ l'image de l'ensemble A , définie par

$$f(A) = \{y \mid y \in B, \exists x \in A, \text{ tel que } y = f(x)\}.$$

L'image inverse d'un sous-ensemble $Y \subset B$ est définie par

$$f^{-1}(Y) = \{x \mid x \in A, f(x) \in Y\}.$$

Une application $f : A \longrightarrow B$ est dite *injective* si pour tout $x, y \in A$, on a $f(x) = f(y)$ implique $x = y$. Elle est dite *surjective* si $f(A) = B$, i.e., pour tout $y \in B$, il existe un $x \in A$ tel que $y = f(x)$. Une application est dite *bijjective* si elle est à la fois injective et surjective.

Si $f : A \longrightarrow B$ et $g : B \longrightarrow C$ sont deux applications, on note $g \circ f$, ou encore gf , l'application, dite *composée*, définie par

$$\begin{aligned} g \circ f : A &\longrightarrow C \\ x &\longrightarrow g(f(x)). \end{aligned}$$

La composée des applications est une opération associative, i.e., étant données trois applications $A \xrightarrow{f} B \xrightarrow{g} C \xrightarrow{h} D$, on a

$$h \circ (g \circ f) = (h \circ g) \circ f.$$

I.1.2. Ensembles de nombres.— Dans tout ce cours, nous supposons connus les ensembles de nombres suivants et les opérations d'addition, de soustraction, de multiplication et de division sur ces ensembles :

- l'ensemble des entiers naturels, $0, 1, 2, \dots$, noté $\mathbb{N}$,
- l'ensemble des entiers relatifs, noté $\mathbb{Z}$, formé des entiers naturels et de leurs opposés, $-1, -2, \dots$,
- l'ensemble des rationnels, noté $\mathbb{Q}$, formé des quotients $\frac{p}{q}$, où p et q sont des entiers relatifs, avec q non nul,
- l'ensemble des réels, noté $\mathbb{R}$, qui contient les nombres rationnels et les nombres irrationnels,
- l'ensemble des complexes, noté $\mathbb{C}$, formé des nombres $a + ib$, où a et b sont des réels et i un complexe vérifiant $i^2 = -1$.

Si p et q sont deux entiers relatifs, on notera

$$[p, q] = \{a \in \mathbb{Z} \mid p \leq a \leq q\}.$$

§ 2 Les corps

Un *corps* est un objet algébrique constitué d'un ensemble et de deux opérations sur cet ensemble, une addition et une multiplication, qui satisfont à certaines relations. Intuitivement, cette structure est proche de notre intuition de nombres et des opérations que l'on peut leur appliquer. Avant d'énoncer les relations des deux opérations de la structure de corps, rappelons la structure de groupe.

I.2.1. Les groupes.— Un *groupe* est un ensemble G muni d'une opération $\star$, associant à deux éléments a et b de G un troisième élément de G , noté $a \star b$, satisfaisant les assertions suivantes

i) l'opération est *associative*, i.e., pour tous éléments a, b et c de G ,

$$a \star (b \star c) = (a \star b) \star c,$$

ii) il existe un élément e dans G , appelé *neutre*, tel que, pour tout élément a de G ,

$$a \star e = e \star a = a,$$

iii) pour tout élément a de G , il existe un élément *inverse*, que nous noterons a^{-1} , tel que

$$a \star a^{-1} = e = a^{-1} \star a.$$

Exercice 1.—

1. Montrer qu'un groupe possède un unique élément neutre.
2. Montrer que dans un groupe, l'inverse d'un élément est unique.

I.2.2. Exemples.—

- 1) Le groupe *trivial* est le groupe à un seul élément, l'élément neutre.
- 2) L'ensemble des entiers $\mathbb{Z}$ forme un groupe pour l'addition usuelle. Il ne forme pas un groupe pour la multiplication.
- 3) L'ensemble des nombres rationnels $\mathbb{Q}$ forme un groupe pour l'addition. L'ensemble $\mathbb{Q} - \{0\}$ des nombres rationnels non nul est un groupe pour la multiplication.
- 4) L'ensemble des complexes non nuls $\mathbb{C} - \{0\}$, muni de la multiplication usuelle des complexes.
- 5) L'ensemble $\mathbb{R}^n$ des n -uplets ordonnées

$$(x_1, \dots, x_n)$$

de nombres réels, muni de l'opération

$$(x_1, \dots, x_n) + (y_1, \dots, y_n) = (x_1 + y_1, \dots, x_n + y_n),$$

forme un groupe.

Exercice 2.— Justifier toutes les propriétés précédentes. Dans le cas de $\mathbb{R}^n$, déterminer l'élément neutre du groupe et l'inverse d'un n -uplet $(x_1, \dots, x_n)$.

I.2.3. Les groupes abéliens.— Un groupe est dit *abélien*, ou *commutatif*, si tous éléments a et b vérifient

$$a \star b = b \star a.$$

Les groupes des exemples I.2.2 sont abéliens.

Exercice 3.— Soit X un ensemble.

1. Montrer que l'ensemble des permutations de X , i.e. des bijections de X dans lui-même, forment un groupe.
2. Montrer que ce groupe n'est pas commutatif lorsque X possède au moins trois éléments.

I.2.4. Les corps.— Un *corps* (commutatif) est un ensemble $\mathbb{K}$ sur lequel une opération d'addition $(a, b) \rightarrow a + b$ et une opération de multiplication $(a, b) \rightarrow ab$ sont définies et satisfont aux assertions suivantes :

- i) $\mathbb{K}$ est un groupe abélien pour l'addition,
- ii) $\mathbb{K} - \{0\}$ est un groupe abélien pour la multiplication,
- iii) la multiplication est distributive par rapport à l'addition, i.e., pour tous éléments a, b et c , on a

$$a(b + c) = ab + ac.$$

L'élément neutre pour l'addition, appelé *zero*, est noté 0, l'inverse de a est appelé l'*opposé* de a et noté $-a$, l'élément neutre pour la multiplication est appelé *unité* et noté 1, l'*inverse* de a pour la multiplication est noté a^{-1} .

I.2.5. Exemples.—

- 1) L'ensemble des nombres rationnels $\mathbb{Q}$, l'ensemble des nombres réels $\mathbb{R}$ et l'ensemble des nombres complexes $\mathbb{C}$, munis des opérations d'addition et de multiplication usuelles sont des corps.
- 2) L'ensemble $\mathbb{Z}$ des entiers relatifs n'est pas un corps.
- 3) Un exemple de corps fini, i.e., avec un nombre fini d'éléments, est donné par l'ensemble, noté $\mathbb{Z}/p\mathbb{Z}$, des entiers modulo un entier premier p , muni des opérations d'addition et de multiplication induites de celles de $\mathbb{Z}$.

Exercice 4. — Montrer que $\mathbb{Z}/4\mathbb{Z}$ n'est pas un corps.

Exercice 5. — Montrer que dans un corps, l'élément neutre de l'addition joue le rôle d'*annulateur*, i.e., pour tout élément a , on a :

$$a0 = 0.$$

Par définition, un groupe ne peut être vide, il contient au moins un élément. Un corps contient donc au moins deux éléments 0 et 1 qui sont nécessairement distincts.

Exercice 6. — Montrer qu'un corps ne contient pas de diviseur de zero, c'est-à-dire que si a et b sont deux éléments non nul d'un corps $\mathbb{K}$, alors leur produit ab est non nul.

Il n'existe qu'un seul corps à deux éléments (à isomorphisme près), noté $\mathbb{F}_2$.

Exercice 7. — Établir les tables d'addition et de multiplication du corps à deux éléments.

I.2.6. Extension de corps. — Un sous-ensemble $\mathbb{L}$ d'un corps $\mathbb{K}$ est un *sous-corps* de $\mathbb{K}$ si les opérations du corps $\mathbb{K}$ munissent $\mathbb{L}$ d'une structure de corps. On dit alors que $\mathbb{K}$ est une *extension* du corps $\mathbb{L}$. Par exemple, le corps des réels $\mathbb{R}$ est une extension du corps des rationnels $\mathbb{Q}$ et le corps des complexes $\mathbb{C}$ est une extension du corps $\mathbb{R}$.

§ 3 Les anneaux

La structure d'anneau généralise celle de corps. Un ensemble muni d'une opération d'addition et d'une opération de multiplication qui satisfont à tous les axiomes de corps, excepté l'existence d'un élément inverse a^{-1} , pour tout élément a non nul, est appelé un *anneau commutatif*. Pour que notre définition soit complète, on convient, qu'il existe un anneau qui possède un seul élément.

Par exemple, l'ensemble des entiers relatifs $\mathbb{Z}$, muni de l'addition et de la multiplication, n'est pas un corps - les éléments non nuls ne sont pas tous inversibles - mais il forme un anneau commutatif. Nous verrons que l'ensemble $A[x]$ des polynômes à une indéterminée à coefficients dans un anneau ou un corps A forme un anneau ; les principales constructions sur les anneaux de polynômes sont rappelées dans la section suivante.

I.3.1. Les anneaux. — Un *anneau* est un ensemble A muni d'une opération d'*addition* $(a, b) \rightarrow a + b$ et d'une opération de *multiplication* $(a, b) \rightarrow ab$ qui satisfont aux assertions suivantes

- i) A est un groupe abélien pour l'addition,
- ii) la multiplication est associative, i.e., pour tous éléments a, b et c de A ,

$$(ab)c = a(bc).$$

- iii) la multiplication possède un élément neutre dans A , appelé *unité* et noté 1, vérifiant pour tout élément a de A ,

$$1a = a1 = a.$$

- iv) la multiplication est *distributive* par rapport à l'addition, i.e., pour tous éléments a, b, c de A , on a :

$$a(b + c) = ab + ac, \quad (b + c)a = ba + ca.$$

Un anneau est dit *commutatif* si sa multiplication est commutative.

Exercice 8. — Montrer que dans un anneau A , on a, pour tous éléments a et b ,

1. $0a = a0 = 0$,
2. $(-1)a = -a$,
3. $-(ab) = (-a)b = a(-b)$,
4. $(-a)(-b) = ab$.

I.3.2. Exemples.—

- 1) L'ensemble des entiers relatifs $\mathbb{Z}$, muni de l'addition et de la multiplication usuelles, forme un anneau commutatif.
- 2) Un corps (commutatif) est un anneau $\mathbb{K}$ non réduit à $\{0\}$, tel que la multiplication muni $\mathbb{K} - \{0\}$ d'une structure de groupe abélien.
- 3) Si $1 = 0$ dans un anneau A , alors A est réduit à $\{0\}$, car pour tout élément a de A , $a = 1a = 0a = 0$.

I.3.3. Endomorphismes d'un groupe abélien. — Rappelons qu'un *endomorphisme* d'un groupe $(G, \star)$ est un morphisme de groupes de G dans lui-même, c'est-à-dire, une application $f : G \rightarrow G$ vérifiant, pour tous $a, b \in G$,

$$f(a \star b) = f(a) \star f(b).$$

L'ensemble des endomorphismes d'un groupe abélien $(G, +)$, muni de l'addition induite de celle sur G et de la composition, est un anneau non commutatif en général.

I.3.4. Formule du binôme. — Dans un anneau, si deux éléments a et b commutent, i.e., $ab = ba$, alors on a la formule dite du *binôme de Newton*, pour tout entier naturel n ,

$$(a + b)^n = \sum_{p=0}^n \binom{n}{p} a^p b^{n-p}.$$

Exercice 9. — Démontrer la formule du binôme de Newton.

I.3.5. Caractéristique d'un anneau commutatif.— Soit A un anneau commutatif. La *caractéristique* de A est le plus petit entier naturel non nul q , tel que l'addition de q fois l'unité soit égale à zéro :

$$q \cdot 1 = \underbrace{1 + 1 + \dots + 1}_{q \text{ fois}} = 0.$$

Si un tel entier n'existe pas, on dit que l'anneau est de caractéristique nulle.

Exercice 10. —

1. Montrer qu'un anneau commutatif fini est de caractéristique non nulle.
2. Montrer que la caractéristique d'un corps fini est un nombre premier.

Exercice 11. — Construire un corps de caractéristique 3.

Exercice 12. — Montrer que dans un anneau commutatif de caractéristique un nombre premier p , alors, pour tous éléments a et b de A , on a

$$(a + b)^p = a^p + b^p.$$

I.3.6. Division euclidienne dans l'anneau $\mathbb{Z}$.— La *division euclidienne* est un résultat fondamental de l'arithmétique élémentaire sur les entiers ou les polynômes. Avant d'identifier les anneaux dans lesquels, un tel algorithme est disponible, rappelons la division euclidienne sur les entiers.

I.1 Théorème (division euclidienne).— Soient $a, b \in \mathbb{Z}$, avec $b > 0$. Il existe un couple unique (q, r) d'entiers dans $\mathbb{Z}$ tel que :

$$a = bq + r, \quad \text{avec } 0 \leq r < b.$$

L'entier q est appelé le *quotient* de la division euclidienne de a par b et l'entier r est appelé le *reste* de la division euclidienne de a par b .

Preuve. Montrons dans un premier temps l'unicité du couple. Supposons que (q, r) et (q', r') soient deux couples vérifiant la condition, alors

$$a = bq + r = bq' + r'.$$

D'où $r' - r = b(q - q')$, par suite b divise $r' - r$. Comme, par hypothèse, $0 \leq r < b$ et $0 \leq r' < b$, on a

$$b|q - q'| = |r' - r| < b.$$

Par suite, $|q - q'| = 0$, d'où $q = q'$ et $r = r'$.

Montrons l'existence du couple. Considérons l'ensemble $A = \{k \in \mathbb{Z} \mid bk \leq a\}$. C'est une partie non vide et majorée de $\mathbb{Z}$. En effet, si $a \geq 0$, alors $0 \in A$, d'où A est non vide, et comme $1 \leq b$, l'entier a majore A . Si $a < 0$, alors $a \in A$, d'où A est non vide et 0 majore A . Par suite, l'ensemble A admet un plus grand élément q . On a

$$bq \leq a < b(q + 1).$$

En posant $r = a - bq$, on a $0 \leq r < b$. $\square$

De l'unicité du quotient et du reste de la division euclidienne, on déduit qu'un entier b divise un entier a si, et seulement si, le reste de division euclidienne de a par b est nul.

Exercice 13. — Soit n un entier naturel. Calculer la division euclidienne de

1. l'entier $n^3 + n^2 + 2n + 1$ par $n + 1$,
2. l'entier $n^4 + 4n^3 + 6n^2$ par $n^2 + 2$.



FIGURE I.1.: Euclide de Samos (325 - 265 av. J.-C.)

Euclide est un mathématicien de la Grèce antique né vers 325 av. J.C. et mort vers 265 av. J.C.. Nous n'avons que très peu d'information sur la vie d'Euclide. L'article de Fabio Acerbi du site Image des mathématiques¹ présente ce que nous savons à ce jour sur le personnage d'Euclide. Euclide est l'auteur des Éléments qui est un texte fondateur de la géométrie.

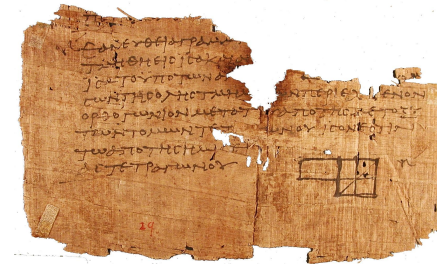


FIGURE I.2.: Un fragment des éléments d'Euclide, papyrus daté d'entre 75 et 125 de notre ère.

I.3.7. Les anneaux euclidiens.— Soit A un anneau commutatif. On appelle *algorithme euclidien* sur A toute application

$$\varphi : A - \{0\} \longrightarrow \mathbb{N},$$

telle que, pour tout $a \in A$ et tout $b \in A - \{0\}$, il existe $q \in A$ et $r \in A$, tels que

$$a = bq + r, \quad \text{avec } \varphi(r) < \varphi(b) \text{ ou } r = 0.$$

1. Fabio Acerbi, « Euclide » - Images des Mathématiques, CNRS, 2010. En ligne, URL : <http://images.math.cnrs.fr/Euclide.html>

Un anneau commutatif A est dit *euclidien*, s'il vérifie les deux propriétés suivantes

i) A est *intègre*, i.e., pour tous éléments a et b de A ,

$$ab = 0 \Rightarrow (a = 0 \text{ ou } b = 0).$$

ii) il existe sur A un algorithme euclidien.

I.3.8. Exemple.— L'anneau $\mathbb{Z}$ est euclidien. Il est en effet intègre et l'application valeur absolue $|| : \mathbb{Z} - \{0\} \rightarrow \mathbb{N}$ est un algorithme euclidien, car, pour tout $a \in \mathbb{Z}$ et tout $b \in \mathbb{Z} - \{0\}$, il existe $q, r \in \mathbb{Z}$ tels que

$$a = bq + r, \text{ avec } |r| < |b| \text{ ou } r = 0.$$

Attention, le couple (q, r) n'est pas ici unique, par exemple, on a

$$5 = (-3)(-2) + (-1) \text{ avec } |-1| < |-3|,$$

et

$$5 = (-3)(-1) + 2 \text{ avec } |2| < |-3|.$$

Dans la suite, nous montrerons que si $\mathbb{K}$ est un corps, l'anneau $\mathbb{K}[x]$ est euclidien.

Exercice 14.— Montrer que l'anneau $\mathbb{D}$ des nombres décimaux, i.e., le sous-anneau de $\mathbb{Q}$, engendré par $1/10$, est euclidien.

I.3.9. Les idéaux.— Soit A un anneau commutatif. Un sous-ensemble I de A est appelé *idéale* de A , s'il vérifie les assertions suivantes

i) $0 \in I$,

ii) si $u, v \in I$, alors $u + v \in I$,

iii) si $a \in A$ et $u \in I$, alors $au \in I$.

En particulier un idéal est un sous-groupe abélien de A pour l'addition.

Exercice 15.— Montrer que $\{0\}$ et A sont des idéaux de A .

Exercice 16.— Montrer que les idéaux de l'anneau $\mathbb{Z}$ des entiers relatifs sont les $n\mathbb{Z}$, où n est un entier naturel.

Dans la suite de ce cours, nous verrons quelques propriétés remarquables sur les idéaux des anneaux euclidiens. En particulier, nous montrerons que tout idéal d'un anneau euclidien est engendré par un élément. La notion d'idéal est centrale dans ce cours, nous la considérerons plus particulièrement dans le contexte des anneaux de polynômes à plusieurs indéterminées.

§ 4 Les polynômes à une indéterminée

I.4.1. Polynômes sur un corps.— Avant d'aborder la notion de polynôme, rappelons qu'il est important de distinguer les polynômes des fonctions polynomiales. En effet, considérons le polynôme $f = x^2 - x$ à coefficients dans le corps $\mathbb{Z}/2\mathbb{Z}$. La fonction polynomiale associée $\tilde{f} : \mathbb{Z}/2\mathbb{Z} \rightarrow \mathbb{Z}/2\mathbb{Z}$, définie par

$$\tilde{f}(a) = a^2 - a, \text{ pour tout } a \in \mathbb{Z}/2\mathbb{Z},$$

est nulle, car $\tilde{f}(0) = 0$ et $\tilde{f}(1) = 0$, alors que le polynôme f n'est pas nul.

Exercice 17.— Montrer qu'il n'existe que quatre fonctions polynomiales à coefficients dans le corps $\mathbb{Z}/2\mathbb{Z}$ et une infinité de polynômes à coefficients dans ce corps.

La situation est différente pour les polynômes à coefficients dans les corps infinis, dans ce cas, il existe une correspondance biunivoque entre les polynômes et les fonctions polynomiales, cf. section I.4.5.

I.4.2. Les polynômes.— Soit $\mathbb{K}$ un corps. On appelle *polynôme* à coefficients dans $\mathbb{K}$, toute suite $f = (a_n)_{n \in \mathbb{N}}$ d'éléments de $\mathbb{K}$, nulle à partir d'un certain rang. On note $\mathbb{K}^{(\mathbb{N})}$ l'ensemble de ces suites.

On définit sur l'ensemble $\mathbb{K}^{(\mathbb{N})}$ une addition et un produit externe par un scalaire en posant, pour tous $f = (a_n)_{n \in \mathbb{N}}$, $g = (b_n)_{n \in \mathbb{N}}$ et $\lambda \in \mathbb{K}$,

$$f + g = (a_n + b_n)_{n \in \mathbb{N}}, \quad \lambda f = (\lambda a_n)_{n \in \mathbb{N}}.$$

En outre, on définit une multiplication en posant, pour tous $f = (a_n)_{n \in \mathbb{N}}$, $g = (b_n)_{n \in \mathbb{N}}$,

$$fg = (c_n)_{n \in \mathbb{N}}, \quad \text{avec} \quad c_n = \sum_{i=0}^n a_i b_{n-i}.$$

I.4.3. L'algèbre des polynômes.— Ces trois opérations munissent l'ensemble $\mathbb{K}^{(\mathbb{N})}$ d'une structure de $\mathbb{K}$ -algèbre associative, commutative et unitaire, c'est-à-dire,

i) $\mathbb{K}^{(\mathbb{N})}$ muni de l'addition et du produit par un scalaire est un $\mathbb{K}$ -espace vectoriel,

ii) $\mathbb{K}^{(\mathbb{N})}$ muni de l'addition et de la multiplication est un anneau commutatif,

iii) pour tous $f, g \in \mathbb{K}^{(\mathbb{N})}$ et tous scalaires $\lambda, \mu \in \mathbb{K}$, on a

$$(\lambda f)(\mu g) = (\lambda \mu)(fg).$$

I.4.4. Notion d'indéterminée.— L'écriture des polynômes sous forme de suite est peu manipulable, aussi, on préfère la notation basée sur la notion d'*indéterminée*. Notons x le polynôme de $\mathbb{K}^{(\mathbb{N})}$ dont tous les termes sont nuls, sauf celui de degré 1 :

$$x = (0, 1, 0, \dots).$$

Par convention, on pose $x^0 = 1$. On définit les puissances de x par récurrence, pour tout entier k , $x^{k+1} = x x^k$. Ainsi, si $f = (a_n)_{n \in \mathbb{N}}$, on montre que

$$f = \sum_{i=0}^{+\infty} a_i x^i.$$

Les scalaires a_i sont appelés les *coefficients* du polynôme f . On montre que deux polynômes sont égaux si, et seulement si, ils ont les mêmes coefficients :

$$\sum_{k=0}^{+\infty} a_k x^k = \sum_{k=0}^{+\infty} b_k x^k \quad \text{si, et seulement si,} \quad a_k = b_k, \text{ pour tout } k \in \mathbb{N}.$$

On notera alors $\mathbb{K}[x]$ l'ensemble des *polynômes à une indéterminée* à coefficients dans le corps $\mathbb{K}$. Avec ces notations, l'addition des polynômes est définie de la façon suivante, pour

$f = \sum_{i=0}^m a_i x^i$ et $g = \sum_{j=0}^n b_j x^j$, alors

$$f + g = \sum_{k=0}^{\max\{m,n\}} (a_k + b_k) x^k,$$

avec $a_k = 0$, pour $k > m$ et $b_k = 0$ pour $k > n$. Par ailleurs, pour la multiplication, on a

$$fg = \sum_{k=0}^{m+n} \left(\sum_{\substack{i,j \geq 0 \\ i+j=k}} (a_i b_j) \right) x^k$$

I.4.5. Fonction polynomiale.— Étant donné un polynôme $f = \sum_{i=0}^n a_i x^i$ de $\mathbb{K}[x]$, on définit la fonction polynomiale associée comme l'application

$$\tilde{f} : \mathbb{K} \longrightarrow \mathbb{K},$$

qui, à tout $a \in \mathbb{K}$, associe le scalaire $f(a) \in \mathbb{K}$, obtenu en remplaçant dans l'expression de f l'indéterminée x par a .

Nous avons vu en I.4.1 que sur un corps fini, les notions de polynômes et de fonction polynomiale ne coïncident pas. Nous allons voir que c'est le cas lorsque le corps est infini, par exemple lorsque $\mathbb{K}$ est $\mathbb{R}$ ou $\mathbb{C}$.

Exercice 18.— Supposons que $\mathbb{K}$ est le corps $\mathbb{R}$ ou $\mathbb{C}$.

1. Montrer que l'application

$$\varphi : \mathbb{K}[x] \longrightarrow \mathbb{K}^{\mathbb{K}}$$

définie par $\varphi(f) = \tilde{f}$ est injective.

2. Montrer que deux polynômes à coefficients dans $\mathbb{K}$ sont égaux si, et seulement si leurs fonctions polynomiales associées sont égales.

I.4.6. Degré d'un polynôme.— Soit f un polynôme de $\mathbb{K}[x]$. Si $f = 0$, on pose $\deg(f) = -\infty$, si $f = \sum_{i=0}^m a_i x^i$ est non nul, on note $\deg(f)$ le plus grand entier naturel n tel que a_n soit non nul. L'entier $\deg(f)$ est appelé le *degré* du polynôme f .

Un polynôme non nul f de degré $n \geq 0$ s'écrit de façon unique sous la forme

$$f = a_0 + a_1 x + \dots + a_n x^n,$$

où a_n est non nul. Le degré de f est le plus grand exposant de x apparaissant dans f .

I.4.7. Les monômes.— On appellera *monôme* un polynôme de la forme x^k , où k est un entier naturel. La famille de monômes $(x^n)_{n \in \mathbb{N}}$ forme une base du $\mathbb{K}$ -espace vectoriel $\mathbb{K}[x]$. On l'appelle base canonique de $\mathbb{K}[x]$.

I.4.8. Terme de plus haut degré.— Le *coefficient de plus haut degré* (*leading coefficient*) d'un polynôme f de $\mathbb{K}[x]$, noté $\text{lc}(f)$, est le coefficient du monôme de plus grand exposant. Le *terme*

de plus haut degré d'un polynôme f (*leading term*), noté $\text{lt}(f)$, est le terme de plus haut degré de f . Par exemple, pour le polynôme $f = a_0 + a_1 x + \dots + a_n x^n$, on a

$$\deg(f) = n, \quad \text{lt}(f) = a_n x^n, \quad \text{lc}(f) = a_n.$$

Un polynôme est dit *unitaire*, si le coefficient de son terme de plus haut degré est égal à 1.

Exercice 19.— Montrer que pour tous polynômes f et g de $\mathbb{K}[x]$, on a

1. $\text{lc}(fg) = \text{lc}(f)\text{lc}(g)$,
2. $\text{lt}(fg) = \text{lt}(f)\text{lt}(g)$.

§ 5 Arithmétique des polynômes

I.5.1. Divisibilité.— Soient f et g deux polynômes de $\mathbb{K}[x]$. On dit que g *divise* f , ou que f est *divisible* par g , ou encore que f est un multiple de g , s'il existe un polynôme q de $\mathbb{K}[x]$ tel que $f = gq$. On note alors $g|f$.

Exercice 20.— Montrer que le polynôme $x+3$ divise le polynôme x^3+27 .

Exercice 21.— Montrer que pour deux polynômes f et g non nuls de $\mathbb{K}[x]$, $\deg(f) \leq \deg(g)$ si, et seulement si, $\text{lt}(f) | \text{lt}(g)$.

Exercice 22.— Soient f et g deux polynômes de $\mathbb{K}[x]$. Montrer que $f|g$ et $g|f$ si, et seulement si, il existe un scalaire non nul λ de $\mathbb{K}$ tel que $f = \lambda g$.

I.5.2. La division euclidienne dans $\mathbb{K}[x]$.— Il existe sur l'anneau $\mathbb{K}[x]$ une division euclidienne comme celle que nous avons vue sur l'anneau $\mathbb{Z}$. Par exemple, considérons deux polynômes

$$f = x^3 - 3x^2 + 4x + 7, \quad g = 2x^2 + 4x + 6,$$

de $\mathbb{Q}[x]$. La division de f par g a pour quotient $\frac{1}{2}x - \frac{5}{2}$ et pour reste $11x + 22$. On les obtient en procédant de la même façon que la division des entiers :

$$\begin{array}{r|l} x^3 - 3x^2 + 4x + 7 & 2x^2 + 4x + 6 \\ \hline x^3 + 2x^2 + 3x & \frac{1}{2}x - \frac{5}{2} \\ \hline -5x^2 + x + 7 & \\ -5x^2 - 10x - 15 & \\ \hline 11x + 22 & \end{array}$$

La première étape consiste à multiplier le polynôme g par $\frac{1}{2}x$, puis à soustraire le résultat à f , soit

$$f - \frac{x^3}{2x^2}g = f - \frac{1}{2}xg = -5x^2 + x + 7.$$

L'idée consiste à multiplier g par un terme, ici $\frac{x^3}{2x^2}$, de telle façon que le terme de plus haut degré de g multiplié par ce terme annule le terme de plus haut degré de f . On obtient ainsi un nouveau polynôme $h = -5x^2 + x + 7$, on dit que h est une *réduction* de f par g , on note

$$f \xrightarrow{g} h.$$

On répète alors ce processus, jusqu'à obtenir le reste

$$r = h - \left(-\frac{5}{2}\right)g = 11x + 22.$$

La division se compose ainsi d'une suite de réductions par g :

$$f \xrightarrow{g} h \xrightarrow{g} r.$$

I.5.3. Le cas général.— Plus généralement, considérons deux polynômes

$$f = a_n x^n + \dots + a_1 x + a_0, \quad g = b_m x^m + \dots + b_1 x + b_0,$$

avec $\deg(f) = n \geq \deg(g) = m$. La première étape dans la division de f par g consiste à soustraire à f le produit

$$\frac{a_n}{b_m} x^{n-m} g,$$

qui, avec les notations définies en I.4.8, s'écrit

$$\frac{\text{lt}(f)}{\text{lt}(g)} g.$$

On obtient ainsi comme premier reste le polynôme

$$h = f - \frac{\text{lt}(f)}{\text{lt}(g)} g.$$

On dit que f se *réduit* en h par g , on note

$$f \xrightarrow{g} h.$$

On répète alors l'opération de réduction par g , pour obtenir un nouveau reste :

$$h' = h - \frac{\text{lt}(h)}{\text{lt}(g)} g.$$

Dans la réduction $f \xrightarrow{g} h$, on notera que le reste h a un degré strictement inférieur au degré de f . On peut alors poursuivre le processus de réduction, jusqu'à obtenir un reste, dont le degré est strictement inférieur au degré du polynôme g . On obtient ainsi une suite de réductions par g qui termine sur un reste r , tel que $\deg(r) < \deg(g)$:

$$f \xrightarrow{g} h \xrightarrow{g} h' \xrightarrow{g} \dots \xrightarrow{g} r.$$

On montre ainsi l'existence du quotient et du reste dans le théorème suivant :

I.2 Théorème (division euclidienne).— Soient f et g deux polynômes de $\mathbb{K}[x]$, avec $g \neq 0$. Il existe un couple unique (q, r) de polynômes de $\mathbb{K}[x]$ tel que :

$$f = gq + r,$$

avec $\deg(r) < \deg(g)$.

Le polynôme q est appelé le *quotient* de la division euclidienne de f par g et le polynôme r est appelé le *reste* de la division euclidienne de f par g . Si le reste de la division euclidienne de f par g est nul, alors le polynôme g divise f .

Exercice 23.— Montrer l'unicité des polynômes q et r .

Exercice 24.— Étant donnés deux éléments distincts a et b d'un corps $\mathbb{K}$. Calculer le reste de la division euclidienne d'un polynôme f de $\mathbb{K}[x]$ par le polynôme $(x-a)(x-b)$ en fonction de $f(a)$ et $f(b)$.

Exercice 25.— Calculer le reste de la division de f par g avec

1. $f = x^3 + x^2 + x + 1, \quad g = x + 1,$
2. $f = x^3 + x^2 + x + 1, \quad g = x - 1,$
3. $f = x^3 + 3x^2 - 7x + 5, \quad g = x^2 - 3,$
4. $f = x^4 + 2x^3 - 4x^2 + 5, \quad g = x^3 + 5.$

I.3 Théorème.— Si $\mathbb{K}$ est un corps, l'anneau $\mathbb{K}[x]$ est euclidien.

Preuve. D'après le théorème I.2, l'application $\deg(\cdot) : \mathbb{K}[x] - \{0\} \rightarrow \mathbb{N}$ est un algorithme euclidien sur $\mathbb{K}[x]$. $\square$

ENTRÉE : $f, g \in \mathbb{K}[x]$ avec $g \neq 0$,

SORTIE : $q, r \in \mathbb{K}[x]$ tels que $f = gq + r$ avec $(r = 0 \text{ ou } \deg(r) < \deg(g))$.

INITIALISATION : $q := 0; r := f$

TANT QUE : $r \neq 0$ **ET** $\deg(g) \leq \deg(r)$ **FAIRE**

$$q := q + \frac{\text{lt}(r)}{\text{lt}(g)}$$

$$r := r - \frac{\text{lt}(r)}{\text{lt}(g)} g.$$

Algorithme de la division des polynômes d'une indéterminée.

Nous reviendrons sur cet algorithme de la division dans un prochain chapitre, en particulier pour ses nombreuses applications.

I.5.4. Polynômes premiers entre eux.— Deux polynômes sont dits *premiers entre eux*, si leurs seuls diviseurs communs sont les polynômes de degré nul. Plus généralement, des polynômes $f_1, \dots, f_s$ de $\mathbb{K}[x]$ sont dits

- *premiers entre eux dans leur ensemble*, si les seuls polynômes qui divisent simultanément les polynômes $f_1, \dots, f_s$ sont de degré nul,
- *premiers entre eux deux à deux*, si, pour tout i différent de j , les polynômes f_i et f_j sont premiers entre eux.

Si f_i et f_j sont premiers entre eux, alors les polynômes $f_1, \dots, f_i, \dots, f_j, \dots, f_s$ sont premier entre eux dans leur ensemble. Attention, les polynômes $f_1 = x - 1$, $f_2 = (x - 1)(x - 2)$ et $f_3 = x - 3$ sont premiers entre eux dans leur ensemble, alors que les polynômes f_1 et f_2 ne sont pas premiers entre eux.

I.4 Théorème (Identité de Bézout). — Les polynômes $f_1, \dots, f_s \in \mathbb{K}[x]$ sont premiers entre eux dans leur ensemble si, et seulement si, il existe des polynômes $u_1, \dots, u_s$ de $\mathbb{K}[x]$, tels que

$$u_1 f_1 + \dots + u_s f_s = 1.$$

L'égalité $u_1 f_1 + \dots + u_s f_s = 1$ s'appelle une *identité de Bézout*.

I.5.5. Exemples. — Les polynômes $x - 1$ et $x + 2$ sont premiers entre eux, on a l'identité de Bézout

$$-\frac{1}{3}(x - 1) + \frac{1}{3}(x + 2) = 1.$$

Les polynômes $x^2 - 1$ et $x + 2$ sont premiers entre eux, une identité de Bézout est donnée par

$$\frac{1}{3}(x^2 - 1) + \left(-\frac{1}{3}x + \frac{2}{3}\right)(x + 2) = 1.$$

I.5.6. Calculer une identité de Bézout. — L'algorithme d'Euclide permet de calculer une identité de Bézout. Étant donnés deux polynômes f_1 et f_2 , premiers entre eux, l'algorithme suivant permet de calculer une identité de Bézout

$$u_1 f_1 + u_2 f_2 = 1.$$

Soient $f_1, f_2 \in \mathbb{K}[x] - \{0\}$ deux polynômes premiers entre eux. On pose $r_0 = f_1$, $r_1 = f_2$. On calcule les divisions euclidiennes

$$\begin{aligned} r_0 &= r_1 q_1 + r_2, & \deg(r_2) < \deg(r_1), \\ r_1 &= r_2 q_2 + r_3, & \deg(r_3) < \deg(r_2), \\ &\vdots \\ r_{n-2} &= r_{n-1} q_{n-1} + r_n, & \deg(r_n) < \deg(r_{n-1}), \end{aligned}$$

Alors, il existe $n_0 \geq 0$ tel que, pour tout $n \geq n_0$, $r_n = 0$. Les polynômes f_1 et f_2 sont premiers entre eux, par suite le dernier reste non nul r_{n_0-1} est une constante $b \in \mathbb{K} - \{0\}$. Pour déterminer u_1 et u_2 dans l'identité de Bézout, il suffit de partir de

$$r_{n_0-1} = b = r_{n_0-3} - r_{n_0-2} q_{n_0-2},$$

et en utilisant toutes les relations entre les restes, obtenir une relation de Bézout entre r_0 et r_1 , comme dans l'exemple suivant.

I.5.7. Exemple. — Les polynômes $x^4 + 1$ et $x^3 + 1$ sont premiers entre eux. On calcule la division euclidienne de $x^4 + 1$ par $x^3 + 1$:

$$x^4 + 1 = (x^3 + 1)(x) + (-x + 1),$$

on calcule alors la division euclidienne de $x^3 + 1$ par $-x + 1$:

$$x^3 + 1 = (-x + 1)(-x^2 - x - 1) + 2.$$

Le dernier reste non nul est 2, on a alors

$$\begin{aligned} 2 &= (x^3 + 1) - (-x + 1)(-x^2 - x - 1), \\ &= (x^3 + 1) - ((x^4 + 1) - (x^3 + 1)(x))(-x^2 - x - 1), \\ &= (x^3 + 1) - (x^4 + 1)(-x^2 - x - 1) + (x^3 + 1)x(-x^2 - x - 1), \\ &= (x^3 + 1)(1 - x - x^2 - x^3) + (x^4 + 1)(1 + x + x^2). \end{aligned}$$

On obtient ainsi une relation de Bézout :

$$1 = \frac{1}{2}(1 - x - x^2 - x^3)(x^3 + 1) + \frac{1}{2}(1 + x + x^2)(x^4 + 1).$$

Exercice 26. — Trouver une relation de Bézout entre les polynômes f et g , avec

1. $f = x^2 + 2x - 1$, $g = x + 2$,
2. $f = x^4 + 2x^3 - x$, $g = x^3 + 5$,
3. $f = x^2 + 2x - 1$, $g = x + 2$.

Exercice 27 (Lemme de Gauss). — Soient f, g, h des polynômes de $\mathbb{K}[x]$. Montrer que si f et g sont premiers entre eux et que f divise gh , alors f divise h .

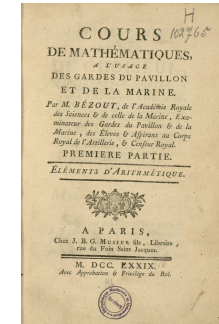


FIGURE I.3.: Étienne Bézout (1730 - 1783)

Étienne Bézout est un mathématicien français, auteur d'une *Théorie générale des équations algébriques sur la théorie de l'élimination et des fonctions symétriques sur les racines d'une équation*. Examineur des élèves du corps de l'artillerie, il rédige un *cours de mathématiques à l'usage de la marine et de l'artillerie*, qui deviendra un ouvrage de référence pour les candidats au concours d'entrée à l'École polytechnique.

I.5.8. Racine d'un polynôme. — Soit f un polynôme de $\mathbb{K}[x]$. Un scalaire $a \in \mathbb{K}$ est dit *racine* de f si $f(a) = 0$, c'est-à-dire, lorsque a est un zéro de la fonction polynomiale $\tilde{f}$. On peut dire aussi que a est racine de f si, et seulement si, $x - a$ divise f .

Si $a_1, \dots, a_p$ sont p racines distinctes de f , alors f est divisible par le polynôme

$$\prod_{i=1}^p (x - a_i).$$

Un polynôme non nul f de degré n admet au plus n racines distinctes. Si f admet n racines distinctes $a_1, \dots, a_n$, alors, il se décompose sous la forme

$$f = \text{lc}(f) \prod_{i=1}^n (x - a_i).$$

Exercice 28. — 1. Montrer les assertions ci-dessus.

2. En déduire que si f est un polynôme non nul à coefficients dans un corps K infini, alors sa fonction polynômiale associée $\tilde{f}$ n'est pas nulle.
3. Généraliser les résultats de l'exercice 18 à tout corps infini.

I.5.9. Racines multiples.— Soient f un polynôme de $\mathbb{K}[x]$ et a une racine de f . On appelle *ordre de multiplicité* de la racine a l'exposant de la plus grande puissance de $x - a$ qui divise f . Autrement dit, c'est l'entier h tel que $(x - a)^h$ divise f et $(x - a)^{h+1}$ ne divise pas f . Soit f un polynôme tel que

$$f = (x - a)^h q.$$

Alors a est racine d'ordre de multiplicité h si, et seulement si, a n'est pas racine du polynôme q .

I.5.10. Polynômes scindés.— Soit $f \in \mathbb{K}[x]$ un polynôme. On dit que f est *scindé* sur $\mathbb{K}$ s'il admet des racines $a_1, \dots, a_p$ dans $\mathbb{K}$ d'ordre de multiplicité respectifs $h_1, \dots, h_p$ telles que $h_1 + \dots + h_p = \deg(f)$. On a alors

$$f = \text{lc}(f) \prod_{i=1}^p (x - a_i)^{h_i},$$

avec $a_i \neq a_j$ si $i \neq j$ et $h_1 + \dots + h_p = \deg(f)$.

I.5 Théorème (de D'Alembert-Gauss).— Tout polynôme non constant à coefficients dans $\mathbb{C}$ possède au moins une racine dans $\mathbb{C}$.

Ce théorème est appelé aussi théorème de D'Alembert-Gauss, ou encore *théorème fondamental de l'algèbre*.

On dit qu'un corps $\mathbb{K}$ est *algébriquement clos*, si tout polynôme non constant de $\mathbb{K}[x]$ possède une racine dans $\mathbb{K}$.

Exercice 29. — Montrer que si un corps $\mathbb{K}$ est algébriquement clos alors tout polynôme non nul de $\mathbb{K}[x]$ est scindé sur $\mathbb{K}$.

I.6 Corollaire. — Tout polynôme non nul de $\mathbb{C}[x]$ est scindé sur $\mathbb{C}$.

Exercice 30. — Montrer que le corps $\mathbb{R}$ n'est pas algébriquement clos.

Soit $\mathbb{L}$ une extension d'un corps $\mathbb{K}$. On dit qu'un élément a de $\mathbb{L}$ est *algébrique* sur $\mathbb{K}$ s'il est racine d'un polynôme non nul de $\mathbb{K}[x]$. Par exemple $\sqrt{2} \in \mathbb{R}$ est algébrique sur $\mathbb{Q}$ mais $\pi \in \mathbb{R}$ ne l'est pas (théorème d'Hermite-Lindemann, 1882). On dit que $\mathbb{L}$ est une *extension algébrique* de $\mathbb{K}$ si tout élément de $\mathbb{L}$ est algébrique sur $\mathbb{K}$.

Exercice 31. — Montrer que $\mathbb{C}$ est une extension algébrique de $\mathbb{R}$.

Le corps $\mathbb{C}$ est l'unique extension algébrique² de $\mathbb{R}$ qui est algébriquement close. Plus généralement, on peut montrer que, pour tout corps $\mathbb{K}$, il existe une unique extension algébrique² $\mathbb{L}$ qui est algébriquement close. Le corps $\mathbb{L}$ est appelé la *clôture algébrique* de $\mathbb{K}$. Par exemple $\mathbb{C}$ est la clôture algébrique de $\mathbb{R}$.

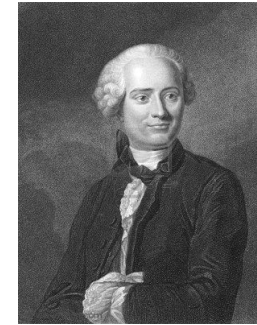


FIGURE I.4.: Jean Le Rond D'Alembert (1717 - 1783)

Jean Le Rond D'Alembert est un mathématicien, philosophe et encyclopédiste français. Il énonce le théorème de D'Alembert-Gauss dans le Traité de dynamique, qui ne sera démontré qu'un siècle après par Carl Friedrich Gauss. D'Alembert est célèbre pour ses nombreux travaux mathématiques, notamment sur les équations différentielles et les équations aux dérivées partielles. Il aborda des problèmes difficiles en physique avec le Traité de dynamique des systèmes, en astronomie avec le problème des trois corps, ou encore en musique avec la vibration des cordes.

§ 6 Les relations d'ordre

I.6.1. Relations d'ordre.— Soit E un ensemble non vide. Une *relation d'ordre* $\preccurlyeq$ sur E est une relation binaire $\preccurlyeq$ sur E satisfaisant les propriétés suivantes :

- i) *réflexivité* : pour tout $x \in E$, $x \preccurlyeq x$,
- ii) *antisymétrie* : $(x \preccurlyeq y \text{ et } y \preccurlyeq x) \Rightarrow x = y$.
- iii) *transitivité* : $(x \preccurlyeq y \text{ et } y \preccurlyeq z) \Rightarrow x \preccurlyeq z$.

Un ensemble muni d'une relation d'ordre est appelé *ensemble ordonné*.

2. unique à isomorphisme près.

I.6.2. Exemples.— La relation $\leq$ est une relation d'ordre sur l'ensemble $\mathbb{R}$ des réels. La relation de divisibilité sur les entiers naturels non nuls : $n|m$ si, et seulement si, n divise m est une relation d'ordre sur $\mathbb{N} - \{0\}$. La relation d'inclusion $\subset$ est une relation d'ordre sur l'ensemble $\mathcal{P}(E)$ des parties d'un ensemble E .

I.6.3. Ordre total.— Une relation d'ordre $\preceq$ sur E est dite *totale* si deux éléments de E sont toujours comparables par la relation d'ordre :

iv) pour tous $x, y \in E$, $x \preceq y$ ou $y \preceq x$.

On dit alors que l'ensemble est *totalelement ordonné*. Par exemple l'ensemble $(\mathbb{N}, \leq)$ est totalelement ordonné.

Exercice 32.—

1. Montrer que l'ensemble $(\mathbb{N}, |)$ n'est pas totalelement ordonné.
2. Étant donné un ensemble E possédant au moins deux éléments, montrer que l'ensemble $(\mathcal{P}(E), \subset)$ n'est pas totalelement ordonné.

I.6.4. Bon ordre.— Soient $(E, \preceq)$ un ensemble ordonné, A une partie non vide de E et x un élément de E . On dit que

- x est un *majorant* de A , ou que x *major*e A , lorsque, pour tout $a \in A$, $a \preceq x$,
- x est un *minorant* de A , ou que x *minore* A , lorsque, pour tout $a \in A$, $x \preceq a$,
- x est un *plus grand élément* de A , si $x \in A$ et x est un majorant de A ,
- x est un *plus petit élément* de A , si $x \in A$ et x est un minorant de A .

Un ensemble ordonné $(E, \preceq)$ est dit *bien ordonné* et la relation $\preceq$ est appelée une *bon ordre* si la condition suivante est satisfaite :

v) toute partie non vide de E possède un plus petit élément pour la relation $\preceq$.

I.6.5. Remarque.—

- Un bon ordre ne possède pas de suite strictement décroissante infinie.
- Un bon ordre est un ordre total.
- Un ordre total qui ne possède pas de suite strictement décroissante infinie est un bon ordre.

En particulier, un ordre total est un bon ordre si et seulement s'il ne possède pas de suite strictement décroissante infinie.

I.6.6. Exemples.— On montre que l'ensemble $\mathbb{N}$ est bien ordonné par l'ordre $\leq$, c'est une conséquence de la définition de $\mathbb{N}$. L'ensemble $(\mathbb{Z}, \leq)$ n'est pas bien ordonné, car l'ensemble $\mathbb{Z}$ lui-même n'admet pas de plus petit élément. L'ensemble des réels positifs, muni de l'ordre $\leq$, n'est pas bien ordonné, l'intervalle ouvert $]0, 1[$ ne possède pas de plus petit élément.

I.6.7. Principe de récurrence sur un bon ordre.— Le principe de récurrence sur $\mathbb{N}$ s'étend aux ensembles bien ordonnés :

I.7 Proposition.— Soit un ensemble bien ordonné $(I, \preceq)$ et une famille $(P_i)_{i \in I}$ de propriétés. Si pour chaque $i \in I$, la propriété P_i est satisfaite dès que les propriétés P_j sont satisfaites pour tout $j \prec i$, alors les propriétés P_i sont satisfaites pour tout $i \in I$.

Autrement dit,

$$\text{si } \forall i \in I, (\forall j \prec i P_j) \Rightarrow P_i \text{ alors } \forall i \in I, P_i.$$

Preuve. Soit A l'ensemble des $i \in I$ tel que P_i n'est pas satisfaite. Si A est non vide, il possède un plus petit élément i_0 . La propriété P_{i_0} n'est en particulier pas satisfaite, mais par contre les propriétés P_j le sont toutes pour $j < i_0$. $\square$

Exercice 33.— Montrer la remarque I.6.5.

Exercice 34 (ordre produit).— Soit $(E, \preceq)$ un ensemble ordonné. On définit la relation $\preceq_{\text{prod}}$ sur $E \times E$ en posant

$$(x, y) \preceq_{\text{prod}} (x', y'), \quad \text{si, et seulement si, } x \preceq x' \text{ et } y \preceq y'.$$

1. Montrer que $\preceq_{\text{prod}}$ est une relation d'ordre.
2. Montrer que cette relation n'est pas totale lorsque E contient au moins deux éléments.

Exercice 35 (ordre lexicographique).— Soit $(E, \preceq)$ un ensemble ordonné. On définit la relation $\preceq_{\text{lex}}$ sur $E \times E$ en posant

$$(x, y) \preceq_{\text{lex}} (x', y'), \quad \text{si, et seulement si, } (x \preceq x' \text{ et } x \neq x') \text{ ou } (x = x' \text{ et } y \preceq y').$$

1. Montrer que $\preceq_{\text{lex}}$ est une relation d'ordre.
2. Montrer que si $\preceq$ est une relation d'ordre total sur E , alors $\preceq_{\text{lex}}$ est une relation d'ordre totale.
3. Montrer que si $\preceq$ est un bon ordre sur E , alors $\preceq_{\text{lex}}$ est un bon ordre sur $E \times E$.

Exercice 36.— On considère l'ensemble ordonné $(\mathbb{N}, \leq)$.

1. Montrer que $\preceq_{\text{prod}}$ n'est pas un bon ordre sur $\mathbb{N} \times \mathbb{N}$.
2. Montrer que $\preceq_{\text{lex}}$ est un bon ordre sur $\mathbb{N} \times \mathbb{N}$.

Exercice 37.— Soit Σ un alphabet fini (un ensemble fini de lettres totalelement ordonné, c.à.d. muni d'un ordre alphabétique) et Σ^* l'ensemble des mots sur cet alphabet (ensemble des suites finies de lettres de l'alphabet). (Par exemple, si $\Sigma = \{a, b, c\}$, alors $abac, ccbaba, bacaaccbb$ sont des mots dans Σ^* .)

1. Montrer que si Σ contient au moins deux lettres, alors l'ordre alphabétique sur Σ^* n'est pas un bon ordre.
2. Définir un bon ordre sur Σ^* .

Polynômes, ensembles algébriques affines et idéaux

Sommaire

1.	Les polynômes à plusieurs indéterminées	23
2.	Les ensembles algébriques affines	25
3.	Les idéaux	31

§ 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.

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

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

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

$$\alpha_1 + \alpha_2 + \dots + \alpha_n.$$

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.

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

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

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

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

II.1.3. Les polynômes.— Un *polynôme* f d'indéterminées $x_1, \dots, x_n$ à coefficients dans un corps $\mathbb{K}$ est une combinaison linéaire (finie) à coefficients dans $\mathbb{K}$ de monômes d'indéterminées $x_1, \dots, x_n$. 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 $\alpha = (\alpha_1, \dots, \alpha_n)$.

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

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

II.1.4. Notation.— Lorsque l'on considérera des polynômes avec un petit nombre d'indéterminées, on utilisera les lettres sans indice $x, y, z, \dots$, 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

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

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

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

- 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 maximum $|\alpha|$, 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.

II.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 :

$$(A[x_1])[x_2] \longrightarrow (A[x_2])[x_1]$$

$$\sum_{\alpha_2} \left(\sum_{\alpha_1} a_{\alpha_1, \alpha_2} x_1^{\alpha_1} \right) x_2^{\alpha_2} \longmapsto \sum_{\alpha_1} \left(\sum_{\alpha_2} a_{\alpha_1, \alpha_2} x_2^{\alpha_2} \right) x_1^{\alpha_1}$$

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

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

ses éléments sont les sommes finies

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

§ 2 Les ensembles algébriques affines

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

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

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

II.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 $\tilde{f}: \mathbb{K}^n \longrightarrow \mathbb{K}$ est la fonction nulle.

Exercice 38.— L'objectif est de montrer la proposition II.2.

1. Montrer que la fonction polynomiale du polynôme nul est la fonction nulle.

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.

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

1. Considérons le polynôme $f = x^2y + y^2x$ de $\mathbb{K}[x, y]$. Montrer que la fonction polynomiale $\tilde{f}$ 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 II.2, le résultat suivant

II.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 $\tilde{f} : \mathbb{K}^n \rightarrow \mathbb{K}$ et $\tilde{g} : \mathbb{K}^n \rightarrow \mathbb{K}$ sont égales.

Exercice 40. — Montrer la proposition II.3.

II.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*.

II.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

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

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

$$\begin{cases} f_1(a_1, \dots, a_n) = 0 \\ f_2(a_1, \dots, a_n) = 0 \\ \vdots \\ f_s(a_1, \dots, a_n) = 0 \end{cases}$$

Exercice 41. — Montrer que l'ensemble vide et l'espace affine $\mathbb{K}^n$ sont des ensembles algébriques affines.

Exercice 42. — Montrer qu'un point de $\mathbb{K}^n$ est un ensemble algébrique affine.

Exercice 43. — 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 44. — Montrer que deux polynômes différents peuvent définir le même ensemble algébrique affine.

II.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.

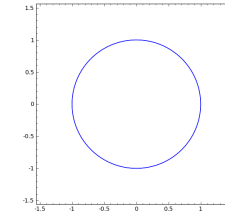


FIGURE II.1.: Cercle $\mathbf{V}(1 - x^2 - y^2)$

Les commandes Sage pour tracer la figure II.1 sont

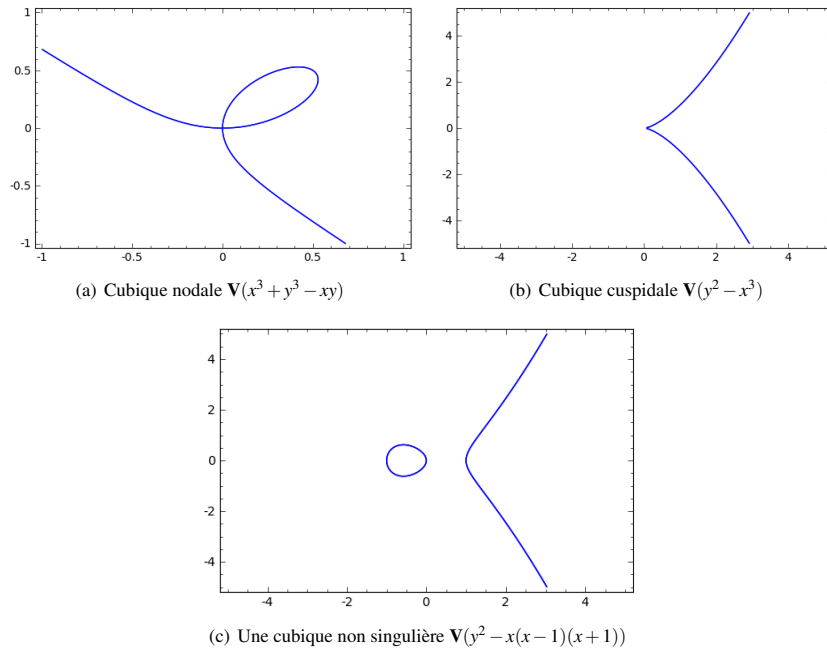
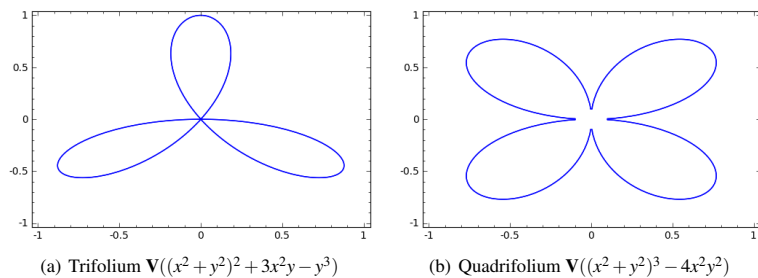
```
sage: R.<x,y> = PolynomialRing(RR,'x,y')
sage: C = Curve(x^2 + y^2 - 1)
sage: C.plot((x,-1.5,1.5), (y,-1.5,1.5))
```

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

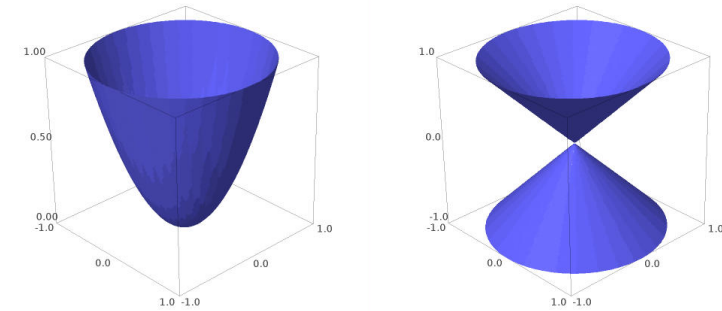
Exercice 45. — Montrer qu'un ensemble algébrique affine $\mathbf{V}(f)$ défini par un polynôme f de $\mathbb{R}[x, y]$ n'est pas toujours une partie connexe de $\mathbb{R}^2$.

Exercice 46. — 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. $\mathbf{V}(y^2 - x(x - 1)(x - 2))$.

FIGURE II.2.: Des cubiques $V(f)$ (f de degré 3).

II.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 .



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, adaptive=True)
sage: f
```

Exercice 47. — Tracer les ensembles algébriques suivants dans $\mathbb{R}^3$:

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

Exercice 48. — Décrire l'équation de l'ensemble algébrique affine constitué du cylindre de rayon 1 centré sur l'axe des y .

Exercice 49. — 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 $\tilde{f}$ s'annule sur X , alors $f(1, 1) = 0$.
2. En déduire que X n'est pas un ensemble algébrique affine de $\mathbb{R}^2$.

II.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 comme 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

$$\begin{cases} x^2 + y^2 = 4, \\ (x-z)^2 + (y-w)^2 = 1. \end{cases}$$

Par exemple, l'origine $(z, w) = (0, 0)$ n'est pas atteignable par l'extrémité du bras du robot. En effet, le système

$$\begin{cases} x^2 + y^2 = 4, \\ x^2 + y^2 = 1. \end{cases}$$

ne possède pas de solution. Par contre, le point $(z, w) = (1, 0)$ est atteignable, car le système

$$\begin{cases} x^2 + y^2 = 4, \\ (x-1)^2 + y^2 = 1. \end{cases}$$

est équivalent au système

$$\begin{cases} x^2 + y^2 = 4, \\ -2x = -4. \end{cases}$$

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

$$\begin{cases} x^2 + y^2 = 4, \\ x^2 + (y-4)^2 = 1. \end{cases}$$

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.

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

II.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

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

On a

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

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

Par ailleurs, on a

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

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 $(a_1, \dots, a_n) \in$

$\mathbf{V}(f_i g_j)$, on a soit $(a_1, \dots, a_n) \in \mathbf{V}$ qui termine le raisonnement, soit $f_{i_0}(a_1, \dots, a_n) \neq 0$, pour au moins un $i_0 \in \llbracket 1, s \rrbracket$. Comme $f_{i_0} g_j(a_1, \dots, a_n) = 0$, pour tout j , alors $g_j(a_1, \dots, a_n) = 0$, pour tout j , ainsi $(a_1, \dots, a_n) \in \mathbf{W}$. Par suite, $\mathbf{V}(f_i g_j) \subset \mathbf{V} \cup \mathbf{W}$. $\square$

De ce résultat, on déduit

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

II.2.8. Exemples.— L'ensemble algébrique affine de $\mathbb{R}^3$ 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 50. — Montrer que tout sous-ensemble fini de $\mathbb{K}^n$ est un ensemble algébrique affine.

Exercice 51. — Décrire et tracer l'ensemble algébrique affine de $\mathbb{R}^2$ défini par

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

Exercice 52. — Donner une description géométrique de l'ensemble algébrique affine $\mathbf{V}(x^2 + y^2)$ de $\mathbb{C}^2$.

§ 3 Les idéaux

Définition II.6. — Un sous-ensemble I de $\mathbb{K}[x_1, \dots, x_n]$ 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 $f \in I$ et $h \in \mathbb{K}[x_1, \dots, x_n]$, alors $hf \in I$.

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

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

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

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

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

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 $h \in \mathbb{K}[x_1, \dots, x_n]$, on a

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

Ainsi, $\langle f_1, \dots, f_s \rangle$ est un idéal. $\square$

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

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

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

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

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

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

$$g_j = h_{1j} f_1 + \dots + h_{sj} f_s,$$

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

Exercice 53. — Soit I un idéal de $\mathbb{K}[x_1, \dots, x_n]$ et soient $f_1, \dots, f_s$ des polynômes de $\mathbb{K}[x_1, \dots, x_n]$. Montrer que les deux assertions suivantes sont équivalentes

- i) $f_1, \dots, f_s \in I$,
- ii) $\langle f_1, \dots, f_s \rangle \subset I$.

Exercice 54. — Montrer les égalités des idéaux suivants de $\mathbb{Q}[x, y]$,

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

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

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

II.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 $(a_1, \dots, a_n)$ de $\mathbf{V}$, on a

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

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

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

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

Définition II.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 55. — Montrer que $I(\mathbf{V}(x^n, y^m)) = \langle x, y \rangle$.

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

$$f_1, \dots, f_s.$$

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

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

puis l'idéal de l'ensemble algébrique affine

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

Une question naturelle est : a-t-on

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

La réponse est négative en général :

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

$$\langle f_1, \dots, f_s \rangle \subset I(\mathbf{V}(f_1, \dots, f_s)), \quad (\text{II.1})$$

de plus, cette inclusion est stricte en général.

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

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

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

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

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

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

Exercice 57. — 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, $I(\mathbf{V}) = I(\mathbf{W})$.

Exercice 58. — On considère les polynômes $f_1 = x + y^2 - z^3 + 2z$, $f_2 = x - y^2 - z^3 + 2z^2 - 2z + 2$, $g_1 = x - z^3 + z^2 + 1$ et $g_2 = y^2 - z^2 + 2z - 1$ de $\mathbb{Q}[x, y, z]$.

1. Montrer que les idéaux $I = \langle f_1, f_2 \rangle$ et $J = \langle g_1, g_2 \rangle$ de $\mathbb{Q}[x, y, z]$ sont égaux ; c'est-à-dire l'égalité suivante :

$$\langle x + y^2 - z^3 + 2z, x - y^2 - z^3 + 2z^2 - 2z + 2 \rangle = \langle x - z^3 + z^2 + 1, y^2 - z^2 + 2z - 1 \rangle.$$

2. On considère les ensembles algébriques affines de $\mathbb{Q}^3$ suivants :

$$W = V(x + y^2 - z^3 + 2z, x - y^2 - z^3 + 2z^2 - 2z + 2), \quad W_1 = V(x - z^3 + z^2 + 1, y - z + 1) \text{ et } W_2 = V(x - z^3 + z^2 + 1, y + z - 1).$$

Montrer l'égalité $W = W_1 \cup W_2$; c'est-à-dire l'égalité

$$V(x + y^2 - z^3 + 2z, x - y^2 - z^3 + 2z^2 - 2z + 2) = V(x - z^3 + z^2 + 1, y - z + 1) \cup V(x - z^3 + z^2 + 1, y + z - 1).$$

II.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 $\mathbb{K}[x_1, \dots, x_n]$ possède un nombre fini de générateurs ? Autrement dit, existe-t-il une famille de polynômes $f_1, \dots, f_s$ tels que $I = \langle f_1, \dots, f_s \rangle$?

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

- c) **Problème de la résolution d'équations polynomiales :**

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

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

- d) **Problème d'impliciter une présentation paramétrée :** étant donné un paramétrage

$$x_i = g_i(t_1, \dots, t_m), \quad i \in \llbracket 1, n \rrbracket, \quad g_i \in \mathbb{K}[x_1, \dots, x_m],$$

d'un ensemble algébrique affine $\mathbf{V}$ de $\mathbb{K}^n$, déterminer des polynômes $f_1, \dots, f_s$ de $\mathbb{K}[x_1, \dots, x_n]$, tels que

$$\mathbf{V} = \mathbf{V}(f_1, \dots, f_s).$$