Structures Algébriques

1. Lois de composition interne

<u>déf</u> On appelle <u>loi de composition interne</u> sur un ensemble non vide E toute application $* : E \times E \to E$
$(x, y) \mapsto x * y$.

<u>notation</u> On utilise aussi les notations :
- $x + y$ (en notation additive).
- $x \times y$, $x . y$, $x \circ y$, … (en notation multiplicative)

<u>exple</u>
- $\cup$ et $\cap$ sont des LCI dans l'ensemble $\mathcal{P}(E)$
- $+$ et $\times$ pour $\mathbb{N}, \mathbb{Q}, \mathbb{Z}, \mathbb{R}$ ou $\mathbb{C}$.
- La somme de 2 vecteurs dans $\mathbb{R}^2$ ou $\mathbb{R}^3$.
- produit vectoriel $\wedge$ dans $\mathbb{R}^3$.
- En revanche, le prod scalaire n'est pas une LCI dans $\mathbb{R}^3$, puisque $\langle \vec{u}, \vec{v} \rangle \in \mathbb{R}$ $\forall \vec{u}, \vec{v} \in \mathbb{R}^3$.

<u>déf</u> Une LCI $*$ définie sur un ensemble E est dite
- commutative si : $\forall x, y \in E$, $x * y = y * x$.
- associative si : $\forall x, y, z \in E$, $(x * y) * z = x * (y * z)$

<u>exple</u>
- $\cup$ et $\cap$ sont commutatives et associatives pour $\mathcal{P}(E)$
- $+$ et $\times$ sont commutatives et associatives dans $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ ou $\mathbb{C}$.
- La somme de 2 vecteurs est associative et commutative dans $\mathbb{R}^2$ et $\mathbb{R}^3$
- En revanche, le prod vect n'est ni commutatif, ni associatif.
$\vec{u} \wedge \vec{v} = -\vec{v} \wedge \vec{u}$ et $\begin{cases} \vec{u} \wedge (\vec{v} \wedge \vec{w}) = \langle \vec{u}, \vec{w} \rangle \vec{v} - \langle \vec{u}, \vec{v} \rangle \vec{w} \\ (\vec{u} \wedge \vec{v}) \wedge \vec{w} = \langle \vec{w}, \vec{u} \rangle \vec{v} - \langle \vec{w}, \vec{v} \rangle \vec{u} \end{cases}$

définition E un ensemble muni d'une LCI $*$.
On appelle élément neutre tout élément $e \in E$ tel que
$$\forall x \in E \quad e * x = x * e = x.$$

prop Si une LCI $*$ dans un ens E admet un élément neutre, celui-ci est unique.

exple × neutre pour $\cap$: E , neutre pour $\cup$: $\emptyset$ dans $P(E)$
× neutre pour + : 0 , neutre pour × : 1 dans $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ ou $\mathbb{C}$.
× neutre pour + dans $\mathbb{R}^2$ ou $\mathbb{R}^3$: $\vec{0}$.
× pas d'élément neutre pour $\wedge$: sinon $\exists \vec{e} \in E$ tq.
$\vec{e} \wedge \vec{v} = \vec{v} \wedge \vec{e} = \vec{v} \quad \forall \vec{v} \Rightarrow \vec{v} \perp \vec{v} \quad \forall \vec{v} \rightarrow$ contr.

déf E un ens muni d'une LCI $*$ admettant un élément neutre e.
On dit que $x \in E$ est symétrisable, ou inversible, s'il admet un symétrique ou un inverse y, ie si :
$$\exists y \in E \text{ tq } \quad x * y = y * x = e.$$

exple × $\cap$ a pour seul inversible E :
si $F \subsetneq E$, $\nexists G$ tq $F \cap G = G \cap F = E$
× $\cup$ a pour seul inversible $\emptyset$.
si $F \neq \emptyset$, $\nexists G$ tq $F \cup G = G \cup F = \emptyset$
× Les seuls inversible pour × dans $\mathbb{Z}$ sont 1 et −1.
× Tout élément $\neq 0$ sont inversible pour × dans $\mathbb{Q}, \mathbb{R}$ et $\mathbb{C}$.

prop Si E ens muni d'une LCI $*$ associative admettant un élément neutre, alors le symétrique d'un élément x, s'il existe, est unique. On le note :
* $-x$ en notation additive. (opposé de x)
* x^{-1} ou $1/x$ en notation multiplicative (inverse de x)

prop E un ens muni d'une LCI * associative admettant un élément neutre. Alors :

- Le symétrique d'un symétrisable est symétrisable et :

$$(x^{-1})^{-1} = x \quad (\text{ou } -(-x) = x).$$

- Si x et $y \in E$ sont symétrisable, alors $x * y$ est symétrisable, et

$$(x*y)^{-1} = y^{-1} * x^{-1}.$$

déf E muni d'une LCI *. On dit que $x \in E$ est régulier (ou simplifiable) si :

- $\forall a, b \in A,\ a * x = b * x \Rightarrow a = b$
- $\forall a, b \in A,\ x * a = x * b \Rightarrow a = b$

exple

- Pour $\cap$, le seul élément régulier est E
- Pour $\cup$, le seul élément régulier est $\emptyset$.
- Pour + dans $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ ou $\mathbb{C}$, tous les éléments sont réguliers
- Pour × dans $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, tous les éléments sont réguliers sauf 0.
- Pour $\wedge$ dans $\mathbb{R}^3$, aucun élément n'est régulier.

$$\vec{a} \wedge \vec{x} = \vec{b} \wedge \vec{x} \Rightarrow (\vec{a} - \vec{b}) \wedge \vec{x} = 0,$$ ie $\vec{a} - \vec{b}$ colin à $\vec{x}$ et pas $\vec{a} - \vec{b} = \vec{0}$!

prop E un ens muni de * une LCI associative avec un élément neutre. Alors tout élément inversible est régulier.
La réciproque est fausse en général.

exple $(\mathbb{Z}, \times)$: les éléments non nuls sont réguliers, mais non inversibles (sauf 1 et -1).

2_ Groupes

2.1. Groupes et exemples de groupes

<u>définition</u> On dit qu'un ens G muni d'une LCI $*$ est un groupe, si
- $*$ est associative
- $*$ admet un élément neutre e dans G.
- Tout élément $x \in G$ est symétrisable dans G.

De plus, $(G, *)$ est un groupe commutatif (ou abélien) si la loi $*$ est commutative.

<u>notation</u> $(G, *)$ un groupe.

i) si G est non abélien, on utilise la notation multiplicative : $x \times y$, $x.y$ ou $x * y$, 1 ou 1_G ou e pour le neutre x^{-1} pour le symétrique (inverse).

ii) Si G est abélien, on utilise la notation additive $x+y$, 0 ou 0_G pour le neutre, $-x$ pour le symétrique (opposé).

<u>propriétés des groupes</u>
- L'élément neutre de G est unique
- Le symétrique de tout élément est unique

De plus $\forall x, y \in G$, $(xy)^{-1} = y^{-1} * x^{-1}$!
- Les éléments d'un groupes sont réguliers, car symétrisables

<u>expls de groupes</u>
- $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ sont des groupes commutatifs. ⚠ $(\mathbb{N}, +)$ n'est pas un groupe
- $(\mathbb{Q}^*, *)$, $(\mathbb{R}^*, \times)$, $(\mathbb{C}^*, \times)$ sont des groupes commut.

③ . $(\mathbb{R}^2,+)$, $(\mathbb{R}^3,+)$ sont des groupes commutatifs.

× Groupe des racines n-ièmes de l'unité dans $\mathbb{C}$, U_n.
Rappelons que les racines n-ièmes de 1 sont :

$$\exp\left(\frac{2ik\pi}{n}\right) \qquad k=0,1,\dots,n-1.$$

× Groupe des translations du plan pour la loi de composition.
× Groupe des permutations d'un ensemble non vide E : non commutatif.

$E=\{1,\dots,n\}$, on note ce groupe S_n, appelé groupe symétrique. Il possède $n!$ éléments.

2.2. Sous-groupes

déf On dit qu'une partie H d'un groupe $(G,*)$ est un sous-groupe si :
(i) H est stable pour $*$, i.e : $\forall x,y\in H$, $x*y\in H$.
(ii) H muni de la LCI induite par $*$ est un groupe

exple Sous-groupes triviaux de G : $\{e\}$ et G.

prop Tout sous-groupe H d'un groupe $(G,*)$ satisfait :
× l'élément neutre de H est égal à l'élément neutre de G.
× le symétrique d'un élément de H dans G est égal à son symétrique dans H.

Thme $(G,*)$ un groupe, $H\subseteq G$ ~~est un sous-groupe de G.~~

$(H,*)$ est un ~~sous-groupe de G~~ $\Leftrightarrow$ $\begin{cases} \text{(i) } H\neq\emptyset \\ \text{(ii) } \forall x\in H,\ x^{-1}\in H \\ \text{(iii) } \forall (x,y)\in H^2,\ x*y\in H^2 \end{cases}$

$(H,*)$ $\Leftrightarrow$ $\left[\begin{array}{l} H \neq \emptyset \\ \forall (x,y) \in H^2, \quad x * y^{-1} \in H. \end{array}\right.$

expls
- $\mathbb{Z}$ sous-groupe de $(\mathbb{Q},+)$.
- $\mathbb{Q}^*$ sous groupe de $(\mathbb{R}^*,\times)$.
- L'ens $\mathbb{U}$ des nb complexes de module 1 est un sous-gr de $(\mathbb{C}^*,\times)$.
- L'ens $\mathbb{U}_n$ des racines n-èmes de l'unité est un sous groupe de $(\mathbb{U},\times)$

2.3. Morphismes de Groupes

déf Soient $(G,*)$ et $(G',*')$ deux groupes. On dit qu'une appli. $f: G \to G'$ est un morphisme (ou homomorphisme) de groupes si : $\forall x,y \in G, \quad f(x*y) = f(x) *' f(y)$.

- Si f est bijective, on dit que f est un isomorphisme de grps
- Si f est bijective et que $G = G'$, on dit que f est un automorphisme du groupe G.

exple
- $\exp : (\mathbb{R},+) \to (\mathbb{R}_+^*,\times)$ isomorphismes de groupes.
  $\forall x,y \in \mathbb{R}, \quad \exp(x+y) = \exp(x) \times \exp(y)$.
- $\ln : (\mathbb{R}_+^*,\times) \to (\mathbb{R},+)$ isomorphisme de groupes.
  $\ln(xy) = \ln(x) + \ln(y)$.
- $\varphi : \mathbb{R}^2 \to \{\text{translations de } \mathbb{R}^2\}$ isomorph de groupes
  $\vec{u} \mapsto t_{\vec{u}}$: translation de vecteur $\vec{u}$

(4)

prop Soit f un morphisme du groupe $(G, *)$ dans $(G', *')$, on a :

- $f(e_G) = e_{G'}$.
- $f(x^{-1}) = [f(x)]^{-1}$

déf f un morphisme du groupe $(G, *)$ dans $(G', *')$. On appelle

× noyau de f l'ensemble :

$$\operatorname{Ker} f = f^{-1}(\{0_{G'}\}) = \{x \in G \,/\, f(x) = e_{G'}\}.$$

× image de f l'ensemble.

$$\operatorname{Im} f = \{f(x) \,/\, x \in G\}.$$

prop f un morphisme du groupe $(G, *)$ dans $(G', *')$.

(iii) $\operatorname{Ker} f = \{e_G\} \Leftrightarrow f$ est injective

(iv) $\operatorname{Im} f = G' \Leftrightarrow f$ est surjective

(i) $\operatorname{Ker} f$ est un sous-groupe de G.

(ii) $\operatorname{Im} f$ est un sous-groupe de G'.

exple $\varphi : (\mathbb{R}, +) \longrightarrow (\mathbb{U}, \times)$, $\theta \longmapsto e^{i\theta}$ est un morphisme de groupes. De plus φ est surjective, et non injective.

$$\operatorname{Ker} \varphi = \{2k\pi,\ k \in \mathbb{Z}\}$$

PROP (i) $f : (G, *) \longrightarrow (G', *')$ et $g : (G', *') \longrightarrow (G'', *'')$ deux morphismes de groupes. Alors $g \circ f$ est un morphisme de groupes.

(ii) Si $f : (G, *) \longrightarrow (G', *')$ est un isomorphisme de groupes, alors $f^{-1} : (G', *') \longrightarrow (G, *)$ est un morphisme de gpes.

3. Anneaux et corps

3.1. Définition et exemples

déf Un ensemble A muni de deux LCI notées $+$ et $\times$ est un anneau si

(i) $(A, +)$ est un groupe commutatif.

(ii) $\times$ est associative, distributive par rapport à $+$, ie :

$$\forall x, y, z \in A \quad \begin{cases} x \times (y+z) = x \times y + x \times z \\ (y+z) \times x = y \times x + z \times x. \end{cases}$$

(iii) $\times$ admet un élément neutre noté 1_A (ou 1).

On dit de plus que $(A, +, \times)$ est un anneau commutatif si $\times$ est commutative.

exple $(\mathbb{Z}, +, \times)$, $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$ sont des anneaux commutatifs.

Règles de calcul

- $0_A \times x = x \times 0_A = 0_A$.
- $x \times (-y) = (-x) \times y = -(x \times y)$
- Formule du binôme de Newton :

Si $x, y \in A$ commutent, ie $x \times y = y \times x$ alors $\forall n \in \mathbb{N}^*$

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$$

5

3.2. Sous-anneaux, idéaux

<u>définition</u> Soit $(A, +, \times)$ un anneau et $B \subseteq A$. On dit que B est un sous anneau de A si B est stable par $+$ et $\times$, et si $(B, +, \times)$ est un anneau pour les lois $+, \times$ (induites) avec $1_B = 1_A$.

<u>Thm</u> $(A, +, \times)$ un anneau et $B \subseteq A$.

$$(B, +, \times) \text{ est un sous-anneau de } A \iff \begin{cases} (i) & 1_A \in B \quad (\Rightarrow B \setminus \{0_A\} \neq \emptyset) \\ (ii) & \forall (b_1, b_2) \in B^2,\ b_1 - b_2 \in B. \\ (iii) & \forall (b_1, b_2) \in B^2,\ b_1 \times b_2 \in B. \end{cases}$$

<u>exple</u> $(\mathbb{Z}, +, \times)$ sous-anneau de $(\mathbb{Q}, +, \times)$.

<u>déf</u> Une partie I d'un anneau A est un idéal (à droite, resp à gauche) si

(i) $(I, +)$ est un sous groupe de $(A, +)$

(ii) $\forall x \in I$, $\forall a \in A$, $a * x \in I$ (Resp $x * a \in I$)

On dit que I est absorbant à droite (resp à gauche)

<u>Rem</u> Si $(A, +, \times)$ est commutatif, alors

Idéal à droite = Idéal à gauche.

Dans ce cas, on parlera d'idéal sans avoir à préciser.

<u>exple</u> $\times$ Soit $\mathcal{F}(X, \mathbb{R})$ l'ensemble des fonctions de X dans $\mathbb{R}$.

On le munit d'une structure d'anneaux en posant.

$\forall x \in X$, $(f+g)(x) = f(x) + g(x)$.

$(f \times g)(x) = f(x) \cdot g(x)$.

De plus : $0_{\mathcal{F}(X,\mathbb{R})}$: fonction constante égale à 0

$1_{\mathcal{F}(X,\mathbb{R})}$: fonction constante égale à 1.

alors $\forall x \in X$, $I_x = \{ f \in \mathcal{F}(X,\mathbb{R}) \,/\, f(x) = 0 \}$ est un idéal de $F(X,\mathbb{R})$.

× Soit $(A,+,\times)$ un anneau et $x \in A$. Alors l'ensemble $Ax := \{ax \,/\, a \in A\}$ est un idéal à gauche, appelé l'idéal principal à gauche engendré par x.

3.3. <u>groupe des inversibles, anneaux intègres</u>

<u>prop</u> Dans un anneau $(A,+,\times)$, les éléments inversibles (pour la loi $\times$) forment un groupe $(A^*,\times)$.

<u>exple</u> × éléments inversibles de l'anneau $\mathcal{F}(X,\mathbb{R})$.

<u>déf</u> Un anneau $(A,+,\times)$ est un corps si l'ensemble des éléments inversibles est $A \setminus \{0_A\}$. Le corps est dit commutatif si l'anneau associé l'est.

<u>exple</u> $(\mathbb{R},+,\times)$, $(\mathbb{Q},+,\times)$, $(\mathbb{C},+,\times)$.

<u>déf</u> Un anneau $(A,+,*)$ est intègre s'il vérifie :

$$\forall a,b \in A, \quad a*b = 0 \Leftrightarrow (a = 0_A \text{ ou } b = 0_A).$$

<u>exple</u> - $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, tout sous-anneau d'un anneau intègre

- $\mathcal{F}(X,\mathbb{R})$ n'est pas un anneau intègre.

<u>prop</u> Un corps est un anneau intègre. La réciproque est fausse en général.

3.4 <u>Exemple : Anneau des entiers de Gauss :</u>

On considère $\mathbb{Z}[i] = \{a+ib \,/\, a,b \in \mathbb{Z}\} \subseteq \mathbb{C}$.

On mq : - $\mathbb{Z}[i]$ est un anneau intègre commutatif.

- Son groupe des inversibles est $U_4 = \{1,-1,i,-i\}$.

⑥

3.5. Morphismes d'anneaux

<u>déf</u> Soient $(A, +, \times)$ et $(A', +', \times')$ des anneaux.

On dit que $f : A \to A'$ est un morphisme d'anneaux si

(i) $\forall x, y \in A, \quad f(x+y) = f(x) +' f(y)$

(ii) $\quad f(x \times y) = f(x) \times' f(y)$

(iii) $\quad f(1_A) = 1_{A'}$

- Si f est bijective, on dit que f est un isomorphisme d'anneaux.
- Si f est bij et $A = A'$, f est un automorphisme de l'anneau A.

<u>exple</u>
- $z \in \mathbb{C} \to \bar{z}$ est un autom de $\mathbb{C}$.
- $\forall x \in X$, $\varphi_x : f \in \mathcal{F}(X, \mathbb{R}) \longmapsto f(x) \in \mathbb{R}$ est un morph d'ann de $\mathcal{F}(X, \mathbb{R})$ dans $\mathbb{R}$.

<u>prop</u>
- $f(0_A) = 0_{A'}$, $\quad f(-x) = -f(x) \quad \forall x$.
- $f(1_A) = 1_{A'}$ et $\forall x \in A^*$, $f(x^{-1}) = [f(x)]^{-1}$

<u>déf</u> $f : (A, +, \times) \to (A', +, \times)$ morph d'anneaux

- On appelle noyau de f l'ensemble

$$\mathrm{Ker}(f) = f^{-1}(\{0_{A'}\}) = \{x \in A \,/\, f(x) = 0_{A'}\} \subseteq A$$

- On appelle image de f l'ensemble

$$\mathrm{Im}(f) = \{f(x) \,/\, x \in A\} \subseteq A'$$

prop (i) $\ker f$ est un idéal de A. De plus :

$$\ker f = \{0_A\} \iff f \text{ est injective}$$

(ii) $\mathrm{Im} f$ est un sous-anneau de A'. De plus :

$$\mathrm{Im} f = A' \iff f \text{ surjective.}$$

prop $f : A \to A'$, $g : A' \to A''$ des morphismes d'anneaux.

Alors : (i) $g \circ f$ est un morph d'ann de A dans A''

(ii) Si f est bijective, f^{-1} est un morph d'ann de A' dans A.

4. Espaces vectoriels et algèbres

4.1. Esp vectoriels

déf Soit K un corps commutatif.

Un esp vect (EV) est un groupe abélien $(E,+)$ muni d'une LC externe (LCE)

$$\begin{aligned} K \times E &\to E \\ (\lambda, x) &\to \lambda . x \end{aligned}$$

tq $\forall \lambda, \mu \in K$ et $\forall x, y \in E$,

(i) $\lambda(x+y) = \lambda . x + \lambda . y$

(ii) $(\lambda + \mu) . x = \lambda . x + \mu . x$

(iii) $(\lambda \mu) . x = \lambda . (\mu . x)$

(iv) $1_K . x = x$

4.2. Algèbres

déf $(A,+,.)$ un ev.
Alors A est une K-alg si A est munie d'une LCI $\times$ tq :

(i) $(A,+,\times)$ est un anneau.

(ii) $\forall (x,y)\in A$, $\forall \lambda \in K$, $\lambda.(x\times y) = (\lambda.x)\times y = x\times(\lambda.y)$.

déf $B\subseteq A$ est une sous-alg de A si

(i) $B \neq \emptyset$

(ii) $(B,+,.)$ est un sev de $(A,+,.)$

(iii) $\forall x,y\in B$, $x\times y\in B$.

déf A et B deux algèbres et $f : A\to B$. Alors f est un morph d'algèbres si :

(i) $f\in \mathcal{L}((A,+,.),(B,+,.))$.

(ii) $\forall x,y\in A$, $f(x\times y) = f(x)\times f(y)$.