Structures algébriques usuelles

I - Groupes :

1/ Loi de composition interne (LCI)

Def 1 :

Soit G un ensemble non vide.
On appelle **Loi de composition interne** sur G, toute application de $G \times G$ vers G

NB : 1/ Notons par exemple $T : G \times G \longrightarrow G$ une **LCI** sur G.

$$(x,y) \longrightarrow T(x,y)$$

On notera désormais xTy au lieu de $T(x,y)$.

2/ En pratique, on définit une LCI par la donnée de xTy ; voir ci-après pour les LCI usuelles qu'on aura à manipuler le plus souvent.

3/ Soit T est une LCI sur G, on a donc :

$$\forall x,y \in G, \ (xTy) \in G$$

Exemples usuels de LCI 1 :

1/ L'addition "+" dans $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{N}$
En effet : Par exemple, $\forall x,y \in \mathbb{Z}$, $x+y \in \mathbb{Z}$

2/ Le produit "×" dans $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{N}$
En effet : Par exemple $\forall x,y \in \mathbb{N}$, $x \times y \in \mathbb{N}$

3/ Le produit "×" est une LCI aussi sur :
$\mathbb{R}^{+*} =]0,+\infty[$, $\mathbb{R}^*$, $\mathbb{C}^*$, $\mathbb{U}$, $\mathbb{U}_n$ (où $n \geq 1$), $\mathbb{Q}^*$, $\mathbb{Q}^{*+}$

Vocabulaire :

Soit E un ensemble non vide.

Une bijection de E sur E s'appelle *permutation* de E.

Notation :

S_E : L'ensemble des permutations dans E.

Exemples de LCI usuelles :

E étant un ensemble non vide.

1/ La composition "$\circ$" est une lci sur $E^E = \mathcal{F}(E,E)$.

2/ "$\circ$" est aussi une LCI sur S_E.

En effet :

2/ si f et $g \in S_E$ alors $f \circ g \in S_E$

Car la composée de deux bijections est une bijection.

Exemple 3 : (de LCI usuelles)

X un ensemble non vide quelconque.

$\mathbb{R}^X = \mathcal{F}(X,\mathbb{R})$, l'ens des applic de X vers $\mathbb{R}$.

1/ "$+$" est une LCI sur $\mathcal{F}(X,\mathbb{R})$

où $\left\{\begin{array}{l} \text{si } f \text{ et } g \in \mathcal{F}(X,\mathbb{R}) \\ f+g : X \longrightarrow \mathbb{R} \\ \qquad x \longmapsto \underbrace{f(x)}_{\in\mathbb{R}} + \underbrace{g(x)}_{\in\mathbb{R}} \end{array}\right.$

2/ "$\times$" est une LCI sur $\mathcal{F}(X,\mathbb{R})$.

où $\left\{\begin{array}{l} \text{si } f \text{ et } g \in \mathcal{F}(X,\mathbb{R}) \\ f \times g : X \longrightarrow \mathbb{R} \\ \qquad x \longmapsto \underbrace{f(x)}_{\in\mathbb{R}} \times \underbrace{g(x)}_{\in\mathbb{R}} \end{array}\right.$

NB$_1$: "$+$" et "$\times$" sont aussi deux lois de LCI sur $\mathcal{F}(X,\mathbb{C})$.

NB2 : "$+$" et "$\times$" sont deux LCI sur $\mathcal{F}(\mathbb{N},\mathbb{R})=\mathbb{R}^{\mathbb{N}}$ et $\mathbb{C}^{\mathbb{N}}$; l'ensemble des suites réelles et complexes.

NB3 : "$+$" et "$\times$" sont des LCI sur

1) $\mathcal{F}([0,1],\mathbb{R})$ et $\mathcal{F}([0,1],\mathbb{C})$.
2) $\mathcal{F}([0,+\infty[,\mathbb{R})$ et $\mathcal{F}([0,+\infty[,\mathbb{C})$
3) $\mathcal{F}(I,\mathbb{K})$ où I intervalle non vide et $\mathbb{K}=\mathbb{R}$ ou $\mathbb{C}$.

Déf 2 : Soit $*$ une LCI sur E.

1) Commutativité :

$*$ est dite commutative si et ssi $(\forall x,y\in E,\ x*y=y*x)$

2) Associativité :

$*$ est dite associative si et ssi $(\forall x,y,z\in E,\ (x*y)*z=x*(y*z))$

3) Element neutre :

Soit $e\in E$

e est dite element neutre si et ssi :

$$\forall x\in E,\ \begin{cases} x*e=x \\ e*x=x \end{cases}$$

4) Élement inversible :

Soit $a\in E$, Soit e l'élement neutre.

a est dite inversible si et ssi : $\exists b\in E$ $\begin{cases} a*b=e \\ \text{et} \\ b*a=e \end{cases}$

Voc et notation :

Dans ce cas, b s'appelle l'inverse de a et se note a^{-1}.

5) Distributivité

$*$ et T deux LCI sur E.
On dit que $*$ est distributive par rapport à T.
si et ssi :
$$\forall x,y,z \in E, \quad x*(yTz) = (x*y)T(x*z)$$

NB :

1) Supp a est inversible, on a : $\begin{cases} a*a^{-1}=e \\ a^{-1}*a=e \end{cases}$

2) e inversible et $e^{-1}=e$

car $e*e=e$.

Prop 3 : Supp que a et b sont inversibles.
$*$ étant associative
Alors $(a*b)$ est aussi inversible et on a
$$(a*b)^{-1} = b^{-1}*a^{-1}$$

Démo :

M que $(a*b)*(b^{-1}*a^{-1}) = e$ On a :

$$(a*b)*(b^{-1}*a^{-1}) = a*\underbrace{b*b^{-1}}_{=e}*a^{-1}$$
$$= \underbrace{a*e}_{=a}*a^{-1} = a*a^{-1} = e$$

De même, on montre que $(b^{-1}*a^{-1})*(a*b) = e$

d'où $\begin{cases} (a*b) \text{ inversible} \\ \text{et } (a*b)^{-1} = b^{-1}*a^{-1} \end{cases}$

Déf 4 : (Partie stable par $*$)

Soit $*$ une LCI sur E.
Soit H une partie de E.
H est dite stable par $*$ si et ssi
$(\forall x, y \in H, x * y \in H)$

Exemple :

1/ Ici $\mathbb{C}$ est muni de la LCI $+$:
Les parties suivantes de $\mathbb{C}$ stables par $+$:
$\mathbb{C}, \mathbb{R}, \mathbb{Q}, \mathbb{Z}, \mathbb{N}$ et $n\mathbb{Z} = \{nk, k \in \mathbb{Z}\}$.

2/ Ici $\mathbb{C}$ est muni de $\times$:
Les parties suivantes sont stables par $\times$.
→ $\mathbb{C}, \mathbb{R}, \mathbb{Q}, \mathbb{N}$
→ $\mathbb{C}^*, \mathbb{R}^*, \mathbb{R}^{+*}$
→ $\mathbb{U}, \mathbb{U}_n$ $(n \in \mathbb{N}^*)$

2°/ Groupes :

Déf 1 : Soit $*$ une LCI sur l'ensemble non vide G.
$(G, *)$ est dit groupe si et ssi :
1/ $*$ est associative
2/ $*$ admet un élément neutre.
3/ Tout élément de G est inversible.

Vocabulaire :

Si $(G, *)$ est un groupe et que $*$ est commutative, on dit que $(G, *)$ est un groupe commutatif ou abelien.

Exemples usuels de groupes (à savoir)

Exemples de groupes additifs (càd avec la loi $+$) et abeliens :

$(\mathbb{C},+)$, $(\mathbb{R},+)$, $(\mathbb{Q},+)$, $(\mathbb{Z},+)$

NB : 1/ L'élément neutre est 0.

2/ L'inverse de a est $(-a)$ (l'opposé de a)

Exemples de groupe abeliens multiplicatifs.

(càd avec la loi $\times$).

$(\mathbb{C}^*,\times)$, $(\mathbb{R}^*,\times)$; $(\mathbb{Q}^*,\times)$

$(\mathbb{U},\times)$; $(\mathbb{U}_n,\times)$

Démo : (Faite oralement en classe)

R/R

1/ Si on lit « considérons le groupe $\mathbb{R}$ », la lci est $+$.

2) Si on lit « considérons le groupe $\mathbb{R}^*$ », la lci est $\times$.

NB :

1°/ $(\mathbb{R}^*, +)$ n'est pas un groupe.

2°/ $(\mathbb{R}, \times)$ " " " " .

En effet :

1/ $+$ n'est pas une LCI sur $\mathbb{R}^*$.

2/ 0 n'est pas inversible.

Prop2 :

X un ensemble non vide (qlq).

$\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$.

$(\mathbb{K}^X, +)$ est un groupe abélien d'élément neutre la fonction nulle.

Prop3 :

E est un ensemble non vide.

$(S_E, \circ)$ est un groupe d'élément neutre I_E.

Démo : En bref

1/ $\circ$ est associative

2/ L'élément neutre est I_E car

$$\forall f \in S_E, \quad \begin{cases} f \circ I_E = f \\ I_E \circ f = f \end{cases}$$

3/ Si $f \in S_E$, on a $\begin{cases} f \circ f^{-1} = I_E \\ f^{-1} \circ f = I_E \end{cases}$

d'où f est inversible et son inverse est f^{-1}.

NB : $(S_E, \circ)$ n'est en général pas commutatif.

NB₂ : S_E s'appelle le groupe symétrique sur E.
d'où la notation S_E.

Notation :

1/ Si $(G,\times)$ groupe d'élément neutre 1.
Soit $a \in G$, soit $n \in \mathbb{N}^*$.
$\underbrace{a \times \cdots \times a}_{n \text{ fois}}$ se note a^n ; et $a^0 = 1$ par convention

2/ Si $(G,+)$ groupe d'élément neutre 0.
Soient $a \in G$ et $n \in \mathbb{N}^*$.
$\underbrace{a + \cdots + a}_{n \text{ fois}}$ se note na ; et $0.a = 0$ par convention.

NB₁ : Ici $(G,\times)$ est un groupe multiplicatif.
Soient $a \in G$ et $n \in \mathbb{N}$.
On a $(a^n)^{-1} = (a^{-1})^n = a^{-n}$

NB₂ : Ici $(G,+)$ est un groupe additif.
Soient $a \in G$ et $n \in \mathbb{N}$.
On a $-(na) = n(-a) = (-n)a$.

3/ Sous-groupes

Def 1 :
Soient $(G,*)$ un groupe d'élément neutre e, et $H \subset G$.
H est dit sous groupe de G si et ssi
1/ $e \in H$
2/ $\forall x, y \in H$, $x * y \in H$
3/ $\forall x \in H$, $x^{-1} \in H$

NB$_1$: Ici $(G,+)$ est un groupe d'élément neutre 0, et $H \subset G$; H est dit un **sous-groupe** de G si et ssi

1) $0 \in H$
2) $\forall x, y \in H$, $x+y \in H$
3) $\forall x \in H$, $(-x) \in H$

Prop2 :

$(G,*)$ est un groupe et $H \subset G$, On a :

$$H \text{ sous-groupe de } G \iff \begin{cases} i) & e \in H \\ ii) & \forall x,y \in H,\ x*y^{-1} \in H \end{cases}$$

NB$_1$: Ici $(G,+)$ groupe d'élément neutre 0 et $H \subset G$, On a :

$$H \text{ est s-groupe de } G \iff \begin{cases} i) & 0 \in H \\ ii) & \forall x,y \in H,\ x-y \in H \end{cases}$$

Démo de prop2 :

Par double implication :

$(\Longrightarrow)$ i) OK (c'est 1)

ii) Soient x et $y \in H$. M.q $x*y^{-1} \in H$

$y \in H \Longrightarrow y^{-1} \in H$ (c'est 3)

$x \in H$ et $y^{-1} \in H \Longrightarrow x*y^{-1} \in H$ (c'est 2)

$(\Longleftarrow)$

1) OK (C'est i)

3) Soit $x \in H$. Mque $x^{-1} \in H$.

On a e et $x \in H \overset{ii)}{\Longrightarrow} \underbrace{e*x^{-1}}_{x^{-1}} \in H$

$\Longrightarrow x^{-1} \in H$.

2) Soient $x, y \in H$. Mque $x*y \in H$

$x*y = x*(y^{-1})^{-1} \in H$, grace à $ii)$
et du fait que $y^{-1} \in H$ (3°)

Exemples :

1/ $\forall n \in \mathbb{N}$, $n\mathbb{Z}$ est un s-groupe de $(\mathbb{Z},+)$.
2/ $\mathbb{R}^{+*}$ et $\{-1,1\}$ deux s-groupes de $(\mathbb{R}^*,\times)$.
3/ $\mathbb{U}$ et $\mathbb{U}_n$ deux s-gr de $(\mathbb{C}^*,\times)$.

NB : $\{e\}$ et G sont deux sous groupes de $(G,*)$.

Prop 3 :
Si H est un s-groupe du groupe $(G,*)$
alors $(H,*)$ est aussi un groupe

Démo (Faite oralement en classe)

Remarque pratique :
Pour montrer qu'un ensemble est un groupe, des fois il est plus facile de procéder en montrant que c'est un sous groupe.

Exemple : (Traiter l'ex 4 du TD)

Prop 4 (Intersection de s-gr)
Soit $(G,*)$ un groupe.
Toute intersection de sous groupes de G est un sous-groupe de G.

Càd : Si $(H_i)_{i\in I}$ est une famille de s-gr de G
alors $\bigcap_{i\in I} H_i$ est un s-gr de G.

Démo : Supp que ($\forall i \in I$, H_i est un s-gr de G)

Montrons que $\bigcap_{i\in I} H_i$ est un s-gr de G.

Rappel : $x \in \bigcap_{i\in I} H_i \Longleftrightarrow (\forall i \in I, x \in H_i)$

1) $e \in \bigcap_{i\in I} H_i$, car ($\forall i \in I, e \in H_i$) puisque ce sont des sous-groupes de G.

2) Soient x et $y \in \bigcap_{i\in I} H_i$. M.que $(x * y^{-1}) \in \bigcap_{i\in I} H_i$.

On a $(\forall i \in I, x$ et $y \in H_i)$

$\Longrightarrow (\forall i \in I, x * y^{-1} \in H_i)$, car H_i est s-gr de G.

D'où $x * y^{-1} \in \bigcap_{i\in I} H_i$

Attention

La réunion de deux s-gr n'est en général pas un s-gr.

Exo 5 : du TD, on a :

($H \cup K$ s-gr de G) $\Longleftrightarrow$ ($H \subset K$ ou $K \subset H$).

II - Anneaux :

1/ Déf et exemples :

Déf 1

Soit A un ensemble non vide muni de deux LCI "+" et "×".

On dit que $(A, +, \times)$ est un anneau si et ssi :

1/ $(A, +)$ est un groupe commutatif (avec la $1^{ère}$ loi).

2/ × est associative et admet un élément neutre ($2^{ème}$ loi).

3/ × est distributive par rapport à +

R/R :

1/ Dans un anneau, on a 2 LCI.

2/ Leur ordre importe.

Vocabulaire : Si la loi $\times$ est commutative on dit que l'anneau $(A,+,\times)$ est commutatif.

Exemple 1 :

1) $(\mathbb{Z},+,\times)$ anneau commutatif

2) Idem pour $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{C}$.

Exemple 2 :

$\mathbb{K}=\mathbb{R}$ ou $\mathbb{C}$. X ensemble non vide qlque.
$(\mathbb{K}^X,+,\times)$ est un anneau commutatif d'éléments neutres respectifs la fonction nulle 0 et la fonction constante 1.

Exemple 3 :

Cas particulier de l'exemple 2 avec $\mathbb{N}=X$.
L'ensemble des suites $\mathbb{R}^{\mathbb{N}}$ (resp complexes $\mathbb{C}^{\mathbb{N}}$) est un anneau commutatif d'éléments neutres resp la suite nulle et la suite constante 1.

2/ Anneau intègre

R/R : Soit $(A,+,\times)$ un anneau. On sait que :

$$\forall a,b\in A,\ (a=0 \text{ ou } b=0)\Rightarrow ab=0$$

Mais la réciproque n'est pas tj vraie (voir plus tard)

Déf : Soit $(A,+,\times)$ un anneau.
A est dit **anneau intègre** si et ssi :

$$\forall a,b \in A,\ ab=0 \Rightarrow (a=0 \text{ ou } b=0)$$

NB₁ : Dans un anneau intègre on a :

$$ab=0 \Leftrightarrow (a=0 \text{ ou } b=0)$$

NB₂ : Si A intègre on a :

$$ab \neq 0 \Leftrightarrow (a\neq 0 \text{ et } b\neq 0)$$

Exemples d'anneaux intègres :
$(\mathbb{Z},+,\times)$; $(\mathbb{Q},+,\times)$; $(\mathbb{R},+,\times)$ et $(\mathbb{C},+,\times)$ sont des anneaux intègres.

Exemple 2 : (Un anneau non intègre)

Définissons sur $\mathbb{R}^2$ les deux lois usuelles $+$ et $\times$:

$$(a,b)+(a',b')=(a+a',\ b+b')$$

$$(a,b)\times(a',b')=(aa',\ bb')$$

1/ Mq $(\mathbb{R}^2,+,\times)$ est un anneau et préciser ses éléments neutres.

2/ Mq $\mathbb{R}^2$ n'est pas un anneau intègre

Sol :

1/ OK (démo faite

$(0,0)$ l'élément neutre pour $+$.
$(1,1)$ l'élément neutre pour $\times$.

2) $(\mathbb{R}^2, +, \times)$ n'est pas intègre car :

$$\begin{cases} (1,0) \times (0,1) = (0,0) \\ \text{mais } (1,0) \neq (0,0) \text{ et } (0,1) \neq (0,0) \end{cases}$$

Exemple 3 (Un 2ème anneau non intègre)

L'anneau $(\mathbb{R}^{\mathbb{R}}, +, \times)$ n'est pas intègre

Démo :

Trouver deux fonctions f et $g \in \mathbb{R}^{\mathbb{R}}$ telles que

$f \neq 0$, $g \neq 0$ mais $f \times g = 0$

Par exemple :

$$f(x) = \begin{cases} 0 & \text{si } x \leq 1 \\ 2021 & \text{si } x > 1 \end{cases} \qquad g(x) = \begin{cases} ? & \text{si } x \leq 1 \\ ? & \text{si } x > 1 \end{cases}$$

Exemple 4 : (Un 2ème anneau non intègre)

$(\mathbb{R}^{\mathbb{N}}, +, \times)$ n'est pas intègre.

Démo (en exo)

3) Calculs dans un anneau

Prop 1 :

Soit $(A, +, \times)$ anneau. On a :

$$\forall a \in A, \ 0 \times a = 0 \text{ et } a \times 0 = 0$$

Démo :

$$0 \times a = (0+0)\cdot a$$
$$0\times a = 0\times a + 0\times a$$
$$0\times a - (0\times a) = 0\times a$$
$$0 = 0\times a$$

Réflexes sur les groupes :

1/ $(G, \cdot)$ groupe d'élément neutre e.

$ab = c \Leftrightarrow b = a^{-1}c$; (non pas : $b = ca^{-1}$)

$ab = ac \Leftrightarrow b = c$

2/ $(G, +)$ groupe d'élément neutre e

$a+b = c \Leftrightarrow b = -a + c$

$a+b = c \Leftrightarrow a = c - b$ (non pas $a = -b + c$)

$a+b = a+c \Leftrightarrow b = c$

Prop :

$(A, +, \times)$ anneau.

Soient a et $b \in A$ tq $ab = ba$. On a :

1/ $\forall n \in \mathbb{N},\ (ab)^n = a^n b^n$

2/ $\forall n \in \mathbb{N},\ (a+b)^n = \sum_{k=0}^{n} C_n^k a^k b^{n-k}$

Formule de binôme de Newton

3/ $\forall n \in \mathbb{N},\ a^n - b^n = (a-b)\sum_{k=0}^{n-1} a^{n-1-k} b^k$

Egalité de Bernoulli

4) Éléments inversibles d'un anneau.

Déf 1 :
Soit $(A,+,\times)$ un anneau.
Les éléments inversibles de A sont les inversibles pour la 2ème loi $\times$.

NB : Pour la 1ère loi $+$, tous les éléments sont inversibles puisque $(A,+)$ est un groupe.

Notation :
$\sqcup(A)$: désignera l'ensemble des éléments inversibles de A.

Prop 2 : Soit $(A,+,\times)$ un anneau.
$(\sqcup(A),\times)$ est un groupe.

R/R : $(\sqcup(A),\times)$ est le groupe des éléments inversibles de A.

Démo de la prop 2 :
Il s'agit de montrer les points suivants :

1) $\times$ est une lci sur $\sqcup(A)$
2) $\times$ est associative
3) $\times$ admet un élément neutre dans $\sqcup(A)$
4) Tout élément de $\sqcup(A)$ est inversible dans $\sqcup(A)$.

Pour 1) : Càd $\left(\forall x,y \in \sqcup(A),\ x\times y \in \sqcup(A)\right)$
C'est vérifié car le produit de deux éléments inversibles est un élément inversible.

Pour 2) : $\times$ associative dans $\mathcal{U}(A)$ car assoc dans A.

Pour 3) : On a $\begin{cases} \forall x \in \mathcal{U}(A),\ x \times 1 = 1 = 1 \times x \\ \text{et } 1 \in \mathcal{U}(A),\ \text{car } 1 \text{ inversible} \end{cases}$

Pour 4) : Soit $x \in \mathcal{U}(A)$.

On a $\begin{cases} x \cdot x^{-1} = 1 \\ x^{-1} \cdot x = 1 \end{cases}$

$\Rightarrow x^{-1}$ inversible ; càd $x^{-1} \in \mathcal{U}(A)$

Ainsi : x inversible dans $\mathcal{U}(A)$

NB $\mathcal{U}(A)$ se note aussi $A^{\times}$

Exemples

L'anneau $(A,+,\times)$	Le groupe $(\mathcal{U}(A),\times)$
$(\mathbb{C},+,\times)$	$(\mathbb{C}^*,\times)$
$(\mathbb{R},+,\times)$	$(\mathbb{R}^*,\times)$
$(\mathbb{Q},+,\times)$	$(\mathbb{Q}^*,\times)$
$(\mathbb{Z},+,\times)$	$(\{-1,1\},\times)$

5) Corps

Déf 1

Soit $(K,+,\times)$ un anneau commutatif, non réduit à $\{0\}$.
$(K,+,\times)$ est un corps si et seulement si tout élément non nul de K est inversible.

Exemples usuels de corps

$(\mathbb{Q},+,\times)$; $(\mathbb{R},+,\times)$, $(\mathbb{C},+,\times)$ sont des corps.

$(\mathbb{Z},+,\times)$ est un anneau intègre mais n'est pas un corps.

NB 1

1) Si $(K,+,\times)$ est un corps, alors $U(K)=K^*$.

2) Un corps est par définition commutatif.

NB 2 :

1) Tout corps est un anneau intègre.

2) La réciproque est en général fausse.

Démo de 1) :

Supp que $(K,+,\times)$ corps. Mq que K est intègre.
Soient a et $b \in K$ tels que $ab=0$.
Mq que $a=0$ ou $b=0$.
Raisonnons par l'absurde, et supposons que $a\neq 0$ et $b\neq 0$.
On a $a\neq 0 \Longrightarrow a$ inversible, car K corps.
Ainsi $ab=0 \Longrightarrow \underbrace{a^{-1}a}_{=1}b=0$

$\Longrightarrow b=0$; absurde car $b\neq 0$.

Fin