Structures algébriques

1 Loi de compositions internes

1.1 Notion de Magma

Définition – **Magma - loi de composition interne**
Soit E un ensemble non vide. On dit que $\star$ est une loi de composition interne sur E si $\star : E \times E \to E$ c'est à-dire si pour tout $x, y \in E$, $x \star y \in E$.
*On appelle **magma** tout ensemble muni d'une loi de composition interne, noté $(E, \star)$.*

Exemple
$(\mathbb{R}, \times)$, $(\mathbb{R}, +)$ sont des magmas ; mais la soustraction n'est pas une loi interne sur $\mathbb{N}$.

Exercice : Donner des exemples de magmas.

[1] à compléter

Solution –

[2] à compléter

Exemple
Compléter le tableau de la LCI $\times$ sur $E = \{\pm 1, \pm i\}$

$\times$ ↱	1	-1	i	$-i$
1				
-1				
i				
$-i$				

1.2 Associativité et commutativité

Définition – **Associativité et commutativité**
Soit $(E, \star)$ un magma. On dit que :
(i) $(E, \star)$ est associatif si : $\forall x, y, z \in E, \quad a \star (b \star c) = (a \star b) \star c$
(ii) $(E, \star)$ est commutative si : $\forall x, y \in E, \quad a \star b = b \star a$

NOTATION – Lorsque la loi est associative, les parenthèses peuvent être omises.
- si la loi est multiplicative alors $x^n = \underbrace{x \times x \times \cdots \times x}_{n \text{ fois}}$
- si la loi est additive alors $nx = \underbrace{x + x + \cdots + x}_{n \text{ fois}}$

[3] à compléter

Exercice : Donner des exemples de magmas en précisant la nature de la LCI.

Solution –

Exercice : Montrer que $\mathbb{R}$ muni de $\star : (x, y) \mapsto x^2 y^2$ est un magma commutatif mais non associatif.

[4] à compléter

Solution –

1.3 Élément neutre et inversibilité

Définition – Élément neutre
On appelle ***élément neutre*** *d'un magma $(E,\star)$, un élément $e \in E$ tel que pour tout $x \in E$, $x\star e = e\star x = x$.*

Proposition – *Si un magma possède un élément neutre alors il est unique.*

[5] à compléter

Démonstration –

■

Proposition - Définition – Élément inversible
Soit $(E,\star)$ un magma associatif possédant un élément neutre. Un élément $x \in E$ est dit inversible s'il existe $y \in E$ tel que $x \star y = y \star x = e$ En particulier, l'inverse est unique, on le note x^{-1}.

[6] à compléter

Démonstration –

■

Remarque – On trouve la terminologie de *symétrique* pour définir l'inverse d'un élément. Lorsuqe la loir est additive, on parle d'opposé et o note $-x$.

[7] à compléter

Exercice : Compléter le tableau suivant :

magma	e	x^{-1}
$(\mathbb{R}^*, \times)$		
$(\mathbb{Z}, +)$		
$(\mathbb{R}^*, \div)$		
$(\mathcal{M}_n(\mathbb{R}), \times)$		
$(\mathcal{GL}_n(\mathbb{R}), \times)$		
$(\mathcal{T}_n^{\sup}(\mathbb{R}), +)$		
$(]1, +\infty[, \times)$		

Remarque – L'existence de l'élément neutre ou encore de l'inverse d'un élément n'est pas automatique.

Proposition – *Soit $(E,\star)$ un magma associatif et possédant un élément neutre ; alors,*
(i) Soit $x \in E$ inversible, pour $y, z \in E$, alors $x\star y = x\star z \quad \Rightarrow \quad y = z$; $y\star x = z\star x \quad \Rightarrow \quad y = z$
(ii) Soit $x, y \in E$ deux éléments inversibles ; alors $x\star y$ est inversible et $(x\star y)^{-1} = y^{-1}\star x^{-1}$.
(iii) Soit $x \in E$ inversible et $n \in \mathbb{N}^*$; alors, x^n est inversible et $\left(x^n\right)^{-1} = \left(x^{-1}\right)^n$ que l'on note x^{-n}.
(iv) Soit $x \in E$ inversible ; alors x^{-1} est inversible et $\left(x^{-1}\right)^{-1} = x$.

[8] à compléter

Démonstration –

■

1.4 Distributivité d'une loi sur une autre

Définition – Distributivité
Soit E un ensemble non vide et $\star, \diamond$ deux lois de composition interne. On dit que $\diamond$ est distributive sur $\star$ si pour tout $x, y, z \in E$, $x \diamond (y \star z) = (x \diamond y) \star (x \diamond z)$
$(y \star z) \diamond x = (y \diamond x) \star (z \diamond x)$

Exemples
1. La multiplication est distributive sur l'addition dans $\mathbb{R}$, $\mathcal{M}_n(\mathbb{R})$, ...
2. Dans $\mathcal{P}(E)$ où E est un ensemble, $\cap$ est distributive sur $\cup$ et $\cup$ est distributive sur $\cup$.

1.5 Partie stable par une loi

Définition – Partie stable
Soit $(E, \star)$ un magma et $A \subset E$. On dit que A est stable par $\star$ si pour tout $x, y \in A$, $x \star y \in A$.
On conserve la notation $\star$ pour la restriction de $\star$ sur A^2 ; en particulier, $(A, \star)$ est un magma.

Exemple
$\mathbb{R}_+$ est stable par $\times$ dans $(\mathbb{R}, \times)$, $\mathbb{R}_+^*$ et $[2, +\infty[$ aussi.

Remarques –

1. Les propriétés de la loi (associativité, commutativité, distributivité) s'héritent par stabilité ; c'est-à-dire si $(E, \star)$ est associatif alors $(A, \star)$ aussi ...
2. L'existence de l'élément neutre ou de l'inversibilité ne s'héritent pas.

[9] à compléter

Exercice : Donner des exemples et contre-exemple de caractères héréditaires ou non.

2 Structures de groupe

2.1 Groupes

Définition – Groupe
Un groupe est un magma associatif possédant un élément neutre et dont tous les éléments sont inversibles.

Notation – On note $(G, \times)$ pour un loi multiplicative et $(G, +)$ pour une loi additive. S'il n'y a pas de confusion possible, on note simple G.

Exemples
1. $(\mathbb{Z}, +)$, $(\mathbb{R}_+^*, \times)$, $(\mathcal{M}_n(\mathbb{R}), +)$, $(\mathrm{GL}_n(\mathbb{R}), \times)$, $(\mathbb{C}, +)$, $(\mathbb{C}^*, \times)$ sont des groupes.
2. $(\mathbb{Q}, \times)$, $(\mathbb{N}, +)$ sont seulement des magmas.

Proposition - Définition – Groupe des permutation
*Soit E un ensemble non vide. On appelle **permutation** tout application bijective de E^E.*
*On appelle **groupe symétrique** de E, noté $\mathcal{S}_E$, l'ensemble des permutations de E muni de la composition.*

[10] à compléter

Démonstration –

2.2 Sous-groupes

Définition – Sous-groupe

*Soit G un groupe et H une partie **non vide** de G. On dit que H est sous-groupe de G si :*

(i) H est stable par la loi de composition interne, et

(ii) H muni de cette loi est un groupe.

En particulier, le neutre est le même dans H et G, les inverses sont respectivement les mêmes.

Théorème – Caractérisation d'une sous-groupe

Soit $(G,\times)$ un groupe. H, une partie de G, est un sous-groupe de G si et seulement si :

(i) H est non vide,

(ii) $\forall x,y\in H,\quad x\times \underbrace{y^{-1}}_{\in G}\in H$.

[11] à compléter

Démonstration –

■

Remarques –

1. La stabilité par le "quotient" pour une loi multiplicative (et par la différence pour une loi additive) suffit à établir qu'une partie est un sous-groupe.
2. **Méthode :** , en pratique, pour montrer qu'un ensemble muni d'une loi est un groupe :
   - on considère un groupe usuel le contenant,
   - on applique la caractérisation d'un sous-groupe.
3. Dans un groupe, les éléments étant inversibles, la simplification est possible :

$$\forall x,y,z\in(G,\times),\quad ab=ac\quad\Rightarrow\quad b=c\qquad\text{(on applique } x^{-1}\text{ aux deux membres)}$$

4. Vocabulaire ; un groupe est dit commutatif, ou abélien, si sa loi de composition interne est commutative.

Exemples

1. Considérons $\mathbb{U}=\{z\in\mathbb{C};\ |z|=1\}=\{e^{i\theta},\theta\in\mathbb{R}\}$, $(\mathbb{U},\times)$ est un sous-groupe de $(\mathbb{C}^*,\times)$. En effet :

$$\forall\theta,\theta'\in\mathbb{R},\qquad e^{i\theta}\times\left(e^{i\theta'}\right)^{-1}=e^{i(\theta-\theta')}\in\mathbb{U}$$

2. Considérons $\mathbb{U}_n=\{z\in\mathbb{C};\ z^n=1\}=\{e^{i\frac{2k\pi}{n}},k\in[\![0,n-1]\!]\}$, $(\mathbb{U}_n,\times)$ est un sous-groupe de $(\mathbb{U},\times)$:

$$\forall k,k'\in[\![0,n-1]\!],\qquad e^{i\frac{2k\pi}{n}}\times\left(e^{i\frac{2k'\pi}{n}}\right)^{-1}=e^{i\frac{2(k-k')\pi}{n}}\in\mathbb{U}_n$$

3. $\left(\mathcal{T}_n^{inf}(\mathbb{K}),+\right)$ est un sous-groupe de $\left(\mathcal{M}_n(\mathbb{K}),+\right)$.
4. L'ensemble de matrices de $\mathcal{T}_n^{inf}(\mathbb{K})$ dont les coefficients diagonaux sont non nuls est un sous-groupe de $(\mathrm{GL}_n(\mathbb{K}),\times)$

Exercice : Soit E un ensemble non vide et $x\in E$. On note $\mathrm{Stab}(x)$ l'ensemble des permutations de E laissant x invariant. Montrer que $\mathrm{Stab}(x)$ est un sous-groupe de $\mathcal{S}_E$.

[12] à compléter

Solution –

■

2.3 Morphisme de groupes

Définition – Morphisme

Soit $(G, \triangleleft)$ et $(G', \square)$ deux groupes. On appelle ***morphisme*** *(de groupes) de G dans G' tout application $f : G \to G'$ telle que*

$$\forall x, y \in G, \quad f(x \triangleleft y) = f(x) \square f(y)$$

Remarque – Lorsque la loi n'est pas spécifique, on adopte la notation multiplicative de neutre 1_G et x^{-1} est l'inverse de x.

Vocabulaire :

- si f est bijective on dit que f est un **isomorphisme** de groupes ;
- si $G = G'$, on dit que f est un **endomorphisme** de groupe ;
- si $G = G'$ et f est bijective, on dit que f est un **automorphisme** de groupe.

Exemples

1. $f : t \mapsto |t|$ est un endomorphisme de $(\mathbb{R}^*, \times)$ et un morphisme de $(\mathbb{C}^*, \times)$ dans $(\mathbb{R}_+^*, \times)$: $\forall x, y,\ |xy| = |x|\,|y|$
2. exp est un isomorphisme de $(\mathbb{R}, +)$ dans $(\mathbb{R}_+^*, \times)$: $\forall x, y \in \mathbb{R},\ \exp(x+y) = \exp(x)\exp(y)$
3. $g : t \mapsto e^{it}$ est un morphisme de $(\mathbb{R}, +)$ dans $(\mathbb{U}, \times)$

Proposition – *Soient G, G' deux groupes et $f \in G'^G$ un morphisme de groupes.*

(i) $f(1_G) = 1_{G'}$

(ii) $\forall x \in G,\ f\left(x^{-1}\right) = f(x)^{-1}$

(iii) si H est un sous-groupe de G, alors $f(H)$ est un sous-groupe de G'

(iv) si H' est un sous-groupes de G', alors $f^{-1}(H')$ est un sous-groupe de G.

[13] à compléter

Démonstration –

■

Proposition – *Soient G, G', G'' trois groupes et $f \in G'^G$, $g \in G''^{G'}$ deux morphismes de groupes. Alors $g \circ f$ est un morphisme de G dans G''.*

[14] à compléter

Démonstration –

■

Définition - Théorème – Noyau, image

Soient G, G' deux groupes et $f \in G'^G$ un morphisme.

(i) On appelle ***image*** *de f l'ensemble $f(G)$, noté $\mathrm{Im}\,(f)$, qui est un sous-groupe de G'.*
De plus, f est surjective si et seulement si $\mathrm{Im}\,(f) = G'$.

(ii) On appelle ***noyau*** *de f l'ensemble $f^{-1}(\{1_{G'}\}) = \{x \in G ; f(x) = 1_{G'}\}$, noté $\mathrm{Ker}\,(f)$, qui est un sous-groupe de G.*

(iii) f est injective si et seulement si $\mathrm{Ker}\,(f) = \{1_G\}$

[15] à compléter

Démonstration –

■

Exemples

1. $f : t \mapsto |t|$ est un morphisme de $(\mathbb{C}^*, \times)$ dans $(\mathbb{R}_+^*, \times)$: $\mathrm{Ker}\,(f) = \{z \in \mathbb{C}^*;\ |z| = 1\} = \mathbb{U}$
2. $g : t \mapsto e^{it}$ est un morphisme de $(\mathbb{R}, \times)$ dans $(\mathbb{U}, \times)$: $\mathrm{Ker}\,(g) = \{t \in \mathbb{R};\ e^{it} = 0\} = \{t \in \mathbb{R};\ t \equiv 0\ [2\pi]\} = 2\pi\mathbb{Z}$

Exercice : Considérons $h : k \mapsto e^{i\frac{2k\pi}{n}}$.
1. Vérifier que h est un morphisme de $(\mathbb{Z}, +)$ dans $(\mathbb{U}, \times)$.
2. Déterminer $\mathrm{Ker}\,(h)$ et $\mathrm{Im}\,(h)$.

[16] à compléter

Solution –

Proposition –
(i) La composée de deux isomorphismes est un isomorphisme.
(ii) La bijection réciproque d'un isomorphisme de groupes est un isomorphisme de groupes.
(iii) La relation binaire "être isomorphe à" est une relation d'équivalence.

[17] à compléter

Démonstration –

Exercice : Montrer que l'ensemble des automorphismes d'un groupe est un groupe pour la composition.

[18] à compléter

Solution –

3 Structure d'anneau et de corps

3.1 Anneaux

Définition –
On appelle anneau ("unitaire"), tout triplet $(E, +, \times)$ tel que :
(i) E est muni de deux loi de composition internet : $+$ et $\times$
(ii) $(E, +)$ est un groupe commutatif (le neutre est noté 0_E)
(iii) $(E, \times)$ est un magma associatif possédant un élément neutre noté 1_E
(iv) la loi $\times$ est distributive sur $+$.
On dit que l'anneau est commutatif si le magma $(E, \times)$ est commutatif.

Exemple
$(\mathbb{Z}, +, \times)$, $(\mathbb{R}, +, \times)$, $(\mathbb{Q}, +, \times)$, $(\mathcal{M}_n(\mathbb{K}), +, \times)$ son des anneaux.

Théorème – Règles de calcul
Soient $(A, +, \times)$ un anneau et $a, b \in A$ alors :
(i) $a \times 0_A = 0_A \times a = 0_A$
(ii) $\forall n \in \mathbb{Z},\ n(ab) = (na)b = a(nb)$ et en particulier $-(ab) = (-a)b = a(-b)$.
(iii) $(-a)(-b) = ab$ et $(-1_A)^2 = 1_A$.
(iv) Si a et b commutent ($a \times b = b \times a$), alors pour tout $n \in \mathbb{N}$,

$$\underbrace{(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k}_{\text{formule du binôme}} \qquad a^n - b^n = (a-b) \sum_{k=0}^{n-1} a^{n-k} b^k$$

[19] à compléter

Démonstration –

Définition – **Anneau intègre**
Un anneau $(A,+,\times)$ est dit intègre si pour tout $a,b\in A$

$$ab=0_A \quad\Leftrightarrow\quad a=0_A \text{ ou } b=0_A$$

Exemple
$(\mathcal{M}_n(\mathbb{K}),+,\times)$ n'est pas intègre : $\begin{pmatrix}1&1\\0&0\end{pmatrix}\begin{pmatrix}1&0\\-1&0\end{pmatrix}=\begin{pmatrix}0&0\\0&0\end{pmatrix}$. $(\mathbb{C},+,\times)$ est un anneau intègre.

Exercice : Que dire de $(\mathrm{GL}_n(\mathbb{K}),+,\times)$, $(\mathbb{Q},+,\times)$, et $\left(\mathbb{R}^{\mathbb{R}},+,\times\right)$?

[20] à compléter

Solution –

Proposition - Définition – $U(A)$
On appelle groupe des inversibles, noté $U(A)$, l'ensemble des inversibles pour $\times$ de l'anneau $(A,+,\times)$.

[21] à compléter

Démonstration –

Exemple
$U(\mathbb{R})=\mathbb{R}^*$, $U(\mathbb{Z})=\{\pm1\}$, $U(\mathcal{M}_n(\mathbb{K}))=\mathrm{GL}_n(\mathbb{K})$.

3.2 Sous-anneaux

Définition –
Soit A un anneau, B une partie non vide de A. On dit que B est un sous-anneau de A si :
(i) B est stable pour les deux lois de composition interne
(ii) $1_A\in B$
(iii) B est un anneau pour les mêmes lois de composition interne.

Exemple
$(\mathbb{Z},+,\times)$ est un sous-anneau de $(\mathbb{Q},+,\times)$.

Proposition – **Caractérisation**
Soient $(A,+,\times)$ un anneau et B une partie de A. B est un sous-anneau de A si et seulement si
(i) $1_A\in B$ (et B est non vide)
(ii) $\forall x,y\in B,\quad x+(-y)\in B$
(iii) $\forall x,y\in B,\quad x\times y\in B$

[22] à compléter

Démonstration –

Remarque – Les propriétés d'associativité, de commutativité et de distributivité sont hérités de la stabilité des lois.

Exemple
L'ensemble $\mathbb{Z}[i]=\{a+ib;a,b\in\mathbb{Z}\}$, appelé *anneau des entiers de Gauss* est un sous-anneau de $\mathbb{C}$: pour $a,a',b,b'\in\mathbb{Z}$
- $1=1+0i\in\mathbb{Z}[i]$
- $(a+ib)-(a'+ib')=(a-a')+i(b-b')\in\mathbb{Z}[i]$
- $(a+ib)(a'+ib')=(aa'-bb')+i(ab'+ba')\in\mathbb{Z}[i]$

Exemple
$(\mathcal{T}_n^{inf}(\mathbb{K}),+,\times)$ est un sous-anneau de $\mathcal{M}_n(\mathbb{K})$.

3.3 Morphisme d'anneaux

Définition – morphisme d'anneaux
Soit $(A, \square, \wedge)$, $(B, \triangleleft, \vee)$ deux anneaux.
On appelle morphisme d'anneaux de A dans B tout application $f : A \mapsto B$ telle que
(i) $f(1_A) = 1_B$
(ii) $\forall x, y \in A, \quad f(x \square y) = f(x) \triangleleft f(y)$ *et* $f(x \wedge y) = f(x) \vee f(y)$

Remarques –

1. On utilise par défaut les notations $(+, \times)$ ce qui donne $f(x+y) = f(x) + f(y)$ et $f(xy) = f(x)f(y)$.
2. En particulier, f est un morphisme de groupes de $(A, +)$.
3. Si $A = B$ on dit que f est un endomorphisme (d'anneaux).
4. L'image directe et l'image réciproque d'une sous-anneau par un morphisme est un sous anneau.
5. Si f est bijective, on dit que f est un isomorphisme et si $A = B$, on dit que f est un automorphisme.

Exemple
$x \mapsto \overline{x}$ est un automorphisme (d'anneau) de $\mathbb{C}$ car $\overline{1} = 1$ et pour tout $x, y \in \mathbb{C}$, $\overline{x+y} = \overline{x} + \overline{y}$ et $\overline{xy} = \overline{x}\ \overline{y}$.

3.4 Corps

Définition – Corps
On appelle corps tout anneau commutatif dont tout élément on nul (différent du neutre de la première loi) est inversible (pour la seconde loi) c'est-à-dire $U(K) = K \backslash \{0_K\}$.
Concrètement, $(K, +, \times)$ est un corps si :
(i) $(K, +)$ *est un groupe commutatif*
(ii) $(K \backslash \{0_K\}, \times)$ *est un groupe commutatif*
(iii) $\times$ *est distributive sur* $+$

Remarque – On note qu'un corps est forcément intègre car l'inversibilité des éléments non nuls permet la simplification : $ab = O_K \quad \Rightarrow \quad a = 0_k$ ou $b = 0_k$.

Exemple
$(\mathbb{R}, +, \times)$,$(\mathbb{Q}, +, \times)$, $(\mathbb{C}, +, \times)$ sont des corps. $(\mathbb{Z}, +, \times)$ est un anneau mais pas un corps car 2 n'est pas inversible.

Exercice : Donner une caractérisation d'un sous-corps de $(K, +, \times)$.

[23] à compléter

Solution – ■

Exercice : Monter que $\mathbb{Q}[i] = \{a + ib;\ a, b \in \mathbb{Q}\}$ est un corps.

[24] à compléter

Solution – ■