C13 - Structures algébriques usuelles

I. Lois de composition internes

Définition

Soit M un ensemble quelconque.
Une L.C.I. "$\top$" sur M est une application

$$\top : \begin{cases} M \times M \to M \\ (x, y) \mapsto x \top y \end{cases}$$

Remarque

Le couple $(M, \top)$ est appelé un magma

Exemple

$+$ sur $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, 2\mathbb{N}, 42\mathbb{Z}$
$\times$ sur $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{U}, \mathbb{U}_n$
$\circ$ sur $\mathbb{R}^{\mathbb{R}}$, sur $Bij(\mathbb{R}, \mathbb{R})$, $Inj(\mathbb{R}, \mathbb{R})$, $Surj(\mathbb{R}, \mathbb{R})$
$\oplus$ addition "sans retenue" sur $\mathbb{N}$

$$\begin{array}{rr} & 127 \\ + & 398 \\ \hline & 415 \end{array}$$

$\wedge$ Le produit vectoriel dans $\mathbb{R}^3$ euclidien orienté
$+$ et $\times$ sur $M_2(\mathbb{R})$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} aa' + bc' & ab' + bd' \\ ca' + dc' & cb' + dd' \end{pmatrix}$$

$\cup, \cap, \setminus, \triangle$ sue $P(E)$ (ou E un ensemble)
$\wedge, \vee$ sur $\mathbb{N}$ ou $\mathbb{Z}$

Attention : Le produit scalaire dans $\mathbb{R}^2$ ou $\mathbb{R}^3$ n'est pas une LCI.

2. Propositions des LCI

Définition

Soit $(M, \top)$ un magma
Alors la loi $\top$

- Est associative ssi $\forall x, y, z \in M, (x \top y) \top z = x \top (y \top z)$
- Est commutative ssi $\forall x, y \in M, x \top y = y \top x$
- Admet $e \in M$ pour élément neutre ssi

$$\forall x \in M, \begin{cases} x \top e = x \\ e \top x = x \end{cases}$$

Propriété

Avec ces notations, si $\top$ admet un neutre alors ce neutre est unique.

Démonstration :
Soit e, e' deux neutres pour $\top$. Alors

$$e = e \top e' = e'$$

Définition

Soit $(M, \top)$ unitaire i.e. tel que $\top$ admette un neutre e qui est alors unique.
Pour $x, y \in M$,
On dit que x admet y pour symétrique (pout $\top$) ssi

$$\begin{cases} x \top y = e \\ y \top x = e \end{cases}$$

Propriété

Si $(M, \top)$ est un magma unitaire associatif (i.e. $\top$ est associative)
Alors lorsque pour $x \in M$, si il admet un symétrique, ce symétrique est unique.

Démonstration :
Soit e le neutre de $\top$,
Soit $x \in M$, et y, y' deux symétriques de x.
$y = y \top e$ e neutre
$= y \top (x \top y')$ (y' symétrique de x)
$= (y \top x) \top y'$ (associativité)
$= e \top y'$ (y symétrique de x)
$= y'$ (e neutre)

Convention d'écriture

Dans de cadre (neutre et associativité), on peut donc parler du symétrique de $x \in M$ lorsqu'il existe et le noter avec une notation qu dépends de x

1. Lorsque la loi est notée $+$ on convient de le noter $-x$ et l'appeler l'opposé de x
2. La loi est notée $\times$ (ou ·), on convient de noter x^{-1} le symétrique de x et de l'appeler l'inverse de x.

Propriété

Si $(M, \top)$ est un magma unitaire associatif (i.e. $\top$ est associative)
Si $x, y \in M$, sont symétrisables, de symétriques x', y' alors xy est aussi symétrisables.

Démonstration :

$$(x \top y) \top (y' \top x') = x \top (y \top y') \top x' = (x \top e) \top x' = x \top x' = e$$

et

$$(y' \top x') \top (x \top y) = e$$

Notation additive

$$-(x + y) = (-y) + (-x) = (-x) + (-y)$$

car $+$ est commutative

Notation multiplicative

$$(xy)^{-1} = y^{-1}x^{-1}$$

Car $\times$ n'est pas commutative

Exemple des propriétés

$(\mathbb{N}, +)$: $A, C, N(0)$, seul 0 admet un opposé
$(\mathbb{Z}, +)$: $A, C, N(0)$, tout élément admet un opposé.
$(\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +), ()$
$(\mathbb{N}, \oplus)$: $A, C, N(0)$, tout élément admet un opposé
$(\mathbb{Z}, \times), A, C, N(1)$ Seuls -1 et 1 admettent un inverse(QQ)
$(\mathbb{Q},)$
$(\mathbb{R}^{\mathbb{R}}, \circ)$, $A, \mathrm{non}C, N(Id_{\mathbb{R}})$ (seules les bijections ont un symétrique)
Bij$(E, E) = S_E$, $(S_E, \circ)$ A, N, S non commutatif en général (non abélien)
Sur $P(E)$:
$\cap$: $A, C, N(E)$ pas beaucoup de symétriques
$\cup$: $A, C, N(\varnothing)$ pas beaucoup de symétriques
$\backslash$: $\mathrm{non}A, nonC,$ -> bof bof...
$\triangle$: $A, C, N(\varnothing)$, X admet X par symétrie (groupe abélien)

$(\mathcal{M}_2(\mathbb{R}), +)$: $A, C, N(0_{\mathcal{M}_2(\mathbb{R})}), S$
$(\mathcal{M}_2(\mathbb{R}), \times)$: $A, nonC, N(I_2)$ certaines non null admettent une inverse mais pas toutes.
$(\mathbb{N}, \wedge)$: $A, C, N(0)$, seul 0 est symétrique à lui même
$(\mathbb{Z}, \wedge)$: A, C

Distributivité :
$(\mathbb{N}, +, \times)$: $\times$ par rapport à $+$
$\mathbb{Z}$: $\times$ par rapport à $+$
$\mathbb{Q}$: $\times$ par rapport à $+$
$\mathbb{R}$: $\times$ par rapport à $+$
$\mathbb{C}$: $\times$ par rapport à $+$ mais

Exercice :
$(\mathcal{M}_2(\mathbb{R}), +, \times)$:

$(P(E), \triangle, \cap)$:

Définition

Soit $(M, \top, \perp)$ un magma
On dit que $\perp$ est distribuable par rapport a $\top$
ssi $\forall x, y, z \in M$,

$$\begin{cases} x \perp (y \top z) = (x \perp y) \top (x \perp y) \\ (x \top y) \perp z = (x \perp z) \top (y \perp z) \end{cases}$$

3. Construction de nouvelles

a. Lois induites

Définition stabilité

Soit $(M, \top)$ un magma.
Une partie $A \subset M$ est dite stable par $\top$ ssi

$$\forall x, y \in A, x \top y \in A$$

Propriété

Si A est une partie stable par M par $\top$, la loi induite $\top_A$ définie par :

$$\top_A : \begin{cases} A \times A \to A \\ (x, y) \mapsto x \top y \end{cases}$$

est bien définie et est une LCI sur A

Remarques :

- On peut dire que $(A, \top_A)$ est un sous magma de $(M, \top)$
- En général la loi induite est souvent noté $\top$: on parle de magma $(A, \top)$

b. Produit cartésien de LCI

Définition : Produit cartésien de LCI

Soient $(M_1, \top_1)$, $(M_2, \top_2)$ deux magmas.
Alors $(M_1 \times M_2, \top)$

$$\top : \begin{cases} (M_1 \times M_2) \times (M_1 \times M_2) \to M_1 \times M_2 \\ ((x_1, y_1), (y_1, y_2)) \mapsto (x_1 \top_1 y_1, x_2 \top_2 y_2) \end{cases}$$

c'est un magma appelé produit de $(M_1, \top_1)$ et $(M_2, \top_2)$ (abusivement de M_1 et M_2)
La loi $\top$ est la LCI : produit de $\top_1$ et $\top_2$

- Exemple : $(\mathbb{R}^2, +)$

Extension du produit cartésien de LCI

Loi produit d'un nombre fini de lois

- Exemple : $(\mathbb{R}^n, +)$:

$$(x_1, \ldots, x_n) + (y_1, \ldots, y_n) = (x_1 + y_1, \ldots, x_n + y_n)$$

c. Loi produit sur M^E

Définition

Soit $(M, \top)$ un magma de E un ensemble quelconque.
On définit la loi $\dot{\top}$ sur M^E par :

$$\dot{\top} : \begin{cases} M^E \times M^E \\ (f, g) \mapsto f \dot{\top} g : \begin{cases} E \to M \\ x \mapsto f(x) \top g(x) \end{cases} \end{cases}$$

Remarque

On note par abus $\top$ au lieu de $\dot{\top}$

Exemple

$$\text{Si } f, y \in \mathbb{R}^I \text{ alors } f + g : \begin{cases} I \to \mathbb{R} \\ x \mapsto f(x) + g(x) \end{cases}$$

Ainsi $(\mathbb{R}^I, +)$ et $(\mathbb{R}^I, \times)$ sont des magmas

d. Héritage des propriétés

Cas 1 :

Soit $(M, \top)$ un magma et $A \subset M$ stable par $\top$ Ainsi,

- $(M, \top)$ associatif $\Rightarrow (A, \top)$ associatif
- Si M admet un neutre $e \in A$ et $e \in A$, alors e est neutre de A
- Si $e \in A$ et $x \in A$ admet un symétrique x' dans M et $x' \in A$ alors x est symétrisable dans A

Cas 2 : Produit cartésien

Exo :

- Si $(M_1, \top_1)$ et $(M_2, \top_2)$ sont associatifs (resp. commutatifs) alors $M_1 \times M_2, \top$ l'est aussi ($\top$ loi produit)
- Si $(M_1, \top_1)$ et $(M_2, \top_2)$ admettent un neutre (resp. e_1 et e_2) alors (e_1, e_2) est neutre de $M_1 \times M_2$
- Dans le cas précédent, si de plus $x = (x_1, x_2) \in M_1 \times M_2$ vérifie que x_1 est symétrisable dans M_1 et x_2 symétrisable dans M_2 alors x est symétrisable

Cas 3 : M^E

De même pour le cas 2

II. Groupes

1. Structure de groupe

Définition

Un groupe est un magma associatif unitaire dont tout élément est symétrisable
Même ANS

Définition : Groupe Abélien

Un groupe est dit Abélien ou commutatif lorsque sa loi est commutative

- Exemple :
  $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathcal{M}_2(\mathbb{R})$ sont des groupes abélien pour la loi $+$: on parle de groupe additif et dans ce cas :
  -> Le neutre est toujours noté 0
  -> Le symétrique de x est appelé opposé et est noté $-x$
  -> Si x est un élément de ce groupe et $n \in \mathbb{Z}$ on définit $n \cdot x = nx$ par
  $0x = 0$
  $nx = x + x + \cdots + x$ si $n > 0$
  $nx = (-(-n)x)$ si $n < 0$
- Exemple :
  $\mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*, \mathbb{U}, \mathbb{U}_{\mathbb{n}}, GL_2(\mathbb{R})$ (ensemble des matrices 2×2 inversibles)
  Sont des groupes pour $\times$
  On parle de groupes "multiplicatifs" et dans ce cas :
  -> Le neutre est en général noté 1
  -> Le symétrique de x est appelé inverse et est noté x^{-1}
  -> Si x est dans le groupe et $n \in \mathbb{Z}$, on définit x^n aussi :
  Si $n = 0$, $x^n = 1$
  Si $n > 0$, x^n = $x \cdot x \cdot \cdots \cdot x$ <- n fois
  Si $n < 0$, $x^n = (x^{(-n)})^{(-1)}$

Remarque importante

La notation additive n'est utilisé que pour des groupes abéliens
La notation multiplicative peut être utilisé dans n'importe quel cadre.
C'est pourquoi on fait en général la théorie avec la notation multiplicative
On prend $(G, \cdot)$ un groupe et on note 1 son élément neutre (par défault)

Définition

Si E est un ensemble quelconque,
On note $S_E = \mathrm{Bij}(E, E)$ l'ensemble des bijections de E vers E.
On introduit le vocabulaire suivant :
Un bijection de E vers E est appelé une permutation de E

Propriété

$(S_E, \circ)$ est un groupe qu'on appelle groupe des permutations de E vers E ou un groupe symétrique de E

Démonstration :
ANS
Associative : IdE
Symétrique : Pour $\sigma \in S_E$, σ^{-1} est sa bijection réciproque

Remarque

On omet souvent le $\circ$ dans les calculs i.e. on utilise la notation multiplicative (d'ou la notation σ^{-1} pour l'inverse)

Autre Exemples

$\mathbb{Z}^n, \mathbb{R}^{\mathbb{N}}, \mathbb{R}^I$ (I, intervalle de $\mathbb{R}$)

Définition

Pour $\mathbb{K} \in \{\mathbb{R}, \mathbb{C}\}$ on note $GL_n(\mathbb{K})$ l'ensemble des matrices carré d'ordre n inversibles

Propriété (Avant première)

$GL_n(\mathbb{K}, \times)$ est un groupe

- Exercice :
  Determiner explicitement $GL_2(\mathbb{K})$ et trouver une formule pour a^{-1} si $A \in GL_2(\mathbb{K})$

Autre exemples

$(Sim^+, \circ)$ est un groupe

Définition

Pour $n \in \mathbb{N}^*$,
On définit $S_n = S_{[1;...;n]}$

Notation

$\sigma \in S_n$ est noté sous forme "matricielle" aussi

$$\begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}$$

Par exemple si $n = 4$

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}$$

est la bijection σ : $[\![1, n]\!] \to [[1, n]]$
tel que

$$\begin{cases} \sigma(1) = 4 \\ \sigma(2) = 2 \\ \sigma(3) = 1 \\ \sigma(4) = 3 \end{cases}$$

Dans cet exemple σ est appelé un 3-cycle et noté plus simplement
$(143) = (431) = (314)$

Définition

Soit $p \in [\![2, n]\!]$
Un p-cycle de S_n est une transposition c telle qu'il existe $a_1, .., a_p \in [\![1, n]\!]$
différents tq $\sigma(a_1) = a_2, \dots \sigma(a_{p-1}) = a_p$ et $\sigma(a_p) = a_1$ et pour tout
$x \notin \{a_1, \dots, a_p\}$, $\sigma(x) = x$
On note alors $c = (a_1 a_2 \dots ap)$ ($= a_2 \dots a_p a_1$ etc)

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 4 & 3 & 2 & 6 & 5 & 7 & 1 & 8 \end{pmatrix} \in S_9$$

$$S_9 = \text{Bij}([\![1, 9]\!], [\![1, 9]\!])$$

Diagramme de Venn : Excalibur 1.

σ a deux points fixes : 3 et 7
et $\sigma = (1\ 9\ 8) \circ (2\ 4) \circ (5\ 6)$
C'est un résultat général

Théorème

Toute $\sigma \in S_n$ s'écrit comme un produit commutatif de cycles à supports disjoints

Définition

Si $\sigma \in S_n$, $sup(\sigma) = \{k \in [\![1, n]\!] | \sigma(k) \neq k\}$ (support de k)

Lemme

Deux permutations à support deux à deux disjoints commutent

Définition

Un 2-cycle est appelé une transposition

Rappel

Les cycles sont de taille ≥ 2 (pas de monocycle)

Application

Avec l'exemple précédent que vaut σ^{2023}
On a

$$\sigma^{2023} = ((1\ 9\ 8) \circ (2\ 4) \circ (5\ 6))^{2023} = (1\ 9\ 8)^{2023}(2\ 4)^{2023}(5\ )^{2023}$$

Car σ (commutent ils sont a supports disjoints 2 a 2)

Si on faisait la division euclidienne de 2023 par 3
On aurait :

$$2023 = 3q + r$$

$$(1\ 9\ 8)^{2023} = (1\ 9\ 8)^{3q}(198)^r = ((1\ 9\ 8)^3)^q(1\ 9\ 8)^r = (1\ 9\ 8)^r$$

Ainsi si $k, l \in \mathbb{Z}$ tq $k \equiv l[3]$ alors

$$(1\ 9\ 8)^k = (1\ 9\ 8)^l$$

Ici

$$2023 \equiv 2+0+2+3 \equiv 1[3]$$

Donc,

$$(1\ 9\ 8)^{2023} = (198)$$

On fait la meme avec les autres

$$\sigma^{2023} = \sigma$$

Remarque

$$\sigma^{2024} = (1\ 8\ 4)$$

$$(1234)^2 = (1234)(1234) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} = (13)(24)$$

Une puissance d'un cycle n'est pas toujours un cycle

Exemple :

Soit,

$$\sigma' = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 \end{pmatrix}$$

$$\sigma\sigma' = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 4 & 3 & 2 & 6 & 5 & 7 & 1 & 8 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 \end{pmatrix}$$

$$\sigma\sigma'(1) = \sigma(\sigma'(1)) = \sigma(9) = 8$$

$$\sigma\sigma' = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 8 & 1 & 7 & 5 & 6 & 2 & 3 & 4 & 9 \end{pmatrix}$$

$$\sigma'\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 6 & 7 & 8 & 4 & 5 & 3 & 9 & 2 \end{pmatrix}$$

$$\sigma\sigma' = (184562)(37)$$

$$\sigma'\sigma = (265489)(37)$$

$$(\sigma')^{2024} = (19)^{2024}(28)^{2024}(37)^{2024}(46)^{2024} = 1$$

2. Sous-Groupes

Définition

Soir $(G, \cdot)$ un groupe
Une parte de $H \subset G$ est appelé un sous-groupe de G (en fait de $(G, \cdot)$) ssi

1. H est stable par $\cdot$
2. H munie de la loi induite par $\cdot$ est un groupe

Notation $H \underset{sg}{\subset} G$

$$\mathcal{HT} \underset{sg}{\subset} \mathrm{Sim}_{+}(\text{par la loi } \circ)$$

$\mathcal{HT}$ ensemble des réunions de l'ensemble des translations ($Id_{\mathcal{P}}$ composé)

Corollaire

1. La composé de 2 translations est une translation et les composées de 2 Homothéties est soit une Homothétie soit une translation donc, $\mathcal{HT} \cdot$ est stable par $\circ$
2. On pourrait vérifier qui la loi induite est $A \cdot$ admet $Id_{\mathcal{P}}$ comme neutre et que tout élément de $\mathcal{HT}$ est inversible.

On a vu pleins d'autres sous groupes de Sim_{+} (Le groupe des rotations qui fixent un point (en incluant $Id_{\mathcal{P}}$))

$$Sim_{+} \underset{sg}{\subset} S_{\mathcal{P}}$$

Soit X in ensemble quelconque non vide et $x \in X$ alors

$$\{\sigma \in S_X | \sigma(x) = x\} (= Fix(x)) \underset{sg}{\subset} S_X$$

Si $E \subset F$,

$$P(F) \underset{sg}{\subset} P(E)$$

pour Δ

Aussi :

$$\{u \in \mathbb{R}^{\mathbb{N}} | u \subset v\} \underset{sg}{\subset} \mathbb{R}^{\mathbb{N}}$$

Pour $+$

Lemme

Soit $(G, \cdot)$ un groupe et $H \subset G$,

$$H \underset{sg}{\subset} G \Rightarrow 1_H = 1_G$$

Démonstration :
Supposons que $H \underset{sg}{\subset} G$,
On note 1_G le neutre de G et 1_H ne neutre de H
On a dans H :

$$1_H \cdot_H 1_H = 1_H$$

On a : 1_H est le neutre de H et $1_H \in H$
Mais comme $\cdot_H$ est la loi induite sur H par $\cdot$,
alors $1_H \cdot 1_H = 1_H$ en multipliant par 1_H dans G, on obtient : s

$$1_H = 1_G$$

Caractérisation

Soit G un groupe,
Alors les trois propositions sont équivalentes,
Pour H un ensemble.

1. $$H \underset{sg}{\subset} G$$

2. $$\begin{cases} H \subset G \\ H \neq \varnothing \\ H \text{ est stable par } \cdot \\ H \text{ est stable par passage a l'inverse} \end{cases}$$

3.

$$\begin{cases} H \subset G \\ 1_G \in H \\ \forall x, y \in H, xy^{-1} \in H \end{cases}$$

Démonstration : $1 \Rightarrow 2$

Supposons que $H \underset{sg}{\subset} G$,

Alors $H \subset G$ et H est stable par $\cdot$ (par définition des sous groupes)

De plus $1_H \in H$ ($(H, \cdot)$ est un groupe)

Donc $H \neq \varnothing$

Soit $x \in H$,

En notant x' l'inverse de x dans H

On a $x \cdot_H x' = 1$ et $x' \cdot_H x = 1$

Donc $x \cdot x' = 1$ et $x' \cdot x = 1$

Donc par l'unicité de l'inverse dans G, $x' = x^{-1}$

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

Démonstration : $2 \Rightarrow 3$

Supposons que

$$\begin{cases} H \subset G \\ H \neq \varnothing \\ H \text{ est stable par } \cdot \\ H \text{ est stable par passage a l'inverse} \end{cases}$$

On a alors $H \subset G$

Comme $H \neq \varnothing$, on peut prendre $x \in H$

Comme H est stable par passage a l'inverse, $x^{-1} \in H$

Comme H est stable par produit $1_G = xx^{-1} \in H$

Soient $x, y \in H$,

Comme H est stable par passage a l'inverse $y^{-1} \in H$ Comme H est stable par produit

$$xy^{-1} \in H$$

Démonstration : $3 \Rightarrow 1$

Supposons

$$\begin{cases} H \subset G \\ 1_G \in H \\ \forall x, y \in H, xy^{-1} \in H \end{cases}$$

On a alors $H \subset G$
Soit $x \in H$,
Comme $1_G \in H$ et $x \in H$ alors $1_G \cdot x^{-1} \in H$ i.e. $x^{-1} \in H$
Soient $x, y \in H$, $y^{-1} \in H$.
Puis $x(y^{-1})^{-1} \in H$ ie $xy \in H$
Ainsi d'une part, H est stable par produit
D'autre part H est stable par passage a l'inverse donc $\cdot_{_H}$ vérifie :

- Elle admet un neutre (car $1_G \in H$ et est neutre pour $\cdot_{_H}$)
- Tout $x \in H$ admet un inverse pour $\cdot_{_H}$ car son inverse pour $\cdot_{_G}$ est dans H
- Par "héritage" de la loi $\cdot_{_G}$, la loi $\cdot_{_H}$ est associative

Ainsi,

$$(H, \cdot_{_H}) \text{ est un groupe donc : } H \underset{sg}{\subset} G$$

Remarque

Pour montrer $H \underset{sg}{\subset} G$ on se sert toujours des caractérisations

Théorème

Les sous groupes de $(\mathbb{Z}, +)$ sont les $n\mathbb{Z}$ où $n \in \mathbb{N}$

Démonstration (Importante) :
Soit $n \in \mathbb{N}$,
Mq $n\mathbb{Z} \in \underset{sg}{\subset} \mathbb{Z}$ par la caractérisation des sous groupes :

- $n\mathbb{Z} \subset \mathbb{Z}$ (car un produit d'entiers est entier)
- $0 \in n\mathbb{Z}$ ($0 \equiv 0[n]$)
- Soient $a, b \in n\mathbb{Z}$ (Comme $a \equiv 0[n]$ et $b \equiv 0[n]$, alors $a - b \equiv 0[n]$ i.e. $a - b \in n\mathbb{Z}$)

Ainsi

$$n\mathbb{Z} \underset{sg}{\subset} \mathbb{Z}$$

Réciproquement, soit $H \underset{sg}{\subset} \mathbb{Z}$ Montrons qu'il existe $n \in \mathbb{N}$ tel que $H = n\mathbb{Z}$.

On fait une disjonction de cas :

- Si $H = \{0\}$ alors $H = 0\mathbb{Z}$ avec $0 \in \mathbb{N}$
- Sinon il existe $a \in H \backslash \{0\}$ et quitte à changer a en $-a \in H$, on peut supposer $a > 0$
  Ainsi $H \cap \mathbb{N}^* \neq \varnothing$
  Toute partie non vide de $\mathbb{N}^*$ admet un plus petit élément
  $n = min(H \cap \mathbb{N}^*)$
  Montrons que $H = n\mathbb{Z}$ par double inclusion soit $a \in n\mathbb{N}$. Alors il existe $k \in \mathbb{Z}$ tel que $a = nk$
  - Si $k > 0$,
    $a = n + n + \cdots + n \in H$
    Car H est stable par addition
  - Si $k = 0$, alors $a = 0 \in H$
  - Si $k < 0$,
    $-a = n(-k) \in H$ par le cas ci dessus car $-k > 0$
    Puis H étant stable par passage à l'opposé, $a = -(-a) \in H$
    Dans tous les cas : $a \in H$
    Ainsi $n\mathbb{Z} \subset H$

Soit $a \in H$, On fait la division euclidienne de a par n ($n \neq 0$ par définition)

$$a = nq + r \text{ avec } q \in \mathbb{Z} \text{ et } r \in [\![0, n-1]\!]$$

Alors comme $n\mathbb{Z} \subset H$ (inclusion précédente) $nq \in H$ et donc
$r = a - nq \in H$
Comme $r < n$ il ne peut être strictement positif, sinon cela contredirait
$n = min(H \cap \mathbb{N}^*)$
Ainsi $r = 0$ et $a = nq \in n\mathbb{Z}$
Ainsi $H \subset n\mathbb{Z}$ et finalement $H = n\mathbb{Z}$

3. Morphismes de groupes

Définition

Soient $(G, \cdot_G)$ et $(G', \cdot_{G'})$
Deux groupes
Un morphisme (de groupes) de G vers G' est une application $\phi : G \to G'$ qui préserve la loi

$$\forall x, y \in G, \phi(x \cdot_G y) = \phi(x) \cdot_{G'} \phi(y)$$

Exemple

$$\tilde{\exp} : (\mathbb{R}, +) \to (\mathbb{R}_+^*, \times)$$

est un morphisme de groupe puisque

$$\forall x, y \in \mathbb{R}, \exp(x+y) = \exp(x)\exp(y)$$

Propriété

Soit $\phi : G \to G'$ un morphisme de groupes. Alors

1. $\phi(1_G) = 1_{G'}$
2. $\forall x \in G, \phi(x^{-1}) = (\phi(x))^{-1}$

Démonstration :

1. $\phi(1_G) = \phi(1_G 1_G) = \phi(1G)\phi(1G)$
   En multipliant par $\phi(1_G)^{-1}, 1_{G'} = \phi(1_G)$
2. Soit $x \in G$,

$$\phi(x)\phi(x^{-1}) = \phi(xx^{-1}) = \phi(1_G) = 1_{G'}$$

$$\phi(x^{-1})\phi(x) = \phi(x^{-1}x) = \phi(1_G) = 1_{G'}$$

   Donc $\phi(x^{-1})$ est l'inverse de $\phi(x)$

Propriété

Soient $\phi : G \to G'$
et $\Psi : G' \to G''$
Deux morphismes de groupes
Alors,

$$\Psi \circ \phi : G \to G''$$

est un morphisme de groupes

Demonstration : TRIVIALE

Propriété

$$\phi : (\mathbb{Z}, +) \to (G, \cdot)$$

Un morphisme,
est uniquement déterminé par $g = \phi(1)$:

$$\forall n \in \mathbb{Z}, \pi(n) = g^n$$

Démonstration :
Soit ϕ un tel morphisme et $g = \phi(1)$
Pour $n > 0$,

$$\phi(n) = \phi(1 + 1 \cdots + 1) \text{ (n fois)} = g^n$$

Pour $n = 0$,

$$\phi(0) = 1_G = g^0$$

Pour $n < 0$,

$$\phi(n) = \phi(-(-n)) = \phi(-n)^{-1} = (g^{-n})^{-1} = g^n$$

Exemple

$$\begin{cases} (GL_2(\mathbb{K}), \times) \to (\mathbb{K}^*, \times) \\ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto ad - bc \end{cases}$$

est un morphisme de groupe

$$\tilde{\tilde{\exp}} : \begin{cases} (\mathbb{C}, +) \to (\mathbb{C}^*, \circ) \\ z \mapsto e^z \end{cases}$$

$$g : \begin{cases} (\mathbb{R}, +) \to (\mathbb{U}, \circ) \\ t \mapsto e^{it} \end{cases}$$

est un morphisme

$$f : \begin{cases} (\mathbb{R}^2, +) \to (\mathbb{R}^2, +) \\ (x, y) \mapsto (2x - y, x + y) \end{cases}$$

est un morphisme

$$\phi : \begin{cases} (\mathcal{C}^0_{\mathbb{R}}([0,1]), +) \to (\mathbb{R}, +) \\ f \mapsto \int_0^1 f \end{cases}$$

est un morphisme de groupes

Remarque

Ces deux derniers exemples préservent plus que l'addition, elles préservent les combinaisons linéaires -> il y a une "superstructure" d'espace vectorielle

Propriété

Soit $\phi : G \to G'$
Le morphisme de groupes
Alors

1. Pour tout $H \underset{sg}{\subset} G$,
   On a $\phi(H) \underset{sg}{\subset} G'$
2. Pour tout $H' \underset{sg}{\subset} G'$,
   On a $\phi^{-1}(H') \underset{sg}{\subset} G$

Démonstration :

1. On utilise la caractérisation des sous groupes
   Soit $H \underset{sg}{\subset} G$ Alors

- $\phi(H) \subset G'$ (par définition de l'image directe)
- $1_{G'} = \phi(1_G) \in \phi(H)$ car $1_G \in H$
  car $H \underset{sg}{\subset} G$
- Soient $x', y' \in \phi(H)$
  Par définition de $\phi(H)$, il existe $x, y \in H$ tel que $\begin{cases} \phi(x) = x' \\ \phi(y) = y' \end{cases}$

  On a alors

$$\phi'(y')^{-1} = \phi(x)(\phi(y))^{-1} = \phi(x)\phi(y^{-1}) = \phi(xy^{-1})$$

  Car ϕ est un morphisme
  Or $x, y \in H$ et $H \underset{sg}{\subset} G$ donc $xy^{-1} \in H$
  Donc $x'(y')^{-1} \in \phi(H)$
  Ainsi $\phi(H) \underset{sg}{\subset} G'$

Définition

Avec les notations précédentes :
On note $\mathrm{Im}(\phi) = \phi(G)$ l'image de ϕ qui est un sous groupe de G' par la propriété
On note :

$$Ker\,\phi = \phi^{-1}(\{1_{G'}\})$$

Le noyau de ϕ qui est un sous groupe de G pa la propriété

Propriété

Avec ces notations
ϕ est surjective ssi $\mathrm{Im}\,\phi = G'$
et ϕ est injective ssi $Ker\,\phi = \{1_G\}$

Démonstration
Pour l'image c'est la définition de la sujectivité.
Montrons la deuxième équivalence :
Supposons que ϕ est injective Comme $\phi(1_G) = 1_{G'}$
Par injectivité

$$\phi^{-1}(\{1_{G'}\}) = \{1_G\}$$

Réciproquement, supposons que $Ker\,\phi = \{1_G\}$
Soient $x, y \in G$ tel que $\phi(x) = \phi(y)$
Alors $\phi(x)(\phi(y))^{-1} = 1_{G'}$
et comme ϕ est un morphisme

$$\phi(xy^{-1}) = 1_{G'}$$

Comme

$$Ker\,\phi = \{1_G\}, xy^{-1} = 1_G$$

Donc $x = y$
Ainsi ϕ est injective

Définition

Un morphisme de groupes es un morphisme de groupes bijectif un automorphisme d'un groupe G est un isomorphisme de G vers G (l'ensemble des automorphismes de G est noté $Aut(G)$)

Propriété

Soir ϕ : $G \to G'$ un isomorphisme de groupes
Alors ϕ^{-1} : $G' \to G$ est "automatiquement" un morphisme de groupe (Donc un isomorphisme)

Démonstration :
Pour $x', y' \in G'$,

$$\phi(x't') = \phi^{-1}(\phi(\phi^{-1}(x'))\phi(\phi^{-1}(y'))) = \phi^{-1}(x')\phi^{-1}(y')$$

Exemple

$$\tilde{\exp} : (\mathbb{R}, +) \to (\mathbb{R}_+^*, \times)$$

est un isomorphisme (l'isomorphime réciproque étant ln)

Propriété

Soit $(G,\cdot)$ un groupe
Pour $g\in G$ fixé on note

$$C_g : \begin{cases} G \to G \\ x \mapsto gxg^{-1} \end{cases}$$

(conjugaison par g)
qui est un automorphisme de G

Exercice

1. ($Aut(G),\circ$) est un groupe
2. $\{C_g; g\in G\}$ est un sous groupe de $Aut(G)$

Proposition

Soit G un groupe
Alors
$G \to S_G$
$g \mapsto \begin{cases} G \to G \\ x \mapsto gx \end{cases}$
est un isomorphisme de groupes injectif

(Tout groupe se prolonge dans un groupe symétrique i.e. "peut être vu" comme un sous groupe du groupe symétrique)

Théorème : Avant première

Pour $n\geq 2$ il existe un unique morphisme ϵ non trivial ($\neq (x\mapsto 1)$) de $(S_n,\circ)$ vers ($\{\pm 1\}, x$)
Il vérifie que pour toute transposition τ (2-cycle)

$$\epsilon(\tau) = -1$$

ϵ s'appelle la signature.

Définition

$$Ker\ \epsilon = A_n$$

est le sous groupe symétrique alterné qui est un sous groupe de S_n

$$S_4 = (1 \quad 2 \quad 3 \quad 4)$$

Théorème de Cayley

$S(G) = bij(G, G)$
Soit G un groupe alors il existe un morphisme injectif $\phi : G \to S(G)$
i.e. G est isomorphe à un sous-groupe de $S(G)$

$\mathbb{Z}/_{n\mathbb{Z}} \xrightarrow{\sim} \mathbb{U}_\mathbb{n}$ isomorphisme

Démonstration
On pose pour $g \in G$,

$$\phi(g) : \begin{cases} G \to G \\ x \mapsto gx \end{cases}$$

Soit $g \in G$,
On remarque que $\phi(g) \circ \phi(g^{-1}) = Id_G$
et $\phi(g^{-1}) \circ \phi(g) = Id_G$

Ainsi $\phi(g^{-1})$ est application réciproque de $\phi(g)$ donc ϕ est bijective
ie $\phi(g) \in S(G)$
On a construit ainsi :

$$\phi : \begin{cases} G \to S(G) \\ g \mapsto \phi(g) \end{cases}$$

Montrons que ϕ est un morphisme de groupes :
Soient $g, g' \in G$
Alors $\phi(gg') \in G^G$
Et par composition $\phi(g) \circ \phi(g') \in G^G$
Pour montrer que ces applications sont égales il suffit de montrer qu'elles donnent la même image pour chaque $x \in G$:

$$(\phi(gg'))(x) = (gg')x = (\phi(g))(\phi(g'))(x) = (\phi(g) \circ \phi(g'))(x)$$

Ainsi :

$$\phi(gg') = \phi(g) \circ \phi(g')$$

Donc ϕ est un morphisme de groupes

Pour montrer que ϕ est injectif, on calcule son noyau

Remarquons qu'on a toujours $1_G \in Ker\ \phi$
(puisque $\phi(1_G) = Id_G$ et plus généralement l'image d'un neutre par un morphisme est le neutre du groupe d'arrivée)

En pratique pour montrer l'injectivité
ie $Ker\ \phi = \{1_G\}$ on montre seulement $Ker\ \phi \subset \{1_G\}$
ie on prend $g \in G$ tq $\phi(g) = Id_G$ et on montre que $g = 1_G$

Soit $g \in G$ tq $\phi(g) = Id_G$
ie

$$\forall x \in G, gx = x$$

On a en particulier $g1_G = 1_G$ donc $g = 1_G$
Ainsi $Ker\ \phi = \{1_G\}$
Donc ϕ est injectif

Remarque

Si G est fini $|S(G)| = |G|!$

III. Anneaux et corps

1. Anneaux

Définition Anneau

Un anneau est un magma $(A, +, \times)$ qui vérifie :

- $(A, +)$ est un groupe abélien (de neutre 0_A)
- $\times$ est associative et $\times$ admet un neutre $1_A \neq 0_A$
- $\times$ est distributive par rapport a $+$ (a gauche et a droite)

Définition Anneau commutatif

Un anneau commutatif est un anneau $(A, +, \times)$ tq $\times$ soit commutative

Remarque

On ne dit pas anneau Abélien

Exemple

$(\mathbb{N}, +, \times)$ n'est pas un anneau

$(\mathbb{Z}, +, \times)$
...
$(\mathbb{C}, +, \times)$
Sont des anneaux

$(\mathcal{M}_2(\mathbb{R}), +, \times)$ est un anneau
Démo :
$(\mathcal{M}_2(\mathbb{R}), +)$ est un groupe abélien "coefficient par coefficient" avec neutre

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

$\times$ est associative (faire le calcul)

$$I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

est neutre pour $\times$
$\times$ est distributive par rapport a $+$ (à gauche et a droite) (faire les deux calculs)

Soit E un ensemble quelconque Alors,
$(P(E), \Delta, \cap)$ est un anneau
Associativité de Δ :
On utilise

$$\mathbb{1} : \begin{cases} P(E) \to \{\bar{0}, \bar{1}\}^E \\ A \mapsto \left(\mathbb{1}_A : \begin{cases} E \to \{\bar{0}, \bar{1}\} \\ x \mapsto \begin{cases} \bar{1} \text{ si } x \in A \\ \bar{0} \text{ si } x \notin A \end{cases} \end{cases} \right) \end{cases}$$

Dont on a déjà vu qu'elle est bijective

Pour $A, B \in P(E)$

$$\mathbb{1}_{A\Delta B} = \mathbb{1}_{A\Delta B} \dot{+} \mathbb{1}_B$$

ou $\dot{+}$ est addition modulo 2

Donc pour $A, B, C \in P(E)$

$\mathbb{1}_{(A\Delta B)\Delta C} = \mathbb{1}_{A\Delta B} \dot{+} \mathbb{1}_C = (\mathbb{1}_A \dot{+} \mathbb{1}_B) \dot{+} \mathbb{1}_C = \mathbb{1}_A \dot{+} (\mathbb{1}_B \dot{+} \mathbb{1}_C) = \mathbb{1}_A \dot{+} \mathbb{1}_{B\Delta C} =$

Comme $\mathbb{1}$ est bijective, elle est injective
Donc

$$(A\Delta B)\Delta C = A\Delta(B\Delta C)$$

Plus conceptuellement $(\mathbb{Z}/2\mathbb{Z}, \dot{+}, \dot{\times})$ est un anneau commutatif

Automatiquement avec les tables d'addition et de multiplication $(\mathbb{Z}/2\mathbb{Z})^E$
est muni d'une addition et d'une multiplication
(déjà vu, $f + g : x \mapsto f(x) \dot{+} g(x)$).
On voit forcément que $((\mathbb{Z}/2\mathbb{Z})^E, \dot{+}, \dot{\times})$ est un anneau commutatif

Par ailleurs on a une bijection
$\mathbb{1} : P(E) \to (\mathbb{Z}/2\mathbb{Z})^E$
Donc on peut ramener les lois sur $P(E)$ pour $A, B \in P(E)$, on pose

$$A \tilde{+} B = \mathbb{1}^{-1}(\mathbb{1}_A \dot{+} \mathbb{1}_B)$$

$$A \tilde{\times} B = \mathbb{1}^{-1}(\mathbb{1}_A \dot{\times} \mathbb{1}_B)$$

et on obtiens un anneau $(P(E), \tilde{+}, \tilde{\times})$
On remarque que

$$\begin{cases} \tilde{+} = \Delta \\ \tilde{\times} = \cap \end{cases}$$

car pourtant $A, B \in P(E)$,

$$\begin{cases} \mathbb{1}_{A\tilde{+}B} = \mathbb{1}_A \dot{+} \mathbb{1}_B = \mathbb{1}_{A\Delta B} \\ \mathbb{1}_{A\tilde{\times}B} = \mathbb{1}_A \dot{\times} \mathbb{1}_B = \mathbb{1}_{A\cap B} \end{cases}$$

On dit que $(P(E), \Delta, \cap)$ et $((\mathbb{Z}/2\mathbb{Z})^E, \dot{+}, \dot{\times})$ sont des anneaux isomorphes

Propriété

Soit $(A,+,\times)$ un anneau
Alors 0_A est absorbant pour $\times \$ ie \forall x \in A, x \times O_A = O_A \times = O_A \$$

Démonstration
Soit $x \in A$,

$$O_A x = O_A x + x - x = (O_A + 1_A)x - x = 1_A x - x = x - x = O_A$$

Théorème Binôme de Newton

Soit $(A,+,\times)$ un anneau, $x, y \in A$ et $n \in \mathbb{N}$

Si $xy = yx$, alors

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

Démonstration la même que dans $\mathbb{R}, \mathbb{C}$

Formule de Bernoulli

Soit $(A,+,\times)$ un anneau, $x, y \in A$ et $n \in \mathbb{N}$,

Si $xy = yx$, alors

$$x^{n+1} - y^{n+1} = (x-y) \sum_{k=0}^{n} x^{n-k} y^k$$

Démonstration la même que dans $\mathbb{R}, \mathbb{C}$

Notation

Soit $(A,+,\times)$
On note $A^\times$ (se dit "A croix") l'ensemble des éléments de A i.e. l'ensemble des éléments x de A qui admettent un symétrique pour $\times$ ($x \in A \text{ tq } xx' = x'x = 1_A$ qui est alors unique puisque $\times$ est associative, et qu'on note x^{-1})

Propriété

Pour la loi induite par $\times$ sur $A^\times$, qu'on note encore $\times$

$$(A^\times, \times) \text{ est un groupe}$$

appelé groupe des inversibles de l'anneau A

Démonstration :

1. La loi induite est bien définie car $A^\times$ est stable par $\times$ puisqu'on sait qu'un produit d'inversibles x, y est inversible et $(xy)^{-1} = y^{-1}x^{-1}$
2. La loi induite hérite de l'associativité de $\times$ sur A
3. $1_A \in A^\times$ ($1_A 1_A = 1_A$) et est évidement neutre par la loi induite
4. Pour tout $x \in A^\times$, x est inversible dans A est l'inverse x^{-1} or x^{-1} est inversible (d'inverse x) donc $x^{-1} \in A^\times$ est donc l'inverse de x pour la loi induite. Ainsi $(A^\times, \times)$ est un groupe

Exemple

$\mathbb{Z}^\times = \{-1, 1\}$
$\mathbb{Q}^\times = \{x \in \mathbb{Q} | x \neq 0\} = \mathbb{Q}^*$
$\mathbb{R}^\times = \mathbb{R}^*$
$\mathbb{C}^\times = \mathbb{C}^*$

$(\mathcal{M}_{2(\mathbb{K})})^\times = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{M}_2(\mathbb{K}) | ad - bc \neq 0 \right\}$

Propriété

Si $ad - bc \neq 0$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

$$P(E)^\times = \{E\}$$

2. Corps

Définition

Idée : on rajoute à la définition d'un anneau $\times$ commutative et tout non nul est inversible mais c'est pas ouf.
Un corp K est un anneau commutatif tq $K^\times = K \backslash \{0\} = K^*$

Exemple

$$\mathbb{Q}, \mathbb{R}, \mathbb{C}, (\mathbb{Z}/2\mathbb{Z}, \dot{+}, \dot{\times})$$

Sont des corps
mais $\mathbb{Z}$ et $\mathcal{M}_2(\mathbb{K})$

Exercice

Est-ce que $\mathbb{Z}/4\mathbb{Z}$ est un corp
Pour quels $n \in \mathbb{N}\backslash\{0,1\}$ $\mathbb{Z}/n\mathbb{Z}$ est il un corp

3. Sous-anneaux et morphismes

Soit A un anneau

Définition

Un sous anneau de A est un sous-groupe additif de A qui contient 1_A et est stable par multiplication

Exemple

$\mathbb{Z}$ Sous anneau de $\mathbb{Q}$ de $\mathbb{R}$ de $\mathbb{C}$
$\mathbb{Q}$ sous anneau de $\mathbb{R}$

Propriété

Une partie d'un anneau est un sous anneau ssi :

- Elle contient 1
- Elle est stable par addition, passage à l'opposé et produit

Démonstration
$\Rightarrow$ trivial
$\Leftrightarrow$: Soit A un anneau et $B \subset A$
tq $1 \in B$ et B soit stable par $+$, passage à l'oposé et $\times$.
Comme $B \neq \varnothing$ et est stable par $+$ et passage a l'opposé, c'est un sous groupe additif de A.

Or il contient 1 et stable par x donc par la définition précédente c'est un sous anneau de A

Définition

ϕ : $A \to A'$ (A et A' deux anneaux)
est un morphisme d'anneaux ssi $\phi(1_A) = 1_{A'}$

$$\forall x, y \in A, \begin{cases} \phi(x+y) = \phi(x) + \phi(y) \\ \phi(xy) = \phi(x)\phi(y) \end{cases}$$

En particulier ϕ est un morphisme de groupes de $(A, +)$ vers $A', +$ donc $\phi'(0_A) = O_{A'}$

Définition

Pour ϕ un morphisme d'anneaux,

$$Im\phi = \phi(A)$$

$$Ker\phi = \phi^{-1}(\{O_{A'}\})$$

Propriété

$Im\phi$ est un sous-anneau de A'
$Ker\phi$ est un sous-groupe de A

Remarque

ϕ est en particulier un morphisme de groupes,
ϕ est surjective ssi $Im\phi = A'$
ϕ est injective ssi $Ker\phi = \{O_A\}$

Définition

Un isomorphisme d'anneaux est un morphisme d'anneaux bijectif

Propriété

L'image d'un corp par un morphisme d'anneau est un corps