



ANAS EL MOUJIBI
Matheux Club Community

Les mathématiques
sont une langue
universelle

MATH WITH ANAS

— Algèbre et Géométrie

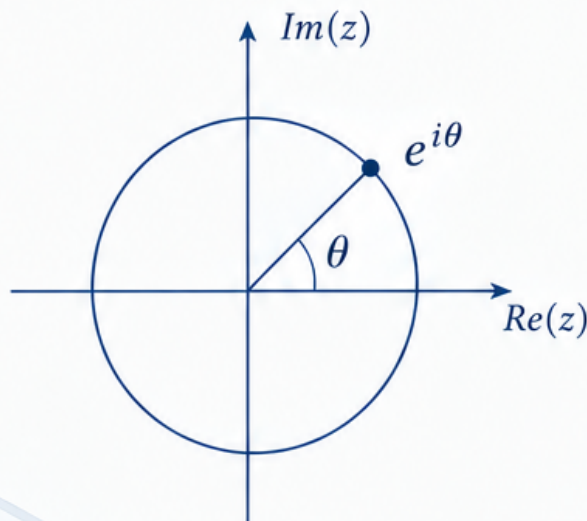
2026 / 2027

MATH WITH ANAS

Polycopie du cours

Algèbre et Géométrie

2^e année du baccalauréat sciences
mathématiques A et B

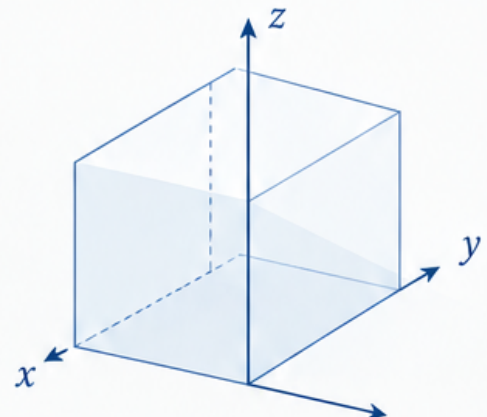


$$e^{i\theta} = \cos \theta + i \sin \theta$$

$$z = a + ib$$

$$|z| = \sqrt{a^2 + b^2}$$

$$\arg(z) = \theta \pmod{2\pi}$$



Matheux Club Community

MATH WITH ANAS

Polycopie du cours

Thèmes : Algèbre et Géométrie

2^e année du baccalauréat sciences

mathématiques A et B

A. El Moujibi : étudiant en FSSM

A.S. 2026/2027

ANAS EL MOUJIBI

Préface

Ce document introduit le programme d'algèbre de la 2^{ème} année Baccalauréat Sciences Mathématiques, soulignant le passage vers l'abstraction mathématique supérieure à travers trois piliers :

- Les Nombres Complexes : L'utilisation du nombre imaginaire i pour résoudre de nouvelles équations et lier algébriquement les transformations géométriques.
- L'Arithmétique dans $\mathbb{Z}$: L'étude exigeante des entiers relatifs, de la divisibilité et des nombres premiers, formant à la rigueur de la démonstration logique.
- Les Structures Algébriques : L'analyse abstraite des lois de composition (groupes, anneaux, corps) pour comprendre l'architecture commune aux différents objets mathématiques.

L'ensemble encourage les futurs scientifiques à cultiver patience et ténacité pour maîtriser ces concepts fondamentaux et préparer sereinement leurs études supérieures.

Malgré toute ma vigilance et celle de mes relecteurs, il est possible que quelques erreurs subsistent dans ce article. J'accueillerai donc volontiers les commentaires, corrections ou critiques qui pourront m'être directement adressés à mon adresse email : elmoujibianas@gmail.com

J'ai eu beaucoup de plaisir à écrire ce document. J'espère qu'il pourra rendre service à ses lecteurs en leur donnant envie de continuer à s'investir dans les mathématiques. Je leur souhaite en tous cas beaucoup de courage, de persévérance et tous mes vœux de réussite.

J'ai décidé de laisser ce document à la disposition de tous plutôt que de le vendre, espérant qu'Allah l'acceptera de ma part et qu'il profitera à quiconque le lira ; je vous demande de prier pour moi et pour mes parents.

Table des matières

1	LES NOMBRES COMPLEXES	6
1.1	Introduction	6
1.1.1	Présentation de $\mathbb{C}$	6
1.2	Le plan complexe	7
1.3	Conjugaison d'un nombre complexe	8
1.4	Module d'un nombre complexe	9
1.5	Argument d'un nombre complexe	12
1.5.1	Exponentielle imaginaire	12
1.5.2	Complexe de module 1	14
1.5.3	Argument d'un nombre complexe non nul	14
1.6	Exponentielle complexe	15
1.7	Applications trigonometriques des nombres complexes	16
1.8	RACINES $n^{\text{ème}}$ D'UN NOMBRE COMPLEXE NON NUL	18
1.8.1	RACINES $n^{\text{ème}}$ DE L'UNITÉ	18
1.8.2	RACINES $n^{\text{ème}}$ D'UN NOMBRE COMPLEXE NON NUL	22
1.9	ÉQUATIONS DU SECOND DEGRÉ DANS $\mathbb{C}$	23
1.9.1	RACINES CARRÉES D'UN NOMBRE COMPLEXE	23
1.9.2	RÉSOLUTION ALGÈBRIQUE D'UNE ÉQUATION DU SECOND DEGRÉ DANS $\mathbb{C}$	24
1.10	TRANSFORMATIONS USUELLES DU PLAN	27
1.10.1	LA TRANSLATION	27
1.10.2	L'HOMOTHÉTIE	28
1.10.3	LA ROTATION	28
1.10.4	COMPOSITION DE QUELQUES TRANSFORMATIONS DU PLAN	29
2	L'Arithmétique dans $\mathbb{Z}$	32
2.1	Divisibilité dans $\mathbb{Z}$	32
2.1.1	Définitions	32
2.1.2	Propriétés	32
2.2	Division Euclidienne	34
2.2.1	Division euclidienne dans $\mathbb{N}$	34
2.2.2	Division euclidienne dans $\mathbb{Z}$	35
2.3	Nombres Premiers	37

2.3.1	Définition d'un nombre premier :	37
2.3.2	Propriétés :	37
2.4	Décomposition en facteurs premiers d'un entier relatif - Applications	39
2.4.1	Propriété	39
2.4.2	Diviseurs d'un entier relatif non nul et différent de -1 et 1	40
2.4.3	Multiples d'un entier non nul et non 1 et -1	41
2.4.4	PGCD de deux entiers naturels non {0 et 1}	42
2.5	PGCD-Algorithmme d'Euclide-PPCM	43
2.5.1	Plus Grand Commun Diviseur (PGCD)	43
2.5.2	Calcul Pratique du P.G.C.D : L'ALGORITHME D'EUCLIDE	44
2.5.3	Plus Petit Commun Multiple (PPCM) :	45
2.6	Congruence modulo n	47
2.6.1	Définition et Exemples :	47
2.6.2	Propriétés :	47
2.7	L'Ensemble $\mathbb{Z}/n\mathbb{Z}$	48
2.7.1	Classes d'Équivalence	48
2.7.2	L'ensemble $\mathbb{Z}/n\mathbb{Z}$	49
2.7.3	Operations dans l'ensemble $\mathbb{Z}/n\mathbb{Z}$	50
2.8	Nombres premiers entre eux	51
2.8.1	Définitions	51
2.8.2	Propriétés	51
2.9	L'équation diophantienne $ax + by = c$ dans $\mathbb{Z}^2$	53
2.9.1	Activité Preuve :	53
2.9.2	Propriétés	55
2.10	PGCD et PPCM de plusieurs entières relatifs	55
2.10.1	Définitions	55
2.10.2	Propriétés	56
2.11	Complément sur les nombres premiers	57
2.11.1	Nombres premiers et divisibilité	57
2.12	Système de Numération	59
2.12.1	Définition des systèmes de Numération	59
2.12.2	Représentation d'un entier naturel dans un système de numération connus	59
2.12.3	Techniques de représentation d'un entier dans une base de numération	60
2.12.4	section D'une base de numération à une autre	60
2.12.5	Addition et multiplication des nombres représentés dans une base	61

2.12.6	Comparaison de deux nombres dans un systèmes de numération	62
2.12.7	Critère de divisibilité dans la base décimal	63
3	LOIS DE COMPOSITION INTERNE (L.C.I)	66
3.1	Introduction	66
3.2	Définition d'une loi de composition interne	67
3.3	Morphismes	69
4	Généralités sur les Matrices carrés	75
4.1	Matrice carrée d'ordre 2	75
4.2	Matrice carrée d'ordre 3	76
5	Groupes, Anneaux et Corps	80
5.1	Groupes	80
5.1.1	Définitions et premiers exemples	80
5.1.2	Sous-groupes	81
5.1.3	Homomorphismes de groupes	82
5.2	Anneaux	84
5.2.1	Distributivité	84
5.2.2	Structure d'Anneaux	85
5.2.3	Règles de calcul dans un Anneaux	85
5.2.4	Diviseurs de zéro dans un Anneaux-Anneaux intègre	86
5.3	Corps	87
6	Espaces Vectoriel Réels ($\mathbb{K} = \mathbb{R}$)	90
6.1	Espace vectoriel réel	90
6.1.1	Loi de composition externe (L.C.E)	90
6.1.2	Définition et propriétés d'un espace vectoriel	90
6.2	Sous-espace vectoriel	92
6.3	Familles libres- Familles génératrice- Bases	93
6.3.1	Combinaisons linéaires	93
6.3.2	Familles Libres-Familles liées	94
6.3.3	Familles génératrice	96
6.3.4	Bases d'un espace vectoriel réel	97
6.3.5	Dimension d'un espace vectoriel	98

Chapitre 1

LES NOMBRES COMPLEXES

1.1 Introduction

1.1.1 Présentation de $\mathbb{C}$

$\mathbb{C}$ est un ensemble contenant $\mathbb{R}$ dont les éléments sont appelés nombres complexes.

$\mathbb{C}$ est muni de deux opérations $+$ et $\times$ prolongeant les opérations existant sur $\mathbb{R}$ et conservant leurs propriétés.

$\mathbb{C}$ ne peut pas être muni d'une relation d'ordre « intéressante » mais en revanche, sur $\mathbb{C}$ l'équation $x^2 = -1$ possède deux solutions opposées notées i et $-i$.

Par construction de $\mathbb{C}$, on a

$$\forall z \in \mathbb{C}, \exists! (a, b) \in \mathbb{R}^2, z = a + i.b$$

Définition 1.1.1. L'écriture $z = a + i.b$ est appelée forme algébrique du complexe z . Les réels a et b sont respectivement appelés parties réelle et imaginaire de z . On note $a = \operatorname{Re}(z)$ et $b = \operatorname{Im}(z)$.

Remarque 1.1.1. La partie imaginaire d'un complexe est un nombre réel !

Proposition 1.1.1. $\forall z, z' \in \mathbb{C}, \operatorname{Re}(z + z') = \operatorname{Re}(z) + \operatorname{Re}(z')$ et $\operatorname{Im}(z + z') = \operatorname{Im}(z) + \operatorname{Im}(z')$. $\forall z, z' \in \mathbb{C}, \operatorname{Re}(zz') = \operatorname{Re}(z)\operatorname{Re}(z') - \operatorname{Im}(z)\operatorname{Im}(z')$ et $\operatorname{Im}(zz') = \operatorname{Re}(z)\operatorname{Im}(z') + \operatorname{Re}(z')\operatorname{Im}(z)$.

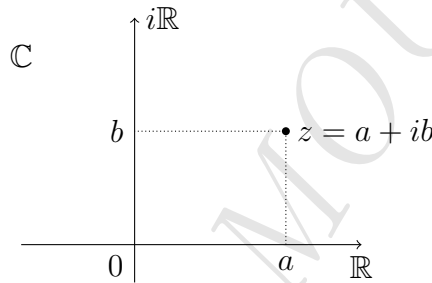
Démonstration On peut écrire $z = a + ib$ et $z' = a' + ib'$ avec $a, b, a', b' \in \mathbb{R}$. On a alors $z + z' = (a + a') + i(b + b')$ avec $a + a', b + b' \in \mathbb{R}$. On en déduit $\operatorname{Re}(z + z') = \operatorname{Re}(z) + \operatorname{Re}(z')$ et $\operatorname{Im}(z + z') = \operatorname{Im}(z) + \operatorname{Im}(z')$. On a aussi $zz' = (aa' - bb') + i(ab' + a'b)$ avec $aa' - bb', ab' + a'b \in \mathbb{R}$. On en déduit $\operatorname{Re}(zz') = \operatorname{Re}(z)\operatorname{Re}(z') - \operatorname{Im}(z)\operatorname{Im}(z')$ et $\operatorname{Im}(zz') = \operatorname{Re}(z)\operatorname{Im}(z') + \operatorname{Re}(z')\operatorname{Im}(z)$.

1.2 Le plan complexe

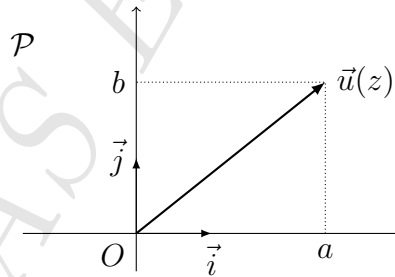
Soit $\mathcal{P}$ un plan géométrique rapporté à un repère orthonormé direct $\mathcal{R} = (O; \vec{i}, \vec{j})$.

Définition 1.2.1. On appelle point d'affixe $z \in \mathbb{C}$ le point M de coordonnées (a, b) avec $a = \operatorname{Re}(z)$ et $b = \operatorname{Im}(z)$. On note $M(z)$ pour signifier que M est le point d'affixe z .

Remarque 1.2.1. Par la notion d'affixe, à tout nombre complexe correspond un point du plan et à tout point correspond un nombre complexe. Cela permet de visualiser $\mathbb{C}$ tel un plan :



Définition 1.2.2. On appelle vecteur d'affixe z le vecteur $\vec{u}$ de composantes (a, b) avec $a = \operatorname{Re}(z)$ et $b = \operatorname{Im}(z)$. On note $\vec{u}(z)$ pour signifier que $\vec{u}$ est le vecteur d'affixe z .



Proposition 1.2.1. Si $\vec{u}$ est d'affixe z et $\vec{v}$ d'affixe z' alors $\vec{u} + \vec{v}$ est d'affixe $z + z'$. Si $\vec{u}$ est d'affixe z et λ un réel alors $\lambda \vec{u}$ est d'affixe λz . Si M est d'affixe z alors $\overrightarrow{OM}$ est d'affixe z et inversement. Si M est d'affixe z et M' d'affixe z' alors $\overrightarrow{MM'}$ est d'affixe $z' - z$.

Démonstration C'est immédiat en raisonnant via les composantes.

Proposition 1.2.2. Si M est d'affixe z alors le point M' d'affixe $-z$ est la symétrique de M par rapport à O .

Démonstration Par les affixes, $\overrightarrow{OM'} = -\overrightarrow{OM}$.

Proposition 1.2.3. Si M est d'affixe z et $a \in \mathbb{C}$ alors le point M' est l'image de M par la translation de vecteur $\vec{u}$ d'affixe a .

Démonstration Par les affixes, $\overrightarrow{OM'} = \overrightarrow{OM} + \vec{u}$.

Proposition 1.2.4. Si M est d'affixe z et $\lambda \in \mathbb{R}$ alors le point M' d'affixe λz est l'image de M par l'homothétie de centre O et de rapport λ .

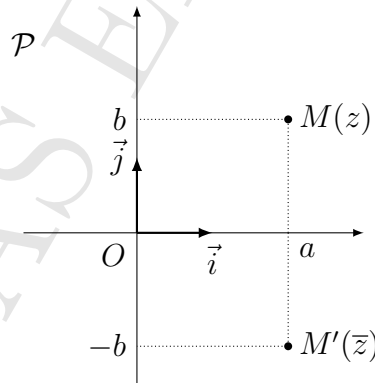
Démonstration Par les affixes, $\overrightarrow{OM'} = \lambda \overrightarrow{OM}$.

1.3 Conjugaison d'un nombre complexe

Définition 1.3.1. On appelle conjugué de $z = a + ib \in \mathbb{C}$ (avec $a, b \in \mathbb{R}$) le complexe $\bar{z} = a - ib$.

Proposition 1.3.1. Si M est d'affixe z alors le point M' d'affixe $\bar{z}$ est la symétrique de M par rapport à l'axe (Ox) .

Démonstration Le point M a pour coordonnées (a, b) et le point M' a pour coordonnées $(a, -b)$.



Proposition 1.3.2. $\forall z \in \mathbb{C}, \bar{\bar{z}} = z$.

Démonstration On peut écrire $z = a + ib$ avec $a, b \in \mathbb{R}$. On a alors $\bar{z} = a - ib = a + i(-b)$ avec $a, -b \in \mathbb{R}$ et donc $\bar{\bar{z}} = a + ib = z$.

Proposition 1.3.3. $\forall z, z' \in \mathbb{C}, \overline{z + z'} = \bar{z} + \bar{z'}, \overline{zz'} = \bar{z}\bar{z'}$ et, si $z \neq 0, \overline{\left(\frac{1}{z}\right)} = \frac{1}{\bar{z}}$.

Démonstration On peut écrire $z = a+ib$ et $z' = a'+ib'$ avec $a, b, a', b' \in \mathbb{R}$. On a $z + z' = (a + a') + i(b + b')$ avec $a + a' \in \mathbb{R}$ et $b + b' \in \mathbb{R}$, donc $\overline{z + z'} = (a + a') - i(b + b') = \overline{z} + \overline{z'}$. On a $zz' = (aa' - bb') + i(a'b + ab')$ avec $aa' - bb' \in \mathbb{R}$ et $ab' + a'b \in \mathbb{R}$, donc $\overline{zz'} = (aa' - bb') - i(a'b + ab') = (a - ib)(a' - ib') = \overline{z} \overline{z'}$. Enfin, puisque $z \times \frac{1}{z} = 1$, on a $\overline{z} \times \overline{\left(\frac{1}{z}\right)} = \overline{1} = 1$ donc $\overline{\left(\frac{1}{z}\right)} = \frac{1}{\overline{z}}$.

Proposition 1.3.4. $\forall z \in \mathbb{C}$,

$$\operatorname{Re}(z) = \frac{1}{2}(z + \overline{z}) \text{ et } \operatorname{Im}(z) = \frac{1}{2i}(z - \overline{z})$$

Démonstration Si $z = a + ib$ avec $a, b \in \mathbb{R}$ alors $\overline{z} = a - ib$ et donc $z + \overline{z} = 2a$ et $z - \overline{z} = 2ib$.

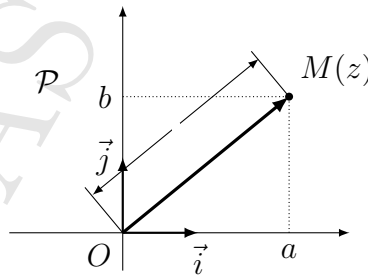
Remarque 1.3.1. Pour montrer qu'un complexe z est réel, on peut montrer que $\overline{z} = z$. Pour montrer qu'un complexe z est imaginaire pur, on peut montrer que $\overline{z} = -z$.

1.4 Module d'un nombre complexe

Définition 1.4.1. On appelle module d'un complexe $z = a+ib$ (avec $a, b \in \mathbb{R}$) le réel positif

$$|z| = \sqrt{a^2 + b^2}$$

Remarque 1.4.1. Si M est d'affixe z alors le module de z correspond à la longueur OM . $|z| = OM$



Remarque 1.4.2. La notion de module d'un complexe prolonge celle de valeur absolue d'un réel, il n'y a donc pas de conflit dans les notations.

Proposition 1.4.1. $\forall z \in \mathbb{C}, |z| = 0 \Leftrightarrow z = 0$.

Démonstration On peut écrire $z = a + ib$ avec $a, b \in \mathbb{R}$ et on a alors

$$|z| = 0 \Leftrightarrow \sqrt{a^2 + b^2} = 0 \Leftrightarrow a^2 + b^2 = 0 \Leftrightarrow a = b = 0 \Leftrightarrow z = 0$$

Proposition 1.4.2. $\forall z, z' \in \mathbb{C}, |z|^2 = z\bar{z} = |\bar{z}|^2, |zz'| = |z||z'|$ et, si $z \neq 0, \left|\frac{1}{z}\right| = \frac{1}{|z|}$.

Démonstration On peut écrire $z = a + ib$ avec $a, b \in \mathbb{R}$. On a alors $z\bar{z} = (a + ib)(a - ib) = a^2 + b^2 = |z|^2$ et aussi $z\bar{z} = \bar{z}\bar{z} = |\bar{z}|^2$. Ainsi $|z|^2 = z\bar{z} = |\bar{z}|^2$. Par suite $|zz'|^2 = zz'\bar{z}\bar{z}' = z\bar{z}z'\bar{z}' = |z|^2|z'|^2$. Cette égalité de carrés engageant des quantités positives, on en déduit $|zz'| = |z||z'|$. De plus, si $z \neq 0, z \times \frac{1}{z} = 1$ donne $|z| \times \left|\frac{1}{z}\right| = 1$ et donc $\left|\frac{1}{z}\right| = \frac{1}{|z|}$.

Remarque 1.4.3. Par une récurrence immédiate,

$$\forall z \in \mathbb{C}, \forall n \in \mathbb{N}, |z^n| = |z|^n$$

Par passage à l'inverse,

$$\forall z \in \mathbb{C}^*, \forall n \in \mathbb{Z}, |z^n| = |z|^n$$

Proposition 1.4.3. (*Inégalité triangulaire*)

$$\forall z, z' \in \mathbb{C}, |z + z'| \leq |z| + |z'|$$

De plus, il y a égalité si, et seulement si, les points d'affixe z et z' figurent sur une même demi-droite d'origine O .

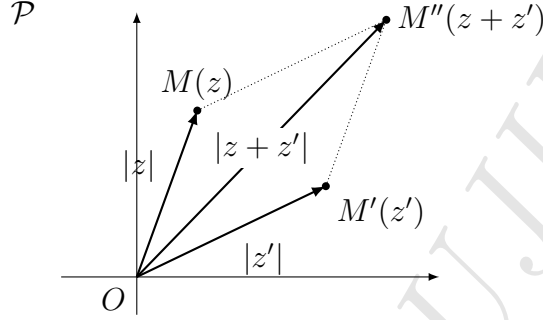
Démonstration Commençons par établir la propriété particulière : $\forall u \in \mathbb{C}, |1 + u| \leq 1 + |u|$ avec égalité si, et seulement si, $u \in \mathbb{R}^+$. Soit $u \in \mathbb{C}$. On peut écrire $u = a + ib$ avec $a, b \in \mathbb{R}$. On a alors

$$|1 + u|^2 = (1 + a)^2 + b^2 = 1 + 2a + a^2 + b^2 = 1 + 2a + |u|^2$$

Puisque $a = \operatorname{Re}(u) \leq |\operatorname{Re}(u)| \leq |u|$, on obtient $|1 + u|^2 \leq 1 + 2|u| + |u|^2 = (1 + |u|)^2$. Cette comparaison de carrés engageant des quantités positives, on en déduit $|1 + u| \leq 1 + |u|$. De plus il y a égalité si, et seulement si, $\operatorname{Re}(u) = |\operatorname{Re}(u)|$ et $|\operatorname{Re}(u)| = |u|$ c'est-à-dire $u \in \mathbb{R}^+$. Démontrons maintenant la propriété de façon générale. Soient $z, z' \in \mathbb{C}$. Cas $z = 0$: On a $|z + z'| = |z'| = |z| + |z'|$. L'inégalité est donc vraie. De plus c'est une égalité et les points d'affixes z et z' figurent sur une même demi-droite d'origine O . Cas $z \neq 0$: En introduisant $u = z'/z$, on a

$$|z + z'| = |z| \left| 1 + \frac{z'}{z} \right| = |z| |1 + u| \leq |z| (1 + |u|) = |z| + |z'|$$

De plus, il y a égalité si, et seulement si, $u \in \mathbb{R}^+$ i.e. $z'/z \in \mathbb{R}^+$. Ceci signifie que le point d'affixe z' figure sur la demi-droite d'origine O passant par le point d'affixe z .



Corollaire 1.4.1.

$$\forall z, z' \in \mathbb{C}, ||z| - |z'|| \leq |z - z'|$$

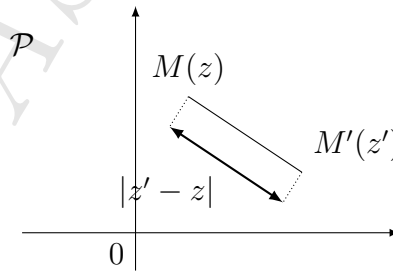
Démonstration. Par l'inégalité triangulaire,

$$|z| = |z - z' + z'| \leq |z - z'| + |z'|$$

donc $|z| - |z'| \leq |z - z'|$. De façon symétrique, $|z'| - |z| \leq |z' - z| = |z - z'|$.

Définition 1.4.2. On appelle distance entre deux complexes z et z' le réel positif $d(z, z') = |z' - z|$.

Remarque 1.4.4. Si M et M' sont les points d'affixes z et z' alors la distance entre z et z' est égale à la longueur MM' .

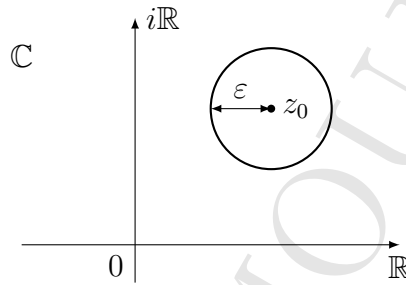


Proposition 1.4.4. Soient $z, z', z'' \in \mathbb{C}$. $d(z, z') = 0 \Leftrightarrow z = z'$ [séparation].
 $d(z', z) = |z - z'| = |z' - z| = d(z, z')$ [symétrie].
 $d(z, z') \leq d(z, z'') + d(z'', z')$ [inégalité triangulaire].

Démonstration. $d(z, z') = 0 \Leftrightarrow |z - z'| = 0 \Leftrightarrow z - z' = 0 \Leftrightarrow z = z'$.
 $d(z', z) = |z - z'| = |z' - z| = d(z, z')$. $d(z, z') = |z' - z| = |z' - z'' + z'' - z| \leq$
 $|z' - z''| + |z'' - z| = d(z'', z') + d(z, z'')$.

Définition 1.4.3. On appelle valeur approchée d'un complexe z_0 à $\varepsilon \in \mathbb{R}^+$ près tout complexe z vérifiant $|z - z_0| \leq \varepsilon$.

Remarque 1.4.5. Si $z = z_0$ à ε près alors le point d'affixe z appartient au disque de centre le point Ω d'affixe z_0 et de rayon ε .

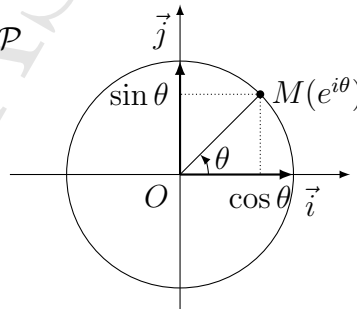


1.5 Argument d'un nombre complexe

1.5.1 Exponentielle imaginaire

Définition 1.5.1. On appelle exponentielle imaginaire d'angle $\theta \in \mathbb{R}$ le complexe : $e^{i\theta} = \cos \theta + i \sin \theta$.

Remarque 1.5.1. Le point M d'affixe $e^{i\theta}$ est le point du cercle trigonométrique déterminé par $(\vec{i}, \overrightarrow{OM}) = \theta \pmod{2\pi}$.



Exemple 1.5.1. $e^{i0} = 1, e^{i\pi/2} = i, e^{i\pi} = -1, e^{3i\pi/2} = -i$ et $e^{2i\pi} = 1$.

Proposition 1.5.1. $\forall \theta \in \mathbb{R}, |e^{i\theta}| = 1$ et $\frac{1}{e^{i\theta}} = e^{-i\theta} = \overline{e^{i\theta}}$.

Démonstration.

$$|e^{i\theta}|^2 = \cos^2 \theta + \sin^2 \theta = 1$$

et

$$\frac{1}{e^{i\theta}} = \frac{\overline{e^{i\theta}}}{|e^{i\theta}|^2} = \overline{e^{i\theta}} = \cos \theta - i \sin \theta = e^{-i\theta}$$

Proposition 1.5.2. $\forall \theta, \theta' \in \mathbb{R}, e^{i\theta} = e^{i\theta'} \Leftrightarrow \theta = \theta' \quad [2\pi]$

Démonstration.

$$e^{i\theta} = e^{i\theta'} \Leftrightarrow \begin{cases} \cos \theta = \cos \theta' \\ \sin \theta = \sin \theta' \end{cases} \Leftrightarrow \theta = \theta' \quad [2\pi]$$

Proposition 1.5.3. $\forall \theta, \theta' \in \mathbb{R}, e^{i\theta} \cdot e^{i\theta'} = e^{i(\theta+\theta')}.$

Démonstration.

$$e^{i\theta} \cdot e^{i\theta'} = (\cos \theta + i \sin \theta)(\cos \theta' + i \sin \theta')$$

En développant

$$e^{i\theta} \cdot e^{i\theta'} = (\cos \theta \cos \theta' - \sin \theta \sin \theta') + i(\cos \theta \sin \theta' + \sin \theta \cos \theta')$$

puis

$$e^{i\theta} \cdot e^{i\theta'} = \cos(\theta + \theta') + i \sin(\theta + \theta') = e^{i(\theta+\theta')}$$

Proposition 1.5.4. (Formule de Moivre) $\forall n \in \mathbb{Z}, \forall \theta \in \mathbb{R}, (e^{i\theta})^n = e^{in\theta}$ i.e.

$$(\cos \theta + i \sin \theta)^n = \cos n\theta + i \sin n\theta$$

Démonstration. Par récurrence, montrons que pour $n \in \mathbb{N}, e^{in\theta} = (e^{i\theta})^n$.
Pour $n = 0, e^{i0} = 1 = (e^{i\theta})^0$. Supposons la propriété établie au rang $n \geq 0$.

$$(e^{i\theta})^{n+1} = (e^{i\theta})^n e^{i\theta} = e^{in\theta} e^{i\theta} = e^{i(n+1)\theta}$$

Récurrence établie. Pour $n \in \mathbb{Z}^-, n = -p$ avec $p \in \mathbb{N}$.

$$(e^{i\theta})^n = (e^{i\theta})^{-p} = \frac{1}{(e^{i\theta})^p} = \frac{1}{e^{ip\theta}} = e^{-ip\theta} = e^{in\theta}$$

Proposition 1.5.5. (Formule d'Euler) $\forall \theta \in \mathbb{R} : \begin{cases} \cos \theta = \frac{e^{i\theta} + e^{-i\theta}}{2} \\ \sin \theta = \frac{e^{i\theta} - e^{-i\theta}}{2i} \end{cases}$

Remarque 1.5.2. (Attention !) Cette formule n'est valable que pour n entier

$$-1 = e^{i\pi} = (e^{2i\pi})^{1/2} = \sqrt{1} = 1!$$

1.5.2 Complexe de module 1

Définition 1.5.2. On note U l'ensemble des complexes de module 1. Ainsi

$$U = \{z \in \mathbb{C} / |z| = 1\}$$

Remarque 1.5.3. L'ensemble des point d'affixe dans U correspond géométriquement au cercle trigonométrique du plan.

Exemple 1.5.2. $\forall \theta \in \mathbb{R}, e^{i\theta} \in U$.

Exemple 1.5.3. Si $z \in U$ alors $1/z = \bar{z}$. En effet $z\bar{z} = |z|^2 = 1$.

Théorème 1.5.1. Pour tout $z \in U$, il existe un unique réel θ unique à 2π près tel que $z = e^{i\theta}$.

Démonstration. Unicité à 2π près : Si $z = e^{i\theta}$ et $z = e^{i\theta'}$ alors $e^{i\theta} = e^{i\theta'}$ et donc $\theta = \theta' \pmod{2\pi}$. Existence : Soit $z \in U$. On peut écrire $z = a + ib$ avec $a, b \in \mathbb{R}$. Puisque $|z|^2 = a^2 + b^2 = 1$, on a $a^2 \leq 1$ et donc $a \in [-1, 1]$. Par suite, il existe $\alpha \in \mathbb{R}$ tel que $a = \cos \alpha$. Puisque $b^2 = 1 - a^2 = \sin^2 \alpha$ donc $b = \sin \alpha$ ou $b = -\sin \alpha$. Si $b = \sin \alpha$ alors $z = e^{i\alpha}$ avec $\theta = \alpha$. Si $b = -\sin \alpha$ alors $z = e^{-i\alpha}$ avec $\theta = -\alpha$.

1.5.3 Argument d'un nombre complexe non nul

Théorème 1.5.2. Pour tout $z \in \mathbb{C}^*$, il existe un réel θ unique à 2π près tel que

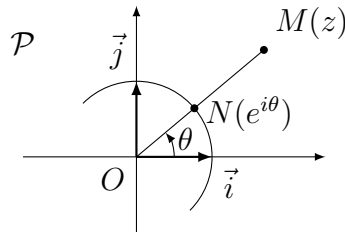
$$z = |z|e^{i\theta}$$

Cette écriture est appelée forme trigonométrique du complexe z .

Démonstration. Unicité à 2π près : Si $z = |z|e^{i\theta}$ et $z = |z|e^{i\theta'}$ alors $e^{i\theta} = e^{i\theta'}$ car $|z| \neq 0$ et donc $\theta = \theta' \pmod{2\pi}$. Existence : Puisque $z/|z| \in U$, il existe $\theta \in \mathbb{R}$ tel que $z/|z| = e^{i\theta}$ et donc $z = |z|e^{i\theta}$.

Définition 1.5.3. Tout réel θ tel que $z = |z|e^{i\theta}$ est appelé argument du complexe z non nul. On note $\arg(z) = \theta \pmod{2\pi}$.

Remarque 1.5.4. Si M est le point d'affixe $z \neq 0$ alors $\arg(z) = (\vec{i}, \overrightarrow{OM}) \pmod{2\pi}$.



Exemple 1.5.4. Déterminons un argument de $z = 1 + i$. $|z| = \sqrt{2}$ donc

$$1 + i = \sqrt{2} \left(\frac{1}{\sqrt{2}} + i \frac{1}{\sqrt{2}} \right) = \sqrt{2} \left(\cos \frac{\pi}{4} + i \sin \frac{\pi}{4} \right) = \sqrt{2} e^{i\pi/4}$$

On en déduit

$$\arg(1 + i) = \frac{\pi}{4} \quad [2\pi]$$

Exemple 1.5.5. Pour $z \in \mathbb{C}^*$,

$$z \in \mathbb{R}^{+*} \Leftrightarrow \arg(z) = 0 \quad [2\pi] \text{ et } z \in \mathbb{R}^{-*} \Leftrightarrow \arg(z) = \pi \quad [2\pi]$$

Par suite

$$z \in \mathbb{R}^* \Leftrightarrow \arg(z) = 0 \quad [\pi]$$

Proposition 1.5.6. Soient $z, z' \in \mathbb{C}^*$. $\arg(\bar{z}) = -\arg(z) \quad [2\pi]$, $\arg(zz') = \arg(z) + \arg(z') \quad [2\pi]$, $\arg(-z) = \arg(z) + \pi \quad [2\pi]$, $\arg(1/z) = -\arg(z) \quad [2\pi]$ et $\forall n \in \mathbb{Z}$, $\arg(z^n) = n \arg(z) \quad [2\pi]$

Démonstration. Soient $\theta = \arg(z)$ et $\theta' = \arg(z') \quad [2\pi]$ de sorte que $z = |z|e^{i\theta}$ et $z' = |z'|e^{i\theta'}$. $\bar{z} = |z|\overline{e^{i\theta}} = |z|e^{-i\theta}$ donc $\arg(\bar{z}) = -\theta \quad [2\pi]$. $zz' = |z||z'|e^{i\theta}e^{i\theta'} = |zz'|e^{i(\theta+\theta')}$ donc $\arg(zz') = \theta + \theta' \quad [2\pi]$. $-z = -|z|e^{i\theta} = |z|e^{i(\theta+\pi)}$ donc $\arg(-z) = \theta + \pi \quad [2\pi]$. $\frac{1}{z} = \frac{1}{|z|} \frac{1}{e^{i\theta}} = \left| \frac{1}{z} \right| e^{-i\theta}$ donc $\arg(1/z) = -\theta \quad [2\pi]$. $z^n = |z|^n (e^{i\theta})^n = |z^n|e^{in\theta}$ donc $\arg(z^n) = n\theta \quad [2\pi]$

Exemple 1.5.6. Déterminons module et argument du complexe $z = e^{i\theta} + 1$.

$$z = e^{i\theta} + 1 = (e^{i\theta/2} + e^{-i\theta/2})e^{i\theta/2} = 2 \cos \frac{\theta}{2} e^{i\theta/2}$$

[Factorisation de l'exponentielle équilibrée] On en déduit

$$|z| = 2 \left| \cos \frac{\theta}{2} \right|$$

Si $\cos \theta/2 > 0$ alors $\arg(z) = \theta/2 \quad [2\pi]$. Si $\cos \theta/2 < 0$ alors $\arg(z) = \theta/2 + \pi \quad [2\pi]$.

1.6 Exponentielle complexe

Définition 1.6.1. On appelle exponentielle complexe de $z = a + ib \in \mathbb{C}$ (avec $a, b \in \mathbb{R}$) le nombre complexe

$$\exp(z) = e^a \cdot e^{ib} = e^a (\cos b + i \sin b)$$

1.7. APPLICATIONS TRIGONOMETRIQUES DES NOMBRES COMPLEXES

Remarque 1.6.1. Si $z = a \in \mathbb{R}$ alors $\exp(z) = e^a \cdot e^{i0} = e^a$. L'exponentielle complexe prolonge l'exponentielle réelle connue. Si $z = i \cdot b \in i \cdot \mathbb{R}$ alors $\exp(z) = e^0 \cdot e^{ib} = e^{ib}$. L'exponentielle complexe prolonge aussi l'exponentielle imaginaire. On note souvent e^z au lieu de $\exp(z)$.

Théorème 1.6.1. Soient $z, z' \in \mathbb{C}$. $\overline{\exp(z)} = \exp(\bar{z})$, $\exp(z+z') = \exp(z) \exp(z')$, $\exp(z) \neq 0$ et $1/\exp(z) = \exp(-z)$.

Démonstration. On peut écrire $z = a + ib$ et $z' = a' + ib'$ avec $a, b, a', b' \in \mathbb{R}$. $\overline{\exp(z)} = \overline{e^a \cdot e^{ib}} = e^a e^{-ib} = \exp(\bar{z})$. $\exp(z+z') = \exp((a+a') + i(b+b')) = e^{a+a'} e^{i(b+b')} = e^a e^{ib} e^{a'} e^{ib'} = e^z e^{z'}$. On en déduit $1 = \exp(0) = \exp(z) \exp(-z)$ et donc $\exp(z) \neq 0$ avec $1/\exp(z) = \exp(-z)$.

Théorème 1.6.2. Soient $z, z' \in \mathbb{C}$.

$$\exp(z) = \exp(z') \Leftrightarrow \exists k \in \mathbb{Z}, z = z' + 2ik\pi$$

Démonstration. ($\Leftarrow$) Si $z = z' + 2ik\pi$ avec $k \in \mathbb{Z}$ alors $\exp(z) = \exp(z') \exp(2ik\pi) = \exp(z')$ car $\exp(2ik\pi) = 1$. ($\Rightarrow$) Supposons $\exp(z) = \exp(z')$. On peut écrire $z = a + ib$ et $z' = a' + ib'$ avec $a, b, a', b' \in \mathbb{R}$. On a alors $e^a e^{ib} = e^{a'} e^{ib'}$. En passant cette relation au module, on obtient $e^a = e^{a'}$ et donc $a = a'$ car l'exponentielle réelle prend des valeurs deux à deux distinctes. Sachant $e^a = e^{a'} \neq 0$, la relation $e^a e^{ib} = e^{a'} e^{ib'}$ donne $e^{ib} = e^{ib'}$ et donc $b = b' + 2k\pi$. Ainsi, il existe $k \in \mathbb{Z}$ tel que $b = b' + 2k\pi$ et donc $z = z' + 2ik\pi$.

1.7 Applications trigonometriques des nombres complexes

La formule du binôme de Newton, la formule de Moivre et les formules d'Euler permettent de transformer certaines expressions trigonométriques.

$\Rightarrow$ **Développement de $\cos(n\theta)$ et $\sin(n\theta)$: ** Soit $n \in \mathbb{N}^*$ et $\theta \in \mathbb{R}$. On a : $\cos(n\theta) + i \sin(n\theta) = (\cos \theta + i \sin \theta)^n = \sum_{k=0}^n C_n^k \cos^{n-k}(\theta) i^k \sin^k(\theta)$

En séparant les parties réelles et imaginaires, on en déduit les expressions de $\cos(n\theta)$ et $\sin(n\theta)$ en fonction de $\cos \theta$ et $\sin \theta$. Voici quelques exemples pratiques : * On a : $\cos(2\theta) + i \sin(2\theta) = (\cos \theta + i \sin \theta)^2 = \cos^2 \theta - \sin^2 \theta + 2i \sin \theta \cdot \cos \theta$, dont on déduit :

$$\cos(2\theta) = \cos^2 \theta - \sin^2 \theta = 2 \cos^2 \theta - 1 = 1 - 2 \sin^2 \theta \quad \text{et} \quad \sin(2\theta) = 2 \sin \theta \cdot \cos \theta.$$

* On a : $\cos(3\theta) + i \sin(3\theta) = (\cos \theta + i \sin \theta)^3$, donc :

$$\cos(3\theta) + i \sin(3\theta) = \cos^3 \theta + 3i \cos^2 \theta \cdot \sin \theta - 3 \cos \theta \cdot \sin^2 \theta - i \sin^3 \theta$$

1.7. APPLICATIONS TRIGONOMETRIQUES DES NOMBRES COMPLEXES

On en déduit :

$$\begin{cases} \cos(3\theta) = \cos^3 \theta - 3 \cos \theta \cdot \sin^2 \theta = \cos^3 \theta - 3 \cos \theta (1 - \cos^2 \theta) = 4 \cos^3 \theta - 3 \cos \theta \\ \sin(3\theta) = 3 \cos^2 \theta \cdot \sin \theta - \sin^3 \theta = 3(1 - \sin^2 \theta) \cdot \sin \theta - \sin^3 \theta = -4 \sin^3 \theta + 3 \sin \theta \end{cases}$$

On peut démontrer la formule plus générale suivante : (à titre d'exercice)
Pour tout $n \in \mathbb{N}^*$:

$$\begin{cases} \cos(n\theta) = \sum_{p=0}^{E(\frac{n}{2})} (-1)^p C_n^{2p} \cos^{n-2p}(\theta) \cdot \sin^{2p}(\theta) \\ \sin(n\theta) = \sum_{p=0}^{E(\frac{n-1}{2})} (-1)^p C_n^{2p+1} \cos^{n-2p-1}(\theta) \cdot \sin^{2p+1}(\theta) \end{cases}$$

($E(\frac{n}{2})$ étant la partie entière de $\frac{n}{2}$)

$\Rightarrow$ **Linéarisation de $\cos^m \theta$, $\sin^n \theta$ et $\cos^m \theta \cdot \sin^n \theta$ pour $(m; n) \in \mathbb{N}^2$: **
Linéariser une expression du genre $\cos^m \theta$, $\sin^n \theta$ et $\cos^m \theta \cdot \sin^n \theta$, c'est la transformer en somme algébrique de termes du genre $a \cos(p\theta) + b \sin(q\theta)$ avec $(a; b) \in \mathbb{R}^2$ et $(p; q) \in \mathbb{N}^2$.

Pour linéariser ces expressions, on utilise les formules d'Euler pour en déduire :

$$\cos^m \theta = \frac{1}{2^m} (e^{i\theta} + e^{-i\theta})^m \quad \text{et} \quad \sin^n \theta = \frac{1}{(2i)^n} (e^{i\theta} - e^{-i\theta})^n$$

On développe les expressions obtenues grâce au binôme de Newton, puis on fait réapparaître les fonctions cosinus et sinus. Voici quelques exemples pratiques :

— Linéarisation de $\cos^4 x$:

$$\cos^4 x = \left(\frac{e^{ix} + e^{-ix}}{2} \right)^4 = \frac{1}{16} ((e^{ix})^4 + 4(e^{ix})^3 e^{-ix} + 6(e^{ix})^2 (e^{-ix})^2 + 4e^{ix} (e^{-ix})^3 + (e^{-ix})^4)$$

$$\text{Donc : } \cos^4 x = \frac{1}{16} (e^{i4x} + e^{-i4x} + 4(e^{i2x} + e^{-i2x}) + 6) = \frac{1}{16} (2 \cos(4x) + 8 \cos(2x) + 6)$$

$$\text{Par suite : } \cos^4 x = \frac{1}{8} (\cos(4x) + 4 \cos(2x) + 3)$$

— Linéarisation de $\sin^5 x$:

$$\sin^5 x = \left(\frac{e^{ix} - e^{-ix}}{2i} \right)^5$$

$$= \frac{1}{32i} ((e^{ix})^5 - 5(e^{ix})^4 e^{-ix} + 10(e^{ix})^3 (e^{-ix})^2 - 10(e^{ix})^2 (e^{-ix})^3 + 5(e^{ix})(e^{-ix})^4 - (e^{-ix})^5)$$

$$\begin{aligned}
 &= \frac{1}{32i} (e^{i5x} - 5e^{i3x} + 10e^{ix} - 10e^{-ix} + 5e^{-i3x} - e^{-i5x}) \\
 &= \frac{1}{32i} ((e^{i5x} - e^{-i5x}) - 5(e^{i3x} - e^{-i3x}) + 10(e^{ix} - e^{-ix}))
 \end{aligned}$$

$$\text{Par suite : } \sin^5 x = \frac{1}{16} (\sin(5x) - 5 \sin(3x) + 10 \sin x)$$

— Linéarisation de $\cos^2(x) \cdot \sin^3(x)$:

$$\text{On a : } \cos^2 x = \left(\frac{e^{ix} + e^{-ix}}{2} \right)^2 = \frac{1}{4} (e^{i2x} + 2 + e^{-i2x}) = \frac{1}{4} (2 \cos(2x) + 2) = \frac{1}{2} (\cos(2x) + 1)$$

$$\text{Et : } \sin^3 x = \left(\frac{e^{ix} - e^{-ix}}{2i} \right)^3 = -\frac{1}{8i} (e^{i3x} - 3e^{ix} + 3e^{-ix} - e^{-i3x}) = -\frac{1}{4} (\sin(3x) - 3 \sin x)$$

Il s'ensuit donc :

$$\cos^2 x \sin^3 x = \left(\frac{1}{2} (\cos(2x) + 1) \right) \left(-\frac{1}{4} (\sin(3x) - 3 \sin x) \right)$$

$$= -\frac{1}{8} (\cos(2x) \sin(3x) - 3 \cos(2x) \sin(x) + \sin(3x) - 3 \sin(x))$$

$$\text{Et puisque : } \cos(2x) \sin(3x) = \frac{1}{2} (\sin(5x) + \sin x) \quad \text{et} \quad \cos(2x) \sin x = \frac{1}{2} (\sin(3x) - \sin x)$$

$$\text{Alors : } \cos^2(x) \cdot \sin^3(x) = -\frac{1}{16} (\sin(5x) - \sin(3x) - 2 \sin x)$$

1.8 RACINES $n^{\text{ème}}$ D'UN NOMBRE COMPLEXE NON NUL

1.8.1 RACINES $n^{\text{ème}}$ DE L'UNITÉ

Définition 1.8.1. Soit n un entier naturel supérieur ou égal à 2. On appelle racine $n^{\text{ème}}$ de l'unité tout nombre complexe u tel que $u^n = 1$. L'ensemble des racines $n^{\text{ème}}$ de l'unité est noté $\mathbb{U}_n$. On a donc : $\mathbb{U}_n = \{z \in \mathbb{C} / z^n = 1\}$

Remarque 1.8.1. Les racines $n^{\text{ème}}$ de l'unité sont les solutions dans $\mathbb{C}$ de l'équation $z^n = 1$.

Exemple 1.8.1. 1) Cas $n = 2$: Les racines carrées de l'unité sont les solutions dans $\mathbb{C}$ de l'équation $z^2 = 1$. Ces solutions sont 1 et -1 . Ainsi : $\mathbb{U}_2 = \{-1; 1\}$

2) Cas $n = 3$: Les racines cubiques de l'unité sont les solutions dans $\mathbb{C}$ de l'équation $z^3 = 1$. Remarquons que si $z^3 = 1$ alors $|z^3| = |z|^3 = 1$ et par suite que $|z| = 1$. Cela montre que les solutions de l'équation $z^3 = 1$ s'écrivent sous la forme $e^{i\theta}$ avec $e^{3i\theta} = 1$, c'est-à-dire $3\theta \equiv 0 \pmod{2\pi}$. Par conséquent, $\theta = k\frac{2\pi}{3}$ avec $k \in \mathbb{Z}$. En posant $\omega_k = e^{ik\frac{2\pi}{3}} = (\omega_1)^k$, on obtient :

- $\omega_0 = 1$.
- $\omega_1 = e^{i\frac{2\pi}{3}} = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$. On note souvent ce nombre par j : $j = e^{i\frac{2\pi}{3}} = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$.
- $\omega_2 = e^{i\frac{4\pi}{3}} = -\frac{1}{2} - i\frac{\sqrt{3}}{2}$. Remarquons que : $\omega_2 = j^2 = \bar{j}$
- $\omega_3 = 1$ et $\omega_4 = \omega_1$ et $\omega_5 = \omega_2$ et ainsi de suite.

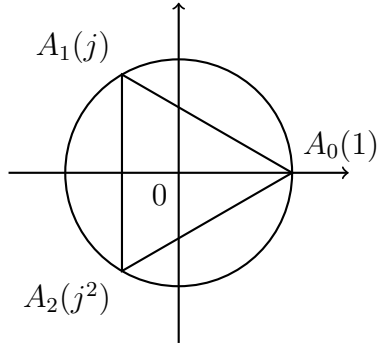
Par suite, les racines cubiques de l'unité sont 1, j et j^2 : $\mathbb{U}_3 = \{1; j; j^2\}$

Remarque 1.8.2. — On a : $1+j+j^2 = 0$ et $z^3 - 1 = (z-1)(z-j)(z-j^2)$ pour tout $z \in \mathbb{C}$.

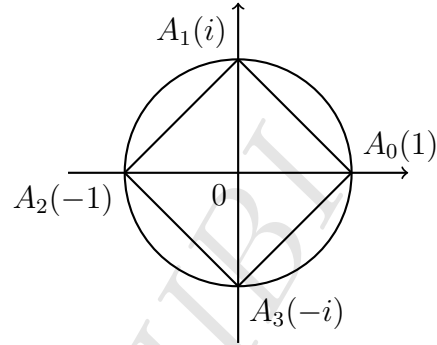
- Pour $n \in \{2; 3; 4\}$, le produit de deux éléments de $\mathbb{U}_n$ est aussi élément de $\mathbb{U}_n$. En fait, ce résultat est valable pour tout entier $n \geq 2$.
- Pour $n \in \{2; 3; 4\}$, l'inverse et le conjugué de tout élément de $\mathbb{U}_n$ sont aussi des éléments de $\mathbb{U}_n$. En fait, ce résultat est valable pour tout entier $n \geq 2$. On a donc pour tout $z \in \mathbb{C}$:

$$z \in \mathbb{U}_n \Leftrightarrow \bar{z} \in \mathbb{U}_n \Leftrightarrow \frac{1}{z} \in \mathbb{U}_n$$

- Soit A_0, A_1 et A_2 les points du plan d'affixes respectives 1, j et j^2 . Alors, $A_0A_1A_2$ est un triangle équilatéral inscrit dans le cercle trigonométrique.
- Soit A_0, A_1, A_2 et A_3 les points du plan d'affixes respectives 1, i , -1 et $-i$. Alors, $A_0A_1A_2A_3$ est un carré inscrit dans le cercle trigonométrique.



Interprétation des racines cubiques de l'unité.



Interprétation des racines quatrièmes de l'unité.

Proposition 1.8.1. Soit n un entier naturel supérieur ou égal à 2. Les racines $n^{\text{ème}}$ de l'unité sont les nombres qui s'écrivent sous la forme $e^{i\frac{2k\pi}{n}}$ où $k \in \{0; 1; 2; \dots; n-1\}$. On a donc :

$$\mathbb{U}_n = \left\{ e^{i\frac{2k\pi}{n}} / k \in \{0; 1; \dots; n-1\} \right\} \quad \text{et} \quad \text{card } \mathbb{U}_n = n$$

Démonstration. Soit z une racine $n^{\text{ème}}$ de 1. On a donc $z^n = 1$. En passant au module, on obtient $|z^n| = 1$, d'où $|z|^n = 1$. Puisque $|z|$ est positif, on déduit que $|z| = 1$. Ainsi, z est de la forme $z = e^{i\theta}$. On a alors :

$$z^n = 1 \Leftrightarrow e^{in\theta} = 1 \Leftrightarrow (n\theta = 0 \quad [2\pi]) \Leftrightarrow \left(\theta = 0 \quad \left[\frac{2\pi}{n} \right] \right)$$

Le réel θ est donc de la forme $\frac{2k\pi}{n}$ avec $k \in \mathbb{Z}$. On obtient finalement $z = e^{i\frac{2k\pi}{n}}$. Or, on constate que :

$$e^{i\frac{2n\pi}{n}} = 1 \quad ; \quad e^{i\frac{2(n+1)\pi}{n}} = e^{i\frac{2\pi}{n}} \quad ; \quad e^{i\frac{2(n+2)\pi}{n}} = e^{i\frac{4\pi}{n}} \quad ; \dots$$

Autrement dit, si k et k' sont deux entiers relatifs tels que $k - k'$ est un multiple de n , alors, $e^{i\frac{2k\pi}{n}} = e^{i\frac{2k'\pi}{n}}$. On peut donc se contenter de faire varier k dans l'ensemble des entiers compris entre 0 et $n-1$. Réciproquement, si $z = e^{i\frac{2k\pi}{n}}$ avec $k \in \{0; 1; 2; \dots; n-1\}$, alors $z^n = \left(e^{i\frac{2k\pi}{n}} \right)^n = e^{i2k\pi} = 1$, d'où z est bien une racine $n^{\text{ème}}$ de l'unité.

Proposition 1.8.2. Soit n un entier naturel supérieur ou égal à 2. Pour tous u et v de $\mathbb{U}_n$: $u \times v \in \mathbb{U}_n$ et $\frac{1}{u} \in \mathbb{U}_n$ et $\bar{u} \in \mathbb{U}_n$ ($\bar{u} = \frac{1}{u}$)

Démonstration. Soit u et v deux éléments de $\mathbb{U}_n$, c'est-à-dire que $u^n = 1$ et $v^n = 1$. Donc :

- $(u \times v)^n = u^n \times v^n = 1 \times 1 = 1$, et donc $u \times v \in \mathbb{U}_n$.
- $\left(\frac{1}{u}\right)^n = \frac{1}{u^n} = \frac{1}{1} = 1$, et donc $\frac{1}{u} \in \mathbb{U}_n$.
- $(\bar{u})^n = \overline{u^n} = \overline{1} = 1$, et donc $\bar{u} \in \mathbb{U}_n$.

Ce qui achève la démonstration.

Exemple 1.8.2. 1) Les racines $6^{\text{ème}}$ de l'unité sont les nombres complexes $\omega_k = e^{i\frac{2k\pi}{6}} = e^{i\frac{k\pi}{3}}$ avec $k \in \{0; 1; \dots; 5\}$. Il s'ensuit donc : $\omega_0 = 1$; $\omega_1 = e^{i\frac{\pi}{3}} = \frac{1}{2} + \frac{\sqrt{3}}{2}i$; $\omega_2 = e^{i\frac{2\pi}{3}} = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$; $\omega_3 = e^{i\frac{3\pi}{3}} = e^{i\pi} = -1$; $\omega_4 = e^{i\frac{4\pi}{3}} = \overline{\omega_2} = -\frac{1}{2} - \frac{\sqrt{3}}{2}i$; $\omega_5 = e^{i\frac{5\pi}{3}} = \overline{\omega_1} = \frac{1}{2} - \frac{\sqrt{3}}{2}i$

2) Les racines $8^{\text{ème}}$ de l'unité sont les nombres complexes $\omega_k = e^{i\frac{2k\pi}{8}} = e^{i\frac{k\pi}{4}}$ avec $k \in \{0; 1; \dots; 7\}$. Il s'ensuit donc : $\omega_0 = 1$; $\omega_1 = e^{i\frac{\pi}{4}} = \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}$; $\omega_2 = e^{i\frac{2\pi}{4}} = i$; $\omega_3 = e^{i\frac{3\pi}{4}} = -\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}$; $\omega_4 = e^{i\pi} = -1$; $\omega_5 = e^{i\frac{5\pi}{4}} = -\frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2}$; $\omega_6 = e^{i\frac{6\pi}{4}} = -i$; $\omega_7 = e^{i\frac{7\pi}{4}} = \frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2}$. Remarquer bien qu'on a : $\omega_5 = \overline{\omega_3}$; $\omega_6 = \overline{\omega_2}$; $\omega_7 = \overline{\omega_1}$.

Proposition 1.8.3. Soit n un entier naturel supérieur ou égal à 2. Posons, pour tout $k \in \{0; 1; \dots; n-1\}$: $\omega_k = e^{i\frac{2k\pi}{n}}$. Alors : 1) Pour tout $k \in \{1; \dots; n-1\}$: $\overline{\omega_k} = \omega_{n-k}$. 2) Pour tout $k \in \{0; 1; \dots; n-1\}$: $\omega_k = \omega_1^k$. 3) La somme des n racines $n^{\text{ème}}$ de l'unité est nulle. 4) Les racines $n^{\text{ème}}$ de l'unité sont représentées dans le plan complexe par les sommets d'un polygone régulier à n côtés inscrit dans le cercle trigonométrique, et dont l'un des sommets est le point d'abscisse 1. Ce polygone est symétrique par rapport à l'axe des abscisses.

Démonstration. 1) On a $\overline{\omega_k} = \overline{e^{i\frac{2k\pi}{n}}} = e^{-i\frac{2k\pi}{n}}$ et $\omega_{n-k} = e^{i\frac{2(n-k)\pi}{n}} = e^{i(2\pi - \frac{2k\pi}{n})} = e^{i2\pi} \times e^{-i\frac{2k\pi}{n}} = e^{-i\frac{2k\pi}{n}}$, d'où l'égalité annoncée.

2) On a : $\omega_k = e^{i\frac{2k\pi}{n}} = \left(e^{i\frac{2\pi}{n}}\right)^k = \omega_1^k$.

3) D'après 2), on peut écrire : $\omega_0 + \omega_1 + \dots + \omega_{n-1} = 1 + \omega_1 + \omega_1^2 + \omega_1^3 + \dots + \omega_1^{n-1}$. Nous reconnaissons la somme des termes de la suite géométrique de premier terme 1 et de raison $\omega_1 \neq 1$ (car $n \geq 2$), d'où : $\omega_0 + \omega_1 + \dots + \omega_{n-1} = \frac{1 - \omega_1^n}{1 - \omega_1} = \frac{1 - e^{i2\pi}}{1 - \omega_1} = \frac{1 - 1}{1 - \omega_1} = 0$. Ainsi, la somme des n racines $n^{\text{ème}}$ de l'unité est nulle.

4) Les racines $n^{\text{ème}}$ de l'unité sont au nombre de n , toutes de module 1, donc, situées sur le cercle trigonométrique. Elles sont représentées par les sommets d'un polygone à n côtés inscrit dans ce cercle. D'autre part : Pour

tout $k \in \{0; 1; \dots; n-2\}$:

$$\begin{aligned} \arg(\omega_{k+1}) - \arg(\omega_k) &= \frac{2(k+1)\pi}{n} - \frac{2k\pi}{n} \quad [2\pi] & \arg(\omega_0) - \arg(\omega_{n-1}) &= 0 - \frac{2(n-1)\pi}{n} \quad [2\pi] \\ &= \frac{2\pi}{n} \quad [2\pi] & \text{et} & &= \frac{2\pi}{n} \quad [2\pi] \end{aligned}$$

On passe donc d'un sommet du polygone au suivant en effectuant une rotation de centre O et d'angle $\frac{2\pi}{n}$. On peut donc dire que les racines $n^{\text{ème}}$ de l'unité sont représentées par les sommets d'un polygone régulier à n côtés inscrit dans le cercle trigonométrique. Enfin, la propriété 1) montre la symétrie par rapport à l'axe (Ox) .

1.8.2 RACINES $n^{\text{ème}}$ D'UN NOMBRE COMPLEXE NON NUL

Définition 1.8.2. Soit Z un nombre complexe non nul et n un entier naturel supérieur ou égal à 2. Une racine $n^{\text{ème}}$ de Z est un nombre complexe z tel que $z^n = Z$.

Proposition 1.8.4. Soit $n \in \mathbb{N}^* - \{1\}$ et Z un nombre complexe non nul d'argument φ : $Z = |Z|.e^{i\varphi}$. Le nombre Z admet exactement n racines $n^{\text{ème}}$ données par :

$$z_k = \sqrt[n]{|Z|} e^{i\left(\frac{\varphi+k2\pi}{n}\right)} \quad \text{avec } k \in \{0; 1; \dots; n-1\}$$

Démonstration. Soit $n \in \mathbb{N}^* - \{1\}$. On cherche les racines $n^{\text{ème}}$ de Z sous la forme $z = re^{i\theta}$ avec $r > 0$.

L'égalité $z^n = Z$ se traduit par $r^n = |Z|$ et $n\theta = \varphi \quad [2\pi]$, donc par : $r = \sqrt[n]{|Z|}$ et $\theta = \frac{\varphi}{n} \quad \left[\frac{2\pi}{n}\right]$.

En posant $z_k = \sqrt[n]{|Z|} e^{i\left(\frac{\varphi+k2\pi}{n}\right)}$, l'égalité $z_{k'} = z_k$ se traduit par : $\frac{\varphi+2k'\pi}{n} = \frac{\varphi+2k\pi}{n} \quad [2\pi]$

c'est-à-dire $k' = k \quad [n]$.

Les racines $n^{\text{ème}}$ de Z sont donc les n nombres complexes deux à deux distincts :

$$z_k = \sqrt[n]{|Z|} e^{i\left(\frac{\varphi+k2\pi}{n}\right)} \quad \text{avec } k \in \{0; 1; \dots; n-1\}$$

Remarque 1.8.3. — Les racines $n^{\text{ème}}$ de Z s'obtiennent à partir de l'une d'entre elles en multipliant celle-ci par chacune des racines $n^{\text{ème}}$ de l'unité. En effet, si z_0 est l'une des racines $n^{\text{ème}}$ de Z , on a :

$$z^n = Z \Leftrightarrow z^n = z_0^n \Leftrightarrow \left(\frac{z}{z_0}\right)^n = 1 \Leftrightarrow [(\exists \omega \in \mathbb{U}_n) \quad z = \omega z_0]$$

1.9. ÉQUATIONS DU SECOND DEGRÉ DANS $\mathbb{C}$

Par suite, l'ensemble des racines $n^{\text{ème}}$ de Z est : $\{z_0\omega/\omega \in \mathbb{U}_n\}$.

Ainsi, pour trouver les racines $n^{\text{ème}}$ de Z , il suffit donc d'en exhiber une et de la multiplier par toutes les racines $n^{\text{ème}}$ de l'unité.

- Une bonne connaissance des racines $n^{\text{ème}}$ de l'unité est donc capitale pour résoudre ce type de problème.

Exemple 1.8.3. 1) Déterminons les racines cubiques du nombre complexe : $Z = 4\sqrt{2}(-1+i)$

On a $|Z| = 4\sqrt{2}|-1+i| = 8$, donc : $Z = 8 \left(-\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2} \right) = 8e^{i\frac{3\pi}{4}} = (2e^{i\frac{\pi}{4}})^3$

Par suite, les racines cubiques de Z sont les nombres : $z_0 = 2e^{i\frac{\pi}{4}}$ et $z_1 = jz_0$ et $z_2 = j^2z_0$

Et comme $j = e^{i\frac{2\pi}{3}}$ et $j^2 = e^{i\frac{4\pi}{3}}$, alors : $z_1 = 2e^{i(\frac{\pi}{4} + \frac{2\pi}{3})} = 2e^{i\frac{11\pi}{12}}$ et $z_2 = 2e^{i(\frac{\pi}{4} + \frac{4\pi}{3})} = 2e^{i\frac{19\pi}{12}}$.

On peut aussi déterminer les écritures algébriques de ces racines cubiques à partir de celles de z_0, j et j^2 .

2) Déterminons les racines quatrièmes (ou d'ordre 4) de nombre -1 , c'est-à-dire les solutions de $z^4 = -1$.

$$\text{On a : } z^4 = -1 \Leftrightarrow z^4 = e^{i\pi} \Leftrightarrow z^4 = (e^{i\frac{\pi}{4}})^4$$

et Par suite, les racines quatrièmes 4 de nombre -1 sont :

$$z_0 = e^{i\frac{\pi}{4}} \quad ; \quad z_1 = e^{i(\frac{\pi}{4} + \frac{\pi}{2})} = e^{i\frac{3\pi}{4}} \quad ; \quad z_2 = e^{i(\frac{\pi}{4} + \pi)} = -e^{i\frac{\pi}{4}} \quad ; \quad z_3 = e^{i(\frac{\pi}{4} + \frac{3\pi}{2})} = e^{i\frac{7\pi}{4}} = e^{-i\frac{\pi}{4}}$$

1.9 ÉQUATIONS DU SECOND DEGRÉ DANS $\mathbb{C}$

1.9.1 RACINES CARRÉES D'UN NOMBRE COMPLEXE

On sait que tout nombre complexe non nul Z admet exactement deux racines carrées opposées. Ce sont les solutions dans $\mathbb{C}$ de l'équation $z^2 = Z$.

L'utilisation des formes trigonométrique ou exponentielle donne facilement les expressions des racines carrées d'un nombre complexe non nul quelconque mais on a parfois besoin d'exprimer une racine sous forme algébrique. Dans la pratique, on rencontre deux cas :

1.9. ÉQUATIONS DU SECOND DEGRÉ DANS $\mathbb{C}$

1^{er} cas : Si $Z = |Z|e^{i\varphi}$ alors, d'après la proposition précédente, les racines carrées du nombre Z sont :

$$\sqrt{|Z|}e^{i\frac{\varphi}{2}} \quad \text{et} \quad \sqrt{|Z|}e^{i(\frac{\varphi}{2}+\pi)}$$

2nd cas : Si $Z = X + iY$ avec $(X; Y) \in \mathbb{R}^2 - \{(0; 0)\}$. On pose $z = x + iy$ avec $(x; y) \in \mathbb{R}^2$. On a :

$$z^2 = Z \Leftrightarrow X + iY = (x + iy)^2 \Leftrightarrow \begin{cases} x^2 - y^2 = X \\ 2xy = Y \end{cases}$$

On peut ajouter à ce dernier système d'équations celle obtenue en considérant les modules :

$$x^2 + y^2 = |z|^2 = |Z| = \sqrt{X^2 + Y^2}$$

$$\text{Ainsi, on obtient : } z^2 = Z \Leftrightarrow \begin{cases} x^2 - y^2 = X \\ x^2 + y^2 = \sqrt{X^2 + Y^2} \\ 2xy = Y \end{cases} \Leftrightarrow \begin{cases} x^2 = \frac{1}{2}(X + \sqrt{X^2 + Y^2}) \\ y^2 = \frac{1}{2}(-X + \sqrt{X^2 + Y^2}) \\ 2xy = Y \end{cases}$$

Puisque $(X; Y) \neq (0; 0)$, les deux premières équations du dernier système fournissent chacune deux solutions. La troisième équation $2xy = Y$ permet de sélectionner les deux uniques couples solutions $x + iy$ en raisonnant sur le signe.

Remarque 1.9.1. *Il n'est pas indispensable d'apprendre par cœur les résultats énoncés ci-dessus. Il faut plutôt savoir la démarche à suivre pour la détermination des racines carrées d'un nombre complexe selon le contexte.*

Exemple 1.9.1. 1) Les racines carrées du nombre $Z = -5$ sont : $\sqrt{5}i$ et $-\sqrt{5}i$.

2) Les racines carrées du nombre $Z = 6i$ sont : $\sqrt{3}(1 + i)$ et $-\sqrt{3}(1 + i)$.

1.9.2 RÉOLUTION ALGÈBRIQUE D'UNE ÉQUATION DU SECOND DEGRÉ DANS $\mathbb{C}$

Soit $(a; b; c) \in \mathbb{C}^* \times \mathbb{C} \times \mathbb{C}$. On considère l'équation $az^2 + bz + c = 0$, d'inconnue $z \in \mathbb{C}$.

Pour résoudre cette équation, on utilise la forme canonique du trinôme :

$$az^2 + bz + c = a \left[\left(z + \frac{b}{2a} \right)^2 + \left(\frac{c}{a} - \frac{b^2}{4a^2} \right) \right] = a \left[\left(z + \frac{b}{2a} \right)^2 - \frac{b^2 - 4ac}{4a^2} \right]$$

En désignant par $\Delta = b^2 - 4ac$ le discriminant du trinôme, on a :

1.9. ÉQUATIONS DU SECOND DEGRÉ DANS $\mathbb{C}$

- Si $\Delta \neq 0$, l'équation admet deux solutions distinctes z_1 et z_2 données par :

$$z_1 = \frac{-b - \delta}{2a} \quad \text{et} \quad z_2 = \frac{-b + \delta}{2a}$$

où δ est une racine carrée de Δ (obtenue, par exemple, par une des méthodes exposées dans 8.1).

De plus : $(\forall z \in \mathbb{C}) \quad az^2 + bz + c = a(z - z_1)(z - z_2)$

Enfin, les solutions z_1 et z_2 vérifient les relations suivantes, connues sous le nom de formules de Viète :

$$z_1 + z_2 = \frac{-b - \delta}{2a} + \frac{-b + \delta}{2a} = \frac{-2b}{2a} = -\frac{b}{a} \quad \text{et} \quad z_1 \times z_2 = \frac{-b - \delta}{2a} \times \frac{-b + \delta}{2a} = \frac{b^2 - \Delta}{4a^2} = \frac{4ac}{4a^2} = \frac{c}{a}$$

En notant $s = z_1 + z_2$ et $p = z_1 \times z_2$, on obtient l'égalité suivante :

$$az^2 + bz + c = a(z^2 - sz + p)$$

- Si $\Delta = 0$, l'équation a une seule solution, dite double, donnée par : $z = \frac{-b}{2a}$.

De plus : $(\forall z \in \mathbb{C}) \quad az^2 + bz + c = a\left(z + \frac{b}{2a}\right)^2$

Proposition 1.9.1. Soit $(a; b; c) \in \mathbb{C}^* \times \mathbb{C} \times \mathbb{C}$ ainsi que l'équation d'inconnue $z \in \mathbb{C}$: $az^2 + bz + c = 0$

On note $\Delta = b^2 - 4ac$ son discriminant.

- Si $\Delta \neq 0$, l'équation admet deux solutions distinctes z_1 et z_2 données par :

$$z_1 = \frac{-b - \delta}{2a} \quad \text{et} \quad z_2 = \frac{-b + \delta}{2a} \quad \text{où } \delta \text{ est tel que } \delta^2 = \Delta.$$

De plus, on a la factorisation : $(\forall z \in \mathbb{C}) \quad az^2 + bz + c = a(z - z_1)(z - z_2)$

- Si $\Delta = 0$, l'équation a une seule solution, dite double, donnée par : $z = \frac{-b}{2a}$.

De plus, on a la factorisation : $(\forall z \in \mathbb{C}) \quad az^2 + bz + c = a\left(z + \frac{b}{2a}\right)^2$

Remarque 1.9.2. Afin de simplifier les calculs, on peut multiplier les membres de l'équation par le conjugué du coefficient de z^2 . Par exemple, l'équation $(1+i)z^2 - (1+7i)z + 14+21i = 0$ est équivalente à : $z^2 - (4+3i)z + 13-i = 0$ et qui a pour discriminant $-45 + 28i = (2+7i)^2$.

Corollaire 1.9.1. Soit a, b et c trois réels, a étant non nul, ainsi que l'équation dans $\mathbb{C}$: $(E) \quad az^2 + bz + c = 0$ On note $\Delta = b^2 - 4ac$ son discriminant.

1.9. ÉQUATIONS DU SECOND DEGRÉ DANS $\mathbb{C}$

- Si $\Delta > 0$, alors l'équation (E) a deux racines réelles distinctes z_1 et z_2 données par :

$$z_1 = \frac{-b - \sqrt{\Delta}}{2a} \quad \text{et} \quad z_2 = \frac{-b + \sqrt{\Delta}}{2a}$$

- Si $\Delta = 0$, l'équation a une racine double réelle donnée par : $z = \frac{-b}{2a}$.
- Si $\Delta < 0$, alors l'équation (E) a deux racines complexes distinctes conjuguées z_1 et z_2 données par :

$$z_1 = \frac{-b - i\sqrt{-\Delta}}{2a} \quad \text{et} \quad z_2 = \frac{-b + i\sqrt{-\Delta}}{2a}$$

Exemple 1.9.2. Étant donné un réel θ , résolvons l'équation : (E) $z^2 - 2z \cos \theta + 1 = 0$ Le discriminant de cette équation est : $\Delta = 4 \cos^2 \theta - 4 = -4 \sin^2 \theta = (2i \sin \theta)^2$

- Si $\theta = 0 \pmod{\pi}$, alors $\Delta = 0$ et l'équation (E) admet une racine double : $z = 1$ si $\theta = 0 \pmod{2\pi}$; $z = -1$ si $\theta = \pi \pmod{2\pi}$
- Si $\theta \neq 0 \pmod{\pi}$, alors $\Delta < 0$ et l'équation (E) admet deux racines distinctes conjuguées : $z_1 = \cos \theta + i|\sin \theta|$ et $z_2 = \cos \theta - i|\sin \theta|$
En fait, dans ce cas, l'ensemble solution de (E) peut aussi s'écrire :

$$S = \{\cos \theta + i \sin \theta; \cos \theta - i \sin \theta\} = \{e^{i\theta}; e^{-i\theta}\}$$

Proposition 1.9.2. Soit a, b et c trois nombres complexes, avec $a \neq 0$.

Les nombres complexes z_1 et z_2 (éventuellement égaux) vérifient : $z_1 + z_2 = -\frac{b}{a}$ et $z_1 \times z_2 = \frac{c}{a}$
si, et seulement si, z_1 et z_2 sont les deux racines (éventuellement confondues) de l'équation :

$$az^2 + bz + c = 0$$

Remarque 1.9.3. On utilise la proposition précédente sous plusieurs formes :

- Si l'on sait que z_1 et z_2 sont les racines de l'équation $az^2 + bz + c = 0$, alors on peut simplifier toute expression symétrique en z_1 et z_2 , et l'évaluer en fonction de $z_1 + z_2$ et $z_1 \times z_2$, et donc de a, b et c , sans avoir à expliciter z_1 et z_2 . Dans la pratique, on rencontre souvent les expressions symétriques :

$$z_1^n + z_2^n \quad ; \quad z_1^n \times z_2^n \quad ; \quad \frac{1}{z_1^n} + \frac{1}{z_2^n} \quad ; \quad \left(\frac{z_1}{z_2}\right)^n + \left(\frac{z_2}{z_1}\right)^n \quad (\text{avec } n \in \{1; 2; 3; 4\})$$

- Si z_1 et z_2 sont les racines de l'équation $az^2 + bz + c = 0$, et si l'on connaît une de ces racines, alors on peut facilement en déduire l'autre.

- Si l'on connaît deux complexes s et p , et si l'on cherche z_1 et z_2 tels que $z_1 + z_2 = s$ et $z_1 z_2 = p$, alors une façon élégante et efficace de faire est de dire que z_1 et z_2 sont les racines de l'équation :

$$z^2 - sz + p = 0$$

Exemple 1.9.3. Soit z_1 et z_2 les deux solutions (ou racines) de l'équation $z^2 - z + 4 = 0$.

Exprimer $z_1^2 + z_2^2 - z_1 z_2$ en fonction de $z_1 + z_2$ et $z_1 z_2$, et en déduire sa valeur.

Réponse :

$$\text{On a : } z_1^2 + z_2^2 - z_1 z_2 = z_1^2 + z_2^2 + 2z_1 z_2 - 2z_1 z_2 - z_1 z_2 = (z_1 + z_2)^2 - 3z_1 z_2.$$

$$\text{On a } z_1 + z_2 = 1 \text{ et } z_1 z_2 = 4, \text{ d'où : } z_1^2 + z_2^2 - z_1 z_2 = (z_1 + z_2)^2 - 3z_1 z_2 = 1^2 - 3 \times 4 = -11$$

1.10 TRANSFORMATIONS USUELLES DU PLAN

Si F est une application du plan $\mathcal{P}$ dans lui-même, on peut lui associer une unique application f de $\mathbb{C}$ dans $\mathbb{C}$ telle que pour tous points $M(z)$ et $M'(z')$ on ait $M' = F(M)$ si, et seulement si, $z' = f(z)$. Réciproquement, la donnée de f caractérise l'application F . On dit alors que f est représentée par F dans le plan complexe $\mathcal{P}$.

1.10.1 LA TRANSLATION

Définition 1.10.1. Soit $\vec{u}$ un vecteur du plan. La translation de vecteur $\vec{u}$ est l'application du plan dans lui-même qui, à tout point M , associe l'unique point M' tel que : $\overrightarrow{MM'} = \vec{u}$

Proposition 1.10.1. Soit $\vec{u}$ un vecteur du plan et a son affixe. La translation de vecteur $\vec{u}$ est représentée dans le plan complexe $\mathcal{P}$ par l'application :

$$\begin{aligned} \mathbb{C} &\rightarrow \mathbb{C} \\ z &\mapsto z' = z + a \end{aligned}$$

La relation $z' = z + a$ s'appelle **l'écriture (ou la formule)* complexe de la translation T de vecteur $\vec{u}(a)$.*

1.10.2 L'HOMOTHÉTIE

Définition 1.10.2. Soit Ω un point du plan et $\lambda \in \mathbb{R}^*$. L'homothétie de centre Ω et de rapport λ est l'application du plan dans lui-même qui, à tout point M , associe l'unique point M' tel que : $\overrightarrow{\Omega M'} = \lambda \overrightarrow{\Omega M}$

Proposition 1.10.2. L'homothétie de centre Ω , d'affixe ω , et de rapport λ est représentée dans le plan complexe $\mathcal{P}$ par l'application :

$$\begin{aligned} \mathbb{C} &\rightarrow \mathbb{C} \\ z &\mapsto z' = \omega + \lambda(z - \omega) \end{aligned}$$

La relation $z' = \omega + \lambda(z - \omega)$ s'appelle *l'écriture (ou la formule)* complexe de l'homothétie H de centre $\Omega(\omega)$ et de rapport λ .

Exemple 1.10.1. Soit f l'application du plan $\mathcal{P}$ dans lui-même qui, à tout point $M(z)$, associe le point $M'(z')$ telle que :

$$z' = -2z + 3 - 3i$$

Déterminons les points invariants par l'application $f : f(M) = M \Leftrightarrow z = -2z + 3 - 3i \Leftrightarrow z = 1 - i$. Par conséquent, f admet un point invariant qui est $\Omega(1 - i)$. On a donc : $z' - (1 - i) = -2(z - (1 - i))$. Par suite, f est l'homothétie de centre $\Omega(1 - i)$ et de rapport -2 .

1.10.3 LA ROTATION

Définition 1.10.3. Soit Ω un point du plan et $\theta \in \mathbb{R}$. La rotation de centre Ω et d'angle θ est l'application du plan dans lui-même qui transforme Ω en Ω , et tout point $M \neq \Omega$ en l'unique point M' tel que :

$$\Omega M' = \Omega M \quad \text{et} \quad (\overrightarrow{\Omega M}; \overrightarrow{\Omega M'}) \equiv \theta \quad [2\pi]$$

Proposition 1.10.3. La rotation de centre Ω , d'affixe ω , et d'angle θ est représentée dans le plan complexe $\mathcal{P}$ par l'application :

$$\begin{aligned} \mathbb{C} &\rightarrow \mathbb{C} \\ z &\mapsto z' = \omega + e^{i\theta}(z - \omega) \end{aligned}$$

La relation $z' = \omega + e^{i\theta}(z - \omega)$ s'appelle *l'écriture (ou la formule)* complexe de la rotation R de centre $\Omega(\omega)$ et d'angle θ .

Exemple 1.10.2. 1) Déterminons l'écriture complexe de la rotation R de centre $\Omega(1+i)$ et d'angle $\frac{3\pi}{4}$:

On a : $e^{i\frac{3\pi}{4}} = \frac{\sqrt{2}}{2}(-1+i)$. L'écriture complexe de la rotation R est : $z' = (1+i) + e^{i\frac{3\pi}{4}}(z - (1+i))$.

c'est-à-dire : $z' = \frac{\sqrt{2}}{2}(-1+i)z + \sqrt{2} + 1 + i$.

2) Soit R_1 la rotation de centre $\Omega_1(i)$ et qui transforme O (l'origine du repère) en le point $O_1\left(\frac{-\sqrt{3}+i}{2}\right)$.

On sait que l'écriture complexe de la rotation R_1 s'écrit sous la forme : $z_1 = e^{i\theta}(z-i) + i$.

Et puisque $R_1(O) = O_1$, alors $e^{i\theta} = \frac{\frac{-\sqrt{3}+i}{2}-i}{0-i} = \frac{1}{2} - i\frac{\sqrt{3}}{2}$. On en déduit alors que : $\theta \equiv -\frac{\pi}{3} \pmod{2\pi}$

1.10.4 COMPOSITION DE QUELQUES TRANSFORMATIONS DU PLAN

Dans ce paragraphe, nous allons examiner plusieurs compositions à partir des exemples :

I) Composée de deux rotations :

On considère le point $A(i)$. Soit R_0 la rotation de centre O (origine du repère) et d'angle $\frac{\pi}{6}$, et soit R_1 la rotation de centre A et d'angle $\frac{\pi}{3}$. Déterminons $R_1 \circ R_0$:

Pour tout point M d'affixe z , on pose $M' = R_0(M)$ et $M'' = R_1(M')$.

Soit z' l'affixe de M' et z'' l'affixe de M'' .

On a $z' = e^{i\frac{\pi}{6}}z$ et $z'' - z_A = e^{i\frac{\pi}{3}}(z' - z_A)$ où z_A est l'affixe de A (autrement dit, $z_A = i$).

Il s'ensuit donc : $z'' - i = e^{i\frac{\pi}{3}}(z' - i)$, et alors : $z'' = i + e^{i\frac{\pi}{3}}(z' - i)$.

On en déduit alors : $z'' = e^{i\frac{\pi}{3}} \cdot e^{i\frac{\pi}{6}}z + i(1 - e^{i\frac{\pi}{3}})$. Comme $e^{i\frac{\pi}{3}} \cdot e^{i\frac{\pi}{6}} = e^{i\frac{\pi}{2}} = i$, alors : $z'' = iz + \frac{\sqrt{3}}{2} + \frac{1}{2}i$.

On sait que la composée de deux rotations est une rotation. On va maintenant déterminer le centre de la rotation $R_1 \circ R_0$, et qui n'est rien d'autre que le point invariant $\Omega(\omega)$ par la transformation $R_1 \circ R_0$. On a $\omega = i\omega + \frac{\sqrt{3}}{2} + \frac{1}{2}i$, ce qui donne $\omega = \frac{\sqrt{3}-1}{4} + i\frac{\sqrt{3}+1}{4}$. Et comme $i = e^{i\frac{\pi}{2}}$, alors $R_1 \circ R_0$ est la rotation de centre $\Omega(\omega)$ et d'angle $\frac{\pi}{2}$.

II) Composée d'une rotation et d'une translation :

Soit ABC un triangle isocèle et rectangle en A tel que $(\overrightarrow{AB}; \overrightarrow{AC}) \equiv \frac{\pi}{2} \pmod{2\pi}$.

Soit R la rotation de centre A et qui transforme B en C , et soit T la translation de vecteur $\overrightarrow{AB}$.

Déterminons $F_1 = R \circ T$ et $F_2 = T \circ R$:

On munit le plan du repère orthonormé $(A; \overrightarrow{AB}, \overrightarrow{AC})$.

L'angle de la rotation R est $(\overrightarrow{AB}; \overrightarrow{AC})$; ainsi R est la rotation de centre A et d'angle $\frac{\pi}{2}$.

L'écriture complexe de la rotation R est $z' = e^{i\frac{\pi}{2}}z$, c'est-à-dire, $z' = iz$. L'écriture complexe de la translation T est $z'' = z + 1$. Pour tout M d'affixe z , on pose : $M_1 = F_1(M)$, et on note z_1 l'affixe de M_1 ; $M_2 = F_2(M)$, et on note z_2 l'affixe de M_2 .

On a : $z_1 = i(z + 1)$ et $z_2 = iz + 1$. Et puisque : $z = i(z + 1) \Leftrightarrow (1 - i)z = i \Leftrightarrow z = \frac{-1+i}{2}$ alors $\Omega_1 \left(\frac{-1+i}{2} \right)$ est l'unique point invariant par l'application F_1 .

L'écriture complexe de l'application F_1 s'écrit : $z_1 = e^{i\frac{\pi}{2}}z + \omega_1 (1 - e^{i\frac{\pi}{2}})$ où $\omega_1 = \frac{-1+i}{2}$.

F_1 est donc la rotation de centre $\Omega_1 \left(\frac{-1+i}{2} \right)$ et d'angle $\frac{\pi}{2}$.

De plus, $\Omega_2 \left(\frac{1+i}{2} \right)$ est l'unique point invariant par l'application F_2 .

F_2 est donc la rotation de centre $\Omega_2 \left(\frac{1+i}{2} \right)$ et d'angle $\frac{\pi}{2}$; ceci car $z_2 = e^{i\frac{\pi}{2}}z + \omega_2 (1 - e^{i\frac{\pi}{2}})$ où $\omega_2 = \frac{1+i}{2}$.

De l'égalité $z_2 - z_1 = 1 - i$ on tire $\overrightarrow{M_1M_2} = \overrightarrow{CB}$, ce qui montre que CBM_1M_2 est un parallélogramme.

III) Composée d'une homothétie et d'une translation :

Soit $k \in \mathbb{R}^* - \{1\}$, et H l'homothétie de centre un point $\Omega(\omega)$ donné et de rapport k . Soit b un nombre complexe donné et $\vec{u}(b)$ le vecteur image de b , et T la translation de vecteur $\vec{u}$.

On pose : $F = H \circ T$ et $G = T \circ H$.

L'écriture complexe de l'homothétie H est : $z_1 = kz + \omega(1 - k)$. L'écriture complexe de la translation T est : $z_2 = z + b$. Déterminons l'écriture complexe des transformations F et G : Pour tout $M(z)$, on pose $F(M) = M'$ et $G(M) = M''$. On note z' l'affixe de M' , et z'' l'affixe de M'' .

— On a $M' = H(M_2)$ où $M_2 = T(M)$, donc : $z' = kz_2 + \omega(1 - k) = k(z + b) + \omega(1 - k)$

Par suite, $z' = kz + kb + (1 - k)\omega$ est l'écriture complexe de la transformation F . Il est facile de montrer que l'application F admet $A \left(\frac{k}{1-k}b + \omega \right)$ comme unique point invariant, et que F est l'homothétie de centre A et de rapport k .

— On a $M'' = T(M_1)$ où $M_1 = H(M)$, donc : $z'' = z_1 + b$.

Par suite, $z'' = kz + b + (1 - k)\omega$ est l'écriture complexe de la transformation G .

Il est facile de montrer que l'application G admet $B \left(\frac{b}{1-k} + \omega \right)$ comme unique point invariant, et que G est l'homothétie de centre A et de rapport k .

IV) Composée d'une rotation et d'une homothétie :

Soit A le point d'affixe 2, et soit φ l'application du plan $\mathcal{P}$ dans lui-même qui, à chaque point $M(z)$, associe le point $M_2(z_2)$ tel que : $z_2 = \frac{3+i\sqrt{3}}{4}z + \frac{1-i\sqrt{3}}{2}$

Soit h l'homothétie de centre A et de rapport $\frac{2}{\sqrt{3}}$ et on pose $f = \varphi \circ h$.

- On pose $z_A = 2$. On a : $\frac{3+i\sqrt{3}}{4}z_A + \frac{1-i\sqrt{3}}{2} = z_A$, donc $\varphi(A) = A$. Cela signifie donc que A est invariant par φ .
- L'écriture complexe de l'homothétie h est : $z_1 = \frac{2}{\sqrt{3}}(z - 2) + 2$
- Pour tout point $M(z)$, on pose $M' = f(M)$ et on note z' l'affixe de M' .

On a : $z' = \frac{3+i\sqrt{3}}{4}z_1 + \frac{1-i\sqrt{3}}{2}$, qu'on peut écrire encore : $z' - 2 = \frac{3+i\sqrt{3}}{4}(z_1 - 2)$.

Comme $z_1 - 2 = \frac{2}{\sqrt{3}}(z - 2)$ alors $z' - 2 = \frac{3+i\sqrt{3}}{4} \times \frac{2}{\sqrt{3}}(z - 2)$, et donc : $z' - 2 = \frac{\sqrt{3}+i}{2}(z - 2)$.

Et puisque $\frac{\sqrt{3}+i}{2} = e^{i\frac{\pi}{6}}$ alors : $z' - 2 = e^{i\frac{\pi}{6}}(z - 2)$.

ce qui montre bien que f est la rotation de centre A et d'angle $\frac{\pi}{6}$.

Et puisque $f = \varphi \circ h$, alors $f \circ h^{-1} = (\varphi \circ h) \circ h^{-1} = \varphi \circ (h \circ h^{-1}) = \varphi$ (car $h \circ h^{-1} = Id_{\mathcal{P}}$). D'où :

$\varphi = f \circ h^{-1}$. Ainsi, l'application φ est la composée de la rotation de centre A et d'angle $\frac{\pi}{6}$,

et de l'homothétie de centre A et de rapport $\frac{\sqrt{3}}{2}$.

Chapitre 2

L'Arithmétique dans $\mathbb{Z}$

2.1 Divisibilité dans $\mathbb{Z}$

2.1.1 Définitions

Définition 2.1.1. Soit $(a, b) \in \mathbb{Z}^2$. On dit que a divise b , et on note $a \mid b$, s'il existe $k \in \mathbb{Z}$ tel que :

$$b = a \cdot k$$

Remarque 2.1.1. $a \mid b \iff \exists k \in \mathbb{Z}, b = k \cdot a$

Exemple 2.1.1. — $3 \mid 6$ car $6 = 2 \times 3$

— $7 \mid 0$ car $0 = 0 \times 7$

— $0 \mid 0$ car $0 = 0 \times 0$

— $\forall n \in \mathbb{Z}, n \text{ est pair} \iff \exists k \in \mathbb{Z}, n = 2k \iff 2 \mid n$

2.1.2 Propriétés

Proposition 2.1.1. Soit $(a, b, c, d) \in \mathbb{Z}^4$:

1. $a \mid a$, $a \mid -a$, $a \mid |a|$ et $|a| \mid a$.
2. $a \mid ab$.
3. $a \mid b \iff a \mid -b$.
4. $(a \mid b \text{ et } b \mid c) \implies a \mid c$ (Transitivité).
5. $(a \mid b \text{ et } b \mid a) \iff |a| = |b|$.
6. $(a \mid b \text{ et } c \mid d) \implies ac \mid bd$.
7. $(a \mid b \text{ et } a \mid c) \implies a \mid (b + c) \text{ et } a \mid (b - c)$.
8. $\forall (\alpha, \beta) \in \mathbb{Z}^2, (a \mid b \text{ et } a \mid c) \implies a \mid (\alpha b + \beta c)$ (Combinaison linéaire).

Démonstrations (Preuves)

1. On a $a = 1 \times a$, donc $a \mid a$. De même $-a = (-1) \times a$, donc $a \mid -a$.
Si $a \geq 0$, $|a| = a$, donc $a \mid |a|$. Si $a < 0$, $|a| = -a$, donc $a \mid -a$, d'où $a \mid |a|$.
2. On a $ab = b \times a$, donc $a \mid ab$.
3. ($\implies$) Supposons $a \mid b$. Il existe $k \in \mathbb{Z}$ tel que $b = k \cdot a$. Donc $-b = (-k) \cdot a$. Comme $-k \in \mathbb{Z}$, on a $a \mid -b$.
($\impliedby$) Supposons $a \mid -b$. Il existe $k \in \mathbb{Z}$ tel que $-b = k \cdot a$, donc $b = (-k) \cdot a$, d'où $a \mid b$.
4. Supposons $a \mid b$ et $b \mid c$. Il existe $(k, k') \in \mathbb{Z}^2$ tels que $b = ka$ et $c = k'b$. Alors $c = k'(ka) = (k'k)a$. Comme $k'k \in \mathbb{Z}$, on a $a \mid c$.
5. ($\implies$) Supposons $a \mid b$ et $b \mid a$. Il existe $(k, k') \in \mathbb{Z}^2$ tels que $b = ka$ et $a = k'b$.
Donc $b = k(k'b) \implies b(kk' - 1) = 0$.
Si $b = 0$, alors $a = k' \times 0 = 0$, d'où $|a| = |b| = 0$.
Si $b \neq 0$, alors $kk' = 1$, ce qui impose $k \in \{-1, 1\}$, donc $|k| = 1$.
Comme $|b| = |k| \cdot |a|$, on en déduit $|a| = |b|$.
($\impliedby$) Supposons que $|a| = |b|$:
donc $a = b$ ou $a = -b$. si $a = b$, alors $a \mid b$ et $b \mid a$. si $a = -b$, alors $a \mid -b$ et $-b \mid a$.
donc, $a = (-1) \cdot b$ et $b = (-1) \cdot a$.
d'où $a \mid b$ et $b \mid a$.
6. Supposons que $a \mid b$ et $c \mid d$:
donc il existe $(k, k') \in \mathbb{Z}^2$, $b = k \cdot a$ et $d = k' \cdot c$. alors, $bd = (kk')ac$.
D'où $ac \mid bd$ (car $(k \cdot k') \in \mathbb{Z}$).
7. Supposons que $a \mid b$ et $a \mid c$:
donc il existe $(k, k') \in \mathbb{Z}^2$, $b = k \cdot a$ et $c = k' \cdot a$. donc
$$\begin{cases} b + c = (k + k')a \\ b - c = (k - k')a \end{cases}$$

Alors
$$\begin{cases} a \mid b + c \text{ (car } (k + k') \in \mathbb{Z}) \\ a \mid b - c \text{ (car } (k - k') \in \mathbb{Z}) \end{cases}$$
8. Supposons que $a \mid b$ et $a \mid c$:
Soit $\alpha, \beta \in \mathbb{Z}$. donc il existe $(k, k') \in \mathbb{Z}^2$, $b = k \cdot a$ et $c = k' \cdot a$.
d'où $\alpha b = \alpha k \cdot a$ et $\beta c = \beta k' \cdot a$. Alors, $\alpha b + \beta c = (\alpha k + \beta k')a$. D'où, $a \mid \alpha b + \beta c$ (car, $\alpha k + \beta k' \in \mathbb{Z}$).

Proposition 2.1.2. Soit $(a, b) \in \mathbb{Z}^2$ avec $b \neq 0$. Si $a \mid b$, alors $|a| \leq |b|$.

Démonstration : Supposons que $a \mid b$

Donc il existe $k \in \mathbb{Z}$, tel que $b = k \cdot a$. Par passage à la valeur absolue, on a : $|b| = |k| \cdot |a|$. Comme $b \neq 0$, alors $k \neq 0$ (car si $k = 0$, alors $b = 0$). Puisque k est un entier non nul ($k \in \mathbb{Z}^*$), on en déduit que $|k| \geq 1$. En multipliant par $|a|$ (qui est positif), on obtient : $|a| \cdot |k| \geq |a|$. D'où $|b| \geq |a|$, ce qui revient à écrire $|a| \leq |b|$.

Exercices d'application

les deux questions son indépendants

1. Soit $(d, n) \in \mathbb{Z}^2$ tels que $d \mid n^2 + 3$ et $d \mid 2n - 1$. Montrer que $d \mid 13$.
2. Déterminer les ensembles suivants :
 - $E = \{n \in \mathbb{Z} \mid n \mid (n + 8)\}$
 - $F = \{m \in \mathbb{Z} \mid (m - 4) \mid (3m + 24)\}$
 - $G = \{n \in \mathbb{N} \mid \frac{15n-3}{7n+1} \in \mathbb{Z}\}$

2.2 Division Euclidienne

2.2.1 Division euclidienne dans $\mathbb{N}$

Théorème 2.2.1. Soit $(a, b) \in \mathbb{N}^2$ avec $b \neq 0$. Il existe un unique couple $(q, r) \in \mathbb{N} \times \mathbb{N}$ tel que :

$$\begin{cases} a = b \cdot q + r \\ 0 \leq r < b \end{cases}$$

Exemple 2.2.1. — Pour $a = 5$ et $b = 2$: $5 = 2 \times 2 + 1$, donc $q = 2$ et $r = 1$.
 — Pour $a = 17$ et $b = 2$: $17 = 2 \times 8 + 1$, donc $q = 8$ et $r = 1$.

Démonstration Soit $(a, b) \in \mathbb{N} \times \mathbb{N}^*$

1. L'existence On a $a = bq + r$ et $0 \leq r < b$
 donc $\frac{a}{b} = q + \frac{r}{b}$ et $0 \leq \frac{r}{b} < 1$

Alors $E\left(\frac{a}{b}\right) = E\left(q + \frac{r}{b}\right) = q + E\left(\frac{r}{b}\right)$
 et comme $\frac{r}{b} \in [0, 1[$, donc $E\left(\frac{r}{b}\right) = 0$
 D'où l'existence de $q = E\left(\frac{a}{b}\right)$ est vérifiée.

Comme $r = a - bq$, alors $a = bq + r$
 Comme $\frac{a}{b} - 1 < E\left(\frac{a}{b}\right) \leq \frac{a}{b}$ avec $q = E\left(\frac{a}{b}\right)$

donc $-a \leq -bE\left(\frac{a}{b}\right) < b - a$ avec $q = E\left(\frac{a}{b}\right)$

Alors $0 \leq a - b \cdot E\left(\frac{a}{b}\right) < b$ avec $q = E\left(\frac{a}{b}\right)$

D'où $0 \leq r < b$

Ainsi l'existence de r vérifiant $0 \leq r < b$ est établie.

D'où il existe $(q, r) \in \mathbb{N}^2$ tel que $a = bq + r$ et $0 \leq r < b$.

2. L'unicité Supposons qu'il existe $(q, r, q', r') \in \mathbb{N}^4$ tel que :

$$\begin{cases} a = bq + r \\ 0 \leq r < b \end{cases} \quad \text{et} \quad \begin{cases} a = bq' + r' \\ 0 \leq r' < b \end{cases} \quad \text{et} \quad (q, r) \neq (q', r')$$

donc $bq + r = bq' + r'$

Alors $b(q - q') = r' - r$

Or, on a $-b < -r \leq 0$, donc $-b < r' - r < b$

Alors $-b < (q - q')b < b$

donc $-1 < q - q' < 1$

Alors nécessairement $q - q' = 0$

D'où $r = r'$ et $q = q'$ (**Absurde**)

Ainsi le couple (q, r) , s'il existe, est unique.

2.2.2 Division euclidienne dans $\mathbb{Z}$

Théorème 2.2.2. Soit $(a, b) \in \mathbb{Z}^2$ avec $b \neq 0$.

Il existe un unique couple $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tel que :

$$\begin{cases} a = bq + r \\ 0 \leq r < |b| \end{cases}$$

Exemple 2.2.2. — Pour $a = 5$ et $b = -3$:

$$5 = -3 \times 2 + 1$$

donc $q = 2$ et $r = 1$.

— Pour $a = 7$ et $b = -1$:

$$7 = (-1) \times (-7) + 0$$

donc $q = -7$ et $r = 0$.

Démonstration : Soit $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$

1. L'existence On a $a = bq + r$ et $0 \leq r < |b|$
donc $\frac{a}{b} = q + \frac{r}{b}$ et $0 \leq \frac{r}{|b|} < 1$

$$\text{Alors } E\left(\frac{a}{b}\right) = E\left(q + \frac{r}{|b|}\right) = q + E\left(\frac{r}{|b|}\right)$$

et comme $\frac{r}{|b|} \in [0, 1[$, donc $E\left(\frac{r}{|b|}\right) = 0$

D'où l'existence de $q = E\left(\frac{a}{b}\right)$ est vérifiée.

Comme $r = a - bq$, alors $a = bq + r$

Comme $\frac{a}{b} - 1 < E\left(\frac{a}{b}\right) \leq \frac{a}{b}$ avec $q = E\left(\frac{a}{b}\right)$
donc $-a \leq -bE\left(\frac{a}{b}\right) < b - a$ avec $q = E\left(\frac{a}{b}\right)$

Alors $0 \leq a - b \cdot E\left(\frac{a}{b}\right) < b$ avec $q = E\left(\frac{a}{b}\right)$

D'où $0 \leq r < b$

Ainsi l'existence de r vérifiant $0 \leq r < |b|$ est établie.

D'où il existe $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tel que $a = bq + r$ et $0 \leq r < |b|$.

2. L'unicité Supposons qu'il existe $(q, r, q', r') \in \mathbb{Z} \times \mathbb{N} \times \mathbb{Z} \times \mathbb{N}$ tel que :

$$\begin{cases} a = bq + r \\ 0 \leq r < |b| \end{cases} \quad \text{et} \quad \begin{cases} a = bq' + r' \\ 0 \leq r' < |b| \end{cases} \quad \text{et } (q, r) \neq (q', r')$$

$$\text{donc } bq + r = bq' + r'$$

$$\text{Alors } b(q - q') = r' - r$$

$$\text{Or, on a } -b < -r \leq 0, \text{ donc } -|b| < r' - r < |b|$$

$$\text{Alors } -|b| < (q - q')b < |b|$$

en tout cas, on a : $-1 < q - q' < 1$

$$\text{Alors nécessairement } q - q' = 0$$

D'où $r = r'$ et $q = q'$ (**Absurde**)

Ainsi le couple (q, r) , s'il existe, est unique.

Proposition 2.2.1. Soit $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$, Alors on a :

$b \mid a$ si et seulement si le reste de la division euclidienne de a par b est nul.

Preuve : ($\implies$) Supposons que $b \mid a$:

donc il existe $k \in \mathbb{Z}$ tel que : $a = bk$

$$\text{alors : } \begin{cases} a = bk + 0 \\ 0 \leq 0 < |b| \end{cases}$$

d'où le reste de la division euclidienne de a par b est nulle. ($\impliedby$) Réciproquement supposons que le reste de la division euclidienne de a par b est 0

donc il existe $q \in \mathbb{Z}$ tel que : $a = bq + 0$

$$\text{alors } a = b \cdot q$$

d'où $b \mid a$ (car $q \in \mathbb{Z}$)

Exercices d'application

1. Soit $n \in \mathbb{N} \setminus \{0, 1\}$.
Déterminer le reste et le quotient de la division euclidienne de $a = 2n^2 + n$ par $b = n + 1$.
2. Soit $n \in \mathbb{N}$.
Déterminer le reste et le quotient de la division euclidienne de $a = (2n + 1)^2$ par 8.

2.3 Nombres Premiers**2.3.1 Définition d'un nombre premier :**

Définition 2.3.1. Soit $a \in \mathbb{Z} \setminus \{-1; 0; 1\}$.

On dit que a est un nombre premier si et seulement si les seuls diviseurs de a sont : $-1, 1, a$ et $-a$.

Exemple 2.3.1. 13 est un nombre premier, $13 \neq -1$ et $13 \neq 1$
et $D_{13} = \{-13; -1; 1; 13\}$

Remarque : $(a \text{ est premier}) \iff (\text{card}(D_a) = 4)$

2.3.2 Propriétés :

Proposition 2.3.1. Soit $p \in \mathbb{Z} \setminus \{-1, 0, 1\}$.

$(p \text{ est premier}) \iff (-p \text{ est premier})$.

Proposition 2.3.2. Soit $a \in \mathbb{Z}$.

Si a n'est pas premier et $a \neq 0$, $a \neq 1$, $a \neq -1$, alors le plus petit diviseur de a différent de 1 et -1 est un nombre premier.

Preuve : Soit a un nombre non premier, et soit p son plus petit diviseur positif tel que $p \neq 1; a; -a, .1$

Supposons par l'absurde que p est non premier. Alors il existe un diviseur p_1 de p tel que $p_1 \neq 1, -1$ et $p_1 \neq p, -p$.

On a $p_1 | p \implies |p_1|$ divise $|p|$, alors $|p_1| < |p|$.
D'où $|p_1| < p$.

Comme $p_1|p$ et $p|a$, par transitivité $p_1|a$. On trouve alors un diviseur $|p_1|$ de a qui est plus petit que p , ce qui est absurde puisque p est défini comme le plus petit diviseur de a (différent de 1 et -1).

Par conséquent, p est premier.

Proposition 2.3.3. *Soient p et p' deux nombres premiers de $\mathbb{Z}$.
Si $p|p' \implies |p| = |p'|$.*

Preuve : On sait que l'ensemble des diviseurs de p' dans $\mathbb{Z}$ est :

$$\mathcal{D}_{p'} = \{-1, 1, p', -p'\}$$

On a $p|p' \implies p \in \mathcal{D}_{p'}$.

C'est-à-dire : $p = 1$ ou $p = -1$ ou $p = p'$ ou $p = -p'$.

Or, comme p est un nombre premier par hypothèse, alors $p \neq 1$ et $p \neq -1$.
Il ne reste donc que les possibilités :

$$p = p' \quad \text{ou} \quad p = -p'$$

Ce qui implique directement :

$$|p| = |p'|$$

Remarque 2.3.1. *Si $(p, p') \in \mathbb{N}^2$, alors $p|p' \implies p = p'$.*

Proposition 2.3.4. *Soit $a \in \mathbb{N}^* \setminus \{1\}$, tel que a est non premier.
Alors il existe un nombre premier p tel que :*

$$p|a \quad \text{et} \quad p^2 \leq a$$

Preuve : On a a est un nombre non premier, alors son plus petit diviseur p est premier.

Ainsi $\exists k \in \mathbb{N}^*$ tel que $a = kp$ et $k \neq 1$.

D'où k est un diviseur de a , alors $k \geq p$.

D'où $kp \geq p \times p \implies a \geq p^2$.

Proposition 2.3.5 (Application contraposée de la propriété 4).

$$\left\{ \begin{array}{l} p \nmid a \\ \text{ou} \\ p^2 > a \end{array} \right\} \implies (a \text{ est premier})$$

2.4. DÉCOMPOSITION EN FACTEURS PREMIERS D'UN ENTIER RELATIF - APPLICATIONS

Exemple 2.3.2. Vérifions que $a = 173$ est premier.

On a $\sqrt{173} \approx 13,15$, alors les nombres premiers inférieurs à $\sqrt{173}$ sont 2, 3, 5, 7, 11, 13.

$* 2 \nmid 173 \quad * 3 \nmid 173 \quad * 5 \nmid 173 \quad * 7 \nmid 173 \quad * 11 \nmid 173 \quad * 13 \nmid 173$

D'où $a = 173$ est un nombre premier.

Proposition 2.3.6. L'ensemble des nombres premiers est infini.

Preuve : Voir AL MOUFID en Math (Tome 1) page : 302

Remarque 2.3.2. Le plus grand nombre premier trouvé jusqu'à maintenant est $2^{136\,279\,841} - 1$. Il a été découvert le 12 octobre 2024.

Exercice d'application

Les questions 1 et 2 sont indépendantes.

1) Soit n un élément de $\mathbb{Z}$. On pose : $\alpha_n = n^4 - n^2 + 16$.

a) Montrer que les entiers $n^2 - 3n + 4$ et $n^2 + 3n + 4$ sont pairs.

b) En déduire que le nombre α_n n'est pas premier.

2) Soit $m \in \mathbb{N}^*$ tel que $2^m + 1$ soit premier. Montrer que $m = 2^k$ avec $k \in \mathbb{N}$

2.4 Décomposition en facteurs premiers d'un entier relatif - Applications

2.4.1 Propriété

Proposition 2.4.1. Soit $a \in \mathbb{Z}$ tel que $|a| \geq 2$.

Le nombre entier a s'écrit sous une forme unique :

$$a = \varepsilon \times p_1^{\alpha_1} \times p_2^{\alpha_2} \times \cdots \times p_n^{\alpha_n}$$

telle que $\varepsilon = \pm 1$ et $(\alpha_1, \alpha_2, \dots, \alpha_n) \in \mathbb{N}^n$ et les $p_1, p_2, \dots, p_n$ sont des nombres premiers.

Cette écriture s'appelle la **décomposition en facteurs premiers** du nombre entier a .

Preuve : voir AL MOUFID page : 303

2.4.2 Diviseurs d'un entier relatif non nul et différent de -1 et 1

Proposition 2.4.2. Soit $a \in \mathbb{Z} \setminus \{-1, 0, 1\}$ dont la décomposition en facteurs premiers est :

$$a = \varepsilon \cdot p_1^{\alpha_1} \times p_2^{\alpha_2} \times \cdots \times p_n^{\alpha_n}$$

Alors les diviseurs de a sont les nombres d de la forme :

$$d = \varepsilon \times p_1^{\beta_1} \times p_2^{\beta_2} \times \cdots \times p_n^{\beta_n}$$

avec $\varepsilon \in \{-1, 1\}$ et pour tout $i \in \{1, \dots, n\}$, $0 \leq \beta_i \leq \alpha_i$.

Exemple 2.4.1. (Détermination de diviseurs de 72) On a : $72 = 2^3 \times 3^2$
Les diviseurs positifs de 72 sont de la forme :

$$d = 2^\alpha \times 3^\beta \quad \text{avec} \quad \begin{cases} 0 \leq \alpha \leq 3 \\ 0 \leq \beta \leq 2 \end{cases}$$

— **Si** $\alpha = 0$:

- $\beta = 0 \Rightarrow d = 1$
- $\beta = 1 \Rightarrow d = 3$
- $\beta = 2 \Rightarrow d = 9$

— **Si** $\alpha = 1$:

- $\beta = 0 \Rightarrow d = 2$
- $\beta = 1 \Rightarrow d = 6$
- $\beta = 2 \Rightarrow d = 18$

— **Si** $\alpha = 2$:

- $\beta = 0 \Rightarrow d = 4$
- $\beta = 1 \Rightarrow d = 12$
- $\beta = 2 \Rightarrow d = 36$

— **Si** $\alpha = 3$:

- $\beta = 0 \Rightarrow d = 8$
- $\beta = 1 \Rightarrow d = 24$
- $\beta = 2 \Rightarrow d = 72$

Proposition 2.4.3. Le nombre de diviseurs positifs d'un entier relatif a tel que $a = \varepsilon \cdot p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \cdots \cdot p_n^{\alpha_n}$, est :

$$\prod_{i=1}^{i=n} (\alpha_i + 1) = (\alpha_1 + 1)(\alpha_2 + 1)(\alpha_3 + 1) \dots (\alpha_n + 1)$$

2.4. DÉCOMPOSITION EN FACTEURS PREMIERS D'UN ENTIER RELATIF - APPLICATIONS

Preuve : Si d est un diviseur de a alors d s'écrit sous la forme : $d = p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}$ avec $0 \leq \beta_i \leq \alpha_i$ et $i \in \{1; 2; \dots; k\}$.

Par conséquent, le nombre de diviseurs positifs de a est le nombre des entiers d lorsque β_i varie sur l'ensemble $\{0; 1; \dots; \alpha_i\}$. Dans ce cas, il y a $1 + \alpha_i$ choix pour la valeur de β_i . Enfin, et d'après le principe fondamental de dénombrement, le nombre total des diviseurs de a vaut :

$$(1 + \alpha_1)(1 + \alpha_2) \dots (1 + \alpha_n)$$

Signalons au passage que le nombre de diviseurs de a dans $\mathbb{Z}$ est :

$$2(1 + \alpha_1)(1 + \alpha_2) \dots (1 + \alpha_n)$$

2.4.3 Multiples d'un entier non nul et non 1 et -1

Proposition 2.4.4. Soit $a \in \mathbb{Z}/a \notin \{-1, 0, 1\}$ et la décomposition de a en facteurs premiers est :

$$a = \varepsilon \cdot p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_n^{\alpha_n}$$

Alors les multiples de a sont :

$$M = \varepsilon(p_1^{\beta_1} \cdot p_2^{\beta_2} \dots p_n^{\beta_n}) \cdot K$$

avec $\forall i \in \{1, \dots, n\} ; \beta_i \geq \alpha_i$
tel que K est le produit des nombres premiers autres que les p_i avec $i \in \{1, 2, \dots, n\}$.

Exemple 2.4.2. On a $a = 75$ et $m = 1500$.
 m est le multiple de a car $m = 1500$

$$\begin{aligned} m &= 15 \times 100 \\ &= 3 \times 5 \times 5^2 \times 2^2 \\ &= 2^2 \times 3 \times 5^3 \text{ et on a } 75 = 5^2 \times 3 \\ &= 5^2 \times 3 \times 2^2 \times 5 = a \times k \times 5 \end{aligned}$$

où $k = 2^2$.

2.4.4 PGCD de deux entiers naturels non $\{0 \text{ et } 1\}$

Soit $(a, b) \in (\mathbb{N}^* - \{1\})^2$.

On considère les deux décompositions de a et b suivantes :

$$a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot p_3^{\alpha_3} \dots p_n^{\alpha_n} \text{ et } b = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot p_3^{\beta_3} \dots p_n^{\beta_n}$$

avec $\alpha_i = 0$ si p_i n'appartient pas à la décomposition de a ,
et $\beta_i = 0$ si p_i n'appartient pas à la décomposition de b .

Tous les diviseurs de a et b sont :

$$d = p_1^{\gamma_1} \cdot p_2^{\gamma_2} \cdot p_3^{\gamma_3} \dots p_n^{\gamma_n}, \text{ tel que } \forall i \in \{1, \dots, n\}$$

$$0 \leq \gamma_i \leq \inf(\alpha_i, \beta_i)$$

Et par suite le plus grand diviseur de a et b soit :

$$\begin{aligned} a \wedge b &= p_1^{\inf(\alpha_1, \beta_1)} \cdot p_2^{\inf(\alpha_2, \beta_2)} \dots p_n^{\inf(\alpha_n, \beta_n)} \\ &= \prod_{i=1}^n p_i^{\inf(\alpha_i, \beta_i)} \end{aligned}$$

Et tous les multiples de a et b sont :

$$\begin{aligned} M &= p_1^{\varepsilon_1} \cdot p_2^{\varepsilon_2} \cdot p_3^{\varepsilon_3} \dots p_n^{\varepsilon_n} \times k, \text{ tel que } \varepsilon_i \geq \sup(\alpha_i, \beta_i) \\ &\text{et } i \in \{1; 2; 3; \dots; n\} \end{aligned}$$

Alors le plus petit multiple commun de a et b est :

$$\begin{aligned} a \vee b &= p_1^{\sup(\alpha_1, \beta_1)} \cdot p_2^{\sup(\alpha_2, \beta_2)} \dots p_n^{\sup(\alpha_n, \beta_n)} \\ &= \prod_{i=1}^n p_i^{\sup(\alpha_i, \beta_i)} \end{aligned}$$

Exemple 2.4.3. Déterminer $a \wedge b$ et $a \vee b$ avec $a = 488$ et $b = 198$.

La décomposition en facteurs premiers des deux nombres a et b est :

- $a = 2^3 \times 61 = 2^3 \times 3^0 \times 11^0 \times 61^1$
- $b = 2 \times 3^2 \times 11 = 2^1 \times 3^2 \times 11^1 \times 61^0$

$$\begin{aligned} a \wedge b &= 2^{\inf(3;1)} \times 3^{\inf(0;2)} \times 11^{\inf(0;1)} \times 61^{\inf(1;0)} \\ &= 2^1 \times 3^0 \times 11^0 \times 61^0 = 2 \end{aligned}$$

$$\begin{aligned} a \vee b &= 2^{\sup(3;1)} \times 3^{\sup(0;2)} \times 11^{\sup(0;1)} \times 61^{\sup(1;0)} \\ &= 2^3 \times 3^2 \times 11 \times 61 = 48312 \end{aligned}$$

2.5 PGCD-Algorithmme d'Euclide-PPCM

2.5.1 Plus Grand Commun Diviseur (PGCD)

Définition 2.5.1. Soit a et b deux entiers relatifs non nuls.

Le plus grand commun diviseur de a et b , noté $a \wedge b$ ou $\text{PGCD}(a, b)$ ou $\Delta(a, b)$, est le plus grand des diviseurs strictement positifs communs à a et b .

Exemple 2.5.1. 1. Les diviseurs positifs du nombre -30 sont : 1 ; 2 ; 3 ; 5 ; 6 ; 10 ; 15 ; 30.
Les diviseurs positifs du nombre 12 sont : 1 ; 2 ; 3 ; 4 ; 6 ; 12.
Par conséquent : $12 \wedge 30 = 6$

2. Les diviseurs positifs du nombre -19 sont : 1 ; 19.
Les diviseurs positifs du nombre 15 sont : 1 ; 3 ; 5 ; 15. Par suite :
 $(-19) \wedge 15 = 1$

Remarque 2.5.1. — On convient que pour tout $a \in \mathbb{Z}$: $a \wedge 0 = |a|$.

— La définition précédente peut être encore formulée par l'équivalence suivante :

$$\delta = a \wedge b \Leftrightarrow \begin{cases} \delta | a \text{ et } \delta | b \\ (\forall d \in D_a \cap D_b) : d \leq \delta \end{cases}$$

— Soit a et b deux entiers relatifs non nuls. Si $\delta = a \wedge b$ alors :

- $\delta \geq 1$ et $\delta | a$ et $\delta | b$;
- Pour tout $d \in \mathbb{Z}^*$: $(d | a \text{ et } d | b) \Rightarrow d | \delta$.

Proposition 2.5.1. Soit a, b et c des entiers relatifs non nuls et n un entier naturel non nul. Alors :

1. $a \wedge b = |a| \wedge |b|$; 2) $a \wedge b = b \wedge a$; 3) $a \wedge a = a \wedge 0 = |a|$; 4) $a \wedge 1 = 1$
2. $(a \wedge b) \wedge c = a \wedge (b \wedge c)$; 6) $a | b \Leftrightarrow a \wedge b = |a|$; 7) $a^n \wedge a = |a|$

Preuve

- Les résultats 1), 2), 3), 4) et 7) sont des conséquences immédiates de la définition précédente.
- Le résultat 5) découle de fait que : $(D_a \cap D_b) \cap D_c = D_a \cap (D_b \cap D_c)$.
- Pour le résultat 6) : On suppose que $a | b$, donc : $(\exists k \in \mathbb{Z}) ; b = ak$. Par conséquent :

$$D_a \cap D_b = D_a \cap D_{ka} = D_a \quad (\text{car : } D_a \subset D_{ka})$$

Il s'ensuit donc que : $a | b \Rightarrow a \wedge b = |a|$.

Réciproquement, si $a \wedge b = |a|$ alors $|a|/b$, c'est-à-dire que : a/b .
D'où : $a|b \Leftrightarrow a \wedge b = |a|$.

Pour tout $(x; y) \in \mathbb{N}^2$:
 $x|y \Leftrightarrow D_x \subset D_y$

Proposition 2.5.2. *Soit a, b et c des entiers relatifs non nuls. Alors :*

1. $(c | a \text{ et } c | b) \Leftrightarrow c | a \wedge b$
2. $(ca) \wedge (cb) = |c|(a \wedge b)$
3. $\begin{cases} c | a \\ c | b \end{cases} \Rightarrow \left(\frac{a}{c}\right) \wedge \left(\frac{b}{c}\right) = \frac{a \wedge b}{|c|}$

Preuve : Soit a, b et c des entiers relatifs non nuls et n un entier naturel.

1. Si $c | a \wedge b$ alors $c | a$ et $c | b$ car $a \wedge b | a$ et $a \wedge b | b$. Par conséquent :
 $c | a \wedge b \Rightarrow (c | a \text{ et } c | b)$.

La réciproque se découle immédiatement de la définition du plus grand commun diviseur.

2. Pour la relation $(ca) \wedge (cb) = |c|(a \wedge b)$, il suffit d'utiliser les décompositions des entiers a et b en produit de facteurs premiers.
3. Supposons que : $c \in D_a \cap D_b$. Il existe donc $(a'; b') \in \mathbb{Z}^2$ tel que :
 $a = ca'$ et $b = cb'$.

Il en résulte donc que : $a \wedge b = (ca') \wedge (cb') = |c|(a' \wedge b')$; d'où :
 $\left(\frac{a}{c}\right) \wedge \left(\frac{b}{c}\right) = \frac{a \wedge b}{|c|}$.

2.5.2 Calcul Pratique du P.G.C.D : L'ALGORITHME D'EUCLIDE

Proposition 2.5.3. *Soit a et b deux entiers naturels non nuls.*

Si $a = bq + r$ et $0 < r < b$, alors : $a \wedge b = b \wedge r$. En d'autres termes :

Lorsque b ne divise pas a , le plus grand commun diviseur des entiers a et b est égal au dernier reste non nul obtenu grâce à l'algorithme d'Euclide.

Explication de l'algorithme d'Euclide :

On considère deux entiers $a \in \mathbb{Z}^*$ et $b \in \mathbb{N}^*$.

- * On effectue la division euclidienne de a par b : $a = bq_1 + r_1$ avec
 $0 \leq r_1 < b$.
- o Si $r_1 = 0$, on arrête l'algorithme en déduisant que : $a \wedge b = b$

- o Si $r_1 \neq 0$, on continue.
- * On effectue la division euclidienne de b par r_1 : $b = r_1 q_2 + r_2$ avec $0 \leq r_2 < r_1$.
 - o Si $r_2 = 0$, on arrête l'algorithme en déduisant que : $a \wedge b = r_1$
 - o Si $r_2 \neq 0$, on continue.
- * Etc.

Notons que le processus engagé va s'arrêter, car sinon, on construirait une suite d'entiers naturels strictement décroissante, ce qui est impossible. Il existe donc un entier $p \in \mathbb{N}$ tel que $r_p \neq 0$ et $r_{p+1} = 0$.
Par conséquent : $a \wedge b = r_p$

Exemple 2.5.2. Calculons $6468 \wedge 1547$ en appliquant l'algorithme d'Euclide :

$$\begin{aligned} 6468 &= 1547 \times 4 + 280 \\ 1547 &= 280 \times 5 + 147 \\ 280 &= 147 \times 1 + 133 \\ 147 &= 133 \times 1 + 14 \\ 133 &= 14 \times 9 + \boxed{7} \\ 14 &= 7 \times 2 + 0 \end{aligned}$$

Le dernier reste non nul dans l'algorithme est 7, ce qui permet de conclure que : $6468 \wedge 1547 = 7$.

2.5.3 Plus Petit Commun Multiple (PPCM) :

Définition 2.5.2. Soit a et b deux entiers relatifs non nuls.

Le plus petit commun multiple de a et b , noté $a \vee b$ ou $PPCM(a, b)$ ou $M(a; b)$, est le plus petit des multiples strictement positifs communs à a et b .

- Exemple 2.5.3.**
1. Les multiples positifs du nombre -9 sont : $0 ; 9 ; 18 ; 27 ; 36 ; 45 ; 54 ; 63 ; \dots$
Les multiples positifs du nombre 15 sont : $0 ; 15 ; 30 ; 45 ; 60 ; 75 ; \dots$
Par conséquent : $15 \vee (-9) = 45$
 2. On montre de même que : $5 \vee 15 = 15 ; (-7) \vee 16 = 112 ; (-12) \vee (-30) = 60$

Remarque 2.5.2. — On convient que pour tout $a \in \mathbb{Z}$: $a \vee 0 = 0$.

- En notant $a\mathbb{Z}$ l'ensemble des multiples de a , alors : $a\mathbb{Z} = \{\dots; -3a; -2a; -a; 0; a; 2a; 3a; \dots\}$
Le plus petit élément de l'ensemble $(a\mathbb{Z} \cap b\mathbb{Z}) \cap \mathbb{N}^*$ est donc $a \vee b$.
- Soit a et b deux entiers relatifs non nuls. Si $m = a \vee b$ alors :
 - $m \geq 1$ et $a \mid m$ et $b \mid m$;
 - Pour tout $c \in \mathbb{Z}$: $(a \mid c \text{ et } b \mid c) \Rightarrow m \mid c$.

Proposition 2.5.4. Soit a, b et c des entiers relatifs non nuls. Alors :

1. $a \vee b = |a| \vee |b|$
2. $a \vee b = b \vee a$
3. $a \vee a = |a|$
4. $a \vee 1 = |a|$
5. $(a \vee b) \vee c = a \vee (b \vee c)$
6. $a \mid b \iff a \vee b = |b|$
7. $a \vee b \mid ab$

Preuve :

- Les résultats 1), 2), 3) et 4) sont des conséquences de la définition et la remarque précédentes.
- Le résultat 5) découle de fait que : $(a\mathbb{Z} \cap b\mathbb{Z}) \cap c\mathbb{Z} = a\mathbb{Z} \cap (b\mathbb{Z} \cap c\mathbb{Z})$.
- Pour le résultat 6) : On sait que : $a \mid b \iff b\mathbb{Z} \subset a\mathbb{Z} \iff a\mathbb{Z} \cap b\mathbb{Z} = b\mathbb{Z}$
On en déduit donc que : $(a\mathbb{Z} \cap b\mathbb{Z}) \cap \mathbb{N}^* = b\mathbb{Z} \cap \mathbb{N}^*$. Ainsi : $a \mid b \iff a \vee b = |b|$
- Pour le résultat 7) : On a le produit ab est un multiple commun de a et b ; et par définition de $a \vee b$, on en déduit que ab est un multiple de $a \vee b$, c'est-à-dire que : $a \vee b \mid ab$.

Proposition 2.5.5. Soit a, b et c des entiers relatifs non nuls. Alors :

1. $(ca) \vee (cb) = |c|(a \vee b)$
2. $\begin{cases} c \mid a \\ c \mid b \end{cases} \Rightarrow \left(\frac{a}{c}\right) \vee \left(\frac{b}{c}\right) = \frac{a \vee b}{|c|}$
3. $(a \wedge b) \cdot (a \vee b) = |ab|$

Preuve : Fait comme exercice !

Exercice d'Application

1. Montrer que pour tout entiers relatifs a , on a : $a \wedge (a + 1) = 1$
2. Soit $n \in \mathbb{N}$, On considère les deux nombres $A = n^2 + 3$ et $B = n + 2$
 - a) Montrer que $A \wedge B = (n + 2) \wedge 7$
 - b) Déterminer l'entier naturel n tel que $\frac{n^2+3}{n+2} \in \mathbb{N}$
3. Soit $n \in \mathbb{N}$, On a $a = (25^n - 1)(36^n - 1)$ et $b = (5^n - 1)(6^n - 1)$. Calculer $a \vee b$

2.6 Congruence modulo n

Dans cette section, n est un entier naturel non nul

2.6.1 Définition et Exemples :

Définition 2.6.1. Soit $(a, b) \in \mathbb{Z}^2$

On dit que a est congru à b modulo n , et on note $a \equiv b[n]$, si et seulement si n divise $a - b$.

$$\begin{aligned} a \equiv b[n] &\iff n \mid (a - b) \\ &\iff \exists k \in \mathbb{Z} / a - b = kn \\ &\iff \exists k \in \mathbb{Z} / a = kn + b \end{aligned}$$

Exemple 2.6.1. — $7 \equiv 2[5] \iff 5 \mid 7 - 2$

— Si $a = bq + r \implies a \equiv r[b]$, si $b \in \mathbb{N}^*$

— $1 \equiv -3[4]$

Exemple 2.6.2. Déterminer l'ensemble des entiers relatifs n vérifiant $n \equiv 3[5]$:

$$\begin{aligned} n \equiv 3[5] &\iff 5 \mid n - 3 \\ &\iff \exists k \in \mathbb{Z} ; n - 3 = 5k \\ &\iff \exists k \in \mathbb{Z} ; n = 5k + 3 \end{aligned}$$

D'où l'ensemble A est : $A = \{5k + 3 / k \in \mathbb{Z}\}$.

2.6.2 Propriétés :

Proposition 2.6.1. Soit $n \in \mathbb{N}^*$.

i) $\forall a \in \mathbb{Z} : a \equiv a[n]$

ii) $\forall (a, b) \in \mathbb{Z}^2 : a \equiv b[n] \iff b \equiv a[n]$

iii) $\forall (a, b, c) \in \mathbb{Z}^3 : \begin{cases} a \equiv b[n] \\ b \equiv c[n] \end{cases} \implies a \equiv c[n]$

iv) $\forall (a, b, c, d) \in \mathbb{Z}^4$ et $\forall p \in \mathbb{N} :$

— $a \equiv b[n] \implies a + c \equiv b + c[n] \implies a \cdot c \equiv b \cdot c[n]$

- $\begin{cases} a \equiv b[n] \\ c \equiv d[n] \end{cases} \implies a + c \equiv b + d[n]$
- $\begin{cases} a \equiv b[n] \\ c \equiv d[n] \end{cases} \implies ac \equiv bd[n]$
- $a \equiv b[n] \implies a^p \equiv b^p[n]$
- v) $\forall a \in \mathbb{Z} : n \mid a \iff a \equiv 0[n]$
- vi) $\forall a \in \mathbb{Z} : \text{Si } r \text{ est le reste de la division euclidienne de } a \text{ par } n, \text{ alors } a \equiv r[n].$

Remarque 2.6.1. *Tout entier relatif est congru à son reste de la division euclidienne de a par n modulo n .*

Exercices d'application :

1. Déterminer le plus petit entier naturel qui est congru à 2025 modulo 4.
2. Montrer que $\forall n \in \mathbb{N} : 7 \mid (3^{2n} - 2^n)$.
3. Déterminer tous les entiers relatifs a tel que 7 divise $a^2 - a + 2$

2.7 L'Ensemble $\mathbb{Z}/n\mathbb{Z}$

2.7.1 Classes d'Équivalence

Définition 2.7.1. *Soit a un entier relatif.*

La classe de a modulo n , est l'ensemble noté $\bar{a}$, qui contient tous les entiers relatifs congrus à a modulo n .

$$\begin{aligned} \bar{a} &= \{x \in \mathbb{Z} \mid x \equiv a \pmod{n}\} \\ &= \{x = kn + a \mid k \in \mathbb{Z}\} \end{aligned}$$

Exemple 2.7.1. $\bar{n} = n\mathbb{Z} = \{kn \mid k \in \mathbb{Z}\}$

La classe de 3 modulo 4 est :

$$\begin{aligned} \bar{3} &= \{x \in \mathbb{Z} \mid x \equiv 3 \pmod{4}\} \\ &= \{x = 4k + 3 \mid k \in \mathbb{Z}\} \end{aligned}$$

Proposition 2.7.1. $\forall a, b \in \mathbb{Z} :$

- $a \equiv b \pmod{n} \iff \bar{a} = \bar{b}$
- $a \not\equiv b \pmod{n} \iff \bar{a} \cap \bar{b} = \emptyset$

2.7.2 L'ensemble $\mathbb{Z}/n\mathbb{Z}$

Définition 2.7.2.

$$\mathbb{Z}/n\mathbb{Z} = \{\bar{a} \mid a \in \mathbb{Z}\}$$

Preuve :

***Détermination de $\mathbb{Z}/n\mathbb{Z}$:** Soit $a \in \mathbb{Z}$, $\exists r \in \mathbb{N}$ tel que $a \equiv r \pmod{n}$ et on a $r \in \mathbb{N}$; $0 \leq r < n$.
 $\Rightarrow r \in \{0, 1, 2, \dots, n-1\}$
 Et on a $a \equiv r \pmod{n} \iff \bar{r} = \bar{a}$.
 D'où $\bar{a} \in \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{n-1}\}$.
 $\mathbb{Z}/n\mathbb{Z} = \{\bar{a} \mid a \in \mathbb{Z}\} = \{\bar{r} \mid r \in \{0, 1, 2, \dots, n-1\}\}$.
 D'où $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{n-1}\}$.

*** Montrons que $\text{Card}(\mathbb{Z}/n\mathbb{Z}) = n$:** C'est-à-dire montrons que les classes sont deux à deux distinctes.

On suppose $\exists(r, r') \in \{0, 1, 2, \dots, n-1\}^2$ tel que $r \neq r'$ et $\bar{r} = \bar{r}'$.

On a :

$$\begin{aligned} \bar{r} = \bar{r}' &\iff r \equiv r' \pmod{n} \\ &\iff n \mid (r - r') \\ &\iff r - r' = kn \\ &\iff |r - r'| = |k|n \end{aligned}$$

et $0 \leq r < n$ et $0 \leq r' < n$

donc $-n < r - r' < n$

donc $|r - r'| < n$

donc $|k| \cdot n < n$

donc $|k| < 1$

d'où $k = 0 \implies r = r'$, ce qui est absurde !

Proposition 2.7.2. L'ensemble $\mathbb{Z}/n\mathbb{Z}$ contient exactement n classes d'équivalence :

$$\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{n-1}\}$$

Exemple 2.7.2.

$$\mathbb{Z}/5\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$$

2.7.3 Opérations dans l'ensemble $\mathbb{Z}/n\mathbb{Z}$

Définition 2.7.3. On définit les opérations somme "+" et multiplication "×" dans $\mathbb{Z}/n\mathbb{Z}$ par : $\forall \bar{x}, \bar{y} \in \mathbb{Z}/n\mathbb{Z}$:

- $\bar{x} + \bar{y} = \overline{x + y}$
- $\bar{x} \times \bar{y} = \overline{x \times y}$

La somme dans $\mathbb{Z}/n\mathbb{Z}$

1. **Commutative** : $\bar{x} + \bar{y} = \bar{y} + \bar{x}$
2. **Associative** : $\bar{x} + (\bar{y} + \bar{z}) = (\bar{x} + \bar{y}) + \bar{z} = \overline{x + y + z}$
3. **Admet un élément neutre $\bar{0}$** :
Car $\forall \bar{x} \in \mathbb{Z}/n\mathbb{Z}$; $\bar{x} + \bar{0} = \bar{x}$
4. **Tout élément admet un opposé noté $-\bar{x}$** :
tel que $\bar{x} + (-\bar{x}) = \bar{0}$, où $\overline{n - x} = -\bar{x}$

Preuve de l'opposé :

$$\bar{x} + (-\bar{x}) = \bar{x} + \overline{n - x} = \overline{x + n - x} = \bar{n} = \bar{0}$$

La multiplication dans $\mathbb{Z}/n\mathbb{Z}$

est commutative, associative et admet un élément neutre $\bar{1}$.

Exemple 2.7.3. (La somme et la multiplication dans $\mathbb{Z}/4\mathbb{Z}$:) On a : $\mathbb{Z}/4\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$

Table de l'addition (+)

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

Table de la multiplication (×)

×	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{0}$	$\bar{2}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Exercices d'application

1. Résoudre dans $\mathbb{Z}/4\mathbb{Z}$:

$$3\bar{x} + \bar{1} = \bar{0}$$

2. Résoudre dans $(\mathbb{Z}/4\mathbb{Z})^2$:

$$\begin{cases} 2\bar{x} + \bar{y} = \bar{1} \\ 3\bar{x} - 2\bar{y} = \bar{2} \end{cases}$$

2.8 Nombres premiers entre eux

2.8.1 Définitions

Définition 2.8.1. Soient $a, b \in \mathbb{Z}^*$.

On dit que les nombres a et b sont premiers entre eux, si et seulement si :

$$a \wedge b = 1$$

Exemple 2.8.1. les nombres 4 et 5 sont premiers entre eux.

2.8.2 Propriétés

Proposition 2.8.1. Pour tout $a, b \in \mathbb{Z}^*$:

$$a \wedge b = 1 \implies a \vee b = |ab|$$

Preuve Soient $a, b \in \mathbb{Z}^*$. On a $(a \vee b)(a \wedge b) = |ab|$.

Et comme $a \wedge b = 1$, alors $a \vee b = |ab|$.

Théorème 2.8.1. (Théorème de Bézout) $\forall a, b \in \mathbb{Z}^*$:

$$a \wedge b = 1 \iff \exists u, v \in \mathbb{Z}, au + bv = 1$$

Démonstration Soient $a, b \in \mathbb{Z}^*$.

($\implies$) On suppose que $a \wedge b = 1$. c'est à dire 1 divise a et 1 divise b , il existe $u, v \in \mathbb{Z}$ tels que $au + bv = 1$.

($\impliedby$) Réciproquement, si $au + bv = 1$, tout diviseur commun de a et b divise aussi 1, donc $a \wedge b = 1$.

Lemme 2.8.1. (de Bézout) $\forall a, b \in \mathbb{Z}$, si $d = a \wedge b$:

$$\exists \alpha, \beta \in \mathbb{Z}, d = a\alpha + b\beta$$

Proposition 2.8.2. $\forall a, b \in \mathbb{Z}, d = a \wedge b \implies \frac{a}{d} \wedge \frac{b}{d} = 1$.

Démonstration On suppose que $d = a \wedge b$. Donc $\exists \alpha, \beta \in \mathbb{Z}, a\alpha + b\beta = d$.
 Soit $u = \frac{a}{d}$ et $v = \frac{b}{d}$.
 Alors $d(u\alpha + v\beta) = d \implies u\alpha + v\beta = 1$.
 Ainsi $\frac{a}{d} \wedge \frac{b}{d} = 1$.

Théorème 2.8.2. (de Gauss) $\forall a, b, c \in \mathbb{Z}^*$:

$$(a|bc \text{ et } a \wedge c = 1) \implies a|b$$

Démonstration Soient $a, b, c \in \mathbb{Z}$.

On a $a|bc \implies \exists k \in \mathbb{Z}, bc = ka$.

Et $a \wedge c = 1 \implies \exists u, v \in \mathbb{Z}, au + cv = 1$.

En multipliant par $b : b(au + cv) = b \implies abu + bcv = b$.

Donc $a(bu + kv) = b \implies a|b$.

Corollaire 2.8.1. (Gauss et congruence) i) $\forall a, b \in \mathbb{Z}^*$:

$$(ab \equiv 0 [n] \text{ et } b \wedge n = 1) \implies a \equiv 0 [n]$$

ii) $\forall a, b \in \mathbb{Z}^* : (a \wedge c = 1 \text{ et } a \wedge b = 1) \iff a \wedge bc = 1$.

iii) $\forall a, b \in \mathbb{Z}^* : a \wedge b = 1 \iff a^n \wedge b = 1$

Proposition 2.8.3. Soient $a, b, c \in \mathbb{Z}$:

$$(a|c, b|c \text{ et } a \wedge b = 1) \implies ab|c$$

Démonstration (Par deux Méthodes)

Méthode 1 $a|c \implies c = ak$ et $b|c \implies c = bk'$.

$a \wedge b = 1 \implies \exists u, v \in \mathbb{Z}, au + bv = 1$.

Alors $c(au + bv) = c \implies acu + bcv = c$.

Donc $ab(k'u + kv) = c \implies ab|c$.

Méthode 2 : laisser en exercice

Proposition 2.8.4. $\forall a, b, c \in \mathbb{Z}, \forall n \in \mathbb{N}^*$:

$$(ac \equiv bc [n] \text{ et } n \wedge c = 1) \implies a \equiv b [n]$$

Preuve : $ac \equiv bc [n] \implies n|(ac - bc) \implies n|c(a - b)$.

Comme $n \wedge c = 1$, d'après le théorème de Gauss : $n|(a - b) \implies a \equiv b [n]$.

Proposition 2.8.5. $\forall a, b, c \in \mathbb{Z}, \forall n \in \mathbb{N}$. si $n \wedge c = d$ alors :

$$ac \equiv bc [n] \implies a \equiv b \left[\frac{n}{d} \right]$$

Exercice d'application

1. Montrer que $\forall (a, b) \in \mathbb{N}^{*2}, \forall n \in \mathbb{N}^*$:

$$a^n \wedge b^n = (a \wedge b)^n$$

2. En déduire que :

$$\forall (a, b, n) \in \mathbb{N}^{*3}$$

$$a \mid b \iff a^n \mid b^n$$

2.9 L'équation diophantienne $ax + by = c$ dans $\mathbb{Z}^2$

2.9.1 Activité Preuve :

Énoncé : Soient $a, b, c \in \mathbb{Z}$ tels que $a \neq 0$ et $b \neq 0$.

On considère l'équation $(E) : ax + by = c$ où $x, y \in \mathbb{Z}$.

Soit S l'ensemble des solutions de (E) .

1. Montrer que $S \neq \emptyset \iff (a \wedge b) \mid c$.
2. On suppose que $(a \wedge b) \mid c$ et soit (x_0, y_0) une solution de (E) .
Montrer que $(E) \iff a'(x - x_0) = b'(y_0 - y)$, tel que :

$$a' = \frac{a}{a \wedge b} \quad \text{et} \quad b' = \frac{b}{a \wedge b}$$

3. En déduire l'ensemble des solutions de (E) en fonction de (x_0, y_0) .

Réponse :

1. Condition d'existence des solutions ($S \neq \emptyset$)

- **Sens ($\Leftarrow$) :** On suppose que $(a \wedge b) \mid c$. Montrons que $S \neq \emptyset$.

Comme $(a \wedge b) \mid c$, il existe $k \in \mathbb{Z}$ tel que $c = k(a \wedge b)$.

D'après le lemme de Bezout, il existe $\alpha, \beta \in \mathbb{Z}$ tels que $\alpha a + \beta b = a \wedge b$.

En multipliant par k , on obtient :

$$c = k(a \wedge b) \implies c = (k\alpha)a + (k\beta)b$$

D'où $(k\alpha, k\beta) \in S$, alors $S \neq \emptyset$.

• **Sens** ($\Rightarrow$) : On suppose $S \neq \emptyset$. Montrons que $(a \wedge b) \mid c$.
 $S \neq \emptyset \Rightarrow \exists (x_0, y_0) \in \mathbb{Z}^2$ tel que $ax_0 + by_0 = c$.
 On a $\begin{cases} a \wedge b \mid a \\ a \wedge b \mid b \end{cases} \Rightarrow \begin{cases} a \wedge b \mid ax_0 \\ a \wedge b \mid by_0 \end{cases} \Rightarrow a \wedge b \mid (ax_0 + by_0) \Rightarrow a \wedge b \mid c$.
 D'où $(a \wedge b) \mid c \iff S \neq \emptyset$.

2. Transformation de l'équation (E)

Soit (x_0, y_0) une solution particulière de (E) $\iff ax_0 + by_0 = c$.
 Pour tout $(x, y) \in \mathbb{Z}^2$:

$$\begin{aligned} (E) &\iff ax + by = ax_0 + by_0 \\ &\iff a(x - x_0) = b(y_0 - y) \end{aligned}$$

On pose $a = a'(a \wedge b)$ et $b = b'(a \wedge b)$ avec $a' \wedge b' = 1$. L'équation devient :

$$a'(a \wedge b)(x - x_0) = b'(a \wedge b)(y_0 - y)$$

En simplifiant par $a \wedge b$, on obtient :

$$a'(x - x_0) = b'(y_0 - y)$$

3. Ensemble des solutions

On a $a'(x - x_0) = b'(y_0 - y)$.
 $\Rightarrow b' \mid a'(x - x_0)$. Or $a' \wedge b' = 1$, donc d'après le théorème de Gauss :
 $b' \mid (x - x_0) \Rightarrow \exists k \in \mathbb{Z}$ tel que $x - x_0 = kb' \Rightarrow x = x_0 + kb'$.
 En remplaçant dans l'équation :

$$a'(kb') = b'(y_0 - y) \Rightarrow a'k = y_0 - y \Rightarrow y = y_0 - ka'$$

Réciproquement : Si $(x, y) = (x_0 + kb', y_0 - ka')$, on vérifie bien que $a'(x - x_0) = a'kb'$ et $b'(y_0 - y) = b'(ka')$. Les deux membres sont égaux.

L'ensemble des solutions est :

$$S = \{(x_0 + kb', y_0 - ka') \mid k \in \mathbb{Z}\}$$

2.9.2 Propriétés

Proposition 2.9.1. Soient $a, b, c \in \mathbb{Z}$ avec $a \neq 0$ et $b \neq 0$, et (E) l'équation définie par :

$$(E) : ax + by = c \quad , \quad (x, y) \in \mathbb{Z}^2$$

et S l'ensemble des solutions de (E) .

- i) Si $a \wedge b$ ne divise pas c , alors $S = \emptyset$.
- ii) Si $a \wedge b$ divise c , alors $S = \left\{ \left(x_0 + k \frac{b}{a \wedge b} ; y_0 - \frac{a}{a \wedge b} k \right) / k \in \mathbb{Z} \right\}$ tel que (x_0, y_0) est une solution particulière de (E) .

Preuve : Voir activité

Exercices d'application :

Exercice (1) On considère l'équation $(E) : 3x + 4y = 1$, $(x, y) \in \mathbb{Z}^2$.

1. Déterminer $(x_0; y_0)$ une solution particulière de (E) , si elle existe.
2. En déduire l'ensemble des solutions de (E) .

Exercice (2) On considère l'équation $(E) : 21x - 18y = 9$.

1. Montrer que S , l'ensemble des solutions, est non vide.
2. En utilisant l'algorithme d'Euclide, déterminer une solution particulière $(x_0; y_0)$ de (E) .
3. Déterminer S , l'ensemble des solutions de (E) .

2.10 PGCD et PPCM de plusieurs entiers relatifs

2.10.1 Définitions

Définition 2.10.1. Soit $n \in \mathbb{N}^*$ et $n \geq 3$.

Soient $a_1, a_2, \dots, a_n$ des entiers relatifs.

— Le plus grand diviseur commun des entiers $a_1, a_2, \dots, a_n$ est l'entier

naturel noté $\bigwedge_{i=1}^n a_i$, tel que :

$$\bigwedge_{i=1}^n a_i = \sup \left(\bigcap_{i=1}^n \mathcal{D}_{a_i}^+ \right)$$

— Le plus petit multiple commun des entiers $a_1, a_2, \dots, a_n$ est l'entier

naturel noté $\bigvee_{i=1}^{i=n} a_i$, tel que :

$$\bigvee_{i=1}^{i=n} a_i = \inf \left(\bigcap_{i=1}^{i=n} \mathcal{M}_{a_i}^{*+} \right)$$

2.10.2 Propriétés

Proposition 2.10.1. Les opérations de détermination du PGCD et PPCM sont associatives et commutatives.

Exemple 2.10.1. Déterminons $32 \wedge 14 \wedge 63 \wedge 18$. On a :

$$32 \wedge 14 \wedge 63 \wedge 18 = (14 \wedge 63) \wedge (32 \wedge 18) = 7 \wedge 2 = 1$$

Proposition 2.10.2. (Coefficient de Bezout) $\forall (a_1, a_2, \dots, a_n) \in (\mathbb{Z}^*)^n, \exists (\alpha_1, \alpha_2, \dots, \alpha_n) \in \mathbb{Z}^n$ tel que :

$$\bigwedge_{i=1}^{i=n} a_i = \sum_{i=1}^n \alpha_i a_i$$

Proposition 2.10.3. (Théorème de Bezout) $\forall (a_1, a_2, \dots, a_n) \in (\mathbb{Z}^*)^n$, tel que :

$$\bigwedge_{i=1}^{i=n} a_i = 1 \iff \exists (\alpha_1, \alpha_2, \dots, \alpha_n) \in \mathbb{Z}^n / \sum_{i=1}^n \alpha_i a_i = 1$$

Remarque 2.10.1. Si $\bigwedge_{i=1}^{i=n} a_i = 1$, alors on dit que tous les nombres sont premiers entre eux (ça ne veut pas dire qu'ils sont deux à deux premiers entre eux).

Par exemple : car $32 \wedge 14 \wedge 63 \wedge 18 = 1$ mais $18 \wedge 32 \neq 1$.

Proposition 2.10.4. $\forall (a_1, a_2, \dots, a_n) \in (\mathbb{Z}^*)^n$ et $d \in \mathbb{Z}^*$

$$d \mid \bigwedge_{i=1}^{i=n} a_i \iff d \mid a_i ; \forall i \in \{1, 2, \dots, n\}$$

Attention ! :

La propriété $\left(\bigwedge_{i=1}^{i=n} a_i\right) \times \left(\bigvee_{i=1}^{i=n} a_i\right) = \left|\prod_{i=1}^{i=n} a_i\right|$ n'est pas toujours vraie pour plusieurs entiers relatifs.

Exemple 2.10.2. On considère les nombres : $a = 4$, $b = 8$ et $c = 7$.

- $a \wedge b \wedge c = (a \wedge b) \wedge c = (4 \wedge 8) \wedge 7 = 4 \wedge 7 = 1$
 - $a \vee b \vee c = (a \vee b) \vee c = (4 \vee 8) \vee 7 = 8 \vee 7 = 56$
 - Or $(a \wedge b \wedge c) \cdot (a \vee b \vee c) = 56$ mais $|a \times b \times c| = 224$
- Alors $(a \wedge b \wedge c) \cdot (a \vee b \vee c) \neq |a \times b \times c|$.

2.11 Complément sur les nombres premiers

2.11.1 Nombres premiers et divisibilité

Proposition 2.11.1. Soient $a, b \in \mathbb{Z}$:

$$\left(\begin{array}{l} \text{si } a \text{ est premier} \\ \text{et } a \text{ ne divise pas } b \end{array} \right) \implies a \wedge b = 1$$

Preuve : On a $D_a = \{-a, -1, 1, a\}$

On a $a \nmid b \implies \{a, -a\} \not\subset D_b$

D'où $a \wedge b = \sup(D_a \cap D_b) = \sup(\{-1, 1\}) = 1$

Proposition 2.11.2. i) Si a et b sont deux nombres premiers de $\mathbb{Z}$, alors on a :

$$a \wedge b = 1 \iff |a| \neq |b|$$

ii) Si a et b sont deux entiers naturels premiers, alors :

$$a \mid b \iff a = b$$

iii) Soit p un nombre premier dans $\mathbb{Z}$:

$$\forall a, b \in \mathbb{Z} : p \mid a \times b \implies p \mid a \text{ ou } p \mid b$$

Preuve : i) et ii) Sont des connaissances immédiates très simples à démontrer.

(iii) Soit p un nombre premier, et soit $(a, b) \in \mathbb{Z}^2$.

$$\text{— Si } p \mid a \implies p \mid a \times b \implies p \mid a \text{ ou } p \mid b \quad \textcircled{1}$$

$$\begin{aligned} \text{— Si } p \nmid a \implies p \wedge a = 1 \text{ et } p \mid ab \\ \implies p \mid b \text{ (d'après Gauss)} \end{aligned} \quad \textcircled{2}$$

De $\textcircled{1}$ et $\textcircled{2}$, si $p \mid a \times b \implies p \mid a$ ou $p \mid b$.

Généralisation :

Soit $n \in \mathbb{N}^* \setminus \{1\}$ et soit p un nombre premier et soient $(a_1, a_2, \dots, a_n) \in \mathbb{Z}^n$.

$$p \mid \prod_{i=1}^n a_i \Rightarrow \exists i \in \{1, 2, \dots, n\} \text{ tel que } p \mid a_i$$

Corollaire 2.11.1. Soit p un nombre premier et soit $n \in \mathbb{N}^*$

i) $\forall a \in \mathbb{Z} ; p \mid a^n \Rightarrow p \mid a$

ii) $\forall (a, b) \in \mathbb{Z}^2 ; a \cdot b \equiv 0 [p] \Rightarrow a \equiv 0 [p] \text{ ou } b \equiv 0 [p]$

iii) Si $1 \leq n < |p| \Rightarrow n \wedge p = 1$

Proposition 2.11.3. (Petit Théorème de FERMAT) Soit p un nombre premier

i) $\forall a \in \mathbb{Z} ; a^p \equiv a [p]$

ii) $\forall a \in \mathbb{Z} ; a \wedge p = 1 \Rightarrow a^{p-1} \equiv 1 [p]$

Exercices d'application

Exercice 1 : Déterminer les entiers relatifs n tel que :

$$\frac{n^3 - 3}{n - 3} \in \mathbb{Z}$$

Exercice 2 : Soit p un nombre premier positif.

1. Montrer que $\forall k \in \{1, \dots, p-1\} : p \mid \binom{p}{k}$

$$\text{tel que } \binom{p}{k} = \frac{p!}{k!(p-k)!}$$

2. En déduire que $\forall a \in \mathbb{N} : (a+1)^p \equiv a^p + 1 \pmod{p}$

3. (a) Montrer que $\forall n \in \mathbb{N} : n^p \equiv n \pmod{p}$

(b) En déduire que si $n \wedge p = 1 \Rightarrow n^{p-1} \equiv 1 \pmod{p}$

4. Montrer que $\forall a \in \mathbb{Z} :$

(a) $a^p \equiv a \pmod{p}$

(b) Si $a \wedge p = 1$ alors $a^{p-1} \equiv 1 \pmod{p}$

2.12 Système de Numération

2.12.1 Définition des systèmes de Numération

Définition 2.12.1. *On appelle système de numération l'ensemble des symboles et des chiffres dans lesquels on peut exprimer les nombres entiers naturels.*

Exemple 2.12.1. 1. *Le système de numération décimale :*

C'est le système le plus fréquent et le nombre de ses chiffres est 10 :

$$0 - 1 - 2 - 3 - 4 - 5 - 6 - 7 - 8 - 9$$

Le nombre 10 s'appelle la base du système de numération.

2. *Le système de numération binaire :*

Il est souvent utilisé au domaine informatique.

Sa base est 2 et ses chiffres sont 0 et 1.

3. *Le système duodécimal :*

C'est un système à base 12.

Le nombre de ses chiffres est 12 :

$$0 - 1 - 2 - 3 - 4 - 5 - 6 - 7 - 8 - 9 - A - B$$

Remarque 2.12.1. *Le système de numération binaire est le plus existant*

2.12.2 Représentation d'un entier naturel dans un système de numération connus

Proposition 2.12.1. *Soit $b \in \mathbb{N}$ tel que $b \geq 2$.*

Pour tout entier naturel N , il existe un unique entier n tel que :

$$N = a_n b^n + a_{n-1} b^{n-1} + \dots + a_2 b^2 + a_1 b^1 + a_0 b^0$$

où $\forall i \in \{0, \dots, n\}, 0 \leq a_i < b$.

On écrit $N = \overline{a_n a_{n-1} a_{n-2} \dots a_0}_{(b)}$ et on dit que N est représenté dans la base b .

Exemple 2.12.2. *On considère le nombre $N = 181234$ dans la base décimale.*

$$\begin{aligned} N &= 100000 + 80000 + 1000 + 200 + 30 + 4 \\ &= 1 \times 10^5 + 8 \times 10^4 + 1 \times 10^3 + 2 \times 10^2 + 3 \times 10^1 + 4 \times 10^0 \end{aligned}$$

Entre deux bases de numération autre que la base décimale

On représente le nombre dans la base décimale, après on le représente dans la base demandée.

Exemple 2.12.6. Représenter $N = \overline{4302}_{(5)}$ dans la base 8.

On a :

$$\begin{aligned} N &= 2 \times 5^0 + 0 \times 5^1 + 3 \times 5^2 + 4 \times 5^3 \\ &= 2 + 75 + 500 = 577 \end{aligned}$$

2.12.5 Addition et multiplication des nombres représentés dans une base

Exemple 2.12.7. On pose $A = \overline{212}_{(3)}$ et $B = \overline{11}_{(3)}$.

Calculons $A + B$ et $A \times B$.

Méthode 1 : Conversion en base 10

$$A = 2 \cdot 3^0 + 1 \cdot 3^1 + 2 \cdot 3^2 = 2 + 3 + 18 = 23_{(10)}$$

$$B = 1 \cdot 3^0 + 1 \cdot 3^1 = 1 + 3 = 4_{(10)}$$

$$\begin{array}{r} 27 \\ 0 \\ \hline 03 \\ 01 \\ \hline 10 \end{array} \begin{array}{l} 3 \\ 9 \ / \ 3 \\ 3 \ / \ 3 \\ 1 \ 0 \end{array} \Rightarrow A + B = \overline{1000}_{(3)}$$

$$\begin{array}{r} 92 \\ 2 \\ \hline 30 \\ 10 \\ 13 \\ 01 \\ \hline 10 \end{array} \begin{array}{l} 3 \\ 30 \ / \ 3 \\ 10 \ / \ 3 \\ 3 \ / \ 3 \\ 1 \ 0 \end{array} \Rightarrow A \times B = \overline{10102}_{(3)}$$

Méthode 2 : Développement polynomial

Addition :

$$\begin{aligned} A + B &= (2 \cdot 3^0 + 1 \cdot 3^1 + 2 \cdot 3^2) + (1 \cdot 3^0 + 1 \cdot 3^1) \\ &= 3 \cdot 3^0 + 2 \cdot 3^1 + 2 \cdot 3^2 \\ &= 3 + 2 \cdot 3 + 2 \cdot 3^2 \\ &= 3 \cdot 3 + 2 \cdot 3^2 = 3^2 + 2 \cdot 3^2 = 3 \cdot 3^2 = 3^3 \\ &= 1 \cdot 3^3 + 0 \cdot 3^2 + 0 \cdot 3^1 + 0 \cdot 3^0 = \overline{1000}_{(3)} \end{aligned}$$

Multiplication :

$$\begin{aligned}
 A \times B &= (2 \cdot 3^0 + 1 \cdot 3^1 + 2 \cdot 3^2) \times (1 \cdot 3^0 + 1 \cdot 3^1) \\
 &= 2 \cdot 3^0 + 2 \cdot 3^1 + 1 \cdot 3^1 + 1 \cdot 3^2 + 2 \cdot 3^2 + 2 \cdot 3^3 \\
 &= 2 \cdot 3^0 + 3 \cdot 3^1 + 3 \cdot 3^2 + 2 \cdot 3^3 \\
 &= 2 \cdot 3^0 + 3^2 + 3^3 + 2 \cdot 3^3 = 2 \cdot 3^0 + 3^2 + 3 \cdot 3^3 \\
 &= 1 \cdot 3^4 + 0 \cdot 3^3 + 1 \cdot 3^2 + 0 \cdot 3^1 + 2 \cdot 3^0 = \overline{10102}_{(3)}
 \end{aligned}$$

Méthode 3 : Position verticale

$$\begin{array}{r}
 \begin{array}{r}
 {}^{(1)}({}_1) \\
 212 \\
 + 11 \\
 \hline
 1000 \quad \text{en base } (3)
 \end{array}
 \qquad
 \begin{array}{r}
 212 \\
 \times 11 \\
 \hline
 212 \\
 + 2120 \\
 \hline
 10102 \quad \text{en base } (3)
 \end{array}
 \end{array}$$

2.12.6 Comparaison de deux nombres dans un systèmes de numération

Proposition 2.12.2. Soient $A = \overline{a_n a_{n-1} a_{n-2} \dots a_0}_{(b)}$ et $B = \overline{b_m b_{m-1} b_{m-2} \dots b_0}_{(b)}$ deux entiers naturels représentés dans le même système de numérotation à base b .

i) Si $m \neq n$

- $m > n \implies B > A$
- $m < n \implies A > B$

ii) Si $m = n$

$$a_n > b_n \implies A > B$$

Si $a_n = b_n$ et $a_{n-1} = b_{n-1}$ et ... et $a_k \neq b_k$ avec $k \in \{0, 1, \dots, n-1\}$:

- Si $a_k > b_k \implies A > B$
- Si $a_k < b_k \implies B > A$

2.12.7 Critère de divisibilité dans la base décimal

Dans tout ce qui vient N est un entier naturel représenté dans le système décimal par :

$$\begin{aligned} N &= \overline{a_n a_{n-1} a_{n-2} \dots a_0}_{(10)} \quad \text{avec } a_n \neq 0 \\ &= a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \dots + a_0 \cdot 10^0 \\ &= \sum_{k=0}^n a_k 10^k \end{aligned}$$

a) Divisibilité par 3 et 9

On a $10 \equiv 1 \pmod{3}$

Alors, $\forall k \in \{0, 1, \dots, n\}$, $10^k \equiv 1^k \equiv 1 \pmod{3}$

$$\text{---} \implies a_k 10^k \equiv a_k \pmod{3}$$

$$\text{---} \implies \sum_{k=0}^n a_k 10^k \equiv \sum_{k=0}^n a_k \pmod{3}$$

$$\text{---} \implies N \equiv \sum_{k=0}^n a_k \pmod{3}$$

$$\text{Alors } 3 \mid N \iff 3 \mid \sum_{k=0}^n a_k$$

De même, on montre que :

$$9 \mid N \iff 9 \mid \sum_{k=0}^n a_k \quad \text{avec } 10 \equiv 1 \pmod{9}$$

Proposition 2.12.3. *i) Le nombre N est divisible par 3, si et seulement si, la somme de ses chiffres est divisible par 3.*

ii) Le nombre N est divisible par 9, si et seulement si, la somme de ses chiffres est divisible par 9.

b) Divisibilité par 2 et par 5

On a $10 \equiv 0[2]$ et $10^0 \equiv 1[2]$

$$\text{---} \implies \forall k \in \{1, 2, \dots, n\} : 10^k \equiv 0[2] \text{ et } 10^0 \equiv 1[2]$$

$$\text{---} \implies a_k 10^k \equiv 0[2] \text{ et } 10^0 a_0 \equiv a_0[2]$$

$$\text{---} \implies \sum_{k=1}^n a_k 10^k \equiv 0[2] \text{ et } a_0 \equiv a_0[2]$$

$$\text{---} \implies \sum_{k=0}^n a_k 10^k \equiv a_0[2]$$

— $\implies N \equiv a_0[2]$
 Alors $2 \mid N \iff 2 \mid a_0 \quad / a_0 \in \{0, 2, 4, 6, 8\}$
 De même on a $10 \equiv 0[5]$ et $10^0 \equiv 1[5]$
 Ainsi $N \equiv a_0[5]$
 D'où $5 \mid N \iff 5 \mid a_0 \quad / a_0 \in \{0, 5\}$

Proposition 2.12.4. (i) *Le nombre N est divisible par 2, si et seulement si son chiffre d'unité est 0, 2, 4, 6 ou 8.*
 (ii) *Le nombre N est divisible par 5, si et seulement si son chiffre d'unité est 0 ou 5.*

c) Divisibilité par 4, par 25 et 50

On a $10^0 \equiv 1[4]$ et $10 \equiv 2[4]$ et $10^2 \equiv 0[4]$.
 — $\implies \forall k \in \{2, \dots, n\}; 10^k \equiv 0[4]$ et $10^0 \equiv 1[4]$ et $10^1 \equiv 10[4]$
 — Alors $a_k 10^k \equiv 0[4]$ et $a_0 10^0 \equiv a_0[4]$ et $a_1 10^1 \equiv 10a_1[4]$
 — d'où $\sum_{k=2}^n a_k 10^k \equiv 0[4]$ et $a_0 + 10 \times a_1 \equiv a_0 + 10a_1[4]$
 — d'où $\sum_{k=0}^n a_k 10^k \equiv a_0 + a_1 \times 10[4]$
 — d'où $N \equiv \overline{a_1 a_0}_{(10)}[4]$
Alors $4 \mid N \iff 4 \mid \overline{a_1 a_0}_{(10)}$
 $\overline{a_1 a_0}_{(10)} \in \{0, 4, 8, 12, 16, 20, 24, 28, 32, \dots, 96\}$
 — On a $10 \equiv 10[25] \implies 10^2 \equiv 0[25]$
 — alors $\forall k \in \{2, \dots, n\}; 10^k \equiv 0[25]$
 — alors $a_k 10^k \equiv 0[25]$
 — donc $\sum_{k=2}^n a_k 10^k \equiv 0[25]$
 — Alors $\sum_{k=2}^n a_k 10^k + 10 \times a_1 + 10^0 \times a_0 \equiv \overline{a_1 a_0}_{(10)}[25]$
 — D'où $N \equiv \overline{a_1 a_0}_{(10)}[25]$
Alors $25 \mid N \iff 25 \mid \overline{a_1 a_0}_{(10)}$
 $\overline{a_1 a_0}_{(10)} \in \{0, 25, 50, 75\}$
 — $10^2 \equiv 0[50]$, alors $\forall k \in \{2, \dots, n\}; 10^k \equiv 0[50]$
 — alors $a_k 10^k \equiv 0[50]$
 — Ainsi $\sum_{k=2}^n a_k 10^k \equiv 0[50]$
 — D'où $N \equiv \overline{a_1 a_0}_{(10)}[50]$

Alors $50/N \iff 50/\overline{a_1 a_0}_{(10)}$
 $\overline{a_1 a_0}_{(10)} \in \{0, 50\}$

Proposition 2.12.5. 1. N est divisible par 4, si $\overline{a_1 a_0}_{(10)}$ est un multiple de 4.
 2. N est divisible par 25, si $\overline{a_1 a_0}_{(10)}$ est un multiple de 25.
 3. N est divisible par 50, si $\overline{a_1 a_0}_{(10)}$ est un multiple de 50.

D) Divisibilité par 11

On a $10^0 \equiv 1[11]$ et $10 \equiv -1[11]$.
 $10^2 \equiv 1[11]$ et $10^3 \equiv -1[11]$.

$$\left. \begin{array}{l} 10^k \equiv 1[11] \text{ si } k = 2p / p \in \mathbb{N} \\ 10^k \equiv -1[11] \text{ si } k = 2p + 1 / p \in \mathbb{N} \end{array} \right\} 0 \leq k \leq n$$

$$N = a_0 \cdot 10^0 + a_1 \cdot 10^1 + \cdots + a_{n-1} \cdot 10^{n-1} + a_n \cdot 10^n \pmod{11}$$

$$\equiv a_0 - a_1 + a_2 - a_3 + \cdots + \varepsilon \cdot a_n \pmod{11}$$

$$\text{tel que } \begin{cases} \varepsilon = 1 & \text{si } n \text{ pair} \\ \varepsilon = -1 & \text{si } n \text{ impair} \end{cases}$$

$$\text{donc } N \equiv \sum_{k=0}^n (-1)^k a_k \pmod{11}$$

$$\text{d'où } 11/N \iff 11 / \sum_{k=0}^n (-1)^k a_k$$

Exemple 2.12.8. $\overline{121}_{(10)} = 1 \times 10^0 + 2 \times 10^1 + 1 \times 10^2$

$$\begin{aligned} 11/\overline{121}_{(10)} &\iff 11 / \sum_{k=0}^2 (-1)^k a_k \\ &\iff 11/(-1)^0 a_0 + (-1)^1 a_1 + (-1)^2 a_2 \\ &\iff 11/1 - 2 + 1 \\ &\iff 11/0 \end{aligned}$$

$$\sum_{k=0}^n (-1)^k a_k = \sum a_{2p} - \sum a_{2p+1}$$

Chapitre 3

LOIS DE COMPOSITION INTERNE (L.C.I)

3.1 Introduction

« Pour bien comprendre le contenu de ce chapitre, en général, on se propose pour revues du except et des rappels concernant les opérations usuels dans quelques ensembles fondamentales et particulière. »

1) L'ensemble des classes modulo n ($\mathbb{Z}/n\mathbb{Z}$)

On a $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$

Pour tout $(\bar{x}, \bar{y}) \in (\mathbb{Z}/n\mathbb{Z})^2$:

$$\begin{cases} \bar{x} + \bar{y} = \overline{x + y} \\ \bar{x} \times \bar{y} = \overline{x \times y} \end{cases}$$

2) L'ensemble des polynômes de degré $\leq n$ ($\mathbb{R}_n[X]$)

$\forall (P, Q) \in \mathbb{R}_n[X]^2, \forall x \in \mathbb{R}$, on a :

$$\begin{cases} (P + Q)(x) = P(x) + Q(x) \\ (P \times Q)(x) = P(x) \times Q(x) \end{cases}$$

3) L'ensemble des fonctions de I vers $\mathbb{R}$ ($\mathcal{F}(I, \mathbb{R})$)

On a $\mathcal{F}(I, \mathbb{R}) = \{f \mid f : I \rightarrow \mathbb{R}, x \mapsto f(x)\}$

$\forall (f, g) \in \mathcal{F}(I, \mathbb{R})^2, \forall x \in I$, on a :

$$\begin{cases} (f + g)(x) = f(x) + g(x) \\ (f \times g)(x) = f(x) \times g(x) \end{cases}$$

4) L'ensemble des parties d'un ensemble E ($\mathcal{P}(E)$)

$$X \subset E \iff X \in \mathcal{P}(E)$$

Pour tout $(X, Y) \in \mathcal{P}(E)^2$:

i) $x \in X \cap Y \iff x \in X \text{ et } x \in Y$

ii) $x \in X \cup Y \iff x \in X \text{ ou } x \in Y$

iii) $x \in \overline{X} \iff x \in E \text{ et } x \notin X$

iv) $x \in X \setminus Y \iff x \in X \text{ et } x \notin Y$

v) $X \Delta Y = (X \setminus Y) \cup (Y \setminus X) = (X \cup Y) \setminus (X \cap Y)$

5) L'ensemble des transformations du plan ($\mathcal{T}$)

Toute application bijective de $\mathcal{P}$ vers $\mathcal{P}$ s'appelle une transformation du plan.

Les transformations usuelles sont : les translations, l'homothétie, la rotation.

$(\forall R, h \in \mathcal{T}^2)(\forall M \in \mathcal{P})$, on a :

$$(R \circ h)(M) = R(h(M))$$

3.2 Définition d'une loi de composition interne

Définition 3.2.1. Soit E un ensemble non vide. Une loi de composition (opération ou loi) sur E est la donnée d'une application de $E \times E$ dans E . On note souvent une loi de composition par $*$, $\top$, $+$, etc. Pour un couple (x, y) de $E \times E$ on note $x * y$, $x \top y$, $x + y$ son image. Enfin on écrit $(E, *)$ pour dire que $*$ est une loi de composition sur E .

Exemple 3.2.1. 1. Les lois usuelles $+$, $\times$ sur $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$.

2. Les lois $\cap, \cup, \Delta$ sur $\mathcal{P}(E)$.

3. Soit E un ensemble non vide muni d'une loi $*$ et soit X un ensemble. On munit l'ensemble $\mathcal{F}(X, E)$ des applications de X dans E , d'une loi, notée aussi $*$, comme suit :

$$\forall f, g \in \mathcal{F}(X, E), \forall x \in X : (f * g)(x) = f(x) * g(x)$$

3.2. DÉFINITION D'UNE LOI DE COMPOSITION INTERNE

Définition 3.2.2. Soit $(E, *)$ et soit F une partie de E . On dit que F est stable par la loi $*$ si :

$$\forall x, y \in F, x * y \in F$$

La restriction de la loi sur $F \times F$ définit une loi de composition sur F dite la loi induite par $*$ sur F .

Exemple 3.2.2. 1. Pour la loi usuelle $+$ sur $\mathbb{Z}$, la partie $5\mathbb{Z}$ des multiples de 5, est une partie stable.

2. Pour la loi usuelle $\times$ sur $\mathbb{R}$, la partie $\mathbb{R}^+$ est une partie stable tandis que la partie $\mathbb{R}^-$ ne l'est pas.

Définition 3.2.3. Soit E un ensemble muni d'une loi $*$. Un élément e de E s'appelle un élément neutre pour la loi si :

$$\forall x \in E, x * e = e * x = x$$

On dit aussi que la loi possède un élément neutre e .

Proposition 3.2.1. Si une loi possède un élément neutre, il est unique.

Preuve Soient e et e' deux éléments neutres pour une loi $*$.

Comme e est un élément neutre il vient $e * e' = e' * e = e'$.

Et comme e' est un élément neutre on a $e * e' = e' * e = e$.

D'où $e = e'$.

Notation 3.2.1. Souvent on note $+$ une loi commutative et 0 son élément neutre. L'élément neutre d'une loi $\times$, notée multiplicativement, est noté 1.

Exemple 3.2.3. Dans $\mathcal{P}(E)$ l'ensemble E est l'élément neutre pour l'intersection. Pour la réunion, l'élément neutre est l'ensemble vide.

Définition 3.2.4. Soit E un ensemble muni d'une loi $*$.

1. La loi $*$ est dite associative si : $\forall x, y, z \in E, (x * y) * z = x * (y * z)$.
2. La loi est dite commutative si : $\forall x, y \in E, x * y = y * x$.

Définition 3.2.5. Soit E un ensemble non vide muni d'une loi de composition qui admet un élément neutre e .

Un élément x de E est dit symétrisable ou inversible s'il existe un élément x' de E tel que $x * x' = x' * x = e$.

L'élément x' s'appelle un symétrique de x .

Remarque 3.2.1. Si la loi est associative, le symétrique d'un élément, lorsqu'il existe, est unique.

Notation 3.2.2. 1. Pour une loi notée additivement $+$, le symétrique (ou opposé) d'un élément x de E est noté $-x$.
 2. Pour une loi notée multiplicativement $\times$, le symétrique (ou inverse) d'un élément x de E est noté x^{-1} ou $\frac{1}{x}$.
 3. Les expressions $y + (-x)$ et yx^{-1} se simplifient respectivement en $y - x$ et $\frac{y}{x}$.

Remarque 3.2.2. 1. On a $e^{-1} = e$.
 2. Si x et y sont inversibles pour la loi, alors $x * y$ est inversible et on a $(x * y)^{-1} = y^{-1} * x^{-1}$.
 3. Pour la multiplication, le nombre 3 est inversible dans $\mathbb{R}$ mais ne l'est pas dans $\mathbb{Z}$.

Exemple 3.2.4. 1. Dans $(\mathbb{N}, +)$, le seul élément qui admet un opposé est 0.
 2. Dans $(\mathbb{Z}, \times)$, les seuls éléments inversibles sont -1 et 1 .

Définition 3.2.6. Soit E un ensemble muni d'une loi. Un élément x de E est dit :

- simplifiable (ou régulier) à gauche si $\forall y, z \in E, x * y = x * z \Rightarrow y = z$.
- simplifiable (ou régulier) à droite si $\forall y, z \in E, y * x = z * x \Rightarrow y = z$.
- simplifiable (ou régulier) s'il est simplifiable à gauche et à droite.

Remarque 3.2.3. Pour une loi commutative, la régularité à gauche est équivalente à la régularité à droite.

Exemple 3.2.5. 1. Dans un ensemble non vide E muni d'une loi de composition associative, tout élément inversible est simplifiable.
 2. Un élément simplifiable n'est pas nécessairement inversible. Dans $(\mathbb{Z}, \times)$, tout élément non nul est simplifiable mais seuls -1 et 1 sont inversibles.

3.3 Morphismes

Définition 3.3.1. Soit $(E, *)$ et $(F, \top)$ deux ensembles munis de lois de composition interne et soit $f : E \rightarrow F$ une application.

On dit que f est un morphisme (homomorphisme) de $(E, *)$ dans $(F, \top)$, lorsque :

$$(\forall x, y \in E); \quad f(x * y) = f(x) \top f(y)$$

Définition 3.3.2. — Un endomorphisme de $(E, *)$ est un morphisme de $E \longrightarrow E$ (dans lui-même).

- Un isomorphisme est un morphisme bijectif.
- Un automorphisme est un endomorphisme bijectif.

Exemple 3.3.1. 1. On considère l'application :

$$f : (\mathbb{Z}, +) \rightarrow (\mathbb{Z}^*, \times)$$

$$x \mapsto 5^x$$

On a pour tout $(x, y) \in \mathbb{Z}^2$: $f(x + y) = 5^{x+y} = 5^x \times 5^y = f(x) \times f(y)$
Par conséquent, f est un morphisme de $(\mathbb{Z}, +)$ dans $(\mathbb{Z}^*, \times)$.

2. On considère l'application :

$$g :]0, +\infty[\rightarrow \mathbb{R}$$

$$x \mapsto \ln x$$

On a pour tout $(x, y) \in]0, +\infty[^2$: $g(xy) = \ln(xy) = \ln x + \ln y = g(x) + g(y)$

Par conséquent, g est un morphisme de $]0, +\infty[$ dans $\mathbb{R}$.

3. On considère l'application :

$$h : \mathbb{C} \rightarrow \mathbb{R}$$

$$z \mapsto |z|$$

On a pour tout $(z_1, z_2) \in \mathbb{C}^2$: $h(z_1 \times z_2) = |z_1 \times z_2| = |z_1| \times |z_2| = h(z_1) \times h(z_2)$

Par conséquent, h est un morphisme de $(\mathbb{C}, \times)$ dans $(\mathbb{R}, \times)$.

Proposition 3.3.1. Soit f un morphisme de $(E, *)$ dans $(F, \top)$.

1. $f(E)$ est une partie stable de $(F, \top)$.
2. Si la loi $*$ est associative dans $(E, *)$, alors la loi $\top$ est associative dans $(f(E), \top)$.
3. Si la loi $*$ est commutative dans $(E, *)$, alors la loi $\top$ est commutative dans $(f(E), \top)$.
4. Si la loi $*$ admet un élément neutre e dans $(E, *)$, alors $f(e)$ est un élément neutre dans $(f(E), \top)$.
5. Si la loi $*$ admet un élément neutre e dans $(E, *)$, et un élément x admet un symétrique x' dans $(E, *)$, alors $f(x)$ admet un symétrique dans $(f(E), \top)$ qui est $f(x')$.

Démonstration

1. Soit y_1 et y_2 deux éléments de $f(E)$. Il existe donc $(x_1; x_2) \in E^2$ tel que : $y_1 = f(x_1)$ et $y_2 = f(x_2)$.
Puisque f un morphisme de $(E; *)$ dans $(F; \top)$, alors : $y_1 \top y_2 = f(x_1) \top f(x_2) = f(x_1 * x_2)$.
Comme $*$ est une loi de composition interne sur E , alors $x_1 * x_2 \in E$, et donc $f(x_1 * x_2) \in f(E)$.
Par suite, $y_1 \top y_2 \in f(E)$. Ainsi, $f(E)$ est une partie stable de $(F; \top)$.
2. Soit $(u; v; w) \in (f(E))^3$. Il existe donc $(x; y; z) \in E^3$ tel que : $u = f(x)$ et $v = f(y)$ et $w = f(z)$.
Puisque f un morphisme de $(E; *)$ dans $(F; \top)$, alors :

$$(u \top v) \top w = (f(x) \top f(y)) \top f(z) = f(x * y) \top f(z) = f[(x * y) * z]$$

Si la loi $*$ est associative dans $(E; *)$, alors :

$$(u \top v) \top w = f[x * (y * z)] = f(x) \top f(y * z) = f(x) \top [f(y) \top f(z)] = u \top (v \top w)$$

Par suite, la loi $\top$ est associative dans $(f(E); \top)$.

3. Supposons que la loi $*$ est commutative dans $(E; *)$. En conservant les notations de 1), on obtient :

$$y_1 \top y_2 = f(x_1) \top f(x_2) = f(x_1 * x_2) = f(x_2 * x_1) = f(x_2) \top f(x_1) = y_2 \top y_1$$

ce qui montre bien que la loi $\top$ est commutative dans $(f(E); \top)$.

4. Soit $u \in f(E)$. Il existe alors $x \in E$ tel que $u = f(x)$. On suppose que la loi $*$ admet un élément neutre e dans $(E; *)$. Il s'ensuit donc : $u \top f(e) = f(x) \top f(e) = f(x * e) = f(x) = u$. On montre de même que $f(e) \top u = u$, ce qui entraîne immédiatement que $f(e)$ est l'élément neutre dans $(f(E); \top)$.
5. Soit x' le symétrique de x dans $(E; *)$. De $x * x' = e$ et $x' * x = e$, ajouté au fait que f un morphisme de $(E; *)$ dans $(F; \top)$, on déduit : $f(x) \top f(x') = f(x * x') = f(e)$ et $f(x') \top f(x) = f(x' * x) = f(e)$. Comme $f(e)$ est un élément neutre dans $(f(E); \top)$, alors $f(x)$ admet un symétrique dans $(f(E); \top)$ qui est $f(x')$.

Corollaire 3.3.1. *Si f un isomorphisme de $(E; *)$ dans $(F; \top)$ (c'est-à-dire morphisme bijectif), alors f transfère les propriétés de la loi $*$ dans $(E; *)$ vers la loi $\top$ de $(F; \top)$, et va ainsi conserver toutes les propriétés liées à cette loi. On exprime ce résultat en disant que $(E; *)$ et $(F; \top)$ ont la même structure.*

Démonstration c'est un morphisme **bijectif**. Par conséquent, pour tout élément $y \in F$, il existe un unique $x \in E$ tel que $y = f(x)$.

- **Associativité** : Soient $u, v, w \in F$. Comme f est surjective, il existe $x, y, z \in E$ tels que $u = f(x)$, $v = f(y)$ et $w = f(z)$.

$$(u \top v) \top w = (f(x) \top f(y)) \top f(z) = f(x * y) \top f(z) = f((x * y) * z)$$

Si $*$ est associative, $(x * y) * z = x * (y * z)$, d'où :

$$(u \top v) \top w = f(x * (y * z)) = f(x) \top f(y * z) = f(x) \top (f(y) \top f(z)) = u \top (v \top w)$$

- **Élément neutre** : Supposons que e soit l'élément neutre de $(E; *)$. Pour tout $u \in F$, soit $x \in E$ tel que $u = f(x)$:

$$u \top f(e) = f(x) \top f(e) = f(x * e) = f(x) = u$$

De même, $f(e) \top u = u$. Ainsi, $f(e)$ est l'unique élément neutre de $(F; \top)$.

- **Élément symétrique** : Soit $u \in F$ et x son antécédent ($u = f(x)$). Si x possède un symétrique x' dans E , alors :

$$u \top f(x') = f(x) \top f(x') = f(x * x') = f(e)$$

Puisque $f(e)$ est le neutre de F , $f(x')$ est le symétrique de u dans $(F; \top)$.

- **Commutativité** : Si $*$ est commutative, pour tous $u, v \in F$ (avec $u = f(x), v = f(y)$) :

$$u \top v = f(x) \top f(y) = f(x * y) = f(y * x) = f(y) \top f(x) = v \top u$$

L'isomorphisme f crée donc une copie conforme de la structure de E sur l'ensemble F .

Exercices d'applications

(Al moufid en maths)

EXO :1

1. Pour tout x et y dans $\mathbb{R} - \{\frac{1}{2}\}$ on pose $x * y = x + y - 2xy$. Montrer que $*$ est une loi de composition interne sur $\mathbb{R} - \{\frac{1}{2}\}$.
2. Sur l'intervalle $I =]-1, 1[$ on définit la relation $\perp$ par :

$$\forall (x, y) \in I^2 : x \perp y = \frac{x + y}{1 + xy}$$

La relation $\perp$ est-elle une loi de composition interne sur I ? Justifier.

EXO :2

1. Étudier la commutativité et l'associativité de la loi de composition interne définie sur $\mathbb{R}$ par

$$(\forall (x, y) \in \mathbb{R}^2) \quad x * y = 2^{xy}$$

2. Étudier la commutativité et l'associativité de la loi de composition interne définie sur $E = \mathbb{Z} \times \mathbb{Z}$ par

$$(a, b) * (x, y) = (ax, ay + bx)$$

3. Étudier la commutativité et l'associativité de la loi de composition interne définie sur $\mathbb{C}$ par :

$$(\forall (z, z') \in \mathbb{C}^2) \quad z * z' = izz' + 2z + (1 + i)z' + 2$$

4. On munit un ensemble E d'une loi de composition interne $*$ telle que

$$(\forall (x, y) \in E^2) : x * (x * y) = (y * x) * x = y$$

Montrer que la loi est commutative.

EXO :3

On munit $\mathbb{R}$ d'une loi de composition interne définie par :

$$(\forall (x, y) \in \mathbb{R}^2) : x * y = x + y + \frac{1}{2}xy$$

1. Montrer que la loi $*$ est associative.
2. Montrer que $*$ admet un élément neutre que l'on déterminera.
3. Déterminer les éléments symétrisables pour la loi $*$.
4. Montrer que le symétrique de -1 est 2 et que le symétrique de 6 est $-\frac{3}{2}$.

EXO :4

On considère l'ensemble $A = \{a + ib \mid (a, b) \in \mathbb{Z}\}$, on considère l'application

$$\phi : A \rightarrow \mathbb{Z}, \quad z = a + ib \mapsto \sqrt{a^2 + b^2}$$

1. Montrer que l'application ϕ est un morphisme de $(A, \cdot)$ dans $(\mathbb{Z}, \cdot)$.
2. Soit $z \in A$, montrer que z admet un symétrique par la loi $\times$ (multiplication dans A) si et seulement si $\phi(z) = 1$.
3. On note B le sous-ensemble de A admettant un symétrique dans $(A, \cdot)$. Déterminer en extension B .

Chapitre 4

Généralités sur les Matrices carrés

4.1 Matrice carrée d'ordre 2

Définition 4.1.1. 1) Une matrice carrée d'ordre 2 à coefficients réels est un tableau de quatre nombres (Il n'y a pas de séparation verticale ou horizontale, contrairement aux tableaux)

2) l'ensemble des matrices carrées d'ordre 2

On le note :

$$M_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} / (a; b; c; d) \in \mathbb{R}^4 \right\}$$

Définition 4.1.2. La somme et la multiplication et l'égalité de deux matrices A et B dans $M_2(\mathbb{R})$ sont définies par :

$$\begin{aligned} \begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} &= \begin{pmatrix} a + a' & b + b' \\ c + c' & d + d' \end{pmatrix} \\ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \times \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} &= \begin{pmatrix} aa' + bc' & ab' + bd' \\ ca' + dc' & cb' + dd' \end{pmatrix} \\ \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} &\iff \begin{cases} a = a' \\ b = b' \\ c = c' \\ d = d' \end{cases} \end{aligned}$$

Remarque 4.1.1. La somme et le produit de deux matrices sont des lois de compositions internes dans $M_2(\mathbb{R})$

on écrit : $(M_2(\mathbb{R}); +)$; $(M_2(\mathbb{R}); \times)$

Proposition 4.1.1 (Déterminant). Pour une matrice carrée d'ordre 2 de la forme :

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

Le ****déterminant**** se calcule avec la formule suivante :

$$\det(A) = (a \times d) - (b \times c)$$

En gros, vous multipliez les éléments de la ****diagonale principale**** et vous soustrayez le produit des éléments de l'autre diagonale.

Exemple 4.1.1.

$$M = \begin{pmatrix} 5 & 2 \\ 3 & 4 \end{pmatrix}$$

****Calcul :****

$$\det(M) = (5 \times 4) - (2 \times 3)$$

$$\det(M) = 20 - 6$$

$$\det(M) = 14$$

Proposition 4.1.2 (inverse). Si le déterminant est différent de zéro, l'inverse A^{-1} est donné par :

$$A^{-1} = \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

Remarque 4.1.2. 1) la matrice : $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ s'appelle la matrice unitaire

Et on a : $A \times I_2 = A \quad \forall A \in M_2(\mathbb{R})$

2) la matrice : $O_2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ s'appelle la matrice nulle

Et on a : $A + O_2 = A \quad \forall A \in M_2(\mathbb{R})$

4.2 Matrice carrée d'ordre 3

Définition 4.2.1. 1) Une matrice carrée d'ordre 3 à coefficients réels est un tableau de 9 nombres

2) l'ensemble des matrices carrées d'ordre 3

On le note : $M_3(\mathbb{R})$, tel que :

$$M_3(\mathbb{R}) = \left\{ \begin{pmatrix} a & d & g \\ b & e & h \\ c & f & i \end{pmatrix} / (a; b; c; d; e; f; g; h; i) \in \mathbb{R}^9 \right\}$$

Définition 4.2.2. La somme et la multiplication de deux matrices A et B dans $M_3(\mathbb{R})$ sont définies par :

$$\begin{pmatrix} a & d & g \\ b & e & h \\ c & f & i \end{pmatrix} + \begin{pmatrix} a' & d' & g' \\ b' & e' & h' \\ c' & f' & i' \end{pmatrix} = \begin{pmatrix} a+a' & d+d' & g+g' \\ b+b' & e+e' & h+h' \\ c+c' & f+f' & i+i' \end{pmatrix}$$

$$\begin{pmatrix} a & d & g \\ b & e & h \\ c & f & i \end{pmatrix} \times \begin{pmatrix} a' & d' & g' \\ b' & e' & h' \\ c' & f' & i' \end{pmatrix} = \begin{pmatrix} a'' & d'' & g'' \\ b'' & e'' & h'' \\ c'' & f'' & i'' \end{pmatrix}$$

Avec : $a'' = aa' + db' + gc'$
 $d'' = ad' + de' + gf'$
 $b'' = ba' + eb' + hc'$
 $e'' = bd' + ee' + hf'$
 $c'' = ca' + fb' + ic'$
 $f'' = cd' + fe' + if'$
 $g'' = ag' + dh' + gi'$
 $h'' = bg' + eh' + hi'$
 $i'' = cg' + fh' + ii'$

Proposition 4.2.1 (Déterminant). Le déterminant d'une matrice carrée d'ordre 3 peut se calculer de deux manières principales :

1. La règle de Sarrus (la plus simple) : Pour une matrice $A = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix}$, on additionne les produits des diagonales descendantes et on soustrait ceux des diagonales montantes :

$$\det(A) = (aei + bfg + cdh) - (ceg + afh + bdi)$$

2. Le développement par rapport à une ligne ou colonne : On choisit une ligne (souvent la première) et on multiplie chaque élément par son ***mineur*** (le déterminant 2×2 restant en supprimant sa ligne et sa colonne), en alternant les signes (+, -, +) :

$$\det(A) = a \begin{vmatrix} e & f \\ h & i \end{vmatrix} - b \begin{vmatrix} d & f \\ g & i \end{vmatrix} + c \begin{vmatrix} d & e \\ g & h \end{vmatrix}$$

Ce qui donne : $\det(A) = a(ei - fh) - b(di - fg) + c(dh - eg)$.

Remarque 4.2.1. Si la matrice contient des zéros, développez toujours par rapport à la ligne ou la colonne qui en possède le plus pour simplifier les calculs.

Proposition 4.2.2 (Inverse). on peut trouver l'inverse d'une matrice carrée d'ordre 3 dans le programme du bac la méthode des puissance : Si on trouve que :

$$A^n = I_3 \quad (\forall n \in \mathbb{N}^*)$$

Alors que :

$$A \times A^{n-1} = I_3$$

$$D'où : A^{-1} = A^{n-1}$$

Remarque 4.2.2. 1) la matrice : $I_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ s'appelle la matrice

unitaire et on a : $A \times I_3 = A \quad \forall A \in M_3(\mathbb{R})$

2) la matrice : $O_3 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$ s'appelle la matrice

nulle et on a : $A + O_3 = A \quad \forall A \in M_3(\mathbb{R})$

Exercices d'applications

(Al moufid en maths)

EXO :1

On considère l'ensemble

$$G = \left\{ \begin{pmatrix} 1 & 0 & 0 \\ a & 1 & 0 \\ b & c & 1 \end{pmatrix} \mid (a, b, c) \in \mathbb{R}^3 \right\}$$

Montrer que G est une partie stable de $(\mathcal{M}_3(\mathbb{R}), \times)$.

EXO :2

On considère l'ensemble :

$$A = \left\{ \begin{pmatrix} \alpha & \beta \\ 0 & \alpha \end{pmatrix} \mid (\alpha, \beta) \in \mathbb{R}^2 \right\}$$

1. Montrer que la multiplication matricielle $(\times)$ est une loi de composition interne sur A .
2. Est-ce que $(A, \times)$ admet un élément neutre ? Justifier.

EXO :3

1. On considère la matrice $A = \begin{pmatrix} 3 & 1 \\ -2 & 0 \end{pmatrix}$. Montrer que $\forall n \in \mathbb{N}$:

$$A^n = \begin{pmatrix} 2^{n+1} - 1 & 2^n - 1 \\ 2 - 2^{n+1} & 2 - 2^n \end{pmatrix}$$

2. Montrer que $\forall n \in \mathbb{N}$: A^n est inversible dans $(\mathcal{M}_2(\mathbb{R}), \times)$ et déterminer son inverse.

EXO :4

On considère l'ensemble

$$H = \left\{ \begin{pmatrix} 2^n & 0 & 2^n \\ 0 & 1 & 0 \\ 2^n & 0 & 2^n \end{pmatrix} \mid n \in \mathbb{Z} \right\}$$

1. Montrer que $H \neq \emptyset$.
2. Montrer que H est stable dans $(\mathcal{M}_3(\mathbb{R}), \times)$.
3. Déterminer l'élément neutre de $(H, \times)$.
4. La loi $\times$ est-elle commutative dans H ?
5. On pose $A = \begin{pmatrix} 2 & 0 & 2 \\ 0 & 1 & 0 \\ 2 & 0 & 2 \end{pmatrix}$. Calculer A^{2017} .

Chapitre 5

Groupes, Anneaux et Corps

5.1 Groupes

5.1.1 Définitions et premiers exemples

Définition 5.1.1. Soit G un ensemble muni d'une loi $*$. On dit que $(G, *)$ est un groupe si :

- i) La loi est associative et possède un élément neutre ($(G, *)$ est un monoïde).
- ii) Tout élément de G possède un symétrique pour la loi $*$.

On note e_G l'élément neutre d'un groupe G et on le note simplement e s'il n'y a pas de confusion. Si la loi est commutative, on dit que le groupe $(G, *)$ est un groupe commutatif (ou abélien).

Exemple 5.1.1. 1. Les ensembles $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ sont des groupes commutatifs.

2. Soit E un ensemble fini de cardinal supérieur ou égal à 3. L'ensemble des bijections de E dans E muni de la loi de composition est un groupe non abélien.

3. Soit $P \subset \mathbb{R}^2$ un polygone régulier à n côtés. L'ensemble des isométries du plan préservant P est un groupe, muni de la loi de composition. Ce groupe s'appelle le groupe diédral et se note D_n .

4. L'ensemble $\mathbb{R}^n$, muni de l'addition vectorielle est un groupe :

$$\forall (x_1, \dots, x_n), (y_1, \dots, y_n) \in \mathbb{R}^n, (x_1, \dots, x_n) + (y_1, \dots, y_n) = (x_1 + y_1, \dots, x_n + y_n)$$

Remarque 5.1.1. Tout élément d'un groupe est régulier.

Exemple 5.1.2. Soit $n \in \mathbb{N}^+$ fixé. Soit $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$ l'ensemble des classes d'équivalence pour la relation de congruence modulo n . On munit cet ensemble d'une structure de groupe additif en définissant une loi de la façon suivante :

$$\bar{a} + \bar{b} = \overline{a + b}$$

Cette définition ne dépend pas des représentants choisis. En effet :

$$\bar{a} + \bar{b} = \overline{a + kn} + \overline{b + k'n} = \overline{a + b + (k + k')n} = \overline{a + b}$$

Définition 5.1.2. Soient $(G, *)$ et $(G', \top)$ deux groupes d'éléments neutres e et e' . On appelle groupe produit de G et G' , que l'on note $G \times G'$, l'ensemble $G \times G'$ muni de la loi produit $\perp$ définie par :

$$\forall (a, b), (a', b') \in G \times G', (a, b) \perp (a', b') = (a * a', b \top b')$$

On montre facilement que la loi est associative d'élément neutre (e, e') . Si (a, b) est un élément de $G \times G'$ alors l'inverse de (a, b) est (a^{-1}, b^{-1}) .

Soit $(G, *)$ un groupe, on définit le groupe G^2 comme étant le groupe produit $G \times G$ et pour un entier $n \geq 3$ on définit le groupe G^n comme étant le groupe produit $G^{n-1} \times G$ (ou $G \times G^{n-1}$).

5.1.2 Sous-groupes

Définition 5.1.3. Une partie H d'un groupe $(G, *)$ est dite un sous-groupe de G si :

- i) H est non vide.
- ii) $(H, *)$ est un groupe.

Exemple 5.1.3. 1. Soit $(G, *)$ un groupe d'élément neutre e . Alors $\{e\}$ et G sont des sous-groupes de G

2. Pour n un entier naturel, l'ensemble $n\mathbb{Z}$ des multiples de n est un sous-groupe de $\mathbb{Z}$

3. L'ensemble $\mathbb{R}^{+*}$ des réels strictement positifs est un sous-groupe du groupe multiplicatif $(\mathbb{R}^*, \times)$

Proposition 5.1.1. Soit $(G, *)$ un groupe et soit H une partie de G . Alors H est un sous-groupe de G si et seulement si

- i) $H \neq \emptyset$
- ii) $\forall x, y \in H, x * y \in H$ (H est stable pour $*$)
- iii) $\forall x \in H, x^{-1} \in H$ (H est stable par passage à l'inverse).

Proposition 5.1.2. Soit $(G, *)$ un groupe et soit H une partie de G . Alors H est un sous-groupe de G si et seulement si :

- i) $H \neq \emptyset$.
- ii) $\forall x, y \in H, x * y^{-1} \in H$.

Démonstration L'implication directe découle de la définition de H en tant que groupe. Montrons la réciproque. Comme H est non vide, il existe $x_0 \in H$. Par le deuxième point, on a $e = x_0 * x_0^{-1} \in H$. Soit maintenant $x \in H$, alors par hypothèse, on obtient $x^{-1} = e * x^{-1} \in H$. Enfin considérons deux éléments x et y de H . On applique encore le deuxième point au couple (x, y^{-1}) et on a $x * y = x * (y^{-1})^{-1} \in H$. Ceci termine la preuve.

Exemple 5.1.4. 1. $(\mathbb{Q}, \times)$ est un sous-groupe de $(\mathbb{R}^*, \times)$.

2. L'ensemble des nombres complexes de module 1 est un sous-groupe de $(\mathbb{C}^*, \times)$.

3. Pour un entier naturel non nul n , l'ensemble $\mathbb{U}_n = \{z \in \mathbb{C}, z^n = 1\}$ des racines n -èmes de l'unité est un sous-groupe de $(\mathbb{C}^*, \times)$.

Proposition 5.1.3. Les sous-groupes de $(\mathbb{Z}, +)$ sont de la forme $n\mathbb{Z}$, avec $n \in \mathbb{N}$.

Démonstration Soit H un sous-groupe de $(\mathbb{Z}, +)$. Si $H = \{0\}$ alors $H = 0\mathbb{Z}$. Supposons que $H \neq \{0\}$ et soit n le plus petit élément de la partie $H \cap \mathbb{N}^*$. On va montrer que $H = n\mathbb{Z}$. Considérons $m \in H$ alors il existe $(q, r) \in (\mathbb{Z} \times \mathbb{N})$ tel que $m = qn + r$ avec $0 \leq r < n$. Il est clair que $r \in H$ et par minimalité de n , on a nécessairement $r = 0$. D'où $H = n\mathbb{Z}$.

Proposition 5.1.4. L'intersection d'une famille quelconque de sous-groupes d'un groupe G est un sous-groupe de G .

Remarque 5.1.2. La réunion de deux sous-groupes d'un groupe n'est pas en général un sous-groupe. On montre que si H et K sont deux sous-groupes d'un groupe G , alors $H \cup K$ est un sous-groupe de G si et seulement si $H \subset K$ ou $K \subset H$.

5.1.3 Homomorphismes de groupes

Définition 5.1.4. Soient $(G, *)$ et $(G', \top)$ deux groupes. Un homomorphisme (ou morphisme) de $(G, *)$ dans $(G', \top)$ est une application f de G dans G' telle que :

$$\forall x, y \in G, \quad f(x * y) = f(x) \top f(y)$$

Si $G = G'$, on parle d'endomorphisme de G . Si f est bijectif, on dit que c'est un isomorphisme de groupes et que G et G' sont isomorphes.

Exemple 5.1.5. 1. Soit $n \in \mathbb{N}$. L'application $\mathbb{Z} \rightarrow n\mathbb{Z}$ définie par $m \mapsto nm$ est un homomorphisme de groupes de $\mathbb{Z}$ dans $n\mathbb{Z}$.

2. L'exponentielle $\exp : \mathbb{R} \rightarrow \mathbb{R}^{+*}$ est un homomorphisme du groupe additif $(\mathbb{R}, +)$ dans le groupe multiplicatif $(\mathbb{R}^{+*}, \times)$.

Proposition 5.1.5. Soit $f : (G, *) \rightarrow (G', \top)$ un isomorphisme de groupes. Alors f^{-1} est aussi un isomorphisme de groupes.

Démonstration. Soit $x', y' \in G'$. On a :

$$f(f^{-1}(x') * f^{-1}(y')) = f(f^{-1}(x')) \top f(f^{-1}(y')) = x' \top y'$$

Ceci montre que $f^{-1}(x' \top y') = f^{-1}(x') * f^{-1}(y')$ et donc f^{-1} est un homomorphisme. D'où f^{-1} est un isomorphisme de groupes.

Dans la suite, on dit que deux groupes G et G' sont isomorphes s'il existe un isomorphisme de G dans G' .

Exemple 5.1.6. 1. Le groupe additif $\mathbb{R}$ est isomorphe au groupe multiplicatif $\mathbb{R}^{+*}$ via l'application exponentielle.

2. Les groupes $\mathbb{Z}/n\mathbb{Z}$ et $U_n = \{e^{\frac{2ik\pi}{n}}, 0 \leq k \leq n-1\}$ sont isomorphes. L'application $\bar{k} \mapsto e^{\frac{2ik\pi}{n}}$ est un isomorphisme de groupes de $\mathbb{Z}/n\mathbb{Z}$ dans U_n .

Notation 5.1.1. Soit $(G, *)$ un groupe d'élément neutre e et soit $g \in G$. On note :

- $g^0 = e$.
- $\forall n \in \mathbb{N}, g^{n+1} = g * g^n$.
- $\forall n \in \mathbb{N}, g^{-n} = (g^n)^{-1}$.

Remarque 5.1.3. Soit g un élément d'un groupe $(G, *)$, alors on a :

- $\forall n, m \in \mathbb{Z}, g^n * g^m = g^{n+m}$.
- $\forall n, m \in \mathbb{Z}, (g^n)^m = g^{nm}$.

Proposition 5.1.6. Soit $f : G \rightarrow G'$ un morphisme de groupes. Alors :

1. $f(e_G) = e_{G'}$.
2. Pour tout g dans G , on a $f(g^{-1}) = (f(g))^{-1}$.
3. Pour tout $n \in \mathbb{Z}$ et tout $g \in G$, on a $f(g^n) = (f(g))^n$.

Démonstration.

1. Soit $g \in G$. On a $f(g) = f(e_G g) = f(e_G) f(g)$ donc $f(e_G) = f(g) f(g)^{-1} = e_{G'}$.
2. Soit $g \in G$. On a $f(g) f(g^{-1}) = f(g g^{-1}) = f(e_G) = e_{G'}$. D'où $f(g^{-1}) = (f(g))^{-1}$.

3. Le cas $n = 0$ correspond au premier point. Pour $n > 0$, on raisonne par récurrence et pour $n < 0$ on utilise le deuxième point.

Proposition 5.1.7. *Soit $f : (G, *) \rightarrow (G', \top)$ un homomorphisme de groupes.*

1. *Si H est un sous-groupe de $(G, *)$ alors $f(H)$ est un sous-groupe de $(G', \top)$.*
2. *Si H' est un sous-groupe de $(G', \top)$ alors $f^{-1}(H')$ est un sous-groupe de $(G, *)$.*

Démonstration.

1. On a $e_G \in H$, donc par la proposition précédente $e_{G'} = f(e_G) \in f(H)$ et $f(H) \neq \emptyset$. Soit $y, y' \in f(H)$, il existe x, x' tels que $y = f(x)$ et $y' = f(x')$. Alors $y \top y'^{-1} = f(x) \top f(x')^{-1} = f(x) \top f(x'^{-1}) = f(x * x'^{-1}) \in f(H)$ car $x * x'^{-1} \in H$. D'où $f(H)$ est un sous-groupe de G' .
2. Comme $f(e_G) = e_{G'} \in H'$ il vient $e_G \in f^{-1}(H')$. Soit $x, x' \in f^{-1}(H')$, alors $f(x) \in H'$ et $f(x') \in H'$. Or H' est un sous-groupe de G' , donc $f(x) \top f(x')^{-1} \in H'$. Mais $f(x) \top f(x')^{-1} = f(x) \top f(x'^{-1}) = f(x * x'^{-1})$, et on a $x * x'^{-1} \in f^{-1}(H')$. Ceci montre que $f^{-1}(H')$ est un sous-groupe de G .

5.2 Anneaux

5.2.1 Distributivité

Définition 5.2.1. *Soit E un ensemble muni de deux lois $*$ et $\top$. On dit que :*

1. *La loi $*$ est distributive à gauche par rapport à la loi $\top$ si : $\forall x, y, z \in E, x * (y \top z) = (x * y) \top (x * z)$.*
2. *La loi $*$ est distributive à droite par rapport à la loi $\top$ si : $\forall x, y, z \in E, (x \top y) * z = (x * z) \top (y * z)$.*
3. *La loi $*$ est distributive par rapport à la loi $\top$ si elle est distributive à gauche et à droite.*

Exemple 5.2.1. 1. Dans $\mathbb{C}$, la multiplication est distributive par rapport à l'addition.

2. Dans $\mathcal{P}(E)$, les deux lois $\cap$ et $\cup$ sont distributives l'une par rapport à l'autre.

5.2.2 Structure d'Anneaux

Définition 5.2.2. Soit A un ensemble muni de deux lois de composition interne $\oplus$ et $\otimes$.

On dit que $(A; \oplus; \otimes)$ est **un anneau** lorsque :

1. $(A; \oplus)$ est un groupe commutatif.
2. La loi $\otimes$ est associative et distributive par rapport à la loi $\oplus$.

On dit que l'anneau $(A; \oplus; \otimes)$ est **commutatif** si la loi $\otimes$ est **commutative**.

On dit que l'anneau $(A; \oplus; \otimes)$ est **unitaire** si la loi $\otimes$ possède un élément neutre pour la loi $\otimes$.

Notation 5.2.1. — Lorsqu'il n'y a pas d'ambiguïté, on note les lois $\oplus$ et $\otimes$ respectivement $+$ (notation additive) et $\times$ (notation multiplicative). Dans le cas habituel :

- ✓ On note 0 (ou 0_A), appelé **le zéro de l'anneau A** , l'élément neutre pour $+$, et
 - ✓ On note 1 (ou 1_A), appelé **l'élément unité de l'anneau A** , l'élément neutre pour $\times$ si A est **unitaire**.
 - ✓ On note couramment $x.y$ ou même xy à la place de $x \times y$.
 - ✓ Le symétrique de $x \in A$ pour l'addition (opposé de x) est noté $-x$.
 - ✓ Le symétrique de $x \in A$ pour la multiplication (inverse de x), **s'il existe**, est noté x^{-1} .
- Soit $(A; +; \times)$ un anneau unitaire. Soient $x \in A$ et $n \in \mathbb{Z}$. On peut définir le symbole nx dans A par :

$$nx = \underbrace{x + x + \cdots + x}_{n \text{ fois}} \text{ si } n \geq 1 \quad ; \quad nx = \underbrace{(-x) + (-x) + \cdots + (-x)}_{-n \text{ fois}} \text{ si } n \leq -1 \quad ;$$

on donne : $0x = 0_A$

De même, on peut définir le symbole x^n dans A par :

$$x^n = \underbrace{x \times x \times \cdots \times x}_{n \text{ fois}} \text{ si } n \geq 1 \quad ; \quad x^n = \underbrace{x^{-1} \times \cdots \times x^{-1}}_{-n \text{ fois}} \text{ si } x \text{ est inversible et } n \leq -1 \quad ;$$

on donne : $x^0 = 1_A$

Ces notations sont très utiles dans les calculs numériques (réels et complexes) et matriciels.

5.2.3 Règles de calcul dans un Anneaux

Proposition 5.2.1. Soit $(A; +; \cdot)$ un anneau unitaire. On a les propriétés suivantes :

1. Pour tout $x \in A : 0_A \cdot x = x \cdot 0_A = 0_A$.
2. Pour tout $x \in A : (-1_A) \cdot x = x \cdot (-1_A) = -x$.
3. Pour tout $(x; y) \in A^2 : (-x) \cdot y = x \cdot (-y) = -(x \cdot y)$.
4. Pour tout $(x; y) \in A^2 : (-x) \cdot (-y) = x \cdot y$.

Démonstration il est évident

Remarque 5.2.1. Soit $a_k, \dots, a_m$ une famille finie d'éléments de A . On pose

$$a_k + \dots + a_m = \sum_{i=k}^m a_i \text{ et } a_k \times \dots \times a_m = \prod_{i=k}^m a_i$$

Lorsque $k > m$, on pose $\sum_{i=k}^m a_i = 0$ et $\prod_{i=k}^m a_i = 1$. Nous avons les égalités suivantes :

1. (hors programme)

$$\left(\sum_{i=k}^m a_i \right) \left(\sum_{j=p}^q b_j \right) = \sum_{i=k}^m a_i \left(\sum_{j=p}^q b_j \right) = \sum_{i=k}^m \sum_{j=p}^q a_i b_j$$

2. Si a et b commutent, on a la formule du binôme de Newton :

$$\forall a, b \in A, \forall n \in \mathbb{N} : (a + b)^n = \sum_{k=0}^n C_n^k a^k b^{n-k},$$

où

$$C_n^k = \frac{n!}{k!(n-k)!}.$$

3. Si a et b commutent, on a :

$$\forall a, b \in A, \forall n \in \mathbb{N}^* : a^n - b^n = (a - b) \left(\sum_{k=0}^{n-1} a^{n-1-k} b^k \right)$$

5.2.4 Diviseurs de zéro dans un Anneaux-Anneaux intègre

Définition 5.2.3. Soit A un anneau. Un élément non nul a de A est dit un diviseur de zéro s'il existe un élément non nul b de A tel que $ab = 0$ ou $ba = 0$.

Remarque 5.2.2. 1. Un diviseur de zéro n'est pas inversible. Il s'ensuit qu'un élément inversible de A n'est pas un diviseur de zéro.

2. Dans l'anneau $(\mathbb{Z}, +, \times)$, l'élément 3 n'est ni inversible ni un diviseur de zéro.

Définition 5.2.4. Un anneau commutatif sans diviseur de zéro s'appelle un anneau commutatif intègre. Autrement dit, un anneau commutatif intègre est un anneau commutatif A dans lequel :

$$\forall a, b \in A, ab = 0 \Rightarrow a = 0 \text{ ou } b = 0$$

Exemple 5.2.2. 1. Les anneaux $(\mathbb{Z}, +, \times)$, $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$ et $(\mathbb{C}, +, \times)$ sont des anneaux intègres.

2. L'anneau $(A \times A, +, \times)$ n'est pas un anneau intègre.

Définition 5.2.5. Soit A un anneau commutatif et soient $a, b \in A$. On dit que a divise b ou que b est un multiple de a s'il existe c dans A tel que $b = ac$.

Définition 5.2.6. Soit A un anneau commutatif.

1. Un élément non nul a de A est dit **irréductible** si a est non inversible et si $a = bc$, avec $b, c \in A$, alors b ou c est inversible.
2. Un élément non nul a de A est dit **premier** si a est non inversible et si a divise bc , avec $b, c \in A$, alors a divise b ou a divise c .

5.3 Corps

les règles de calcul et réflexes acquis dans les anneaux $\mathbb{R}$ et $\mathbb{C}$ y sont valables encore dans les Corps

Définition 5.3.1. On appelle **corps** tout anneau unitaire $(K; +; \cdot)$ non réduit à $\{0_K\}$ tel que tout élément autre que 0_K est inversible pour la loi $\cdot$.

Un corps est dit **commutatif** si sa multiplication $\cdot$ est commutative.

Exemple 5.3.1. 1. $(\mathbb{Q}; +; \times)$, $(\mathbb{R}; +; \times)$ et $(\mathbb{C}; +; \times)$ sont des corps commutatifs, mais $(\mathbb{Z}; +; \times)$ n'est pas un corps car l'élément 2 n'a pas d'inverse pour la loi $\times$ dans $\mathbb{Z}$.

2. Si p est un nombre premier, alors $(\mathbb{Z}/p\mathbb{Z}; +; \times)$ est un corps commutatif. C'est une conséquence du théorème du cours d'arithmétique et du fait que $(\mathbb{Z}/p\mathbb{Z}; +; \times)$ est un anneau commutatif.

3. $(M_2(\mathbb{R}); +; \times)$ n'est pas un corps car la matrice $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ n'a pas d'inverse pour la loi $\times$ dans $M_2(\mathbb{R})$.

4. $(\mathbb{Z}/6\mathbb{Z}; +; \times)$ n'est pas un corps.

Proposition 5.3.1. Soit $(K; +; \cdot)$ un ensemble muni de deux lois de composition interne $+$ et $\cdot$.

Pour que $(K; +; \cdot)$ soit un corps, il faut et il suffit que les trois axiomes suivants soient vérifiés :

1. $(K; +)$ est un groupe commutatif.
2. $(K - \{0_K\}; \cdot)$ est un groupe.
3. La loi $\cdot$ est distributive par rapport à la loi $+$.

Proposition 5.3.2. Soit $(K; +; \cdot)$ un corps. On a alors les propriétés suivantes :

1. Tout élément a de $K - \{0_K\}$ est **régulier** pour l'opération $\cdot$:
Pour tout $(x; y) \in K^2 : a \cdot x = a \cdot y \implies x = y$ et $x \cdot a = y \cdot a \implies x = y$
2. $(K; +; \cdot)$ est un **anneau intègre** :
 $(\forall (x; y) \in K^2) [x \cdot y = 0_K \implies (x = 0_K \text{ ou } y = 0_K)]$
3. Pour tous $a \in K - \{0_K\}$ et $b \in K$, on a :
 $a \cdot x = b \iff x = a^{-1} \cdot b$ et $x \cdot a = b \iff x = b \cdot a^{-1}$

Exercices d'applications

(Al moufid en maths)

EXO : 1

On munit $\mathbb{R}$ d'une loi de composition interne $*$ comme suit :

$$(\forall (x; y) \in \mathbb{R}^2) \quad x * y = x\sqrt{y^2 + 1} + y\sqrt{x^2 + 1}$$

et on considère l'application s définie de $\mathbb{R}$ dans $\mathbb{R}$ par :

$$s(x) = \frac{e^x - e^{-x}}{2}$$

1. Montrer que s est un isomorphisme de $(\mathbb{R}; +)$ dans $(\mathbb{R}; *)$.
2. En déduire la structure de $(\mathbb{R}; *)$ en déterminant son élément neutre et le symétrique de tout élément dans $(\mathbb{R}; *)$.
3. Pour tout $x \in \mathbb{R}$ et pour tout entier $n \geq 2$, on pose :

$$x^{(n)} = \underbrace{x * x * \dots * x}_{n \text{ fois}}$$

Calculer $x^{(n)}$.

EXO : 2

On considère l'ensemble : $\mathbb{Z}[i] = \{a + ib \mid (a; b) \in \mathbb{Z}^2\}$

1. Montrer que $\mathbb{Z}[i]$ est une partie stable de $(\mathbb{C}; +)$ et de $(\mathbb{C}; \times)$.
2. Montrer que $(\mathbb{Z}[i]; +; \times)$ est un anneau commutatif unitaire.
3. Soit $\mathcal{U}$ l'ensemble des éléments inversibles dans $(\mathbb{Z}[i]; \times)$. On pose :

$$(\forall z \in \mathbb{C}) \quad N(z) = z \times \bar{z} = |z|^2$$

- (a) Soit $x \in \mathbb{Z}[i]$. Montrer que : $x \in \mathcal{U} \iff N(x) = 1$
- (b) En déduire que : $\mathcal{U} = \{1; -1; i; -i\}$

EXO : 3

On considère l'ensemble :

$$E = \left\{ M(x; y) = \begin{pmatrix} x & y \\ -y & x + y \end{pmatrix} \mid (x; y) \in \mathbb{R}^2 \right\}$$

1. Montrer que E est une partie stable pour l'addition et la multiplication dans $\mathbb{M}_2(\mathbb{R})$.
2. Montrer que $(E; +; \times)$ est un anneau commutatif.
L'anneau $(E; +; \times)$ est-il intègre ? Justifier.
3. Montrer que $(E; +; \times)$ est un corps commutatif.
4. Résoudre dans E l'équation : $-X^2 + 4X - 3I = 0$

Chapitre 6

Espaces Vectoriel Réels ($\mathbb{K} = \mathbb{R}$)

Dans tout la suite $\mathbb{K}$ désigne un corps commutatif ($\mathbb{K} = \mathbb{R}$)

6.1 Espace vectoriel réel

6.1.1 Loi de composition externe (L.C.E)

Définition 6.1.1. Soit E un ensemble. Une loi de composition interne dans E est une application de $E \times E$ dans E .

Une loi de composition externe est une application de $\mathbb{K} \times E$ dans E .

Exemple 6.1.1. Soit $E = \mathbb{R}^2$. L'application notée $+$, définie de $\mathbb{R}^2 \times \mathbb{R}^2$ vers $\mathbb{R}^2$ par :

$$(x, y) + (z, t) = (x + z, y + t) \quad \forall (x, y), (z, t) \in \mathbb{R}^2$$

$+$ est une loi de composition interne dans $\mathbb{R}^2$.

L'application notée $.$ définie de $\mathbb{R} \times \mathbb{R}^2$ vers $\mathbb{R}^2$ par :

$$\alpha.(x, y) = (\alpha x, \alpha y) \quad \forall (x, y) \in \mathbb{R}^2, \forall \alpha \in \mathbb{R}$$

$.$ est une loi de composition externe sur $\mathbb{R}^2$.

6.1.2 Définition et propriétés d'un espace vectoriel

Définition 6.1.2. On appelle espace vectoriel sur $\mathbb{K}$ (ou $\mathbb{K}$ -espace vectoriel), un ensemble non vide E muni de deux lois :

1. **Une loi de composition interne**, notée $+$, telle que :
 - i) $+$ est associative : $\forall u, v, w \in E \quad (u + v) + w = u + (v + w)$
 - ii) E possède un élément neutre 0_E pour $+$: $\forall v \in E \quad v + 0_E = 0_E + v = v$
 - iii) Tout élément de E admet un symétrique : $\forall v \in E \exists w \in E$ tel que $v + w = w + v = 0_E$
 - iv) $+$ est commutative : $\forall u, v \in E \quad u + v = v + u$

2. Une loi de composition externe notée $\cdot$, telle que :

- i) $\forall \alpha, \beta \in \mathbb{K}, \forall u \in E \quad (\alpha + \beta) \cdot u = \alpha \cdot u + \beta \cdot u$;
- ii) $\forall \alpha \in \mathbb{K}, \forall u, v \in E \quad \alpha \cdot (u + v) = \alpha \cdot u + \alpha \cdot v$;
- iii) $\forall \alpha, \beta \in \mathbb{K}, \forall u \in E \quad \alpha \cdot (\beta \cdot u) = (\alpha\beta) \cdot u$;
- iv) $\forall u \in E \quad 1 \cdot u = u$.

L'espace vectoriel muni de ces deux lois est noté $(E, +, \cdot)$.

Les éléments de E sont appelés des **vecteurs** de E et ceux de $\mathbb{K}$ s'appellent des **scalaires**.

0_E est appelé le vecteur nul de l'espace vectoriel E .

Exemple 6.1.2. 1. L'ensemble des fonctions de $\mathbb{R}$ dans $\mathbb{R}$, $\mathcal{F}(\mathbb{R}, \mathbb{R})$ est un $\mathbb{R}$ -espace vectoriel pour les deux lois :

la loi interne définie par : $(f + g)(x) = f(x) + g(x) \quad \forall f, g \in \mathcal{F}(\mathbb{R}, \mathbb{R})$.

la loi externe définie par : $(\alpha \cdot f)(x) = \alpha f(x) \quad \forall \alpha \in \mathbb{R} \text{ et } \forall f \in \mathcal{F}(\mathbb{R}, \mathbb{R})$.

2. Soit $n \in \mathbb{N}^*$, l'ensemble $\mathbb{K}^n$ est un $\mathbb{K}$ -espace vectoriel pour les deux lois

La loi interne définie par :

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} + \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = \begin{pmatrix} x_1 + y_1 \\ \vdots \\ x_n + y_n \end{pmatrix}.$$

La loi externe définie par :

$$\alpha \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} \alpha x_1 \\ \vdots \\ \alpha x_n \end{pmatrix}.$$

Notation 6.1.1. — En l'absence d'informations sur la nature des éléments de E , un élément de E sera noté généralement $\vec{x}$.

- On utilise l'écriture $\alpha \vec{x}$ au lieu de $\alpha \cdot \vec{x}$ où $\alpha \in \mathbb{R}$ et $\vec{x} \in E$.
- L'élément neutre de $(E, +)$ sera noté $\vec{0}$. C'est le **vecteur nul** de l'espace vectoriel E .
- Si $\alpha \in \mathbb{R}^*$ et $\vec{x} \in E$, on peut « diviser $\vec{x}$ par α » : cela revient à multiplier le vecteur $\vec{x}$ par le scalaire α^{-1} . Ainsi $\frac{1}{\alpha} \vec{x}$ se note aussi $\frac{\vec{x}}{\alpha}$.
- Si $\vec{u}$ et $\vec{v}$ sont deux vecteurs de E , le vecteur $\vec{u} + (-\vec{v})$ s'écrit $\vec{u} - \vec{v}$. Le vecteur $\vec{u} - \vec{v}$ s'appelle la **différence** des vecteurs $\vec{u}$ et $\vec{v}$ dans cet ordre.

- En pratique, les opérations « $+$ » et « $\cdot$ » sont le plus souvent utilisées sans ambiguïté. En conséquence, l'espace vectoriel réel $(E, +, \cdot)$ sera plus simplement noté E , et on dira que E est un $\mathbb{R}$ -espace vectoriel.

Définition 6.1.3. $(E, +, \cdot)$ est un **espace vectoriel réel** (ou $\mathbb{R}$ -espace vectoriel) lorsque :

1. $(E, +)$ est un groupe commutatif.
2. $\forall (\alpha, \beta) \in \mathbb{R}^2, \forall \vec{x} \in E, \quad (\alpha + \beta)\vec{x} = \alpha\vec{x} + \beta\vec{x}.$
3. $\forall \alpha \in \mathbb{R}, \forall (\vec{x}, \vec{y}) \in E^2, \quad \alpha(\vec{x} + \vec{y}) = \alpha\vec{x} + \alpha\vec{y}.$
4. $\forall (\alpha, \beta) \in \mathbb{R}^2, \forall \vec{x} \in E, \quad (\alpha\beta)\vec{x} = \alpha(\beta\vec{x}).$
5. $\forall \vec{x} \in E, \quad 1\vec{x} = \vec{x}.$

Proposition 6.1.1 (Règles de calcul dans un espace vectoriel réel). Les propriétés suivantes se déduisent de la définition d'un $\mathbb{K}$ -espace vectoriel E :

1. Pour tout vecteur v de E , on a $0 \cdot v = 0_E$.
2. Pour tout scalaire α de $\mathbb{K}$, on a $\alpha \cdot 0_E = 0_E$.
3. $\forall \alpha \in \mathbb{K} \quad \forall v \in E \quad (\alpha \cdot v = 0_E \iff \alpha = 0_{\mathbb{K}} \text{ ou } v = 0_E)$
4. $\forall \alpha, \beta \in \mathbb{K} \quad \forall v \in E \quad (\alpha - \beta) \cdot v = \alpha \cdot v - \beta \cdot v$. En particulier $(-1) \cdot v = -v$.
5. $\forall \alpha \in \mathbb{K} \quad \forall v, w \in E \quad \alpha \cdot (v - w) = \alpha \cdot v - \alpha \cdot w$.

6.2 Sous-espace vectoriel

Définition 6.2.1. Étant donné un espace vectoriel réel $(E, +, \cdot)$, une partie F de E est un **sous-espace vectoriel** de E lorsque :

1. $F \neq \emptyset$.
2. F est stable pour l'addition : $(\forall (\vec{x}, \vec{y}) \in F^2) \quad \vec{x} + \vec{y} \in F$.
3. F est stable pour le produit externe : $(\forall (\alpha, \vec{x}) \in \mathbb{R} \times F) \quad \alpha \cdot \vec{x} \in F$.
4. $(F, +, \cdot)$ est un espace vectoriel réel.

Exemple 6.2.1. 1. L'ensemble $\mathbb{P}_n$ ($n \in \mathbb{N}^*$) : ensemble des polynômes de degré inférieur ou égal à n est un sous-espace vectoriel de $\mathcal{F}(\mathbb{R}; \mathbb{R})$.

2. Dans l'espace vectoriel $(\mathcal{F}(\mathbb{R}; \mathbb{R}); +, \cdot)$, l'ensemble F des solutions d'une équation différentielle linéaire de la forme $ay'' + by' + cy = 0$ (avec $(a; b; c) \in \mathbb{R}^3$) est un sous-espace vectoriel de $(\mathcal{F}(\mathbb{R}; \mathbb{R}); +, \cdot)$.

En effet, F n'est pas vide car il contient au moins la fonction nulle. Si deux fonctions f_1 et f_2 sont solutions de l'équation différentielle, il en est de même de la fonction somme $f_1 + f_2$. Enfin, si f_1 est une solution et $a \in \mathbb{R}$, alors la fonction af_1 est solution.

Corollaire 6.2.1. *Une partie F de E est un sous-espace vectoriel de E si et seulement si :*

1. F est non vide,
2. $\forall \alpha \in \mathbb{K} \quad \forall v, w \in F \quad \alpha \cdot v + w \in F$.

Exemple 6.2.2. 1. Le singleton $\{0_E\}$ et E sont des sous-espaces vectoriels de E .

2. L'ensemble des fonctions continues de $\mathbb{R}$ dans $\mathbb{R}$ est un sous-espace vectoriel de $\mathcal{F}(\mathbb{R}, \mathbb{R})$.
3. L'ensemble des polynômes de $\mathbb{K}[X]$ de degré inférieur ou égal à un entier n est un sous-espace vectoriel de $\mathbb{K}[X]$. On le note $\mathbb{K}_n[X]$.

Remarque 6.2.1. — Dans un contexte de sous-espaces vectoriels, on étudie l'appartenance de $\vec{0}$ à F :

- $\vec{0} \in F$ donne $F \neq \emptyset$,
- $\vec{0} \notin F$, alors F n'est pas un sous-espace vectoriel de E .
- Lorsqu'on souhaite montrer qu'un ensemble F est un sous-vectoriel d'un espace vectoriel E , on aura le choix, ou bien d'utiliser la définition ou bien de se ramener à la proposition 3.
- Dans la pratique, pour montrer qu'un ensemble F est un espace vectoriel réel, il peut être beaucoup plus facile de démontrer que c'est un sous-espace vectoriel d'un espace vectoriel réel connu. C'est pour cette raison qu'il faut connaître quelques espaces vectoriels réels les plus familiers, à savoir :

$$(\mathbb{R}, +, \times) ; (\mathbb{C}, +, \cdot) ; (\mathbb{R}^n, +, \cdot) ; (\mathcal{M}_2(\mathbb{R}), +, \cdot) ; (\mathcal{M}_3(\mathbb{R}), +, \cdot) ; (\mathcal{F}(\mathbb{R}, \mathbb{R}), +, \cdot), \dots$$

Remarque 6.2.2. La réunion de deux sous-espaces vectoriels n'est pas en général un sous-espace vectoriel.

6.3 Familles libres- Familles génératrice- Bases

6.3.1 Combinaisons linéaires

Définition 6.3.1. Soit $n \in \mathbb{N}^*$ ainsi que $\vec{x}_1, \vec{x}_2, \dots, \vec{x}_n$ des vecteurs d'un espace vectoriel réel $(E, +, \cdot)$.

On appelle **combinaison linéaire** des vecteurs $\vec{x}_1, \vec{x}_2, \dots, \vec{x}_n$, ou encore combinaison linéaire de la famille $(\vec{x}_1, \vec{x}_2, \dots, \vec{x}_n)$, tout vecteur de la forme :

$$a_1 \vec{x}_1 + a_2 \vec{x}_2 + \dots + a_n \vec{x}_n = \sum_{i=1}^n a_i \vec{x}_i \quad \text{avec} \quad a_1, a_2, \dots, a_n \in \mathbb{R}$$

Les réels $a_1, a_2, \dots, a_n$ sont appelés les **coefficients** de la combinaison linéaire $\sum_{i=1}^n a_i \vec{x}_i$.

Exemple 6.3.1. 1. Les combinaisons linéaires de la famille à un seul élément $(\vec{u})$ sont les vecteurs $a\vec{u}$ où $a \in \mathbb{R}$, celles de la famille à deux éléments $(\vec{u}, \vec{v})$ sont les vecteurs $a\vec{u} + \beta\vec{v}$ où $(a, \beta) \in \mathbb{R}^2$.

2. Dans l'espace vectoriel $(\mathcal{M}_2(\mathbb{R}), +, \cdot)$, on considère les matrices : $M_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ et $M_2 = \begin{pmatrix} 1 & 1 \\ 0 & 4 \end{pmatrix}$. La matrice $M = \begin{pmatrix} 2 & 5 \\ 3 & 8 \end{pmatrix}$ est une combinaison linéaire de M_1 et M_2 car :

$$3M_1 + 2M_2 = 3 \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} + 2 \begin{pmatrix} 1 & 1 \\ 0 & 4 \end{pmatrix} = M$$

3. Dans l'espace vectoriel $(\mathbb{P}_3, +, \cdot)$, on considère les polynômes : $P_0(x) = 1, P_1(x) = x, P_2(x) = x^2, P_3(x) = x^3$. Tout élément $P \in \mathbb{P}_3$ s'écrit $P(x) = ax^3 + bx^2 + cx + d$, soit $P = aP_3 + bP_2 + cP_1 + dP_0$.

4. Dans l'espace vectoriel réel $(\mathbb{C}, +, \times)$, tout $z \in \mathbb{C}$ est combinaison linéaire de 1 et i : $(\forall z \in \mathbb{C})(\exists(a, b) \in \mathbb{R}^2) z = a(1) + b(i)$.

6.3.2 Familles Libres-Familles liées

Définition 6.3.2. Soit E un espace vectoriel réel, $n \in \mathbb{N}^*$ et $(\vec{x}_1, \vec{x}_2, \dots, \vec{x}_n)$ une famille de vecteurs de E .

— On dit que la famille $(\vec{x}_1, \vec{x}_2, \dots, \vec{x}_n)$ est une **famille libre** de E , si :

$$(\forall(a_1, a_2, \dots, a_n) \in \mathbb{R}^n) : \sum_{i=1}^n a_i \vec{x}_i = \vec{0} \implies a_1 = a_2 = \dots = a_n = 0$$

On dit encore dans ce cas-là que les vecteurs $\vec{x}_1, \vec{x}_2, \dots, \vec{x}_n$ sont **linéairement indépendants**.

— On dit que la famille $(\vec{x}_1, \vec{x}_2, \dots, \vec{x}_n)$ est une **famille liée** de E , si elle n'est pas libre. Cela signifie donc qu'il existe une famille $(a_1, a_2, \dots, a_n)$ de réels **non tous nuls** vérifiant $\sum_{i=1}^n a_i \vec{x}_i = \vec{0}$:

On dit encore dans ce cas-là que les vecteurs $\vec{x}_1, \vec{x}_2, \dots, \vec{x}_n$ sont **linéairement dépendants**.

Exemple 6.3.2. 1. La famille (0_E) est liée. Plus généralement, toute famille contenant 0_E est une famille liée.

2. Soient $v_1 = (1, 2, 0)$, $v_2 = (1, 1, 1)$ et $v_3 = (2, 1, -1)$.

Soient $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{R}$ tels que $\alpha_1 v_1 + \alpha_2 v_2 + \alpha_3 v_3 = 0$. Cette relation

nous conduit à la résolution du système linéaire suivant :

$$\begin{cases} \alpha_1 + \alpha_2 + 2\alpha_3 = 0 \\ 2\alpha_1 + \alpha_2 + \alpha_3 = 0 \\ \alpha_2 - \alpha_3 = 0 \end{cases}$$

qui admet l'unique solution $(0, 0, 0)$. Donc les vecteurs v_1, v_2 et v_3 sont linéairement indépendants dans $\mathbb{R}^3$.

3. Soient f_1, f_2 et f_3 trois fonctions de $\mathbb{R}$ dans $\mathbb{R}$ définies comme suit :

$$\forall x \in \mathbb{R} : f_1(x) = \cos^2(x), f_2(x) = \sin(2x), f_3(x) = 1$$

La relation $\cos(2x) = 2\cos^2(x) - 1$ implique que la famille (f_1, f_2, f_3) est une famille liée dans le $\mathbb{R}$ -espace vectoriel $\mathcal{F}(\mathbb{R}, \mathbb{R})$.

Remarque 6.3.1. Dans la pratique, lorsqu'on s'intéresse à la liberté éventuelle d'une famille $(\vec{x}_1, \vec{x}_2, \dots, \vec{x}_n)$, on considère $(a_1, a_2, \dots, a_n) \in \mathbb{R}^n$ tel que :

$$a_1\vec{x}_1 + a_2\vec{x}_2 + \dots + a_n\vec{x}_n = \vec{0}$$

Si cette égalité nous conduit forcément vers $a_1 = a_2 = \dots = a_n = 0$, alors la famille $(\vec{x}_1, \vec{x}_2, \dots, \vec{x}_n)$ est libre. Dans le cas contraire, elle est liée.

Proposition 6.3.1. Soit E un espace vectoriel réel.

1. Une famille $(\vec{x})$ constituée d'un seul vecteur est libre si, et seulement si, $\vec{x} \neq \vec{0}$.
2. Les éléments d'une famille libre sont deux à deux distincts.
3. Si une famille $B = (\vec{x}_1, \vec{x}_2, \dots, \vec{x}_n)$ est libre, alors toute famille contenue dans B est aussi libre.
4. Si une famille $B = (\vec{x}_1, \vec{x}_2, \dots, \vec{x}_n)$ est liée, alors toute famille contenant B est aussi liée.
5. Une famille $B = (\vec{x}_1, \vec{x}_2, \dots, \vec{x}_n)$ est liée si, et seulement si, l'un des vecteurs de B est une combinaison linéaire des $n - 1$ autres.

Démonstration

1. Supposons que la famille $(\vec{x})$ est libre. Si $\vec{x}$ était nul, on aurait $1 \cdot \vec{x} = \vec{0}$ ce qui entraînerait $(\vec{x})$ liée.
Réciproquement, si $\vec{x} \neq \vec{0}$, l'égalité $\alpha\vec{x} = \vec{0}$ entraîne $\alpha = 0$, ce qui prouve la liberté de $(\vec{x})$.

2. Supposons que la famille $B = (\vec{x}_1, \vec{x}_2, \dots, \vec{x}_n)$ contient deux vecteurs égaux. Supposons par exemple que $\vec{x}_1 = \vec{x}_2$. Alors : $\vec{x}_1 - \vec{x}_2 + 0\vec{x}_3 + \dots + 0\vec{x}_n = \vec{0}$, ce qui est en contradiction avec le fait que la famille $B = (\vec{x}_1, \vec{x}_2, \dots, \vec{x}_n)$ est libre. D'où le résultat.
3. Supposons que la famille $B = (\vec{x}_1, \vec{x}_2, \dots, \vec{x}_n)$ est libre. Considérons une sous-famille, par exemple $(\vec{x}_1, \vec{x}_2, \dots, \vec{x}_p)$ et supposons que $\alpha_1\vec{x}_1 + \alpha_2\vec{x}_2 + \dots + \alpha_p\vec{x}_p = \vec{0}$. On peut encore écrire cette égalité :

$$\alpha_1\vec{x}_1 + \alpha_2\vec{x}_2 + \dots + \alpha_p\vec{x}_p + 0\vec{x}_{p+1} + 0\vec{x}_{p+2} + \dots + 0\vec{x}_n = \vec{0}$$

ce qui entraîne la nullité des α_i .

4. Supposons que la famille $B = (\vec{x}_1, \vec{x}_2, \dots, \vec{x}_n)$ est liée. Soit $(\vec{y}_1, \vec{y}_2, \dots, \vec{y}_p) \in E^p$. Si la famille de vecteurs $(\vec{x}_1, \vec{x}_2, \dots, \vec{x}_n, \vec{y}_1, \vec{y}_2, \dots, \vec{y}_p)$ était libre, sa sous-famille $(\vec{x}_1, \vec{x}_2, \dots, \vec{x}_n)$ serait aussi libre d'après 3), ce qui est faux.
5. Supposons que la famille $(\vec{x}_1, \vec{x}_2, \dots, \vec{x}_n)$ est liée. Par définition, il existe $(\alpha_1, \alpha_2, \dots, \alpha_n) \in \mathbb{R}^n \setminus \{(0, 0, \dots, 0)\}$ tel que $\alpha_1\vec{x}_1 + \alpha_2\vec{x}_2 + \dots + \alpha_n\vec{x}_n = \vec{0}$. L'un des α_i est non nul. Supposons qu'il s'agit de α_1 . On peut donc écrire :

$$\vec{x}_1 = - \sum_{k=2}^n \frac{\alpha_k}{\alpha_1} \vec{x}_k$$

ce qui montre que l'un des vecteurs peut s'écrire comme combinaison linéaire des autres.

Réciproquement, supposons que l'un des vecteurs peut s'écrire comme combinaison linéaire des $n - 1$ autres. On a, par exemple $\vec{x}_1 = \sum_{k=2}^n \beta_k \vec{x}_k$, d'où $\vec{x}_1 - \sum_{k=2}^n \beta_k \vec{x}_k = \vec{0}$. Nous avons donc une combinaison linéaire nulle des vecteurs $\vec{x}_1, \vec{x}_2, \dots, \vec{x}_n$ avec au moins un coefficient non nul ($1 \neq 0$), donc la famille est liée.

6.3.3 Familles génératrice

Définition 6.3.3. Soit E un espace vectoriel réel, $n \in \mathbb{N}^*$ et $(\vec{x}_1, \vec{x}_2, \dots, \vec{x}_n)$ une famille de vecteurs de E .

- On dit qu'un vecteur $\vec{x}$ est **engendré** par la famille $(\vec{x}_1, \vec{x}_2, \dots, \vec{x}_n)$ s'il peut s'écrire comme combinaison linéaire des vecteurs de cette famille. Autrement dit :

$$(\exists (\alpha_1, \alpha_2, \dots, \alpha_n) \in \mathbb{R}^n) \quad \vec{x} = \sum_{i=1}^n \alpha_i \vec{x}_i$$

6.3. FAMILLES LIBRES- FAMILLES GÉNÉRATRICE- BASES

— On dit que la famille $(\vec{x}_1, \vec{x}_2, \dots, \vec{x}_n)$ est une **famille génératrice** de E , si :

$$(\forall \vec{x} \in E) (\exists (\alpha_1, \alpha_2, \dots, \alpha_n) \in \mathbb{R}^n) \quad \vec{x} = \sum_{i=1}^n \alpha_i \vec{x}_i$$

On dit encore dans ce cas-là que la famille $(\vec{x}_1, \vec{x}_2, \dots, \vec{x}_n)$ **engendre** l'espace vectoriel E .

Exemple 6.3.3. 1. La famille $(1; i)$ est une famille génératrice de l'espace vectoriel réel $(\mathbb{C}; +; \cdot)$ car tout nombre complexe z peut s'écrire sous la forme $z = a + ib$ avec $(a, b) \in \mathbb{R}^2$.

2. Si $n \in \mathbb{N}^*$, alors la famille des vecteurs $(\vec{e}_1; \vec{e}_2; \dots; \vec{e}_n)$ définie par :

$$\vec{e}_1 = (1; 0; \dots; 0) \quad ; \quad \vec{e}_2 = (0; 1; 0; \dots; 0) \quad ; \quad \vec{e}_3 = (0; 0; 1; 0; \dots; 0) \quad ; \quad \dots \quad ; \quad \vec{e}_n = (0; \dots; 0; 1)$$

est une famille génératrice de l'espace vectoriel réel $(\mathbb{R}^n; +; \cdot)$, puisque, pour tout vecteur $\vec{x} = (x_1, x_2, \dots, x_n) \in \mathbb{R}^n$, on a :

$$\vec{x} = \sum_{i=1}^n x_i \vec{e}_i = x_1 \vec{e}_1 + x_2 \vec{e}_2 + \dots + x_n \vec{e}_n$$

6.3.4 Bases d'un espace vectoriel réel

Définition 6.3.4. Soit E un espace vectoriel réel, $n \in \mathbb{N}^*$ et $B = (\vec{x}_1; \vec{x}_2; \dots; \vec{x}_n)$ une famille de vecteurs de E .

On dit que la famille B est une **base** de E si c'est une famille libre et génératrice de E , ce qui revient à écrire :

$$(\forall \vec{x} \in E) (\exists! (a_1; a_2; \dots; a_n) \in \mathbb{R}^n) \quad \vec{x} = \sum_{i=1}^n a_i \vec{x}_i$$

Dans ces conditions, les nombres $a_1; a_2; \dots; a_n$ s'appellent les **composantes** (ou coordonnées) du vecteur $\vec{x}$ dans la base B , et on écrit $\vec{x}(a_1; \dots; a_n)_{(B)}$ ou tout simplement $\vec{x}(a_1; \dots; a_n)$.

Le réel a_k s'appelle la $k^{\text{ème}}$ **composante** (ou coordonnée) de $\vec{x}$ dans la base B .

Exemple 6.3.4. 1) Posons $E = \mathcal{P}_n$, où $n \in \mathbb{N}^*$. Considérons les polynômes suivants :

$$P_0 : x \mapsto 1 \quad ; \quad P_1 : x \mapsto x \quad ; \quad P_2 : x \mapsto x^2 \quad ; \quad P_3 : x \mapsto x^3 \quad ; \dots \quad ; \quad P_n : x \mapsto x^n$$

6.3. FAMILLES LIBRES- FAMILLES GÉNÉRATRICE- BASES

Montrons que la famille $B = (P_0, P_1, \dots, P_n)$ est une base de l'espace vectoriel réel $\mathcal{P}_n$:

On sait que tout polynôme $P : x \mapsto a_n x^n + \dots + a_1 x + a_0$ est par définition une combinaison linéaire des polynômes $P_0, \dots, P_n$. La famille B est donc génératrice de $\mathcal{P}_n$. Par ailleurs, si $a_n x^n + \dots + a_1 x + a_0 = 0$, alors, par définition d'un polynôme nul, tous les coefficients a_i sont nuls, ce qui montre que B est libre.

Cette famille de polynômes est donc une base, appelée **base canonique** de l'espace vectoriel $\mathcal{P}_n$.

2) La famille $B = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}; \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}; \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}; \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \right\}$ est une base de l'espace vectoriel $(\mathcal{M}_2(\mathbb{R}), +, \cdot)$.

Remarque 6.3.2. — Plaçons-nous dans l'espace vectoriel réel $(\mathbb{R}^n, +, \cdot)$. On a déjà vu que la famille de vecteurs $B = (\vec{e}_1, \vec{e}_2, \dots, \vec{e}_n)$ définie par :

$$\vec{e}_1 = (1, 0, \dots, 0) \quad ; \quad \vec{e}_2 = (0, 1, 0, \dots, 0) \quad ; \quad ; \dots ; \quad \vec{e}_n = (0, \dots, 0, 1)$$

est une famille génératrice de l'espace vectoriel réel. Par ailleurs, si $\alpha_1 \vec{e}_1 + \alpha_2 \vec{e}_2 + \dots + \alpha_n \vec{e}_n = \vec{0}$, alors $(\alpha_1, \alpha_2, \dots, \alpha_n) = (0, 0, \dots, 0)$, d'où $\alpha_1 = \alpha_2 = \dots = \alpha_n = 0$, ce qui montre que la famille B est libre. C'est donc une base, appelée **base canonique** de l'espace vectoriel réel $(\mathbb{R}^n, +, \cdot)$. C'est la base la plus naturelle et la plus simple de $\mathbb{R}^n$.

— Une fois choisie une base $B = (\vec{x}_1, \vec{x}_2, \dots, \vec{x}_n)$ de E , il arrive souvent que l'on identifie chaque vecteur $\vec{x} \in E$ avec le n -uplet de ses composantes. C'est pourquoi, une base doit être une famille (ordonnée) et non un ensemble. Par exemple, si $B = (\vec{e}_1, \vec{e}_2, \vec{e}_3)$ est une base de E , alors le vecteur de composantes $(1, 2, 3)$ dans la base B est $\vec{e}_1 + 2\vec{e}_2 + 3\vec{e}_3$ et non pas $\vec{e}_2 + 2\vec{e}_1 + 3\vec{e}_3$.

Proposition 6.3.2. Soit E un espace vectoriel réel, $n \in \mathbb{N}^*$ et $B = (\vec{x}_1; \vec{x}_2; \dots; \vec{x}_n)$ une base de E . Soit $\vec{x}$ et $\vec{y}$ deux vecteurs de E tels que : $\vec{x}(\alpha_1; \dots; \alpha_n)_{(B)}$ et $\vec{y}(\beta_1; \dots; \beta_n)_{(B)}$. Alors :

$$\vec{x} + \vec{y}(\alpha_1 + \beta_1; \dots; \alpha_n + \beta_n)_{(B)} \quad \text{et} \quad \lambda \vec{x}(\lambda \alpha_1; \dots; \lambda \alpha_n)_{(B)} \quad (\text{où } \lambda \in \mathbb{R})$$

6.3.5 Dimension d'un espace vectoriel

Proposition 6.3.3. Soit E un espace vectoriel réel, $n \in \mathbb{N}^*$ et $B = (\vec{x}_1; \vec{x}_2; \dots; \vec{x}_n)$ une base de E . Alors, toutes les bases de E ont le même cardinal. Ce cardinal est appelé la **dimension** de E et noté $\dim E$, et on écrit $\dim E = n$.

Exemple 6.3.5. 1) Pour tout $n \in \mathbb{N}^*$: $\dim \mathbb{R}^n = n$. En particulier :

- L'espace vectoriel $\mathbb{R}$ est de dimension 1. Il admet pour base (1) et plus généralement toute famille formée d'un unique élément non nul.
- L'espace vectoriel $\mathbb{R}^2$ est de dimension 2. Il admet pour base $B = ((1; 0); (0; 1))$.
- L'espace vectoriel $\mathbb{R}^3$ est de dimension 3. Il admet pour base $B = ((1; 0; 0); (0; 1; 0); (0; 0; 1))$.

Ainsi : $\dim \mathbb{R} = 1$; $\dim \mathbb{R}^2 = 2$; $\dim \mathbb{R}^3 = 3$.

2) L'espace vectoriel réel $(\mathbb{C}; +; \times)$ est de dimension 2 : $\dim \mathbb{C} = 2$.

3) L'espace vectoriel réel $(\mathcal{M}_2(\mathbb{R}); +; \cdot)$ est de dimension 4 : $\dim \mathcal{M}_2(\mathbb{R}) = 4$. Il admet pour base $B = (A_1; A_2; A_3; A_4)$ avec :

$$A_1 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} ; \quad A_2 = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} ; \quad A_3 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} ; \quad A_4 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

Proposition 6.3.4. 1) Soit E un espace vectoriel réel de dimension 2 et $B = (\vec{i}, \vec{j})$ une base de E .

Soit $B' = (\vec{u}; \vec{v})$ une famille de vecteurs de E tels que $\vec{u}(a; b)$ et $\vec{v}(a'; b')$ dans la base B . Alors :

$$(B' \text{ est une base de } E) \Leftrightarrow (B' \text{ est génératrice de } E) \Leftrightarrow (B' \text{ est libre dans } E) \Leftrightarrow \begin{vmatrix} a & a' \\ b & b' \end{vmatrix} \neq 0$$

2) Soit E un espace vectoriel réel de dimension 3 et $B = (\vec{i}, \vec{j}, \vec{k})$ une base de E .

Soit $B' = (\vec{u}; \vec{v}; \vec{w})$ une famille de vecteurs de E tels que $\vec{u}(a; b; c)$ et $\vec{v}(a'; b'; c')$ et $\vec{w}(a''; b''; c'')$ dans la base B . Alors :

$$(B' \text{ est une base de } E) \Leftrightarrow (B' \text{ est génératrice de } E) \Leftrightarrow (B' \text{ est libre dans } E) \Leftrightarrow \begin{vmatrix} a & a' & a'' \\ b & b' & b'' \\ c & c' & c'' \end{vmatrix} \neq 0$$

Exercices d'applications

(Al moufid en maths)

EXO : 1

On considère l'ensemble :

$$E = \{(x; y; z) \in \mathbb{R}^3 \mid x + y + z = 0\}$$

1. Montrer que pour tous $(x; y; z)$ et $(x'; y'; z')$ de E et pour tout $\alpha \in \mathbb{R}$:

$$(x; y; z) + (x'; y'; z') \in E \quad \text{et} \quad \alpha \cdot (x; y; z) \in E$$

2. Montrer que $(E; +; \cdot)$ est un espace vectoriel réel.
3. Montrer qu'il existe deux vecteurs $\vec{u}_1$ et $\vec{u}_2$ de $\mathbb{R}^3$ tels que la famille $(\vec{u}_1; \vec{u}_2)$ engendre l'espace E .

EXO :2

Soit $(U; +; \cdot)$ l'espace vectoriel des suites réelles, les ensembles ci-après sont-ils des sous-espaces vectoriels de U ?

1. L'ensemble U_1 des suites croissantes.
2. L'ensemble U_2 des suites décroissantes.
3. L'ensemble U_3 des suites convergentes.
4. L'ensemble U_4 des suites réelles (u_n) vérifiant $\lim_{n \rightarrow +\infty} u_n = +\infty$.
5. L'ensemble U_5 des suites réelles (u_n) vérifiant la relation de récurrence :

$$(\forall n \in \mathbb{N}) \quad u_{n+2} = 2u_{n+1} - u_n$$

EXO :3

Soit $\mathcal{E}$ l'ensemble des fonctions polynomiales :

$$f : x \mapsto ax^2 + bx + c \text{ telles que : } \int_0^1 x^n f(x) dx = 0$$

où $n \in \mathbb{N}^*$ et $(a; b; c) \in \mathbb{R}^3$.

1. On considère les deux fonctions polynomiales u et v définies par :

$$u(x) = x - \frac{n+1}{n+2} \quad \text{et} \quad v(x) = x^2 - \frac{n+1}{n+3}$$

- (a) Montrer que la famille $(u; v)$ est libre dans l'espace vectoriel réel $(\mathcal{F}(\mathbb{R}, \mathbb{R}); +; \cdot)$.
- (b) Montrer que :

$$(\forall f \in \mathcal{E})(\exists(\alpha; \beta) \in \mathbb{R}^2) \quad f = \alpha u + \beta v$$

- (c) Montrer que $(\mathcal{E}; +; \cdot)$ est un espace vectoriel réel de dimension 2.

EXO : 4

Soit $n \in \mathbb{N}^*$ et $\alpha \in \mathbb{R}^*$. On désigne par $\mathcal{P}_n$ l'ensemble des polynômes de degré inférieur ou égal à n .

On pose pour tout $x \in \mathbb{R}$:

$$P_k(x) = x^k \quad \text{et} \quad Q_k(x) = (x - \alpha)^k \quad \text{avec } k \in \{0; 1; \dots; n\}$$

1. Montrer que $(\mathcal{P}_n; +; \cdot)$ est un espace vectoriel réel.
2. Montrer que la famille $(P_0; P_1; \dots; P_n)$ est une base de l'espace vectoriel réel $(\mathcal{P}_n; +; \cdot)$.
3. (a) Montrer que pour tout $k \in \{0; 1; \dots; n\}$:

$$P_k = \sum_{i=0}^k C_k^i \alpha^{k-i} Q_i$$

- (b) En déduire que la famille $B' = (Q_0; Q_1; \dots; Q_n)$ est une base de l'espace vectoriel réel $(\mathcal{P}_n; +; \cdot)$.
4. Pour tout $k \in \{0; 1; \dots; n\}$, on considère la fonction numérique G_k définie sur $\mathbb{R}$ par :

$$\begin{cases} G_k(x) = \frac{1}{x} \int_x^{2x} P_k(t) dt & \text{si } x \in \mathbb{R}^* \\ G_k(0) = 0 \end{cases}$$

- (a) Montrer que pour tout $k \in \{0; 1; \dots; n\}$: $G_k \in \mathcal{P}_n$.
 - (b) Pour tout $k \in \{0; 1; \dots; n\}$, déterminer les coordonnées de G_k dans la base B' .

Bibliographie

- [1] David Delaunay. Cours Mathématiques MPSI 2005
- [2] Nicolas Basbois . Algèbre MPSI 2015
- [3] Hicham Ajana, Ahmed Sani et Abderrahman Agourram .Al Moufid en mathématique tome 2 Algèbre et Géométrie 2Bac SM A et B . Dar Attakafa 2022
- [4] Brahim Sadik .Polycopie d'Algèbre 2 filière MI FSSM 2025/2026
- [5] Claude Deschamps, André Warusfel.Mathématiques tout-en-un MPSI (édition Dunod,17 juin 2015)
- [6] Daniel Guinin et E. Ladame . Tout-en-un Mathématiques MPSI (édition Bréal, 16 août 2013)
- [7] Alain Bouvier et Michel George.Dictionnaire des mathématiques (édition 21 février 2013)
- [8] Elisabeth Beauvois et Joël Berhouet.Math'X Tle S spécifique (édition 2016)
- [9] Agnès Choquer et Boris Hanouch.Maths Repères Tle S spécifique (édition 2012)
- [10] Guillaume Connan.Visa pour la prépa 2016-2017 - MPSI-PCSI-PTSI-BCPST-ECS (6 mai 2009)
- [11] François Liret.Arithmétique dans $\mathbb{Z}$ et dans $K(X)$ Cours Complet avec Exercices (7 juin 2016)