Universitè Ibn Zohr	**Module : Algèbre 1**
École Nationale des Sciences Appliquées	**Semestre 1**
1ére année cycle préparatoire	**Année universitaire : 2020-2021**

Serie 1 (Structures Algébriques)

13. Soit $(G,*)$ un groupe. Pour $a \in G$, on note f_a l'application de G vers G définie par

$f_a(x) = a * x * sym(a)$.

(a) Montrer que f_a est un endomorphisme du groupe $(G,*)$.
(b) Vérifier que $\forall a, b \in G, f_a o f_b = f_{a*b}$
(c) Montrer que f_a est bijective et déterminer son application réciproque.
(d) En déduire que (F,o) est un groupe avec $F = \{f_a | a \in G\}$.

Solution :

(a) On a $f_a(e) = a * e * sym(a) = e$.
$\forall x, y \in G$, $f_a(x*y) = a*x*y*sym(a) = a*x*sym(a)*a*y*sym(a) = f_a(x) * f_a(y)$. Donc f_a est un endomorphisme du groupe $(G,*)$.
(b) $(f_a \circ f_b)(x) = f_a(b*x*sym(b)) = a*b*x*sym(b)*sym(a) = (a*b)*x*sym(a*b) = f_{a*b}(x)$. Donc $f_a \circ f_b = f_{a*b}$.

(c) Utilisons le résultat de la question (b), on obtient :

$$f_a \circ f_{sym(a)} = f_{a*sym(a)} = f_e.$$

De même

$$f_{sym(a)} \circ f_a = f_{sym(a)*a} = f_e,$$

et $f_e(x) = e*x*sym(e) = x$ donc $f_e = Id_G$ et $f_a \circ f_{sym(a)} = f_{sym(a)} \circ f_a = Id_G$ donc f_a est bijective et $sym(f_a) = f_{sym(a)}$.

(d) Montrons que F est un sous-groupe de $(G,\circ)$.
- $F \subset G$ et $Id_G \in F$ car $Id_G = f_e$ et $e \in G$.
- $\forall g, h \in F$, $\exists a, b \in G$ tels que $g = f_a$ et $h = f_b$.
  $g \circ sym(h) = f_a \circ sym(f_b) = f_a \circ f_{sym(b)} = f_{a*sym(b)} \in F$ car $a * sym(b) \in G$.

Ainsi F est un sous-groupe de $(G,\circ)$ et donc $(F,\circ)$ est un groupe.
(Nous avons utilisé le théorème suivant :
Si F est un sous-groupe de $(G,*)$ alors $(F,*)$ est un groupe).

14. Soit $(G,*)$ et Soit (G',T) deux groupes et $f : G \longrightarrow G'$ un morphisme de groupes. Montrer que tout sous groupe H de G, $f(H)$ est un sous groupe de G'.

Solution :

$f(H)$ est un sous groupe de G', en effet
- $f(H) \subset G'$, notons e le neutre de G et e' le neutre de G' $e' = f(e) \in f(H)$ car $e \in H$ (car H est un sous groupe de G).
- $\forall y, y' \in f(H)$, on peut écrire $y = f(x)$ et $y' = f(x')$ avec $x, x' \in H$.

  $y \top sym(y') = f(x) \top sym(f(x')) = f(x) \top f(sym(x')) = f(x * sym(x'))$ avec $x * sym(x') \in H$ (car H est un sous groupe de G). Donc $y \top sym(y') \in f(H)$.

  Ainsi $f(H)$ est un sous groupe de $(G', \top)$.

15 Soit $H = \{(x,y,z) \in \mathbb{R}^3 / x + 2y - z = 0\}$

(a) Montrer que $(H,+)$ est un sous groupe de $(\mathbb{R}^3,+)$.
(b) Soit $f : H \to H$ définie par : $\forall (x,y,z) \in H,\ f(x,y,z) = (x-2z, z-y, x-2y)$. Monter que f est un morphisme de groupes, déterminer son noyau et son image.

Solution :

(a) $(H,+)$ est un sous groupe de $(\mathbb{R}^3,+)$, en effet :
- $H \subset \mathbb{R}^3$ et $0_{\mathbb{R}^3} = (0,0,0) \in H$ (car $0 + 2.0 - 0 = 0$).
- Soit $X = (x,y,z),\ Y = (x',y',z') \in H$, on montre que $X + Y \in H$, on a :

$$X + Y = (x + x', y + y', z + z')$$

$$(x + x') + 2(y + y') - (z + z') = (x + 2y - z) + (x' + 2y' - z') = 0 + 0 = 0.$$

Donc $X + Y \in H$.
- Soit $X = (x,y,z) \in H$, on montre que $sym(X) = -X$ (car le sym(X) de la loi + est -X) $\in H$, on a

$$-X = (-x,-y,-z), \quad -x - 2y + z = -(x + 2y - z) = 0 \text{ (car (x,y,z) } \in \text{ H)}.$$

Donc $-X \in H$.

Donc est un sous groupe de $(\mathbb{R}^3,+)$.

(b) On montre que $\forall X = (x,y,z),\ Y = (x',y',z') \in H,\ f(X+Y) = f(X) + f(Y)$.

On a

$$\begin{aligned} f(X+Y) &= ((x+x') - 2(z+z'), (z+z') - (y+y'), (x+x') - 2(y+y')) \\ &= (x - 2z, z - y, x - 2y) + (x' - 2z', z' - y', x' - 2y'). \\ &= f(X) + f(Y). \end{aligned}$$

Donc f est un morphisme de groupes.

Le noyau de f est :

$$Kerf = \{X = (x,y,z) \in H / f(X) = 0_{\mathbb{R}^3}\}, \text{ car } 0_{\mathbb{R}^3} \text{ est l'élément neutre de (H,+)}$$

$$\begin{aligned} (x,y,z) \in Kerf &\Longrightarrow (x - 2z = 0, z - y = 0, x - 2y = 0) \quad et \quad (x,y,z) \in H \\ &\Longrightarrow (x = 2y, z = y) \quad et \quad x + 2y - z = 0 \\ &\Longrightarrow (x = 2y, z = y) \quad et \quad 2y + 2y - y = 0 \\ &\Longrightarrow x = y = z = 0 \end{aligned}$$

$$Kerf = \{(0,0,0)\}.$$

Donc f est injective.

$(x,y,z) \in Imf \Longrightarrow \exists (x',y',z') \in H$tel que $f(x',y',z') = (x,y,z)$

$$(x' - 2z', z' - y', x' - 2y') = (x,y,z)$$

$$\Longrightarrow x + 2y = x' - 2y' = z$$

$$\Longrightarrow Imf = \{(x,y,z) \in \mathbb{R}^3 / x + 2y - z = 0\} = H.$$

Donc f est surjective.

16. Soit $p \in N^*$. Déterminer la signature des permutation suivantes :

(a)

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & 2\text{p-1} & 2\text{p} \\ 2\text{p} & 2\text{p-1} & \cdots & 2 & 1 \end{pmatrix}$$

(b)

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & \text{p} & \text{p+1} & \text{p+2} & \cdots & 2\text{p-1} & 2\text{p} \\ 1 & 3 & 5 & \cdots & 2\text{p-1} & 2 & 4 & \cdots & 2\text{p-2} & 2\text{p} \end{pmatrix}$$

Solution :

Calculons le nombre d'inversion :

Rappel : On dit σ réalise une inversion sur le couple (i, j) ssi $\sigma(i) > \sigma(j)$.

(a) Pour 1, on a $(2p-1)$ inversions,$(1,2)$.....$(1,2p)$, en effet :

$$\Leftrightarrow \begin{cases} 2p > 2p-1 \text{ et } 1 < 2 \\ 2p > 2p-2 \text{ et } 1 < 3 \\ 2p > 2p-2 \text{ et } 1 < 3 \\ \ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots \\ 2p > 1 \text{ et } 1 < 2p. \end{cases}$$

Pour 2, on a $(2p-2)$ inversions $(2,3)$.....$(2,2p)$, et ainsi de suite,
Pour $2p-1$, on a une seule inversion $(2p-1, 2p)$, on obtient

$$I(\sigma) = (2p-1) + (2p-2) + ... + 1 + 0 = \frac{2p(2p-1)}{2}$$

donc $\varepsilon(\sigma) = (-1)^{p(2p-1)}$.

(b) On a

$$\Leftrightarrow \begin{cases} \text{pour } 1 \rightarrow 0 \text{ inversion.} \\ \text{pour } 2 \rightarrow 1 \text{ inversion } (2,\text{p+1}). \\ \text{pour } 3 \rightarrow 2 \text{ inversions } (3,\text{p+1}),(3,\text{p+2}). \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \text{pour p} \rightarrow (\text{p-1}) \text{ inversions } (\text{p},\text{p+1}).....(2,\text{2p-1}). \\ \text{pour p+1} \rightarrow 0 \text{ inversion.} \\ \text{pour p+2} \rightarrow 0 \text{ inversion.} \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \text{pour 2p-1} \rightarrow 0 \text{ inversion.} \\ \text{pour 2p} \rightarrow 0 \text{ inversion.} \end{cases}$$

$I(\sigma) = 0 + 1 + 2 + ... + (p-1) + 0 + ... + 0 + 0 = \frac{p(p-1)}{2}$ donc $\varepsilon(\sigma) = (-1)^{\frac{p(p-1)}{2}}$.

17. Décomposer les permutations ci-dessous sous forme de produit de cycles à supports disjoints puis déterminer leur signatures. Sont-elles des cycles ?

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 1 & 2 \end{pmatrix}, \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 4 & 2 & 5 \end{pmatrix}, \quad \sigma^2\tau.$$

Solution :

On commence par étudier les images successives de 1. Ce sont 3,4. On étudie ensuite les images

successives de 2. On trouve 5 (ensuite on revient à 2). On a épuisé tous les éléments de 1,. . . ,5.
La décomposition canonique de σ en produits de cycles disjoints est

$$\sigma = (1 \quad 3 \quad 4)(2 \quad 5)$$

$$\varepsilon(\sigma) = (-1)^{5-2} = -1 (\text{car on a 2 orbites } \{1,3,4\} \text{ et } \{2,5\})$$

Pour les inversions : Il y'a 7 inversions sont $(1,4),(1,5),(2,3),(2,4),(2,5),(3,4),(3,5)$.

$$\varepsilon(\sigma) = (-1)^7 = -1.$$

De même pour τ, on obtient :

$$\tau = (2 \quad 3 \quad 4).$$

La signature de τ vaut

$$\varepsilon(\sigma) = (-1)^{5-3} = 1. \text{ (car il y'a trois orbites :}\{1\} \ \{2,3,4\},\{5\}).$$

Pour les inversions : Il y'a 2 inversions sont $(2,4),(3,4)$.

$$\varepsilon(\sigma) = (-1)^2 = 1.$$

Calculons $\sigma^2\tau$

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

$$\sigma^2\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 1 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 4 & 2 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 3 & 2 & 5 \end{pmatrix} = (1 \quad 4 \quad 2)$$

$$\varepsilon(\sigma^2\tau) = (-1)^{5-3} = 1 (\text{car on a 3 orbites } \{1,4,2\} \text{ et } \{3\},\{5\})$$

Pour les inversions : Il y'a 4 inversions sont $(1,2),(1,3),(1,4),(3,4)$.

$$\varepsilon(\sigma) = (-1)^4 = 1.$$

18 . Sur $(\mathbb{Z}^2,+)$, on définit une nouvelle loi $*$ par

$$(x_1,x_2)*(y_1,y_2) = (x_1y_1 + rx_2y_2, x_1y_2 + x_2y_1)$$

où $r \in \mathbb{Z}^*$.

(a) Montrer que $(\mathbb{Z}^2,+,*)$ est un anneau commutatif. Pour quels entiers cet anneau est unitaire.

(b) Pour quels entiers cet anneau est intégre, unitaire.

Solution :

(a) $(\mathbb{Z}^2,+)$ est un groupe commutatif.

La loi $*$ est commutative car le produit et la somme sont commutatives dans $\mathbb{Z}$ et

$$(x_1,x_2)*(y_1,y_2) = (y_1,y_2)*(x_1,x_2).$$

$((x_1,x_2)*(y_1,y_2))*(z_1,z_2) = (x_1y_1+rx_2y_2, x_1y_2+x_2y_1)*(z_1,z_2) = (x_1y_1z_1+rx_2y_2z_1+rx_1y_2z_2+rx_2y_1z_2), x_1y_1z_2 + rx_2y_2z_2 + x_1y_2z_1 + x_2y_1z_1) = (x_1,x_2)*((y_1,y_2)*(z_1,z_2))$.

$((x_1,x_2)+(y_1,y_2))*(z_1,z_2)=(x_1+y_1,x_2+y_2)*(z_1,z_2)=(x_1z_1+y_1z_1+rx_2z_2+ry_2z_2,x_1z_2+y_1z_2+x_2z_1+y_2z_1)$,
donc $((x_1,x_2)+(y_1,y_2))*(z_1,z_2)=(x_1z_1+rx_2z_2,x_1z_2++x_2z_1)+(y_1z_1+ry_2z_2,y_1z_2+y_2z_1)$.

$$=(x_1,x_2)*(z_1,z_2+(y_1,y_2)*(z_1,z_2).$$

Donc $*$ est distributive sur $+$.
Par conséquent $(\mathbb{Z}^2,+,*)$ est un anneau commutatif.

(b) L'anneau $(\mathbb{Z}^2,+,*)$ est dit intègre si pour tous (x_1,x_2) et (y_1,y_2) dans $\mathbb{Z}^2$ tels que $(x_1,x_2)*(y_1,y_2)=(x_1y_1+rx_2y_2,x_1y_2+x_2y_1)=(0,0)\Longrightarrow(x_1,x_2)=(0,0)$ ou $(y_1,y_2)=(0,0)$.
Si $(x_1,x_2)\neq(0,0)$

$$\begin{cases} x_1y_1+rx_2y_2=0 \\ x_1y_2+x_2y_1=0 \end{cases}$$

donc

$$\delta=\begin{vmatrix} x_1 & rx_2 \\ x_2 & x_1 \end{vmatrix}=x_1^2-rx_2^2 \quad \delta_{y_1}=\begin{vmatrix} 0 & rx_2 \\ 0 & x_1 \end{vmatrix}=0 \quad \delta_{y_2}=\begin{vmatrix} x_1 & 0 \\ x_2 & 0 \end{vmatrix}=0$$

Si $r<0$ donc $y_1=\frac{\delta_{y_1}}{\delta}=0, y_2=\frac{\delta_{y_2}}{\delta}=0$ donc l'anneau $(\mathbb{Z}^2,+,*)$ est intègre si $r<0$.
Soit (e_1,e_2) est l'élément neutre pour la loi $*$ dans $\mathbb{Z}^2$ alors
$\forall(x_1,x_2)\in\mathbb{Z}^2$ on a $x_1,x_2)*(e_1,e_2)=(x_1,x_2)\Longrightarrow(x_1e_1+rx_2e_2,x_1e_2+x_2e_1)=(x_1,x_2)$
$\Longrightarrow x_1e_1+rx_2e_2=x_1 \quad et \quad x_1e_2+x_2e_1=x_2$ donc

$$\delta=\begin{vmatrix} x_1 & rx_2 \\ x_2 & x_1 \end{vmatrix}=x_1^2-rx_2^2 \quad \delta_{e_1}=\begin{vmatrix} x_1 & rx_2 \\ x_2 & x_1 \end{vmatrix}=x_1^2-rx_2^2 \quad \delta_{e_2}=\begin{vmatrix} x_1 & x_1 \\ x_2 & x_2 \end{vmatrix}=0$$

Si $r<0$ donc $(1,0)$ est est l'élément neutre pour la loi $*$ dans $\mathbb{Z}^2$.

19. $\forall x\ y\in\mathbb{R}$, on pose $x\top y=x+y-1$ et $x*y=xy-x-y+2$. Soit

$$\varphi:(\mathbb{R},\top,*)\to(\mathbb{R},+,.)$$

$$x\to x-1$$

Montrer que φ est isomorphisme d'anneau. En déduire que $(\mathbb{R},\top,*)$ est un corps.

Solution :

Les élément neutres de $(\mathbb{R},\top,*)$ sont 1 et 2, en effet $x\top 1=x$ et $x*2=x$.
Soit $\varphi:\mathbb{R}\to\mathbb{R}$ définie par $\varphi:x\mapsto x-1$. φ est une bijection, en effet :

- Injectivité :

$$\forall x,\ x^{'}\in\mathbb{R},\ \varphi(x)=\varphi(x^{'})\to x=x^{'}.\text{ Donc }\varphi\text{ est injetive.}$$

- Surjectivité :

$$\forall y\in\mathbb{R},\ \exists x\in\mathbb{R},\ y=\varphi(x).$$

Soit $y\in\mathbb{R},\ y=\varphi(x)=x-1\Leftrightarrow x=y+1$.
Donc $\forall y\in\mathbb{R},\ \exists x=y+1\in\mathbb{R},\ y=\varphi(x)$.
$\varphi(1)=0$.
On vérifie $\varphi(x\top y)=\varphi(x)+\varphi(y)$

$$\varphi(x\top y)=x\top y-1=x+y-2=x-1+y-1=\varphi(x)+\varphi(y).$$

$\varphi(2) = 1$.
On vérifie également : $\varphi(x * y) = \varphi(x) \times \varphi(y)$.

$$\varphi(x * y) = x * y - 1 = xy - x - y + 2 - 1 = xy - x - y - 3 = (x-1)(y-1) = xy - x - y + 1.$$

Par conséquent φ est isomorphisme d'anneau.

On sait que $(\mathbb{R}, +, \times)$ est un corps Par la bijection de $\varphi^{-1}(\mathbb{R}, +, \times) = (\mathbb{R}, \top, *)$ est un corps.

20 . Soit $d \in \mathbb{N}$ tel que $\sqrt{d} \notin \mathbb{Q}$. On note $\mathbb{Q}\sqrt{d} = \{a + b\sqrt{d}/(a, b) \in \mathbb{Q}^2\}$. Montrer que $(\mathbb{Q}\sqrt{d}, +, .)$ est un corps.

Solution :

Rappel : Si $\mathbb{Q}\sqrt{d}$ est un sous-corps de $(\mathbb{R}, +, .)$ alors $(\mathbb{Q}\sqrt{d}, +, .)$ est un corps.

Montrons que $\mathbb{Q}\sqrt{d}$ est un sous corps de $(\mathbb{Q}\sqrt{d}, +, .)$. Remarquons d'abord qu'il est bien contenu dans $\mathbb{R}$ et que $0, 1 \in \mathbb{Q}\sqrt{d}$.
Soient $x, y \in \mathbb{Q}\sqrt{d}$. On les écrit : $x = a + b\sqrt{d}$ et $x = a^{'} + b^{'}\sqrt{d}$. Alors :

$$x - y = (a - a^{'}) + (b - b^{'})\sqrt{d}$$

$$xy = (aa^{'} + dbb^{'}) + (ab^{'} + a^{'}b)\sqrt{d},$$

ce qui prouve que $x - y$ et $xy \in \mathbb{Q}\sqrt{d}$.

D'autre part, si $x \neq 0$, alors

$$\frac{1}{x} = \frac{1}{a + b\sqrt{d}} = \frac{a - b\sqrt{d}}{a^2 - b^2 d} = \frac{a}{a^2 - b^2 d} - \frac{b\sqrt{d}}{a^2 - b^2 d} \in \mathbb{Q}\sqrt{d},$$

et donc $\frac{1}{x} \in \mathbb{Q}\sqrt{d}$. Remarquons qu'il était possible de multiplier par la quantité conjuguée $(a - b\sqrt{d})$ qui est non-nulle car $\sqrt{d} \in \mathbb{Q}$. Finalement, on a bien prouvé que $\mathbb{Q}\sqrt{d}$ est un sous corps de $(\mathbb{Q}\sqrt{d}, +, .)$ et c'est donc un corps.