Structures algébriques

I. Loi de composition interne

E désigne un ensemble.

1°) Définition

Déf : On appelle loi de composition interne (l.c.i.) ou opération sur E toute application de $E\times E$ vers E.
Lorsque cette loi de composition interne est notée $\star$, on note $x\star y$ l'image du couple (x,y) par l'application précédente.
L'élément $x\star y$ est appelé composé de x par y via $\star$.
Les l.c.i. sont généralement notées $\star,\top,\perp,+,\times,\circ,...$

Déf : On appelle magma tout couple $(E,\star)$ formé d'un ensemble E et d'une loi de composition interne $\star$ sur E.

2°) Partie stable

Déf : On appelle partie stable d'un magma $(E,\star)$ toute partie A de E telle que $\forall x,y\in A, x\star y\in A$.

Déf : Soit A une partie stable d'un magma $(E,\star)$.
L'application restreinte $\begin{cases}A\times A\to A\\(x,y)\mapsto x\star y\end{cases}$ définit une loi de composition interne sur A appelée loi de composition interne induite par $\star$.
On la note $\star_{|A}$ ou plus couramment $\star$ et on peut ainsi donner un sens au magma $(A,\star)$.

3°) Propriétés d'une loi de composition interne

a) commutativité

Déf : Soit $\star$ une loi de composition interne sur E. On dit que deux éléments a et b de E commutent pour la loi $\star$ ssi $a\star b=b\star a$.

Déf : Une loi de composition interne $\star$ sur E est dite commutative ssi tous les éléments de E commutent deux à deux. Le magma $(E,\star)$ est alors dit commutatif.

b) associativité

Déf : Une loi de composition interne $\star$ sur E est dite associative ssi $\forall a,b,c\in E,(a\star b)\star c=a\star(b\star c)$.
Le magma $(E,\star)$ est alors dit associatif.

4°) Eléments particuliers

Soit $(E,\star)$ un magma

a) élément régulier

Déf : On appelle élément régulier de $(E,\star)$ tout élément x de E tel que $\forall a,b\in E$, $x\star a=x\star b\Rightarrow a=b$ (régularité à gauche) et $a\star x=b\star x\Rightarrow a=b$ (régularité à droite).

b) élément neutre

Déf : On appelle élément neutre de $(E,\star)$ tout élément e de E tel que $\forall x\in E$, $e\star x=x$ (neutre à gauche) et $x\star e=x$ (neutre à droite).

Prop : Si $(E,\star)$ possède un élément neutre celui-ci est unique.

Déf : On appelle monoïde tout magma $(E,\star)$ associatif et possédant un élément neutre.
Si de plus $\star$ est commutative, le monoïde $(E,\star)$ est dit commutatif.

c) élément symétrisable

Soit $(E,\star)$ un monoïde d'élément neutre e.

Déf : On appelle élément symétrisable de $(E,\star)$ tout élément x de E tel qu'il existe $y\in E$ pour lequel $x\star y=e$ (symétrisabilité à gauche) et $y\star x=e$ (symétrisabilité à droite).

Prop : Si x est symétrisable alors $\exists! y \in E$ tel que $x \star y = y \star x = e$.

Déf : Si x est symétrisable, l'unique élément y de E tel que $x \star y = y \star x = e$ est appelé symétrique de x et on le note $y = \text{sym}(x)$.

Prop : Si x est symétrisable alors $\text{sym}(x)$ l'est aussi et $\text{sym}(\text{sym}(x)) = x$.

Prop : Si x et y sont symétrisables alors $x \star y$ l'est aussi et $\text{sym}(x \star y) = \text{sym}(y) \star \text{sym}(x)$.

Prop : Si x est un élément symétrisable de $(E, \star)$ alors x est régulier.

5°) Itéré d'un élément

Soit $(E, \star)$ un monoïde de neutre e.

Soit $x \in E$. Pour $n \in \mathbb{N}^*$, on note $x^{\star n} = x \star x \star \ldots \star x$ (n termes). De plus on pose $x^{\star 0} = e$.

Déf : $x^{\star n}$ est appelé itéré d'ordre n de l'élément x.

Prop : $\forall p, q \in \mathbb{N}, x^{\star p} \star x^{\star q} = x^{\star (p+q)}$ et $(x^{\star p})^{\star q} = x^{\star (pq)}$.

Supposons que x soit symétrisable. Pour $n \in \mathbb{N}^*$, on note $x^{\star (-n)} = \text{sym}(x) \star \text{sym}(x) \star \ldots \star \text{sym}(x)$ (n termes)

Prop : Soit x un élément symétrisable de E. $\forall n \in \mathbb{Z}, x^{\star n}$ est symétrisable et $\text{sym}(x^{\star n}) = x^{\star (-n)}$.
$\forall p, q \in \mathbb{Z}, x^{\star p} \star x^{\star q} = x^{\star (p+q)}$ et $(x^{\star p})^{\star q} = x^{\star (pq)}$.

6°) Structures produits

a) structure sur E^n

Soit $(E, \star)$ un magma et X un ensemble non vide.

Déf : On définit une loi de composition interne, encore notée $\star$, sur E^n par $\forall (x_1, \ldots, x_n), (y_1, \ldots, y_n) \in E^n$ on pose $(x_1, \ldots, x_n) \star (y_1, \ldots, y_n) = (x_1 \star y_1, \ldots, x_n \star y_n)$.

Prop : Si $(E, \star)$ est un monoïde (resp. commutatif) d'élément neutre e alors $(E^n, \star)$ est un monoïde (resp. commutatif) d'élément neutre $\varepsilon = (e, \ldots, e)$.
De plus, un élément $x = (x_1, \ldots, x_n)$ est symétrisable ssi $\forall i \in \{1, \ldots, n\}$, x_i l'est, et si tel est le cas, $\text{sym}(x) = (\text{sym}(x_1), \ldots, \text{sym}(x_n))$.

b) structure sur $\mathcal{F}(X, E)$

Soit $(E, \star)$ un magma et X un ensemble non vide.

Déf : On définit une loi de composition interne, encore notée $\star$, sur $\mathcal{F}(X, E)$ par $\forall f, g \in \mathcal{F}(X, E)$ on pose $\forall x \in X, (f \star g)(x) = f(x) \star g(x)$.

Prop : Si $(E, \star)$ est un monoïde (resp. commutatif) d'élément neutre e alors $(\mathcal{F}(X, E), \star)$ est un monoïde (resp. commutatif) d'élément neutre $\varepsilon : x \mapsto e$. De plus, un élément $f \in \mathcal{F}(X, E)$ est symétrisable ssi $\forall x \in X$, $f(x)$ l'est, et si tel est le cas, $(\text{sym}\, f)(x) = \text{sym}(f(x))$.

7°) Notation additive et multiplicative

Déf : Un monoïde est dit noté additivement (resp. multiplicativement) ssi sa loi de composition interne est notée $+$ (resp. $\times$)

Notation par défaut	Notation additive	Notation multiplicative
$\star$	$+$	$\times$ ou $.$
e	0	1
$x \star y$	$x + y$	xy ou $x.y$
$\text{sym}(x)$	$-x$	x^{-1}
$\overset{n}{\underset{i=1}{\star}} x_i$	$\sum_{i=1}^{n} x_i$	$\prod_{i=1}^{n} x_i$
$x^{\star n}$	$n.x$	x^n

II. Groupes

1°) Définition

Déf : On appelle groupe tout magma $(G,\star)$ tel que

1) $\star$ est associative,

2) $(G,\star)$ possède un élément neutre e,

3) tout élément de $(G,\star)$ est symétrisable.

Si de plus $\star$ est commutative, le groupe $(G,\star)$ est dit commutatif ou plus couramment abélien.

Prop : Si $(G,\star)$ est un groupe alors $(G^n,\star)$ l'est aussi.

Prop : Si $(G,\star)$ est un groupe alors $(\mathcal{F}(X,G),\star)$ l'est aussi.

2°) Sous-groupe

a) définition

Soit $(G,\star)$ un groupe d'élément neutre e.

Déf : On appelle sous-groupe de $(G,\star)$ toute partie H de G telle que :

1) $e\in H$,

2) $\forall x\in H, \text{sym}(x)\in H$ (stabilité par passage au symétrique),

3) $\forall x,y\in H, x\star y\in H$ (stabilité).

Théorème :

Si H est un sous-groupe de $(G,\star)$ alors $(H,\star)$ est un groupe.

Si de plus $(G,\star)$ est abélien alors $(H,\star)$ l'est aussi.

Prop : (Caractérisation rapide des sous-groupes)

Soit H une partie de G. On a équivalence entre :

(i) H est un sous-groupe de $(G,\star)$,

(ii) $\begin{cases} H\neq\varnothing \\ \forall x,y\in H, x\star \text{sym}(y)\in H \end{cases}$.

Prop : Soit H_1,H_2 deux sous-groupes de $(G,\star)$.

$H_1\cap H_2$ est un sous-groupe de $(G,\star)$.

b) groupe des racines n^{ème} de l'unité

Soit $n\in\mathbb{N}^*$ et $U_n=\left\{z\in\mathbb{C}/z^n=1\right\}$. *Prop :* $(U_n,\times)$ est un groupe abélien.

Pour $n=1, U_1=\{1\}$.

Pour $n=2, U_2=\{1,-1\}$. On a

$\times$	1	-1
1	1	-1
-1	-1	1

Pour $n=3, U_3=\left\{1,j,j^2\right\}$. On a

$\times$	1	j	j^2
1	1	j	j^2
j	j	j^2	1
j^2	j^2	1	j

Pour $n=4, U_4=\{1,i,-1,-i\}$. On a

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

c) groupes géométrique

$\mathcal{P}$ le plan géométrique de direction P.

$t_{\vec{u}}$: translation de vecteur $\vec{u}$.

$H_{O,\lambda}$: homothétie de centre O et de rapport λ.

$\text{Rot}_{O,\theta}$: rotation de centre O et d'angle θ.

Prop : $\mathcal{T} = \{t_{\vec{u}} / \vec{u} \in P\}$ est un sous-groupe de $(\mathfrak{S}(\mathcal{P}), \circ)$.

Prop : Soit $O \in \mathcal{P}$. $\mathcal{H}_O = \{H_{O,\lambda} / \lambda \in \mathbb{R}^*\}$ est un sous-groupe de $(\mathfrak{S}(\mathcal{P}), \circ)$.

Prop : Soit $O \in \mathcal{P}$. $\mathcal{R}_O = \{\text{Rot}_{O,\theta} / \theta \in \mathbb{R}\}$ est un sous-groupe de $(\mathfrak{S}(\mathcal{P}), \circ)$.

On appelle isométrie du plan tout $f \in \mathfrak{S}(\mathcal{P})$ telle que $\forall A, B \in \mathcal{P}$, $f(A)f(B) = AB$.

Prop : L'ensemble $\mathcal{I}$ des isométries du plan est un sous-groupe de $(\mathfrak{S}(\mathcal{P}), \circ)$.

3°) Morphisme de groupes

Soit $(G, \star)$, $(G', \top)$ et $(G'', \perp)$ trois groupes d'éléments neutres e, e' et e''.

a) définition

Déf : On appelle morphisme du groupe $(G, \star)$ vers $(G', \top)$ toute application $\varphi : G \to G'$ telle que :
$\forall x, y \in G, f(x \star y) = f(x) \top f(y)$.
(image de la composée est la composée des images).
Si f est bijective, on dite que f est un isomorphisme.
Si $(G', \top) = (G, \star)$, on dit que f est un endomorphisme.
Si $(G', \top) = (G, \star)$ et f est bijective on dit que f est un automorphisme.

Prop : Soit $a \in G$. $\varphi : \begin{cases} \mathbb{Z} \to G \\ n \mapsto a^{\star n} \end{cases}$ est un morphisme de groupes.

b) propriétés

Prop : Soit $f : G \to G'$ un morphisme de groupes.
$f(e) = e'$, $\forall x \in G, f(\text{sym}(x)) = \text{sym}(f(x))$, $\forall x \in G, \forall p \in \mathbb{Z}, f(x^{\star p}) = (f(x))^{\top p}$ et
$\forall x_1, \ldots, x_n \in G, f(\overset{n}{\underset{i=1}{\star}} x_i) = \overset{n}{\underset{i=1}{\top}} f(x_i)$.

Prop : Si $f : G \to G'$ et $g : G' \to G''$ sont deux morphismes de groupes alors $g \circ f : G \to G''$ est aussi un morphisme de groupes.

Prop : Soit $f : G \to G'$.
Si f est un isomorphisme alors $f^{-1} : G' \to G$ l'est aussi.

c) noyau et image

Prop : Soit $f : G \to G'$ un morphisme de groupes.
Si H est un sous-groupe de $(G, \star)$ alors $f(H)$ est un sous-groupe de $(G', \top)$.
Si H' est un sous-groupe de $(G', \top)$ alors $f^{-1}(H)$ est un sous-groupe de $(G, \star)$.

Déf : Soit $f : G \to G'$ un morphisme de groupes.
On appelle image de f, l'ensemble $\text{Im} f = f(G)$. C'est un sous-groupe de $(G', \top)$.
On appelle noyau de f, l'ensemble $\ker f = f^{-1}(\{e'\})$. C'est un sous-groupe de $(G, \star)$.

Théorème :
Soit $f : G \to G'$ un morphisme de groupes.
+ f est surjective ssi $\text{Im} f = G$,
+ f est injective ssi $\ker f = \{e\}$.

d) morphisme géométrique

$\mathcal{P}$ le plan géométrique

Prop : Soit $O \in \mathcal{P}$. $\lambda \mapsto H_{O,\lambda}$ est un morphisme de $(\mathbb{R}^*, \times)$ vers $(\mathfrak{S}(\mathcal{P}), \circ)$ d'image $\mathcal{H}_O$ et de noyau $\{1\}$.

Prop : Soit $O \in \mathcal{P}$. $\theta \mapsto \text{Rot}_{O,\theta}$ est un morphisme de $(\mathbb{R}, +)$ vers $(\mathfrak{S}(\mathcal{P}), \circ)$ d'image $\mathcal{R}_O$ et de noyau $2\pi\mathbb{Z}$.

III. Etude du groupe symétrique

1°) Permutation de $\mathbb{N}_n = \{1,2,...,n\}$

Déf : Pour $n \in \mathbb{N}^*$, on note $\mathfrak{S}_n$ l'ensemble des permutations de $\mathbb{N}_n$.
$(\mathfrak{S}_n, \circ)$ est un groupe d'élément neutre $\mathrm{Id}_{\mathbb{N}_n} = \mathrm{Id}$ appelé groupe symétrique d'ordre n.

Déf : Pour $\sigma \in \mathfrak{S}_n$, on note $\sigma = \begin{pmatrix} 1 & 2 & ... & n \\ \sigma(1) & \sigma(2) & ... & \sigma(n) \end{pmatrix}$ pour visualiser l'action de σ.

Prop : Pour $n \geq 3$ le groupe $(\mathfrak{S}_n, \circ)$ n'est pas commutatif.

2°) Cycles

Soit $p \in \mathbb{N}$ tel que $2 \leq p \leq n$.
Soit $a_1,...,a_p$ une liste de p éléments deux à deux distincts de $\mathbb{N}_n$.
Soit $c : \mathbb{N}_n \to \mathbb{N}_n$ définie par :
$c(a_1) = a_2, c(a_2) = a_3, ..., c(a_{p-1}) = a_p, c(a_p) = a_1$ et $\forall x \in \mathbb{N}_n \setminus \{a_1,...,a_p\}, c(x) = x$.
c est une permutation de $\mathbb{N}_n$.

Déf : c est appelée cycle de longueur p (ou p cycle).
On le note $c = (a_1 \quad a_2 \quad ... \quad a_p)$.
L'ensemble $S = \{a_1,...,a_p\}$ est appelé support du cycle c.

Déf : Les cycles de longueur 2 sont appelés transpositions.
Une transposition $\tau = (i \quad j)$ a pour effet d'échanger i et j.

Prop : Si c est un cycle de longueur p alors $c^p = \mathrm{Id}$.

3°) Décomposition d'une permutation en produit de transpositions

Prop : Tout cycle de longueur p peut se décomposer en un produit de $p-1$ transpositions.

Théorème :
Toute permutation de $\mathbb{N}_n$ peut se décomposer en un produit d'au plus $n-1$ transpositions.

Prop : Toute permutation de $\mathbb{N}_n$ peut se décomposer en un produit de transpositions de la forme $(1 \quad k)$ avec $2 \leq k \leq n$.

4°) Signature d'une permutation

Déf : Soit $\sigma \in \mathfrak{S}_n$ et un couple (i,j) avec $1 \leq i < j \leq n$.
On dit σ réalise une inversion sur le couple (i,j) ssi $\sigma(i) > \sigma(j)$.
On note $I(\sigma)$ le nombre de couples (i,j) (avec $1 \leq i < j \leq n$) sur lesquels σ réalise une inversion.

Déf : On appelle signature d'une permutation σ de $\mathfrak{S}_n$ le réel $\varepsilon(\sigma) = (-1)^{I(\sigma)}$.

Prop : La signature d'une transposition est -1.

Théorème :
L'application $\varepsilon : \mathfrak{S}_n \to \{-1,1\}$ est un morphisme du groupe $(\mathfrak{S}_n, \circ)$ sur $(\{-1,1\}, \times)$.

Par suite $I(\sigma' \circ \sigma)$ à même parité que $I(\sigma) + I(\sigma')$,
puis $\varepsilon(\sigma' \circ \sigma) = (-1)^{I(\sigma' \circ \sigma)} = (-1)^{I(\sigma)+I(\sigma')} = \varepsilon(\sigma')\varepsilon(\sigma)$.
Ainsi ε est un morphisme de groupes.

Cor : Ainsi $\varepsilon(\sigma_1 \circ \cdots \circ \sigma_p) = \varepsilon(\sigma_1) \times \cdots \times \varepsilon(\sigma_p)$.
$\forall p \in \mathbb{Z}, \varepsilon(\sigma^p) = \varepsilon(\sigma)^p$ et en particulier $\varepsilon(\sigma^{-1}) = \varepsilon(\sigma)$.

Prop : La signature d'un p cycle est $(-1)^{p-1}$.

Déf : Une permutation de signature 1 est dite paire.
Une permutation de signature -1 est dite impaire.
On note $\mathfrak{A}_n$ l'ensemble des permutations paires de $\mathfrak{S}_n$.

Prop : $\mathfrak{A}_n$ est un sous-groupe de $(\mathfrak{S}_n, \circ)$.

Déf : $(\mathfrak{A}_n, \circ)$ est appelé groupe alterné d'ordre n.

Prop : Pour $n \geq 2$, $\text{Card}\,\mathfrak{A}_n = n!/2$.

IV. Anneaux

1°) Définition

Déf : Soit $\top$ et $\star$ deux lois de composition internes sur un ensemble E.
On dit que $\star$ est distributive sur $\top$ ssi $\forall a,b,c \in E$: $a \star (b \top c) = (a \top b) \star (a \top c)$ (distributivité à gauche) et $(b \top c) \star a = (b \top a) \star (c \top a)$ (distributivité à droite).

Déf : On appelle anneau tout triplet $(A, \top, \star)$ formé d'une ensemble A et deux loi de composition internes $\top$ et $\star$ tels que :
1) $(A, \top)$ est un groupe abélien,
2) $(A, \star)$ est un monoïde,
3) $\star$ est distributive sur $\top$.
Si de plus $\star$ est commutative, l'anneau $(A, \top, \star)$ est dit commutatif.

Prop : Si $(A, +, \times)$ est un anneau et $n \in \mathbb{N}^*$ alors $(A^n, +, \times)$ est un anneau.

Prop : Si $(A, +, \times)$ est un anneau et X un ensemble alors $(\mathcal{F}(X, A), +, \times)$ est un anneau.

2°) Sous-anneau

Déf : On appelle sous-anneau d'un anneau $(A, +, \times)$ toute partie B incluse dans A telle que :
1) $1_A \in B$,
2) $\forall x, y \in B, x - y \in B$,
3) $\forall x, y \in B, xy \in B$.

Théorème :
Si B est un sous-anneau de $(A, +, \times)$ alors $(B, +, \times)$ est un anneau.
Si de plus $(A, +, \times)$ est commutatif alors $(B, +, \times)$ l'est aussi.

3°) Règles de calculs dans un anneau

Soit $(A, +, \times)$ un anneau de neutres 0 et 1.

Prop : $\forall a \in A, 0 \times a = a \times 0 = 0$.

Prop : $\forall a, b \in A, (-a)b = -(ab) = a(-b)$.

Prop : $\forall a, b \in A, \forall p \in \mathbb{Z}, (p.a)b = p.(ab) = a(p.b)$.

Prop : $\forall a, b \in A, (a+b)^2 = a^2 + ab + ba + b^2, (a+b)^3 = ...$

Théorème : (Formule du binôme de Newton)
Soit $a, b \in A$ tels que a et b commutent.

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

Théorème :
Soit $a, b \in A$ tels que a et b commutent.

$$\forall n \in \mathbb{N}, a^n - b^n = (a-b) \sum_{k=0}^{n-1} a^{n-1-k} b^k = (a-b)(a^{n-1} + a^{n-2}b + ... + ab^{n-2} + b^{n-1})$$

4°) Eléments inversibles

Déf : Un élément $a \in A$ est dit inversible ssi il est symétrisable pour $\times$ i.e. ssi il existe $b \in A$ tel que $ab = ba = 1_A$. Cet élément b est alors unique, on l'appelle inverse de a, on le note a^{-1}.

Prop : Si x est inversible alors x^{-1} est inversible et $(x^{-1})^{-1} = x$.

Prop : Si x et y sont inversibles alors xy est inversible et $(xy)^{-1} = y^{-1}x^{-1}$.

5°) Diviseurs de zéro

Soit $(A,+,\times)$ un anneau

a) définition

Déf : Soit $a \in A$ tel que $a \neq 0_A$. On dit que a est diviseur de zéro ssi $\exists b \in A \setminus \{0_A\}$ tel que $ab = 0_A$ ou $ba = 0_A$.

Prop : Un diviseur de zéro est non régulier pour $\times$.

Prop : Les éléments inversibles de A ne sont pas diviseurs de zéro.

b) anneau sans diviseurs de zéro

Prop : Si $(A,+,\times)$ ne possède pas de diviseurs de zéro alors $\forall a,b \in A, ab = 0_A \Rightarrow a = 0_A$ ou $b = 0_A$ (implication d'intégrité)

Prop : Dans un anneau $(A,+,\times)$ sans diviseurs de zéro tout élément non nul est régulier.

c) idempotent et nilpotent

Déf : Un élément $a \in A$ est dit idempotent ssi $a^2 = a$.

Déf : Un élément $a \in A$ est dit nilpotent ssi $\exists n \in \mathbb{N}^*, a^n = 0_A$.

V. Corps

1°) Définition

Déf : On appelle corps tout anneau commutatif $(K,+,\times)$ non réduit à $\{0_K\}$ dont tous les éléments, sauf 0_K, sont inversibles.

Prop : Un corps n'a pas de diviseurs de zéro.

2°) Sous-corps

Soit $(K,+,\times)$ un corps.

Déf : On appelle sous-corps d'un $(K,+,\times)$ toute partie L de K telle que :

1) L est un sous-anneau de $(K,+,\times)$,

2) $\forall x \in L \setminus \{0_K\}, x^{-1} \in L$.

Théorème :

Si L est un sous-corps de $(K,+,\times)$ alors $(L,+,\times)$ est un corps.