Illustrated by Ethan Lu

Pr. Hamza El Mahjour

Algèbre I : Notes de cours
SMP/SMIA

First Edition

Morocco

PREFACE

Chers étudiant(e)s, il est tout à fait normal que tu sois surpris, voire frustré par les nouvelles notions que tu vas confronter. Sache que ces nouvelles idées que tu découvriras doivent former un défi pour toi afin de prouver aue tu peux surmonter toute difficulté -in chaa Alah- quelque soit son degré de complexité. Et même si tu ne réussis pas, tu auras au moins tenté et tu n'auras pas de remords à te faire et aucune personne ne pourra te blâmer. En fait, les structures algébriques abstraites qui vont nous accompagner tout au long de ce livre sont en réalité des objets concrets que nous manipulons depuis notre enfance, dans ce cours nous allons juste les situer dans un cadre plus rigoureux mathématiquement. Les opérations usuelles que nous manipulons avec des nombres réels ou complexes sont un cas particulier d'une notion plus générale. Il est alors essentiel pour nous de comprendre que ce que nous arrivons à utiliser et prévoir intuitivement nécessite unenrigueur mathématique qui n'accompagne pas nécessairment cette intuition et qui permet aussi de réfléchir attentivement avant de jeter une fausse généralisation due à cette intuition. Pour bâtir cette rigueur mathématique impérative, nous commençons rappeler dans le début du Chapitre I certains éléments importants de la théorie des ensembles. Un lecteur maîtrise bien les notions de bases de la théorie des ensembles est invité á sauter directement à la deuxièmes section qui traitera à travers des exemples des lois de composition interne et des groupes ainsi que les morphismes entre groupes. Ensuite, dans des sections plus ultérieures on courvrira les anneaux, les idéaux des anneaux et puis les corps. Le deuxième chapitre sera plutôt concentré sur l'étude des polynômes, leurs racines, dérivés ainsi que la présentation du théorème fondamental de l'algèbre. Finalement on traitera dans le chapitre final les fractions rationnelles et leur simplification. Je vous souhaite une bonne lecture.

– Pr. El Mahjour
2022-08-27

TABLE DES MATIÈRES

Partie I

Logique, Ensembles et Structures Algébriques

Cette partie va traiter les éléments essentiels à connaître en logique et en théorie des ensembles avant d'introduire les plus importantes structures algébrique de base.

1

LOGIQUE ET ENSMBLES

Partie I

Les générations suivantes considéreront Mengenlehre (théorie des ensembles) comme une maladie dont on s'est remis ... Henri Poincaré

Sec 1.1 Ensembles, sous-ensembles et parties

Une **collection d'objets** en mathématique est un **ensemble**. Généralement on note les ensembles par des lettres majuscules. Par exemple, on peut prendre l'ensemble des lettres de l'alphabet français, on écrit

$$E = \{a, b, c, \ldots, y, z\}.$$

Dans l'**écriture ensembliste** l'ordre des objets n'est pas important. Autrement dit,

$$\{a, c, b, f, e\} = \{c, b, f, e, a\}.$$

On dit que $a, b, c \ldots$ sont des éléments de E. On peut écrire alors $a \in E$, $b \in E$, $c \in E$, ... et on lit "a appartient à E","a est un élément de E" ou bien "c est dans E". Quand un élément n'appartient pas à un ensemble on écrit par exemple $12 \notin E$ car 12 n'est pas une lettre de l'alphabet. Les ensembles peuvent être contenus dans d'autres ensembles, on parle de **sous-ensembles**. Par exemple, si on prend l'ensemble $H = \{a, b, c, d\}$ qui ne contient que les toutes première lettre de l'alphabet, on constate que H est un sous-ensemble de E et on peut écrire $H \subset E$ et on lit "F est inclus dans E" ou bien "E contient F". Quand un ensemble quelconque G est composé d'un nombre d'éléments finis on dit que G est **fini**. Imaginons que G est fini contenant cinq éléments alors on dit que "le **cardinal** de G est cinq" et on écrit $\text{card } G = 5$. Si G n'est pas fini comme l'ensemble des nombres entiers ou réels alors le cardinal de G est infini. L'ensemble qui ne contient aucun élément est l'ensemble **vide** noté $\emptyset$. L'ensemble vide est un sous-ensemble de n'importe quel ensemble. En fait, on peut créer l'ensemble des parties de G qui est composé de tous les sous-ensembles possibles de G. On note $\mathcal{P}(G)$ l'**ensemble des parties** de G. Il est facile d'énumérer explicitement $\mathcal{P}(G)$ quand G est fini. Par exemple, prenons $G = \{a, b, c\}$ alors les sous ensembles de G sont $\{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, G\} = \mathcal{P}(G)$. Pour tout ensemble G constitué de n éléments, l'ensemble des parties $\mathcal{P}(G)$ est de cardinal 2^n. Soient E et F deux sous-ensembles d'une ensemble G.

Définition 1.1.1. 1. *L'**intersection** de E et F est*

$$E \cap F = \{x \in G, \quad x \in E \text{ et } x \in F\}.$$

2. *L'**union** de E et F est*

$$E \cup F = \{x \in G, \quad x \in E \text{ ou } x \in F\}.$$

3. *Le **complémentaire** de E dans G est*

$$C_G^E = \overline{E} = \{x \in G, x \notin E\}.$$

Exemple 1.1. 1. *Si $E = \{1, -1, 0, 2, 13\}$ et $F = \{11, -1, 1, 3\}$. Alors, $E \cap F = \{-1, 1\}$, $E \cup F = \{-1, 0, 1, 2, 3, 11, 13\}$, $C_{E \cup F}^E = \{3, 11\}$.*

2. *Soit $E = [-2, 5]$ et $F = [2, 7]$ dans $\mathbb{R}$. Alors, $E \cap F = [2, 5]$, $E \cup F = [-2, 7]$ et le complémentaire de*

F dans $\mathbb{R}$ c'est $\overline{F} =]-\infty, -2[\cup]2, +\infty[$.

Pour visualiser les intersections, unions et complémentaires des ensembles, on peut utiliser dans certains cas le **diagramme de Venn** comme dans la figure 1.1.

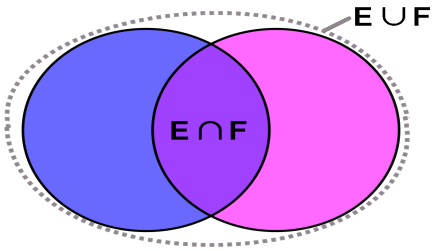

FIGURE 1.1 – Diagramme de Venn illustrant les intersection et l'union de deux ensembles.

Remarque. — *Si $A \cap B = \emptyset$ on dit que A et B sont **disjoints**.*
— *Si $E \subset F$ alors $E \cap F = E$ et $E \cup F = F$.*

Sec 1.2 Applications : surjection, injection et bijection

On peut définir des relations entre deux ensembles en mettant en liaison les éléments de ces ensembles. Pour clarifier cette idée, on sollicite le graphe 1.2. L'ensemble $E = \{a, b, c, d, e\}$ s'appelle un ensemble de **départ** et $F = \{1, 2, 3, 4, 5, 6\}$ s'appelle un ensemble d'**arrivé**. On remarque que les liaisons entre les éléments de E et F sont : $a \to 1$, $b \to 2$, $a \to 4$, $a \to 1$, $d \to 2$ et $e \to 4$. On écrit formellement

$$f(a) = 1, f(c) = 4, \ldots,$$

et on dit l'**image** de a par f est 1. On voit que des éléments différents de E peuvent avoir des images identiques. On dit que les **antécédents** de 4 sont b et d et on écrit

$$f^{-1}(2) = \{b, d\}.$$

1. Chaque élément de E doit avoir une unique image.
2. La notation f^{-1} est à ne pas confondre avec la notion de fonction inverse.

Définition 1.2.1. *Soit E un ensemble non vide. L'application de E vers E qui à x associe x se note Id_E et s'appelle l'identité de E. Ainsi, $Id_E(x) = x$ pour tout x dans E.*

Définition 1.2.2 (Injection)**.** *Soit $f : E \longrightarrow F$ une application. f est **injective** ssi*

$$\forall x, y \in E, \qquad x \neq y \implies f(x) \neq f(y),$$

ou bien

$$\forall x, y \in E, \qquad f(x) = f(y) \implies x = y.$$

Autrement dit, deux éléments différents de E ne peuvent pas avoir la même image dans F.

Définition 1.2.3 (Surjection)**.** *Soit $f : E \longrightarrow F$ une application. f est **surjective** ssi*

$$\forall y \in F, \exists x \in E, \qquad y = f(x).$$

C'est à dire, chaque élément de l'ensemble d'arrivée admet au moins un antécédent.

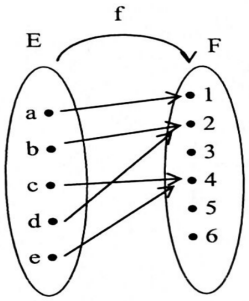

FIGURE 1.2 – Application de E dans F.

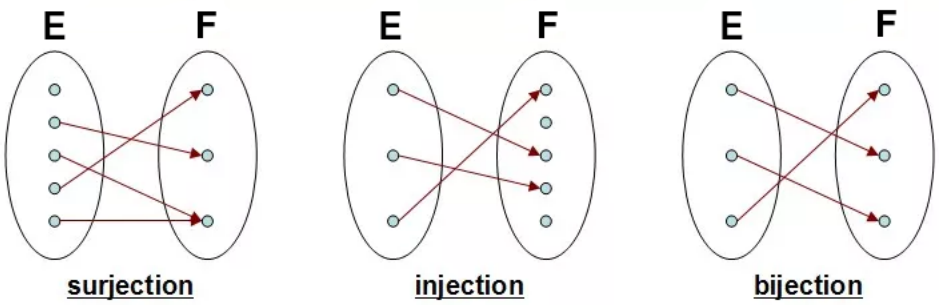

FIGURE 1.3 – Les trois types d'applications : surjective, injective et bijective.

Définition 1.2.4 (bijection)**.** *Si $f : E \longrightarrow F$ est une application surjective et injective alors elle est* ***bijective****.*

Les graphes de la figure 1.3 résument les trois cas de figures quand E et F sont finis. Si nous avons deux applications définis $f : A \longrightarrow B$ et $g : B \longrightarrow C$, on peut en extraire une nouvelle application en combinant les deux. Considérons l'exemple suivant qui est représenté graphiquement dans la figure 1.4. Quelle est l'image par g de l'image par f de l'élément 1 ? Cette question demande de savoir $g\,(f(1))$. Tout d'abord on doit impérativement se rappeler que pour la **composition des fonctions on commence de droite à gauche** ! C'est à dire que nous calculons $f(1) = 1 \to g(f(1)) = g(1) = 2 \to g\,(f(1) = 2)$. On peut alors entièrement définir toutes les autres images des autres éléments par la fonction "$g(f)$" qui est plutôt notée $g \circ f$.

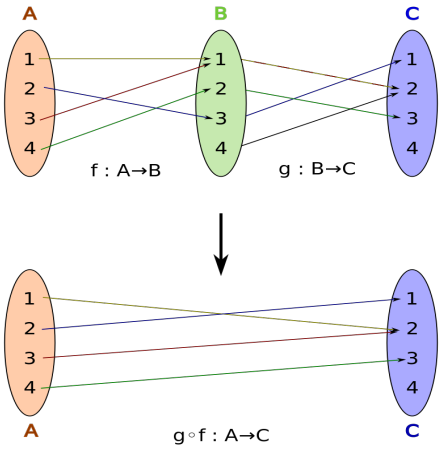

FIGURE 1.4 – f est composée avec g ce qui donne $f \circ g$.

Définition 1.2.5 (Composée de fonctions)**.** *Soient $f : E \longrightarrow F$ et $f : F \longrightarrow G$ deux applications. On définit*

*la **composée** de f et g telle que*

$$g \circ f : \begin{array}{ccc} E & \longrightarrow & G \\ x & \longmapsto & g(f(x)), \end{array}$$

pour tout x dans E.

Le théorème suivant est très important et concerne la composition des fonctions aussi.

Proposition 1.2.1. *Soit X, Y, et Z des ensembles, et soit $f : X \longrightarrow Y$ et $g : Y \longrightarrow Z$ deux applications.*

(a) *Si f et g sont injectives alors $g \circ f$ l'est aussi.*

(b) *Si f et g sont surjectives alors $g \circ f$ l'est aussi.*

En particulier, si f et g sont bijectives alors $g \circ f$ est aussi bijective.

***Proof* (Preuve).** (a) Soient x et y dans E tels que $g \circ f(x) = g \circ f(y)$. Puisque g est injective alors $f(x) = f(y)$. Et puisque f est injective alors $x = y$. Donc $g \circ f$ est injective.

(b) Soit $z \in Z$. Puisque g est surjective il existe $y_z \in Y$ tel que $g(y_z) = z$. De plus y_z est dans Y et f est surjective donc il existe $x_{yz} \in X$ tel que $f(x_{yz}) = y_z$. En remplaçant dans g on obtient $g(f(x_{yz}) = z$ c'est à dire $z = g\,(x_{yz})$ donc $g \circ f$ est bijective.

■

Pour alléger les notations et quand toute ambiguïté est absente, on remplacera $g \circ f$ par une notation multiplicative $g \circ f$. L'opération $\underbrace{f \circ f \circ \ldots f \circ}_{n fois}$ sera noté f^n.

Si $f : E \longrightarrow F$ est une bijection, il existe alors une bijection inverse $f^{-1} : F \longrightarrow E$ telle que $ff^{-1}(x_F) = x$ et $f^{-1}f(x_E)$ pour tout $x_E \in E$ et tout $x_F \in F$.

Sec 1.3 Produit Cartésien

On prend deux ensembles $E = \{a, b, c, d\}$ et $F = \{1, 2, 3\}$. On représente les deux ensembles sur deux axes perpendiculaires (voir figure 1.5). Le point rose est de coordonnées $(c, 1)$ et le point vert $(b, 3)$. Si on énumère

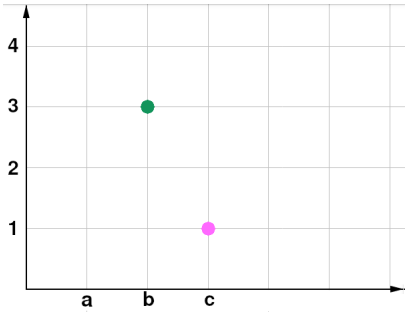

FIGURE 1.5 – Coordonnées des points suivant les axes E et F.

toutes les coordonnées possibles où les éléments de E sont des abscisses et F sont des ordonnées on retrouve l'ensemble

$$\{(a,1);(a,2);(a,3);(a,4);(b,1);(b,2);(b,3);(b,4);(c,1);(c,2);(c,3);(c,4)\}.$$

on appelle l'ensemble précédent le **produit cartésien** de E et F qu'on note $E \times F$. Plus généralement on a la définition suivante

Définition 1.3.1 (Produit Cartésien)**.** *Soit $E_1, E_2, \ldots, E_n$ des ensembles quelconques. On définit le produit cartésien $\Pi_{i=1}^{n} E_i = E_1 \times E_2 \ldots \times E_n$ comme l'ensemble des n-uplets $(x_1, x_2, \ldots, x_n)$ où $x_1 \in E_1$, $x_2 \in E_2, \ldots,$*

$x_{n-1} \in E_{n-1}$ *et* $x_n \in E_n$.

Remarque. 1. *On note* $\underbrace{E \times E \times \ldots \times E}_{n \text{ fois}} := E^n$.

2. *On appelle* (a, b) *un couple, et on appelle* (a, b, c) *un triplet, etc.*
3. $\text{card } (E \times F) = \text{card } (E) \times \text{card } (F)$.

Définition 1.3.2. *On dit que* $\mathcal{R}$ *est une relation d'équivalence si elle satisfait les propriétés suivantes*

1. $x\mathcal{R}x$ *(Réflexive)*
2. $x\mathcal{R}y \implies y\mathcal{R}x$ *(Symétrique)*
3. *Si* $x\mathcal{R}y$ *et* $y\mathcal{R}z$ *alors* $x\mathcal{R}z$ *(Transitive)*

Définition 1.3.3. *Soit* $\mathcal{R}$ *une relation d'équivalance sur un ensemble* E. *On appelle classe d'équivalence* $\overline{a}$ *l'ensemble*

$$\overline{a} = \{x \in E, \qquad a \sim x\},$$

a *est un représentant de la classe d'équivalence* $\overline{a}$.
On appelle ***ensemble quotient*** *de* E *par* $\mathcal{R}$, *l'ensemble des classes d'équivalence*

$$E/\mathcal{R} = \{\overline{a} | \quad a \in E\}.$$

La relation d'équivalence permet de décomposer un ensemble en une union disjointe d'éléments.

Notons que $E/\mathcal{R} \subset \mathcal{P}(E)$.

Exemple 1.2. 1. *Dans l'ensemble des droites du plan affine, la relation "parallèle à" est une relation d'équivalence. Par contre la relation "perpendiculaire à" ne l'est pas.*

2. *Soit* n *un entier naturel non-nul et* p, q *deux éléments de* $\mathbb{Z}$. *On dit que* p *congrue à* q *modulo* n *si* $p - q$ *est divisible par* n *c'est à dire*

$$\exists k \in \mathbb{Z}, \quad q - p = k \cdot n,$$

et on écrit $p \equiv q[n]$. *Par exemple* $27 \equiv 1\ [13]$ *et* $21 \equiv 5\ [4]$. *La relation. La relation* $\equiv$ *est une relation d'équivalence. Si on étudie les entiers relatifs par rapport à la divisibilité par 2, on peut dire qu'il y a deux catégories, soit les nombres pairs (de reste 0) soit les nombres impairs (de reste 1). Donc les deux classes d'équivalences qu'on peut extraire sont* $\overline{0} = \{x \in \mathbb{Z}, \qquad x \equiv 0\ [2]\}$ *et* $\overline{1} = \{x \in \mathbb{Z}, \qquad x \equiv 1\ [2]\}$. *L'ensemble quotient et donc*

$$\mathbb{Z}/\equiv = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \ldots\}$$

Mais à vrai dire $\overline{0} = \overline{2} = \overline{4} = \ldots$ *et* $\overline{1} = \overline{3} = \overline{5} = \ldots$ *donc* $\mathbb{Z}/\equiv$ *ne contient que deux éléments* $\{\overline{0}, \overline{1}\}$. *On note cet ensemble plutôt* $\mathbb{Z}/2\mathbb{Z}$. *On peut définir la même relation d'équivalence sur* $\mathbb{Z}$ *par rapport aux à la divisibilité sur un autre nombre et obtenir par conséquent d'autres ensemble quotients :* $\mathbb{Z}/3\mathbb{Z}, \mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/5\mathbb{Z}, \ldots$

2 STRUCTURES USUELLES : GROUPES, ANNEAUX ET CORPS

Partie I

Il est impossible d'être mathématicien sans être poète dans l'âme. *Sofia Kovalevskaya*

Sec 2.1 Groupes

On commencera ce chapitre par un exemple simple que nous manipulons chaque jour : l'addition des nombres entiers relatifs ! Il est évident pour vous que $5+3=8$ et $-176+76=100$. Mais, ce ne sont pas les résultats de ces opérations qui nous intéressent, plutôt les types de manipulations que nous pouvons appliquer dessus. Si je nomme x un nombre et y un autre nombre, on constate que $x+y$ doit aussi être un nombre qui est le résultat de la somme $x+y$ donc $x\in\mathbb{Z}$ et $y\in\mathbb{Z}$ implique que $x+y\in\mathbb{Z}$. On peut constater aussi que les nombres opposés sont de somme nulle, par exemple $5+(-5)=0$. Donc, pour chaque x de $\mathbb{Z}$ il existe $-x$ de $\mathbb{Z}$ tel que $x+(-x)=0$. On sait aussi que pour tout x dans $\mathbb{Z}$ on a $x+0=0+x=x$, on peut dire que 0 est un élément 'neutre' qui ne change pas le résultat de l'opération $+$ quand il est combiné avec n'importe quel autre nombre. Bien sûr, on est aussi d'accord que $7+((-8)+5)=(7+(-8))+5=4$. Plus généralement $(x+y)+z=x+(y+z)$ pour tout x,y et z dans $\mathbb{Z}$. Pour récapituler, on peut dire que l'ensemble $\mathbb{Z}$ muni de l'opération $+$ vérifie les axiomes suivants :

(i) $\forall x,y\in\mathbb{Z},\quad x+y\in Z,$

(ii) $\forall x\in\mathbb{Z},\exists y:=-x\in\mathbb{Z},\quad x+(-x)=0,$

(iii) $\exists\, 0\in\mathbb{Z},\forall x\in Z, 0+x=x+0=x,$

(iv) $\forall x,y$ et z dans $\mathbb{Z}$, (x+y)+z = x + (y+z).

Il serait intéressant si nous pouvons étendre ces propriétés pour des ensembles plus abstraits où les éléments ne sont pas des nombres mais des ensembles ou des fonctions ! Mais avant de généraliser, remarquons que les axiomes précédents ne sont pas forcément toujours réalisables pour n'importe quel ensemble et n'importe quelle opération, on sera peut être déçue que certains ensembles très simples et aussi des opérations simples échouent certains axiomes précédents. Prenons $(\mathbb{N},+)$ l'ensemble des entiers naturels muni de l'addition, on constate que le deuxième axiome n'est pas valide, car on ne peut pas additionner deux entiers naturels non-nuls et obtenir une somme nulle. Gardons cette fois le même ensemble muni de la soustraction usuelle on remarque que $2-3=-1$ or $-1\notin\mathbb{N}$.

Définition 2.1.1. *Soit E un ensemble quelconque. On dit que $\star$ est une* ***loi de composition interne*** *si*

$$\forall(x,y)\in E\times E,\qquad x\star y\in E.$$

Donc l'axiome (i) on lui attribue un nom comme indiqué dans la définition, c'est à dire qu'en combinant/composant deux éléments de E, on doit être sûr que le résultat de cette composition reste dans E.

Exemple 2.1.

1. *L'addition usuelle sur $\mathbb{R}$ est une loi de composition interne. De même pour $\mathbb{C},\mathbb{Z}$ ou $\mathbb{Q}$.*
2. *L'intersection $\bigcap$ et l'union $\bigcup$ définis sur $\mathcal{P}(E)$ l'ensemble des parties de E représentent tous les deux des lois de composition interne.*
3. *Sur l'ensemble des fonctions numériques de $\mathbb{R}$ dans $\mathbb{R}$, chacune des opérations suivantes forme une loi de composition interne*

Cette loi de composition interne est essentielle pour pouvoir construire la première structure algébrique de ce cours qui est un **groupe**.

Définition 2.1.2. *Soit $(E, \star)$ l'ensemble E muni de loi de composition interne $\star$. Si*

(a) $\forall x, y, z \in E \ \ (x \star y) \star z = x \star (y \star z)$ *(associativité),*

(b) $\exists e \in E, \forall x \in E, \ \ x \star e = e \star x = x$ *(élément neutre),*

(c) $\forall x \in E, \exists \bar{x} \in E, \ \ x \star \bar{x} = \bar{x} \star x = e$ *(opposé ou inverse[a]),*

*alors on dit que $(E, \star)$ est un **groupe**. Si de plus $x \star y = y \star x$, on dit qu'il est un groupe **commutatif** ou **abélien**[b].*

a. Cette appellation dépend du contexte, si la loi de composition interne est plutôt additive on utilise le terme opposé. Si elle est multiplicative on parle d'inverse.

b. Porte son nom en hommage au mathématicien norvégien **Niels Henrik Abel**, né en 1802 et mort en 1829. Il est connu pour ses travaux en sur la semi-convergence des séries numériques, des suites et séries de fonctions, les critères de convergence d'intégrale généralisée, sur la notion d'intégrale elliptique ; en algèbre, sur la résolution des équations algébriques.

On peut tester avec des exemples et découvrir si les ensembles définis forment bien un groupe ou pas.

Exemple 2.2.

1. *$(\mathbb{Z}, +)$ est un groupe, on la discutait dans l'introduction. De même sont $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$.*
2. *L'ensemble $F = \{-1, 1, i, -i\} \subset \mathbb{C}$ muni de la multiplication usuelle des nombres complexes est bien un groupe (Vérifier comme exercice).*
3. *Il existe des groupes multiplicatifs bien sûr comme $(\mathbb{Q}^*, \cdot)$, $(\mathbb{R}^*, \cdot)$ et $(\mathbb{C}^*, \cdot)$.*

Remarque. *L'opposé est généralement noté $-x$ tandis que l'inverse est noté x^{-1}.*

2.1.1 Groupe symétrique

On va maintenant étudier un ensemble particulier de groupes qui sont les groupes de symétries. La notion de symétrie nous est familière car elle a une interprétation géométrique claire. On en connaît par exemple la symétrie axiale et la symétrie centrale. C'est pourquoi, pour se baser sur un outil tangible, nous préférons commencer par un exemple très simple et très riche. On étudiera un triangle équilatéral en nommant ses sommets consécutivement 1,2 et 3. Plus précisément on va appliquer des transformations géométriques sur le triangle qui permettent de garder le même triangle en changeant seulement les noms des sommets. La symétrie axiale et la rotation sont utilisés afin d'accomplir cet objectif comme le montre la figure 2.1. Pour formaliser l'approche géométrique précédente, on considère l'ensemble des transformations $\mathcal{S} = \{\mathrm{Id}, \mathrm{Ax}_1, \mathrm{Ax}_2, \mathrm{Ax}_3, \mathrm{R}_{120°}, \mathrm{R}_{-120°}\}$. Puisque nous avons besoin d'un groupe, on doit attribuer $\mathcal{S}$ une loi de composition interne, on va travailler avec la loi "$\circ$" qui compose des applications. Maintenant nous allons résumer les différentes composées des transformations de $\mathcal{S}$ dans le tableau 2.1. On remarque dans ce tableau que chaque élément combiné avec un autre donne un élément du même ensemble. Ceci confirme que $\circ$ est une loi de composition interne pour $\mathcal{S}$. De plus, en prenant n'importe quel élément $T \in \mathcal{S}$ on a $T \circ Id = Id \circ T = T$, c'est à dire que la transformation Id (qui garde chaque sommet dans sa place initial) est un élément neutre pour la loi $\circ$, en effet on appelle Id l'application "identité". On remarque aussi que pour chaque ligne et chaque colonne il existe une unique case contenant l'élément Id, c'est à dire que chaque transformation à une transformation inverse qui renvoie vers l'élément neutre. L'associativité est une propriété intrinsèque à la loi "$\circ$ (voir l'annexe sur la théorie des ensembles). On en conclut que $(\mathcal{S}, \circ)$ est un groupe fini composé de six éléments. On va voir dans la suite qu'il existe une manière plus élégante de définir et représenter ce cas particulier de la famille des **groupes symétriques**.

mini-exercice : Trouvez l'élément opposé/inverse de chaque élément de $(\mathcal{S}, \circ)$.

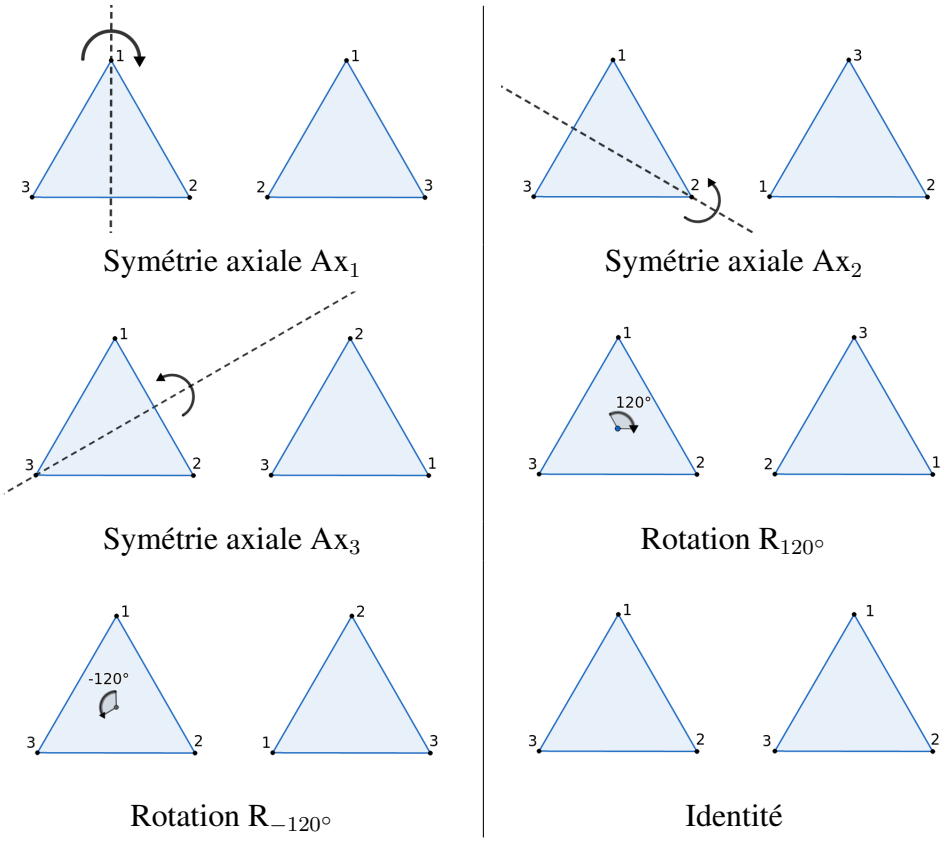

FIGURE 2.1 – Transformations préservant la forme et la position du triangle en interchangeant l'ordre des sommets.

$\circ$	Id	Ax_1	Ax_2	Ax_3	$R_{120°}$	$R_{-120°}$
Id	Id	Ax_1	Ax_2	Ax_3	$R_{120°}$	$R_{-120°}$
Ax_1	Ax_1	Id	$R_{-120°}$	$R_{120°}$	Ax_3	Ax_2
Ax_2	Ax_2	$R_{-120°}$	Id	$R_{120°}$	Ax_3	Ax_1
Ax_3	Ax_3	$R_{120°}$	$R_{-120°}$	Id	Ax_1	Ax_2
$R_{120°}$	$R_{120°}$	Ax_3	Ax_1	Ax_2	$R_{-120°}$	Id
$R_{-120°}$	$R_{-120°}$	Ax_2	Ax_3	Ax_1	Id	$R_{120°}$

TABLE 2.1 – Composées des transformations de l'ensemble $\mathcal{S}$.

Définition 2.1.3. *Soit Ω un ensemble fini ou infini. On définit*

$$\mathrm{Perm}(\Omega) = \{f : \Omega \longrightarrow \Omega, \quad f \textit{ est bijective}\}.$$

On a utilisé "Perm" pour indiquer qu'il s'agit de l'ensemble des permutations possibles au sein d'un ensemble. Une bijection d'un ensemble fini dans lui même n'est autre qu'une substitution de la position de ces éléments.

Théorème 2.1.1. *L'ensemble Perm(Ω) muni de la composition $\circ$ est un groupe.*

Proof. 1. Il est claire, en appliquant le Théorème 1.2.1 (voir l'annexe) que $\circ$ est une loi de composition interne pour l'ensemble Perm(Ω).

2. On a déjà montré dans l'annexe qu'il existe une application bijective Id (l'identité) qui fait que $f \circ Id = Id \circ f = f$ pour tout f bijective. Donc Id est un élément neutre dans Perm.

3. On a aussi montré dans l'annexe que chaque bijection f admettait une bijection inverse f^{-1} telle que $f^{-1}f = ff^{-1} = Id$.

4. Par construction, $h \circ (g \circ f) = (h \circ g) \circ f$ donc $\circ$ est une loi associative.
Par ce qui précède on conclut que $(\mathrm{Perm}(\Omega), \circ)$ est un groupe. ■

Quand $\mathrm{card}\ (\mathrm{Perm}(\Omega) = n < \infty$, on l'appelle **groupe de permutation** et on le note généralement $\mathfrak{S}_n$. En revenant un autre exemple de triangles équilatéral sur lequel on applique des transformations qui permutent ses sommets. Cette idée pourrait être exprimé autrement. On considère l'ensemble des sommets $S_3 = \{1, 2, 3\}$, si on considère le groupe $\mathfrak{S}_3 = (S, \circ)$. Dans ce qui on énumère les bijections possibles de S_3 dans S_3. Pour représenter les bijections de manière plus élégante on écrira $\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ qui veut dire la bijection $\sigma_1 : S \longrightarrow S$ telle que $\sigma_3(1) = 2, \sigma_3(2) = 1$ et $\sigma_3(3) = 3$. Remarquez que cette permutation échange les sommets 1 et 2 et ne change pas le sommet 3, c'est en effet la symétrie axiale Ax_3. La notation intorduite est simple et on peut compter toutes les permutations possibles comme suit

$$Id = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad \sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \quad \sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$
$$\rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \rho_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \quad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

On peut constater que les permutations σ_i correspondent aux symétries axiales et ρ_i aux rotations. C'est ainsi qu'on retrouve le même nombre de transformations montrés sur les dessins de la Figure 2.1. Bien que nous ayons réussi à simplifier les notations des éléments du groupe symétrique $\mathfrak{S}_n$ (généralisable à tout autre dimension finie), il existe une notation encore plus simple qui est plus utile d'un point de vu algébrique. Dorénavant $S_n := \{1, 2, 3, \ldots, n\}$.

Définition 2.1.4. *Soit $n \in \mathbb{N}^*$ et soit $\mathfrak{S}_n$ le groupe symétrique de degré n. Soient $\{a_1, a_2, \ldots, a_m\} \subset S_n$. Soit la permutation σ de $\mathfrak{S}_n$ qui envoie a_1 vers a_2 et a_2 vers a_3 et ainsi de suite jusqu'à renvoyer a_m au point de départ a_1 tout en gardant les autres éléments fixés. Cet élément σ sera noté $(a_1\ a_2\ a_3\ \ldots\ a_n)$, on l'appelle **cycle** de longueur m.*

Définition 2.1.5. *Soit $\sigma \in \mathfrak{S}_n$ et soit $a \in S_n$ fixé. On appelle **orbite** de a par σ l'ensemble*

$$\mathcal{O}_{a,\sigma} = \{\sigma^n(a), \quad n \in \mathbb{N}\}.$$

Exemple 2.3. *Soit $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 2 & 1 & 3 \end{pmatrix} \in \mathfrak{S}_5$.*

— *L'orbite de 1 par σ est symboliquement*

$$1 \to 4 \to 1 \to 4 \ldots$$

donc $\mathcal{O}_{1,\sigma} = \{1, 4\} = \mathcal{O}_{4,\sigma}$.

— *L'orbite de 3 par σ symboliquement est*

$$3 \to 2 \to 5 \to 3 \to 2 \to \ldots$$

donc $\mathcal{O}_{3,\sigma} = \{2, 3, 5\} = \mathcal{O}_{5,\sigma} = \mathcal{O}_{2,\sigma}$.

Soit $\mu = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 3 & 2 & 4 \end{pmatrix} \in \mathfrak{S}_5$. On voit bien que $\mathcal{O}_{1,\mu} = \{1\}, \mathcal{O}_{3,\mu} = \{3\}$ et $\mathcal{O}_{2,\mu} = \mathcal{O}_{4,\mu} = \mathcal{O}_{5,\mu} = \{2, 4, 5\}$. Cet exemple que dans certains cas les permutations ont une seule orbite qui contient plus de deux éléments et toutes les autres en contiennent un seul.

Définition 2.1.6. *Une permutation de $\mathfrak{S}_n$ est un **cycle** si elle contient au plus une orbite avec plusieurs éléments. La **longueur** d'un cycle est le cardinal de sa plus grande orbite.*

Dans l'exemple 2.3 μ est un cycle. On notera μ plutôt $(2\ 5\ 4)$. Cette notation est spécifique aux orbites de $\mathfrak{S}_n$. En effet, il y a le résultat suivant qui montre l'utilité des cycles et leur notation.

Théorème 2.1.2. *Toute permutation de $\mathfrak{S}_n$ s'écrit comme composée de cycles disjoints.*

Proof. Soit $\mathcal{O}_{1,\sigma}, \mathcal{O}_{2,\sigma}, \ldots, \mathcal{O}_{r,\sigma}$ les orbites de $\sigma \in \mathfrak{S}_n$ tels que $\mathcal{O}_{i,\sigma}$ sont deux à deux disjoints. Cette famille des $\mathcal{O}_i$ existe il suffit juste de considérer que toutes les orbites qui ont exactement les mêmes éléments sont en effet une unique orbite, par ce processus d'élimination on arrive à $r \leq n$ orbites disjointes. On construit le cycle μ_i tel que

$$\mu_i(x) = \begin{cases} \sigma(x), & \text{si } x \in \mathcal{O}_{i,\sigma} \\ x, & \text{sinon.} \end{cases}$$

On remarque que par construction les cycles μ_i sont disjoints car $\mathcal{O}_{i,\sigma}$ sont disjoints. Prenons un x_0 quelconque de S_n, il appartient forcément à une orbite $\mathcal{O}_{i_0,\sigma}$. Par conséquent, pour tout $i \neq i_0, \mu_i(x) = Id(x) = x$, ceci est vrai pour tout x dans $\mathcal{O}_{i_0,\sigma}$, en particulier pour $\sigma(x_0)$ car il appartient aussi à $\mathcal{O}_{i_0,\sigma}$. C'est pourquoi $\forall i \neq i_0, \mu_i(\sigma(x_0)) = Id(\sigma(x_0)) = \sigma(x_0)$. Donc

$$\mu_1 \circ \mu_2 \ldots \circ \mu_{i_0} \ldots \circ \mu_r(x_0) = Id \circ Id \circ \ldots \mu_{i_0} \circ \ldots \circ Id(x) = \mu_{i_0}(x) = \sigma(x).$$

En appliquant la même idée pour tous les éléments de $S_n = \{1, 2, \ldots, n\}$ on trouve que

$$\mu_1 \circ \mu_2 \circ \ldots \mu_r = \sigma.$$

C'est le résultat désiré. ■

Le cardinal de $\mathfrak{S}_n$ est $n! = n \cdot (n-1) \cdot (n-2) \ldots 3 \cdot 2 \cdot 1$

2.1.2 Homomorphisme de groupes

Soit f une fonction de $(\mathbb{R}, +)$ vers $(\mathbb{R}, +)$ telle que $f(x) = 5x$. Par un calcul simple nous avons $f(x+y) = 5(x+y) = 5x + 5y = f(x) + f(y)$. Donc f est une appplication qui transfert la loi $+$ entre le groupe de départ et le groupe d'arrivée. Prenons un autre exemple, soit g une fonction de $(\mathbb{R}, +)$ vers $(\mathbb{R}^*, \cdot)$ telle que $g(x) = e^x$. On a pour tout x, y de $\mathbb{R}$, $g(x+y) = e^{x+y} = e^x \cdot e^y = g(x) \cdot g(y)$. C'est à dire que l'application g préserve la loi de composition interne dans les deux groupes $(\mathbb{R}, +)$ et $(\mathbb{R}^*, \cdot)$. Plus généralement ce type de fonctions représente des **morphismes/homomorphisme** entre groupes.

Définition 2.1.7. *Soit $(G, *)$ et $(G', \star)$ deux groupes. Soit $\phi : G \longrightarrow G'$ une application telle que*

$$\forall x, y \in G, \qquad \phi(x * y) = \phi(x) \star \phi(y).$$

*Alors ϕ est un **homomorphisme/morphisme**.*

Définition 2.1.8. *Soit $(G, *)$ et $(H, \star)$ deux groupes d'éléments neutres e_G et e_H consécutivement. On définit le **noyau**[a] d'un morphisme $\phi : G \longrightarrow H$ tel que*

$$\ker \phi = \{x \in G, \qquad \phi(x) = e_H\}.$$

a. Le mot "kernel" veut dire en anglais noyau, d'où la notation $\ker \phi$.

Lemme 2.1.1. *Soit ϕ un morphisme de $(G, *)$ vers $(H, \star)$ alors*

1. *$\phi(e_G) = e_H$,*
2. *L'inverse de $\phi(y)$ dans H est $\phi(y^{-1})$ où y^{-1} est l'inverse de y dans G.*

Proof. 1. On a pour tout x dans G,

$$\phi(x) = \phi(x * e_G) \underbrace{=}_{\phi \text{ morphisme}} \phi(x) \star \phi(e_G),$$

de même

$$\phi(x) = \phi(e_G * x) = \phi(e_G) \star \phi(x),$$

Donc $\phi(e_G) = e_H$ par unicité de l'élément neutre.

2. Soit y dans G et y^{-1} son inverse. On sait que $\phi(e_G) = e_H$. Donc $\phi\left(y * y^{-1}\right) = e_H$. En appliquant la propriété du morphisme on a $\phi(y) \star \phi(y^{-1}) = e_H$ donc $\phi(y^{-1})$ est l'inverse de $\phi(y)$.

■

Proposition 2.1.1. *Soit $\phi : G \longrightarrow H$. Si $\ker \phi = \{e_G\}$ alors ϕ est injective.*

Proof. Soit x et y de G tels que $\phi(x) = \phi(y)$. Notons que $\phi(y) \in (H, \star)$ donc il existe l'inverse de $\phi(y)$ dans H qui est l'élément $\phi(y^{-1})$. C'est à dire qu'on peut écrire

$$\phi(x) \star \phi(y^{-1}) = \phi(y) \star \phi(y^{-1}) = e_H.$$

Et puisque ϕ est un morphisme alors $\phi(x) \star \phi(y^{-1}) = \phi(x * y^{-1}) = e_H$. Celà veut dire que l'élément $x * y^{-1} \in \ker \phi$. Or $\ker \phi = \{e_G\}$, donc $x * y^{-1} = e_G$. En multipliant par y l'inverse de y^{-1} des deux côtés on obtient

$$x * y^{-1} * y = x * e = x = e * y = y.$$

Donc $x = y$ et l'application ϕ est injective. ■

2.1.3 Sous-groupes

Chaque ensemble contient des sous-ensembles. On peut se poser la question suivante concernant les sous-ensembles d'un groupe : quelles sont les conditions suffisantes et nécessaires pour qu'un sous-ensemble d'un groupe soit aussi un groupe ? Une des réponses possibles est de dire que le sous-ensemble doit avoir toutes les propriétés du groupe et par conséquent il doit valider tous les axiomes donnés dans la Définition 2.1.2, mais ce serait pénible de vérifier tous ces axiomes à chaque fois ! C'est pourquoi la proposition suivante permet de donner un critère qui permet de réduire le nombre de conditions à vérifier.

Proposition 2.1.2. *Soit $(G, *)$ un groupe et soit H une partie non-vide de G. H est un **sous-groupe** de G si*

1. *$*$ est une loi de composition interne pour H*
2. *Pour tout $h \in H$, son inverse est aussi dans H.*

Dans ce cas $(H, *)$ est aussi un groupe.

Proof. La démonstration est évidente puisqu'il reste à montrer que $*$ est associative et qui est une propriété qui est vrai pour tous les éléments de G, en particulier ceux de H. Et il faut montrer que l'élément neutre de G est aussi celui de G. Soit h dans H. En utilisant le point 2 de la Prop 2.1.2 il existe h^{-1} aussi dans H tel que $h * h^{-1} = e$ où e est l'élément neutre de G. Puisque h et h^{-1} sont dans H et en utilisant le point 1 de la proposition 2.1.2 on en déduit que $h * h^{-1} \in H$, donc $e \in H$. C'est à dire que H admet un élément neutre. Donc $(H, *)$ est un groupe. ■

Exemple 2.4.
1. *Les groupes $(\mathbb{Z}, +)$ et $(\mathbb{Q}, +)$ sont des sous-groupes de $(\mathbb{R}, +)$.*
2. *$(\mathbb{Q}^*, \cdot)$ est un sous-groupe de $(\mathbb{R}, \cdot)$.*

Sec 2.2 Anneaux

La richesse des groupes dépasse le contenu de ce cours, néanmoins nous allons élargir notre esprit afin de construire une structure plus complexe basée sur la structure du groupe.

Définition 2.2.1. *Un **anneau** (aussi appelé anneau unitaire) est un triplet $(\mathbb{A}, +, \cdot)$ où $(A, +)$ est un groupe commutatif et $\cdot$ est une loi de composition interne qui vérifie*

1. $\forall x, y, z \in \mathbb{A}, \quad x \cdot (y + z) = x \cdot y + x \cdot z.$ *(distributivité)*
2. $\exists \mathbb{1}_{\mathbb{A}}, \forall x \in \mathbb{A}, \quad \mathbb{1}_{\mathbb{A}} \cdot x = x \cdot \mathbb{1}_{\mathbb{A}} = x.$ *(élément neutre pour $\cdot$)*

*Si de plus la loi $\cdot$ est commutative dans $\mathbb{A}$ alors l'**anneau est commutatif**.*

Sauf mention contraire, les anneaux considérés sont tous commutatifs et différents de l'anneau nul $(\{0_A\}, +, \cdot)$. L'anneau est le seul anneau oùn les éléments neutres de la loi $+$ et $\cdot$ sont le même.

Exemple 2.5. 1. *Les triplets $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$,$(\mathbb{R}, +, \cdot)$sont des anneaux.*

2. *Soient f et g des fonctions numériques de $\mathbb{R}$ dans $\mathbb{R}$. On définit les lois $+$ et $\cdot$ pour l'ensemble des fonctions numériques de la manière suivante*

$$(f + g)(x) = f(x) + g(x), \qquad (f \cdot g)(x) = f(x) \cdot g(x), \forall x \in \mathbb{R}.$$

Dans ce cas $(\mathcal{F}(\mathbb{R}, \mathbb{R}), +, \cdot)$ est un anneau, l'élément neutre pour la loi $+$ est la fonction nulle $(\theta(x) = 0, \forall x \in \mathbb{R})$, est l'élément neutre pour $\cdot$ est la fonction constante $\mathbb{1}(x) = 1, \forall x \in \mathbb{R}$.

Définition 2.2.2. *On définit $\mathbb{A}^*$ comme l'ensemble des inversibles d'un anneau $(\mathbb{A}, +, \cdot)$ c'est à dire*

$$\mathbb{A}^* = \left\{ y \in \mathbb{A}, \exists y^{-1} \in \mathbb{A} \qquad y \cdot y^{-1} = \mathbb{1}_{\mathbb{A}} \right\}.$$

Remarque. *On appelle $0_{\mathbb{A}}$ un élément **absorbateur** car pout tout $a \in (\mathbb{A}, +, \cdot)$ $0_{\mathbb{A}} \cdot a = a \cdot 0_{\mathbb{A}} = 0_{\mathbb{A}}$.*

Définition 2.2.3. *On dit que $(\mathbb{A}, +, \cdot)$ est un anneau **intègre** si le seul élément absorbant est $0_{\mathbb{A}}$. Autrement dit*

$$x \cdot y = 0_{\mathbb{A}} \quad \Longrightarrow \quad x = 0_{\mathbb{A}} \quad \text{ou} \quad y = 0_{\mathbb{A}}.$$

Exemple 2.6. 1. *L'anneau $(\mathbb{Z}, +, \cdot)$ est intègre.*

2. *L'anneau de $\mathbb{Z}/4\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$ n'est pas intègre car $\overline{2} \cdot \overline{2} = \overline{4} = \overline{0}$.*

Nous avons déjà défini un homomorphisme entre groupes. On peut définir de la même façon un morphisme d'anneaux. Afin de ne pas trop embrouiller le lecteur par des symboles de lois compliqués on se contentera de noter $+$ pour la loi des groupes et $\cdot$ la deuxième loi de l'anneau même si les anneaux de départ et d'arrivée sont de natures différentes.

Définition 2.2.4. *Soit $(\mathbb{A}, +, \cdot)$ et $(\mathbb{B}, +, \cdot)$ deux anneaux. Un homomorphisme entre anneaux est une application $\psi : \mathbb{A} \longrightarrow \mathbb{B}$ telle que*

1. $\psi(x + y) = \psi(x) + \psi(y), \quad \forall x, y \in \mathbb{A},$
2. $\psi(x \cdot y) = \psi(x) \cdot \psi(y), \quad \forall x, y \in \mathbb{A},$
3. $\psi(\mathbb{1}_{\mathbb{A}}) = \mathbb{1}_{\mathbb{B}}.$

Concernant le troisième point de la Définition 2.2.4, il n'est pas mentionné par redondance, en effet, on sait que ψ est un morphisme entre les groupes $(\mathbb{A}, +)$ et $(\mathbb{B}, +)$ ce qui permet d'assurer que $\psi(0_{\mathbb{A}}) = 0_{\mathbb{B}}$. Mais pour $(\mathbb{A}, \cdot)$ et $(\mathbb{B}, \cdot)$ ce ne sont pas forcément des groupes, ce qui oblige d'ajouter la troisième condition. La notion est très intéressante parce qu'elle permet des développements algébriques profonds mais aussi des constructions en arithmétique qui dépassent les objectifs de ce cours.

Définition 2.2.5. *Un **idéal** d'un anneau $\mathbb{A}$ est un sou-groupe I de $\mathbb{A}$ tel que :*

$$\forall x \in I, \forall x \in \mathbb{A}, \qquad a \cdot x \in I.$$

Proposition 2.2.1. *L'intersection d'idéaux est un idéal.*

Proof. Soit un (I_i) $(i = 1 \dots n)$ une famille d'idéaux d'un anneau $\mathbb{A}$. Posons $\mathcal{I} = \cup_{i=1}^{n} I_i$ et soit $x \in \mathcal{I}$. Donc x appartient à chacun des I_i. Pour un élément $a \in \mathbb{A}$, on remarque que $a \cdot x \in I_i$ car chaque I_i est un idéal. Par conséquent $a \cdot x \in \cup_{i=1}^{n} I_i = \mathcal{I}$, c'est à dire que $\mathcal{I}$ est un idéal. ■

Proposition 2.2.2. *Si $\psi : \mathbb{A} \longrightarrow \mathbb{B}$ est un homomorphisme d'anneaux commutatifs alors $\ker \psi$ est un idéal de $\mathbb{A}$.*

Proof. Soit $x \in \ker \psi = \{z \in \mathbb{A}, \quad \psi(z) = 0_{\mathbb{B}}\}$ et $a \in \mathbb{A}$. On a

$$\psi(a \cdot x) \underbrace{=}_{\text{morphisme d'anneaux}} \psi(a) \cdot \psi(x) \underbrace{=}_{x \in \ker \psi} \psi(a) \cdot 0_{\mathbb{B}} \underbrace{=}_{0_{\mathbb{B}} \text{ absorbant}} 0_{\mathbb{B}}.$$

Donc $a \cdot x \in \ker \psi$, alors $\ker \psi$ est un idéal. ■

Définition 2.2.6. *Un sous-anneau d'un anneau commutatif $(\mathbb{A}, +, \cdot)$ est une partie de $\mathbb{A}$ stable par addition, par multiplication et contenant l'élément unité de $\mathbb{A}$; c'est un sous- groupe de $(A, +)$ et c'est un anneau.*

Un idéal d'un anneau n'est pas un sous-anneau sauf s'il contient l'élément $\not\exists_{\mathbb{A}}$.

Exemple 2.7. 1. *Les idéaux de $\mathbb{Z}$ sont les ensembles de la forme $n\mathbb{Z}$ où*

$$n\mathbb{Z} = \{\dots, -2n, -n, 0, n, 2n, 3n, \dots\}.$$

2.

On est habitué à l'utilisation de $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$. En effet ce sont ces deux structures il y a quelque chose qui les distingue. C'est le fait que tous ces éléments non nuls admettent un inverse.

Définition 2.2.7. *Soit $(\mathbb{A}, +, \cdot)$ un anneau commutatif. Si $\mathbb{K}^* = \mathbb{K} \setminus \{0_{\mathbb{A}}\}$ alors $\mathbb{K}$ est **un corps**.*

Comme déjà expliqué, un corps est tout simplement un anneau où tous les éléments sont inversibles sauf l'élément neutre pour l'addition.

Exemple 2.8. 1. *On connaît les corps infinis comme $\mathbb{Q}, \mathbb{R}$ et $\mathbb{C}$.*

2. *Il existe aussi des corps finis. Par exemple, les anneaux $\mathbb{Z}/p\mathbb{Z}$ pour p premier.*

Les corps finis ayant un nombre d'éléments égal à une puissance de 2 sont très utilisés dans les problèmes d'informatique, de transport de l'information et de cryptographie.

Partie II

Nombres complexes, polynômes et Fractions Rationnelles

Cette partie va rappeler les notions essentielles sur les nombres complexes ainsi que l'introduction des polynômes et les notions de racines et leur multiplicité. En passant par l'arithmétique sur les polynômes et leur factorisation. Enfin, la réduction en éléments simples est l'objectif technique principal de cette partie.

3 POLYNÔMES

Partie II

Rien n'est beau que le vrai. Hermann Minkowski

Sec 3.1 Introduction

Le paragraphe historique suivant est issu du Chapitre 13 de [**escofier2016toute**]. Mohammed Al-Khawarizmi (vers 780-vers 850), dans son traité d'algèbre écrit vers 825, classifie les équations du second degré en différents types pour ne considérer que des coefficients positifs. Par exemple : un carré et 21 dirhams sont égaux à dix racines qui correspond à l'équation $x^2 + 21 = 10x$, est une équation du type $x^2 + c = bx$ avec $b, c > 0$ (pour Al-Khawarizmi qui traite de problèmes d'héritage, les nombres sont exprimés en dirhams, l'unité monétaire arabe). " Dans ce cas, précise Al-Khawarizmi, saches que si tu divises en 2 la racine (il faut comprendre : le coefficient b de x), que tu la multiplies par elle-même, et que le produit soit plus petit que les dirhams (il faut comprendre : $\frac{b^2}{4} < c$) alors le problème est impossible". On comprend ce que l'auteur veut dire, mais l'usage de lettres rend les choses plus simples. Le calcul littéral, introduit par François Viète (1540-1603), permet à Descartes, en 1637, dans sa Géométrie, de dégager la esnotion de polynôme et de montrer comment faire la division par Xa. Un polynôme à une variable sur un corps $\mathbb{K}$ (où $\mathbb{K} = \mathbb{R}, \mathbb{C}$) est une expression

$$P(X) = a_0 + a_1 X + a_2 X^2 + \ldots + a_n X^n,$$

où les $a_i \in \mathbb{K}$ nommés les **coefficients** du polynôme. On peut noter $P(X) = \sum_{i=0}^{n} a_i X^i$ et par convention on considère que $X^0 = 1$. Une définition plus formelle existe mais qui ne sera pas introduite ici est celle d'une suite infini composée de ces coefficients et nul à partir d'un certain rang : $(a_0, a_1, \ldots, a_n, 0, 0, 0, \ldots)$. Vu qu'on ne s'intéresse pas à la construction rigoureuse des polynômes mais plutôt leur utilisation, on présentera certaines propriétés et utilisera certains objets sans justifier leurs caractéristiques. Par exemple, l'objet X sera traité comme une variable usuelle qui peut être multiplié par un élément de $\mathbb{K}$ et qui vérifie

$$\underbrace{X \cdot X \cdot \ldots \cdot X}_{n \text{ fois}} = X^n,$$

et aussi

$$X^m \cdot X^n = X^{m+n}.$$

On notera $\mathbb{K}[X]$ l'**ensemble des polynômes à coefficients dans** $\mathbb{K}$.

Deux polynômes $P(X) = \sum_i a_i x^i$ et $P(X) = \sum_i b_i X^i$ sont égaux si et seulement si $a_i = b_i$ pour tout i.

Sec 3.2 Structures algébriques des polynômes

Définition 3.2.1.
1. *Le* ***degré*** *d'un polynôme est le plus grand entier n tel que a_n est non nul. On écrit* $\deg P = n$.
2. *Si* $\deg P = 1$, *on appelle P un polynôme* ***unitaire***.
3. *Par convention, le degré du polynôme nul est* $-\infty$.
4. *Si* $\deg P = 0$ *alors P est un polynôme* ***constant***.

Exemple 3.1.
— *Le polynôme* $1 - 5X^3 + 10X$ *est de degré* 3.
— *Le polynôme* $3X + 1 - 12X^2 + X^4$ *est un polynôme unitaire de degré 4.*
— *Le polynôme* $P(X) = 11$ *est un polynôme constant de degré 0.*

Remarque. *Si* $\deg P = n$ *et* a_n *est le coefficient multiplié par* X^n, *alors on appelle* a_n ***coefficient dominant*** *du polynôme P.*

Définition 3.2.2. *Soient P et Q deux polynômes de* $\mathbb{K}[X]$ *avec* $P(x) = \sum_{i=0}^{m} X^i$ *et* $Q(X) = \sum_{i=0}^{n} b_i X^i$. *On appelle* ***somme*** *des polynômes P et Q (ou addition de P et Q) le polynôme de* $\mathbb{K}[X]$, *noté* $P + Q$ *et défini par*

$$(P+Q)(X) = \sum_{i=0}^{\max(m,n)} (a_i + b_i) X^i$$

Exemple 3.2. $P(X) = 1 + 2X - X^2$ *et* $Q(X) = -2X + X^3$ *alors*

$$(P+Q)(X) = (1+0) + (2-2)X + (-1+0)X^2 + (0+1)X^3 = 1 - X^2 + X^3.$$

$\mathbb{K}[X]$ muni de cette loi forme un groupe commutatif. On peut munir aussi les polynômes d'une multiplication entre polynômes pour obtenir finalement une structure d'anneau commutatif ! Mais avant de donner la définition précise d'une multiplication de deux polynômes on travaillera sur un exemple. Soient $A(X) = 1 + 3X - X^2$ et $B(X) = 3 - 2X^2 + 5X^3$. La façon la plus naturelle d'effectuer cette multiplication est d'utiliser la distributivité de la multiplication usuelle par rapport à l'addition. On traitera A et B comme des termes deux expressions algébriques avec l'application de la règle $X^i X^j = X^{i+j}$. Ce qui peut être résumé comme suit

$$(A \cdot B)(X) = (1 + 3X - X^2) \cdot (3 - 2X^2 + 5X^3)$$

$$\begin{aligned}
(AB)(X) &= \underbrace{1 \cdot 3}_{c_0} + \underbrace{(1 \cdot 0 + 3 \cdot 3)}_{c_1} X + \underbrace{(3 \cdot 0 - 1 \cdot 3 + 1 \cdot (-2))}_{c_2} X^2 \\
&\quad + \underbrace{(1 \cdot 5 + 3 \cdot (-2) + (-1) \cdot 0 + 0 \cdot 3)}_{c_3} X^3 + \underbrace{(3 \cdot 5 + (-1) \cdot (-2) + 0 \cdot 5)}_{c_4} X^4 \\
&\quad + \underbrace{((-1) \cdot 5 + 0 \cdot (-2))}_{c_5} X^5, \\
&= 3 + 9X - 5X^2 - X^3 + 17X^4 - 5X^5.
\end{aligned}$$

Nous avons alors la définition suivante

Définition 3.2.3. *Soit* $A(X) = \sum_{i=0}^{m} a_i X^i$ *et* $B(X) = \sum_{i=0}^{n} b_i X^i$ *avec*[a] $m \leq n$. *C'est à dire* $a_{m+1} = a_{m+2} = \ldots = a_(m + (n-m)) = 0$. *On appelle* ***produit*** *de* P *et* Q *le polynôme de* $\mathbb{K}[X]$ *noté* PQ, $P \times Q$ *ou* $P \cdot Q$ *défini par* $PQ(X) = \sum_{k=0}^{m+n} c_k X^k$ *où*

$$c_k = a_0 \cdot b_k + a_1 b_{k-1} + \ldots + a_{n-1} b_1 + a_n b_0$$

a. Pour faciliter les notations, si $m > n$ alors B jouera le rôle de A et vice-versa.

Propriété 3.1. *Soit* P *et* Q *deux polynômes non nuls de degrés* m *et* n *consécutivement.*

1. $\deg(P+Q) \leq \max(m, n)$,
2. $\deg(P \cdot Q) = m \cdot n$.

Voici certains exemples qui illustrent pourquoi on a une inégalité dans la première ligne des Propriétés 3.1 et une égalité dans la deuxième.

Exemple 3.3.

1. *Soit* $P(X) = X + 1$, $Q(X) = -3X^2 - X + 5$. *On a* $(P + Q(X) = X^2 + 2$. *Donc* $\deg(P+Q) = 2 = \max(2, 1)$.
2. *Soit* $P(X) = X^4 - 3X^2 + 11$, $Q(X) = -X^4 + 13X^3 + 5$. *On a* $(P + Q(X) = 13X^3 - 3X^2 + 16$. *Donc* $\deg(P+Q) = 3 < \max(4, 4)$.
3. *Soit* $P(X) = 3X^2 - 11X$, $Q(X) = -\frac{1}{3}X^5 + 5$. *Alors* $(P \cdot Q)(X) = -X^7 + 15X^2 + \frac{11}{3}X^6 - 55X$. *Donc* $\deg(P \cdot Q) = \deg P + \deg Q = 4 + 3 = 7$.

Sec 3.3 Fonctions polynomiales

Quand on traite X comme une variable réelle, on peut percevoir le polynôme P comme une fonction $P : \mathbb{R} \longrightarrow \mathbb{R}$ où $x \mapsto P(x)$. Cette fonction est continue sur $\mathbb{R}$ c'est à dire que $\lim_{x \to x_0} P(x) = P(x_0)$. Pour obtenir l'image d'un élément a par cette fonction il suffit de remplacer x par la valeur de a. On peut évaluer les éléments d'un polynôme P en un point $X = z$. Cette vision est liée au fait que $x \mapsto P(x)$ définit bien une fonction de $\mathbb{R}$ vers $\mathbb{R}$ (ou de $\mathbb{C}$ dans $\mathbb{C}$). Si z est un scalaire du corps $\mathbb{K}$ alors la valeur de P au point z est

$$P(z) = a_n z^n + a_{n-1} z^{n-1} + \ldots a_1 z + a_0.$$

Par exemple si $P(X) = 3X^2 + 5X + 1$ alors $P(1) = 3 \cdot 1 + 5 \cdot 1 + 1 = 9$.

Définition 3.3.1. *On dit que* z_0 *est une racine d'un polynôme* $P \in \mathbb{K}[X]$ *ssi*

$$P(z_0) = 0.$$

De plus $\exists Q \in \mathbb{K}[X]$, $P(X) = (X - z_0) \cdot Q(X)$.

Dans la définition précédente, il se peut que z_0 soit aussi racine du polynôme Q donc il existerait R dans $\mathbb{K}[X]$ tel que $Q(X) = (x - z_0) \cdot R(X)$ ce qui aboutit à $P(X) = (x - z_0)^2 \cdot R(X)$. Si on répète ce processus jusqu'à ce qu'on atteigne m fois avec un polynôme dont z_0 n'est pas une racine alors on dit que z_0 est de multiplicité m. Voici la définition plus formelle.

Définition 3.3.2. *Soit* $z_0 \in \mathbb{K}$ *une racine de d'un polynôme* P *de degré* $n \geq 1$ *et soit* $Q \in \mathbb{K}[X]$ *tel que*

$$P(X) = (X - z_0)^m \cdot Q(X), \qquad (m \leq n)$$

avec $Q(z_0) \neq 0_{\mathbb{K}}$. *On dit que la racine* z_0 *est de* ***multiplicité*** m.

Exemple 3.4. *Les racines du polynôme* $P(X) = (X-3)^4 \cdot (X+2i)^8$ *sont* 3 *est* $-2i$*. La racine* 3 *est de multiplicité* 4 *et la racine* $-2i$ *est de multiplicité* 8*.*

L'écriture d'un polynôme sous la forme $a(X-r_1)^{\alpha_1}(X-r_2)^{\alpha_2}\dots(X-r_k)^{\alpha_k}$ est très utile. C'est ce qu'on appelle un polynôme scindé. Cette écriture est toujours possible dans $\mathbb{C}[X]$ mais pas dans $\mathbb{R}[X]$ grâce au théorème suivant.

Theorem 3.3.1.

Théorème fondamental de l'algèbre Tout polynôme de $\mathbb{C}[X]$ *admet exactement* n *racines complexes.*

Les démonstrations du Théorème 3.3 ne sont pas compliquées, sauf qu'elles reposent sur des notions de topologie ou des notions d'analyse complexe qui dépassent le niveau de ce cours. Un projet précis et concis qui offre quatre démonstrations différentes du théorème peut être consulté sur [**Steed**].

Proposition 3.3.1. *Racines n-ème de l'unité Les solutions de l'équation* $z^n = 1$ *dans* $\mathbb{C}$ *sont* $z_k = e^{i\frac{k\,\pi}{n}}$ *pour* $k = 0 \dots n-1$*.*

Proof. Soit $z \in \mathbb{C}$ alors l'écriture exponentielle de z est $re^{i\theta}$. Donc $z^n = 1$ est équivalent à $re^{in\theta} = 1 = 1 \cdot e^{i\cdot 0}$. C'est à dire $r = 1$ et $n\theta \equiv 0[2\pi]$. Ça veut dire $\theta = \frac{2k\pi}{n}$ pour $k \in \{0, 1, \dots, n-1\}$. ■

Exemple 3.5. *On veut résoudre* $z^3 = 1$ *dans* $\mathbb{C}$*. Les solutions sont* $z_0 = 1, z_1 = e^{\frac{i\pi}{3}}$ *et* $z_1 = e^{i\frac{\pi}{3}}$

Dérivée d'un polynôme

Les fonctions polynomiales sont infiniment dérivables. La dérivée de X^n est le polynôme nX^{n-1} (notons que la dérivée d'une constante est 0). Plus généralement on a la définition suivante.

Définition 3.3.3. *Soit* $P(X) = a_nX^n + a_{n-1}X^{n-1} + \dots + a_1Xa_0$*. La dérivée de* P *est le polynôme* P' *tel que*

$$P'(X) = na_nX^{n-1} + (n-1)a_{n-1}X^{n-2} + \dots + 2a_2X + a_1.$$

On notera $P^{(k)}$ la dérivée k-ème de P.

Exemple 3.6. *Par exemple la dérivée du polynôme* $X \mapsto -X^{13} + 3X^5 + 2X$ *est le polynôme* $-13X^{12} + 15X^4 + 2$*.*

Propriété 3.2.

1. *La dérivée* k*-ème de* X^n *est le polynôme* $n(n-1)(n-2)\dots(n-k+1)X^{n-k}$*,*
2. *On a* $(P+Q)' = P' + Q'$*,*
3. $(P \cdot Q)' = P'Q + PQ'$*.*

Proposition 3.3.2. *Formules de Taylor Soit* P *dans* $\mathbb{K}[X]$*.*

1. *Si* $P(X) = \sum_{i=0}^{n} a_iX^i$ *alors pour* $k = 0, \dots n$ *on a* $a_k = \frac{P^{(k)}(0)}{k!}$*, autrement dit :*

$$\sum_{k \le n} \frac{P^{(k)}(0)}{k!}X^k.$$

2. *On a aussi, si a est un élément de $\mathbb{K}$ on a :*

$$P(X+a) = \sum_{k \leq n} \frac{P^{(k)}(a)}{k!} X^k.$$

3. *En général, soit $x_0 \in \mathbb{K}$ et soit P un polynôme de degré n. Alors*

$$P(X) = P(x_0) + \frac{P'(x_0)}{1!}(X - x_0) + \frac{P^{(2)}(x_0)}{2!}(X - x_0)^2 + \ldots + \frac{P^{(n)}(x_0)}{n!}(X - x_0)^n$$

Sec 3.4 Retour sur les nombres entiers !

On revient vers les nombres entiers, car c'est essentiel pour comprendre les mécanismes de l'arithmétique dans $\mathbb{K}[X]$. On dit que $a \in \mathbb{N}$ est divisible par $b \in \mathbb{N}$ s'il existe $q \in \mathbb{N}$ tel que $a = bq$. Par exemple 14 est divisible par 2 car $14 = 2 \times 7$. On dit aussi que 2 divise 14 et on note $2/14$. On sait aussi qu'un nombre premier est celui qui n'est divisible que par lui même et par 1, par exemple $2, 3, 5, 7, 11, 13, 17$ sont des nombres premiers. Un résultat aussi connu pour les nombres entiers est que chaque nombre entier peut être écrit comme produit de facteurs premiers. Par exemple $50 = 2 \cdot 5 \cdot 5$. Il existe aussi, dans le cadre des entiers, la notion du PGCD (Plus Grand Commun Diviseur). Nous allons par la suite présenté des notions connus en artihmétique de $\mathbb{N}$ avec des nouveaux théorèmes, propositions et exemples. Le but de cette partie est d'avoir en tête une idée claire et la transposer vers $\mathbb{K}[X]$.

Définition 3.4.1 (PGCD de deux entiers)**.** *Soient a et b dans $\mathbb{N}$. On dit que d est le PGCD de a et b si d/a, d/b et si tout diviseur commun de a et b divise d.*

Définition 3.4.2 (Algorithme d'Euclide)**.** *Soient a et b dans $\mathbb{Z}$. L'algorithme de calcul du PGCD est donné par Euclide (proposition 2 du livre 7 des Éléments. Euclide fait des soustractions successives et non des divisions). Il est basé sur la remarque suivante. Quand on écrit la division euclidienne de a par b : $a = bq + r$, un diviseur commun à a et b divise $r = a - bq$; d'autre part, un diviseur commun à a et r divise a. On a donc $PGCD(a, b) = PGCD(b, r)$. Soient donc deux entiers a et $b, a > b > 0$. On définit par récurrence une suite d'entiers en posant : $r_0 = a, r_1 = b$, et si $k \geq 1$ et si $r_k \neq 0, r_{k+1}$ est le reste de la division euclidienne de r_{k-1} par r_k : $r_{k-1} = r_k q_k + r_{k+1}$, avec $0 \leq r_{k+1} < r_k$; si $r_k = 0$, on arrête ; on note N ce dernier indice. Le PGCD est donc le dernier reste non nul : $PGCD(a, b) = r_{N-1}$.*

Montrons-le sur un exemple.

$a = 2\,652$ et $b = 2\,310$. Les divisions successives donnent :

$$\begin{array}{rcrcr} 2\,652 & = & 2\,310 & + & 342 \\ 2\,310 & = & 342 \times 6 & + & 258 \\ 342 & = & 258 & + & 84 \\ 258 & = & 84 \times 3 & + & 6 \\ 84 & = & 6 \times 14 & + & 0 \end{array}$$

Donc $\text{PGCD}(2652, 2310) = 6$.

Exemple 3.7. *On a $PGCD(18, 24) = 6$. En effet les diviseurs de 18 sont $D_{18} = \{1, 2, 3, 6, 9, 18\}$ et $D_{24} = \{1, 2, 3, 4, 6, 8, 12, 24\}$.*

Proposition 3.4.1. *Identité de Bézout Soient a et b dans $\mathbb{Z}$ et $d = PGCD(a, b)$. Il existe u et v tels que $ua + vb = d$.*

***Proof*.** L'idéal (d) est l'idéal engendré par a et b donc contient nécessairement l'ensemble E des éléments de la forme $ma + nb$ avec m et n dans $\mathbb{Z}$, comme E est visiblement un idéal de $\mathbb{Z}$, on a $E = (d)$ donc il existe un entier u et v tels que $ua + vb = d$. ■

Définition 3.4.3. *On dit que deux entiers a et b sont premiers entre eux ssi $PGCD(a,b) = 1$.*

Exemple 3.8. 1. *Les nombres* 16 *et* 14 *ne sont pas premiers entre eux car* $2/16$ *et* $2/14$ *donc* $PGCD(14,16) \geq 2 > 1$.
2. *Les nombres* 26 *et* 21 *sont premiers entre eux car* $PGCD(26,21) = 1$.

Sec 3.5 Arihtmétique des polynômes

Nous allons essayer de transposer ce qu'on a vu en $\mathbb{N}$ pour

Proposition 3.5.1. *Soient A et B des polynômes de $\mathbb{K}[X]$ avec $B \neq 0$. Il existe un couple unique polynômes Q et R de $\mathbb{K}[X]$ tels que $A = BQ + R$ et $\deg(R) < \deg(B)$.*

***Proof*.** Pour l'existence et l'unicité d'un tel couple (Q,R), nous référons le lecteur enthousiaste vers la démonstration du Théorème 6.1 du livre [**AlgAna**]. C'est un processus de construction similaire à l'algorithme d'Euclide pour le PGCD de deux nombres entiers. ■

Voici un exemple concret des étapes à suivre pour effectuer une division euclidienne.

$$\begin{array}{rrrr|l}
X^4 & +2X^3 & -X & +6 & X^3-6X^2+X+4 \\
-X^4 & +6X^3 & -X^2-4X & & \underbrace{X+8}_{\text{Quotient}} \\
\hline
0 & +8X^3 & -X^2-5X & +6 & \\
 & -8X^3 & +48X^2-8X & -32 & \\
\hline
 & & 0 & \underbrace{+47X^2-13X-26}_{\text{Reste}} & U
\end{array}$$

Exemple 3.9.

Le processus s'arrête car $\deg(47X^2-13X-26) < \deg(X^3-6X^2+X+4)$. *On appelle A le dividende et B le diviseur.*

La divisibilité en $\mathbb{K}[X]$ est similaire à ce qui se passe dans $\mathbb{Z}$. En effet, nous avons la même définition

Définition 3.5.1. *On dit qu'un polynôme A est divisible par B (ou B divise A) s'il existe $Q \in \mathbb{K}[X]$ tel que $B = Q \cdot A$*

Exemple 3.10. *Le polynôme $x-1$ divise x^2-1 car $x^2-1 = (x-1)\cdot(x+1)$.*

Définition 3.5.2. *Soit P un polynôme de $\mathbb{K}[X]$ tel que* $\deg P \geq 1$.
*- Le polynôme P est **irréductible** (ou premier) dans $\mathbb{K}[X]$ s'il admet pour diviseur que les polynômes $\alpha \cdot \nVdash_{\mathbb{K}[X]}$ et αP où $\alpha \in \mathbb{K}^*$. Autrement dit, le polynôme P de $\mathbb{K}[X]$ est irréductible lorsque les seuls polynômes qui le divisent sont, à un facteur multiplicatif près, $\nVdash_{\mathbb{K}[X]}$ et lui même.*
*- Dans le cas contraire, on dit qu'il est **réductible**.*

Un polynôme peut être irréductible dans $\mathbb{R}[X]$ mais pas dans $\mathbb{C}[X]$.

Proposition 3.5.2. 1. *Les seuls polynômes irréductibles dans $\mathbb{R}[X]$ sont de la forme $X+\alpha$ ou bien X^2+pX+q avec $p^2-4c<0$.*

2. *Les seuls polynômes irréductibles dans $\mathbb{C}[X]$ sont ceux de degré 1 seulement $X+\alpha$.*

Définition 3.5.3. *P.G.C.D de deux polynômes Si A et B sont deux polynômes de $\mathbb{K}[X]$, on dit que le polynôme D est **un plus grand commun diviseur** (ou P.G.C.D) de A et B quand*

1. *D est un diviseur commun de A et B,*
2. *tout diviseur commun de A et B divise D. Autrement dit, lensemble des diviseurs de D est égal à celui des diviseurs communs de A et B.*

Par abus de langage, on peut dire "le" P.G.C.D de deux polynômes "à un facteur constant non-nul près". Pour obtenir le P.G.C.D de deux polynômes, nous allons appliquer l'algorithme d'Euclide qui est expliqué par cette exemple.
Soient $A(X)=X^5-2X^4+X^3-X^2+2X-1$ et $B(X)=X^3-X^2+2X-2$. Effectuons D'abord la division euclidienne de A par B, ceci donne

$$\begin{array}{rrrrrr|l}
X^5 & -2X^4 & +X^3 & -X^2 & +2X & -1 & X^3-X^2+2X-2 \\
\cline{7-7}
-X^5 & +X^4 & -2X^3 & +2X^2 & & & X^2-X-2 \\
\cline{1-4}
 & -X^4 & -X^3 & +X^2 & +2X & -1 & \\
 & +X^4 & -X^3 & +2X^2 & -2X & & \\
\cline{2-5}
 & & -2X^3 & +3X^2 & & -1 & \\
 & & +2X^3 & -2X^2 & +4X & -4 & \\
\cline{3-6}
 & & & & & X^2+4X-5 &
\end{array}$$

Maintenant on considère le dividende $A_1(X)=X^3-X^2+2X-2$ et le diviseur $B_1(X)=X^2+4X-5$ qui est le reste de la division euclidienne précédente. On effectue alors la division de A_1 par B_1. On obtient

$$\begin{array}{rrrrr|l}
X^3 & -X^2 & +2X & -2 & & X^2+4X-5 \\
\cline{6-6}
-X^3 & -4X^2 & +5X & & & X-5 \\
\cline{1-3}
 & -5X^2 & +7X & -2 & & \\
 & +5X^2 & +20X & -25 & & \\
\cline{2-4}
 & & & 27X & -27 &
\end{array}$$

On récupère les nouveaux dividendes et diviseurs qui seront $A_2(X)=X^2+4X-5$ et $B_2(X)=27X-27$. Finalement, la division de A_2 par B_2 donne

$$
\begin{array}{rrr|l}
X^2 & +4X & -5 & X-1 \\
\cline{4-4}
-X^2 & +X & & X+5 \\
\cline{1-2}
 & 5X & -5 & \\
 & -5X & -5 & \\
\cline{2-3}
 & & 0 &
\end{array}
$$

Alors $P.G.C.D(A,B) = 27X - 27 = 27(X-1)$ qui représente le dernier reste non-nul dans l'algorithme d'Euclide. On peut dire que le plus grand diviseur commun de A et B est le polynôme $D(X) = X - 1$ (à un facteur constant non-nul près).

Définition 3.5.4. *Deux polynômes sont premiers entre eux si leur PGCD est un polynôme constant.*

Proposition 3.5.3. 1. *Le polynôme $X - \alpha$ divise P si et seulement si $P(\alpha) = 0$.*

2. *Si $A(\alpha) = 0$ et $B(\alpha) = 0$ alors $X - \alpha$ est un diviseur commun de A et B.*

Proof. 1. On sait que la division euclidienne de P par $X - \alpha$ donne $P(X) = (X-\alpha)Q(X) + R(X)$ où $\deg R < \deg X - \alpha$. Si $X - \alpha$ divise P alors $R(X) = 0$. Donc $P(\alpha) = (\alpha - \alpha)Q(\alpha) = 0$. Maintenant, supposons que $P(\alpha) = 0$ donc $(X-\alpha)Q(X) + R(X)$ évalué au point $X = \alpha$ va donner $R(\alpha) = 0$ et puisque $\deg R < \deg(X - \alpha) = 1$ donc $\deg R = 0$, c'est à dire que R est une constante avec $R(\alpha) = 0$ donc $R(X) = 0$. Donc P est divisible par $X - \alpha$.

2. C'est une conséquence immédiate du résultat précédent.

■

ILLUSTRATED BY ETHAN LU

Notes de cours destinés aux étudiants de première année

Morocco

ISBN 978-80-7340-097-2