

UNIVERSITÉ DE LOMÉ

Support du cours en ligne de M. MAGNANI

MATH 102

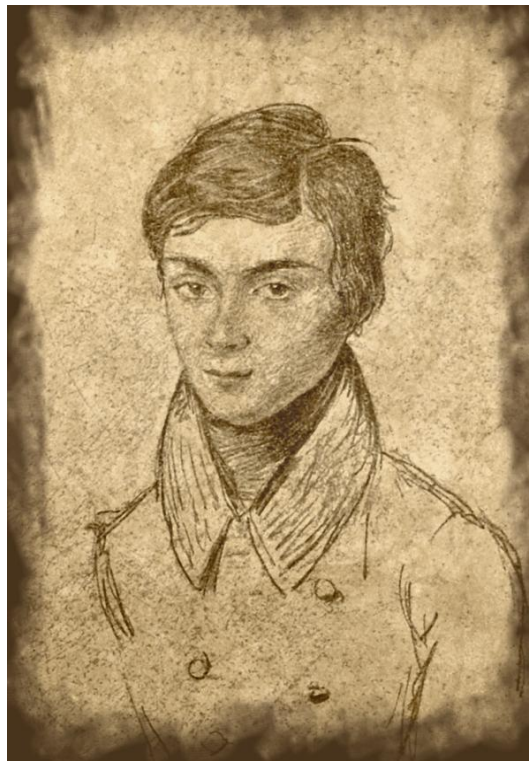
Structures Algébriques

Auteur :

Visseho TCHROKO

Superviseur :

Akoété M. Gildas SOSOE



18 août 2020

Sommaire

1	Introduction	2
2	LES POLYNOMES.	3
3	FRACTIONS RATIONNELLES	12
4	THEORIE DES GROUPES.	21
4.1	Motivation	21
5	Définition :	22
6	La condition pour qu'une loi de composition interne soit associative.	25
7	La condition pour qu'une loi de composition interne soit commutative.	25
8	A quelle condition pouvons-nous dire qu'un ensemble munit d'une loi de composition interne admet un élément neutre	25
9	A quelles conditions pouvons-nous affirmer qu'un ensemble munit d'une loi de composition interne est un groupe ou a une structure de groupe ?	29
9.1	Procédure	29
10	Notion de translation à gauche et à droite.	33
11	Notion de sous-groupe.	33
12	Notion de sous groupe engendré par une partie	34
13	Le centre d'un groupe	34
14	Notion de l'ordre d'un groupe fini	35
15	Le morphisme de groupe et ses propriétés	36
15.1	Définition :	36
16	Extrait des exercices corrigés	37
17	pdf-UL3 les séries d'exercice	37
18	Notion de groupes quotients	38
18.1	Définition	38
19	A quelles conditions peut-on dire qu'un groupe est distingué	38
19.1	Propositions	38
20	Théorème de LAGRANGE	44
21	Etude d'un groupe particulier :groupe des permutation S_n (groupe symétrique)	44

1 Introduction

Dans la vie de tous les jours, lorsque l'on pense à une structure, on pense (parfois) à l'élément sous-jacent d'un objet concret. Par exemple, la structure d'une maison, d'un immeuble ou encore d'une voiture. Cependant, il est possible de considérer la structure à un niveau plus abstrait, par exemple la structure d'un récit ou d'une composition musicale. Toutes ces structures peuvent être composées elles-mêmes de plus petites structures.

En mathématiques, l'idée derrière la notion de structure n'est pas différente de celle que l'on se fait dans le monde réel. Une structure mathématique n'est rien de plus qu'une organisation (potentiellement complexe) de structures plus fondamentales. Formellement, les structures désignent une extension à la théorie des ensembles.

Alors que cette dernière limite ses primitives à la notion d'ensemble (d'éléments) et d'appartenance, une structure propose plus de contraintes, par exemple, la présence d'axiomes, de signes et de règles. Ce sont ces contraintes complémentaires qui permettent de définir de nouvelles structures.

2 LES POLYNOMES.

Support : Fiche cours *ASINSA 1* polynôme.pdf¹

Exemple :

Déterminer le degré et la valuation des polynômes P et Q suivantes : $P = (0, 0, 1, -1, 0, 2, 0, \dots)$
 $Q = (-1, 0, 1, 0, 3, 4, 0, -1, 0, \dots)$

Solution :

$$\text{val}(P) = 2 \qquad \text{deg}(P) = 5$$

$$\text{val}(Q) = 0 \qquad \text{deg}(Q) = 7$$

Les fonctions polynômes associées sont :

$$P(x) = x^2 - x^3 + 2x^5$$

$$Q(x) = -1 + x^2 + 3x^4 + 4x^5 - x^7$$

Rappel :

C'est quoi le degré et la valuation d'un polynôme ?

Soit P un polynôme non nul.

Valuation : C'est le plus petit entier n tel que $a_n \neq 0$.

Degré : C'est le plus grand entier n tel que $a_n \neq 0$.

Division euclidienne.

Exemple :

Effectuer la division euclidienne de $Q(x)$ par $P(x)$.

Solution :

Effectuons la division euclidienne de $P(x) = -x^7 + 4x^5 + 3x^4 + x^2 - 1$ par $Q(x) = 2x^5 - x^3 + x^2$.

1. Presque tout le monde à le support

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

D'après la division euclidienne de $Q(x)$ par $P(x)$ on a :

- le reste : $\frac{7}{2}x^4 + \frac{7}{4}x^3 - \frac{3}{4}x^2 - 1$
- le quotient : $-\frac{1}{2}x^2 + \frac{7}{4}$

Division selon les puissances croissantes.

Quand on parle de division euclidienne c'est une division suivant les puissances décroissantes donc *la division euclidienne est une division suivant les puissances décroissantes et c'est elle que nous avons toujours connus*. Au niveau du transparent n° 27² on a la division selon les puissances croissantes.

Pour que cette division soit possible il faudrait que la **valuation du diviseur soit égale à 0**, autrement dit **le diviseur doit avoir une constante dans l'expression** et donc on effectue la division dans l'ordre croissant.

Exemple :

Effectuer la division selon les puissances croissantes de P par Q à l'ordre 3 ($k = 3$) définies par :

$$P(x) = 2x^3 - x^2 + x$$

$$Q(x) = x^2 + 1$$

Dans cette division, aussi longtemps qu'on continue la division il y aura toujours un résultat c'est-à-dire il y aura toujours un quotient et pas d'arrêt.

dans ce type de division il est important de préciser l'ordre (c'est-à-dire à quel ordre s'arrêter) c'est l'essentiel.

Méthode :

1. L'ordre auquel il faut faire la division selon les puissances croissantes est **le degré du quotient**, donc si on demande de faire la division selon les puissances croissantes à l'ordre k il faut comprendre qu'on s'arrête lorsque le quotient est de degré k .
2. Pour déterminer le R_k donc le reste il faudrait mettre dans le reste trouver x^{k+1} en facteur et donc ce qui reste est le R_k .

Donc essayer de trouver dans notre cas le R_k .

Solution :

Effectuons la division de P par Q à l'ordre 3 suivant les puissances croissantes :

$$\begin{array}{r|l} \begin{array}{r} x \quad -x^2 \quad +2x^3 \\ -(x \quad +x^3) \\ \hline -x^2 \quad +x^3 \\ -(-x^2 \quad -x^4) \\ \hline x^3 \quad +x^4 \\ -(x^3 \quad +x^5) \\ \hline x^4 \quad -x^5 \end{array} & \begin{array}{l} 1+x^2 \\ x-x^2+x^3 \end{array} \end{array}$$

Ainsi donc on a :

- le quotient est : $Q_3 = x^3 - x^2 + x$
- le reste est :

$$\begin{aligned} x^{3+1}R_3 &= x^4 - x^5 \\ R_3 &= x^4(1 - x) \\ R_3 &= 1 - x \end{aligned}$$

Ainsi le x^{k+1} **dans notre cas est** x^{3+1} .
MTH 103³

— Quelles sont les relations qui existent entre les zéros et les coefficients d'un polynôme ?

1. Le zéro d'un polynôme est la valeur qui annule le polynôme.
2. L'ordre de multiplicité est le nombre de fois que le zéro apparaît dans l'annulation du polynôme.

Developper,réduire et ordonner les polynôme suivants :

$$\begin{aligned} P(x) &= (x - x_1)(x - x_2) \\ Q(x) &= (x - x_1)(x - x_2)(x - x_3) \\ K(x) &= (x - x_1)(x - x_2)(x - x_3)(x - x_4) \end{aligned}$$

Résolution :

Developpons,réduisons et ordonnons les polynômes suivants :

$$\begin{aligned} P(x) &= x^2 - (x_1 + x_2)x + x_1x_2 \\ Q(x) &= x^3 - (x_1 + x_2 + x_3)x^2 + (x_1x_2 + x_1x_3 + x_2x_3)x - x_1x_2x_3 \\ K(x) &= x^4 - (x_1 + x_2 + x_3 + x_4)x^3 - (x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4)x^2 - (x_1x_2x_3 + x_1x_2x_4 + x_2x_3x_4 + x_1x_3x_4)x + x_1x_2x_3x_4 \end{aligned}$$

Relation entre coefficients et racines d'un polynôme.

Consulter *le transparent 52* pour cerner la relation entre coefficients et racines d'un polynôme .Sur ce transparent on voit à l'exemple 6.3 où un polynôme a été factorisé et on a écrit les

3. Pour la dérivation des polynômes

relations qui existent entre le polynôme et les coefficients de ce polynôme.

De même dans notre cas pour les polynômes P , Q , et K que nous avons précédemment développer, réduire et ordonner on voit clairement que chacun de ces polynômes a pour coefficient une combinaison des zéros de chaque polynôme, ainsi on voit que les coefficients en x , x^2 , x^3 et x^4 sont des expressions en fonction des x_1 , x_2 , x_3 , et x_4 donc on voit là clairement la relation qui existe entre les coefficients d'un polynôme et les zéros de ce polynôme bien attendu il faudrait que ce polynôme soit scindé, autrement dit ce polynôme admet exactement le nombre de zéro que son degré.

Ainsi donc ce que nous avons obtenu dans nos polynômes P , Q , et K sont des relations d'ordre 2, 3 et 4.

✓ Transparent 53.

Plus généralement, si P est un polynôme scindé de degré n alors il y a n formules reliant les coefficients et les racines de P .

Elles s'écrivent :

$\forall k \in \{1, 2, \dots, n\}$ on a :

$$\sum_{1 \leq i_1 < i_2 < \dots < i_k \leq n} \alpha_{i_1} \alpha_{i_2} \dots \alpha_{i_k} = (-1)^k \frac{a_{n-k}}{a_n}.$$

Chacune d'elles fait apparaître la somme des produits de k racines parmi les n racines de P .

■ Cette somme contient donc autant de termes et de parties à k éléments parmi n éléments.

■ Elle comporte ainsi $\binom{n}{k}$ termes et chacun des termes est constitué d'un produit de k racines.

En particulier lorsque $k = 1$ et $k = n$, on a :

$$\sum_{i=1}^n \alpha_i = -\frac{a_{n-1}}{a_n} \quad \text{et} \quad \prod_{i=1}^n \alpha_i = (-1)^n \frac{a_0}{a_n}$$

Commentaire de M.MAGNANI

D'après le **transparent 53** on voit clairement que la sommation s'effectue par rapport à la longueur des zéros multipliés, autrement dit on regroupe toutes les sommes des produits un par un, deux par deux, trois par trois, quatre par quatre, jusqu'à toutes les sommes de longueur k , autrement dit si on a n zéros et on veut les regrouper deux par deux, donc toutes les sommes, toutes les façons, toutes les combinaisons deux par deux qu'on devrait avoir donc on les sommes, **elles toutes donne quoi comme valeur** et donc si le regroupement se fait de longueur k , autrement dit si on regroupe les zéros par groupe de k distinct bien-sûr donc on aura toutes ces sommes égale à $(-1)^k \times \frac{a_{n-k}}{a_n}$.

Ainsi, le nombre de terme, lorsqu'on voudrait regrouper en k élément **n'est rien d'autre que la combinaison de $\binom{n}{k}$ c'est-à-dire le nombre de partie de k élément qu'on peut avoir dans un ensemble de n élément.**

Donc, il est clair que si on regarde nos polynômes P , Q et K c'est ce qui a été trouvé et donc pour $k = 1$ on a :

$$(-1)^1 = -1 \times \frac{a_{n-1}}{a_n}$$

Et pour $k = n$ on a :

$$(-1)^n = (-1)^n \times \frac{a_0}{a_n}, \text{ donc tous les produits des zéros puisqu'ils sont au nombre de } n.$$

Pour voir ce qui se passe, **les relations qui peuvent exister à l'ordre 3 et 4**, pour avoir une idée essayons de regarder le **transparent 54** où les relations entre les coefficients et les zéros du polynôme ont été établis.

Exercice 2(6 pts)

Soient x_1, x_2, x_3 les racines de $X^3 - 2X^2 + X + 3$, un polynôme de $\mathbb{C}[X]$.

1. Calculer $x_1^2 + x_2^2 + x_3^2$ puis $x_1^3 + x_2^3 + x_3^3$.
2. Déterminer un polynôme du troisième degré dont les trois racines sont x_1^2, x_2^2 et x_3^2

Résolution de l'Exo 2

1. Calculons $x_1^2 + x_2^2 + x_3^2$ puis $x_1^3 + x_2^3 + x_3^3$.

$$\begin{aligned}x_1^2 + x_2^2 + x_3^2 &= (x_1 + x_2 + x_3)^2 - 2(x_1x_2 + x_2x_3 + x_1x_3) \\&= -\left(\frac{a_2}{a_3}\right)^2 - 2\left(\frac{a_1}{a_3}\right)\end{aligned}$$

$$\text{Or } P(x) = x^3 - 2x^2 + x + 3$$

$$\text{Donc } x_1^2 + x_2^2 + x_3^2 = 4 - 2 = 2$$

Ainsi on a : $\boxed{x_1^2 + x_2^2 + x_3^2 = 2}$

- Calculons la deuxième somme.

On sait que $P(x_1) = 0, P(x_2) = 0$ et $P(x_3) = 0$

Donc on a :

$$\left\{ \begin{array}{l} x_1^3 - 2x_1^2 + x_1 + 3 = 0 \\ x_2^3 - 2x_2^2 + x_2 + 3 = 0 \\ x_3^3 - 2x_3^2 + x_3 + 3 = 0 \end{array} \right. \quad \frac{}{x_1^3 + x_2^3 + x_3^3 - 2(x_1^2 + x_2^2 + x_3^2) + (x_1 + x_2 + x_3) + 9 = 0}$$

$$\begin{aligned}\Rightarrow x_1^3 + x_2^3 + x_3^3 &= 2(x_1^2 + x_2^2 + x_3^2) - (x_1 + x_2 + x_3) - 9 \\&= 2 \times 2 - 2 - 9 \\&= -7\end{aligned}$$

Ainsi on a : $\boxed{x_1^3 + x_2^3 + x_3^3 = -7}$

- Réponse : 2

Astuce donné par M.MAGNANI :

Notre polynôme de degré 3 est de la forme $Q(x) = a_3x^3 + a_2x^2 + a_1x + a_0$ avec pour solution x_1^2, x_2^2, x_3^2 .

Les équations de la formule de Viète nous donnent le système suivant :

$$\left\{ \begin{array}{l} x_1^2 + x_2^2 + x_3^2 = -\frac{a_2}{a_3} \\ x_1^2x_2^2 + x_1^2x_3^2 + x_2^2x_3^2 = \frac{a_1}{a_3} \\ x_1^2x_2^2x_3^2 = -\frac{a_0}{a_3} \end{array} \right.$$

Il nous faut déterminer donc a_0, a_1, a_2 et a_3 pour connaître $Q(x)$.

Il faut se rappeler que x_1, x_2 et x_3 sont les racines du polynôme $P(x) = x^3 - 2x^2 + x + 3$.

$x_1^2 + x_2^2 + x_3^2 = 2 = -\frac{a_2}{a_3} \Rightarrow \boxed{a_2 = -2a_3}$
 $x_1^2x_2^2 + x_1^2x_3^2 + x_2^2x_3^2 = (x_1x_2)^2 + (x_1x_3)^2 + (x_2x_3)^2$
 Avec $(x_1x_2)^2 = \alpha$, $(x_1x_3)^2 = \beta$, $(x_2x_3)^2 = \gamma$
 Or on sait bien que

$$\begin{aligned}
 \alpha^2 + \beta^2 + \gamma^2 &= (\alpha + \beta + \gamma)^2 - 2(\alpha\beta + \alpha\gamma + \gamma\beta) \\
 &= (x_1x_2 + x_1x_3 + x_2x_3)^2 - 2(x_1^2x_2x_3 + x_2^2x_1x_3 + x_3^2x_1x_2) \\
 &= 1^2 - 2x_1x_2x_3(x_1 + x_2 + x_3) \\
 &= 1 - 2(-3)(2) \\
 &= 13
 \end{aligned}$$

Ainsi donc on a : $x_1^2x_2^2 + x_1^2x_3^2 + x_2^2x_3^2 = 13$

$$13 = -\frac{a_1}{a_3} \Rightarrow \boxed{a_1 = 13a_3}$$

De plus


$$\begin{aligned}
 x_1^2x_2^2x_3^2 &= (x_1x_2x_3)^2 \\
 &= (-3)^2 \\
 &= 9
 \end{aligned}$$

Ainsi on a :

$$9 = -\frac{a_0}{a_3} \Rightarrow \boxed{a_0 = -9a_3}$$

d'où $Q(x) = a_3(x^3 - 2x^2 + 13x - 9)$ avec $a_3 \in \mathbb{R}^*$.

Td polyôme

les Td seront corrigé mais pas tous les autres exercices seront corrigé mais à part pas dans ce document. 

L'extrait des exercices corrigés.

- 13 • Soit $n \in \mathbb{N}^*$, montrer que le polynôme $nX^{n+2} - (n+2)X^{n+1} + (n+2)X - n$ est divisible par $(X-1)^3$ dans $\mathbb{R}[X]$.
- 14 • Soient x_1, x_2, x_3, x_4 les racines de $P = X^4 + pX^2 + qX + r$ avec $r \neq 0$. Calculer $u = \frac{1}{x_1} + \frac{1}{x_2} + \frac{1}{x_3} + \frac{1}{x_4}$ et $v = \frac{1}{x_1^2} + \frac{1}{x_2^2} + \frac{1}{x_3^2} + \frac{1}{x_4^2}$ en fonction de p, q , et r en utilisant la formule de Viète.
- 15 • On considère $P \in \mathbb{R}[X]$ défini par : $P = X^4 - 2\cos(2\alpha)X^2 + 1$, avec $\alpha \in \mathbb{R}$.
On rappelle que $\cos k\pi = (-1)^k, k \in \mathbb{Z}$.
 - (a) Déterminer les racines de P dans l'ensemble des nombres complexes \mathbb{C} . En déduire la décomposition en produits de polynômes irréductibles de $\mathbb{C}[X]$.
 - (b) Résoudre dans \mathbb{R} l'équation $\sin(2\theta) = 0$.
 - (c) Donner la décomposition de P en produits de polynômes irréductibles de $\mathbb{R}[X]$ (On pourra distinguer les cas où le discriminant $\Delta < 0$, $\Delta = 0$ et discuter suivant les valeurs de α .)

Résolution :

- 13 • Il s'agit de montrer que 1 annule le polynôme. Il annule **sa dérivée première** et **sa dérivée seconde**, étant donné que **l'ordre de multiplicité de 1 est égal à 3**, donc il faudrait vérifier que le polynôme, sa dérivée première et sa dérivée seconde s'annulent en 1. Donc c'est ce qu'il fallait faire.

14 • $P = x^4 + px^2 + qx + r$

$$u = \frac{1}{x_1} + \frac{1}{x_2} + \frac{1}{x_3} + \frac{1}{x_4}$$

$$= \frac{x_2x_3x_4 + x_1x_3x_4 + x_1x_2x_4 + x_1x_2x_3}{x_1x_2x_3x_4}$$

$$u = -\frac{q}{r}$$

$$v = \frac{1}{x_1^2} + \frac{1}{x_2^2} + \frac{1}{x_3^2} + \frac{1}{x_4^2}$$

On sait que :

$$(a + b + c + d)^2 = a^2 + b^2 + c^2 + d^2 + 2(ab + ac + ad + bc + bd + cd)$$

donc

$$\left(\frac{1}{x_1} + \frac{1}{x_2} + \frac{1}{x_3} + \frac{1}{x_4}\right)^2 = v + 2\left(\frac{1}{x_1x_2} + \frac{1}{x_1x_3} + \frac{1}{x_1x_4} + \frac{1}{x_2x_3} + \frac{1}{x_2x_4} + \frac{1}{x_3x_4}\right)$$

$$u^2 = v + 2\frac{x_3x_4 + x_2x_4 + x_2x_3 + x_1x_4 + x_1x_3 + x_1x_2}{x_1x_2x_3x_4}$$

$$= v + 2\frac{p}{r}$$

$$\Rightarrow v = u^2 - \frac{p}{r}$$

$$= \frac{q^2}{r^2} - \frac{2p}{r}$$

$$v = \frac{q^2 - 2pr}{r^2}$$

15 •

- (a) Déterminons les racines P dans l'ensemble des nombres complexes. Puis en déduisons la décomposition en produits de polynômes irréductibles de \mathbb{C} .

$$P = X^4 - 2\cos(2\alpha)X^2 + 1$$

• Changement de variable

$$X^2 - 2\cos(2\alpha)X + 1 = 0$$

$$\Delta = 4\cos^2 2\alpha - 4$$

$$= 4i^2 \sin^2 2\alpha$$

$$X_1 = \cos 2\alpha + i \sin 2\alpha$$

$$= e^{2i\alpha}$$

$$X_2 = \cos 2\alpha - i \sin 2\alpha$$

$$= e^{-2i\alpha}$$

$$x^2 = e^{i2\alpha} \quad x = e^{i\alpha} \text{ ou } -e^{i\alpha}$$

$$x^2 = e^{-i2\alpha} \quad x = e^{-i\alpha} \text{ ou } -e^{-i\alpha}$$

$$S = \{e^{i\alpha}, e^{-i\alpha}, -e^{i\alpha}, -e^{-i\alpha}\}$$

$$\boxed{P = (x - e^{i\alpha})(x + e^{i\alpha})(x - e^{-i\alpha})(x + e^{-i\alpha})}$$

- (b) Résolvons dans \mathbb{R} l'équation $\sin(2\theta) = 0$.

$$P = X^4 - 2 \cos(2\alpha)X^2 + 1$$

- Changement de variable

$$X^2 - 2 \cos(2\alpha)X + 1 = 0$$

$$\Delta = 4 \cos^2 2\alpha - 4$$

$$= 4i^2 \sin^2 2\alpha$$

$$X_1 = \cos 2\alpha + i \sin 2\alpha$$

$$= e^{2i\alpha}$$

$$X_2 = \cos 2\alpha - i \sin 2\alpha$$

$$= e^{-2i\alpha}$$



$$x^2 = e^{i2\alpha} \quad x = e^{i\alpha} \text{ ou } -e^{i\alpha}$$

$$x^2 = e^{-i2\alpha} \quad x = e^{-i\alpha} \text{ ou } -e^{-i\alpha}$$

$$S = \{e^{i\alpha}, e^{-i\alpha}, -e^{i\alpha}, -e^{-i\alpha}\}$$

$$P = (x - e^{i\alpha})(x + e^{i\alpha})(x - e^{-i\alpha})(x + e^{-i\alpha})$$

$$\sin 2\theta = 0 \quad \Rightarrow 2\theta = k\pi \quad k \in \mathbb{Z}$$

$$\Rightarrow \theta = k\frac{\pi}{2}, \quad k \in \mathbb{Z}.$$

$$S = \{k\frac{\pi}{2}, \quad k \in \mathbb{Z}\}$$

- (c) Donnons la décomposition de P en produits de polynômes irréductibles de $\mathbb{R}[X]$.

$$\Delta = -4 \sin^2 2\alpha$$

$$\Delta = 0 \Rightarrow \sin 2\alpha = 0$$

$$\Rightarrow \alpha = k\frac{\pi}{2}, \quad k \in \mathbb{Z}$$

$$P = x^4 - 2 \cos k\pi x^2 + 1$$

$$\text{Or} \quad \cos k\pi = (-1)^k$$

$$P = x^4 - 2(-1)^k x^2 + 1$$

$$* \quad k \text{ pair} :$$

$$P = x^4 - 2x^2 + 1$$

$$= (x^2 - 1)^2$$

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

$$\text{d'où} \quad P = (x+1)^2(x-1)^2$$

$$* \quad k \text{ impair} :$$

$$P = x^4 + 2x^2 + 1$$

$$= (x^2 + 1)^2$$

AINSI PREND FIN LE CHAPITRE SUR LES POLYNOMES.

3 FRACTIONS RATIONNELLES

Pour ce cours on aura besoin du support sur les Fractions.⁴

4. fiche-cours-ASINSA 1-fraction.pdf

Définition :

C'est quoi une fraction rationnelle ? C'est le rapport de deux polynôme. Un polynôme P au numérateur et un polynôme Q au dénominateur. Donc cette forme est appelée fraction rationnelle.

• Exemple de fraction rationnelle

$$A = \frac{P}{Q}$$

$$A = \frac{x^2+1}{x^3-6x^2+11x-6}$$

Méthode :

Comment décomposer une fraction rationnelle en éléments simples ?

Déterminer une décomposition en éléments simples une fraction rationnelle c'est d'écrire cette fraction en somme de fraction.

Procédure :

1. La première des choses à faire est de comparer le degré du numérateur et celui du dénominateur.

Il y a deux situations :

- (a) Soit le degré du polynôme P au numérateur est supérieur au degré du polynôme Q au dénominateur.
- (b) Soit le degré du polynôme P au numérateur est inférieur au degré du polynôme Q au dénominateur.

* Essayons de voir un premier cas où le degré du numérateur est inférieur au degré du dénominateur. C'est exactement notre cas présent le polynôme A .

2. La seconde démarche est la factorisation du dénominateur.

Factorisons le dénominateur du fraction rationnelle A

Méthode.

Comment décomposons nous cette fraction en éléments simples ?

Alors pour le faire, nous avons dit plus haut que c'est une somme de fraction et chaque composant du dénominateur constitue le dénominateur de chacune des fractions, et donc le degré de chaque terme aura à son numérateur son degré -1 . Donc si on devrait constater ici on verra clairement que chaque terme ici est de degré 1, donc, au numérateur de chaque composante nous aurons le degré $1 - 1$ qui est égale à 0. Autrement dit c'est le a qui est une somme de fraction dont chaque dénominateur est une composante ou un facteur entrant dans la factorisation du dénominateur.

$$A = \frac{x^2 + 1}{x^3 - 6x^2 + 11x - 6}$$

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

$$A = \frac{a}{x - 1} + \frac{b}{x - 2} + \frac{c}{x - 3}$$

Donnons la forme de la décomposition en éléments simples du polynôme B suivant :

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

Commentaire de M. MAGNANI

• Ici on voit très bien que le dénominateur de B est déjà sous la forme factorisée. Donc il est important de voir ou d'essayer de trouver l'ordre de multiplicité de chaque annulateur ou de chaque racines du dénominateur. Ici nous avons 0, qui a pour ordre de multiplicité 2, et -1 qui a pour ordre de multiplicité 2. Donc on comprend par là que ce qui importe c'est le degré du facteur entrant dans la décomposition, et donc ici nous avons $(x + 1)^2$ et donc le facteur entrant dans la factorisation est de degré 1 et qui est au **carré**, donc dans la décomposition nous allons essayer d'écrire les sommes de fraction jusqu'à l'ordre de multiplicité. **Nous en ferons de même pour x^2 . Donc nous commencerons par un dénominateur x puis viendras un dénominateur x^2 et comme le degré c'est 2 ça s'arrête là ci ça devrait continuer on continuerais par en croisant jusqu'à l'ordre de multiplicité, et donc le x qui de degré 1 aura pour numérateur une constante, quand nous irons de degré 2 c'est-à-dire le x^2 le dénominateur est toujours une constante c'est-à-dire que c'est le facteur entrant dans la décomposition, c'est son degré qui est important ce n'est pas l'ordre de multiplicité c'est plutôt le degré qu'il faut regarder donc le degré est de 1.**

Ainsi donc on a :

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

$$B = \frac{a}{x} + \frac{b}{x^2} + \frac{c}{x+1} + \frac{d}{(x+1)^2}$$

Remarque :

La décomposition se fait dans un espace vectoriel donné. Donc la décomposition en éléments simples se fait sur $\mathbb{K}[\mathbb{X}]$ où K est le corps de X et donc ici nous sommes entrain de faire une décomposition dans $\mathbb{R}[\mathbb{X}]$.

Les différents étapes données par M.MAGNANI pour décomposer en éléments simples.

$$A = \frac{P(x)}{Q(x)}$$

① Comparer $\deg P$ et $\deg Q$ en premier.

② Si $\deg P < \deg Q$ on effectue directement la décomposition en éléments simples

③ Si $\deg P \leq \deg Q$ on effectue tout d'abord la division euclidienne et on aura la forme

$$A = E(x) + \frac{K(x)}{Q(x)} \text{ avec } \deg K < \deg Q$$

Ensuite on effectue la décomposition pour $\frac{K(x)}{Q(x)}$ et on a l'expression de A .

$E(x)$ est appelé la partie entière de A .

Exemple :

Exercice n° 9 *td-de polynôme*

Décomposer en éléments simples de $\mathbb{R}[X]$ les fractions rationnelles suivantes :

$$(a) \quad f(x) = \frac{x^4}{x^2+3x+2}$$

$$(b) \quad g(x) = \frac{x^2+1}{(x-1)(x^2+x+1)}$$

Résolution :

(a) D'après la division euclidienne on a :

$$f(x) = (x^2 - 3x + 7) - \frac{15x + 14}{x^2 + 3x + 2}$$
$$f(x) = (x^2 - 3x + 7) + \frac{a}{x + 1} + \frac{b}{x + 2}$$

(b) Décomposons le $g(x)$ en éléments simples

$$g(x) = \frac{a}{x-1} + \frac{cx+d}{x^2+x+1}$$

Rappel :

Les transparents 19 et 20 et les exemples aideront à mieux comprendre cette partie.

NB :

Il ne sert à rien de chercher à calculer les coefficients si on a pas réussi à trouver la bonne forme. La mise en forme est très importante avant de chercher à calculer les coefficients. Voilà pourquoi nous nous sommes attelés d'abord à la décomposition en éléments simples et après nous tenterons de voir les techniques de calculs qu'il faut appliquer.

Les techniques de calculs des coefficients

① Technique des zéros.

Comment passer par les zéros du dénominateurs pour calculer rapidement les coefficients ?

Soit $A = \frac{x^2+1}{x^3-6x^2+11x-6}$

D'après la technique des zéros on a :

$$A = \frac{x^2 + 1}{x^3 - 6x^2 + 11x - 6}$$

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

$$A = \frac{a}{x - 1} + \frac{b}{x - 2} + \frac{c}{x - 3}$$

Essayons de calculer le coefficient a

$$(x - 1)A = a + (x - 1) \left[\frac{b}{x - 2} + \frac{c}{x - 3} \right]$$

$$\frac{x^2 + 1}{(x - 2)(x - 3)} = a + (x - 1) \left[\frac{b}{x - 2} + \frac{c}{x - 3} \right]$$

Pour $x = 1$ on a :

$$\frac{2}{(-1)(-2)} = a + 0$$

$$\Rightarrow \boxed{a = 1}$$

De manière analogue on obtient :

$$b = -5 \quad \text{et} \quad c = 5$$

Ainsi donc on a :

$$\boxed{A = \frac{1}{x - 1} + \frac{(-5)}{x - 2} + \frac{5}{x - 3}}$$

• Essayons de considérer la fraction rationnelle B que nous avons eu aussi à traiter. Parmi les coefficients a , b , c , et d dites quels sont les coefficients qu'on peut calculer directement en utilisant **la technique des zéros entre les quatre coefficients**.

NB :

C'est bien les coefficients b , c , et d qu'il faut déterminer.

Résolution :

$$\begin{aligned} B &= \frac{3x-1}{x^2(x+1)^2} \\ &= \frac{a}{x} + \frac{b}{x^2} + \frac{c}{x+1} + \frac{d}{(x+1)^2} \\ &= \frac{3x-1}{(x+1)^2} \end{aligned}$$

$$x^2 B = b + x^2 \left[\frac{c}{x+1} + \frac{d}{(x+1)^2} \right]$$

Pour $x = 0$ on a $-1 = b$

$$(x+1)^2 B = \frac{3x-1}{x^2} = d + c(x+1) + (x+1)^2 [\dots]$$

Pour $x = 1$ on a $-4 = d$

Il nous reste à présent à calculer les coefficients a et c . Pour le calcul de ces coefficients introduisons une autre technique qu'on appelle **technique de limite**.

② Technique de limite.

Pour le calcul de ces coefficients on passera par le calcul des limites à l'infinie (∞).

Exemple :

$$\begin{aligned} x^2 B &= \frac{3x-1}{(x+1)^2} \\ &= b + x \left[\frac{c}{x+1} + \frac{d}{(x+1)^2} \right] + ax \end{aligned}$$

Pour $x = 0$ on a $-1 = b$

$$\begin{aligned} (x+1)^2 B &= \frac{3x-1}{x^2} \\ &= d + c(x+1) + (x+1)^2 [\dots] \end{aligned}$$

Pour $x = -1$ $-4 = b$

$$\begin{aligned}\lim_{x \rightarrow +\infty} xB &= \lim_{x \rightarrow +\infty} \frac{3x - 1}{x(x + 1)^2} \\ &= \lim_{x \rightarrow +\infty} \left[a + \frac{b}{x} + \frac{cx}{(x + 1)^2} + \frac{dx}{(x + 1)^2} \right]\end{aligned}$$

$$0 = a + c$$

Commentaire de M.MAGNANI.

Cette technique consiste à multiplier de part et d'autre par x et à passer au limite à l'infini. Donc on voit clairement que cela nous permet d'obtenir une relation entre le a et le c . Et bien la limite de gauche est égale à 0 et la limite de droite est égale à $a + c$ et nous sommes en face d'une équation à deux inconnues et donc il nous faudrait une seconde équation pour pouvoir résoudre. Là nous serons en face de deux équations à deux inconnues. Pour ce faire nous donnerons une valeur arbitraire à x afin d'obtenir une seconde relation entre le c et le a . La valeur de x arbitraire à choisir, il faut la choisir judicieusement, il faudrait pas prendre une valeur qui annule un dénominateur. Il vaudra mieux choisir une valeur qui vous permet de faire simplement les calculs.

Alors dans ce cas essayons de trouver la seconde équation qui lie a et c .

Ce qu'il fallait trouver.

$$\text{Pour } x = 1 \quad \text{on a } \frac{1}{2} = a - 1 + \frac{c}{2} - 1$$

$$\Rightarrow 1 = 2a + c - 4$$

On a alors :

$$\begin{cases} a + c = 0 \\ 2a + c = 5 \end{cases}$$

$$\Rightarrow a = 5 \quad c = -5$$

Ainsi B est égal :

$$B = \frac{5}{x} + \frac{-1}{x^2} + \frac{-5}{x+1} + \frac{-4}{(x+1)^2}$$

Exercices :

Reprenons l'exercice n° 9 page 14 de se document.

(a) Effectuons la résolution complète.

$$f(x) = (x^2 - 3x + 7) - \frac{15x + 14}{x^2 + 3x + 2}$$

$$f(x) = (x^2 - 3x + 7) + \frac{a}{x - 1} + \frac{b}{x + 2}$$

$$\frac{-15x - 14}{(x + 1)(x + 2)} = \frac{a}{x + 1} + \frac{b}{x + 2}$$

$$\frac{-15x - 14}{(x + 2)} = a + (x + 1)\frac{b}{x + 2}$$

$$x = -1$$

$$1 = a$$

$$\frac{-15x - 14}{x + 1} = b + (x + 2)\frac{a}{x + 1}$$

$$x = -2$$

$$-16 = b$$

$$f(x) = (x^2 - 3x + 7) + \frac{1}{x + 1} + \frac{-16}{x + 2}$$

(b) Resolution complète.

$$g(x) = \frac{x^2 + 1}{(x - 1)(x^2 + x + 1)}$$

$$= \frac{a}{x - 1} + \frac{cx + d}{x^2 + x + 1}$$

$$\text{Pour } x = 1 \quad a = \frac{2}{3} \quad \lim_{x \rightarrow +\infty} xg(x) = 1 = a + c$$

$$\Rightarrow c = 1 - a = \frac{1}{3}$$

$$\text{Pour } x = 0 \text{ on a } -1 = -a + d \quad \Rightarrow d = a - 1 = -\frac{1}{3}$$

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

Séries d'exercice.

Décomposer en éléments simples sur \mathbb{R} les fractions rationnelles suivantes :

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

$$2. g(x) = \frac{x^3}{x^2-2x-3}$$

$$3. h(x) = \frac{x^5}{(x^3-1)(x-1)}$$

$$4. k(x) = \frac{x^2-x+1}{(x^2+4x+5)^2}$$

AINSI PREND FIN LE CHAPITRE SUR LES FRACTIONS RATIONNELLES.

4 THEORIE DES GROUPE.

4.1 Motivation

Évariste Galois a tout juste vingt ans lorsqu'il meurt dans un duel. Il restera pourtant comme l'un des plus grands mathématiciens de son temps pour avoir introduit la notion de groupe, alors qu'il avait à peine dix-sept ans.

Vous savez résoudre les équations de degré 2 du type $ax^2 + bx + c = 0$. Les solutions s'expriment en fonction de a , b , c et de la fonction racine carrée $\sqrt{\cdot}$. Pour les équations de degré 3, $ax^3 + bx^2 + cx + d = 0$, il existe aussi des formules. Par exemple une solution de $x^3 + 3x + 1 = 0$ est $x_0 = \sqrt[3]{\frac{\sqrt{5}-1}{2}} - \sqrt[3]{\frac{\sqrt{5}+1}{2}}$. De telles formules existent aussi pour les équations de degré 4.

Une préoccupation majeure au début du XIX^e siècle était de savoir s'il existait des formules similaires pour les équations de degré 5 ou plus. La réponse fut apportée par Galois et Abel : non il n'existe pas en général une telle formule. Galois parvient même à dire pour quels polynômes c'est possible et pour lesquels ça ne l'est pas. Il introduit pour sa démonstration la notion de groupe. Les groupes sont à la base d'autres notions mathématiques comme les anneaux, les

corps, les matrices, les espaces vectoriels,... Mais vous les retrouvez aussi en arithmétique, en géométrie, en cryptographie !

► Les mises en gardes

Pour bien comprendre ce chapitre il faut et il suffit d'oublier les préjugés sur les techniques de calculs. Et donc ce chapitre permet exclusivement de se consacrer uniquement qu'à ce qu'on a dit au respect strict des conditions et des hypothèses des exercices. Il ne sert à rien d'aborder ces types d'exercices c'est-à-dire de parler des groupes en tenant compte des préjugés.

Par exemple :

$$xy = yx ?$$

A la question est-ce que $xy = yx$ beaucoup parmi nous dirons **Oui** mais on ne diras pas toujours parce que le **produit** xy ne sera égal à yx que lorsque la définition de la loi **produit** est **commutative**. Alors tel qu'écrit il n'est dit nul part que la loi est commutative donc on comprend clairement que toutes les opérations que nous avons eu à faire **la multiplication usuelle dans \mathbb{R} , l'addition usuelle dans \mathbb{R}** ce sont des opérations commutatives c'est ce qui faisait que $xy = yx$, $x + y = y + x$ et nous avons grandi avec et donc à partir de maintenant laissons ces préjugés. Et donc le produit de xy n'est forcément égal à yx cela ne sera possible que lorsque l'opération a une propriété supplémentaire qui est la commutativité sinon il n'y a pas d'égalité entre xy et yx .

De même observons cette fonction :

$$(xy)^n = x^n y^n ?$$

Est-ce que :

$$(xy)^n = x^n y^n ?$$

Beaucoup également dirons **OUI** parce que toutes les opérations qu'on a eu à faire jusqu'à maintenant $(xy)^n = x^n y^n$ et on a toujours cru que c'est comme ça on fait les calculs et que c'est toujours **VRAI**. Mais la réponse est **NON**, pas toujours parce que $(xy)^n$ n'est pas forcément égal à $x^n y^n$ cela n'est vrai que dans un seul cas. Dans le cas où l'opération multiplication définie est une opération commutative sinon $(xy)^n$ n'est pas égal à $x^n y^n$ pas toujours, donc on voit clairement qu'on devrait abandonner certains préjugés qui ne sont que des cas particuliers des opérations ou des situations. Donc à partir de maintenant dès qu'on voit une opération définie il faut s'en tenir aux propriétés de cette définition, uniquement qu'aux propriétés de cette définition, ce que le texte dit, comment l'opération a été définie, quelles sont les propriétés de l'opération définie.

5 Définition :

Soit E un ensemble non vide.

On munit E d'une opération notée $*$.

On appelle loi de composition interne sur E , toute opération binaire

$$E \times E \longrightarrow E$$

$$(x, y) \longmapsto x * y$$

c'est-à-dire $\forall x, y \in (E, *)$ on a

$$x * y \in E.$$

Il est clair que quand l'on parle de loi de composition interne il faudrait que l'ensemble soit muni d'une loi qui reste interne c'est-à-dire que toute opération entre deux éléments de l'en-

semble rester toujours dans l'ensemble donc c'est par là qu'il faut comprendre la notion de loi de composition interne.

Dans notre définition, nous avons nommé cette loi $*$ et donc comprenons par là que le symbole pour désigner la loi est arbitraire c'est-à-dire on peut désigner cette loi par le symbole d'une case, d'une mangue, de l'addition, de la multiplication, ... Retenons que le symbole utilisé pour désigner l'opération n'est pas important ce qui importe **c'est la définition de l'opération c'est-à-dire ce symbole comment on l'exprime, ce symbole là comment on le définit**. C'est la définition qui est importante et non le schéma, la figure pour désigner ce symbole et donc comprenons par là que notre notation $*$ ici ou étoile est arbitraire ça aurait pu être **un ciment, un delta, un L , un M , tout ce qu'on veut** mais ce qui importe est comment est définie cette loi.

Exemple :

Soit $E =]-1, 1[$, on munit E de l'opération $*$ définie par :

$\forall x, y \in E \quad x * y = \frac{x + y}{1 + xy}$ où l'addition et la multiplication dans le second membre sont les lois usuelles de \mathbb{R} . Montrons que $*$ est une loi de composition interne.

COMMENTAIRE DE M. MAGNANI.

Dans cet exemple nous avons considéré un ensemble E qui va de -1 ouvert à 1 ouvert et nous avons muni l'ensemble E de l'opération $*$ que nous avons définie par $\forall x, y \in E$ signifie $x * y = \frac{x + y}{1 + xy}$, donc on voit clairement ce qu'on disait c'est-à-dire que on aurait pu remplacer la loi $*$ par une case, une petite voiturette, on peut le remplacer par n'importe quel symbole, mais ce qui importe c'est la définition de l'opération c'est-à-dire dans notre cas ici le $\frac{x + y}{1 + xy}$ donc l'opération importe peu mais c'est la définition de la loi, l'action de la loi qui est importante. Alors on a considéré le E qui nous ait familier, un intervalle de -1 à 1 parce qu'on est habitué à faire des calculs dans \mathbb{R} . Cela ne voudrait pas dire que les ensembles seront toujours des éléments de l'intervalle de \mathbb{R} mais **NON**. Un ensemble depuis la classe de 6^e c'est juste un sac dans lequel on met des éléments, des choses, donc ces choses ça peut être n'importe quoi, ça peut être un sac de mangues, d'oranges, de cahiers, de bics, donc tout dépend des éléments qui constituent l'ensemble.

Alors ici, pour une telle opération, une telle loi définie on nous demande de montrer que cette loi $*$ est une loi de composition interne.

Alors nous savons qu'après la définition plus haut, quand est-ce qu'on peut dire qu'une loi de composition est interne, donc nous ne ferons que vérifier la définition plus haut.

Ici dans notre cas il s'agira tout simplement de montrer que l'opération $x * y$ appartient à E . Or appartenir à E voudrait dire qu'on ait compris entre -1 et 1 . Cela revient à dire que $x * y$ en valeur absolue est strictement inférieur à 1 et ce qu'il faudra faire c'est de montrer que cette opération entre x et y est strictement supérieur à -1 et strictement inférieur à 1 et le tout est joué.

Résolution

Montrer que $*$ est une loi de composition interne sur E revient à montrer que $x * y = \frac{x+y}{1+x*y}$
 $\in E$
C'est-à-dire $x * y \in]-1, 1[$

Mieux encore $|x * y| < 1$.

On a alors :

$$\begin{cases} x * y < 1 \\ x * y > -1 \end{cases}$$

$$x * y < 1 \iff \frac{x+y}{1+xy} < 1 \text{ ❶}$$

$$x * y > -1 \iff \frac{x+y}{1+xy} > -1 \text{ ❷}$$

Il s'agira donc de prouver que

$$\frac{x+y}{1+xy} < 1 \quad \text{et} \quad \frac{x+y}{1+xy} > -1 \text{ puis conclure.}$$

❧ Dans un premier temps, prouvons que $\forall x, y \in E =]-1, 1[, \frac{x+y}{1+xy} > -1$.

$\forall x, y \in E$ on a $1+x > 0$ et $1+y > 0$

$$\begin{aligned} \Rightarrow (1+x)(1+y) &> 0 \Rightarrow 1+x+y+xy > 0 \\ \Rightarrow x+y &> -(1+xy) \end{aligned}$$

Or $1+xy > 0$ on a donc

$$\text{❶} \quad \frac{x+y}{1+xy} > -1 \text{ par suite } x * y > -1 \quad \forall x, y \in E.$$

☛ Tentons de montrer $x * y < 1$.

Soit $x, y \in E$ on a $1-x > 0$ et $1-y > 0$

$$(1-x)(1-y) = 1-x-y+xy > 0$$

$$\Rightarrow 1+xy > x+y \text{ or } 1+xy > 0$$

$$\text{❷} \Rightarrow 1 > \frac{x+y}{1+xy} \text{ par suite } x * y < 1 \quad \forall x, y \in E.$$

De ❶ et ❷ on conclut donc que

$$x * y \in E$$

D'où la loi $*$ est une loi de composition interne.

Maintenant que nous avons une idée de la définition d'une loi de composition interne, il y a certaines questions que nous pouvons nous poser à présent, à savoir **à quelle condition une loi de composition interne est associative, ou à quelle condition elle est commutative, à quelle condition elle admet un élément neutre et à quelle condition dirons nous qu'un élément est symétrisable** et donc tous ces conditions nous allons essayer de voir quels sont les critères que nous devons réunir avant de tirer telle ou telle conclusion.

6 La condition pour qu'une loi de composition interne soit associative.

Soit E un ensemble non vide munit d'une loi de composition interne notée multiplicativement \bullet .

On dit que la loi \bullet est associative si $\forall x, y \in E$ on a :

$$(x \bullet y) \bullet z = x \bullet (y \bullet z)$$

Exemple

Soit $(E =]-1, 1[, *)$ avec

$$\forall x, y \in E \quad x * y = \frac{x + y}{1 + xy}$$

La loi $*$ est-elle associative sur E ?

Résolution

la solution se trouve dans le livre des exercices et corrigés de MTH 102.

7 La condition pour qu'une loi de composition interne soit commutative.

On dit que la loi \bullet est commutative si et seulement si $\forall x, y \in E$ on a :

$$x \bullet y = y \bullet x$$

8 A quelle condition pouvons-nous dire qu'un ensemble munit d'une loi de composition interne admet un élément neutre .

Soit E un ensemble non vide munit d'une loi de composition interne notée multiplicativement \bullet .

On dit que (E, \bullet) admet un élément neutre si et seulement si :

$\exists e \in E$ tel que $\forall x \in E$ on ait

$$xe = ex = x$$

Il faut savoir qu'on a deux équations à savoir :

$$x \bullet e = x$$

↑

On dit que x admet

un élément neutre à droite

$$\text{et } e \bullet x = x$$

↑

on dit que x admet

un élément neutre à gauche.

Ainsi pour que e soit élément neutre il faudrait qu'il soit soit à la fois à gauche et à droite.

Exemple

Soit $(E =]-1, 1[, \star)$ avec

$$\forall x, y \in E \quad x \star y = \frac{x + y}{1 + xy}$$

Le e munit de cette loi \star admet-elle un élément neutre ?

Résolution

Soit $e \in E =]-1, 1[$ tel que $\forall x \in E \quad x \star e = x$

$$\text{On a } x \star e = \frac{x + e}{1 + xe} = x$$

$$\Rightarrow x + e = (1 + xe)x = x + x^2e$$

$$\Rightarrow (1 - x^2)e = 0 \text{ or } x \in]-1, 1[\text{ donc : } \\ 1 - x^2 \neq 0 \text{ d'où } e = 0$$

Alors 0 est donc un élément neutre à droite

Essaayons de voir ce qui se passerait à gauche 0.

Soit $x \in E =]-1, 1[$

$$0 \star x = \frac{0 + x}{1 + 0x} = x$$

$$\Rightarrow 0 \star x = x$$

Alors 0 est élément neutre à gauche .

On conclut donc que 0 est l'élément neutre de (E, \star)

La notion de symétrie d'un élément.

Quand dit-on qu'un élément x de E admet un symétrique ou est symétrisable dans E ?

Les conditions dans lesquelles nous pouvons conclure qu'un élément x est symétrisable ou admet un élément symétrique ou un inverse sont les suivantes :

Soit E un ensemble non vide.

On munit E d'une loi de composition interne notée multiplicativement \bullet , d'élément neutre e .

Soit $x \in (E, \bullet)$

On dit que x admet un symétrique ou un inverse ou que x est symétrisable dans (E, \bullet) si et seulement si

$$\exists x' \in E \text{ tel que } x \bullet x' = x' \bullet x = e$$

Ici également on a deux équations

$$x \bullet x' = e$$

\uparrow

On dit que x admet
un symétrique à droite

$$\text{et } x' \bullet x = e$$

\uparrow

on dit que x admet
que x admet un symétrique à gauche.

x est symétrisable s'il admet à la fois le même symétrique à gauche et à droite.

Exercice

Considérons l'exemple précédent et essayons de voir quel est l'élément symétrisable d'un x de E , c'est-à-dire si x un élément de E est symétrisable.

Résolution

Dans notre exemple précédent on a vu que 0 est l'élément neutre de $(E =] - 1, 1[, \star)$.

Soit $x \in (E, \star)$.

Déterminons si x admet un symétrique dans (E, \star)

Soit x' tel que $x \star x' = 0$

$$\text{On a } x \star x' = \frac{x + x'}{1 + xx'} = 0 \Rightarrow x + x' = 0$$

$x' = -x$. Donc $(-x)$ est le symétrique de x à droite.

Vérifions si $(-x)$ est le symétrique de x à gauche.

$$\begin{aligned}
(-x) \star x &= \frac{-x + x}{1 + (-x)(x)} \\
&= \frac{0}{1 - x^2} \\
&= 0
\end{aligned}$$

d'où $(-x)$ est le symétrique de x à gauche, x est donc symétrisable dans (E, \star)

Exercice

Soit $G = \begin{pmatrix} 1 & a & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad a, b \in \mathbb{R}$

On munit l'ensemble G de la multiplication ordinaire des matrices.

- 1 • La loi \bullet est-elle interne ?
- 2 • La loi \bullet est-elle associative ?
- 3 • (G, \bullet) admet-il un élément neutre ?
- 4 • Un élément de (G, \bullet) est-il symétrisable ?

Résolution

1- Soit $x, y \in G$ tel que $x = \begin{pmatrix} 1 & a & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ et $y = \begin{pmatrix} 1 & \alpha & \beta \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \alpha, \beta, a, b \in \mathbb{R}$

$$xy = \begin{pmatrix} 1 & a & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & \alpha & \beta \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & \alpha + a & \beta + b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$\alpha + a \in \mathbb{R}$ et $\beta + b \in \mathbb{R}$ on a $xy \in G$
d'où la loi \bullet est interne.

2- Indication : il suffit de prendre $x, y, z \in G$ et vérifier l'égalité $(xy)z = x(yz)$ et conclure.

9 A quelles conditions pouvons-nous affirmer qu'un ensemble munit d'une loi de composition interne est un groupe ou a une structure de groupe ?

9.1 Procédure

Soit G un ensemble non vide munit d'une loi de composition notée multiplicativement \bullet

On dit que (G, \bullet) est un groupe ou que a une structure de groupe si et seulement si les conditions suivantes sont satisfaites :

- 1- La loi \bullet est interne c'est-à-dire $\forall x, y \in G \quad x \bullet y \in G$
- 2- La loi \bullet est associative c'est-à-dire $\forall x, y, z \in G, (x \bullet y) \bullet z = x \bullet (y \bullet z)$
- 3- (G, \bullet) admet un élément neutre c'est-à-dire $\exists e \in G$ tel que $\forall x \in G$ on ait $x \bullet e = e \bullet x = x$
- 4- Tout élément de (G, \bullet) est symétrisable c'est-à-dire $\forall x \in G, \exists x' \in G$ tel que $x \bullet x' = x' \bullet x = e$

Remarque :

La commutativité n'entre pas dans la définition de groupe. Ce n'est qu'une propriété additionnelle c'est-à-dire il faudrait d'abord que ce soit un groupe.
En revanche un groupe peut être commutative c'est-à-dire il a la structure de groupe avant d'être commutative.

Exercice3(8 pts)

On considère les applications suivantes de $\mathbb{R} - \{0, 1\}$ dans lui-même.

$$f_1 : x \mapsto x; \quad f_2 : x \mapsto 1 - x; \quad f_3 : x \mapsto \frac{1}{1 - x}; \quad f_4 : x \mapsto \frac{1}{x}; \quad f_5 : x \mapsto \frac{x}{x - 1}; \quad f_6 : x \mapsto \frac{x - 1}{x}.$$

On munit l'ensemble $G = \{f_1, f_2, f_3, f_4, f_5, f_6\}$ de la composition des applications.

1. Ecrire la table de composition de (G, \circ) . (Les éléments seront écrits suivant les indices)
2. Montrer que (G, \circ) est un groupe.
3. Déterminer l'ordre de chacun des éléments suivantes f_2, f_3 .
4. Quels sont les éléments de $\langle f_3 \rangle$ sous-groupe engendré par f_3 .

Résolution

- 1- La table de composition de (G, \circ) .

	f_1	f_2	f_3	f_4	f_5	f_6
f_1	f_1	f_2	f_3	f_4	f_5	f_6
f_2	f_2	f_1	f_5	f_6	f_3	f_4
f_3	f_3	f_4	f_6	f_5	f_2	f_1
f_4	f_4	f_3	f_2	f_1	f_6	f_5
f_5	f_5	f_6	f_4	f_3	f_1	f_2
f_6	f_6	f_5	f_1	f_2	f_4	f_3

- 2- Il est question de voir si G munit de \circ respecte la définition, les quatre critères que nous avons définis à la page 30.

Nous voyons clairement que l'ensemble G composé de $f_1, f_2, f_3, f_4, f_5, f_6$. G ici est un ensemble fini. On va montrer que G est un groupe en analysant profondément le tableau.

D'abord pour le faire il faut connaître la définition du **groupe**, un groupe est un ensemble munit d'une loi de composition interne associative, contenant un élément neutre et que tout élément est inversible voilà les critères qu'il faut vérifier. Et donc nous allons essayer d'analyser ce tableau voir si les quatre critères sont vérifiés et en ce moment nous allons conclure au vu de ce que nous aurions analysé.

Essayons de voir à présent le premier point. Il s'agit de montrer que la loi de composition interne .

Comment le faire, d'après la table de composition, toutes les lignes et toutes les colonnes sont composées d'éléments de G donc la **loi de composition est interne**.

Il s'agit de montrer que cette loi est associative. Comment le montrer ? En générale la composition des applications est associative, les éléments de G ici étant des applications donc la loi de composition du sujet ici est **associative**.

- 3- Il s'agit de montrer que (G, \circ) admet un élément neutre. Alors d'après la table de composition la ligne de f_1 et la colonne de f_1 laisse invariant tous les autres éléments donc f_1 est l'élément neutre.

Le quatrième point que nous devons vérifier est de montrer si tout élément de G admet un symétrique.

Etant donné que nous avons réussi à identifier l'élément neutre, nous voyons clairement que $f_2 \circ f_2 = f_1$ ce qui nous fait dire que f_2 est son propre symétrique, $f_4 \circ f_4 = f_1$ donc f_4 aussi est son propre symétrique ; f_5 est son propre symétrique. $f_3 \circ f_6 = f_1, f_6 \circ f_3 = f_1$, donc f_3 et f_6 sont symétriques l'un de l'autre, en gros f_1, f_2, f_4, f_5 , pour chacun de ces éléments chacun est son propre symétrique f_3, f_6 sont symétriques l'un de l'autre. Pour avoir parcourir tous les éléments, déterminer les symétriques de tous les éléments de G nous constatons que tout élément de G est symétrisable.

G munit de la loi \circ est donc un groupe. Puisque nous venons de vérifier tous ces critères dans la définition de la notion de groupe sont vérifiés, donc nous concluons que G munit de la loi \circ est un groupe.

Remarque

En face d'un groupe contenant un nombre fini d'éléments, c'est la démarche à suivre c'est-à-dire faire un tableau et l'interpréter. Quand le groupe G est donné comme ça se présente ici de manière discrète. Il faut l'interpréter. Donc c'est la manière dont il faut procéder.

Exercice 2 (8 pts)

Soit G un ensemble fini muni d'une loi de composition interne, associative notée multiplicativement. On admet qu'il existe $e \in G$ tel que :

i. $\forall x \in G, ex = x.$

ii. $\forall x \in G, \exists y \in G$ tel que $yx = e$

1. (G, \bullet) est un groupe.

2. $\mathbb{Z}(G)$ le centre de G est un sous-groupe de G et que $\mathbb{Z}(G) \triangleleft G$ (sous-groupe distingué de G)

Rappel cruciale

Nous avons quatre points à vérifier qui sont montrer qu'une loi de composition est interne, associative, l'ensemble admet un élément neutre, et tout élément est inversible. Ici les hypothèses de l'exercice nous disent déjà que la loi de **composition est interne et quelle est associative** donc les deux premiers points sont validés. Ce qui nous reste à faire est de montrer que les deux derniers points sont validés et conclure.

Le petit i. nous dit que $\forall x \in G, ex = x$. ça veut dire tout simplement que le e ici présent est élément neutre à gauche alors on peut pas dire que le e est élément neutre de G puisque quand on prend la définition il y a tout, notamment deux équations à résoudre. Ici nous avons une seule équation qui est une hypothèse donc nous ne pouvons pas conclure, il revient à montrer que la seconde équation aussi est vraie autrement dit pour ce même e on peut avoir $\forall x \in G, ex = x$.

c'est le travail demander ,donc une fois qu'on aura montrer $\forall x \in G, ex = x$. là on peut conclure que e est l'élément neutre de G .

Le *ii* on dit que $\forall x \in G, \exists y \in G$ tel que $yx = e$ ça ne voudrait pas dire que tout élément est inversible ici ça voudrait dire tout simplement que chaque élément admet un inverse à gauche donc il faudrait montrer que chaque élément admet un inverse à gauche et à droite et que c'est le même .

Résolution de l' exercice2

Soit $x \in G$. D'après *ii* $\exists y \in G$ tel que $xy = e$ et donc il existe $z \in G$ tel que $zy = e$

$$\begin{aligned}
 xe &= e(xe) \quad \text{d'après } i \\
 &= (zy)(xe) \quad \text{car } e = zy \\
 &= z(yx)e \quad \text{car la loi est associative} \\
 &= z(e)e \\
 &= z(ee) \\
 &= ze \\
 ex &= (zy)x \\
 &= z(yx) \\
 &= ze
 \end{aligned}$$

On a $xe = ex = x \quad \forall x \in G$
d'où e est élément neutre de G .

Une autre manière d'aborder cette question.

Soit $x \in G$. D'après *ii* $\exists y \in G$ tel que $yx = e$
Alors $\exists z \in G$ tel que $zy = e$

$$\begin{aligned}
 xe &= e(xe) \quad \text{d'après } i \\
 &= exe = (zy)x(yx) \\
 &= z(yx)yx = z(e)yx = z(ey)x \\
 &= z(y)x = (zy)x = (e)x = ex
 \end{aligned}$$

Donc $\exists e \in G$ tel que $\forall x \in G$
 $xe = ex = x$
D'où e est élément neutre de G

Montrons que tout élément est symétrisable.

Soit $x \in G$ $\exists y \in G$ tel que $yx = e$

$$\begin{aligned} xy &= e(xy) = (zy)(xy) \\ &= z(yx)y = zey = zy = e \end{aligned}$$

Donc $\forall x \in G \exists y \in G$ tel que $xy = yx = e$

Tout élément est donc symétrisable
 (G, \bullet) est un groupe.

10 Notion de translation à gauche et à droite.

Soit G un groupe notée multiplicativement .

On définit deux applications appelées **translations** à gauche et à droite comme suit :

Soit $a \in G$

$$\begin{aligned} \gamma : G &\longrightarrow G \\ x &\longmapsto ax \quad \text{Translation à gauche} \end{aligned}$$

$$\begin{aligned} \delta_a : G &\longrightarrow G \\ x &\longmapsto xa \quad \text{Translation à droite} \end{aligned}$$

Remarque

Les translations à gauche et à droite sont **injectives**. Par conséquent tout élément de G est régulier c'est-à-dire simplifiable à gauche et à droite.

EXERCICE2(7 pts)

Corriger et bien détailler dans le livre d'EXO MTH 102.

11 Notion de sous-groupe.

Soit G un groupe, H un sous ensemble non vide de G

On dit que H est un sous-groupe de G si et seulement si $\forall x, y \in H, x \equiv y[H]$

$(x \equiv y(mod H))$ c'est-à-dire

$$\forall x, y \in H, xy^{-1} \in H$$

Alors d'après la définition pour montrer que H est un sous-groupe de G , il suffit de montrer que $\forall x, y \in H$ on a $xy^{-1} \in H$

Remarque

y^{-1} est le symétrique de y dans G , donc ne pas voir y^{-1} comme étant $\frac{1}{y}$ ce qui ne correspond à rien.

On peut aussi montrer que H est un sous-groupe en deux étapes

1- $\forall x, y \in H$ on a $xy \in H$

2- $\forall x \in H$ on a $x^{-1} \in H$

12 Notion de sous groupe engendré par une partie

Soit A une partie non vide de G l'intersection de tous les sous groupes de G contenant A est un sous groupe de G contenant A . Ce sous groupe est le sous groupe **engendré** par A et on note $\langle A \rangle$.

Remarque

Tout élément de G engendre un sous groupe noté $\langle x \rangle$.

Si G est noté multiplicativement on a :

$$\langle x \rangle = \{x^n, n \in \mathbb{Z}\}$$

Si G est noté additivement on :

$$\langle x \rangle = \{nx, n \in \mathbb{Z}\}$$

$\{e\}$ et G sont appelés sous groupes triviaux de G .

Un sous groupe H de G est dit sous groupe propre si $H \neq \{e\}$ et $H \neq G$

13 Le centre d'un groupe

On définit le centre de G par $\mathbb{Z}(G) = \{x \in G / \forall g \in G, xg = gx\}$

Montrons que $\mathbb{Z}(G)$ est un sous groupe de G .

$\forall g \in G$ on a $ge = eg$ avec e l'élément neutre de G , on a alors $e \in \mathbb{Z}(G)$, $\mathbb{Z}(G) \neq \emptyset$

- Soit $x, y \in \mathbb{Z}(G)$
Soit $g \in G$

$$\begin{aligned}(xy)g &= x(yg) = x(gy) \quad \text{car } y \in \mathbb{Z}(G) \\ &= (xg)y \quad \text{associativité} \\ &= (gx)y \quad \text{car } x \in \mathbb{Z}(G) \\ &= g(xy) \quad \text{associativité}\end{aligned}$$

D'où $xy \in \mathbb{Z}(G)$, $\mathbb{Z}(G)$ est stable.

- Soit $x \in \mathbb{Z}(G)$ on a $\forall g \in G \quad gx = xg$

$$\Rightarrow x^{-1}(gx)x^{-1} = x^{-1}(xg)x^{-1}$$

$$\begin{aligned}\Rightarrow (x^{-1}g)(xx^{-1}) &= (x^{-1}x)(gx^{-1}) \Rightarrow x^{-1}g = gx^{-1} \quad \forall g \in G \\ \Rightarrow x^{-1} &\in \mathbb{Z}(G).\end{aligned}$$

D'où $\mathbb{Z}(G)$ est un sous groupe de G .

14 Notion de l'ordre d'un groupe fini

Soit G un groupe fini .

On désigne par n le cardinal de G et on note $|G| = n$. Cet entier n est aussi appelé ordre de G et on note $o(G) = n$

C'EST QUOI ALORS L'ORDRE D'UN ÉLÉMENT x DE G

L'ordre d'un élément x de G est le plus petit entier positif k_0 tel que $x^{k_0} = e$ et on note $o(x) = k_0$

Reprenons l'exercice 3 page 31 de ce document.

Suite de l'exercice.

$$\begin{aligned}3. \quad f_2 \circ f_2 &= f_1 \quad \Rightarrow o(f_2) = 2 \\ f_3 \circ f_3 \circ f_3 &= f_1 \quad \Rightarrow o(f_3) = 3\end{aligned}$$

$$4. \langle f_3 \rangle = \{f_1, f_3, f_3^2\} = \{f_1, f_3, f_6\}$$

15 Le morphisme de groupe et ses propriétés

15.1 Définition :

Soit (G, \bullet) et (G', \top) deux groupes et f une application de G dans G' .

On dit que $f : G \longleftrightarrow G'$ est un morphisme ou un homomorphisme si et seulement si $\forall x, y \in G$ on a :

$$f(x \bullet y) = f(x) \top f(y).$$

$$\text{Ker } f = \{x \in G / f(x) = e'\}$$

Montrer que le $\text{Ker } f$ est un sous groupe de G

Méthode.

Montrer que le $\text{Ker } f$ est un sous groupe de G

$$f(e) = e' \text{ car } f \text{ est un morphisme}$$

$$e \in \text{Ker } f \Rightarrow \text{Ker } f \neq \emptyset$$

$$\text{Soit } x, y \in \text{Ker } f$$

$$f(xy^{-1}) = f(x) \top f(y^{-1}) = f(x) \top [f(y)]^{-1} = e' \top e' = e \rightarrow xy^{-1} \in \text{Ker } f \text{ d'où } \text{Ker } f \text{ est un sous groupe de } G.$$

$$\text{Im } f = \{f(x), x \in G\}$$

Montrer que $\text{Im } f$ est un sous groupe de G'

Méthode.

Montrer que $\text{Im } f$ est un sous groupe de G'

$$\text{Im } f \subset G'$$

$$e \in G \Rightarrow f(e) = e'$$

$$e' = f(e) \in \text{Im } f \Rightarrow \text{Im } f \neq \emptyset$$

Soit $X, Y \in \text{Im} f$

$\Rightarrow \exists x, y \in G$ tel que $X = f(x)$ et $Y = f(y)$

$$\begin{aligned} X \top Y^{-1} &= f(x) \top [f(y)]^{-1} \\ &= f(x) \top f(y^{-1}) \quad \text{car } f \text{ est un morphisme} \\ &= f(x \bullet y^{-1}) \quad \text{car } f \text{ est un morphisme} \\ X \top Y^{-1} &= f(x \bullet y^{-1}) \in \text{Im} f \quad \text{car } x \bullet y^{-1} \in G \end{aligned}$$

D'où $\text{Im} f$ est un sous groupe de G'

16 Extrait des exercices corrigés

17 pdf-UL3 les séries d'exercice

4.(a) Montrons que H sous-groupe de $G \Rightarrow f(H)$ sous-groupe de G' .

$$H \subset G \quad \Rightarrow f(H) \subset f(G) \subset G'$$

H est un sous groupe de G alors $e \in H$

$$\Rightarrow e' = f(e) \in f(H) \Rightarrow f(H) \neq \emptyset$$

Soit $X, Y \in f(H)$

$$\Rightarrow \exists x, y \in H \text{ tel que } X = f(x), Y = f(y)$$

$$XY^{-1} = f(x)[f(y)]^{-1} = f(x)f(y^{-1}) \text{ car } f \text{ est un homomorphisme.}$$

$$XY^{-1} = f(xy^{-1}) \text{ car } f \text{ est un homomorphisme.}$$

Or H est un sous-groupe de G donc $xy^{-1} \in H$

$$\Rightarrow XY^{-1} = f(xy^{-1}) \in f(H).$$

D'où $f(H)$ est un sous-groupe de G'

(b) $f : G \rightarrow G'$ un morphisme.

Montrons que H' sous-groupe de $G' \Rightarrow f^{-1}(H')$ sous-groupe de G .

H' sous-groupe de G' on a $e' \in H'$ alors

$$f(e) = e' \in H' \Rightarrow e \in f^{-1}(H') \text{ d'où } f^{-1}(H') \neq \emptyset$$

Soit $X, Y \in f^{-1}(H') \subset G$

$\exists x, y \in H'$ tel que $f(X) = x, f(Y) = y$

$$f(X)[f(Y)]^{-1} = xy^{-1} \in H' \text{ car } H' \text{ sous-groupe de } G'$$

$\Rightarrow f(X)[f(Y^{-1}) \in H' \Rightarrow f(XY^{-1}) \in H'$ car f est morphisme.
 $f(XY^{-1}) \in H' \Rightarrow XY^{-1} \in f^{-1}(H')$

On conclut donc que $f^{-1}(H')$ est un sous-groupe de G .

18 Notion de groupes quotients

18.1 Définition

Soit G un groupe et H un sous-groupe de G .

$G/_H = \{gH, g \in G\}$ ensemble des classes à gauche

$G/_H = \{Hg, g \in G\}$ ensemble des classes à droite

$gH = \{gh; h \in H\}$

A quelle condition $G/_H$ à une structure de groupe ?

NB :

Nous retiendrons que $G/_H$ à une structure de groupe lorsque l'ensemble des classes à gauche est égale à l'ensemble des classes à droite c'est-à-dire que $xH = Hx \quad \forall x \in G$ dans cette condition là $G/_H$ à une structure de groupe.

$$xH = Hx$$

c'est-à-dire si H est distingué dans G et on note $H \triangleleft G$.

Remarque

Dans un groupe *abélien* tout sous-groupe est *distingué*.

19 A quelles conditons peut-on dire qu'un groupe est distingué

19.1 Propositions

Soit G un groupe et H un sous-groupe de G .

H est distingué dans G si et seulement si l'une des conditions suivantes est vérifiées :

1. $\forall x \in G, Hx = xH$
2. $\forall x \in G, xHx^{-1} = H$
3. $\forall x \in G, xHx^{-1} \subset H$
4. $\forall x \in G, \forall h \in H, xhx^{-1} \in H$

Montrons que $\mathbb{Z}(G)$, le centre de G est un sous-groupe distingué dans G .

On rappelle qu'on avait déjà montré que $\mathbb{Z}(G)$ est un sous-groupe de G , il nous reste à montrer que $\mathbb{Z}(G)$ est distingué dans G .

$$\mathbb{Z}(G) = \{x \in G / \forall g \in G, xg = gx\}$$

Utilisons le point 4. de la proposition pour montrer que $\mathbb{Z}(G)$, centre de G est distingué dans G .

Résolution détaillée

Soit $x \in \mathbb{Z}(G), z \in G$

Il s'agit de montrer que $zxz^{-1} \in \mathbb{Z}(G)$.

Pour cela il faut montrer que (zxz^{-1}) commute avec tout élément de G

Soit $g \in G$

$$\begin{aligned}
 g(zxz^{-1}) &= g(zx)z^{-1} = g(xz)z^{-1} \quad \text{car } x \in \mathbb{Z}(G) \\
 &= (gx)zz^{-1} = gx = xg \quad \text{car } x \in \mathbb{Z}(G) \\
 &= x(e)g = x(zz^{-1})g = (xz)z^{-1}g \\
 &= (zx)z^{-1}g = (zxz^{-1})g
 \end{aligned}$$

On a donc $\forall g \in G, g(zxz^{-1}) = (zxz^{-1})g$
d'où $zxz^{-1} \in \mathbb{Z}(G)$

On conclut donc que $\mathbb{Z}(G) \triangleleft G$.

Comment utiliser le point 1?

$$\mathbb{Z}(G) = \{x \in G / \forall g \in G, xg = gx\}$$

Soit $a \in G$

$$a\mathbb{Z}(G) = \{ax \in G / \forall g \in G, xg = gx\}$$

$$a\mathbb{Z}(G) = \{xa \in G / \forall g \in G, xg = gx\} = \mathbb{Z}(G)a$$

$$xa = ax \text{ car } x \in \mathbb{Z}(G)$$

$$\text{On a alors } \forall a \in G \quad a\mathbb{Z}(G) = \mathbb{Z}(G)a$$

$$\text{d'où } \mathbb{Z}(G) \triangleleft G$$

Exercice 5

(a) AB sous-groupe de $G \Leftrightarrow AB = BA$

Supposons que AB est un sous-groupe de G

A et B étant des sous-groupes de G on a : $A = A^{-1}$ et $B = B^{-1}$

$$BA = B^{-1}A^{-1} = (AB)^{-1} = AB \text{ car } AB \text{ étant un sous sous-groupe de } G \text{ on a : } AB = (AB)^{-1}$$

On a donc $BA = AB$

Une autre façon de faire.

Supposons que AB sous-groupe de $G \Leftrightarrow AB = BA$

$e = ee \in AB$ car AB sous-groupe de G , on a $AB \neq \emptyset$

Soit $x \in AB, y \in AB$

$\exists a, a_1 \in A, \quad b, b_1 \in B$ tel que

$$x = ab \text{ et } y = a_1b_1$$

$$\begin{aligned} xy^{-1} &= (ab)(a_1b_1) = abb_1^{-1}a_1^{-1} = ab_2a_1^{-1} \quad \text{avec } b_2 = bb_1^{-1} \\ &= aa_2b_3 \quad \text{avec } b_2a_1^{-1} = a_2b_3 \quad \text{avec } BA = AB \\ &= a_3b_3 \quad \text{avec } a_3 = aa_2 \\ xy^{-1} &= a_3b_3 \in AB \end{aligned}$$

D'où AB sous-groupe de G

Attention !

A NE PAS FAIRE

$(AB)^{-1} = B^{-1}A^{-1} = BA = AB$ est du fait que $AB = (AB)^{-1}$ pour conclure que AB est un sous-groupe.

$H = H^{-1}$ est une conséquence dû au fait que H est un sous-groupe et non l'inverse.

5.(b) Supposons que A est distingué dans G .

$e = ee \in AB$ avec $e \in A$ et $e \in B$ car A et B sont des sous-groupes de G .

$e \in AB \Rightarrow AB \neq \emptyset$

Soit $x, y \in AB$, il existe $a, a_1 \in A$ et $b, b_1 \in B$ tel que $x = ab$ et $y = a_1b_1$

$$xy^{-1} = (ab)(a_1b_1)^{-1} = abb_1^{-1}a_1 = ab_2a_1 \text{ avec } b_2 = bb_1^{-1}$$

$$xy^{-1} = a(b_2a_1) = a(a_2b_2) \text{ car } A \text{ étant distingué dans } G \text{ on a } b_2A = Ab_2$$

$$\text{Alors } xy^{-1} = aa_2b_2 = a_3b_2 \in AB$$

d'où AB est un sous-groupe de G

Attention!!!

Dire que $AB = BA$ ne veut pas dire qu'on a $ab = ba$. Cela veut plutôt dire que $ab = a_1b_1$ c'est-à-dire $\forall ab \in AB$ on peut trouver $a_1 \in A$ et $b_1 \in B$ tel que $ab = b_1a_1$

7.(a) Montrer que H est distingué dans G , on dit aussi que $H \subset \mathbb{Z}(G)$ alors la question ne demande pas de montrer que $H \subset \mathbb{Z}(G)$ ça c'est une hypothèse donc pour montrer qu'un sous-groupe est distingué dans un groupe il suffit de montrer que la définition est vérifiée c'est tout.

H sous-groupe de G et $H \subset \mathbb{Z}(G)$

Comprenez que $H \subset \mathbb{Z}(G)$ voudrait dire que les éléments de H ont les propriétés des éléments de $\mathbb{Z}(G)$ à savoir tout élément de G commute avec tout élément de H .

Alors H sous-groupe de $G \Rightarrow H \neq \emptyset$

Soit $h \in H$ et $g \in G$

$$ghg^{-1} = (gh)g^{-1} = (hg)g^{-1} \text{ car } H \subset \mathbb{Z}(G)$$

$$= h(gg^{-1}) = h \in H$$

$$\text{Donc } \forall g \in G \quad \forall h \in H \quad ghg^{-1} \in H$$

d'où $H \triangleleft G$

7.(b) G/H est cyclique veut dire G/H est monogène et fini c'est-à-dire engendré par un élément et est fini.

$G/H = \langle \bar{a} \rangle$ où \bar{a} est le générateur.

Soient $x, y \in G$ et \bar{x}, \bar{y} leurs classes respectives dans G/H . On a

$$\bar{x} = \bar{a}^n \text{ et } \bar{y} = \bar{a}^m, n, m \in \mathbb{N}$$

$$\begin{aligned}\bar{x} &= \bar{a}^n = a^n H & \bar{y} &= \bar{a}^m = a^m H \\ \Rightarrow \exists h, h' \in H \text{ tel que } x &= a^n h & y &= a^m h'\end{aligned}$$

$$\begin{aligned}xy &= (a^n h)(a^m h') = a^n(ha^m)h' \\ &= a^n(ha^m)h' \quad \text{car } H \subset \mathbb{Z}(G) \\ &= a^{n+m}hh' = a^{m+n}hh' \quad \text{car } \mathbb{N} \text{ commutative} \\ &= h'(a^{m+n}h) \quad \text{car } \mathbb{Z}(G) \text{ commutative pour } + \\ &= h'a^m a^n h = (h'a^m)a^n h = (a^m h')(a^n h) \\ &= yx \quad \forall x, y \in G \quad xy = yx \Rightarrow G \text{ abélien}\end{aligned}$$

8.(a) G cyclique engendré par a . On a $G = \langle a \rangle$ d'ordre $n \Rightarrow a^n = e$
 $\forall x \in G \quad \exists k \in \mathbb{N}$ tel que $x = a^k$

Soit H un sous-groupe de G tout élément de H est une puissance de a car a est le générateur de G

Soit n_0 le plus petit des entiers tels que $a^{n_0} \in H$. Le sous groupe engendré $\langle a^{n_0} \rangle$ engendré par a^{n_0} est contenu dans H car $a^{k_0} \in H$ on a alors $\langle a^{n_0} \rangle \subset H$.

Soit $x \in H \quad \exists m \in \mathbb{N}$ tel que $x = a^m \in H$

n_0 étant le plus petit élément on a $q, r \in \mathbb{N}$ tel que $m = qr_0 + r \quad 0 \leq r < n_0$

$$x = a^m = a^{qn_0+r} = a^{n_0q} \times a^r \in H.$$

$$a^m \times a^{-n_0q+r} = a^r \text{ étant sous groupe donc stable pour la multiplication } a^m, a^{-n_0q} \in H$$

Ce qui prouve que $a^r = a^m a^{-n_0q} \in H$

$a^r \in H$ si $r \neq 0$ alors du fait que $r < n_0$ contredit le fait que n_0 soit le plus petit entier tel que $a^{n_0} \in H$ d'où $r = 0$. On a alors $m = n_0q$

$$a^m = a^{n_0q} = (a^{n_0})^q \in \langle a^{n_0} \rangle$$

$$x = a^m \in \langle a^{n_0} \rangle \text{ d'où } H \subset \langle a^{n_0} \rangle$$

On conclut donc que $H = \langle a^{n_0} \rangle$.

Soit $x \in \mathbb{Z}(G), z \in G$

Il s'agit de montrer que $zxz^{-1} \in \mathbb{Z}(G)$

Pour cela il faut montrer que zxz^{-1} commute avec tout élément de G .

Soit $g \in G$

$$\begin{aligned}g(zxz^{-1}) &= g(zx)z^{-1} = g(xz)z^{-1} \quad \text{car } g(zx)z^{-1} \\ &= (gx)zz^{-1} = gx = xg \quad \text{car } g(zx)z^{-1} \\ x(e)g &= x(zz^{-1})g = (xz)z^{-1}g \\ &= (zx)z^{-1}g = (zxz^{-1})g\end{aligned}$$

On a alors $\forall g \in G \quad g(zxz^{-1}) = (zxz^{-1})g$ d'où $zxz^{-1} \in \mathbb{Z}(G)$

On conclut donc que $\mathbb{Z}(G) \triangleleft G$

● Montrons que $\mathbb{Z}(G)$ est distingué dans G

$$\mathbb{Z}(G) = \{x \in G / \forall g \in G \quad xg = gx\}$$

Soit $a \in G$

$$a\mathbb{Z}(G) = \{ax \in G / \forall g \in G \quad xg = gx\} = \mathbb{Z}(G)a$$

$$xa = ax \text{ car } x \in \mathbb{Z}(G)$$

$$\text{On a alors } \forall a \in G \quad a\mathbb{Z}(G) = \mathbb{Z}(G)a$$

$$\text{D'où } \mathbb{Z}(G) \triangleleft G$$

● Exercice 5(a)

$$AB \text{ sous groupe de } G \Leftrightarrow AB = BA$$

Supposons que AB est un sous groupe de G , A et B étant des sous groupes de G on a $A = A^{-1}$ et $B = B^{-1}$

$$BA = B^{-1}A^{-1} = (AB)^{-1} = AB \text{ car } AB \text{ étant un sous groupe de } G \text{ on a } AB = (AB)^{-1} \text{ on a donc } BA = AB.$$

5.b) Supposons que A est distingué dans G , $e = ee \in AB$ avec $e \in A$ et $e \in B$ car A et B sont des sous groupe de G .

$$e \in AB \Rightarrow e \in AB \neq \emptyset$$

$$\text{Soit } x, y \in AB, \text{ il existe } a, a_1 \in A \text{ et } b, b_1 \in B \text{ tel que } x = ab \text{ et } y = a_1b_1$$

$$xy^{-1} = (ab)(a_1b_1)^{-1} = abb_1^{-1}a_1 = ab_2a_1 \text{ avec } b_2 = bb_1^{-1}$$

$$xy^{-1} = aa_2b_2 = a_3b_2 \in AB \text{ d'où } AB \text{ est un sous groupe de } G$$

ATTENTION!!!

Dire que $AB = BA$ ne veut pas dire que qu'on a $ab = ba$. Cela veut plutôt dire que $ab = b_1a_1$ c'est-à-dire $\forall ab \in AB$ on peut trouver $a_1 \in A$ et $b_1 \in B$ tel que $ab = b_1a_1$

7.a) H sous-groupe de G et $H \subset \mathbb{Z}(G)$

Comprenez que $H \subset \mathbb{Z}(G)$ voudrait dire que les éléments de H ont les propriétés des éléments de $\mathbb{Z}(G)$ à savoir tout élément de G commute avec tout élément de H

$$\text{Alors } H \text{ sous groupe de } G \Rightarrow H \neq \emptyset$$

$$\text{Soit } h \in H \text{ et } g \in G$$

$$ghg^{-1} = (gh)g^{-1} = (hg)g^{-1} \text{ car } H \subset \mathbb{Z}(G)$$

$$= h(gg^{-1}) = h \in H$$

$$\text{Donc } \forall g \in G \quad \forall h \in H \quad ghg^{-1} \in H \text{ d'où } H \triangleleft G$$

7.b) G/H est cyclique veut dire G/H est monogène et fini c'est-à-dire engendré par un élément et est fini.

$$G/H = \langle \bar{a} \rangle \text{ où } \bar{a} \text{ est le générateur.}$$

Soient $x, y \in G$ et \bar{x}, \bar{y} leurs classes respectives dans G/H . On a

$$\bar{x} = \bar{a}^n \text{ et } \bar{y} = \bar{a}^m \text{ } n, m \in \mathbb{N}$$

$$\bar{x} = \bar{a}^n = a^n H \quad \bar{y} = \bar{a}^m = a^m H$$

$$\Rightarrow \exists h, h' \in H \text{ tel que } x = a^n h \quad y = a^m h'$$

$$\begin{aligned} xy &= (a^n h)(a^m h') = a^n (ha^m) h' \\ &= a^n (a^m h) h' \text{ car } H \subset \mathbb{Z}(G) \\ &= a^{n+m} h h' = a^{m+n} h h' \text{ car } \mathbb{N} \text{ est commutative pour } + \\ &= h' (a^{m+n}) \text{ car } H \subset \mathbb{Z}(G) \\ &= h' a^m a^n h = (h' a^m) a^n h = (a^m h')(a^n h) \\ &= yx \quad \forall x, y \in G \quad xy = yx \Rightarrow G \text{ abélien} \end{aligned}$$

8.a) $G = \langle a \rangle$ d'ordre $n \Rightarrow a^n = e$

$$\forall x \in G \exists k \in \mathbb{N} \text{ tel que } x = a^k$$

Soit H un sous groupe de G tout élément de H est une puissance de a car a est le générateur de G

Soit n_0 le plus petit des entiers tels que $a^{n_0} \in H$. Le sous groupe $\langle a^{n_0} \rangle$ engendré par a^{n_0} est contenu dans H car $a^{n_0} \in H$ on a alors $\langle a^{n_0} \rangle \subset H$.

Soit $x \in H$ $\exists m \in \mathbb{N}$ tel que $x = a^m \in H$ n_0 étant le plus petit élément on a $q, r \in \mathbb{N}$ tel que $m = qn_0 + r$ $0 \leq r < n_0$
 $x = a^m = a^{qn_0+r} = a^{n_0q} \times a^r \in H$
 $a^m \times a^{-n_0q} = a^r$ H étant sous groupe donc stable pour la multiplication $a^m, a^{-n_0q} \in H$
ce qui prouve que $a^r = a^m a^{-n_0q} \in H$
 $a^r \in H$ si $r \neq 0$ alors du fait que $r < n_0$ contredit le fait que n_0 soit le plus petit entier tel que $a^{n_0} \in H$ d'où $r = 0$. On a alors $m = a^{n_0q} = (a^{n_0})^q \in \langle a^{n_0} \rangle$
 $x = a^m \in \langle a^{n_0} \rangle$ d'où $H \subset \langle a^{n_0} \rangle$
On conclut donc que $H = \langle a^{n_0} \rangle$

8.b) $a^m = e \Leftrightarrow n$ divise m

Supposons que $a^m = e$ n étant l'ordre de G $n \leq m$. Donc il existe $(q, r) \in \mathbb{N} \times \mathbb{N}$ tel que $m = nq + r$
 $a^m = a^{nq+r} = (a^n)^q a^r = a^r$ car $a^n = e$
 $a^m = a^r = e$. Si $r \neq 0$ alors du fait que $r < n$ contredit le fait que n soit le plus petit entier tel que $a^n = e$. D'où $r = 0$
On a alors $m = nq$. n divise m
L'autre sens. Supposons que n divise m
 $\exists q \in \mathbb{N}$ tel que $m = nq$
 $a^m = a^{nq} = (a^n)^q = e^q = e$
On conclut donc que $a^m = e \Leftrightarrow n$ divise m

c.i) $H = \langle a^p \rangle$

$PGCD(n, p) = q$, q divise $p \Rightarrow \exists \alpha \in \mathbb{N}$ tel que $p = \alpha q$
 $a^p = a^{\alpha q} = (a^q)^\alpha \Rightarrow a^p \in \langle a^q \rangle$ le sous groupe engendré par a^q
 $a^p \in \langle a^q \rangle \Rightarrow \langle a^p \rangle \subset \langle a^q \rangle$ d'où $H \subset \langle a^q \rangle$
 $PGCD(n, p) = q \Rightarrow$ d'après le théorème de Bézout

ii) n et p sont premiers entre eux $\Rightarrow PGCD(n, p) = 1$ d'après i) on a $q = 1$

Donc $H = \langle a^p \rangle = \langle a^q \rangle = \langle a \rangle = G$

On a alors $H = G$

\Rightarrow Si $H = G$ alors $G = \langle a^p \rangle$

$G = \langle a \rangle = \langle a^p \rangle$ on a alors d'après ii.) que $PGCD(n, p) = 1$ on conclut donc que n et p sont premiers entre eux

20 Théorème de LAGRANGE

Soit G un groupe fini et H un sous groupe de G .

L'ordre de tout sous groupe divise l'ordre du groupe. On a l'équation :

$$|G| = |H| [G : H]$$

où $[G : H]$ est l'indice de H dans G , $[G : H] = |G/H|$

AINSI PREND FIN LES NOTIONS SUR LA THEORIE DES GROUPES

21 Etude d'un groupe particulier : groupe des permutation S_n (groupe symétrique)

Soit E un ensemble fini. On appelle permutation de E toute **Bijection** de $E \longrightarrow E$

L'ensemble des permutations est noté S_E .

E étant fini notons par n son cardinal c'est-à-dire $|E| = n$

S_E se note aussi S_n pour dire l'ensemble des bijections de n éléments vers le même ensemble de n éléments. L'ensemble S_n muni de la loi de composition \circ des applications fait de (S_n, \circ) un groupe.

A quoi ressemble une permutation ?

Soit $\sigma \in S_n$ on a :

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & k & \cdots & n \\ a_1 & a_2 & \cdots & a_k & \cdots & a_n \end{pmatrix}$$

$\sigma(k) = a_k$ où a_k sont des images de k par σ

Exemple

$$E = \{a, b, c\} \quad |E| = 3$$

$$Id = \begin{pmatrix} a & b & c \\ a & b & c \end{pmatrix} \quad \sigma_1 = \begin{pmatrix} a & b & c \\ a & b & c \end{pmatrix}$$

$$\sigma_2 = \begin{pmatrix} a & b & c \\ a & b & c \end{pmatrix} \quad \sigma_3 = \begin{pmatrix} a & b & c \\ a & b & c \end{pmatrix}$$

$$\alpha = \begin{pmatrix} a & b & c \\ a & b & c \end{pmatrix} \quad \beta = \begin{pmatrix} a & b & c \\ a & b & c \end{pmatrix}$$

$$S_E = S_3 = \{Id, \sigma_1, \sigma_2, \sigma_3, \alpha, \beta\}$$

(S_3, \circ) est un groupe.

$$\alpha \circ \beta = \alpha\beta = \begin{pmatrix} a & b & c \\ a & b & c \end{pmatrix} = Id$$

$$\alpha \circ \alpha = \alpha^2 = \begin{pmatrix} a & b & c \\ a & b & c \end{pmatrix} = \beta$$

$$^{\circ}(S_n) = |S_n| = n!$$

$$= n \times (n-1) \times \cdots \times 5 \times 4 \times 3 \times 2 \times 1$$

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 5 & 7 & 10 & 8 & 9 & 1 & 4 & 6 & 2 \end{pmatrix} \text{ (exercice)}$$