1. Cours 1: Arithmétique dans $\mathbb{Z}$

2. Cours 2: Fonctions et Applications

3. Cours 3: Relations

4. Cours 4: Quelques structures algébriques

4.0.1 Lois de composition intrene:

On appelle lois de composition interne (ou opération binaire) sur un ensemble non vide E , toute application $*$ de $E \times E$ dans E.

** L'image $*(x,y)$ est souvent notée $x * y$ (ou xy s'il n'y a pas de confusion)*

Exemple 1: L'addition uselle $+$ est une lois de composition interne sur $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$,$\mathbb{R}$ et $\mathbb{C}$.

Le multiplication usuelle $\times$ est une lois de composition interne sur $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$,$\mathbb{R}$ et $\mathbb{C}$

La soustraction $-$ est une lois de composition interne sur $\mathbb{Z}$, $\mathbb{Q}$,$\mathbb{R}$ et $\mathbb{C}$, mais pas sur $\mathbb{N}$.

Exemple 2: L'addition uselle $+$ sur l'ensemble $B = \{0,1\}$ n'est pas une lois de composition interne. En effet:

(x,y)	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$+(x,y)$	0	1	1	$2 \notin B$

Le multiplication usuelle $\times$ sur l'ensemble $B = \{0,1\}$ est une lois de composition interne. En effet

(x,y)	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$\times(x,y)$	0	0	0	1

Exemple 3: Le produit scalaire $\diamond : \mathbb{R}^2 \times \mathbb{R}^2 \to \mathbb{R}$ défini par $\begin{pmatrix} x \\ y \end{pmatrix} \diamond \begin{pmatrix} x' \\ y' \end{pmatrix} = xx' + yy'$ n'est pas une lois de composition interne.

Exemple 4: La composition $\circ$ est une lois de composition interne sur $A(E,E)$, l'ensemble des applications de E dans E. En effet: Si $f : E \to E$ et $g : E \to E$ sont deux applications alors $f \circ g : E \to E$ est une application.

Exemple 5: L'intersection $\cap$ est une lois de composition interne sur $\mathcal{P}(E)$, l'ensemble des parties de E .

4.0.2 Définitions:

Un ensemble non vide E muni d'une ou plusieurs lois de composition internes est appelé structure algébrique.

** Si les lois sont notées $*_1, *_2, ..., *_n$, alors la structure,algébrique est notée $(E, *_1, *_2, ..., *_n)$*

Exemple 1**:** $(\mathbb{N}, +), (\mathbb{Z}, +, -), (\mathbb{R}, +, \times), (A(E, E), \circ)$ et $(\mathcal{P}(E), \cap)$ sont des strucrures algébriques.

Exemple 4**:** $(\mathbb{N}, -, \times), (\mathbb{R}^2, \diamond)$, ne sont pas des strucrures algébriques.

4.0.3 Définitions: *Soit $*$ une lois de composition interne sur un ensemble non vide E. Alors:*

1) On dit que la lois $*$ est associative, si pour tous x, y, z de E, ona $(x * y) * z = x * (y * z)$

2) Un élément e de E est dit élément neutre (ou élément unité) de $*$, si pour tout x de E, on a $x * e = x = e * x$

3) Si e est l'élément neutre de $*$, on dit qu'un élément x de E est inversible (ou symétrisable), s'il existe un élément x' de E tel que $x' * x = e = x * x'$

** x' est appelé inverse (ou symétrique) de x et est noté x^{-1}.*

4) On dit que la lois $*$ est commutative, si pour tous x, y de E, ona $x * y = x * y$

4.0.3.1 Remarque: Si la lois $*$ est associative les parethèses, on peut écrire $x * y * z$ au lieu de $(x * y) * z$ et $x * (y * z)$

Exemple 1: L'addition uselle $+$ sur sur $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$,$\mathbb{R}$ et $\mathbb{C}$ est une lois associative, commutative, et elle admet 0 comme élément neutre, et dans $\mathbb{Z}$, $\mathbb{Q}$,$\mathbb{R}$ et $\mathbb{C}$ tout élément x possède $-x$ comme symétrique (inverse).

Dans $\mathbb{N}$, le seul élément symétrisable pour l'addition usuelle est 0.

Le multiplication usuelle $\times$ sur $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$,$\mathbb{R}$ et $\mathbb{C}$ est une lois associative et commutative admettant 1 comme élément neutre, et dans $\mathbb{Q}^*$,$\mathbb{R}^*$ et $\mathbb{C}^*$ tout élément x possède $\frac{1}{x}$ comme inverse (symétrique). L'élément 0 n'a pas d'inverse pour le multiplication usuelle $\times$.

Dans $\mathbb{Z}$, les seuls éléments inversibles pour la multiplication usuelle sont-1et1

Exemple 2: L'opération $\intercal$ définie sur $\mathbb{Z}$ par $n \intercal m = -n - m$ est commutative mais non associative et n'admet pas d'élément neutre. ($0 = (1 \intercal 2) \intercal 3 \neq 1 \intercal (2 \intercal 3) = 4$)

Exemple 3: La composition $\circ$ sur $A(E, E)$, est une lois associative, admettant Id_E comme élément neutre, et les seuls éléments inversibles sont les applications bijectives. ($(f \circ g) \circ h = f \circ (g \circ h)$, $f \circ Id_A = f = Id_A \circ f$, f^{-1}l'application réciproque de f est l'inverse de f pour la composition car $f \circ f^{-1} = Id_A = f^{-1} \circ f$)

La composition $\circ$ n'est pas commutative si E contient au moins deux éléments.

Exemple 4: L'intersection $\cap$ sur $\mathcal{P}(E)$ l'ensemble des parties de E est une lois associative et commutative, admettant E comme élément neutre, et le seul élément inversible est bien E. $((X \cap Y) \cap Z = X \cap (Y \cap Z)$, $X \cap E = X = E \cap X$, si $X \neq E$, on ne peut pas trouver X' vérifiant $X \cap X' = E$, ça marche seulement pour $X = E$.

4.0.4. Théorème: *Soit E un ensemble muni d'une lois de composition interne $*$, alors*

1) L'élément neutre e, s'il existe, il est unique.

2) Si $*$ est associative et admet un élément neutre e, alors

l'élément inverse x^{-1} de x, s'il existe il est unique, de plus $(x^{-1})^{-1} = x$ et $(x * y)^{-1} = y^{-1} * x^{-1}$ (si y^{-1} existe aussi).

Preuve: 1) Supposons e' un autre élément neutre de $*$, alors $e * e' = e$ et comme e est aussi un élément neutre alors $e * e' = e'$, d'où l'égalité $e' = e$.

2) Supposons $\overline{x}$ un autre inverse de x, alors $\overline{x} * x = e$, ainsi $x^{-1} = (\overline{x} * x) * x^{-1} = \overline{x} * (x * x^{-1}) = \overline{x}$ donc l'inverse est unique.

On a $x * x^{-1} = e = x^{-1} * x$, et puisque linverse est unique, alors x est l'inverse de x^{-1}, c.à.d $(x^{-1})^{-1} = x$.

On a aussi $(y^{-1} * x^{-1}) * (x * y) = y^{-1} * x^{-1} * x * y = e$ et puisque linverse est $(x * y) * (y^{-1} * x^{-1}) = x * y * y^{-1} * x^{-1} = e$ unique, alors $y^{-1} * x^{-1}$ et l'inverse de $x * y$, c.à.d $(x * y)^{-1} = y^{-1} * x^{-1}$.

4.1. Structure de groupe

4.1.1. Demi groupe et monoïde:

1) On appelle demi groupe tout ensemble non vide E muni d'une loi de composition interne associative $*$.

2) On appelle monoïde (ou demi groupe unitaire) tout demi groupe $(E, *)$ ayant un élément neutre e.

Si en plus $*$ est commutative, le monoïde est dit commutatif.

Exemple 1: Les structures $(\mathbb{N}, +)$, $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$,$(\mathbb{R}, +)$ et $(\mathbb{C}, +)$ sont des monoïdes commutatifs.

Les structures $(\mathbb{N}, \times)$, $(\mathbb{Z}, \times)$, $(\mathbb{Q}, \times)$,$(\mathbb{R}, \times)$ et $(\mathbb{C}, \times)$ sont des monoïdes commutatifs.

Exemple 2: $(A(E, E), \circ)$, est un monoïde non commutatif si $card(E) > 1$.

Exemple 3: $(\mathcal{P}(E), \cap)$ est un monoïde commutatif.

Exemple 4: $(n\mathbb{Z}, \times)$ est seuelement un demi groupe pour $|n| > 1$.

Exemple 5: $(\mathbb{Z}, \intercal)$ telle que $n \intercal m = -n - m$, n'est même pas un demi groupe.

4.1.1. Groupe: *On appelle groupe tout monoïde* $(G, *)$ *dont tous les éléments sont inversibles.*

Autrement dit: $(G, *)$ *est un groupe si l'opération* $*$ *est associative, et admet un élément neutre* e *et tout élément de* G *est inversible (symétrisable).*

Si en plus $*$ *est commutative, le groupe est dit commutatif ou abélien.*

*Le cardinal de G est appelé ordre du groupe $(G, *)$ et est noté $Card(G)$ où $|G|$

Exemple 1: Les structures $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$,$(\mathbb{R}, +)$ et $(\mathbb{C}, +)$ sont des groupes commutatifs.

Les structures , $(\mathbb{Q}, \times)$,$(\mathbb{R}, \times)$ et $(\mathbb{C}, \times)$ ne sont pas des groupes (L'élément 0 n'a pas d'inverse pour la multiplication usuelle $\times$)

Les structures , $(\mathbb{Q}^*, \times)$,$(\mathbb{R}^*, \times)$ et $(\mathbb{C}^*, \times)$ sont des groupes commutatifs.

Les structures , $(\mathbb{N}, +)$, $(\mathbb{N}, \times)$, $(\mathbb{Z}, \times)$ ne sont pas des groupes.

Exemple 2: $(A(E, E), \circ)$, n'est pas un groupe si $card(E) > 1$, et si on se restreint seulement à l'ensemble $S(E)$ des applications bijectives (inversibles) de E dans E, on aura un groupe. C.à.d $(S(E), \circ)$ est un groupe qui est non commutatif, si $card(E) > 2$. (Dans ce groupe l'inverse d'une application f est l'application réciproque f^{-1})

Exemple 3: $(\mathcal{P}(E), \cap)$ n'est pas un groupe si $E \neq \varnothing$. (l'inverse de $\varnothing$ n'existe pas)

4.1.2. Sous groupe: *On appelle sous groupe d'un groupe* $(G, *)$ *toute partie non vide* H *de* G *qui est elle même un groupe pour la lois* $*$ *restreinte à* H.

4.1.2.1. Proposition: *Une partie* H *de* G *est un sous groupe d'un groupe* $(G, *)$, *ssi*

1) H *contient l'élément neutre* e.

2) Pour tous x,$y \in H : x * y^{-1} \in H$.

Preuve: a) Supposons que H est un sous groupe de $(G, *)$, alors pour tous x et y dans H, on a y^{-1} et $x * y^{-1}$sont aussi dans H, d'où l'assertion 2). Pour l'assertion 1) il suffit de choisir un z de H ($H \neq \varnothing$) et appliquer 2) avec $x = z$ et $y = z$, on aura ainsi $e \in H$.

b) Supposons que H vérifie les assertions 1) et 2), alors H n'est pas vide ($e \in H$) et en choisissant dans l'assertion 2) $x = e$, on conclut que tout $y \in H$ a un inverse dans H, par conséquent pour tous $x, y \in H$, on a $x, y^{-1} \in H$ et par

application de 2), on conclut que $x * (y^{-1})^{-1} = x * y \in H$, ce qui assure que $*$ est bien une lois de composition interne sur H. Puisque $*$ demeure associative sur H, alors $(H, *)$ vérifie toutes les conditions d'un groupe, donc c'est bien un sous groupe de $(G, *)$. ■

Exemple 1: Si $(G, *)$ est un goupe, alors $\{e\}$ et G sont des sous groupes de G appelés sous groupes trivaux

Exemple 2: $(\mathbb{Z}, +)$ est un sous groupe de $(\mathbb{Q}, +)$ qui est un sous groupe de $(\mathbb{R}, +)$ et de $(\mathbb{C}, +)$.

Pour la multiplication $(\{-1, 1\}, \times)$ est un sous groupe de $(\mathbb{Q}^*, \times)$ qui est un sous groupe de $(\mathbb{R}^*, \times)$ et de $(\mathbb{C}^*, \times)$.

Exemple 3: Le cercle unité $S^1 = \{z \in \mathbb{C} \ / \ |z| = 1\}$ est un sous groupe de $(\mathbb{C}^*, \times)$. (l'élément neutre $1 \in S^1$, pour tous $z, z' \in S^1$, on $\left|z\left(z'\right)^{-1}\right| = \left|\frac{z}{z'}\right| = 1$, donc $z\left(z'\right)^{-1} \in S^1$).

Exemple 4: L'ensemble μ_n ($n \in \mathbb{N}^*$) des racines $n-ème$ complexes de l'unité 1 (C.à.d $\mu_n = \{z \in \mathbb{C} \ / \ z^n = 1\}$) est un sous groupe de cercle unité $(S^1, \times)$. (Si $z \in \mu_n$,alors $|z|^n = 1$ donc $|z| = 1$, donc $z \in S^1$, d'où l'inclusion $\mu_n \subset S^1$. On a aussi, l'élément neutre $1 \in \mu_n$, et pour tous $z, z' \in \mu_n$, on $\left(z\left(z'\right)^{-1}\right)^n = \frac{z^n}{z'^n} = 1$, donc $z\left(z'\right)^{-1} \in \mu_n$).

Exemple 5: $(n\mathbb{Z}, +)$ (où $n \in \mathbb{Z}$) est un sous groupe de $(\mathbb{Z}, +)$.(l'élément neutre $0 \in n\mathbb{Z}$, et pour tous $m, m' \in n\mathbb{Z}$, on $m + (-m') \in n\mathbb{Z}$).

4.1.3. Théorème: *Tous les sous groupes de* $(\mathbb{Z}, +)$ *sont de la forme* $(n\mathbb{Z}, +)$ *où* $n \in \mathbb{Z}$
La preuve de ce théorème est donnée dans le **cours 1 (Th.1.3.1)**

4.1.4. Théorème: *L'intersection quelconque de sous groupes d'un groupe* $(G, *)$, *est un sous groupe de* $(G, *)$.

C.à.d: *Si* $(H_i)_{i \in I}$ *est une famille de sous groupes d'un groupe* $(G, *)$, *alors* $\underset{i \in I}{\cap} H_i$ *est un sous groupe de* $(G, *)$.

Preuve: 1) Soit e l'élément neutre de $(G, *)$. Pour tout $i \in I$, on a $e \in H_i$, alors $e \in \underset{i \in I}{\cap} H_i$. 2) Si x, $y \in \underset{i \in I}{\cap} H_i$, alors pour tout $i \in I$, on a $x * y^{-1} \in H_i$, donc $x * y^{-1} \in \underset{i \in I}{\cap} H_i$. Par suite $\underset{i \in I}{\cap} H_i$ est un sous groupe de $(G, *)$ (Voir **Prop.4.1.2.1**).

4.1.5. Remarque: L'union quelconque de sous groupes d'un groupe $(G, *)$, n'est pas nécessairement un sous groupe de $(G, *)$.

4.1.6. Sous groupes engendrés : *Soit A une partie d'un groupe $(G,*)$.*

L'intersection de tous les sous groupes de G contenant A est appelé sous groupe engendré par A et est noté $Gr(A)$ ou $\langle A\rangle$.

* *La partie A est appelée partie génératrice de $Gr(A)$*

4.1.7. Théorème: *Soit A une partie d'un groupe $(G,*)$. Alors:*
1) *$Gr(A)$ est le plus petit*[1] *sous groupe de $(G,*)$, contenant A.*
2) *Si $A=\varnothing$, alors $Gr(A)=\{e\}$ et si $A\neq\varnothing$, alors*
$Gr(A)=\left\{a_1*a_2*...*a_p/p\in\mathbb{N}^*\text{et } a_i\in A \text{ ou } a_i^{-1}\in A\text{pour } i\in\{1,2,\ldots,p\}\right\}$

Preuve: 1) $Gr(A)$ est l'intersection de tous les sous groupes contenant A, alors il contient A et si un sous groupe H contient A, on a $H\cap Gr(A)=Gr(A)$, alors H contient $Gr(A)$, et $Gr(A)$ est le plus petit des sous groupes contenant A.

2) Si $A=\varnothing$, il est clair que $\{e\}$ contient A et c'est le plus petit sous groupe de G, donc $Gr(A)=\{e\}$.

Si $A\neq\varnothing$, soit
$H=\left\{a_1*a_2*...*a_P/p\in\mathbb{N}^*\text{et } a_i\in A \text{ ou } a_i^{-1}\in A\text{pour } i\in\{1,2,\ldots,p\}\right\}$

Pour un $a_1\in A\neq\varnothing$, on a $e=a_1*a_1^{-1}$, alors l'élément neutre $e\in H$ et si $a_1*a_2*...*a_p$, $a_1'*a_2'*...*a_p'\in H$, alors $(a_1*a_2*...*a_p)\left(a_1'*a_2'*...*a_p'\right)^{-1}=a_1*a_2*...*a_p*a_{p+1}*...*a_{p+p'}\in H$, car $a_i\in A$ ou $a_i^{-1}\in A$pour $i\in\{1,2,\ldots,p+p'\}$. Donc H est un sous groupe de G et il contient A, alors $Gr(A)\subset H$. Inversement, tous les éléments de la forme $a_1*a_2*...*a_p$ appartiennent à tout sous groupe contenant A, alors ils appartiennent à $Gr(A)$, d'où l'inclusion $H\subset Gr(A)$ et par suite l'égalité $H=Gr(A)$. ■

4.1.8. Définitions: *1) Un groupe engendré par une partie A finie est appelé groupe de type fini.*

2) Un groupe engendré par un seul élément a (C.à.d $A=\{a\}$) est appelé groupe monogène.

3) Un groupe monogène fini, est appelé groupe cyclique.

Exemple 1: Le groupe $(\mathbb{Z},+)$ est un goupe monogène, car $\mathbb{Z}=Gr(\{1\})=Gr(\{-1\})$ (Tout $n=\underbrace{1+1+...+1}_{n\ termes}$ si $n>0$, $0=1+(-1)$ et
$n=\underbrace{(-1)+(-1)+...+(-1)}_{n\ termes}$ si $n<0$)

Exemple 2: Le groupe μ_n ($n\in\mathbb{N}^*$) des racines $n-ème$ complexes de l'unité

[1] Plus petit au sens de l'inclusion

1 (C.à.d $\mu_n = \{z \in \mathbb{C} \ / \ z^n = 1\}$) est un groupe cyclique engendré par le complexe $a = \cos\left(\frac{2\pi}{n}\right) + i \sin\left(\frac{2\pi}{n}\right)$.(Tout élément de μ_n est de la forme $\cos\left(\frac{2\pi k}{n}\right) + i \sin\left(\frac{2\pi k}{n}\right)$ qui est égale à $a^k = \underbrace{a \times a \times ... \times a}_{k \ facteurs}$)

4.1.9. Puissances entières d'un élément : Dans un groupe $(G, *)$ d'élément neutre e , on définit pour tout élément a de G les puissances entières par:

$$a^0 = e \ et \ pour \ tout \ k \in \mathbb{N}^* : a^{k+1} = a^k * a \ et \ a^{-k} = \left(a^{-1}\right)^k$$

Avec ces notations, on a pour tous k, $k' \in \mathbb{Z}$:

$$a^k * a^{k'} = a^{k+k'} = a^{k'} * a^k \ , \ \left(a^k\right)^{k'} = a^{kk'} = \left(a^{k'}\right)^k \ et \ \left(a^k\right)^{-1} = a^{-k}$$

Attention Pour $a' \in G$, on n'a pas nécessairement $(a * a')^k = a^k * a'^k$, si le groupe n'est pas commutatif.

Par application du **Th.4.1.7**, on aura:

$$Gr(a) = Gr(\{a\}) = \{...a^{-3}, a^{-2}, a^{-1}, e, a, a^2, a^3, ...\}$$

4.1.9.1. Ordre d'un élément : *Soit $(G, *)$ un groupe d'élément neutre e. On appelle ordre d'un élément a de G, et on note $o(a)$, l'ordere de $Gr(a)$.*
$(o(a) = Card(Gr(a)))$

On a deux cas possibles.
$1^{er} cas$: Il existe $k \in \mathbb{N}^*$, $a^k = e$, alors $o(a)$ est fini et c'est le plus petit $k \in \mathbb{N}^*$ vérifiant $a^k = e$.
$2^{ème} cas$: Pour tout $k \in \mathbb{N}^*$, $a^k \neq e$, alors $o(a)$ est infini.

Exemple : Dans le groupe $(\mathbb{Z}, +)$ on a:
$o(1) = \infty = o(-1)$ et $o(0) = 1$

4.1.10. Groupes symétriques :

On sait d'après **4.1.1**, exemple **Ex 2**, que $(S(E), \circ)$ est un groupe qui est non commutatif, si $card(E) > 2$. (où $S(E)$ est l'ensemble des applications bijectives (inversibles) de E dans E.

Dans le cas où E est fini (par exemple $E = \{1, 2, ..., n\}$) ce groupe s'appelle *groupe symétrique* et se note souvent S_n ($n = Card(E)$) au lieu de $S(E)$ et ses éléments qui sont au nombre de $n!$ sont appelés permutations de E.

D'après le cours 2- **2.1.3** , tout élément σ de S_n peut être représenté par la table de valeurs: ce qui peut s'écrire

x	1	2	...	...	$n-1$	n
$\sigma(x)$	$\sigma(1)$	$\sigma(2)$	...	...	$\sigma(n-1)$	$\sigma(n)$

conventionnellement sous la forme $\sigma = \begin{pmatrix} 1 & 2 & \dots & n-1 & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n-1) & \sigma(n) \end{pmatrix}$ l'élément neutre e du groupe S_n est l'identité ou la permutation identique donnée par $e = \begin{pmatrix} 1 & 2 & \dots & n-1 & n \\ 1 & 2 & \dots & n-1 & n \end{pmatrix}$ et la permutation inverse de la permutation σ est l'application réciproque σ^{-1}.

4.1.10.1. Traspositions : *Si $n \geq 2$, on appelle transposition toute permutation appartenant à S_n qui echange deux éléments distincts i et j, et laisse invariants les autres éléments.*

C.à.d: Si on note $T_{i,j}$ cette trasposition, alors: $T_{i,j}(i) = j$, $T_{i,j}(j) = i$ et $T_{i,j}(k) = k$ pour $k \neq i$ et $k \neq j$.

4.1.10.2. Remarque : 1)On pose par convention $T_{i,i} = e$.

2) L'inverse d'une transposition est elle même ($(T_{i,j})^{-1} = T_{i,j}$ C.à.d $T_{i,j} \circ T_{i,j} = e$)

Exemple 1 : Dans le groupe S_5 on a: $T_{2,5} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 3 & 4 & 2 \end{pmatrix}$, il est clair que $(T_{2,5})^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 3 & 4 & 2 \end{pmatrix} = T_{2,5}$

4.1.10.3. Théorème : *Toute permutation appartenant à S_n est la composée d'un nombre fini de transpositions appartenant à S_n.*

Preuve: Faisons la preuve par récurrence sur n.

1) Pour $n = 2$. On a deux permutations, l'une est une transposition $T_{1,2}$ et l'autre est l'identité $e = T_{1,2} \circ T_{1,2}$.

2) Supposons le théorème vrai à l'ordre $n-1$, et soit $\sigma \in S_n$, on a deux cas possibles.

$1^{er} cas : \sigma(n) = n$, alors la restriction σ à $\{1, 2, ..., n-1\}$ est une permutation appartenant à S_{n-1} et par hypothèse de récurrence elle s'écrit comme composée de transpositions appartenant à S_{n-1}. Ces transpositions se prolongent en transpositions appartenant à S_n, dont la composée (dans le même ordre) est exactement σ.

$2^{ème} cas : \sigma(n) = p \neq n$, la permutation $\sigma' = T_{p,n} \circ \sigma$ et telle que $\sigma'(n) = n$, alors d'après le $1^{er} cas$, σ'est la composée de transpositions et en utilisant le fait que $T_{p,n} = T_{p,n}^{-1}$, on écrit $\sigma = T_{p,n} \circ \sigma'$ pour conclure que σ est aussi la composée de transpositions. ■

4.1.10.4. Remarque: La décomposition d'une permutation en composée de traspositions n'est pas unique.

Exemple : Dans le groupe S_5 on a: $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 2 & 5 & 3 \end{pmatrix}$

$\sigma = T_{4,1} \circ T_{4,2} \circ T_{5,3} \circ T_{4,3} = T_{2,1} \circ T_{4,1} \circ T_{4,5} \circ T_{5,3}$

4.1.10.5. Inversion, Parité et signature d'une permutation:

1) On dit que le couple (i,j) présente une inversion dans la permutation σ si $i < j$ et $\sigma(i) > \sigma(j)$

2) On dit qu'une permutetion σ est paire si le nombre $I(\sigma)$ des inversions présentées dans σ est pair, sinon elle est dite impaire.

3) Le nombre $\epsilon(\sigma) = (-1)^{I(\sigma)}$ est appelé signature de σ.

Exemple 1: Pour $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 2 & 5 & 3 \end{pmatrix}$, on a les inersions sont présentées par les couples $(1,2), (1,3), (1,5), (4,5)$, alors $I(\sigma) = 4$ et $\epsilon(\sigma) = 1$

Exemple 2: La permutation identique e n'a aucune inversion, alors $I(e) = 0$ et $\epsilon(e) = 1$

4.1.10.6. Théorème: *Toute transposition est impaire.*

Preuve: Soit $T_{i,j}$ une transposition. on peut considérer $i < j$ (car $T_{i,j} = T_{j,i}$), on a: $T_{i,j} = \begin{pmatrix} 1 & \dots & i-1 & i & i+1 & \dots & j-1 & j & j+1 & \dots & n \\ 1 & \dots & i-1 & j & i+1 & \dots & j-1 & i & j+1 & \dots & n \end{pmatrix}$

a) Les couples (p,q) tels que $1 \leq p \leq i-1$ ne présentent aucune inversion.

b) Les couples (p,q) tels que $p = i$ et $i+1 \leq q \leq j$ présentent tous des inversions, qui sont au nombre de $j-i$.

c) Les couples (p,q) tels que $p = i$ et $j+1 \leq q \leq n$ ne présentent aucune inversion.

b) Les couples (p,q) tels que $i+1 \leq p \leq j-1$ et $q = j$ présentent tous des inversions, qui sont au nombre de $j-i-1$.

c) Les couples (p,q) tels que $j \leq p \leq n$ ne présentent aucune inversion.

Par conséquent le nombre des inversions de $T_{i,j}$ est $2(i-j)-1$, alors elle est impaire.. ■

4.1.10.7. Théorème: *Une permutation est paire, si et seulement, elle est la composée d'un nombre paire de transpositions.*

Pour montrer ce théorème, on a besoin du lemme suivant:

4.1.10.8. Lemme: *Si σ est une permutation et $T_{i,j}$ et une transposition, alors $\sigma \circ T_{i,j}$ et σ sont de parité différentes.(C.à.d: l'une est paire et l'autre est impaire)*

Preuve du lemme: Commençons par une transposition de la forme $T_{i,i+1}$, dans ce cas, si $\sigma = \begin{pmatrix} 1 & \dots & i-1 & i & i+1 & i+2 & \dots & n \\ \sigma(1) & \dots & \sigma(i-1) & \sigma(i) & \sigma(i+1) & \sigma(i+2) & \dots & \sigma(n) \end{pmatrix}$,

et $\sigma \circ T_{i,i+1} = \begin{pmatrix} 1 & \dots & i-1 & i & i+1 & i+2 & \dots & n \\ \sigma(1) & \dots & \sigma(i-1) & \sigma(i+1) & \sigma(i) & \sigma(i+2) & \dots & \sigma(n) \end{pmatrix}$ et comparons les éventuelles inversions de $\sigma \circ T_{i,i+1}$ et σ.

a) Pour les couples (p,q) tels que $1 \leq p < q \leq i-1$ les permutations ont les mêmes inversions.

b) Pour les couples (p,q) tels que $1 \leq p \leq i-1$ et $q = i$, s'il y avait une inversion dans σ, alors elle devient une inversion pour le couple présentée par $(p, i+1)$.

c) Pour les couples (p,q) tels que $1 \leq p \leq i-1$ et $q = i+1$, s'il y avait une inversion dans σ, alors elle devient une inversion pour le couple présentée par (p,i) dans $\sigma \circ T_{i,i+1}$.

d) Pour les couples (p,q) tels que $1 \leq p \leq i-1$ et $i+2 \leq q \leq n$ les permutations ont les mêmes inversions.

e) Le couple (p,q) tel que $p = i$ et $q = i+1$, présente une inversion dans l'une des deux permutations sans qu'elle la présente dans l'autre.

f) Pour les couples (p,q) tels que $p = i$ et $i+2 \leq q \leq n$, s'il y avait une inversion dans σ, alors elle devient une inversion pour le couple présentée par $(i+1,q)$ dans $\sigma \circ T_{i,i+1}$.

g) Pour les couples (p,q) tels que $p = i+1$ et $i+2 \leq q \leq n$, s'il y avait une inversion dans σ, alors elle devient une inversion pour le couple présentée par (i,q) dans $\sigma \circ T_{i,i+1}$.

h) Pour les couples (p,q) tels que $i+2 \leq p < q \leq n$ les permutations ont les mêmes inversions.

Par conséquent, les permutations $\sigma \circ T_{i,i+1}$ et σ, diffèrent d'une inversion, (le cas e)), alors elles sont de parités différrentes.

Pour une transposition quelconque $T_{i,j}$, tel que $i < j$, on a
$T_{i,j} = (T_{j,j-1} \circ T_{j-1,j-2} \circ \dots T_{i+2,i+1}) \circ (T_{i+1,i} \circ T_{i+2,i+1} \dots \circ T_{j-1,j-2} \circ T_{j,j-1})$, alors $T_{i,j}$ est la composée d'un nombre impair ($2(j-i)-1$) de transpositions de la forme $T_{k,k+1}$, alors d'après le cas particulier edudié au début, $\sigma \circ T_{i,j}$ et σ, sont de parités différrentes. ■

Preuve du théorème: Le théorème **th 4.1.10.3** permet de dire qu'une permutation σ est la composée d'un nombre fini de transpositions et la permutation identique e qui est paire, et par application du lemme précédent, la pemutation σ reste paire si le nombre de transpositions est paire sinon elle est impaire. ■

4.2. Structure d'Anneau

4.2.1. Définition: *On appelle anneau toute structure algébrique* $(A, +_A, \cdot_A)$ *vérifiant:*

1) $(A, +_A)$ *est un groupe commutatif.*

2) $(A, \cdot_A)$ *est un demi groupe.(C.à.d:* $\cdot_A$ *est une lois de composition interne associative sur A)*

3) *Pour tous* x, y, z *de* A : $x \cdot_A (y +_A z) = (x \cdot_A y) +_A (x \cdot_A z)$ *et* $(y +_A z) \cdot_A x = (y \cdot_A x) +_A (z \cdot_A x)$. *(Cette assertion est appelée distributivité de la lois* $\cdot_A$ *par rapport à la lois* $+_A$*).*

* *Si la lois* $\cdot_A$ *admet un élément neutre, on dit que l'anneau est unitaire.*

* *Si la lois* $\cdot_A$ *est commutative, on dit que l'anneau est commutatif.*

* *Puisque la première lois de A est notée additivement* $+_A$*, alors son élément neutre est noté* 0_A *et pour la même raison le symétrique d'un élément* x *par rapport à cette lois est noté* $-x$ *et appelé opposé.*

* *Puisque la deuxième lois de A est notée multiplicativement* $\cdot_A$*, alors son élément neutre (s'il existe) est noté* 1_A *et pour la même raison le symétrique d'un élément* x *par rapport à cette lois (s'il existe) est noté* x^{-1} *et appelé inverse.*

4.2.2. Anneau intègre: *On dit qu'un un anneau* $(A, +_A, \cdot_A)$ *est intègre, si pour tous* $x, y \in A$*, on a:* $x \cdot_A y = 0_A$ *implique* $x = 0_A$ *ou* $y = 0_A$

Exemple 1: Les structures $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$,$(\mathbb{R}, +, \cdot)$ et $(\mathbb{C}, +, \cdot)$ sont des anneaux unitaires, commutatifs et intègres.

*Dans l'anneau $(\mathbb{Z}, +, \cdot)$, les seuls éléments inversibles sont 1 et -1.

*Dans les anneaux $(\mathbb{Q}, +, \cdot)$,$(\mathbb{R}, +, \cdot)$ et $(\mathbb{C}, +, \cdot)$, tous les éléments sont inversibles sauf 0.

Exemple 2: La structure $(A(\mathbb{R}, \mathbb{R}), +_A, \cdot_A)$ est un anneau commutatif unitaire non intègre.

$A(\mathbb{R}, \mathbb{R})$ est l'ensemble des applications de $\mathbb{R}$ dans $\mathbb{R}$ muni de l'addition usuelle $+_A$et la multiplication usuelle $\cdot_A$ des applications définies par:
Pour toutes f,$g \in A(\mathbb{R}, \mathbb{R})$: $f +_A g$ et $f \cdot_A g$ sont les applications de $\mathbb{R}$ dans $\mathbb{R}$ telles que: $(f +_A g)(x) = f(x) + g(x)$ et $(f \cdot_A g)(x) = f(x) \cdot g(x)$, pour tout $x \in \mathbb{R}$.

*L'élément unité 1_A est l'application constante $1_A : \mathbb{R} \to \mathbb{R}$ telle que $1_A(x) = 1$

*Dans l'anneau $(A(\mathbb{R}, \mathbb{R}), +_A, \cdot_A)$, les éléments inversibles sont les applications f qui ne s'annulent pas, $(\forall x \in \mathbb{R} : f(x) \neq 0)$, dans ce cas $f^{-1} = \frac{1}{f}$ avec $\frac{1}{f}(x) = \frac{1}{f(x)}$

*On peut avoir $f \cdot_A g = 0_A$ sans que f et g soient nulles. ($f(x) \neq 0$ pour

$x \neq 1$ et $f(1) = 0$ et $g(x) = 0$ pour $x \neq 1$ et $g(1) \neq 0$)

Exemple 3: La structure $(A(\mathbb{R},\mathbb{R}), +_A, \circ)$ est un anneau unitaire non commutatif et non intègre.

$+_A$ et $\circ$ sont respectivement l'addition et la composition usuelles.

*L'élément unité 1_A est l'application identité $Id_{\mathbb{R}} : \mathbb{R} \to \mathbb{R}$ telle que $Id_{\mathbb{R}}(x) = x$

*Dans l'anneau $(A(\mathbb{R},\mathbb{R}), +_A, \circ)$, les éléments inversibles sont les applications f bijectives, dans ce cas f^{-1}est l'application réciproque.

*On peut avoir $f \circ g = 0_A$ sans que f et g soient nulles. ($f(x) \neq 0$ pour $x \neq 1$ et $f(1) = 0$ et $g(x) = 1$ pour tout x)

4.2.3. Remarque: Dans un anneau $(A, +_A, \cdot_A)$, on écrit $x - y$, $x \cdot_A y +_A z$ et $z +_A x \cdot_A y$ respectivement au lieu de $x +_A (-y)$, $(x \cdot_A y) +_A z$ et $z +_A (x \cdot_A y)$. et on pose: $0x = 0_A$, et pour tout $n \in \mathbb{N}^*$: $nx = x +_A (n-1)x$ et $-nx = n(-x)$

Avec cette remarque, on peut énoncer le Théorème suivant:

4.2.4. Théorème: *Soit $(A, +_A, \cdot_A)$ un anneau, alors pour tous $x, y, z \in A$, on a:*

1) $x \cdot_A 0_A = 0_A = 0_A \cdot_A x$

2) $x \cdot_A (-y) = -(x \cdot_A y) = (-x) \cdot_A y$

3) $x \cdot_A (y - z) = x \cdot_A y - x \cdot_A z$ *et* $(y - z) \cdot_A x = y \cdot_A x - z \cdot_A x$

4) Pour tout $n \in \mathbb{Z}$: $x \cdot_A (ny) = n(x \cdot_A y) = (nx) \cdot_A y$

Preuve: 1) $0_A = (x \cdot_A 0_A) - (x \cdot_A 0_A) = x \cdot_A (0_A +_A 0_A) - (x \cdot_A 0_A)$
$= (x \cdot_A 0_A) +_A (x \cdot_A 0_A) - (x \cdot_A 0_A) = (x \cdot_A 0_A)$

de la même façon, on montre que $0_A = 0_A \cdot_A x$

2) $x \cdot_A (-y) +_A x \cdot_A y = x \cdot_A (-y +_A y) = x \cdot_A 0_A = 0_A$, alors $x \cdot_A (-y) = -(x \cdot_A y)$

de la même façon, on montre que $-(x \cdot_A y) = (-x) \cdot_A y$

3) $x \cdot_A (y - z) = x \cdot_A y +_A x \cdot_A (-z) = x \cdot_A y +_A (-x \cdot_A z) = x \cdot_A y - x \cdot_A z$

de la même façon, on montre que $(y - z) \cdot_A x = y \cdot_A x - z \cdot_A x$

4) Pour $n \in \mathbb{N}$, la preuve se fait par récurrence sur n.

*$x \cdot_A (0y) = x \cdot_A 0_A = 0_A = 0(x \cdot_A y)$, alors la propriété est vraie pour $n = 0$

*Supposons la propriété vraie pour n et montrons qu'elle reste vraie pour $n+1$

$x \cdot_A ((n+1)y) = x \cdot_A (y +_A ny) = x \cdot_A y +_A x \cdot_A (ny)$
$= x \cdot_A y +_A n(x \cdot_A y) = (n+1)(x \cdot_A y)$

Pour $-n$ (avec $n \in \mathbb{N}$), on a $x \cdot_A (-ny) = x \cdot_A (n(-y)) = n(x \cdot_A (-y)) = n(-(x \cdot_A y)) = -n(x \cdot_A y)$.

de la même façon, on montre que $n(x \cdot_A y) = (nx) \cdot_A y$ ■

4.2.5. Sous anneau: *On appelle sous anneau d'un anneau $(A, +_A, \cdot_A)$ toute*

partie non vide L de A qui est elle même un anneau pour les lois $+_A, \cdot_A$ restreintes à L.

4.2.5.1. Proposition: *Une partie L de A est un sous anneau d'un anneau $(A, +_A, \cdot_A)$ ssi*

1) L contient l'élément zéro 0_A.

2) Pour tous x,$y \in L : x - y \in L$

3) *Pour tous x,$y \in L : x \cdot_A y \in L$.*

Preuve: a) Supposons que L est un sous anneau de $(A, +_A, \cdot_A)$, alors $(L, +_A)$ est un sous groupe de $(A, +_A)$, donc d'après **Prop.4.1.2.1**, on aura les assertions 1) et 2). L'assertion 3) est du au fait que la restriction de $\cdot_A$ à L est une lois interne sur L.

b) Supposons que L vérifie les assertions 1),2) et 3), alors, d'après **Prop.4.1.2.1**, 1) et 2) implique $(L, +_A)$ est un sous groupe de $(A, +_A)$. L'assertion 3) montre que la restriction de $\cdot_A$ à L est une lois interne sur L donc elle demeure associative et distributive par rapport à $+_A$ sur L. Par suite L est un sous anneau de $(A, +_A, \cdot_A)$. ■

Exemple 1: $(n\mathbb{Z}, +, \cdot)$, avec $n \in \mathbb{Z}$ sont des sous anneaux de $(\mathbb{Z}, +, \cdot)$.

4.2.6. Idéaux d'un anneau: *Une partie I de A est un idéal d'un anneau $(A, +_A, \cdot_A)$ si*

1) $(L, +_A)$ est un sous groupe du groupe $(A, +_A)$

2) Pour tous $a \in A$ et $x \in L : a \cdot_A x \in L$ et $x \cdot_A a \in L$

4.2.6.1. Proposition: *Une partie I de A est un idéal d'un anneau $(A, +_A, \cdot_A)$ ssi*

1) I contient l'élément zéro 0_A.

2) Pour tous x,$y \in I : x - y \in I$

3) *Pour tous $a \in A$ et $x \in L : a \cdot_A x \in L$ et $x \cdot_A a \in L$*

Preuve: Il suffit d'appliquer **Prop.4.1.2.1**. ■

4.2.6.2. Remarque: Il est clair qu'un idéal est un sous anneau.

Exemple: Les ensembles $n\mathbb{Z}$, avec $n \in \mathbb{Z}$ sont de idéaux de $(\mathbb{Z}, +, \cdot)$.

D'une manière générale, si $(A, +_A, \cdot_A)$ est un anneau unitaire et commutatif, alors $aA = \{a \cdot_A x \ / \ x \in A\}$ est un idéal de $(A, +_A, \cdot_A)$.

Cette idéal est le plus petit idéal contenant $\{a\}$, alors on dit qu'il est engendré par a et puisqu'il est engendré par un seul élément on dit qu'il est principal.

4.3. Structure de corps

4.3.1. Définition: *On appelle corps tout anneau unitaire d'élément unité non nul et dont tout élément non nul est inversible.*

* *Le corps est commutatif si l'anneau est commutatif.*

4.3.2. Remarque: 1) Si $(K, +_K, \cdot_K)$ est un corps, alors $(K^*, \cdot_K)$ est un groupe.(où $K^* = K - \{0_K\}$ et 0_K est l'élément neutre de $+_K$)

2) Tout corps K est un anneau intègre.

$$a \cdot_K b = 0_K \Rightarrow \begin{cases} a^{-1} \cdot_K a \cdot_K b = a^{-1} \cdot_K 0_K \\ a \cdot_K b \cdot_K b^{-1} = 0_K \cdot_K b^{-1} \end{cases} \Rightarrow \begin{cases} b = 0_K \\ a = 0_K \end{cases}$$

Exemple : Les structures $(\mathbb{Q}, +, \cdot)$,$(\mathbb{R}, +, \cdot)$ et $(\mathbb{C}, +, \cdot)$ sont des corps commutatifs.

La structure $(\mathbb{Z}, +, \cdot)$ n'est pas un corps.

Université Ibn Khaldoun de Tiaret.
Département d'Informatique.
Module:Algèbre 1 ($1^{ère}$ Année LMD)

Fiche de T.D N^0 4

Exercice 1: Sur $\mathbb{R}$, on définit l'opération $*$ par $x*y=\frac{x^3+y^3}{x^2+y^2}$ si $(x,y)\neq(0,0)$ et $x*y=0$ si $(x,y)=(0,0)$.

Etudier pour cette lois, la commutativité, l'associativité, l'existence de l'élément neutre et l'existence du symétrique.

Exercice 2: Soit E un ensemble muni de deux lois de composition $*_1$ et $*_2$ admettant respectivement les éléments neutres e_1 et e_2, et vérfiant :

Pour tous $x,y,u,v\in E:(x*_1y)*_2(u*_1v)=(x*_2u)*_1(y*_2v)$

1) Montrer que $e_1=e_2$ et que pour tous $x,y\in E:x*_1y=x*_2y$

2) Montrer qu'il s'agit d'un monoïde commutatif

Exercice 3: Sur $\mathbb{Z}$, on définit l'opération $\triangle$ par $n\triangle m=(n+1)(m+1)-1$. Montrer qu'il s'agit d'un monoïde commutatif et trouver ses éléments inversibles.

Exercice 4: Montrer que les éléments inversibles d'un monoïde $(E,*)$ forment un groupe pour la même lois (Ce groupe est souvent noté $(U(E),*)$).

Exercice 5: Soit $Aff(\mathbb{R})$ l'ensemble des applications affines de $\mathbb{R}$ dans $\mathbb{R}$.

$Aff(\mathbb{R})=\left\{\varphi_{(a,b)}:\mathbb{R}\to\mathbb{R}\ /\ (a,b)\in\mathbb{R}^*\times\mathbb{R}\text{ et }\forall x\in\mathbb{R}:\varphi_{(a,b)}(x)=ax+b\right\}$

1) Montrer que $(Aff(\mathbb{R}),\circ)$ est un groupe non commutatif.

2) Montrer que l'ensemble $T(\mathbb{R})=\left\{\varphi_{(1,b)}\ /b\in\mathbb{R}\right\}$ des translations de $\mathbb{R}$, est un sous groupe de que $(Aff(\mathbb{R}),\circ)$.

Exercice 6: Soient $(G,*)$ un groupe et $Z(G)$ l'ensemble des éléments de G qui commutent avec tous les éléments de G. Montrer que $Z(G)$ est un sous groupe de G

Exercice 7: Soient $(G,*)$ un groupe tel que pour tout $x\in G:x^3=e$.

Montrer que pour tous $x,y\in G:(x*y)^2=y^2*x^2$ et $x*y^2*x=y*x^2*y$.

Exercice 8: Soit $\mathcal{R}$ une relation d'équivalence sur un ensemble G muni d'une opération $*$. On dit que $\mathcal{R}$ est compatible avec la lois $*$ si,

Pour tous $x,y,a,b\in G$ on a: $x\mathcal{R}y$ et $a\mathcal{R}b$ implique $(x*a)\mathcal{R}(y*b)$.

On définit l'opération $\overset{\bullet}{*}$ sur $G_{/\mathcal{R}}$ par $\dot{x}\overset{\bullet}{*}\dot{y}=\widehat{x*y}$.

1) Montrer que si $(G,*)$ est un groupe, alors $\left(G_{/\mathcal{R}},\overset{\bullet}{*}\right)$ est aussi un groupe.

2) Application: $(G,*)=(\mathbb{Z},+)$ et $\mathcal{R}_n$ la congruence modulo n.

Exercice 9: Soit $\leq_{\mathcal{R}}$ une relation d'ordre sur un ensemble G muni d'une opération $*$. On dit que $\leq_{\mathcal{R}}$ est compatible avec la lois $*$ si,

Pour tous $x, y, a, b \in G$ on a: $x \leq_{\mathcal{R}} y$ et $a \leq_{\mathcal{R}} b$ implique $(x * a) \leq_{\mathcal{R}} (y * b)$.

Pour A et B des parties de G on pose $A * B = \{a * b \text{ tels que } a \in A \text{ et } b \in B\}$

1) Comparer $\sup(A * B)$ et $\sup A * \sup B$ (s'ils existent).

2) Montrer que $a \leq_{\mathcal{R}} b$ ssi $b^{-1} \leq_{\mathcal{R}} a^{-1}$ (pour a et b inversibles)

Application: $(G, *) = (\mathbb{R}, +)$ et $\mathcal{R}$ l'ordre usuelle $\leq$

Exercice 10: Donner les éléments du groupe symétrique S_3 et sa table de multiplication

Determiner les ordres, les parités et les signatures de certains éléments de S_3 et un sous groupe d'ordre 3.

Exercice 11: Soit G un groupe cyclique d'ordre n engendré par $a (G = Gr(a))$

Montrer que G est aussi engendré par a^k, où k est premier avec n.

Exercice 12: Soient $*$ l'opération définie sur $\mathbb{R}$ donnée dans l'exercice 1 et la multiplication usuelle de $\mathbb{R}$.Etudier la distributivité de chaque lois sur l'autre.

Exercice 13: Montrer que $\left(\mathbb{Z}_{/p\mathbb{Z}}, \dot{+}, \dot{\times}\right)$ est un anneau commutatif unitaire et qu'il s'agit d'un corps si p est premier. $(\dot{x} \dot{+} \dot{y} = \dot{\overbrace{x + y}}$ et $\dot{x} \dot{\times} \dot{y} = \dot{\overbrace{x \times y}})$

Exercice 14: Soit $(A, +_A, \cdot_A)$ un anneau vérifiant $x^2 = x$ pour tout $x \in A$. (On dit que x est idempotent et que A est un anneau de Boole)

1) Montrer que $2x = 0_A$

2) Montrer que A est commutatif. En déduire la valeur de $(x \cdot_A y) \cdot_A (x +_A y)$