University of Tlemcen **Academic year 2023-2024**
Faculty of Sciences **(L1 ING-INF)** **Semester 2**
Department of Informatic **Algebra (First Year)**

Worksheet N°2/ "Algebraic structures"

Exercise 01: In $E =]-1,1[$, we define $*$ by:

$$\forall a, b \in E, a * b = \frac{a+b}{1+ab}.$$

Show that $(E,*)$ is an abelian group.

<u>Correction:</u> (1) Let's check that $*$ is a closure law (Binary operation) in E.
Show that:

$$\forall a, b \in E, a * b \in E,$$

that is:

$$\forall a, b \in E, -1 < \frac{a+b}{1+ab} < 1?$$

Let's calculate:

$$\alpha < \beta \Leftrightarrow \alpha - \beta < 0.$$

(a)

$$\begin{aligned} \frac{a+b}{1+ab} - 1 &= \frac{a+b-1-ab}{(1+ab)} \\ &= \frac{(1-b)(a-1)}{1+ab} < 0 \text{ car: } b < 1 \text{ et } a < 1 \\ &\Rightarrow \frac{a+b}{1+ab} < 1. \end{aligned}$$

(b) Same:

$$\begin{aligned} \frac{a+b}{1+ab} + 1 &= \frac{a+b+1+ab}{1+ab} = \frac{(1+b)(1+a)}{1+ab} > 0 \text{ car: } b > -1 \text{ et } a > -1 \\ &\Rightarrow \frac{a+b}{1+ab} > -1. \end{aligned}$$

So,

$$\forall a, b \in E, a * b \in E,$$

which implies that $*$ is a closure law in E.
(2) Show that $*$ is an associative law?

$$\forall a, b, c \in E; (a * b) * c = a * (b * c)?$$

Let $a, b, c \in E$:

$$(a * b) * c = \frac{a+b}{1+ab} * c = \frac{\frac{a+b}{1+ab} + c}{1 + \frac{a+b}{1+ab} \times c} = \frac{a+b+c+abc}{1+ab+ac+bc}, ...(1)$$

and

$$a*(b*c)=a*\frac{b+c}{1+bc}=\frac{a+\frac{b+c}{1+bc}}{1+a\times\frac{b+c}{1+bc}}=\frac{a+b+c+abc}{1+ab+ac+bc},...(2)$$

(1) = (2), which implies that

$$(a*b)*c=a*(b*c),$$

so $*$ is associative.
(3) $*$ is also commutative because

$$\forall a,b\in E: a*b=\frac{a+b}{1+ab}=\frac{b+a}{1+ba}=b*a.$$

(4) The existence of the identity element? Show that:

$$\forall a\in E,\exists e\in E, a*e=a?$$

$$\begin{aligned}
a*e &= a\Rightarrow\frac{a+e}{1+ae}=a\\
&\Rightarrow a+e=a(1+ae)\\
&\Rightarrow a+e=a+a^2e\\
&\Rightarrow e\left(1-a^2\right)=0,\forall a\in E=]-1,1[\Rightarrow e=0\in E.
\end{aligned}$$

(5) The existence of the inverse element for each element $a\in E$?
a admits a inverse element a^{-1} if:

$$\begin{aligned}
a*a^{-1} &= e=0\Rightarrow\frac{a+a^{-1}}{1+aa^{-1}}=0\\
&\Rightarrow a+a^{-1}=0\\
&\Rightarrow a^{-1}=-a\in E\text{ if }a\in E.
\end{aligned}$$

Conclusion: $(E,*)$ is an abelian group.

Exercise 02: Let $E=\mathbb{R}-\{-3\}$ be a set and $*$ is defined by :

$$\forall(a,b)\in E^2, a*b=ab+3(a+b+2).$$

(1) Verify that $*$ is a closure law (binary operation) in E.

(2) Show that $(E,*)$ is an abelian group.

(3) Let f be the application:

$$\begin{aligned}
f &: (\mathbb{R}^*,\cdot)\to(E,*)\\
x &\mapsto f(x)=x-3.
\end{aligned}$$

Show that f is a group homomorphism. ($\cdot$ is the usual mutiplication)

Correction:

(1) verify that $*$ is a binary operation in E.

$*$ is a binary operation in E if:

$$a*b=ab+3\,(a+b+2)\neq -3.$$

So,

$$\begin{aligned}
ab+3\,(a+b+2) &= -3 \Rightarrow ab+3a+3b+9=0 \\
&\Rightarrow (a+3)\,(b+3)=0, \\
&\Rightarrow a=-3 \text{ or } b=-3 \text{ contradiction with } a,b\in E\ .
\end{aligned}$$

Then:

$$\forall\,(a,b)\in E^2, a*b\in E\Rightarrow * \text{ is a closure law in } E.$$

(2) Show that $(E,*)$ is an abelian group.

(a) The commutativity: $\forall\,(a,b)\in E^2$,

$$a*b=ab+3\,(a+b+2)=ba+3\,(b+a+2)=b*a,$$

then $*$ is commutative.

(b) The associativity: $\forall a,b,c\in E; (a*b)*c=a*(b*c)$?

Let $a,b,c\in E$;

$$(a*b)*c=[ab+3\,(a+b+2)]*c$$

$$\begin{aligned}
&= [ab+3\,(a+b+2)]\,c+3\,[(ab+3\,(a+b+2)+c+2)] \\
&= abc+3ac+3bc+9c+3ab+9a+9b+24...(1)
\end{aligned}$$

and

$$a*(b*c)=a*(bc+3(b+c+2)$$

$$\begin{aligned}
&= a\,(bc+3(b+c+2)+3\,[a+bc+3\,(b+c+2)+2] \\
&= abc+3ab+3ac+9a+3bc+9b+9c+24,...(2)
\end{aligned}$$

$$(1)=(2)\Rightarrow (a*b)*c=a*(b*c)\,.$$

Then $*$ is associative.

(c) The existence of the identity element in E? Show that:

$$\forall a\in E,\exists e\in E, a*e=a?$$

$$\begin{aligned}
a*e &= a\Rightarrow ae+3\,(a+e+2)=a \\
&\Rightarrow ae+3e=-3a-6+a \\
&\Rightarrow e\,(a+3)=-2a-6, \\
&\Rightarrow e=\frac{-2a-6}{(a+3)}=-2\frac{(a+3)}{(a+3)}=-2\in E \text{ because } a\neq -3.
\end{aligned}$$

Then the identity element is $e = -2$.

(d) The existence of the inverse element for each element $a \in E$?
a admits a symmetric element a^{-1} if:

$$\begin{aligned} \forall a &\in E, a * a^{-1} = e = -2 \Rightarrow aa^{-1} + 3\left(a + a^{-1} + 2\right) = -2, \\ &\Rightarrow aa^{-1} + 3a^{-1} = -2 - 3a - 6 \\ &\Rightarrow a^{-1}(a+3) = -8 - 3a \\ &\Rightarrow a^{-1} = \frac{-3a-8}{a+3} \text{ that exists } \forall a \in E, \text{ because } a \neq -3. \end{aligned}$$

Conclusion: $(E, *)$ is an abelian group.

(3) Let the application:

$$\begin{aligned} f &: (\mathbb{R}^*, \times) \rightarrow (E, *) \\ x &\mapsto f(x) = x - 3. \end{aligned}$$

Show that f is a group homomorphism.

(a) Note that: $(\mathbb{R}^*, \times)$ and $(E, *)$ are two groups.

(b) In addition:

$$\forall x, y \in \mathbb{R}^*, f(x \times y) = (x \times y) - 3 = xy - 3,$$

and

$$\begin{aligned} f(x) * f(y) &= (x-3) * (y-3) \\ &= (x-3)(y-3) + 3\left[(x-3) + (y-3) + 2\right] \\ &= xy - 3x - 3y + 9 + 3x + 3y - 12 \\ &= xy - 3. \end{aligned}$$

Then:

$$\forall x, y \in \mathbb{R}^*, f(x \times y) = f(x) * f(y).$$

Conclusion: f is a group homomorphism.

Exercise 03: Let $(G, *)$ be an abelian group.

Reminder: If E is a group and F is subset of E, so F is a subgroup of E and we write $F \subseteq E$ if and only if:

$$\begin{aligned} 1) e_E &\in F. \\ 2) \forall x, y &\in F, x * y \in F \ (* \text{ is a closure law in } F) \\ 3) \forall x &\in F, x^{-1} \in F. \end{aligned}$$

Or:

$$\begin{aligned} 1) e_E &\in F. \\ 2) \forall x, y &\in F, x * y^{-1} \in F. \end{aligned}$$

(1) If $H = \{x \in G : x = x^{-1}\}$, that is, H consists of all elements of G wich are their own inverses, prove that H is a subgroup of G.

$$\begin{aligned}
H &= \left\{\alpha / \underbrace{P(\alpha)}_{\text{Properties}}\right\} \\
1)\alpha &\rightarrow e, P(e) \text{ is true? } \left(e^{-1} = e\right) \\
2)\forall \alpha_1, \alpha_2 &\in H \rightarrow \alpha_1 * \alpha_2 \in H? \rightarrow P(\alpha_1 * \alpha_2) \text{ is true?} \\
3)\forall \alpha &\in H \rightarrow \alpha^{-1} \in H? \rightarrow P\left(\alpha^{-1}\right) \text{ is true?} \\
\left(x^{-1}\right)^{-1} &= x \text{ and } (x * y)^{-1} = y^{-1} * x^{-1}.
\end{aligned}$$

$$H = \left\{\underbrace{x \in G : x = x^{-1}}_{P(x)}\right\}.$$

(a) Show that $e \in H$ ($P(e)$ is it true?). We have:

$$\begin{aligned}
e &\in G \text{ (G is a group) and } e * e = e \\
&\Rightarrow e = e^{-1} \Rightarrow P(e) \text{ is true} \Rightarrow e \in H.
\end{aligned}$$

(b) Show that $\forall x_1, x_2 \in H, x_1 * x_2 \in H? (P(x_1 * x_2)$ is it true?)

$$\forall x_1, x_2 \in H \Rightarrow x_1, x_2 \in G \Rightarrow x_1 * x_2 \in G \text{ (G is a group).}$$

In addition,

$$\begin{aligned}
x_1 * x_2 &= x_1^{-1} * x_2^{-1} \text{ because } x_1, x_2 \in H \\
&= (x_2 * x_1)^{-1} \\
&= (x_1 * x_2)^{-1} \text{ because } * \text{ is commutative} \\
&\Rightarrow x_1 * x_2 \in H.
\end{aligned}$$

(c) Show that $\forall x \in H, x^{-1} \in H?$ ($P(x^{-1})$ is it true?)

$$\forall x \in H \Rightarrow x \in G \Rightarrow x^{-1} \in G \text{ (G is a group).}$$

In addition,

$$\begin{aligned}
x &\in H \Rightarrow x^{-1} = x = \left(x^{-1}\right)^{-1} \\
&\Rightarrow x^{-1} \in H.
\end{aligned}$$

Conclusion: H is subgroup of G.

(2) Let n be a fixed integer, and let $H = \left\{x \in G : \underbrace{x * x * \ldots * x}_{n \text{ times}} = e\right\}$. prove that H is a subgroup of G.

<u>Remark:</u> We can write $\underbrace{x * x * \ldots * x}_{n \text{ times}} = x^n$.

(a) Show that $e \in H$. We have:

$$e \in G, \underbrace{e * e * ... * e}_{n \text{ times}} = e^n = e \Rightarrow e \in H.$$

(b) Show that $\forall x_1, x_2 \in H, x_1 * x_2 \in H$?

$$\forall x_1, x_2 \in H \Rightarrow x_1, x_2 \in G \Rightarrow x_1 * x_2 \in G \ (G \text{ is a group}).$$

In addition,

$$\begin{aligned} \underbrace{(x_1 * x_2) * (x_1 * x_2) * ... * (x_1 * x_2)}_{n \text{ times}} &= \underbrace{x_1 * ... * x_1}_{n \text{ times}} * \underbrace{x_2 * ... * x_2}_{n \text{ times}} \text{because } * \text{ is commutative} \\ &= e * e = e \text{ because } x_1, x_2 \in H \\ &\Rightarrow x_1 * x_2 \in H. \end{aligned}$$

(c) Show that $\forall x \in H, x^{-1} \in H$?

$$\forall x \in H \Rightarrow x \in G \Rightarrow x^{-1} \in G \ (G \text{ is a group}).$$

In addition,

$$\begin{aligned} \underbrace{x^{-1} * ... * x^{-1}}_{n \text{ times}} &= (\underbrace{x * ... * x}_{n \text{ times}})^{-1} = e^{-1} = e \text{ because } x \in H \\ &\Rightarrow x^{-1} \in H. \end{aligned}$$

Conclusion: H is subgroup of G.

Exercise 04: Let $\varphi : (G, *) \to (H, \triangle)$ be a group homomorphism. The kernel of φ is defined to be the set:

$$\ker \varphi = \{g \in G / \varphi(g) = e_H\} \subset G.$$

$$\forall x, y \in G, \varphi(x * y) = \varphi(x) \triangle \varphi(y) \text{ with } (G, *) \text{ and } (H, \triangle) \text{ are groups.}$$

Prove that $\ker \varphi$ is a subgroup of G.

(a) Show that $e_G \in \ker \varphi$.We have $e_G \in G$ because G is a group. We have:

$$\forall x \in G, \varphi(x) = \varphi(x * e_G) = \varphi(x) \triangle \varphi(e_G),$$

and

$$\begin{aligned} \varphi(x) &= \varphi(e_G * x) = \varphi(e_G) \triangle \varphi(x), \\ &\Rightarrow \varphi(e_G) = e_H \text{ (The identity element is unique) with } e_G \in G \\ &\Rightarrow e_G \in \ker \varphi. \end{aligned}$$

(b) Show that $\forall g_1, g_2 \in \ker \varphi, g_1 * g_2 \in \ker \varphi$?

$$\begin{aligned} \forall g_1, g_2 &\in \ker \varphi \Rightarrow g_1, g_2 \in G \\ &\Rightarrow g_1 * g_2 \in G \ (G \text{ is a group}) \\ \varphi(g_1 * g_2) &= \varphi(g_1) \triangle \varphi(g_2) = e_H \triangle e_H = e_H. \\ &\Rightarrow g_1 * g_2 \in \ker \varphi. \end{aligned}$$

(c) Show that $\forall g \in \ker\varphi, g^{-1} \in \ker\varphi$?

$$\begin{aligned}
\forall g &\in \ker\varphi \Rightarrow g \in G \Rightarrow g^{-1} \in G \\
\varphi\left(g^{-1}\right) &= \varphi\left(g^{-1}\right) \triangle e_H = \varphi\left(g^{-1}\right) \triangle \varphi\left(g\right), x \in \ker\varphi \\
&\Rightarrow \varphi\left(g^{-1}\right) = \varphi\left(g^{-1} * g\right), \varphi \text{ is group homomorphism} \\
&\Rightarrow \varphi\left(g^{-1}\right) = \varphi\left(e_G\right) = e_H \text{ using the first propertie.} \\
&\Rightarrow \varphi\left(g^{-1}\right) \in \ker\varphi.
\end{aligned}$$

Conclusion: $\ker\varphi$ is subgroup of G.