Notes de révision du cours de mathématiques

MPSI1

Walter NGAMBOU, walter.ngambou@ac-versailles.fr

Lycée Pasteur, 2024–2025
Version du 22 janvier 2025

Chapitre 11

Structures algébriques

Remerciements à Nicolas LAILLET pour son aide et pour toutes ses ressources mathématiques, jusqu'à son préambule pour écrire en LaTeX.

Sommaire

1 Lois de composition interne (LCI's)

1.1 Définitions

Définition 1 : *Loi de composition interne.*
On considère un ensemble E non vide.
On appelle loi de composition interne (LCI) sur E toute fonction qui part de l'ensemble $E \times E$ des couples composés d'une première et d'une dernière composante dans E, et qui arrive dans E.

Notation. Si $\triangle$: $E \times E \to E$ est une LCI sur E, on note $x \triangle y$ l'image de tout couple (x, y), au lieu de $\triangle\,(x, y)$; et on note $(E, \triangle)$ l'ensemble E muni de la LCI $\triangle$.

Exemples 1.1.

1. L'addition et la multiplication usuelles entre les entiers naturels sont deux LCI's sur $\mathbb{N}$.
2. L'addition, la multiplication et la soustraction usuelles dans $\mathbb{Z}, \mathbb{D}_2, \mathbb{D}, \mathbb{Q}, \mathbb{R}$ et $\mathbb{C}$ sont des LCI's.
3. La division usuelle dans $\mathbb{Q}^*, \mathbb{R}^*$ et $\mathbb{C}^*$ sont des LCI's.

Définition 2 : *LCI associative.*
On considère un ensemble $(E, \triangle)$ non vide muni d'une LCI. On dit que la LCI $\triangle$ est associative, et qu'elle vérifie l'associativité, pour dire que :

$$\forall g \in E,\ \forall m \in E,\ \forall d \in E, \quad (g \triangle m) \triangle d = g \triangle (m \triangle d).$$

Remarque. Pour trois interprétations distinctes de l'associativité, on peut écrire :

- ▷ $\forall x \in E,\ \forall a \in E,\ \forall b \in E, \quad (x \triangle a) \triangle b = x \triangle (a \triangle b)$.
- ▷ $\forall x \in E,\ \forall a \in E,\ \forall b \in E, \quad (a \triangle x) \triangle b = a \triangle (x \triangle b)$.
- ▷ $\forall x \in E,\ \forall a \in E,\ \forall b \in E, \quad (b \triangle a) \triangle x = b \triangle (a \triangle x)$.

Exemples 1.2.

1. Les LCI's pré-citées sont associatives à l'exception de la soustraction et de la division.
2. On définit deux LCI's associatives sur la droite $\mathbb{R}$ des nombres réels en posant :
$$a \wedge b \overset{\text{def.}}{=} \min(a, b) \qquad \text{et} \qquad a \vee b \overset{\text{def.}}{=} \max(a, b).$$
(*Commentaire : sous-entendu : « pour tout* $(a, b) \in \mathbb{R} \times \mathbb{R}$ *»*).
3. On définit également deux LCI's associatives sur l'ensemble $\mathbb{N}^*$ des nombres entiers naturels non nuls en posant :
$$a \wedge b \overset{\text{def.}}{=} \text{PGCD}(a, b) \qquad \text{et} \qquad a \vee b \overset{\text{def.}}{=} \text{PPCM}(a, b).$$

Définition 3 : *LCI commutative.*
On considère $(E, \triangle)$ comme plus haut. On dit que la LCI $\triangle$ est commutative, et qu'elle vérifie la commutativité, pour dire que :

$$\forall a \in E,\ \forall b \in E, \quad a \triangle b = a \triangle b.$$

Exemples 1.3.

1. Toutes les LCI's pré-citées sont commutatives à l'exception, encore une fois, de la soustraction et de la division.
2. La multiplication entre les matrices carrées d'ordre 2 à coefficients dans $\mathbb{Z}$ n'est pas commutative, comme le prouvent les deux matrices...
3. Etant donné un ensemble non vide E, sur l'ensemble $\mathcal{P}(E)$ des parties de E, l'intersection et la réunion ensemblistes sont deux LCI's associatives et commutatives, tandis que la différence ensembliste est une LCI qui n'est ni associative, ni commutative.

4. Etant donné un ensemble E constitué d'au moins deux éléments, la composition entre les fonctions de E dans E n'est pas commutative.

Définition 4 : *Éléments commutants.*
Soit un ensemble E non vide. On dit qu'un élément a commute à un élément b pour une LCI $\triangle$ pour dire que : $a \triangle b = b \triangle a$.

Exemples 1.4. En exemple, pour la composition des fonctions de E dans lui-même, pour tout élément x_0 de E, les fonctions qui commutent à la fonction constante $x \mapsto x_0$ sont...

Définition 5 : *Élément neutre.*
On considère $(E, \triangle)$ comme plus haut. On dit qu'un élément e de E est neutre pour la LCI $\triangle$ pour dire que :

$$\forall x \in E, \qquad e \triangle x = x = x \triangle e \ .$$

Commentaire : les trois expressions ... sont égales.

Remarque. Un élément neutre commute à tout élément.

Exemples 1.5.

1. Le nombre zéro est un élément neutre pour l'addition dans $\mathbb{C}$ tandis la soustraction dans cet ensemble n'admet pas d'élément neutre.

2. Le nombre un est un élément neutre pour la multiplication dans $\mathbb{C}^*$, tandis que la division dans cet ensemble n'admet pas d'élément neutre.

3. Etant donné un ensemble non vide E, la fonction id_E est un élément neutre pour la composition des fonctions de E dans lui-même.

Exo 1. Chercher tous les éléments neutres de chacune des LCI's pré-citées.

Proposition 1 (Unicité de l'élément neutre).
Soit $(E, \triangle)$ comme plus haut. Alors $\triangle$ admet au plus un élément neutre.

Définition 6 : *Élément symétrisable.*
On considère $(E, \triangle)$ un ensemble muni d'une LCI à élément neutre, et deux éléments a et a' de E.

▷ On dit que a' est un symétrique de a pour la LCI $\triangle$ pour dire que :

$$a \triangle a' = e = a' \triangle a \ .$$

▷ On dit qu'un élément est symétrisable pour dire qu'il admet un symétrique.

Remarque. Deux éléments symétriques l'un à l'autre commutent.

Remarque. La symétrisabilité est subordonnée à l'élément neutre et on peut dire « symétrique par rapport à e », où e est cet élément neutre, pour rappeler cette dépendance.

Exemples 1.6.

1. Pour tout nombre complexe z, son opposé $-z$ est un symétrique (par rapport à 0) de z pour l'addition.

2. Pour tout nombre complexe z non nul, son inverse $z^{-1} = \dfrac{1}{z}$ est un symétrique (par rapport à 1) de z pour la multiplication, tandis que 0 n'admet pas de symétrique.

3. Etant donné un ensemble E constitué d'au moins deux éléments, aucune fonction constante de E dans lui-même n'admet de symétrique (par rapport à id_E) pour la composition des fonctions.

Proposition 2 (Unicité du symétrique).
Soit $(E, \triangle)$ comme plus haut. Si la LCI $\triangle$ est associative et à élément neutre e, alors tout élément de E admet au plus un symétrique.

Notation. Pour une LCI associative à élément neutre, le symétrique d'un élément a est noté a^{-1} en général, $-a$ pour une LCI commutative notée additivement.

Remarque. Pour une LCI associative à élément neutre, la relation « est symétrique à » est symétrique.

Proposition 3 (Symétrique d'une composée de deux).
Soient : un ensemble $(E, \triangle)$ muni d'une LCI associative à élément neutre ; puis deux éléments a et b de E. On suppose que a et b sont symétrisables. Ainsi, $a \triangle b$ est symétrisable de symétrique $b^{-1} \triangle a^{-1}$.

Exo 2. Si a est un élément symétrisable pour $\triangle$, que dire des quatre fonctions de E dans E suivantes : **1.** $x \mapsto x \triangle a$; **2.** $x \mapsto x \triangle a^{-1}$; **3.** $x \mapsto a \triangle x$; **4.** $x \mapsto a^{-1} \triangle x$?

Définition 7 : *Élément simplifiable.*
On considère $(E, \triangle)$ un ensemble muni d'une LCI, et un élément a de E. On dit a est simplifiable pour la LCI $\triangle$ pour dire que :

1. ET $\quad \forall x \in E,\ \forall y \in E, \quad a \triangle x = a \triangle y \implies x = y$;

2. ET $\quad \forall x \in E,\ \forall y \in E, \quad x \triangle a = y \triangle a \implies x = y$.

Remarque. Dans un ensemble muni d'une LCI associative à élément neutre, tout élément symétrisable est simplifiable (à droite et à gauche).

Exemples 1.7.

1. Dans $(\mathbb{Z}, \times)$ tout élément non nul est simplifiable.

2. Dans $(\mathcal{F}(\mathbb{R}, \mathbb{R}), \circ)$, toute fonction injective est simplifiable à gauche et toute fonction surjective est simplifiable à droite.

Proposition 4 (Symétrisable, simplifiable).
Dans un ensemble muni d'une LCI associative à élément neutre, quel que soit l'élément, s'il est symétrisable alors il est simplifiable.

Définition 8 : *Élément absorbant.*
On considère $(E, \triangle)$ un ensemble muni d'une LCI, et un élément o de E. On dit o est absorbant pour la LCI $\triangle$ pour dire que :

$$\forall x \in E, \qquad x \triangle o = o = o \triangle x$$

Exemple 1.8. Dans $(\mathbb{C}, \times)$, le nombre 0 est un élément absorbant.

Proposition 5 (Unicité de l'élément absorbant).
Soit $(E, \triangle)$ comme plus haut. Alors $\triangle$ admet au plus un élément absorbant.

Exo 3. Dans $[2025, +\infty[$, les LCI's définies par le minimum et par le maximum admettent-elles des éléments absorbants.

Définition 9 : *Seconde LCI distributive sur une première.*
On considère un ensemble non vide E muni de deux LCI's $\triangle$ et $\triangledown$.
On dit que, par rapport à la première LCI $\triangle$, la dernière LCI $\triangledown$ est :

▷ distributive à gauche pour dire que :

$$\forall x \in E,\ \forall a \in E,\ \forall b \in E, \qquad \begin{cases} (b \triangle a) \triangledown x = (b \triangledown x) \triangle (a \triangledown x) \\ (b \triangledown x) \triangle (a \triangledown x) = (b \triangle a) \triangledown x \end{cases}$$

▷ distributive à droite pour dire que :

$$\forall x \in E,\ \forall a \in E,\ \forall b \in E, \qquad \begin{cases} x \triangledown (a \triangle b) = (x \triangledown a) \triangle (x \triangledown b) \\ (x \triangledown a) \triangle (x \triangledown b) = x \triangledown (a \triangle b) \end{cases}$$

▷ distributive, et qu'elle est doublement distributive, pour dire qu'elle est à la fois distributive à droite et distributive à gauche.

Remarque. On a écrit deux fois deux égalités équivalentes car on a seulement échangés leurs membres. Cela afin de faciliter la maîtrise à la fois du "développement" et de la "factorisation".

Exemples 1.9.

1. Par rapport à l'addition entre les complexes, la multiplication est ditributive ; mais par rapport à la multiplication, l'addition n'est pas distributive.
2. L'intersection et la réunion entre les parties d'un même ensemble sont distributives l'une par rapport à l'autre.
3. Par rapport à l'addition entre les vecteurs de l'espace, le produit vectoriel est distributif (cf cours de Sciences physiques et à venir en mathématiques).
4. Dans $\mathbb{R}^{\mathbb{R}}$, la composition des fonctions est, par rapport à l'addition des fonctions réelles, distributive à gauche, mais elle ne l'est pas à droite.

Exo 4. Que dire des LCI's $\wedge$ et $\vee$ définies sur $\mathbb{R}$ par le minimum et le maximum binaires ?

1.2 Composées « multinaires »

Cadre de travail : Dans la suite, on considère un ensemble E muni d'une LCI $\triangle$ qui est associative et qui admet un élément neutre noté e.

1.2.1 Itérés d'un élément

Définition 10 : *Itérés.*
On considère un élément a de E.

▷ Pour tout entier naturel n, on appelle itéré d'indice n de a, pour la LCI $\triangle$ l'élément de E défini par récurrence comme suit :

$$a^n = \begin{cases} e & \text{si } n = 0 \\ a^{n-1} \triangle a & \text{si } n > 0 \end{cases}$$

▷ Si a est symétrisable pour $\triangle$, alors pour tout entier relatif n, on appelle itéré d'indice n de a pour la LCI $\triangle$ l'élément de E défini comme suit :

$$a^n = \begin{cases} a^n & \text{si } n \geqslant 0 \\ (a^{-1})^{-n} & \text{si } n < 0 \end{cases}$$

Notation. On note $n.a$ ou na pour une LCI noté additivement $+$, $\oplus$, ou $\boxplus$; notations qu'on réserve souvent au LCI's commutatives.

Remarques (Illustration).

Pour a quelconque,

$a^0 = e$;

$a^1 = e \triangle a$;

$a^2 = (e \triangle a) \triangle a$;

$a^3 = ((e \triangle a) \triangle a) \triangle a$.

Pour a symétrisable,

$a^0 = e$;

$a^{-1} = e \triangle a^{-1}$;

$a^{-2} = (e \triangle a^{-1}) \triangle a^{-1}$;

$a^{-3} = ((e \triangle a^{-1}) \triangle a^{-1}) \triangle a^{-1}$.

Commentaire : Peut-être convient-il de parler d'itéré n-ième seulement si n est un entier naturel non nul.

Exemples 1.10.

1. Les itérés naturels du nombre complexe 2 pour l'addition sont $0, 2, 4, 6, 8, \ldots$. On parle d'itérés additifs.
2. Les itérés naturels du nombre complexe $1/2$ pour la multiplication sont $1, 1/2, 1/4, 1/8, 1/16, \ldots$. On parle d'itérés multiplicatifs.
3. Les itérés relatifs multiplicatifs du complexe i sont 1, i, -1, et $-\mathrm{i}$.

Proposition 6 (Symétrique d'un itéré naturel).
Soit un élément a de E. On suppose que a est symétrisable. Ainsi, pour tout entier naturel n, a^n est symétrisable et

$$(a^n)^{-1} = a^{-n}$$

Proposition 7 (Composées d'itérés).
Soit un élément a de E. On a :

1. $\forall k \in \mathbb{N},\ \forall \ell \in \mathbb{N},\quad a^k \vartriangle a^\ell = a^{k+\ell}$.
2. Si a est symétrisable, $\quad \forall k \in \mathbb{Z},\ \forall \ell \in \mathbb{Z},\quad a^k \vartriangle a^\ell = a^{k+\ell}$.

Exo 5. Soit un intervalle ouvert I non trivial de $\mathbb{R}$. Montrer que pour toute fonction $f : I \to \mathbb{R}$ indéfiniment dérivable, pour tous entiers naturels k et ℓ, $\quad f^{(k+\ell)} = (f^{(k)})^{(\ell)}$.

Proposition 8 (Itérés d'itérés).
Soit un élément a de E. On a :

1. $\forall k \in \mathbb{N},\ \forall \ell \in \mathbb{N},\quad \left(a^k\right)^\ell = a^{k\times\ell}$.
2. Si a est symétrisable, $\quad \forall k \in \mathbb{Z},\ \forall \ell \in \mathbb{Z},\quad \left(a^k\right)^\ell = a^{k\times\ell}$.

1.2.2 Composée d'une liste

Commentaire : Une liste est ordonnée d'une première composante à une dernière.

Définition 11 : *Composée d'une liste.*
On considère une suite $(a_0, a_1, a_2, \ldots)$ d'éléments de E ; deux entiers naturels m et n tels que $m \leqslant n$.
Pour la LCI $\vartriangle$ la composée de la liste $(a_m, a_{m+1}, \ldots, a_n)$ est :

$$\prod_{k=m}^{n} a_k \overset{\text{def.}}{=} \begin{cases} a_m & \text{si } n = m \\ \left(\prod_{k=m}^{n-1} a_k\right) \vartriangle a_n & \text{si } m < n \end{cases}.$$

Remarque. On convient que $\prod_{k=m}^{n} a_k$ est égal à l'élément neutre de la LCI $\vartriangle$ si $n < m$.

Remarques (Illustration).

$\prod_{k=0}^{0} a_k = a_0$;

$\prod_{k=0}^{1} a_k = a_0 \vartriangle a_1$;

$\prod_{k=0}^{2} a_k = (a_0 \vartriangle a_1) \vartriangle a_2$;

$\prod_{k=0}^{3} a_k = ((a_0 \vartriangle a_1) \vartriangle a_2) \vartriangle a_3$.

Remarque. On note $\sum$ au lieu de $\prod$ pour une LCI commutative notée additivement.

Proposition 9 (« Passeur » global).
Soit une suite $(a_0, a_1, a_2, \ldots)$ d'éléments de E ; soit une suite $(p_1, p_2, \ldots)$ d'éléments de E.
On suppose que pour tout $k \in [\![1, +\infty[\![$, $a_{k-1} \vartriangle p_k = a_k$.
Ainsi, pour tous entiers naturels m et n tels que $m \leqslant n$,

$$a_m \vartriangle \left(\prod_{k=m+1}^{n} p_k \right) = a_n$$

Proposition 10 (Téléscopage).
Soit une suite $(a_0, a_1, a_2, \ldots)$ d'éléments de E.
On suppose que pour tout $k \in [\![0, \infty[\![$, a_k est symétrisable.
Ainsi, pour tous entiers naturels m et n tels que $m \leqslant n$,

$$a_m \vartriangle \left(\prod_{k=m+1}^{n} \left((a_{k-1})^{-1} \vartriangle a_k \right) \right) = a_n$$

Proposition 11 (Associativité générale).
Soient une suite $(a_0, a_1, a_2, \ldots)$ d'éléments de E ; soit p, q et r dans $\mathbb{N}$ tels que $p < q < r$.
Ainsi,

$$\left(\prod_{k=p}^{q-1} a_k \right) \vartriangle \left(\prod_{k=q}^{r-1} a_k \right) = \prod_{k=p}^{r-1} a_k$$

Notation. De ce fait, la composée $\prod_{k=m}^{n} a_k$ est notée à la fois :

$$a_m \vartriangle a_{m+1} \vartriangle \cdots \vartriangle a_{n-1} \vartriangle a_n$$

et

$$a_m \vartriangle a_{m+1} \vartriangle a_{m+2} \vartriangle \cdots \vartriangle a_n.$$

1.2.3 Composée commutative d'une famille finie

Proposition 12 (Commutativité générale).
Soit une suite $(a_0, a_1, a_2, \ldots)$ d'éléments de E ; soient deux entiers naturels m et n tels que $m \leqslant n$.
Si $k_1, k_2, \ldots, k_{L-1}, k_L$, où $L = 1 + n - m$, est une énumération (un à un et sans répétition de tous les éléments distincts) de $[\![m, n]\!]$,
Alors

$$a_{k_1} \vartriangle a_{k_2} \vartriangle \cdots \vartriangle a_{k_{L-1}} \vartriangle a_{k_L} \quad = \quad a_m \vartriangle a_{m+1} \vartriangle \cdots \vartriangle a_{n-1} \vartriangle a_n$$

Remarque. C'est que $[\![1, L]\!] \to [\![m, n]\!]$, $\ell \mapsto k_\ell$ est une bijection (ou correspondance un à un).

Notation. De ce fait, la composée $\prod_{k=m}^{n} a_k$ est notée à la fois : $\prod_{k \in [\![m,n]\!]} a_k$; $\prod_{\substack{k \in \mathbb{N} \\ m \leqslant k \leqslant n}} a_k$ et $\prod_{m \leqslant k \leqslant n} a_k$.

▶ ***Démonstration.*** Si L est supérieur à 2 et que $k_L \neq n$ alors on peut enchaîner des échanges de termes consécutifs jusqu'à mettre a_n en dernier dans la liste $(a_{k_1}, a_{k_2}, \cdots, a_{k_{L-1}}, a_{k_L})$. Ainsi peut-on raisonner par récurrence sur L pour établir l'égalité en usant de la commutativité (binaire). ***QED*** ◀

Proposition 13 (Itérés d'un produit).
Soient deux éléments a et b de E. On suppose que a et b commutent. Ainsi,

1. $\forall k \in \mathbb{N}, \quad (a \vartriangle b)^k = a^k \vartriangle b^k$.

2. Si a et b sont symétrisables, $\quad \forall k \in \mathbb{Z}, \quad (a \vartriangle b)^k = a^k \vartriangle b^k$.

Définition 12 : *Composée d'une famille finie commutative.*
On considère un ensemble fini K et une famille $(a_k)_{k\in K}$ d'éléments de E qui commutent deux à deux l'un à l'autre.
Pour la LCI $\triangle$ la composée de la famille finie commutative $(a_k)_{k\in K}$ est :

$$\prod_{k\in K} a_k \overset{\text{def.}}{=} a_{k_1} \triangle a_{k_2} \triangle \cdots \triangle a_{k_{L-1}} \triangle a_{k_L}$$

où $L = \operatorname{Card} K$ et $k_1, k_2, \ldots, k_{L-1}, k_L$ une énumération (un à un et sans répétition de tous les éléments distincts) de K, dans n'importe quel ordre.

Remarque. C'est que $[\![1, L]\!] \to K,\ \ell \mapsto k_\ell$ est une bijection (ou correspondance un à un).

Proposition 14 (Groupement par paquets).
Soient un ensemble fini K et une famille $(a_k)_{k\in K}$ d'éléments de E.

On suppose que les éléments a_k, pour $k \in K$, commutent deux à deux l'un à l'autre.

Ainsi,

- Pour toute paire $\{K_1, K_2\}$ de deux parties de K qui sont disjointes et de réunion égale à K,

$$\left(\prod_{k\in K_1} a_k\right) \triangle \left(\prod_{k\in K_2} a_k\right) = \prod_{k\in K} a_k.$$

- Plus généralement, pour tout ensemble fini L et pour toute partition finie $\{K_\ell :\ \ell \in L\}$ de K,

$$\prod_{\ell\in L}\left(\prod_{k\in K_\ell} a_k\right) = \prod_{k\in K} a_k.$$

Commentaire : On rappelle qu'une partition d'un ensemble est le résultat d'une mise de l'ensemble en parties non vides et deux à deux disjointes, en sorte que tout élément de l'ensemble appartienne à exactement une composante de la partition.

Proposition 15 (Ligne après ligne, colonne après colonne).
Soient deux ensembles finis I et J et une famille $(a_{i,j})_{(i,j)\in I\times J}$ d'éléments de E qui commutent deux à deux l'un à l'autre. Ainsi,

$$\prod_{i\in I}\left(\prod_{j\in J} a_{i,j}\right) = \prod_{(i,j)\in I\times J} a_{i,j} = \prod_{j\in J}\left(\prod_{i\in I} a_{i,j}\right).$$

1.3 LCI's par héritage

Définition 13 : *Partie stable et loi induite.*
On considère une partie A de E. On dit que la partie A est stable par la LCI $\triangle$ pour dire que :

$$\forall x \in E,\ \forall y \in E, \qquad (x \in A) \wedge (y \in A) \implies x \triangle y \in A.$$

Définition 14 : *Loi produit.*
On considère deux ensembles $(E_1, \triangle_1)$ et $(E_2, \triangle_2)$ munis chacun d'une LCI.
On munit l'ensemble produit cartésion $E_1 \times E_2$ de la loi produit de $\triangle_1$ par $\triangle_2$ en posant :

$$(x_1, x_2) \triangle (y_1, y_2) \overset{\text{def.}}{=} \big(x_1 \triangle_1 y_1\ ,\ x_2 \triangle_2 y_2\big).$$

Remarque. On adapte cela à des listes de plus de deux composantes.

Définition 15 : *Loi entre fonctions.*
On considère un ensemble non vide X.
On munit l'ensemble $\mathcal{F}(X,E) = E^X$ de la loi produit induite par $\triangle$ en posant :

$$f \triangle g : \begin{array}{ccc} X & \longrightarrow & E \\ x & \longmapsto & f(x) \triangle g(x) \end{array} .$$

Remarque. C'est que, $\forall f \in E^X,\ \forall g \in E^X,\quad \forall x \in X,\quad (f \triangle g)(x) \overset{\text{def.}}{=} f(x) \triangle g(x)$.

Exo 6 (Loi image). Soient un ensemble muni d'une LCI associative à élément neutre $(E, \triangle)$, un ensemble F et une fonction bijective de E dans F.
Montrer qu'on peut munir F d'une unique LCI $\triangledown$ telle que : $\forall x \in E,\ \forall y \in E,\quad f(x \triangle y) = f(x) \triangledown f(y)$.

1.4 Homomorphismes

Définition 16 : *Homomorphisme et isomorphisme.*
On considère deux $(E_1, \triangle_1)$ et $(E_2, \triangle_2)$ munis chacun d'une LCI ; puis une fonction $f : E_1 \to E_2$.

- ▷ On dit que la fonction f est/induit un homomorphisme de $(E_1, \triangle_1)$ dans $(E_2, \triangle_2)$, et on note
$$f : \begin{array}{ccc} (E_1, \triangle_1) & \longrightarrow & (E_2, \triangle_2), \\ x & \longmapsto & f(x) \end{array}$$
pour dire que f porte de la LCI du départ à la LCI d'arrivée :
$$\forall x_1 \in E_1,\ \forall y_1 \in E_1,\quad f(x_1 \triangle_1 y_1) = f(x_1) \triangle_2 f(y_1).$$
- ▷ Si tel est le cas, on dit plus précisément que f est/induit un isomorphisme de $(E_1, \triangle_1)$ dans $(E_2, \triangle_2)$ pour dire que $f : E_1 \to E_2$ est une fonction inversible et que sa réciproque $f^{-1} : E_2 \to E_1$ est/induit un homomorphisme de $(E_2, \triangle_2)$ dans $(E_1, \triangle_1)$.

Remarque. Dire que f est un homomorphisme c'est dire que le graphe Γ_f de f est une partie stable de $E_1 \times E_2$ pour la loi produit :

$$\forall (x_1,x_2) \in E_1 \times E_2,\quad \forall (y_1,y_2) \in E_1 \times E_2,\qquad \begin{cases} (x_1,x_2) \in \Gamma_f \\ (y_1,y_2) \in \Gamma_f \end{cases} \quad \Longrightarrow \quad \big(x_1 \triangle_1 y_1\ ,\ x_2 \triangle_2 y_2\big) \in \Gamma_f.$$

Commentaire : penser aux tableaux de proportionalité.

Exemples 1.11. On a les homomorphismes suivants :

1. $(\mathbb{R}^2, +) \to (\mathbb{C}, +),\ (a,b) \mapsto a + \mathrm{i}\, b$ et $(\mathbb{C}, +) \to (\mathbb{R}^2, +),\ z \mapsto (\mathrm{Re}(z), \mathrm{Im}(z))$.
2. $(\mathbb{C}, +) \to (\mathbb{C}, +),\ z \mapsto az$, pour tout $a \in \mathbb{C}$, et $(\mathbb{C}, +) \to (\mathbb{C}, +),\ z \mapsto \overline{z}$.
3. $(\mathbb{C}, +) \to (\mathbb{C}, \times),\ z \mapsto \exp(z)$.
4. $(\mathbb{C}, \times) \to (\mathbb{C}, \times),\ z \mapsto z^n$, pour tout $n \in \mathbb{N}$, $(\mathbb{C}, \times) \to (\mathbb{C}, \times),\ z \mapsto \overline{z}$, et $(\mathbb{C}, \times) \to (\mathbb{R}_+, \times),\ z \mapsto |z|$.
5. $(\mathbb{R}_+, \times) \to (\mathbb{R}_+, \times),\ x \mapsto x^p$, pour tout $p \in \mathbb{R}_+$.
6. $(\mathbb{R}_+^*, \times) \to (\mathbb{R}_+^*, \times),\ x \mapsto x^r$, pour tout $r \in \mathbb{R}$.
7. $(\mathbb{R}_+^*, \times) \to (\mathbb{R}, +),\ x \mapsto \ln(x)$.

Exo 7. Montrer que si une fonction inversible induit un homomorphisme de alors sa fonction réciproque également.

Proposition 16 (Composée d'homomorphismes).
Soient trois ensembles $(E_1, \triangle_1)$, $(E_2, \triangle_2)$ et $(E_3, \triangle_3)$ munis chacun d'une LCI. Ainsi, la composée d'un homomorphisme de $(E_1, \triangle_1)$ dans $(E_2, \triangle_2)$ suivi d'un homomorphisme de $(E_2, \triangle_2)$ dans $(E_3, \triangle_3)$ est un homomorphisme de $(E_1, \triangle_1)$ dans $(E_3, \triangle_3)$.

Commentaire : Qu'en est-il de la composée de deux isomorphismes ?

Définition 17 : *Endomorphisme et automorphisme.*
Plus précisément, pour un homomorphisme et un isomorphisme de $(E, \triangle)$ dans $(E, \triangle)$ lui-même, on parle espectivement d'endomorphisme et d'automorphisme de $(E, \triangle)$.

Commentaire : Que dire de la composée de deux endomorphismes ou de deux automorphismes ?

2 Structures de groupes

2.1 Généralités

Définition 18 : *Groupe.*
On considère un ensemble G muni d'une LCI $\star$.
On dit que le couple $(G, \star)$ est un groupe pour dire qu'à la fois la LCI $\star$:

(i) est associative ;

(ii) admet un élément neutre ;

(iii) admet (par rapport à son élément neutre) un symétrique à tout élément de G.

Exemples 2.1.

1. Le couple $(\mathbb{N}, +)$ n'est pas un groupe, tandis que $(\mathbb{Z}, +)$ en est un.

2. Les couples $(\mathbb{C}, +)$ et $(\mathbb{C}^*, \times)$ sont deux groupes.

Proposition 17 (Groupe des symétrisables).
Soit un ensemble $(E, \triangle)$ muni d'une LCI.
On suppose que la LCI $\triangle$ est associative et à élément neutre.
Ainsi, la LCI $\triangle$ induit sur l'ensemble des éléments symétrisables de $(E, \triangle)$ une structure de de groupe.

Exemples 2.2.

1. Les ensembles des éléments symétrisables des ensembles munis de LCI's associatifs à éléments neutres $(\mathbb{N}, +)$ et $(\mathbb{N}, \times)$ sont respectivement $\{0\}$ et $\{1\}$.

2. Etant donné un ensemble non vide X, la composition des fonctions de X dans X lui-même munit d'une structure de groupe l'ensemble des bijections de X dans X lui-même.
C'est le groupe des permutations de X.

3. La multiplication des (tables) matrices munit d'une structure de groupe l'ensemble des (tables) matrices carrées d'ordre 2 à coefficients dans le plan complexe qui sont inversibles.
C'est le deuxième groupe général linéaire sur $\mathbb{C}$.

Remarque. Pour tous éléments a et b de G, la translation à gauche associée à a :

$$\begin{array}{rccc} L_a & : & G & \longrightarrow & G \\ & & g & \longmapsto & a \star g \end{array}$$

et la translation à droite associée à b :

$$\begin{array}{rccc} R_b & : & G & \longrightarrow & G \\ & & g & \longmapsto & g \star b \end{array}$$

sont deux permutations de l'ensemble G de réciproques respectives $L_{a^{-1}}$ et $R_{b^{-1}}$.

Définition 19 : *Groupe commutatif/abélien.*
On dit à la fois qu'un groupe est commutatif et qu'il est abélien pour dire que sa LCI est commutative.

Exemples 2.3.

1. Etant donné un ensemble X constitué d'au trois éléments, le groupe des permutations de X est non commutatif comme le prouvent tout échange d'une paire d'éléments et tout échange d'un autre paire d'éléments.

2. Etant donné un plan $\mathcal{P}$ et un point O de ce plan, le groupe des similitudes du plan $\mathcal{P}$ fixant O est non commutatif comme le prouvent toute symétrie d'axe portant O et tout quart de tour de centre O.

3. Le deuxième groupe général linéaire sur $\mathbb{C}$ n'est pas commutatif comme le prouvent les deux matrices $\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}$ et $\begin{bmatrix}0 & -1\\ 1 & 0\end{bmatrix}$; ou encore les deux matrices $\begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix}$ et $\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}$.

2.2 Groupes par héritage

2.2.1 Sous-groupes

Définition 20 : *Sous-groupe.*
On considère un groupe $(G,\star)$, et une partie H de de l'ensemble G.
On dit que la partie H est un sous-groupe de $(G,\star)$ pour dire qu'à la fois H :

(i) possède l'élément neutre du groupe $(G,\star)$;

(ii) possède le symétrique de tout élément qui lui appartient ;

(iii) est stable par la LCI $\star$.

Remarque. Dire que la partie H est un sous-groupe de $(G,\star)$ s'écrit :

(i) $e \in H$;

(ii) $\forall a \in G, \quad a \in H \implies a^{-1} \in H$;

(iii) $\forall a \in G,\ \forall b \in G, \quad \begin{cases} a \in H \\ b \in H \end{cases} \implies a \star b \in H.$

Exemples 2.4.

1. La partie $\{2\,\mathrm{i}\,k :\ k \in \mathbb{Z}\} \overset{\text{not.}}{=} 2\,\mathrm{i}\,\pi\mathbb{Z}$ est un sous-groupe de $(\mathbb{C},+)$.

2. La partie $\{2^k :\ k \in \mathbb{Z}\}$ est un sous-groupe de $(\mathbb{C}^*,\times)$.

3. Les parties $\mathbb{Q}_+^*$, $\mathbb{R}_+^*$, et $\mathbb{U}$ sont des sous-groupes de $(\mathbb{Q}^*,\times)$, $(\mathbb{R}^*,\times)$, et $(\mathbb{C}^*,\times)$ respectivement.

4. Etant donné un plan $\mathcal{P}$ et un point O de ce plan, les similitudes du plan $\mathcal{P}$ fixant O constituent un sous-groupe des permutations de $\mathcal{P}$, qu'on appelle plutôt transformations du plan.

5. Si $(G,\star)$ est un groupe d'élément neutre e, les parties $\{e\}$ et G sont des sous-groupes de $(G,\star)$.

Proposition 18 (Caractérisation des sous-groupes).
Soit un groupe $(G,\star)$; soit une partie H de de l'ensemble G.
Ainsi, que H soit un sous-groupe de $(G,\star)$ est équivalent à ce qu'à la fois :

(i) ET H soit non vide ;

(ii) ET $\forall a \in G,\ \forall b \in G, \quad \begin{cases} a \in H \\ b \in H \end{cases} \implies a^{-1} \star b \in H.$

Remarque. On peut substituer $a \star b^{-1}$ à $a^{-1} \star b$ ci-haut.

Proposition 19 (Intersection de sous-groupes).
Soit un groupe $(G,\star)$. Soient un ensemble I et une famille $(H_i)_{i\in I}$ de sous-groupes de $(G,\star)$. Ainsi, l'intersection des H_i,

$$\bigcap_{i\in I} H_i$$

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

Définition 21 : *Sous-groupe engendré, éléments générateurs.*
On considère : un groupe $(G,\star)$; un entier naturel n non nul ; et des éléments $g_1,\dots,g_n$ de de l'ensemble G.

- ▷ On appelle sous-groupe de $(G,\star)$ engendré par $g_1,\dots,g_n$, qu'on note $\langle g_1,\dots,g_n\rangle$, l'intersection des sous-groupes de $(G,\star)$ qui possèdent les éléments $g_1,\dots,g_n$.
- ▷ On dit aussi que $g_1,\dots,g_n$ constituent un système de générateurs de $\langle g_1,\dots,g_n\rangle$.

Remarques.

- ▷ Le sous-groupe $\langle g_1,\dots,g_n\rangle$ est le plus petit, pour l'ordre partiel d'inclusion, des sous-groupes de $(G,\star)$ qui possèdent les éléments $g_1,\dots,g_n$.
- ▷ Le sous-groupe $\langle g_1,\dots,g_n\rangle$ est exactement constitué de toutes les composées des listes dont chaque composante est égale à un des g_i ou au symétrique d'un de ces éléments.
- ▷ Le sous-groupe engendré par un élément a de G est l'ensemble de ses itérés relatifs. On note multiplicativement
$$\langle a\rangle = \{a^k : k\in\mathbb{Z}\}.$$

Exemple 2.5.

1. La partie $2\,\mathrm{i}\,\pi\mathbb{Z}$ est le sous-groupe additif de $\mathbb{C}$ engendré par $2\,\mathrm{i}\,\pi$. Plus généralement...
2. La partie $\mathbb{U}_4=\{1,\mathrm{i},-1,-\mathrm{i}\}$ est le sous-groupe multiplicatif de $\mathbb{C}$ engendré par i. Plus généralement...
3. Le sous-groupe additif de $\mathbb{C}$ engendré par 1 et i est $\langle 1,\mathrm{i}\rangle=\{a+\mathrm{i}\,b : (a,b)\in\mathbb{Z}\times\mathbb{Z}\}$

Définition 22 : *Groupe monogène, générateur.*
On dit qu'un groupe est monogène pour dire qu'il peut être engendré par un seul élément, lequel est alors un générateur du groupe.

Exo 8. Montrer que pour tout entier naturel n, si n est non nul alors n est le plus grand commun diviseur des éléments de $n\mathbb{Z}$ au sens où il est le plus grand des entiers qui divisent à la fois tous les éléments de $n\mathbb{Z}$.

Exo 9. Montrer que pour tous entiers relatifs a et b, a est divisible par b si, et seulement si, $a\mathbb{Z}\subset b\mathbb{Z}$.

Proposition 20 (Sous-groupes additifs de $\mathbb{Z}$.).

1. Pour tout entier naturel n, la partie $n\mathbb{Z}$ de $\mathbb{Z}$ est un sous-groupe de $(\mathbb{Z},+)$ et l'entier n est son générateur positif.
2. Pour toute partie G de $\mathbb{Z}$, si G est un sous-groupe de $(\mathbb{Z},+)$, alors il existe un unique entier naturel n tel que $G=n\mathbb{Z}$.

Remarque. On étend les définitions du PGCD et du PPCM pour des listes quelconques d'entiers relatifs comme des générateurs positifs de sous-groupes additifs de $\mathbb{Z}$. (*voir exo 10*).

Exo 10. Soient deux entiers naturels a et b. Seulement à l'aide des définitions du plus grand commun diviseur et du plus petit commun multiple (selon l'ordre naturel),

1. Montrer que si a et b sont non tous les deux nuls alors le générateur positif du sous-groupe additif $a\mathbb{Z}+b\mathbb{Z}$ de $\mathbb{Z}$ est égal au plus grand commun diviseur de a et b :
$$a\mathbb{Z}+b\mathbb{Z}=\mathrm{PGCD}(a,b)\mathbb{Z}.$$
2. Montrer que si a et b sont tous les deux non nuls alors le générateur positif du sous-groupe additif $a\mathbb{Z}\cap b\mathbb{Z}$ de $\mathbb{Z}$ est égal au plus petit commun multiple de a et b :
$$a\mathbb{Z}\cap b\mathbb{Z}=\mathrm{PPCM}(a,b)\mathbb{Z}.$$

Définition 23 : *Groupe fini.*
On dit qu'un groupe $(G,\star)$ est fini pour dire que l'ensemble sous-jacent G est fini.

Remarque (2ème année). On appelle ordre d'un groupe fini $(G,\star)$ le cardinal de l'ensemble G.

Proposition 21 (Sous-groupes multiplicatifs finis de $\mathbb{C}$.).

1. Pour tout entier naturel n, la partie $\mathbb{U}_n$ de $\mathbb{C}$ est un sous-groupe fini de $(\mathbb{C}^*, \times)$ et l'entier n est son cardinal.
2. Pour toute partie G de $\mathbb{C}^*$, si G est un sous-groupe fini de $(\mathbb{C}^*, \times)$, alors il existe un unique entier naturel n tel que $G = \mathbb{U}_n$.

2.2.2 Groupe produit

On adapte ce qu'on dit des lois produits.

Remarque. La paire $\{(1,0)\ ;\ (0,1)\}$ est une partie génératrice du groupe produit $(\mathbb{Z}^2, +)$.

2.3 Homomorphismes de groupes

Définition 24 : *Homomorphisme de groupes.*
On considère deux groupes $(G_1, \star_1)$ et $(G_2, \star_2)$; puis une fonction $f : G_1 \to G_2$.

▷ On dit que la fonction f induit un homomorphisme du groupe $(G_1, \star_1)$ dans le groupe $(G_2, \star_2)$, et on note

$$\begin{aligned} f :\ (G_1, \star_1) &\longrightarrow (G_2, \star_2), \\ x &\longmapsto f(x) \end{aligned}$$

pour dire que les trois propositions suivantes tiennent :

1. f porte du neutre du départ au neutre de l'arrivée : $f(e_1) = f(e_2)$, où e_1 et e_2 sont les neutres des deux groupes ;
2. f préserve la symétrisation : $\forall x_1 \in G_1, \quad f(x_1^{-1}) = f(x_1)^{-1}$;
3. f porte de la LCI $\star_1$ à la LCI $\star_2$: $\forall x_1 \in G_1,\ \forall y_1 \in G_1, \quad f(x_1 \star_1 y_1) = f(x_1) \star_2 f(y_1)$.

▷ Si tel est le cas, on dit plus précisément que f induit un isomorphisme du groupe $(G_1, \star_1)$ dans le groupe $(G_2, \star_2)$ pour dire que $f : G_1 \to G_2$ est une fonction inversible et que sa réciproque $f^{-1} : G_2 \to G_1$ induit un homomorphisme du groupe $(G_2, \star_2)$ dans le groupe $(G_1, \star_1)$.

Remarques.

▷ Dire que f est un homomorphisme de groupes c'est dire que le graphe Γ_f de f est un sous-groupe du groupe produit :

- ET Γ_f est non vide (ou possède le couple des neutres) ;
- ET

$$\forall (x_1, x_2) \in G_1 \times G_2, \quad \forall (y_1, y_2) \in G_1 \times G_2, \qquad \begin{cases} (x_1, x_2) \in \Gamma_f \\ (y_1, y_2) \in \Gamma_f \end{cases} \implies \left(x_1^{-1} \vartriangle_1 y_1\ ,\ x_2^{-1} \vartriangle_2 y_2\right) \in \Gamma_f.$$

▷ On adapte la définition d'un endomorphisme (resp. d'automorphisme) d'un ensemble muni d'une LCI à celle d'un endomorphisme (resp. d'automorphisme) d'un groupe.

Exemples 2.6.

1. La fonction $\mathbb{C} \to \mathbb{C},\ z \mapsto \overline{z}$ induit un automorphisme du groupe $(\mathbb{C}, +)$ et un automorphisme du groupe $(\mathbb{C}^*, \times)$.
2. Étant donnés un groupe $(G, \star)$ et un élément a de G, d'après la proposition 7 on a l'homomorphisme de groupes : $(\mathbb{Z}, +) \to (G, \star),\ n \mapsto a^n$.
3. Étant donnés deux ensembles X et Y, et une bijection $p : X \to Y$; on a l'isomorphisme de groupes : $(\mathcal{S}_X, \circ) \to (\mathcal{S}_Y, \circ),\ u \mapsto v = pup^{-1}$.
4. Étant donnés un groupe $(G, \star)$ et un élément a de G, on a l'automorphisme de groupe : $(G, \star) \to (G, \star),\ g \mapsto aga^{-1}$.

Proposition 22 (Homomorphismes de groupes).
Soient deux groupes $(G_1, \star_1)$ et $(G_2, \star_2)$; puis une fonction $f : G_1 \to G_2$.
Pour que la fonction f induise un homomorphisme du groupe $(G_1, \star_1)$ dans le groupe $(G_2, \star_2)$, il est suffisant (et nécessaire) que f porte de la LCI du départ à la LCI d'arrivée :

$$\forall x_1 \in G_1,\ \forall y_1 \in G_1, \qquad f(x_1 \star_1 y_1) = f(x_1) \star_2 f(y_1).$$

Proposition 23 (Images réciproques et images directes).
Soient deux groupes $(G_1, \star_1)$ et $(G_2, \star_2)$; puis une fonction $f : G_1 \to G_2$.

On suppose que f est induit un homomorphisme de groupes.

Ainsi :

a) Pour tout sous-groupe H_2 de $(G_2, \star_2)$ à l'arrivée, l'image réciproque par f de H_2 :

$$\begin{aligned} f^{-1}(H_2) &\overset{\text{def.}}{=} \{g_1 \in G_1 \mid\ f(g_1) \in H_2\} \\ &= \{g_1 \in G_1 \mid\ \exists h_2 \in H_2 \ /\ f(g_1) = h_2\} \end{aligned}$$

est un sous-groupe de $(G_1, \star_1)$ au départ.

b) Pour tout sous-groupe H_1 de $(G_1, \star_1)$ au départ, l'image directe par f de H_1 :

$$\begin{aligned} f(H_1) &\overset{\text{def.}}{=} \{f(h_1) :\ h_1 \in H_1\} \\ &= \{g_2 \in G_2 \mid\ \exists h_1 \in H_1 \ /\ g_2 = f(h_1)\} \end{aligned}$$

est un sous-groupe de $(G_2, \star_2)$ à l'arrivée.

Définition 25 : *Noyau, image.*
On considère un homomorphisme f d'un groupe de départ $(G_1, \star_1)$ dans un groupe d'arrivée $(G_2, \star_2)$ de neutre e_2.

- ▷ On appelle noyau de f le sous-groupe du départ image réciproque par f du sous-groupe trivial de l'arrivée (constitué de tout élément duquel f porte au neutre de l'arrivée) :

$$\operatorname{Ker}(f) \overset{\text{def.}}{=} \{g_1 \in G_1 \mid\ f(g_1) = e_2\}$$

- ▷ On appelle image de f le sous-groupe de l'arrivée image directe par f du groupe de départ (constitué de tout élément auquel f porte d'au moins un élément du départ) :

$$\begin{aligned} \operatorname{Im}(f) &\overset{\text{def.}}{=} \{f(g_1) :\ g_1 \in G_1\} \\ &= \{g_2 \in G_2 \mid\ \exists g_1 \in G_1 \ /\ g_2 = f(g_1)\} \end{aligned}$$

Commentaire : Parmi les éléments du départ, les éléments du noyau sont ceux qui envoient par f au neutre de l'arrivée ou encore ceux dont l'image commune par f est neutre à l'arrivée. Et parmi les éléments de l'arrivée, les éléments de l'image sont ceux qui reçoivent par f d'au moins un élément du départ.

Exo **11.** Quels sont les noyaux et images des homomorphismes de groupes suivants ?

1. $(\mathbb{C}, +) \to (\mathbb{R}, +),\ z \mapsto \operatorname{Re}(z)$; et $(\mathbb{C}, +) \to (\mathbb{R}, +),\ z \mapsto \operatorname{Im}(z)$.

2. $(\mathbb{C}, +) \to (\mathbb{C}, +),\ z \mapsto az$, pour tout $a \in \mathbb{C}^*$; et $(\mathbb{C}, +) \to (\mathbb{C}, +),\ z \mapsto \overline{z}$.

3. $(\mathbb{C}, +) \to (\mathbb{C}^*, \times),\ z \mapsto \exp(z)$; $(\mathbb{R}, +) \to (\mathbb{C}^*, \times),\ t \mapsto \exp(\mathrm{i}\, 2\pi \dfrac{t}{T})$, pour tout $T \in]0, +\infty[$; et $(\mathbb{Z}, +) \to (\mathbb{C}^*, \times),\ k \mapsto \exp(\mathrm{i}\, 2\pi \dfrac{k}{n})$, pour tout $n \in \mathbb{N}^*$.

4. $(\mathbb{C}^*, \times) \to (\mathbb{C}^*, \times),\ z \mapsto z^k$, pour tout $k \in \mathbb{Z}$; $(\mathbb{C}^*, \times) \to (\mathbb{C}^*, \times),\ z \mapsto \overline{z}$; et $(\mathbb{C}^*, \times) \to (\mathbb{R}_+^*, \times),\ z \mapsto |z|$.

5. $(\mathbb{R}_+^*, \times) \to (\mathbb{R}_+^*, \times),\ x \mapsto x^r$, pour tout $r \in \mathbb{R}$.

6. $(\mathbb{R}_+^*, \times) \to (\mathbb{R}, +),\ x \mapsto \ln(x)$.

7. $(\mathbb{R} \times \mathbb{R}, +) \to (\mathbb{C}, +),\ (x, y) \mapsto x + \mathrm{i}\, y$.

Proposition 24 (Noyau et translation à gauche, à droite).
Soit un homomorphisme f d'un groupe de départ $(G,\star)$. Soit un élément x_0 de G. Ainsi,

$$\{x_0 \star k :\ k \in \mathrm{Ker}(f)\} = \{k' \star x_0 :\ k' \in \mathrm{Ker}(f)\}$$

Notation. $x_0 \star \mathrm{Ker}(f)$ et $\mathrm{Ker}(f) \star x_0$.

Proposition 25 (Ensembles d'antécédents).
Soit un homomorphisme f d'un groupe de départ $(G,\star)$ dans un groupe d'arrivée $(H,\bullet)$. Soient un élément x_0 de G et un élément y_0 de H.
On suppose que $f(x_0) = y_0$.
Ainsi, l'ensemble des solutions dans G de l'équation

$$f(x) = y_0\ , \qquad x \in G$$

est

$$x_0 \star \mathrm{Ker}(f) = \{x \in G \mid\ f(x) = y_0\} = \mathrm{Ker}(f) \star x_0$$

Exo 12. Soient : un groupe $(G,\star)$; une partie A de G ; et un élément g de G. Montrer que les deux parties $g \star A$ et $A \star g$ sont en bijection avec A.

Proposition 26 (CNS d'injectivité.).
Quel que soit l'homomorphisme de groupes, pour qu'il soit injectif il est nécessaire et suffisant que son noyau soit trivial.

Commentaire : Par définition, dire qu'il est surjectif c'est dire que son image est ...

Exo 13. Soit un entier naturel n supérieur à 1. Soit un entier relatif p.
Pour quelles valeurs de p la fonction $\mathbb{U}_n \to \mathbb{U}_n,\ z \mapsto z^p$ est-elle bijective ?

Proposition 27 (Cardinalité dans le cas fini au départ.).
Soit un homomorphisme f d'un groupe de départ $(G,\star)$.

On suppose que l'ensemble G est fini.

Ainsi,

a) Les parties $\mathrm{Ker}(f)$ au départ et $\mathrm{Im}(f)$ à l'arrivée sont finies et leurs cardinaux divisent $|G|$;

b) $\dfrac{|G|}{|\mathrm{Ker}(f)|} = |\mathrm{Im}(f)|$.

▶ ***Démonstration.***

Comme la fonction $G \to \mathrm{Im}(f),\ x \mapsto f(x)$ part d'un ensemble fini et qu'elle est surjective, son ensemble d'arrivée est fini. C'est que $\mathrm{Im}(f)$ est un ensemble fini.

Les ensembles des antécédents par f des éléments de $\mathrm{Im}(f)$ à l'arrivée constituent une partition de G au départ. Et cette partition est finie.

Pour tout $x_0 \in G$, la fonction $G \to G,\ x \mapsto x_0 \star x$ est injective, donc elle induit une bijection de toute partie sur son image.

Ainsi, chaque composante de la partition ci-avant correspond un à un avec $\mathrm{Ker}(f)$ d'après la description des ensembles d'antécédents par un homomorphisme de groupes.

QED ◀

Exo 14. Ce résultat subsiste-t-il si on suppose plutôt que c'est le groupe d'arrivée qui est fini ?

2.4 Groupe symétrique d'un ensemble

Définition 26 : *Permutation et groupe symétrique d'un ensemble.*
On considère un ensemble non vide X.

- ▷ On appelle permutation de X toute bijection de l'ensemble X sur lui-même.
- ▷ On appelle groupe symétrique de X le groupe que constituent les permutations de X avec la composition des fonctions. On le note $(\mathcal{S}_X, \circ)$.

Exemples 2.7.

1. $\{1;2;3\} \to \{1;2;3\};\ 1 \mapsto 3,\ 2 \mapsto 2,\ 3 \mapsto 1.$

2. $[a,b] \to [a,b],\ x \mapsto a+b-x$, pour tous réels a et b tels que $a < b$.

3. $\mathbb{C} \to \mathbb{C},\ z \mapsto z+b$, pour tout complexe b.

4. $\mathbb{C}^2 \to \mathbb{C}^2,\ (z_1,z_2) \mapsto (z_1+z_2\ ,\ -z_1+z_2)$.

Remarque. On peut, notamment, représenter une permutation d'un ensemble fini par

- ▷ Une table de ses valeurs ;
- ▷ Un graphe orienté dont les états indiquent les éléments sur lesquels agit la permutation tandis que les transitions indiquent l'action de la permutation ;
- ▷ Une table à double entrée des valeurs de la fonction indicatrice de son graphe.

Exo 15. Définir deux permutations σ et ρ en complétant les écritures suivantes, puis les représenter selon les deux autres modes pré-cités :

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ \cdot & \cdot & \cdot & \cdot & \cdot \end{pmatrix},\ \rho = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \end{pmatrix}$$

Proposition 28 (Groupes isomorphes de permutations).
Soient deux ensembles E et F.
On suppose que E et F sont en bijection.
Ainsi, les groupes $(\mathcal{S}_E, \circ)$ et $(\mathcal{S}_F, \circ)$ sont isomorphes.

Plus précisément, si $f : E \to F$ est une bijection, alors on a l'isomorphisme suivant :

$$\begin{aligned} (\mathcal{S}_E, \circ) &\longrightarrow (\mathcal{S}_F, \circ) \\ \sigma &\longmapsto \rho = f \circ \sigma \circ f^{-1} \end{aligned}$$

associé au schéma suivant :

$$\begin{array}{ccc} E & \xleftarrow{\sigma} & E \\ f\downarrow & & \downarrow f. \\ F & \xleftarrow[\rho]{} & F \end{array}$$

Commentaire : On peut dire couramment que les deux groupes sont semblables : ils se correspondent un à un en gardant les rapports entre leurs éléments.

Remarques.

- ▷ La fonction $E \times E \to F \times F,\ (x\ ,\ y) \mapsto \big(f(x)\ ,\ f(y)\big)$ est une bijection qui transforme le graphe de σ en le graphe de ρ :

$$\forall y \in E,\ \forall x \in E, \qquad y = \sigma(x) \quad \Longleftrightarrow \quad f(y) = \rho\big(f(x)\big).$$

- ▷ De ce fait, pour tout entier naturel n non nul, l'étude du groupe symétrique de tout ensemble à n éléments se ramène à l'étude du groupe symétrique de $[\![1,n]\!]$.

Définition 27 : *n-ième groupe symétrique.*
Pour tout entier naturel n non nul, l'ensemble des permutations de $[\![1,n]\!]$ est noté $\mathcal{S}_n$ et le groupe $(\mathcal{S}_n, \circ)$ est appelé n-ième groupe symétrique.

Proposition 29 (Nombre de permutations).
Soit un ensemble non vide est fini de cardinal égal à un entier naturel n non nul, alors l'ensemble de ses permutations est fini de cardinal égal à $n!$.

▶ ***Démonstration.*** En exercice. *(Indication : On pourra représenter une telle permutation par un tableau carré des valeurs de la fonction indicatrice de son graphe. Voir traité du dénombrement.)* ***QED*** ◀

Remarques (Énumérations). On se donne un entier naturel n non nul.

Si $n = 1$, alors la seule énumération de $[\![1, n]\!]$ est :

1. 1.

Si $n = 2$, alors les énumérations de $[\![1, n]\!]$, en croissant dans l'ordre lexicographique de gauche à droite, sont :

1. 1 2 ;
2. 2 1.

Si $n = 3$, alors les énumérations de $[\![1, n]\!]$, en croissant dans l'ordre lexicographique de gauche à droite, sont :

1. 1 2 3 ;
2. 1 3 2 ;
3. 2 1 3 ;
4. 2 3 1 ;
5. 3 1 2 ;
6. 3 2 1.

Commentaire : Rappelons que le support d'une suite numérique est le complémentaire de l'ensemble des rangs auxquels la suite est nulle. De manière générale, on veut que le support d'une fonction soit la partie de son ensemble de définition où « il se passe quelque chose ».

Définition 28 : *Points fixes, support.*
On considère : un ensemble non vide X ; et une permutation f de X.

▷ On appelle point fixe de f tout élément x de X qui envoie par f à lui-même : $x \overset{f}{\mapsto} x$:

$$\mathrm{Fix}(f) \overset{\text{def.}}{=} \{x \in X \mid \ x = f(x)\}.$$

▷ On appelle support de f le complémentaire dans X de l'ensemble des points fixes de f :

$$\mathrm{Supp}(f) \overset{\text{def.}}{=} \{x \in X \mid \ x \neq f(x)\}.$$

Exo 16. Quelles sont les permutations non triviales dont les supports sont les plus petits possibles ?

Remarques.

▷ On parle aussi de point (ou d'état) variant et de point (ou d'état) invariant par f.
Ainsi le support de f est l'ensemble des points variants par f.

▷ Le support de toute permutation est stable par la permutation.
Ainsi, toute permutation d'un ensemble induit une permutation de son support.

Proposition 30 (CS de commutativité).
Si deux permutations d'un même ensemble sont à supports disjoints alors elles commutent.

Définition 29 : *Transposition.*
On considère : un ensemble X non vide ; puis une permutation f de X.
On dit que f est une transposition pour dire qu'on peut trouver 2 états distincts x_0 et x_1 de X tels que :

▷ ET $\quad x_0 \overset{f}{\mapsto} x_1 \quad$ et $\quad x_1 \overset{f}{\mapsto} x_0$.

▷ ET $\quad \forall x \in X, \quad x \notin \{x_1, x_2\} \quad \Longrightarrow \quad x \overset{f}{\mapsto} x$.

Notation. De manière abrégée, une transposition comme ci-avant est notée $\begin{pmatrix} x_0 & x_1 \end{pmatrix}$.

Proposition 31 (Produits de transpositions).
Soit un ensemble non vide et fini. Toute permutation de cet ensemble s'écrit comme produit de transpositions.

Commentaire : En d'autres mots, on peut obtenir toute permutation en enchaînant des transpositions.

▶ ***Démonstration.***
Procédure de décomposition : on considère une permutation non triviale puis on la compose successivement à gauche/après/en arrière/en aval, ou successivement à droite/avant/en avant/en amont, par des transpositions jusqu'à obtenir la permutation qui fixe tout point/état , i.e. l'identité. Puis on recompose.
Ainsi, on peut raisonner par récurrence sur le cardinal du support de la permutation pour prouver que la procédure décrite est satisfaisante. ***QED*** ◀

Exo 17. Décomposer en produits de transpositions les permutations de l'exo 15.

Remarque. A cela s'ajoute que :

- ▷ Les transpositions de tout ensemble fini non vide variant un même point donné engendrent le groupe de ses permutations.
- ▷ Les transpositions de tout intervalle non vide des entiers naturels échangeant deux entiers consécutifs engendrent le groupe de ses permutations.

Définition 30 : *Orbite d'un point.*
On considère : un ensemble non vide X ; et une permutation f de X.
Pour tout état x_0 de X, on appelle orbite de x_0 suivant f l'ensemble des points images de x_0 par les itérés relatifs de f :

$$\big\{f^k(x_0) :\ k \in \{\ldots, -2\ ;\ -1\ ;\ 0\ ;\ 1\ ;\ 2\ ;\ \ldots\}\big\}.$$

Commentaire : Dans ces circonstances, en langage courant, dire « antécédent et conséquent » ou encore « envoyeur/émetteur et receveur », plutôt que « antécédent et image », peut-être plus intelligible.

Exo 18. Décrire les orbites des permutations de l'exo 15.

Proposition 32 (Partition suivant les orbites).
Soit un ensemble X non vide. Les orbites distinctes suivant toute permutation de X constituent une partition de X lui-même.

▶ ***Démonstration.*** Etant donnée une permutation f de X, la relation « être dans l'orbite suivant f de » est une relation d'équivalence sur X : elle est réflexive, symétrique et transitive à causes des propriétés de calculs des itérés de f. ***QED*** ◀

Définition 31 : *Cycle.*
On considère : un ensemble X non vide ; puis une permutation f de X.

1. Pour tout entier naturel L supérieur à 2, on dit à la fois que f est un cycle de longueur L et que f est un L-cycle pour dire qu'on peut trouver L états distincts $x_0, x_1, \ldots, x_{L-2}, x_{L-1}$ de X tels que :
   a) ET $\quad x_0 \overset{f}{\mapsto} x_1 \overset{f}{\mapsto} \cdots \overset{f}{\mapsto} x_{L-2} \overset{f}{\mapsto} x_{L-1} \overset{f}{\mapsto} x_0$;
   b) ET $\quad \forall x \in X,\ x \notin \{x_0, x_1, \ldots, x_{L-2}, x_{L-1}\} \implies x \overset{f}{\mapsto} x.$
2. On dit que f est un cycle pour dire qu'on peut trouver un entier naturel L supérieur à 2 tel que f est un cycle de longueur L.

Notation. De manière abrégée, un cycle décrit comme ci-avant est notée $(x_0 \quad x_1 \quad \ldots \quad x_{L-2} \quad x_{L-1})$.

Remarque. Un cycle est une permutation de support fini ; et sa longueur est égale au cardinal de son support.

Exo 19. Soit un cycle. Exprimer ses itérés.

Proposition 33 (Produits de cycles à supports disjoints).
Que soit donné un ensemble fini constitué d'au moins deux éléments.
Ainsi, pour toute permutation non triviale de cet ensemble il existe un unique ensemble de cycles à supports disjoints dont le produit commutatif est égal à σ.

▶ ***Démonstration.*** (*Non exigible de tous.*)

On nomme X l'ensemble, et n son nombre d'éléments.

Comme n est supérieur à 2, on se donne une permutation σ non triviale X.

On met l'ensemble X en les parties non vides et disjointes deux à deux que sont les orbites suivant la permutation σ.

(1) Comme σ est non triviale, on se donne une orbite O suivant cette permutation qui possède au moins deux éléments.

Comme l'ensemble X possède n éléments, la partie O possède un nombre d'éléments inférieur à n.

Soit un point x de l'orbite O.

Ainsi, deux au moins des $n+1$ expressions ci-après sont égales : $\sigma^0(x), \sigma^1(x), \dots, \sigma^n(x)$.

Donc on nomme L le petit entier entre 1 et n tel que deux au moins des $L+1$ expressions ci-après sont égales : $\sigma^0(x), \sigma^1(x), \dots, \sigma^L(x)$.

Ainsi, les L expressions ci-après sont inégales : $\sigma^0(x), \sigma^1(x), \dots, \sigma^{L-1}(x)$.

Comme σ est une injection, les L expressions ci-après sont inégales : $\sigma^1(x), \sigma^2(x), \dots, \sigma^L(x)$.

Ainsi, d'après la définition de L, et parce que les fonctions σ^{-L} et σ^L sont réciproques l'une de l'autre, les trois expressions ci-après sont égales : $\sigma^{-L}(x)$, x, $\sigma^L(x)$.

Ainsi, comme l'entier L est supérieur à 1, d'après le théorème de la division euclidienne, l'orbite O est exactement constitué des points désignés par les expressions ci-après :

$$\sigma^0(x)\ ,\ \sigma^1(x)\ ,\ \dots\ ,\ \sigma^{L-1}(x).$$

Or ces expressions sont inégales et au nombre de L. Donc L est égale au cardinal de l'orbite O.

Or par hypothèse, O possède au moins deux éléments, donc L est supérieur à 2.

On a montré que sur chacune de ses orbites non triviales, la permutation qui est égale à σ sur l'orbite et à id_X sur le complémentaire de l'orbite est un cycle de support égal à l'orbite.

On obtient ainsi des cycles à supports disjoints dont la composée commutative est égale à σ.

D'où l'existence de la décomposition.

(2) Réciproquement, si σ s'écrit comme un tel produit, alors pour chacun des cycles en question on trouve par le calcul que son support est égal à une orbite suivant σ et que les deux permutations y coïncident.

D'où l'unicité de la décomposition.

QED ◀

Remarque. Pour toute orbite O suivant σ, pour tout état x de O, si l'orbite O est non triviale alors σ est égale au cycle ci-après sur la partie O :

$$c_\sigma(O) \overset{\text{def.}}{=} \begin{pmatrix} \sigma^0(x) & \sigma^1(x) & \cdots & \sigma^{|O|-2}(x) & \sigma^{|O|-1}(x) \end{pmatrix}$$

lequel est indépendant du choix de x dans l'orbite O. Ainsi, si on note Orb_σ l'ensemble des orbites suivant σ, on obtient la formule ci-après :

$$\sigma = \prod_{O \in \mathrm{Orb}_\sigma} c_\sigma(O).$$

Exo 20. Décomposer en produits de cycles à supports disjoints les permutations de l'exo 15.

3 Structures d'anneaux

3.1 Généralités

Définition 32 : *Anneau.*
On appelle anneau tout triplet $(A, \boxplus, \boxtimes)$ où A est un ensemble non vide, $\boxplus$ est une première LCI sur A et $\boxplus$ est une seconde LCI A tels que :

1. La première LCI $\boxplus$:
   - ***a***) est associative et commutative ;
   - ***b***) admet un élément neutre et un symétrique à tout élément.
2. La seconde LCI $\boxtimes$:
   - ***a***) est associative ;
   - ***b***) admet un élément neutre ;
   - ***c***) est, par rapport à la première LCI $\boxplus$, (doublement) distributive.
3. Les éléments neutres des deux LCI's $\boxplus$ et $\boxtimes$ sont distincts.

Notations.

▷ On note 0_A et 1_A les éléments neutres respectifs des première et seconde LCI's.

▷ Pour tout élément a de A, on note :

- $-a$ le symétrique de a pour la première LCI, et on l'appelle oppposé de a ;
- a^{-1} le symétrique de a pour la seconde LCI s'il existe, et on l'appelle inverse de a.

Remarque. Un anneau est un groupe additif (i.e. groupe commutatif) muni d'une seconde LCI associative à élément neutre qui, par rapport à la première LCI, est distributive.

Exemples 3.1.

1. Anneaux de nombres usuels : $(\mathbb{Z}, +, \times)$, $(\mathbb{D}, +, \times)$, $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$, $(\mathbb{C}, +, \times)$.
2. Anneaux de fonctions partant d'un même ensemble et arrivant dans $\mathbb{A}$: $(\mathbb{A}^X, +, \times)$; où X est un ensemble non vide à l'instar de $\{1; 2\}$, de $\mathbb{N}$ et de $[0, 1]$, et $\mathbb{A} \in \{\mathbb{Z}, \mathbb{D}, \mathbb{Q}, \mathbb{R}, \mathbb{C}\}$.
3. Anneaux des polynômes formels/symboliques à coefficients dans $\mathbb{A}$: $(\mathbb{A}[X], +, \times)$; où $\mathbb{A} \in \{\mathbb{Z}, \mathbb{D}, \mathbb{Q}, \mathbb{R}, \mathbb{C}\}$.
4. Anneaux des (tables) matrices carrées d'un certain ordre à coefficients dans $\mathbb{A}$: $(\mathcal{M}(n, \mathbb{A}), +, \times)$; où $n \in \mathbb{N}^*$ et $\mathbb{A} \in \{\mathbb{Z}, \mathbb{D}, \mathbb{Q}, \mathbb{R}, \mathbb{C}\}$.

Définition 33 : *Sous-anneau.*
Un sous-anneau d'un anneau est une partie qui d'une part possède le zéro et est stable par passage à l'opposé et par addition , et d'autre part possède l'unité et est stable par multiplication.

Exemples 3.2.

1. $\{r + s\sqrt{2} : \ (r, s) \in \mathbb{Z} \times \mathbb{Z}\}$ est un sous-anneau de $(\mathbb{R}, +, \times)$.
2. $\{r + is : \ (r, s) \in \mathbb{Z} \times \mathbb{Z}\}$ est un sous-anneau de $(\mathbb{C}, +, \times)$.

Proposition 34 (Caractérisation des sous-anneaux).
Soient un anneau et une partie de son ensemble sous-jacent. Pour que la partie soit un sous-anneau, il est nécessaire et suffisant qu'elle possède l'unité et qu'elle soit stable par soustraction et par multiplication.

Exo 21. Montrer que que $\mathbb{Z}$ est le plus petit sous-anneau de $(\mathbb{C}, +, \times)$.

Comme pour les sous-groupes, on définit : les anneaux produits, dont les anneaux fonctionnels.

Notation. Le groupe des inversibles / unités d'un anneau $(A, +, \times)$ est noté $A^\times$.

Exemples 3.3. On a : $\mathbb{C}^\times = \mathbb{C}^*$. Et plus généralement, $\mathcal{M}(n,\mathbb{C})^\times$ est noté $\mathrm{GL}(n,\mathbb{C})$ (n-ième groupe général linéaire sur $\mathbb{C}$) pour tout $n \in \mathbb{N}^*$.

Définition 34 : *Homomorphisme d'anneaux.*
On considère deux anneaux $(A,+_1,\times_1)$ et $(B,+_2,\times_2)$; puis une fonction $f : A \to B$.

▷ On dit que la fonction f induit un homomorphisme de l'anneau $(A,+_1,\times_1)$ dans l'anneau $(B,+_2,\times_2)$, et on note

$$f : \begin{array}{ccc} (A,+_1,\times_1) & \longrightarrow & (B,+_2,\times_2), \\ x & \longmapsto & f(x) \end{array}$$

pour dire que :

D'une part,

a) $f(0_A) = 0_B$;
b) $\forall x_1 \in A, \quad f(-x_1) = -f(x_1)$;
c) $\forall x_1 \in A,\ \forall y_1 \in A, \quad f(x_1 +_1 y_1) = f(x_1) +_2 f(y_1)$;

Et d'autre part,

a) $f(1_A) = 1_B$;
b) $\forall x_1 \in A^\times, \quad f(x_1) \in B^\times \ \wedge\ f(x_1^{-1}) = f(x_1)^{-1}$;
c) $\forall x_1 \in A,\ \forall y_1 \in A, \quad f(x_1 \times_1 y_1) = f(x_1) \times_2 f(y_1)$.

▷ Si tel est le cas, on dit plus précisément que f induit un isomorphisme de l'anneau $(A,+_1,\times_1)$ dans l'anneau $(B,+_2,\times_2)$ pour dire que $f : A \to B$ est une fonction inversible et que sa réciproque $f^{-1} : B \to A$ induit un homomorphisme de l'anneau $(B,+_2,\times_2)$ dans l'anneau $(A,+_1,\times_1)$.

Exemple 3.4. $(\mathbb{C},+,\times) \to (\mathbb{C},+,\times),\ z \mapsto \overline{z}$ et $\mathbb{C} \to \mathcal{M}_2(\mathbb{R}) = \mathbb{R}^{2\times 2},\ z \mapsto \begin{bmatrix} \mathrm{Re}(z) & -\mathrm{Im}(z) \\ \mathrm{Im}(z) & \mathrm{Re}(z) \end{bmatrix}$.

Proposition 35 (Homomorphisme d'anneaux).
Que soient donnés deux anneaux $(A,+_1,\times_1)$ et $(B,+_2,\times_2)$; puis une fonction $f : A \to B$.
Pour que la fonction f induise un homomorphisme de l'anneau $(A,+_1,\times_1)$ dans l'anneau $(B,+_2,\times_2)$, il est suffisant (et nécessaire) qu'à la fois :

▷ $f(1_A) = 1_B$;
▷ $\forall x_1 \in A,\ \forall y_1 \in A, \quad f(x_1 +_1 y_1) = f(x_1) +_2 f(y_1)$;
▷ $\forall x_1 \in A,\ \forall y_1 \in A, \quad f(x_1 \times_1 y_1) = f(x_1) \times_2 f(y_1)$.

Définition 35 : *Noyau d'un homomorphisme d'anneaux.*
Le noyau d'un homomorphisme d'anneaux est l'ensemble des éléments du départ dont l'image commune est le zéro de l'arrivée.

Commentaire : Ainsi, le noyau d'un homomorphisme d'anneaux est son noyau en tant qu'homomorphisme entre les groupes additifs.

3.2 Calculs dans un anneau quelconque

Proposition 36 (Absorbance).
Que soit donné un anneau $(A,+,\times)$. Ainsi, pour tout élément a de A,

$$a \times 0_A = 0_A = 0_A \times a\ .$$

Remarque. Ainsi, dans un anneau l'élément neutre de la première LCI est aussi l'élément absorbant de la seconde LCI.

Proposition 37 (Opposé d'un produit ou « règle des signes »).
Que soient donnés : un anneau $(A,+,\times)$; et deux éléments a et b de A.
Ainsi,
$$a\times(-b)=-(a\times b)=(-a)\times b\ .$$

Proposition 38 (Itérés additifs d'un produit).
Que soient donnés : un anneau $(A,+,\times)$; deux éléments a et b de A ; et un entier relatif n.
Ainsi,
$$a\times(nb)=n(a\times b)=(na)\times b\ .$$

Proposition 39 (Double distributivité générale).
Que soient donnés : un anneau $(A,+,\times)$; deux ensembles finis I et J ; et deux familles $(a_i)_{i\in I}$ et $(b_j)_{j\in J}$ d'éléments de A.
Ainsi,
$$\sum_{(i,j)\in I\times J}a_i\times b_j=\left(\sum_{i\in I}a_i\right)\times\left(\sum_{j\in J}b_j\right)\ .$$

Proposition 40 (Formule de Bernoulli).
Que soient donnés : un anneau $(A,+,\times)$; deux éléments a et b de A ; et un entier naturel n.
On suppose que
$$ab=ba\quad\text{ET}\quad n\geqslant 1\ .$$
Ainsi,
$$S\times(a-b)=a^n-b^n=(a-b)\times S\ ;$$
où $\displaystyle S=\sum_{\substack{(i,j)\in\mathbb{N}\times\mathbb{N}\\ i+j=n-1}}a^ib^j=\sum_{k=0}^{n-1}a^{n-1-k}b^k=a^{n-1}b^0+a^{n-2}b^1+\cdots+a^{n-1-k}b^k+\cdots+a^1b^{n-2}+a^0b^{n-1}.$

Exo 22. Soit $a\in A$. Montrer que s'il existe $n\in\mathbb{N}^*$ tel que $a^n=0_A$, alors 1_A-a et 1_A+a sont inversibles.

Proposition 41 (Formule du binôme de Newton).
Que soient donnés : un anneau $(A,+,\times)$; deux éléments a et b de A ; un entier naturel n.
On suppose que
$$ab=ba\ .$$
Ainsi,
$$(a+b)^n=\sum_{\substack{(i,j)\in\mathbb{N}\times\mathbb{N}\\ i+j=n}}\frac{n!}{i!j!}a^ib^j=\sum_{k=0}^{n}\binom{n}{k}a^{n-k}\times b^k=a^nb^0+a^{n-1}b^1+\cdots+a^{n-k}b^k+\cdots+a^1b^{n-1}+a^0b^n\ .$$

Remarque. $a+b=b+a$.

Exo 23. Soient $a,b\in A$. Soient $m,n\in\mathbb{N}^*$. Montrer que si $a^m=0$, $b^n=0$, et que $ab=ba$ alors $(a+b)^{m+n-1}=0$.

3.3 Anneaux commutatifs

Définition 36 : *Anneau commutatif*.
On dit qu'un anneau est commutatif pour dire que sa seconde LCI est commutative.

Exemple 3.5. L'anneau $\big(\mathcal{F}([0;20255],\mathbb{R}),+,\times\big)$ est commutatif tandis que l'anneau $(\mathcal{L}(\mathbb{R}^2,\mathbb{R}^2),+,\circ)$ des fonctions de $\mathbb{R}^2$ dans $\mathbb{R}^2$ lui-même qui respectent l'addition et la multiplication par tout nombre réel (fonctions linéaires) n'est pas commutatif comme le prouvent les deux fonctions $(x\ ,\ y)\mapsto(y\ ,\ x)$ et $(x\ ,\ y)\mapsto(x\ ,\ x+y)$.

Définition 37 : *Anneau intègre.*
On appelle anneau intègre tout anneau commutatif dans lequel tout élément non nul est simplifiable (pour la seconde LCI).

Exemple 3.6. $(\mathbb{Z}, +, \times)$ est intègre tandis que $(\mathbb{Z}^2, +, \times)$ est commutatif non intègre.

Définition 38 : *Corps.*
On appelle corps tout anneau commutatif dans lequel tout élément non nul est inversible.

Exemples 3.7.

1. Corps de nombres usuels : $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$, $(\mathbb{C}, +, \times)$.
2. Corps de fractions rationnels usuels : $(\mathbb{K}(X), +, \times)$; où $\mathbb{K} \in \{\mathbb{Q}, \mathbb{R}, \mathbb{C}\}$.

Commentaire : (2ème année) un usage capital de la structure d'anneau intègre est qu'on peut regarder un tel anneau comme une partie d'un corps, à l'instar de ce qu'on fait quand on regarde $\mathbb{Z}$ comme une partie de $\mathbb{Q}$ et de ce que nous qu'on fait en première année quand on regarde les polynômes formels à coefficients dans un certain corps comme une partie des fractions rationnelles à coefficients dans le même corps.

Définition 39 : *Sous-corps.*
Un sous-corps d'un corps est un sous-anneau qui est stable par passage à l'inverse pour tout nombre non nul.

Proposition 42 (Caractérisation des sous-corps).
Soient un corps et une partie de son ensemble sous-jacent. Pour que la partie soit un sous-corps, il est nécessaire et suffisant qu'elle possède au moins un élément non nul, qu'elle soit stable par soustraction et pas division.

Remarque. Un sous-corps est une partie qui est un sous-groupe additif et tandis que sa différence au singleton nul est un sous-groupe multiplicatif.

Exemples 3.8.

1. $\{r + s\sqrt{2} : \ (r, s) \in \mathbb{Q} \times \mathbb{Q}\}$ est un sous-corps de $(\mathbb{R}, +, \times)$.
2. $\{r + is : \ (r, s) \in \mathbb{Q} \times \mathbb{Q}\}$ est un sous-corps de $(\mathbb{C}, +, \times)$.

Exo 24. Montrer que que $\mathbb{Q}$ est le plus petit sous-corps de $(\mathbb{C}, +, \times)$.

Exo 25. Montrer que l'ensemble des points fixes d'un automorphisme d'un corps est un sous-corps. Donner un exemple d'un tel automorphisme.

Proposition 43 (Homomorphisme injectif de corps).
Tout homomorphisme de corps est injectif.

4 Lois de composition externe (LCE's) : exemples

Commentaire : Cette section pour présenter un cadre de calcul notamment en vue de la définition rigoureuse du nombre déterminant d'une application linéaire, d'un système carré d'équations linéaires ou d'une table matrice carrée. Ce nombre déterminera ultérieurement l'invesibilité et on en fera d'autres usages.

4.1 Ensemble muni d'une opération d'un groupe

4.1.1 Définitions et Exemples

Commentaire : Au fond, un nombre ne fait pleinement sens pour nous que lorsqu'il agit sur des unités. On rappelle la fonction ordinale/positionnelle du nombre comme indiquant une position (en se situant parmi les

nombres) et la fonction arithmétique/variationnelle du nombre comme indiquant une variation (en agissant sur les nombres).

Définition 40 : *Opération/action de groupe.*
On considère : un ensemble non vide X ; et un groupe $(G,\star)$ d'élément neutre e.
On appelle opération / action du groupe $(G,\star)$ sur l'ensemble X :

1. toute fonction $G\times X\to X,\ (g,x)\mapsto g\cdot x$ telle que :
$$\forall x\in X,\quad e\cdot x=x \qquad \text{ET} \qquad \forall h\in G,\ \forall g\in G,\ \forall x\in X,\quad (h\star g)\cdot x=h\cdot(g\cdot x)\ .$$

2. et toute fonction $X\times G\to X,\ (x,g)\mapsto x\cdot g$
$$\forall x\in X,\quad x=x\cdot e \qquad \text{ET} \qquad \forall x\in X,\ \forall g\in G,\ \forall h\in G,\quad (x\cdot g)\cdot h=x\cdot(g\star h)\ .$$

Dans le cas 1. on parle d'opération / d'action à gauche, et dans le cas 2. on parle d'opération / d'action à droite.

Exemples 4.1.

1. On note $\mathcal{E}$ l'ensemble des points de l'espace physique et $\overrightarrow{\mathcal{E}}$ l'ensemble des vecteurs de ce même espace physique. Pour tout point P, et pour tout vecteur $\overrightarrow{v}$, on note $P+\overrightarrow{v}$ l'image du point P par la translation de vecteur $\overrightarrow{v}$.
Ainsi, cela définit une action à droite
$$\begin{aligned}\mathcal{E}\times\overrightarrow{\mathcal{E}}&\longrightarrow\mathcal{E}\\(P,\overrightarrow{v})&\longmapsto P+\overrightarrow{v}\end{aligned}$$
du groupe additif $(\overrightarrow{\mathcal{E}},+)$ sur l'ensemble $\mathcal{E}$.

2. On garde les notations ci-avant. Pour tout vecteur $\overrightarrow{v}$ et tout réel r, on note $\overrightarrow{v}\cdot r$ le produit du vecteur $\overrightarrow{v}$ par le réel r : « $\overrightarrow{v}$ multiplié par r ».
Ainsi, cela définit une action à droite
$$\begin{aligned}\overrightarrow{\mathcal{E}}\times\mathbb{R}&\longrightarrow\overrightarrow{\mathcal{E}}\\(\overrightarrow{v},r)&\longmapsto\overrightarrow{v}.r\end{aligned}$$
du groupe multiplicatif $(\mathbb{R}^*,\times)$ sur l'ensemble $\overrightarrow{\mathcal{E}}$.

3. Etant donné un ensemble non vide X, la fonction
$$\begin{aligned}\mathcal{S}_X\times X&\longrightarrow X\\(f,x)&\longmapsto f(x)\end{aligned}$$
est une opération à gauche du groupe $(\mathcal{S}_X,\circ)$ sur l'ensemble X.

4. Etant donné un groupe $(G,\star)$, les fonctions
$$\begin{aligned}G\times G&\longrightarrow G\\(g,x)&\longmapsto g\star x\end{aligned}\qquad\text{ET}\qquad\begin{aligned}G\times G&\longrightarrow G\\(x,g)&\longmapsto x\star g\end{aligned}$$
sont une opération à gauche et une opération à gauche du groupe $(G,\star)$ sur l'ensemble G de ses opérateurs.

Commentaire : On peut voir un groupe comme un groupe d'opérateurs.

4.1.2 Permutations de variables

Proposition 44 (Opération sur les listes).
Que soient donnés : un ensemble E non vide ; et un entier naturel n supérieur à 2.
Pour toute permutation σ de $[\![1,n]\!]$, pour toute liste $(x_1,x_2,\dots,x_{n-1},x_n)$ de n éléments de E, on pose
$$\sigma\cdot(x_1,x_2,\dots,x_{n-1},x_n)=(x_{\sigma^{-1}(1)},x_{\sigma^{-1}(2)},\dots,x_{\sigma^{-1}(n-1)},x_{\sigma^{-1}(n)}).$$

On définit ainsi une opération à gauche

$$\mathcal{S}_n \times E^n \longrightarrow E^n$$
$$(\sigma\ ,\ (x_1, x_2, \ldots, x_{n-1}, x_n) \longmapsto \sigma \cdot (x_1, x_2, \ldots, x_{n-1}, x_n)$$

du groupe $(\mathcal{S}_n, \circ)$ sur l'ensemble E^n.

Commentaire : la place k envoie à la place $\sigma(k)$ et reçoit de la place $\sigma^{-1}(k)$.

▶ ***Démonstration.*** Soient : deux permutations σ_2 et σ_1 de $[\![1, n]\!]$, et une liste $(x_1, x_2, \ldots, x_{n-1}, x_n)$ de n éléments de E. Poser $(x'_1, x'_2, \ldots, x'_{n-1}, x'_n) = (x_{\sigma^{-1}(1)}, x_{\sigma^{-1}(2)}, \ldots, x_{\sigma^{-1}(n-1)}, x_{\sigma^{-1}(n)})$ ... ***QED*** ◀

Proposition 45 (Opération sur les fonctions à plusieurs variables).
Que soient données : un ensemble E non vide ; et un entier naturel n supérieur à 2.
Pour toute fonction $f : E^n \to \mathbb{C}$ à n variables dans E, pour toute permutation σ_1 de $[\![1, n]\!]$, pour toute liste $(x_1, x_2, \ldots, x_{n-1}, x_n)$ de n éléments de E, on pose

$$(f \cdot \sigma)(x_1, x_2, \ldots, x_{n-1}, x_n) = f\big(\sigma \cdot (x_1, x_2, \ldots, x_{n-1}, x_n)\big).$$

On définit ainsi une opération à droite

$$\mathcal{F}(E^n, \mathbb{C}) \times \mathcal{S}_n \longrightarrow \mathcal{F}(E^n, \mathbb{C})$$
$$(f, \sigma) \longmapsto f \cdot \sigma$$

du groupe $(\mathcal{S}_n, \circ)$ sur l'ensemble $\mathcal{F}(E^n, \mathbb{C})$.

Définition 41 : *Fonction numérique symétrique.*
On considère : un ensemble non vide E, un entier naturel n supérieur à 2, puis une fonction numérique

$$f : \begin{array}{ccc} E^n & \longrightarrow & \mathbb{C} \\ (x_1, x_2, \ldots, x_{n-1}, x_n) & \longmapsto & f(x_1, x_2, \ldots, x_{n-1}, x_n) \end{array}.$$

On dit que la fonction numérique f est symétrique pour dire que tout échange de deux variables la laisse inchangée.

Exemples 4.2. Les fonctions suivantes sont symétriques :

1. $\mathbb{Q}^2 \to \mathbb{C},\ (x_1, x_2) \mapsto x_1 + x_2$.
2. $\mathbb{Q}^3 \to \mathbb{C},\ (x_1, x_2, x_3) \mapsto x_1x_2 + x_1x_3 + x_2x_3$.
3. $\mathbb{R}^2 \times \mathbb{R}^2 \to \mathbb{C},\ \big((x_1, x_2)\ ;\ (y_1, y_2)\big) \mapsto x_1y_2 + y_1x_2$.

Proposition 46 (Symétrie et permutation de variables).
Que soient donnés : un ensemble E non vide ; un entier naturel n supérieur à 2 ; puis une fonction numérique

$$f : \begin{array}{ccc} E^n & \longrightarrow & \mathbb{C} \\ (x_1, x_2, \ldots, x_{n-1}, x_n) & \longmapsto & f(x_1, x_2, \ldots, x_{n-1}, x_n) \end{array}.$$

Ainsi, les deux propositions suivantes sont équivalentes :

1. La fonction est symétrique.
2. Toute permutation des variables la laisse inchangée.

Remarque. Ces deux propositions sont encore équivalentes aux deux suivantes :

3. Tout échange d'une variable quelconque avec la première la laisse inchangée.
4. Tout échange de deux variables consécutives la laisse inchangée.

Définition 42 : *Fonction numérique antisymétrique.*

On considère : un ensemble non vide E, un entier naturel n supérieur à 2, puis une fonction numérique

$$f : \begin{array}{ccc} E^n & \longrightarrow & \mathbb{C} \\ (x_1, x_2, \ldots, x_{n-1}, x_n) & \longmapsto & f(x_1, x_2, \ldots, x_{n-1}, x_n) \end{array} .$$

On dit que la fonction numérique f est antisymétrique pour dire que tout échange de deux variables la change en son opposée.

Exemples 4.3. Les fonctions suivantes sont antisymétriques :

1. $\mathbb{Q}^2 \to \mathbb{C},\ (x_1, x_2) \mapsto (x_2 - x_1)$.

2. $\mathbb{Q}^3 \to \mathbb{C},\ (x_1, x_2, x_3) \mapsto (x_3 - x_2)(x_3 - x_1)(x_2 - x_1)$.

3. $\mathbb{R}^2 \times \mathbb{R}^2 \to \mathbb{C},\ \big((x_1, x_2)\ ;\ (y_1, y_2)\big) \mapsto x_1y_2 - y_1x_2$.

Proposition 47 (Homomorphismes numériques du groupe symétrique).
Soit un ensemble fini X constitué d'au moins deux éléments.
Ainsi, il existe exactement deux homomorphismes de son groupe symétrique $(\mathcal{S}_X, \circ)$ dans le groupe multiplicatif $(\{-1\ ;\ +1\}, \times)$:

1. le trivial par lequel toute permutation envoie à 1 ;

2. et un par lequel toute transposition envoie à -1 :
si on le note ε, alors pour toute permutation σ de X,

$$\varepsilon(\sigma) = (-1)^{|X| - \omega(\sigma)}\ ;$$

où $|X|$ désigne le cardinal de X et $\omega(\sigma)$ le nombre d'orbites dans X suivant σ.

▶ ***Démonstration.*** (*Non exigible de tous.*)
On se donne une fonction $\varphi : \mathcal{S}_X \to \{-1\ ;\ +1\}$.

(1) ANALYSE.
On suppose que φ induit un homomorphisme de $(\mathcal{S}_X, \circ)$ dans $(\{-1\ ;\ +1\}, \times)$.
Comme X possède au moins deux éléments, soit une transposition τ de X.
Soient deux éléments distincts a et b de X tels que $\tau = \big(a \quad b\big)$.

- On vise à montrer que l'homomorphisme φ est constant sur l'ensemble des transpositions de X.
Soit une permutation ρ. On a $\rho\,\big(a \quad b\big)\,\rho^{-1} = \big(\rho(a) \quad \rho(b)\big)$.
Donc, comme que φ est un homomorphisme et que le groupe d'arrivée $(\{-1\ ;\ +1\}, \times)$ est commutatif, $\varphi\Big(\big(\rho(a) \quad \rho(b)\big)\Big) = \varphi\Big(\big(a \quad a\big)\Big)$.
Or pour toute paire $\{a', b'\}$ d'éléments de X, on peut choisir une bijection ρ de X sur X lui-même telle que $\{a', b'\} = \rho\big(\{a, b\}\big)$, en sorte que $(a'\ b') = \rho(a\ b)\rho^{-1}$.
Ainsi, pour toute transposition τ' de X, $\varphi(\tau') = \varphi(\tau)$

- On suppose que $\varphi(\tau) = 1$.
Alors, d'après ce qui précède, comme toute permutation s'écrit comme produit de transposition, φ est la fonction constante égale à 1.

- On suppose que $\varphi(\tau) = -1$.
Alors, d'après ce qui précède, pour tout entier naturel r, l'image par φ de tout produit de r transpositions est égale à $(-1)^r$.
Or pour tout entier naturel L supérieur à 2, pour tous éléments distincts $x_0, x_1, \ldots, x_{L-1}$ de X,

$$\big(x_0 \quad x_1 \quad \ldots \quad x_{L-2} \quad x_{L-1}\big) = \big(x_0 \quad x_1\big)\big(x_1 \quad x_2\big)\cdots\big(x_{L-2} \quad x_{L-1}\big)$$

donc l'image par φ de tout cycle de longueur L est égale à $(-1)^{L-1}$.

Ainsi, d'après la décomposition en produit de cycles à supports disjoints, $\varphi(\sigma) = (-1)^{|\mathrm{Supp}(\sigma)|-\tilde{\omega}(\sigma)}$. quelle que soit la permutation non triviale σ ; où $\tilde{\omega}(\sigma)$ désigne le nombre d'orbites dans $\mathrm{Supp}(\sigma)$ suivant σ.

Ainsi, pour toute permutation σ, comme les orbites suivant σ qui sont constituées d'un seul point chacune sont au nombre de $|X| - |\mathrm{Supp}(\sigma)|$,

$$\varphi(\sigma) = (-1)^{|X|-\omega(\sigma)}.$$

(2) SYNTHESE.

On suppose que φ est égale à la fonction qui à toute permutation σ de X attribut le nombre de $\{-1\ ;\ +1\}$ égal à $(-1)^{|X|-\omega(\sigma)}$.

Ainsi, $\varphi(\mathrm{id}_X) = 1$.

On montre que pour toute transposition τ, multiplier toute permutation σ par τ fait :

- ▷ augmenter le nombre d'orbites de 1 si le support de τ est inclus dans une des orbites suivant σ ;
- ▷ diminuer le nombre d'orbites de 1 si le support de τ n'est inclus dans aucune des orbites suivant σ ;

en sorte que cela fait multiplier $\varphi(\sigma)$ par -1.

Ainsi, pour tout entier naturel r, l'image par φ de tout produit de r transpositions est égale à $(-1)^r$.

Or pour tous entiers naturels r_1 et r_2,

$$(-1)^{r_1}(-1)^{r_1} = (-1)^{r_1+r_2}\ ;$$

et toute permutation s'écrit comme produit de transpositions.

Donc φ induit bien un homomorphisme de $(\mathcal{S}_X, \circ)$ dans $(\{-1\ ;\ +1\}, \times)$ qui porte de toute transposition à -1.

QED ◂

Remarque. $(\{-1\ ;\ +1\}, \times)$ est le sous-groupe multiplicatif de cardinal 2 du plan complexe $\mathbb{C}$, et c'est aussi le groupe des inversibles de l'anneau des entiers relatifs $(\mathbb{Z}, +, \times)$.

Exo 26. Soit un ensemble fini constitué d'au moins deux éléments. Que dire de l'ensemble des homomorphismes de partant de son groupe symétrique et arrivant dans le groupe multiplicatif du plan complexe ?

Définition 43 : *Signature, permutation paire.*
On considère un ensemble fini X constitué d'au moins deux éléments.

- ▷ On appelle signature sur son groupe symétrique l'unique homomorphisme de $(\mathcal{S}_X, \circ)$ dans $(\{-1\ ;\ +1\}, \times)$ qui porte de toute transposition à -1.
- ▷ On dit qu'une permutation est paire pour dire que sa signature est égale à 1.

Exo 27. Un produit d'un nombre pair de transposition peut-il être égal à un produit d'un nombre impair de transpositions ? En déduire une interprétation d'une permutation paire.

Définition 44 : *n-ième groupe alterné.*
Pour tout entier naturel n non nul, l'ensemble des permutations paires de $[\![1, n]\!]$ est noté $\mathcal{A}_n$ et le groupe $(\mathcal{A}_n, \circ)$ est appelé n-ième groupe alterné.

Exo 28. Soit un entier naturel n supérieur à 2. Soit une permutation impaire σ de $[\![1, n]\!]$. Montrer que $\sigma\mathcal{A}_n = \mathcal{A}_n\sigma$ et que la paire de parties $\{\mathcal{A}_n, \sigma\mathcal{A}_n\}$ est une partition de $\mathcal{S}_n$.

Proposition 48 (Antisymétrie et permutation de variables).
Que soient donnés : un ensemble E non vide ; un entier naturel n supérieur à 2 ; puis une fonction numérique

$$f : \begin{array}{ccc} E^n & \longrightarrow & \mathbb{C} \\ (x_1, x_2, \ldots, x_{n-1}, x_n) & \longmapsto & f(x_1, x_2, \ldots, x_{n-1}, x_n) \end{array}.$$

Ainsi, les deux propositions suivantes sont équivalentes :

1. La fonction est antisymétrique.
2. Toute permutation des variables la multiplie par la signature de cette permutation : toute permutation paire la laisse inchangée et toute permutation impaire la change en son opposée.

Remarque. Ces deux propositions sont encore équivalentes aux deux suivantes :

3. Tout échange d'une variable quelconque avec la première la change en son opposée.
4. Tout échange de deux variables consécutives la change en son opposée.

Définition 45 : *Inversion d'une permutation.*
On considère un ensemble fini X constitué d'au moins deux éléments et muni d'un ordre total, et une permutation σ de cet ensemble X.
On appelle inversion de la permutation σ toute paire de X (ensemble de deux éléments distincts de X) pour laquelle ses deux éléments sont dans l'ordre inverse de leurs images par σ.

Proposition 49 (Signature et inversions).
Soit un entier naturel n supérieur à 2.
Alors pour toute permutation σ de $[\![1,n]\!]$, la signature de σ, notée ici $\varepsilon(\sigma)$, est donnée par la formule :

$$\varepsilon(\sigma) = (-1)^{\iota(\sigma)} \ ;$$

où $\iota(\sigma)$ désigne le nombre d'inversions σ.

▶ ***Démonstration.***
On considère la fonction numérique $f : \mathbb{C}^n \to \mathbb{C}$ définie par

$$\begin{aligned} f(x_1, x_2, \dots, x_{n-1}, x_n) &= \prod_{n \geqslant j > i \geqslant 1} (x_j - x_i) \\ &= (x_n - x_{n-1}) \times \cdots \times (x_n - x_1) \\ &\quad \times (x_{n-1} - x_{n-2}) \times \cdots \times (x_{n-1} - x_1) \\ &\quad \times \cdots \\ &\quad \times (x_3 - x_1) \times (x_3 - x_2) \\ &\quad \times (x_2 - x_1). \end{aligned}$$

Pour toute paire P de $[\![1,n]\!]$, pour toute liste $(x_1, x_2, \dots, x_{n-1}, x_n)$ de n complexes, on pose

$$\delta_P(x_1, x_2, \dots, x_{n-1}, x_n) = x_{\max(P)} - x_{\min(P)}.$$

On nomme $\mathcal{P}_2(n)$ l'ensemble des paires de $[\![1,n]\!]$.
Ainsi,

$$\forall (x_1, x_2, \dots, x_{n-1}, x_n) \in \mathbb{C}^n, \qquad f(x_1, x_2, \dots, x_{n-1}, x_n) = \prod_{P \in \mathcal{P}_2(n)} \delta_P(x_1, x_2, \dots, x_{n-1}, x_n).$$

(1) On regarde l'effet de toute permutation sur f en termes d'inversions.
Soit une permutation σ de $[\![1,n]\!]$.
Soit une paire P de $[\![1,n]\!]$.
Soit une liste $(x_1, x_2, \dots, x_{n-1}, x_n)$ de n complexes.
On a :

$$\delta_P(x_{\sigma^{-1}(1)}, x_{\sigma^{-1}(2)}, \dots, x_{\sigma^{-1}(n-1)}, x_{\sigma^{-1}(n)}) = x_{\sigma^{-1}(\max(P))} - x_{\sigma^{-1}(\min(P))}.$$

Donc

$$\delta_P \cdot \sigma = \begin{cases} \delta_{\sigma^{-1}(P)} & \text{si } P \notin \mathrm{Inv}(\sigma^{-1}) \\ (-1)\delta_{\sigma^{-1}(P)} & \text{si } P \in \mathrm{Inv}(\sigma^{-1}) \end{cases}$$

où, pour toute permutation ρ, $\mathrm{Inv}(\rho)$ désigne l'ensemble de ses inversions.

Or

$$f \cdot \sigma = \prod_{P \in \mathcal{P}_2(n)} (\delta_P \cdot \sigma).$$

Donc

$$f \cdot \sigma = (-1)^{|\mathrm{Inv}(\sigma^{-1})|} \prod_{P \in \mathcal{P}_2(n)} \delta_{\sigma^{-1}(P)}.$$

D'une part la fonction $\mathcal{P}_2(n) \to \mathcal{P}_2(n),\ P \mapsto P' = \sigma^{-1}(P)$ est une bijection de réciproque $\mathcal{P}_2(n) \to \mathcal{P}_2(n),\ P' \mapsto P = \sigma(P')$.

Donc

$$f \cdot \sigma = (-1)^{|\mathrm{Inv}(\sigma^{-1})|} \prod_{P' \in \mathcal{P}_2(n)} \delta_{P'}.$$

D'autre part, étant donnés deux entiers distincts i et j de $[\![1, n]\!]$, que i et j soient dans l'autre inverse de $\sigma{-}1(i)$ et $\sigma^{-1}(j)$ équivaut à ce que $\sigma^{-1}(i)$ et $\sigma^{-1}(j)$ soient dans l'autre inverse de $\sigma\big(\sigma^{-1}(i)\big)$ et $\sigma\big(\sigma^{-1}(j)\big)$.

Ainsi, les inversions de σ^{-1} et les inversions de σ se correspondent un à un par la bijection : $\mathrm{Inv}(\sigma^{-1}) \to \mathrm{Inv}(\sigma),\ P \mapsto P' = \sigma^{-1}(P)$.

Donc

$$f \cdot \sigma = (-1)^{|\mathrm{Inv}(\sigma)|} \prod_{P' \in \mathcal{P}_2(n)} \delta_{P'}.$$

En somme,

$$\forall \sigma \in \mathcal{S}_n, \qquad f \cdot \sigma = (-1)^{\iota(\sigma)} f.$$

(2) On vérifie que f est antisymétrique en regardant l'effet de toute transposition sur f.

Pour ce faire, il est suffisant, d'après la formule ci-haut, de compter (modulo 2) les inversions de toute transposition.

Soit une transposition τ de $[\![1, n]\!]$.

On écrit

$$\tau = \begin{pmatrix} i & j \end{pmatrix}$$

où i et j sont deux entiers de $[\![1, n]\!]$ tels que $i < j$.

Soient deux entiers k et ℓ de $[\![1, n]\!]$ tels que $k < \ell$.

Si $k \notin \{i, j\}$ et $\ell \notin \{i, j\}$ alors $\tau(k) = k$ et $\tau(\ell) = \ell$; donc $\tau(k) < \tau(\ell)$.

Sinon, si $k \in \{i, j\}$ et $j < \ell$ alors $\tau(k) \in \{i, j\}$ et $\tau(\ell) = \ell$; donc $\tau(k) < \tau(\ell)$.

Sinon, si $k < i$ et $\ell \in \{i, j\}$ alors $\tau(k) = k$ et $\tau(\ell) \in \{i, j\}$; donc $\tau(k) < \tau(\ell)$.

Sinon, si $k = i$ et $\ell = j$ alors $\tau(k) = j$ et $\tau(\ell) = i$; donc $\tau(\ell) < \tau(k)$.

Sinon, si $k = i$ et $i < \ell < j$; alors $\tau(k) = j$ et $\tau(\ell) = \ell$; donc $\tau(\ell) < \tau(k)$.

Sinon, $i < k < j$ et $\ell = j$ alors $\tau(k) = k$ et $\tau(\ell) = i$; donc $\tau(\ell) < \tau(k)$.

En somme, les inversions de τ sont en nombre impair (égal à $1 + 2\,\mathrm{Card}([\![i+1, i+j-i-1]\!]) = 1 + 2(j-i-1)$).

D'où, la fonction f est antisymétrique : pour toute transposition τ, $\quad f \cdot \tau = (-1) f$.

D'où,

$$\forall \sigma \in \mathcal{S}_n, \qquad f \cdot \sigma = \varepsilon(\sigma) f.$$

(3) On conclut.

Ainsi,

$$\forall \sigma \in \mathcal{S}_n, \qquad (-1)^{\iota(\sigma)} f = \varepsilon(\sigma) f.$$

Or la fonction f prend au moins une valeur non nulle : $\quad f(1; 2; \ldots; n-1; n) \neq 0$.

QED ◂

Exo `29.` La parité du nombre d'inversions d'un permutation dépend-elle de l'ordre choisi sur son ensemble d'action ?

4.2 Espace vectoriel sur un corps

Commentaire : Cette section sera développée dans un chapitre ultérieur.

Définition 46 : *Espace vectoriel sur un corps.*
On considère un corps $(\mathrm{K}, +, \times)$.
On appelle espace vectoriel sur le corps $(\mathrm{K}, +, \times)$ tout triplet $(E, \boxplus, \cdot)$ où

1. $(E, \boxplus)$ est un groupe commutatif ;
2. $E \times \mathrm{K} \to E,\ (\overrightarrow{v}, k) \mapsto \overrightarrow{v} \cdot k$ est une LCE externe sur E telle que :
   - ***a)*** LCE $\cdot$ est compatible avec $\times$:
     - **i.** $\forall \overrightarrow{v} \in E, \quad \overrightarrow{v} = \overrightarrow{v} \cdot 1_{\mathrm{K}}$.
     - **ii.** $\forall \overrightarrow{v} \in E,\ \forall k_1 \in \mathrm{K},\ \forall k_2 \in \mathrm{K}, \quad (\overrightarrow{v} \cdot k_1) \cdot k_2 = \overrightarrow{v} \cdot (k_1 \times k_2)$.
   - ***b)*** la LCE $\cdot$ est doublement distributive (sur $+$ et $\boxplus$) :
     - **iii.** $\forall \overrightarrow{v} \in E,\ \forall k_1 \in \mathrm{K},\ \forall k_2 \in \mathrm{K}, \quad \overrightarrow{v} \cdot k_1 \boxplus \overrightarrow{v} \cdot k_2 = \overrightarrow{v} \cdot (k_1 + k_2)$.
     - **iv.** $\forall \overrightarrow{v}_1 \in E,\ \forall \overrightarrow{v}_2 \in E,\ \forall k \in \mathrm{K}, \quad \overrightarrow{v}_1 \cdot k \boxplus \overrightarrow{v}_2 \cdot k = (\overrightarrow{v}_1 \boxplus \overrightarrow{v}_2) \cdot k$.

Auquel cas,
Les éléments de K sont appelés scalaires.
Les éléments de E sont appelés vecteurs.
L'élément neutre du groupe $(E, \boxplus)$ est appelé vecteur nul.

Commentaire :
On peut voir cela comme un groupe additif muni d'une opération d'un corps : i.e. compatible avec la multiplication des nombres/scalaires et distributive à la fois par rapport à l'addition des nombres/scalaires et par rapport à l'addition des vecteurs.
On rappelle la dénomination « produit scalaire de deux vecteurs » qui désigne un scalaire obtenu par composition de deux vecteurs.

Notations. Le vecteur nul est noté $\overrightarrow{0}_E$.
A cause de la remarque ci-après, ***ON NOTE INDIFFÉREMMENT*** $\overrightarrow{v} \cdot k$ et $k \cdot \overrightarrow{v}$ quels que soient le vecteur $\overrightarrow{v}$ et le scalaire k.

Remarque. On considère un espace vectoriel $(E, \boxplus, \cdot)$ sur un corps $(\mathrm{K}, +, \times)$. Pour tout $\overrightarrow{v}$ de E et pour tout scalaire k de K, on pose

$$k * \overrightarrow{v} \overset{\text{def.}}{=} \overrightarrow{v} \cdot k.$$

Ainsi, comme les trois LCI's sont commutatives,

- **i.** $\forall \overrightarrow{v} \in E, \quad 1_{\mathrm{K}} * \overrightarrow{v} = \overrightarrow{v}$.
- **ii.** $\forall k_2 \in \mathrm{K},\ \forall k_1 \in \mathrm{K},\ \forall \overrightarrow{v} \in E, \quad (k_2 \times k_1) * \overrightarrow{v} = k_2 * (k_1 * \overrightarrow{v})$.
- **iii.** $\forall k_2 \in \mathrm{K},\ \forall k_1 \in \mathrm{K},\ \forall \overrightarrow{v} \in E, \quad (k_2 + k_1) * \overrightarrow{v} = k_2 * \overrightarrow{v} \boxplus k_1 * \overrightarrow{v}$.
- **iv.** $\forall k \in \mathrm{K},\ \forall \overrightarrow{v}_2 \in E,\ \forall \overrightarrow{v}_1 \in E, \quad k * (\overrightarrow{v}_2 \boxplus \overrightarrow{v}_1) = k * \overrightarrow{v}_2 \boxplus k * \overrightarrow{v}_1$.

C'est pourquoi on ne parle pas d'espace vectoriel à gauche ou à droite sur un corps.

Exemples 4.4.

1. L'espacs physique décrit plus haut : $(\overrightarrow{\mathcal{E}}, +, \cdot)$ est un espace vectoriel sur le corps $(\mathbb{R}, +, \times)$; où $\overrightarrow{v} \cdot r$ désigne du vecteur $\overrightarrow{v}$ par le réel r, quels qu'ils soient.
2. $(\mathbb{R}, +, \cdot)$ est un espace vectoriel sur le corps $(\mathbb{R}, +, \times)$, où $v \cdot r \overset{\text{def.}}{=} v \times r$ pour tout réel v et tout réel r.
3. Etant donné un entier naturel d supérieur à 1, on muni naturellement $\mathbb{R}^d$ d'une structure d'espace vectoriel sur $(\mathbb{R}, +, \times)$ en posant :

$$(x_1, \ldots, x_d) + (y_1, \ldots, y_d) \overset{\text{def.}}{=} (x_1 + y_1, \ldots, x_d + y_d)$$
$$(x_1, \ldots, x_d) \cdot r \overset{\text{def.}}{=} (x_1 \times r, \ldots, x_d \times r).$$

4. Etant donné un ensemble non vide X, on muni naturellement $\mathbb{R}^X$ d'une structure d'espace vectoriel sur $(\mathbb{R},+,\times)$ en posant :

$$(f+g)(x) \overset{\text{def.}}{=} f(x)+g(x)$$
$$(r\cdot f)(x) \overset{\text{def.}}{=} r\times f(x).$$

Exo 30. Donner des exemples d'espaces vectoriels sur $(\mathbb{Q},+\times)$, sur $(\mathbb{R},+,\times)$, et sur $(\mathbb{C},+\times)$.

Commentaire : Dans les définitions ci-haut, la nécessité de choisir un corps plutôt qu'un anneau commutatif quelconque n'apparaît pas. Au-delà des limites du programme de CPGE, on étend la définition d'un e.v. sur un corps, qu'on nomme autrement, pour traiter certaines classes de problèmes : en exemple, $\mathbb{Z}^2$ est naturellement muni d'une opération de $(\mathbb{Z},+,\times)$.

La proposition suivante commence à faire paraître l'utilité de considérer un corps.

Proposition 50 (Produit nul).
Que soient donnés : un corps $(\mathrm{K},+,\times)$ et un espace vectoriel $(E,\boxplus,\cdot)$ sur ce corps, un scalaire k et un vecteur $\overrightarrow{v}$. Ainsi,

$$k=0_K \ \vee \ \overrightarrow{v}=\overrightarrow{0}_E \quad \Longleftrightarrow \quad k\cdot\overrightarrow{v}=\overrightarrow{0}_E \ .$$

Proposition 51 (Opposé d'un produit, ou « règle des signes »).
Que soient donnés : un corps $(\mathrm{K},+,\times)$ et un espace vectoriel $(E,\boxplus,\cdot)$ sur ce corps, puis un scalaire k et un vecteur $\overrightarrow{v}$.
Ainsi,

$$(-k)\cdot\overrightarrow{v}=-(k\cdot\overrightarrow{v})=k\cdot(-\overrightarrow{v}).$$

Remarque. Comme pour les anneaux, on a encore une propriété analogue pour les itérés d'un produit.

Exo 31. Dans le $\mathbb{R}$-espace vectoriel $(\mathbb{R}^{\mathbb{N}},+,\cdot)$, que dire des parties suivantes ?

1. L'ensemble des suites à supports finis.

2. L'ensemble des suites stationnaires.

3. L'ensemble des suites nulles à l'infini (de limites nulles).

4. L'ensemble des suites bornées.

5. L'ensemble des suites convergentes.

6. L'ensemble des suites négligeables devant une suite donnée.

7. L'ensemble des suites dominées par une suite donnée.

8. L'ensemble des suites arithmétiques.

9. L'ensemble des suites vérifiant une relation donnée de récurrence linéaire d'ordre 2.

4.3 Algèbre sur un corps (2ème année)

Commentaire : Cette section est en complément pour mentionner une « algèbre » en lien avec les structures « algébrique »

Définition 47 : *Algèbre sur un corps.*
On considère un corps $(\mathrm{K},+,\times)$.
On appelle algèbre sur le corps $(\mathrm{K},+,\times)$ tout quadruplet $(\mathcal{A},\boxplus,\cdot,\boxtimes)$ où

1. $(\mathcal{A},\boxplus,\boxtimes)$ est un anneau ;

2. $\mathrm{K}\times\mathcal{A}\to\mathcal{A},\ (k,f)\mapsto k\cdot f$ est une LCE sur $\mathcal{A}$ telle que :

a) la LCE $\cdot$ est compatible avec $\times$;

b) la LCE $\cdot$ est doublement distributive (sur $+$ et $\boxplus$) ;

c) la LCE $\cdot$ est compatible avec $\boxtimes$:

$$\forall k \in \mathrm{K},\ \forall f_2 \in \mathcal{A},\ \forall f_1 \in \mathcal{A},\quad (k \cdot f_2) \boxtimes f_1 = k \cdot (f_2 \boxtimes f_1) = f_2 \boxtimes (k \cdot f_1)\ .$$

On étend cette définition à celle d'une algèbre sur un anneau commutatif en substituant le corps à un anneau commutatif.

Commentaire : Au-delà des limites du programme de CPGE, on étend la définition d'une algèbre pour traiter certaines classes de problèmes.

Remarques. Dire que $(\mathcal{A}, \boxplus, \cdot, \boxtimes)$ est une algèbre sur un corps $(\mathrm{K}, +, \times)$ c'est dire que $(\mathcal{A}, \boxplus, \boxtimes)$ est un anneau, $(\mathcal{A}, \boxplus, \cdot)$ est un e.v. sur le corps $(\mathrm{K}, +, \times)$ et $\cdot$ est compatible avec $\boxtimes$.

Exemples 4.5.

1. $(\mathbb{R}, +, \cdot, \times)$ est une algèbre sur le corps $(\mathbb{R}, +, \times)$, où $v \cdot r \overset{\text{def.}}{=} v \times r$ pour tout réel v et tout réel r.

2. Étant donné un entier naturel d supérieur à 1, on muni naturellement $\mathbb{R}^d$ d'une structure d'algèbre sur $(\mathbb{R}, +, \times)$ en posant :

$$(x_1, \dots, x_d) + (y_1, \dots, y_d) \overset{\text{def.}}{=} (x_1 + y_1, \dots, x_d + y_d)$$
$$(x_1, \dots, x_d) \cdot r \overset{\text{def.}}{=} (x_1 \times r, \dots, x_d \times r)$$
$$(x_1, \dots, x_d) \times (y_1, \dots, y_d) \overset{\text{def.}}{=} (x_1 \times y_1, \dots, x_d \times y_d).$$

3. Etant donné un ensemble non vide X, on muni naturellement $\mathbb{R}^X$ d'une structure d'algèbre sur $(\mathbb{R}, +, \times)$ en posant :

$$(f + g)(x) \overset{\text{def.}}{=} f(x) + g(x)$$
$$(r \cdot f)(x) \overset{\text{def.}}{=} r \times f(x)$$
$$(f \times g)(x) \overset{\text{def.}}{=} f(x) \times g(x)$$

4. Matrices carrées à coefficients dans un corps donné : $(\mathbb{K}^{n\times n}, +, \cdot, \times)$ est une algèbre sur $(\mathbb{K}, +, \times)$, $n \in \mathbb{N}^*$ et $\mathbb{K} \in \{\mathbb{Q}, \mathbb{R}, \mathbb{C}\}$.

5. Polynômes formels/symboliques à coefficients dans un corps donné : $(\mathbb{K}[X], +, \cdot, \times)$ est une algèbre sur $(\mathbb{K}, +, \times)$, où $\mathbb{K} \in \{\mathbb{Q}, \mathbb{R}, \mathbb{C}\}$.

Exo 32. Dans la $\mathbb{R}$-algèbre $(\mathbb{R}^{\mathbb{R}}, +, \cdot, \times)$, que dire des parties suivantes ?

1. L'ensemble des fonctions polynomiales.

2. L'ensemble des fonctions bornées.

3. L'ensemble des fonctions nulles en un point a donné.

4. L'ensemble des fonctions de limite nulle en un point $a \in \overline{\mathbb{R}}$.

5. L'ensemble des fonctions continues.

6. L'ensemble des fonctions dérivables.

Remarque. Un usage capital de la structure d'algèbre pour calculer est qu'étant donnée une fonction f partant d'une algèbre $(\mathcal{A}_1, \boxplus_1, \cdot_1, \boxtimes_1)$ et arrivant dans une algèbre $(\mathcal{A}_2, \boxplus_2, \cdot_2, \boxtimes_2)$ sur un même corps $(\mathrm{K}, +, \times)$, si la fonction f porte de l'unité du départ à l'unité de l'arrivée, de l'addition à l'addition, de la multiplication par tout scalaire à la multiplication par le même scalaire, de la multiplication interne à la multiplication interne, alors pour toute suite $(k_i)_{i\in\mathbb{N}}$ à support fini de scalaires , pour tout élément a de $\mathcal{A}_1$,

$$f\big(k_0 1_{\mathcal{A}_1} \boxplus_1 k_1 a^1 \boxplus_1 k_2 a^2 \cdots\big) = k_0 1_{\mathcal{A}_2} \boxplus_2 k_1\big(f(a)\big)^1 \boxplus_2 k_2\big(f(a)\big)^2 \cdots$$

d'où un intérêt pour les polynômes formels/symboliques.

En exemple, pour toute suite $(r_i)_{i\in\mathbb{N}}$ à support fini de nombres réels, pour tout nombre complexe z,

$$\overline{r_0 1 + r_1 z^1 + r_2 z^2 \cdots} = r_0 1 + r_1 \overline{z}^1 + r_2 \overline{z}^2 \cdots$$

***

EXOS

1. *Géométrie et groupes.* On considère un plan $\mathcal{P}$.

a) Etant donné un plan $\mathcal{P}$, montrer que les similitudes de ce plan constituent un sous-groupe des transformations de ce plan.

b) Etant donnée une partie non vide d'un plan $\mathcal{P}$, montrer que les similitudes du plan qui laisse stable cette partie constituent un sous-groupe.

c) Déterminer les groupes des similitudes du carré, du rectangle, du losange, du parallélogramme, du du triangle équilatéral, triangle rectangle, du triangle isocèle.

2. $\star$ *Itéré second neutre.* Montrer qu'un groupe $(G, .)$ est commutatif si l'itéré second de tout élément est égal au neutre.

3. $\star\star\star$ *Produit économe de transposition.* Quel est le nombre minimum de transpositions dont le produit est égal à un cycle donné ?

4. *Idempotent.*

a) Soit un ensemble muni d'une l.c.i associative à élément neutre $(E, .)$. Soit $a \in E$. Montrer l'équivalence suivante :

$$\Big(\forall m \in \mathbb{N},\ \forall n \in \mathbb{N},\quad a^n = a^m\Big) \qquad \Longleftrightarrow \qquad a^2 = a.$$

b) Montrer qu'un anneau est commutatif si l'itéré second multiplicatif de tout élément est égal à l'élément lui-même.

5. $\star\star\star$ *Anneau de Bool.* Soit un ensemble non vide E. Pour toutes parties A et B de E, on note $A\Delta B$ la différence symétrique de A et B définie par

$$A\Delta B \overset{\text{def.}}{=} (A \setminus B) \cup (B \setminus A).$$

Montrer que $(\mathcal{P}(E), \Delta, \cap)$ est un anneau. (*Indications : On pourra s'aider des fonctions indicatrices*).

6. *Complexes et matrices de similitudes.* Montrer que la fonction suivante induit un homomorphisme injectif entre les anneaux usuels :

$$\begin{aligned} \rho :\ \mathbb{C} &\longrightarrow \mathcal{M}_2(\mathbb{R}) = \mathbb{R}^{2\times 2} \\ z &\longmapsto \rho(z) = \begin{bmatrix} \mathrm{Re}(z) & -\mathrm{Im}(z) \\ \mathrm{Im}(z) & \mathrm{Re}(z) \end{bmatrix}. \end{aligned}$$

7. *Quaternions de Hamilton.* L'ensemble de matrices complexes :

$$\mathbb{H} = \left\{ \begin{pmatrix} a & -\overline{b} \\ b & \overline{a} \end{pmatrix} :\ (a, b) \in \mathbb{C} \times \mathbb{C} \right\}$$

constitue, avec l'addition et la multiplication matricielle, un anneau non commutatif dont tout élément non nul est inversible.

8. $\star$ *Permutation par tranche.* Soient deux entiers naturels m et n non nuls. Calculer la signature de la permutation de $[\![1, m+n]\!]$ suivante :

$$\begin{pmatrix} 1 & \cdots & n & n+1 & \cdots & n+m \\ m+1 & \cdots & m+n & 1 & \cdots & m \end{pmatrix}.$$

9. $\star\star$ *Autre voie pour définir la signature.* Soit un entier naturel n supérieur à 2. Pour toute permutation σ de $[\![1, n]\!]$, on pose

$$\mathrm{sgn}(\sigma) = \prod_{n \geqslant j > i \geqslant 1} \frac{\sigma(j) - \sigma(i)}{j - i} = \prod_{P \in \mathcal{P}_2(n)} \frac{\sigma(\max(P)) - \sigma(\min(P))}{\max(P) - \min(P)}.$$

***a*)** Montrer que sgn est un homomorphisme de $(\mathcal{S}_n, \circ)$ dans $(\{-1\ ;\ +1\}, \times)$.

***b*)** Calculer $\mathrm{sgn}\big((1\quad 2)\big)$.

***c*)** En déduire l'image par sgn de toute transposition de $[\![1, n]\!]$.

***d*)** En déduire, pour tout ensemble X de cardinal n, un homomorphisme de $(\mathcal{S}_X, \circ)$ dans $\{-1\ ;\ +1\}$ par lequel toute transposition envoie à -1.

10. $\star$ *Sous-espace vectoriel.* Étant donnés un espace vectoriel $(E, +, \cdot)$ sur un corps $(\mathrm{K}, +, \times)$, et une partie V de E, à quelles conditions nécessaires et suffisantes sur V les lois induisent-elles sur V une structure d'espace vectoriel sur le même corps $(\mathrm{K}, +, \times)$?

SOMMAIRE