

Structures Algébriques

Chapitre préliminaire "Rappel"

I - Ensemble et relations

1 - Définition :

Un ensemble est une collection d'objets qui ont un ou plusieurs caractères en commun.

2 - Relations :

- Une relation sur un ensemble E est la description de liens entre certains éléments de E.

- Une relation est identifiée par un graphe.

- Le graphe d'une relation R sur un ensemble E est l'ensemble des couples $(a, b) \in E \times E / a R b$; par exemple: Relation d'ordre et Relation d'équivalence.

- Une relation peut avoir plusieurs propriétés:

a - Réflexivité :

- Une relation R définie sur un ensemble E est dite réflexive si: $\forall x \in E: x R x$

- " \leq " est une relation réflexive, par contre " $<$ " n'est pas une relation réflexive.

b - Symétrie :

- Une relation R définie sur un ensemble E est dite symétrique si: $\forall x, y \in E: x R y \Rightarrow y R x$

- Pour l'ensemble "I_{f1}" muni de la relation " \leq ", " \leq " est symétrique, par contre pour I_N muni de " \leq ", " \leq " n'est pas symétrique.

c - Anti-symétrie :

- Une relation R définie sur un ensemble E est dite anti-symétrique si: $\forall x, y \in E: \begin{cases} x R y \\ y R x \end{cases} \Rightarrow x = y$

- Pour l'ensemble "IR" muni de la relation " \leq ", " \leq " est anti-symétrique

d - Transitivité :

- Une relation R définie sur un ensemble E est dite transitive si:

$$\forall x, y, z \in E: \begin{cases} x R y \\ y R z \end{cases} \Rightarrow x R z$$

e - Relation d'ordre :

Soit R une relation définie sur un ensemble E ,

R est dite relation d'ordre si:

- R est :
 - * Réflexive;
 - * Transitive;
 - * Anti-symétrique.

f - Relation d'équivalences

Soit R une relation définie sur un ensemble E ,

R est dite relation d'équivalence si:

- R est :
 - * Réflexive;
 - * Transitive;
 - * Symétrique.

II - Loi de composition et morphisme :

Application:

1 - Loi de composition interne "LCI":

Si l'application f : $E \times E \rightarrow E$:
On appelle "LCI" sur E , toute application de $E \times E$ vers E .

$$\forall x, y \in E / x = y \Rightarrow f(x) = f(y)$$

Injectivité:

a - Associativité:

Si f est injective si: Soit $(E, *)$ un ensemble muni d'une LCI " $*$ ". On dit que " $*$ " est

$\forall x, y, z \in E / f(x) = f(y) \Rightarrow x = y$ associative si: $\forall a, b, c \in E : (a * b) * c = a * (b * c) = a * b * c$

b - Commutativité:

Soit $(E, *)$ un ensemble muni d'une LCI " $*$ ". On dit que " $*$ " est commutative si: $\forall a, b \in E : a * b = b * a$

c - Élément neutre :

Soit $(E, *)$ un ensemble muni d'une LCI " $*$ ". On dit que " $*$ " admet un élément neutre si: $\exists e \in E, \forall x \in E : x * e = e * x = x$

d - Élément inverse :

Un élément admet un élément inverse dans $(E, *)$ si:

$$\forall x \in E, \exists x' \in E : x * x' = x' * x = e$$

X Exercice 1:

Soit E un espace euclidien

Soit l'ensemble $E^2 = \{ (A, B) \in E \times E \}$

Soit " α " tq $\forall A, B, C, D \in E : (A, B) \alpha (C, D) \Leftrightarrow \begin{cases} A=B=C=D \\ \text{ou} \\ A=C \text{ et } B=D \\ \text{ou} \\ A=D \text{ et } B=C \end{cases}$

Mq " α " est une relation d'équivalence.

* Réflexivité :

Soient $A, B \in E$,

on a : " $A=A$ et $B=B$ " est vraie,

donc : " $\begin{cases} A=B=A=B \\ \text{ou} \\ A=A \text{ et } B=B \\ \text{ou} \\ A=B \text{ et } B=A \end{cases}$ " est vraie,

d'où : " $(A, B) \alpha (A, B)$ " est vraie,

alors : " α " est réflexive.

* Symétrie :

Soient $A, B, C, D \in E$,

on a : $(A, B) \alpha (C, D) \Leftrightarrow \begin{cases} A=B=C=D \\ \text{ou} \\ A=C \text{ et } B=D \\ \text{ou} \\ A=D \text{ et } B=C \end{cases}$

$$\Leftrightarrow \begin{cases} C=D=A=B \\ \text{ou} \\ C=A \text{ et } D=B \\ \text{ou} \\ C=B \text{ et } D=A \end{cases}$$

$$\Leftrightarrow (C, D) \alpha (A, B)$$

alors : " α " est symétrique.

* Transfinitivité :

Soient $A, B, C, D, X, Y \in E$,

on a : $(A, B) \alpha (X, Y) \Leftrightarrow \begin{cases} A=B=X=Y \\ \text{ou} \\ A=X \text{ et } B=Y \\ \text{ou} \\ A=Y \text{ et } B=X \end{cases}$

$(X, Y) \alpha (C, D) \Leftrightarrow \begin{cases} X=Y=C=D \\ \text{ou} \\ X=C \text{ et } Y=D \\ \text{ou} \\ X=D \text{ et } Y=C \end{cases}$

i) " $A=B=X=Y$ " et " $X=Y=C=D$ "

d'où : $A=B=C=D$

ii) " $A=B=X=Y$ " et " $X=C$ " et " $Y=D$ "

d'où : $A=B=C=D$

iii) " $A=B=X=Y$ " et " $X=D$ " et " $Y=C$ "

d'où : $A=B=D=C$ c.-à-d. $A=B=C=D$

iv) "A=x" et "B=y" et "x=y=C=D"

d'où: A=B=C=D

v) "A=x" et "B=y" et "x=c" et "y=d"

d'où: A=c et B=d

vi) "A=x" et "B=y" et "x=d" et "y=c"

d'où: A=d et B=c

vii) "A=y" et "B=x" et "x=y=c=d"

d'où: B=A=C=D c-a-d A=B=C=D

viii) "A=y" et "B=x" et "x=c" et "y=d"

d'où: A=d et B=c

ix) "A=y" et "B=x" et "x=d" et "y=c"

d'où: A=c et B=d

donc:

$$(A, B) \alpha (X, Y) \text{ et } (X, Y) \alpha (C, D) \Leftrightarrow \begin{cases} A=B=C=D \\ \text{ou} \\ A=C \text{ et } B=D \\ \text{ou} \\ A=D \text{ et } B=C \end{cases} \Leftrightarrow (A, B) \alpha (C, D)$$

alors: " α " est transitive.

Conclusion: " α " est une relation d'équivalence sur E.

III - Groupes:

1 - Magma:

Un magma est un ensemble E muni d'une loi " Δ " et on le note (E, Δ) .

2 - Définition d'un groupe:

Le magma (E, Δ) est dit groupe si:

i) " Δ " est associative,

ii) E admet un élément neutre pour " Δ ",

iii) Chaque élément a de E admet un inverse par " Δ ".

Exemple:

x 1) Soit X un ensemble,

L'ensemble $S(X)$, des bijections de X sur X, muni de la loi

"o", des composées des bijections, est un groupe symétrique sur X.

$S(X) = \{ f : X \rightarrow X ; f \text{ est bijective} \}$

X 2) L'ensemble des matrices $GL_n(\mathbb{R})$ ($n \geq 1$) des matrices carrées d'ordre n à coefficients réels et inversible est un groupe pour la multiplication des matrices. (Associativité à vérifier)

X 3) Soit E un espace vectoriel de dim = n , et soit $\{e_1, \dots, e_n\}$ une base de E ,

Soit $P_i : E \rightarrow E$

$$x = (x_1, x_2, \dots, x_n) \mapsto (0, 0, \dots, x_i, \dots, 0)$$

Soit $G = \{P_i : E \rightarrow E\}$ muni de la loi " \circ " est-il un groupe? (Exercice)

3. Sous-groupe:

m'est pas un groupe, car l'élément neutre n'est pas unique: chaque P_i a son e_i .

Déf1: Soit $(G, *)$ un groupe,

on dit que $(H, *)$ est un sous-groupe de $(G, *)$ si $H \subseteq G$ et H est un groupe.

Déf2: Soit (G, ∇) un groupe,

Une partie H de G est dite sous-groupe de G si il vérifie:

i) $H \neq \emptyset$

ii) H est stable par " ∇ "

iii) Chaque élément de H admet un inverse par " ∇ "

Proposition:

Soit $(G, *)$ un groupe, et soit H une partie de G ,

$(H, *)$ est un sous-groupe de G si et

ii) $H \neq \emptyset$

ii) $\forall x, y \in H : x * y^{-1} \in H$

X Exercice 1:

Montrer que l'ensemble des bijections croissantes de $\mathbb{R} \rightarrow \mathbb{R}$ est un sous-groupe de $(S(\mathbb{R}), \circ)$. + Recherche: groupe orthogonal

X Exercice 2:

Soit $(G, *)$ un groupe dont e est l'élément neutre, et soit $(H, *)$ un sous-groupe de G .

Est-ce que $((G \setminus H) \cup \{e\}, *)$ est un sous-groupe?

Propositions:

Soit $(G, *)$ un groupe,

H et K sont deux sous-groupes de G ,

- $H \cap K$ est un sous-groupe de G . En effet:

$H \cap K \neq \emptyset$ (contenant l'élément neutre de G),

et: $\forall x, y \in H \cap K : x, y \in H$ et $x, y \in K$

d'où: $x \cdot y^{-1} \in H$ et $x \cdot y^{-1} \in K$

donc: $x \cdot y^{-1} \in H \cap K$

- $H \cup K$ n'est pas forcément un sous-groupe de G :

Par exemple: $2\mathbb{Z}$ et $3\mathbb{Z}$ sont deux sous-groupe de $(\mathbb{Z}, +)$

or: $2-3 \notin 2\mathbb{Z} \cup 3\mathbb{Z}$

- Si $H \subseteq K$ ou $K \subseteq H$, alors $H \cup K$ est un sous-groupe.

- L'intersection d'une famille qlq de sous-groupes est un sous-groupe.

4- Groupes finis:

- Le cardinal d'un ensemble est le nombre d'éléments qui le constituent.

- On appelle groupe fini un groupe qui a un cardinal fini, ce cardinal est appelé l'ordre du groupe et on le note $|groupe|$ ou $o(groupe)$.

X Théorème de Lagranges

Soit H un sous-groupe d'un groupe fini G ,

Alors: H est fini, et: $|H| / |G|$ (Démon: Exercice / Rechercher si y'a tel)

5- Sous-groupe engendré par une partie: une théorie pour le cas infini)

Soit $(G, *)$ un groupe, et soit H une partie de G non vide,

L'intersection de tous les sous-groupes contenant H est un sous-groupe qui contient H , et c'est le plus petit (dans le sens d'inclusion) de tous les sous-groupes contenant H . On le note $\langle H \rangle$ et on le dénomme: Sous-groupe engendré par H :

$$\langle H \rangle = \bigcap_{\substack{K_i \\ H \subseteq K_i}} K_i ; K_i \text{ sous-groupe de } G, \forall i \in I$$

6 - Sous-groupe engendré par un élément :

Soit (G, \circ) un groupe,

Soit x un élément de G ,

on appelle sous-groupe monogène (engendré par un seul élément) engendré par x dans G , le sous-groupe engendré par $\{x\}$, on le note $\langle x \rangle$.

C'est le plus petit sous-groupe de G contenant x , et l'on a:

$$\langle x \rangle = \langle x^n, n \in \mathbb{Z} \rangle \text{ avec } x^n = \underbrace{x * x * x * \dots * x}_n$$

Exemple:

$$2\mathbb{Z} = \langle 2 \rangle ; \quad 4\mathbb{Z} = \langle 4, 16 \rangle$$

Définition:

Soit (G, \circ) un groupe,

Soit $x \neq e_G$ un élément de G ,

on dit que x est d'ordre fini dans G lorsqu'il existe des entiers $n > 1$ tels que $x^n = e$

Dans ce cas, on appelle ordre de x le plus petit entier entre eux x est d'ordre n dans $G \Leftrightarrow x^n = e$ et $x^m \neq e, \forall 1 < m < n$ et $m \in \mathbb{N}$

Proposition:

Soit (G, \circ) un groupe,

Soit x un élément de G ,

Si x est d'ordre fini dans G , alors le sous-groupe $\langle x \rangle$ est fini et d'ordre n et l'on a: $\langle x \rangle = \{e, x, x^2, x^3, \dots, x^{n-1}\}$

Groupe cyclique:

Un groupe (G, \circ) est cyclique d'ordre n si il est monogène et d'ordre fini,

Exercice: est-ce que le groupe engendré par $\{x\}$ est fini?

sinon, si $\forall i, j \in \mathbb{Z}, i \neq j: x^i \neq x^j$ et $G = \{x^m, m \in \mathbb{Z}\}$ il est dit monogène infini.

Exemple:

$$2\mathbb{Z} = \langle 2 \rangle \text{ est monogène infini.}$$

X Proposition: "Sous-groupe d'un groupe cyclique"

Soit (G, \circ) un groupe cyclique d'ordre $n \geq 1$, et soit H un sous-groupe cyclique de G ,

alors H est cyclique d'ordre d et il existe - pour tout diviseur q de n - un seul sous-groupe d'ordre q

Exemple :

Si on prend un groupe cyclique H d'ordre 101, les sous-groupes de H sont H et $\{e\}$.

✗ Proposition 8 : "Sous-groupe d'un groupe monogène infini"

Tout sous-groupe non trivial d'un groupe est un groupe infini.

✗ Générateur d'un groupe cyclique :

Soit $G = \langle a \rangle$ un groupe cyclique d'ordre $n \geq 2$

Les générateurs de G sont les éléments a^K tels que les entiers K et n sont premiers entre eux

✗ Exercice :

Soit $U_3 = \{z \in \mathbb{C}^* / z^3 = 1\}$

1) Montrer que (U_3, \cdot) est un groupe monogène cyclique.

2) Trouver l'ordre de U_3

3) Donner les générateurs de U_3

1) * Mq (U_3, \cdot) est un groupe,

- Soient $x, y, z \in U_3$: $x^3 = y^3 = z^3 = 1$, $x, y, z \in \mathbb{C}^*$

on a: $x^3 \cdot (y^3 \cdot z^3) = 1$ et $(x^3 \cdot y^3) \cdot z^3 = 1$

d'où: $x^3 \cdot (y^3 \cdot z^3) = (x^3 \cdot y^3) \cdot z^3$

donc: " \cdot " est associatif.

- Soit $x \in U_3$: $x^3 = 1$, $x \in \mathbb{C}^*$

on a: $x^3 \cdot 1 = 1 \cdot x^3 = x^3$ et $1 \in U_3$

donc: 1 est l'élément neutre de U_3 par " \cdot ".

- Soit $x \in U_3$: $x^3 = 1$, $x \in \mathbb{C}^*$

on a: $x^{-1} \in U_3$ car $(x^{-1})^3 = (x^3)^{-1} = 1^{-1} = 1$

comme: $x^3 \cdot (x^{-1})^3 = (x^{-1})^3 \cdot x^3 = 1$ l'élément neutre

d'où: x^{-1} est l'inverse de x sur U_3 pour " \cdot ".

donc: chaque élément de U_3 admet l'inverse par " \cdot ".

Alors (U_3, \cdot) est un groupe.

* Mq (U_3, \cdot) est monogène,

on a: $U_3 = \{1; e^{\frac{4\pi i}{3}}; e^{\frac{2\pi i}{3}}\}$ (en effet: $(e^{\frac{4\pi i}{3}})^3 = e^{4\pi i} = 1$ et $(e^{\frac{2\pi i}{3}})^3 = e^{2\pi i} = 1$)

d'où: $U_3 = \langle e^{\frac{4\pi i}{3}} \rangle = \langle e^{\frac{2\pi i}{3}} \rangle$

Alors, (U_3, \cdot) est monogène.

* Mq (U_3, \cdot) est fini,

on a: $\text{card}(U_3) = 3$ "fini"

Alors, (U_3, \cdot) est fini.

Conclusion: (U_3, \cdot) est un groupe cyclique.

2) on a: $1^3 = (e^{\frac{4\pi i}{3}})^3 = (e^{\frac{2\pi i}{3}})^3 = 1$

donc: $|U_3| = 3$

3) on a: $\forall k \in \{1, 2\}: k \wedge 3 = 1$

donc: Ses générateurs de U_3 sont: $e^{\frac{4\pi i}{3}}$ et $e^{\frac{2\pi i}{3}}$

9- Indicatrice d'Euler:

On appelle indicatrice d'Euler, l'application: $\Phi: \mathbb{N}^* \rightarrow \mathbb{N}^*$ définie par: $\Phi(1) = 1$ et $\forall n \geq 2$, $\Phi(n)$ est le nombre d'entiers K tel que $1 < K \leq n-1$ et $K \wedge n = 1$

d'après le théorème précédent, $\Phi(n)$ est le nombre de générateurs d'un groupe cyclique d'ordre n .

X Exercice 9:

Montrer que: $\Phi(p^\alpha) = p^\alpha - p^{\alpha-1}$, $\forall p$ premier, et $\alpha \geq 1, \alpha \in \mathbb{N}$

X Exercice 9:

Montrer que si $G = \langle x \rangle$ est un groupe monogène infini alors les seuls générateurs de G sont x et x^{-1} .

10- Groupes finis d'ordre premiers:

Soit G un groupe fini d'ordre premier p , alors:

1- G est cyclique,

2- Les seuls sous-groupes de G sont $\{e\}$ et G ,

3- Tous les éléments de G -distincts à e - sont générateurs de G .

Exemples:

$G = \mathbb{Z}/11\mathbb{Z}$ est cyclique d'ordre 11, ses sous-groupes sont $\{0\}$ et G , et ses générateurs sont: $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$

II- Morphismes de groupes:

1-Définitions

Soit G un groupe muni d'une LCI " $*$ ", et soit G' un groupe muni de une LCI " ∇ ".

On dit que f est un morphisme de groupes / un homomorphisme de groupes de G vers G' , si c'est une application vérifiant:

$$\forall x, y \in G: f(x * y) = f(x) \nabla f(y)$$

Exemples:

ex: $(\mathbb{R}, +) \rightarrow (\mathbb{R}_+^*, \times)$ est un homomorphisme de groupes
 $x+y \mapsto e^{xy} = e^x \cdot e^y$

2-Propositions

- * L'image directe Vd d'un sous-groupe de G est un sous-groupe de G' .
- * L'image réciproque Vd^{-1} d'un sous-groupe de G' est un sous-groupe de G .
- * Soient G et G' deux groupes, et soit $f: G \rightarrow G'$ un morphisme de groupes.

on a:

i) G est un sous-groupe trivial de G , donc:

$\text{Im } f = \{x' \in G' / \exists x \in G: f(x) = x'\}$ est un sous-groupe de G' .

ii) Pour tout H sous-groupe de G :

$f(H) = \{x' \in G' / \exists x \in H: f(x) = x'\} = \{f(x) / x \in H\}$ est un sous-groupe de G' .

iii) $\{e\}$ est un sous-groupe trivial de G' , donc

$\text{Ker } f = \{x \in G / f(x) = e\}$ est un sous-groupe de G .

iv) Pour tout H' sous-groupe de G' :

$f^{-1}(H') = \{x \in G / f(x) \in H'\}$ est un sous-groupe de G .

3-Propositions

Le composé de deux morphismes de groupes est un morphisme de groupes:

$f: (G, *) \rightarrow (G', \nabla)$; $g: (G', \nabla) \rightarrow (G'', \tau)$

$g \circ f: (G, *) \rightarrow (G'', \tau)$ est un morphisme de groupes.

$$\forall x, y \in G: g(f(x * y)) = g(f(x) \nabla f(y))$$

$$\forall x, y \in G: g(f(x * y)) = g(f(x) \nabla f(y))$$

$$\forall x, y \in G: g(f(x * y)) = g(f(x)) \tau g(f(y)) = g \circ f(x) \tau g \circ f(y)$$

Cas particulier:

1) Endomorphisme: Si $G = G'$. Dans ce cas: $f: (G, *) \rightarrow (G, *)$

Isomorphisme : Si le morphisme est bijective

Automorphisme : Si le morphisme est endomorphisme + bijective

4- Isomorphismes :

Si f est un isomorphisme de groupes de G sur G' , alors la réciproque f^{-1} est un isomorphisme de groupes de G' sur G . G et G' sont dits isomorphes et on note $G \cong G'$, il en résulte que G et G' ont les mêmes propriétés algébriques.

5- Automorphisme de groupes :

Exemple : $f: (\mathbb{C}, +) \rightarrow (\mathbb{C}, +)$

$$z \mapsto f(z) = \bar{z}$$

Soit $(G, *)$ un groupe,

L'ensemble des automorphismes du groupe G est un groupe pour la loi "o" dont l'élément neutre est Id

on le note : $(\text{Aut}(G), o)$

6- Centre d'un groupe :

Soit $(G, *)$ un groupe,

L'ensemble des éléments de G qui commutent avec tous les éléments de G est un sous-groupe de $(G, *)$, appelé centre du groupe $(G, *)$, et

on le note $Z(G) = \{x \in G / g * x = x * g, \forall g \in G\}$

et on a, * $Z(G)$ est un sous-groupe commutatif

* $Z(G) = G \Leftrightarrow G$ est commutatif

X 7- Automorphisme intérieur

Soit $(G, *)$ un groupe,

on définit l'application $\sigma_x: G \rightarrow G$ qui est un automorphisme de G appelé automorphisme... $g \mapsto x * g * x^{-1}$... intérieur déterminé par x

L'ensemble $\text{Int}(G) = \{\sigma_x / x \in G\}$ de tous les automorphismes de G est un sous-groupe de groupe $\text{Aut}(G)$.

L'application $\sigma: (G, *) \rightarrow (\text{Aut}(G), o)$ est un morphisme de groupes, d'image $\text{Int}(G)$... $x \mapsto \sigma_x$... et de noyau $Z(G)$

Démonstration :

1) Montrons que σ est une morphisme de groupes,

Soient $g, x, y \in G$, on a:

$$\begin{aligned}\sigma(x * y)(g) &= \sigma_{x * y}(g) \\&= (x * y) * g * (x * y)^{-1} \\&= (x * y) * g * (y^{-1} * x^{-1}) \\&= x * (y * g * y^{-1}) * x^{-1} \\&= x * \sigma_y(g) * x^{-1} \\&= \sigma_x(\sigma_y(g))\end{aligned}$$

d'où: $\sigma(x * y)(g) = \sigma_x \circ \sigma_y(g)$

donc: σ est un morphisme de groupes,

2) Montrons que $\text{Im } \sigma = \text{Int } G$:

on a: $\text{Im } \sigma = \{y \in \text{Aut}(G) / \exists x \in G : \sigma(x) = y\}$

et: $\text{Int } G = \{\sigma_x ; x \in G\}$

d'où: $\text{Im } \sigma = \text{Int } G$

3) Montrons que $\text{Ker } \sigma = \Sigma(G)$:

on a: $\begin{aligned}\text{Ker } \sigma &= \{x \in G / \forall g \in G : \sigma_x(g) = \text{Id}(g)\} \\&= \{x \in G / \forall g \in G : \sigma_x(g) = g\} \\&= \{x \in G / \forall g \in G : x * g * x^{-1} = g\} \\&= \{x \in G / \forall g \in G : x * g = g * x\}\end{aligned}$

d'où: $\text{Ker } \sigma = \Sigma(G)$

IV - Produit direct (Externe) de deux groupes

1. Définitions

Soient $(G, +)$ et (G', \cdot) deux groupes d'éléments neutre e_1 et e_2 resp.,

1- Le produit externe: $\text{exc } G \times G' = \{(x_1, x_2) / x_1 \in G \text{ et } x_2 \in G'\}$ est un groupe pour la loi " \cdot " définie par:

$$(x_1, x_2) \cdot (y_1, y_2) = (x_1 * y_1, x_2 \cdot y_2)$$

X Exercice:

montrer que les applications:

* "1^{ère} projection": $p_1: G_1 \times G_2 \rightarrow G_1$

$$(x_1, x_2) \mapsto x_1$$

* "2^{ème} projection": $p_2: G_1 \times G_2 \rightarrow G_2$

$$(x_1, x_2) \mapsto x_2$$

sont des morphismes de groupes, puis déterminer $\text{Im}(P_1)$ et $\text{ker}(P_1)$, et $\text{Im}(P_2)$ et $\text{ker}(P_2)$.

I - Proposition:

Soient G_1 et G_2 deux groupes,

- * G_1 et G_2 sont finis $\Leftrightarrow G_1 \times G_2$ est fini avec: $|G_1 \times G_2| = |G_1| \times |G_2|$
- * G_1 et G_2 sont commutatifs $\Leftrightarrow G_1 \times G_2$ est commutatif
- * $G_1 \times G_2 \cong G_2 \times G_1$

II - Produit direct (interne) de deux groupes:

1 - Définition:

Soient G un groupe, et H et K deux sous-groupes de G ,

on note HK le sous-ensemble de G formé des éléments qui.

s'écrivent comme produit d'un élément de H et d'un élément de K :

$$HK = \{hk / h \in H \text{ et } k \in K\}$$

on dit que G est le produit direct (interne) de H par K si :

i) $G = HK$

ii) $H \cap K = \{e\}$

iii) $\forall h \in H, \forall k \in K: hk = kh$

Exemple :

Soit G un groupe,

G est le produit direct (interne) de ses groupes triviaux $\{e\}$ et G .

X Exercice:

Soit G un groupe, et soient H et K deux sous-groupes de G ,

Soit HK l'ensemble défini par: $HK = \{hk / h \in H \text{ et } k \in K\}$

1) Montrer que: Si $H \cap K = \{e\}$, alors: $\forall x \in HK: x$ s'écrit de façon unique sous la forme hk où $h \in H$ et $k \in K$

2) Montrer que: Si $H \cap K = \{e\}$ et H et K sont finis, alors: HK est fini et $\text{card}(HK) = \text{card}(H) \times \text{card}(K)$ (Indication: montrer $(H, K) \cong HK$)

3) Montrer que: $HK = KH \Leftrightarrow \forall h \in H, \forall k \in K, \exists h' \in H, \exists k' \in K / hk = h'k'$

VII - Groupe symétrique:

1 - Définition:

Pour tout $n \geq 1$, on appelle groupe symétrique, le groupe des bijections

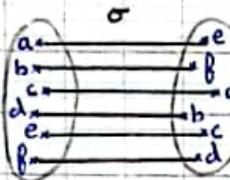
d'un ensemble fini à n éléments quelconques sur lui-même, on note ce groupe S'_n .

Remarque :

* S'_n muni de la loi " \circ " est un groupe fini d'ordre $n!$,

* Ces éléments de S'_n sont appelés les permutations sur n éléments, on note une telle permutation par : $\sigma = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \dots & \sigma(n) \end{pmatrix}$

Exemple 1 :



$$\sigma = (a \ b \ c \ d \ e \ f) \\ (e \ f \ a \ b \ c \ d)$$

Exemple 2 :

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix}$$

2 - Cycle :

Soit n un entier naturel non nul, et soit K un entier compris entre 2 et n ,

Un élément σ de $S'_n \setminus \{\text{id}\}$ s'appelle un cycle de longueur K / K -cycle si il existe une partie $\{a_1, \dots, a_K\}$ de $\{1, 2, \dots, n\}$ telle que :

$$\sigma(a_1) = a_2, \sigma(a_2) = a_3, \dots, \sigma(a_K) = a_1, \sigma(x) = x \text{ si } x \notin \{a_1, \dots, a_K\}$$

Un tel cycle est noté : (a_1, a_2, \dots, a_K)

3 - Transposition :

On appelle transposition de S_n toute permutation δ qui échange deux éléments i et j en laissant fixes les $n-2$ autres éléments, on la note $\delta = [i, j]$

Remarques et notations :

$$\delta^2 = \delta \circ \delta = \text{id} ; \quad \delta^{-1} = \delta$$

on va noter aussi pour les transpositions $\sigma \circ \delta = \sigma \delta$

Théorème :

Toute permutation de S_n est un produit fini de transpositions.

En d'autres termes, le groupe S'_n est engendré par ses transpositions.

4 - Inversion :

Soit σ une permutation de S_n , on appelle inversion de deux éléments

un élément de σ qui vérifie: $i < j$; $\sigma(i) > \sigma(j)$
 et on pose: $I(\sigma) = \text{Card}\{f(i, j) \in \{1, 2, \dots, n\} / i < j \text{ et } \sigma(i) > \sigma(j)\}$

Exemples

Trouvons $I(\sigma)$ pour chacun des cas suivants:

$$1 \backslash \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 4 & 5 & 1 & 6 & 7 \end{pmatrix}$$

on a: * $1 < 5 \Rightarrow \sigma(1) = 2 > \sigma(5) = 1$

* $2 < 5 \Rightarrow \sigma(2) = 3 > \sigma(5) = 1$

* $3 < 5 \Rightarrow \sigma(3) = 4 > \sigma(5) = 1$

* $4 < 5 \Rightarrow \sigma(4) = 5 > \sigma(5) = 1$

donc: $I(\sigma) = 4$

$$2 \backslash \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 3 & 4 & 5 & 2 & 6 & 7 \end{pmatrix}$$

on a: * $2 < 5 \Rightarrow \sigma(2) = 3 > \sigma(5) = 2$

* $3 < 5 \Rightarrow \sigma(3) = 4 > \sigma(5) = 2$

* $4 < 5 \Rightarrow \sigma(4) = 5 > \sigma(5) = 2$

donc: $I(\sigma) = 3$

$$3 \backslash \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 4 & 5 & 3 & 6 & 7 \end{pmatrix}$$

on a: * $3 < 5 \Rightarrow \sigma(3) = 4 > \sigma(5) = 3$

* $4 < 5 \Rightarrow \sigma(4) = 5 > \sigma(5) = 3$

donc: $I(\sigma) = 2$

$$4 \backslash \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{pmatrix}$$

donc: $I(\sigma) = 0$

$$5 \backslash \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 6 & 4 & 2 & 3 & 5 & 7 \end{pmatrix}$$

on a: * $2 < 3 \Rightarrow \sigma(2) = 6 > \sigma(3) = 4$

* $2 < 4 \Rightarrow \sigma(2) = 6 > \sigma(4) = 2$

* $2 < 5 \Rightarrow \sigma(2) = 6 > \sigma(5) = 3$

* $2 < 6 \Rightarrow \sigma(2) = 6 > \sigma(6) = 5$

* $3 < 4 \Rightarrow \sigma(3) = 4 > \sigma(4) = 2$

* $3 < 5 \Rightarrow \sigma(3) = 4 > \sigma(5) = 3$

donc: $I(\sigma) = 6$

$$6 \backslash \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 3 & 6 & 5 & 1 \end{pmatrix}$$

on a: * $1 < 6 \Rightarrow \sigma(1) = 2 > \sigma(6) = 1$

$$2 < 3 \Rightarrow \sigma(2) = 4 > \sigma(3) = 3$$

$$2 < 6 \Rightarrow \sigma(2) = 4 > \sigma(6) = 1$$

$$3 < 6 \Rightarrow \sigma(3) = 3 > \sigma(6) = 1$$

$$4 < 5 \Rightarrow \sigma(4) = 6 > \sigma(5) = 5$$

$$4 < 6 \Rightarrow \sigma(4) = 6 > \sigma(6) = 1$$

$$5 < 6 \Rightarrow \sigma(5) = 5 > \sigma(6) = 1$$

donc $I(\sigma) = 7$

5 - Signature:

On appelle signature de σ l'entier qui vaut -1 ou 1 , défini par :

$$\varepsilon(\sigma) = (-1)^{I(\sigma)}$$

X Exercices:

1) Soit τ une transposition de S_m , montrer que : $\varepsilon(\tau) = -1$

2) Montrer que : $E : (S_n, \circ) \rightarrow (\{-1, 1\}, \times)$ est un morphisme de groupes.

2) b - Démontrer que : $E(\gamma\sigma) = E(\gamma)E(\sigma)$ pour toute permutation γ et σ de S_m .

Corollaire:

Si σ se décompose d'une part en un produit de m transpositions, et d'autre part en un produit de m' transpositions, alors m et m' sont de même parité.

$E(\sigma) = (-1)^m$, avec m est le nombre de transpositions d'une décomposition quelconque de σ en produit de transpositions.

6 - Support et orbites:

Définition: Support

Pour toute $\sigma \in S_m$, on appelle support de σ , l'ensemble des éléments de $\{1, 2, \dots, m\}$ qui ne sont pas fixés par σ :

$$\text{Supp } \sigma = \{i \in \{1, \dots, m\} / \sigma(i) \neq i\}$$

Exemple:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 4 & 5 & 1 & 7 & 6 & 3 \end{pmatrix} \Rightarrow \text{Supp } \sigma = \{1, 2, 3, 4, 5, 7\}$$

X Zemme:

$\forall \sigma \in S_m$ non trivial, la restriction de σ est une permutation de groupe G

Preuves à démontrer

X Exercice:

Soient: $\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 6 & 5 & 4 & 1 \end{pmatrix}$ et $\sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 4 & 5 & 1 & 2 \end{pmatrix}$

Calculer $\sigma_1 \circ \sigma_2$ et $\sigma_2 \circ \sigma_1$

* $\sigma_1 \circ \sigma_2$:

$$1 \xrightarrow{\sigma_2} 3 \xrightarrow{\sigma_1} 6$$

$$2 \xrightarrow{\sigma_2} 6 \xrightarrow{\sigma_1} 1$$

$$3 \xrightarrow{\sigma_2} 4 \xrightarrow{\sigma_1} 5 \quad \text{Alors:}$$

$$4 \xrightarrow{\sigma_2} 5 \xrightarrow{\sigma_1} 4 \quad \sigma_1 \circ \sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 1 & 5 & 4 & 2 & 3 \end{pmatrix}$$

$$5 \xrightarrow{\sigma_2} 1 \xrightarrow{\sigma_1} 2$$

$$6 \xrightarrow{\sigma_2} 2 \xrightarrow{\sigma_1} 3$$

* $\sigma_2 \circ \sigma_1$:

$$1 \xrightarrow{\sigma_1} 2 \xrightarrow{\sigma_2} 6$$

$$2 \xrightarrow{\sigma_1} 3 \xrightarrow{\sigma_2} 4$$

$$3 \xrightarrow{\sigma_1} 6 \xrightarrow{\sigma_2} 2 \quad \text{Alors:}$$

$$4 \xrightarrow{\sigma_1} 5 \xrightarrow{\sigma_2} 1$$

$$5 \xrightarrow{\sigma_1} 4 \xrightarrow{\sigma_2} 5$$

$$6 \xrightarrow{\sigma_1} 1 \xrightarrow{\sigma_2} 3$$

$$\sigma_2 \circ \sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 4 & 2 & 1 & 5 & 3 \end{pmatrix}$$

X Propositions

Deux permutations de S_n dont les supports sont disjoint commutent.

Preuve: à démontrer

Définition: Orbite:

Soit $\sigma \in S_n$ et $i \in \{1, 2, \dots, n\}$; on appelle σ -orbite de i l'ensemble des images de i par les différents éléments du groupe cyclique $\langle \sigma \rangle$.

$$\text{on note: } \mathcal{O}_\sigma(i) = \{\sigma^k(i), k \in \mathbb{Z}\}.$$

Exemple:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix} \Rightarrow \mathcal{O}_\sigma(1) = \{2, 4, 1\}$$

$$\text{en effet: } \sigma(1) = 2; \sigma^2(1) = 4; \sigma^3(1) = 1$$

Structures Algébriques

Groupe Quotient

I - Classe de Conjugaison :

1- Définition : Conjugué :

Soit G un groupe,

Soient $g, g' \in G$,

on dit que g' est conjugué de g si : $\exists x \in G / g' = xgx^{-1}$

X Remarque

La relation "être conjugué dans G " est une relation d'équivalence
Preuve à démontrer

2- Définition : Classe de Conjugaison :

La classe de conjugaison de g est la classe d'équivalence de g
pour la relation de conjugaison

3- Sous-groupe normale :

Soit G un groupe,

Soit H un sous-groupe de G ,

on dit que H est un sous-groupe normale / distingué dans G

Parce que : $\forall x \in G : xHx^{-1} = H$

on note $H \triangleleft G$

4- Classe modulo d'un sous-groupe :

Soit G un groupe,

Soit H un sous-groupe de G ,

$\forall x \in G$ on note : $xH = \{xh / h \in H\}$ et $Hx = \{hx / h \in H\}$

Si sous-ensemble xH (resp. Hx) s'appelle la classe à gauche
(resp. à droite) de x modulo H .

X Lemme :

Soient G un groupe et H un sous-groupe de G ,

$\forall x, y \in G$ on a : $(xH = yH) \Leftrightarrow x^{-1}y \in H$ et $(Hx = Hy) \Leftrightarrow xy^{-1} \in H$

i) Ces classes à gauche (resp. à droite) modulo H forment une partition de G ;

ii) L'ensemble des classes à droite modulo H est une bijection avec

l'ensemble des classes à gauche modulo H ;

iii) Pour tout H sous-groupe de G : $(H \Delta G) \Leftrightarrow (xH = Hy, \forall x \in G)$

Preuve:

$$\text{Mq } (xH = yH) \Leftrightarrow x^{-1}y \in H$$

$$\text{on a: } (xH = yH) \Leftrightarrow (xh = yh', \forall h, h' \in H)$$

$$\text{Soient } h, h' \in H: \quad xh = yh' \Rightarrow xhh'^{-1} = yh'h'^{-1}$$

$$\Rightarrow xhh'^{-1} = y$$

$$\Rightarrow x^{-1}xhh'^{-1} = x^{-1}y$$

$$\Rightarrow x^{-1}y = hh'^{-1} \in H$$

$$\Rightarrow x^{-1}y \in H$$

$$\text{donc: } (xH = yH) \Rightarrow x^{-1}y \in H$$

II - Congruence modulo un sous-groupe normal:

1 - Définition: Ensemble quotient?

Soient G un groupe et H sous-groupe distingué de G ,

la relation binaire définie pour G par: $\forall x, y \in G: x \equiv y$ lorsque $xy^{-1} \in H$ est une relation d'équivalence dans G appelée la congruence modulo H ou encore l'équivalence modulo H .

Les classes d'équivalence vérifient: $\forall x \in G: \bar{x} = xH = Hx$

L'ensemble quotient de G par la relation d'équivalence modulo H est noté G/H , et on a: $G/H = \{\bar{x}; x \in G\}$

Exemple:

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

X Théorème 1:

Soient G un groupe et $H \Delta G$.

on définit une LCI ".:" dans G/H par: $\forall \bar{x}, \bar{y} \in G/H: \bar{x} \cdot \bar{y} = \bar{x.y}$

i) $(G/H, :)$ est un groupe appelé groupe quotient de G par H ;

ii) La surjection canonique $p: G \rightarrow G/H$ est un morphisme de groupe dans le groupe quotient G/H : $p: G \rightarrow G/H$

$$x \mapsto \bar{x}$$

Preuve & Triviale

X Théorème 2:

Soient G et G' deux groupes,

Soit $f: G \rightarrow G'$ un morphisme de groupes,

le groupe quotient de G par le sous-groupe normal $\text{Ker } f$ est isomorphe au sous-groupe $\text{Im } f$ de G' .

$$\begin{array}{ccc} f: & G & \longrightarrow G' \\ & \downarrow & \downarrow \\ \varphi: & G/\text{Ker } f & \longrightarrow \text{Im } f \end{array}$$

φ est un homomorphisme bijectif.

Preuve :

Soit $\bar{x} \in G/\text{Ker } f$,

on pose : $\varphi(\bar{x}) = f(x)$

1) montrons que φ est bien définie :

$$\text{on a: } \bar{x} = \bar{y} \Rightarrow x \bar{y}^{-1} y$$

$$\Rightarrow x^{-1} y \in \text{Ker } f$$

$$\Rightarrow f(x^{-1} y) = e_{G/\text{Ker } f}$$

$$\Rightarrow (f(x))^{-1} f(y) = e_{G/\text{Ker } f}$$

$$\Rightarrow f(y) = f(x)$$

$$\Rightarrow \varphi(\bar{y}) = \varphi(\bar{x})$$

2^e méthode

$$\text{Soient } \bar{x}, \bar{y} \in G/\text{Ker } f : \bar{x} = \bar{y}$$

d'où $\forall x \in \bar{x} : x \in \bar{y}$

$$\text{on a: } \varphi(\bar{x}) = f(x)$$

comme $x \in \bar{y}$,

$$\text{donc: } \varphi(\bar{y}) = f(x)$$

$$\text{d'où: } \varphi(\bar{x}) = \varphi(\bar{y})$$

d'où : φ est bien définie.

2) montrons que φ est un morphisme :

Soient $\bar{x}, \bar{y} \in G/\text{Ker } f$,

$$\text{on a: } \varphi(\bar{x} \cdot \bar{y}) = \varphi(\bar{x}\bar{y}) = f(xy)$$

comme f est un morphisme, donc : $f(xy) = f(x) \cdot f(y)$

$$\text{d'où: } \varphi(\bar{x} \cdot \bar{y}) = f(x) \cdot f(y) = \varphi(\bar{x}) \cdot \varphi(\bar{y})$$

donc : φ est un morphisme.

3) montrons que φ est bijective :

* Surjectivité :

Soit $y \in \text{Im } f$,

$$\text{d'où: } \exists x \in G / y = f(x) = \varphi(\bar{x})$$

$$\text{c.-à-d: } \exists \bar{x} \in G/\text{Ker } f : y = \varphi(\bar{x})$$

donc : φ est surjective.

* Injectivité :

Soient $\bar{x}, \bar{y} \in G/\text{Ker } f$ tels que: $\varphi(\bar{x}) = \varphi(\bar{y})$

on a: $\varphi(\bar{x}) = \varphi(\bar{y}) \Rightarrow f(x) = f(y)$

$$\Rightarrow e' = (f(x))^{-1}f(y) \text{ où } e' \text{ l'élément neutre de } G'$$

$$\Rightarrow f(x^{-1})f(y) = e'$$

$$\Rightarrow f(x^{-1}y) = e'$$

$$\Rightarrow x^{-1}y \in \text{Ker } f$$

$$\Rightarrow \bar{x}\bar{y} = \bar{e}$$

donc: φ est injective.

Alors: φ est bijective.

X Théorème: Propriété universelle du groupe quotient 3

Soient G un groupe, $H \trianglelefteq G$ et $p: G \rightarrow G/H$ la surjection canonique.

$\forall G'$ un groupe et pour tout morphisme $f: G \rightarrow G'$ tel que $H \subset \text{Ker } f$,
il existe un unique morphisme $\varphi: G/H \rightarrow G'$ tel que $f = \varphi \circ p$

$$\begin{array}{ccc} G & \xrightarrow{f} & G' \\ p \downarrow & \nearrow \varphi & \\ G/H & & \end{array}$$

Preuve 3:

Soit $\bar{x} \in G/H$,

on pose: $\varphi(\bar{x}) = f(x)$

φ est bien définie (par coïncidence),

supposons qu'il existe φ' tel que: $f = \varphi' \circ p = \varphi' \circ p$

on a: $\forall \bar{x} \in G/H: \varphi'(\bar{x}) = f(x)$ et $\varphi(\bar{x}) = f(x)$

d'où: $\varphi' = \varphi$

X Propositions:

i) Si f est surjective, alors: φ est surjective;

ii) Si $H = \text{Ker } f$, alors: φ est injective

Preuve i:

i) Si f est surjective: $\forall y \in G', \exists x \in G: y = f(x)$

on prend: $\bar{x} = p(x)$

on a: $y = f(x) = \varphi(p(x)) = \varphi(\bar{x})$ d'où la surjectivité.

Structures Algébriques

Anneaux et Corps

I - Notion d'anneau

1 - Définition :

Un anneau (A, T, \perp) est un ensemble muni de deux opérations T et \perp vérifiant les propriétés suivantes :

i) (A, T) est un groupe abélien.

ii) La loi " \perp " est associative, c.-à-d. $\forall x, y, z \in A$:

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

iii) La loi " \perp " est distributive par rapport à la loi " T ", c.-à-d

$$\forall x, y, z \in A: x \perp (y T z) = (x \perp y) T (x \perp z)$$

$$\text{et: } (x T y) \perp z = (x \perp z) T (y \perp z)$$

* Si de plus " \perp " est commutative dans A , c.-à-d: $\forall x, y \in A$.

$x \perp y = y \perp x$, alors l'anneau est dite commutatif

* Si l'anneau admet un élément neutre qu'on note 1_A pour

La loi " \perp ", c.-à-d: $\forall x \in A: x \perp 1_A = 1_A \perp x = x$, alors l'anneau est dite unitaire.

Exemple :

* $(\mathbb{Z}, +, \times)$ est un anneau unitaire,

$\mathbb{Z}/6\mathbb{Z} = \mathbb{Z}$

$\mathbb{Z}/12\mathbb{Z} = \mathbb{Z}_0$

$(\mathbb{R}, +, \times)$

$(\mathbb{C}, +, \times)$

* $(\mathbb{Z}/p\mathbb{Z}, +, \times)$, $\forall p \in \mathbb{N}^* \setminus \{1\}$ est un anneau unitaire,

* L'ensemble des polynômes $(\mathbb{Z}[X], +, \times)$ est un anneau unitaire,

à coefficients dans \mathbb{A}

* $(M_2(\mathbb{R}), +, \times)$ est un anneau,

* $(\mathbb{F}(I, \mathbb{R}), +, \times)$ est un anneau,

* Soit A un anneau,

à coefficients dans A $B = (A_m)$ l'ensemble des suites de A qui sont à "support fini", c.-à-d dont les termes sont nuls sauf un nombre fini d'entre eux.

On note: $0_B = (0_A, \dots, 0_A)$

Pour tout $f = (a_m)_m$, on appelle degré de f le plus grand entier $n \in \mathbb{N}$

tel que $a_m \neq 0$

on définit "+" et " \times " dans B ,

en posons $\forall f = (a_n)_{n \in \mathbb{N}}$ et $\forall g = (b_n)_{n \in \mathbb{N}}$:

$$(f+g) = (a_n + b_n)_{n \in \mathbb{N}} \text{ et } (f \times g) = (c_n)_{n \in \mathbb{N}} \text{ avec } c_n = \sum_{k=1}^n a_k b_{n-k}$$

$(B, +, \times)$ est un anneau commutatif.

* \mathbb{Z} 'Anneau $\Lambda[X]$:

Pour tout anneau A commutatif des polynômes à 1 indéterminée à coefficients dans A forment un anneau commutatif unitaire noté $A[X]$. Son élément neutre est 0_A pour la 1^{ère} loi et 1_A pour la 2^{ème}.

Pour tout éléments non nul P de $A[X]$, il existe un unique entier naturel n et un unique $(n+1)$ -uplet (a_0, a_1, \dots, a_n) d'éléments de A tel que: $P = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ avec $a_n \neq 0$

L'entier n est appelé le degré de P noté $\deg P$,

L'élément a_n de A est appelé le coefficient dominant de P noté $\text{cd}(P)$,

Par convention: $\deg 0 = -\infty$ et $\text{cd}(0) = 0$

Deux polynômes $P = \sum_{i=0}^m a_i x^i$ et $Q = \sum_{i=0}^n b_i x^i$ sont égaux

$$\Leftrightarrow m = n \text{ et } a_i = b_i, \forall i \in \{0, \dots, n\}$$

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

$$\text{et: } P \cdot Q = \sum_{i=0}^{\max(m,n)} \left(\sum_{j=0}^i a_j b_{i-j} \right) x^i$$

$$\text{d'où: } \deg(P+Q) \leq \max(\deg(P), \deg(Q))$$

$$\deg(PQ) = \deg(P) + \deg(Q)$$

2- Sous anneau: Définition

Soit $(A, +, \times)$ un anneau,

on dit que B est un sous-anneau de A si:

i) $(B, +)$ est un sous-groupe de $(A, +)$

ii) B est stable par la loi " \times ": $\forall x, y \in B: xy \in B$

X Exercice 8

Mq $\mathbb{Z}[i]$ est un sous-anneau de $(\mathbb{C}, +, \times)$, avec:

$$\mathbb{Z}[i] = \{a + ib / a, b \in \mathbb{Z}\}$$

i) on a:

* $\mathbb{Z}[i] \neq \emptyset$ car $0_{\mathbb{C}} \in \mathbb{Z}[i]$ (en effet: $0_{\mathbb{C}} = 0 + i0$ et $0 \in \mathbb{Z}$)

* Soient $x, y \in \mathbb{Z}[i]$ tels que: $x = a + ib$ et $y = c + id$ où $a, b, c, d \in \mathbb{Z}$

on a: $x + (-y) = a + ib - c - id$

$$= \underbrace{(a - c)}_{\in \mathbb{Z}} + i \underbrace{(b - d)}_{\in \mathbb{Z}}$$

d'où: $x + (-y) \in \mathbb{Z}[i]$

donc: $(\mathbb{Z}[i], +)$ est un sous-groupe de $(\mathbb{C}, +)$

ii) Soient $x, y \in \mathbb{Z}[i]$ tels que: $x = a + ib$ et $y = c + id$ où $a, b, c, d \in \mathbb{Z}$

on a: $x \cdot y = (a + ib) \cdot (c + id)$

$$\begin{aligned} &= ac + iad + ibc + i^2 bd \\ &= ac + i(ad + bc) - bd \\ &= \underbrace{(ac - bd)}_{\in \mathbb{Z}} + i \underbrace{(ad + bc)}_{\in \mathbb{Z}} \end{aligned}$$

d'où: $x \cdot y \in \mathbb{Z}[i]$

Alors: $(\mathbb{Z}[i], +, \cdot)$ est un sous-anneau de $(\mathbb{C}, +, \cdot)$.

3- Propriétés:

Soit A un anneau,

* $\{0_A\}$ et A sont des sous-anneaux triviaux de A ,

* B est un sous-anneau de $A \Leftrightarrow B$ est un anneau $\subset A$

Remarque? Soit A un anneau,

$(A_n[X], +, \cdot)$ où $A_n[X]$ l'ensemble des polynômes à coefficients dans A et de degré $\leq n$, n est pas un anneau, car $A_n[X]$ n'est pas stable par " x "

4- Groupes des unités d'un anneau:

a- Définitions:

Le groupe des unités d'un anneau A est l'ensemble des éléments de A qui sont inversibles.

$$U(A) = \{x \in A \mid \exists y \in A, xy = 1_A\}$$

b- Exemples:

$$U(\mathbb{Z}) = \{-1, 1\}$$

$$U(\mathbb{Q}) = \mathbb{Q}^\times$$

$$U(\mathbb{Z}[i]) = \{i, -i, -1, 1\}$$

5 - Corps

Si $\mathcal{U}(A) = A^* = A \setminus \{0_A\}$, alors A est dite un corps.

a - Propositions

$(A, +, \times)$ est un corps \Leftrightarrow $\begin{cases} (A, +) \text{ est un groupe commutatif} \\ (A^*, \times) \text{ est un groupe} \\ "\times" \text{ est distributive par rapport à "+"} \end{cases}$

6 - Sous-corps

Sous K un corps,

on dit que H est un sous-corps de K si :

- * $H \subset K$
- * H est un sous-anneau de K
- * tout élément non nul de H sont inversibles

7 - Intégrité

Un anneau $(A, +, \times)$ est dite intégrée si : $x \times y = 0 \Leftrightarrow x = 0$ ou $y = 0$

~~X~~ Exercice à montrer que :

1/ $\mathbb{Z}/p\mathbb{Z}$ est un corps $\Leftrightarrow p$ est premier $\Leftrightarrow \mathbb{Z}/p\mathbb{Z}$ est intègre

2/ $A[X]$ est intègre $\Leftrightarrow \mathcal{U}(A[X]) = \mathcal{U}(A)$

3/ $A[X]$ est un corps $\Leftrightarrow A$ est un corps

8 - Morphisme d'anneau

Soient $(A, +, \times)$ et (B, \perp, T) deux anneaux unitaires,

Une morphisme f de $(A, +, \times)$ vers (B, \perp, T) est une application qui vérifie : $\forall x, y \in A$:

- * $f(x+y) = f(x) \perp f(y)$
- * $f(x \times y) = f(x) T f(y)$
- * $f(1_A) = 1_B$

a - Propositions

Les caractéristiques de l'anneau A sont identiques à celle de B si

$A \xrightarrow{f} B$ avec f un morphisme :

- * Si K est un sous-anneau de A , alors $f(K)$ est un sous-anneau de B ,
- * Si H est un sous-anneau de B , alors $f^{-1}(H)$ est un sous-anneau de A ,

9 - Idéal

a - Définition

Soit A un anneau,

I est un idéal si et seulement si I est un sous-groupe additive

$$\forall x \in I, \forall a \in A, ax \in I$$

X b-propositions:

Si $1_A \in I$, alors $I = A$

Si $\exists x \in U(A)$; $x \in I$, alors $I = A$

Preuve:

* $I \subseteq A$, car I est un sous-groupe de A ,

$$\forall x \in A, \text{ on a: } x = x \cdot 1_A \in I$$

$$\text{donc: } x \in I$$

Par conséquent $A \subseteq I$.

* $I \supseteq A$, car I est un sous-groupe de A ,

Soit $x \in U(A)$,

$$\exists y \in A, 1_A = \sum_{i=1}^n y_i \in I$$

$$\text{donc: } A = I$$

c-propositions

Soient A et B deux anneaux commutatifs unitaires,

$f: A \rightarrow B$ un morphisme d'anneau unitaire

Si J un idéal de B , alors $f^{-1}(J)$ est un idéal de A .

$\forall I$ idéal de A , $f(I)$ est un idéal de $\text{Im } f(f(A))$

Ker f est un idéal de A

d-propositions:

Soient I et J deux idéaux de A ,

on a:

* $I \cup J$ n'est pas forcément un idéal,

* $IJ = \{a / a = \sum x_i y_i \text{ avec } x_i \in I \text{ et } y_i \in J\}$ est un idéal de A ,

* $I + J = \{x + y / x \in I \text{ et } y \in J\}$ est un idéal de A ,

e-Cas particulier d'idéaux:

Soient A un anneau et $x \in A$,

$$xA = \{xa / a \in A\}$$

c'est le plus petit idéal qui contient x , c'est l'idéal engendré par x

Quotient d'un anneau idéaux

Soient A un anneau commutatif unitaire et I un idéal de A , on considère le groupe quotient A/I définie par :

$$A/I = \{ b \in A / a - b \in I \}$$

et on a : $\bar{a} \in A/I \Leftrightarrow \bar{a} = a + I$ ($\bar{a} + \bar{b} = \overline{a+b}$ et $\bar{a} \cdot \bar{b} = \overline{ab}$)

$(A/I, +, \cdot)$ est un anneau commutatif unitaire,

et on a : $p: A \rightarrow A/I$ est un homéomorphisme d'anneau

Théorème :

Soient A et A' deux anneaux commutatifs unitaires, et

$f: A \rightarrow A'$ un morphisme d'anneau.

Alors : $A/I \cong \text{Im}(f) \subset A'$

$$\begin{array}{ccc} f: A & \longrightarrow & A' \\ \downarrow & & \downarrow \\ A/I & \xrightarrow{\text{isomorphisme}} & f(A) \end{array}$$

Définition :

* M est dite un idéal maximal si $\exists I$ un idéal de A , si $M \subset I$, alors $I = A$

* Un idéal P est dit premier : $\forall x, y \in A / xy \in P$, alors $x \in P$ ou $y \in P$