Chapitre 15 : GROUPES - ANNEAUX - CORPS

I Loi de composition interne sur un ensemble

I.1 Définitions

DÉFINITION

> *Soit E un ensemble.*
>
> *Une* **loi de composition interne** *φ sur E est une application de $E \times E$ sur E.*
>
> *Une partie A de E est stable par la loi φ si :* $\forall (x, y) \in A^2$, $\varphi(x, y) \in A$

Remarque :

a) En général, *notation infixe* : $x * y$, ou $x \times y$, ou $x + y$, ou $x.y$ plutôt que $\varphi(x, y)$.

b) Attention, deux éléments de E ne commutent pas à priori : $x * y$ est en général différent de $y * x$, et on réserve le choix $+$ pour une loi commutative (quand tous les éléments commutent entre eux).

1▶

I.2 Propriétés éventuelles d'une loi de composition interne

DÉFINITION

> *Une loi de composition interne $*$ sur un ensemble E est :*
>
> *a)* **commutative** *si :* $\forall (x, y) \in E^2$, $x * y = y * x$
>
> *b)* **associative** *si :* $\forall (x, y, z) \in E^3$, $(x * y) * z = x * (y * z)$

2▶

Si la loi est associative, on simplifie les parenthèses et on pose, pour $x \in E$ et $n \in \mathbb{N}^*$:

- pour une loi notée additivement : $x + x + \ldots x = \sum\limits_{i=1}^{n} x = nx$ (avec n termes)

- pour une loi notée multiplicativement : $x \times x \times \ldots \times x = \prod\limits_{i=1}^{n} x = x^n$ (avec n facteurs)

On parle alors de « multiple » ou de « puissance », mais cela ne dépend que de la notation !

I.3 Élément neutre, élément inversible

DÉFINITION

> *Soit E un ensemble et $*$ une loi de composition interne sur E.*
>
> *Un élément e de E est un élément neutre pour $*$ si :* $\forall x \in E$, $x * e = e * x = x$

PROPOSITION

> *S'il existe un élément neutre dans $(E, *)$, alors il est unique.*
>
> *Notation additive : si on note $+$ la loi, on note en général 0_E ou 0 l'élément neutre.*
> *Notation multiplicative : si on note $\times$ ou . la loi, on note en général 1_E ou 1 l'élément neutre.*

3▶

Pratique 1 :

Dans les exemples suivants, la loi est-elle associative, commutative ? Y-a-t-il un élément neutre ?

1. $(\mathbb{R}, +)$ **2.** $(\mathbb{Q}^*, \times)$ **3.** $(\mathbb{N}, \times)$ **4.** $(\mathcal{F}(\mathbb{R}, \mathbb{R}), \circ)$ **5.** $(\mathcal{P}(E), \cap)$ **6.** $(\mathcal{P}(E), \cup)$

Proposition

Soit E un ensemble muni d'une loi de composition interne associative et d'un élément neutre.

Notation additive : pour $x \in E$, on pose $0.x = 0_E$ et on a : $\forall n \in \mathbb{N}$, $(n+1)x = nx + x$

Notation multiplicative : pour $x \in E$, on pose $x^0 = 1_E$ et on a : $\forall n \in \mathbb{N}$, $x^{n+1} = x * x^n = x^n * x$

Dans tous les cas, pour tout (m, n) dans $\mathbb{N}^2$:
- $x^{m+n} = x^m * x^n$ et $(x^n)^m = x^{nm}$
- si x et y sont deux éléments qui commutent, alors x^n et y^n commutent et $x^n * y^n = (x * y)^n$.

4▶

Définition

Soit E un ensemble muni d'une loi de composition interne $*$ et possédant un élément neutre.

Un élément x de E est dit **inversible** *s'il existe y dans E tel que $x * y = y * x = e$.*

y est alors un inverse pour x (et x pour y).

Proposition

Soit E un ensemble muni d'une loi de composition interne $*$ associative et possédant un élément neutre. On suppose que $x \in E$ admet un inverse :

a) alors cet inverse est unique,
($-x$ en notation additive, x^{-1} en notation multiplicative)

b) alors cet inverse est aussi inversible, d'inverse x (donc $-(-x) = x$ ou $(x^{-1})^{-1} = x$)

c) en posant pour tout $n \in \mathbb{Z}$, en notation multiplicative : $x^n = x^n$ si $n \geqslant 0$ et $x^n = (x^{-1})^{-n}$ si $n \leqslant 0$, on généralise les égalités vues plus haut

d) si y admet aussi un inverse, alors $x * y$ est aussi inversible et $(x * y)^{-1} = y^{-1} * x^{-1}$.

5▶

Théorème

Soit E un ensemble muni d'une loi de composition interne $*$ associative et possédant un élément neutre. Soit a un élément inversible de E.

Alors : $\forall (x, y) \in E^2$, $a * x = a * y \Longrightarrow x = y$ et : $\forall (x, y) \in E^2$, $x * a = y * a \Longrightarrow x = y$

Autrement dit, tout élément inversible est simplifiable.

6▶

Pratique 2 :

1. Quel est le symétrique de 2 dans $(\mathbb{Z}, +)$? Dans $(\mathbb{N}^*, \times)$? Dans $(\mathbb{Q}, \times)$? Dans $(\mathbb{Z}/3\mathbb{Z}, +)$? Dans $(\mathbb{Z}/5\mathbb{Z} \setminus \{0\}, \times)$? Dans $(\mathbb{Z}/4\mathbb{Z} \setminus \{0\}, \times)$?

2. Quel est le symétrique de $f : x \mapsto 2x + 1$ dans $(\mathcal{F}(\mathbb{R}, \mathbb{R}), \circ)$?
Donner les solutions de l'équation $f \circ g = h$ d'inconnue g avec $h : x \mapsto x^2$.

II Structure de groupe

II.1 Définitions

DÉFINITION

> *Soit E un ensemble et $*$ une loi de composition interne sur E.*
>
> *$(E,*)$ est un groupe si :*
>
> *1) la loi $*$ est associative*
>
> *2) il existe un élément neutre pour $*$ dans E*
>
> *3) tout élément de E admet un inverse.*
>
> *Si de plus $*$ est commutative, on dit que le groupe $(E,*)$ est commutatif, ou abélien.*

7▶

Pratique 3 :

Donner la table d'un groupe multiplicatif de deux, puis de trois éléments. Les reconnaissez-vous ?

PROPOSITION

> *Soit $(E,*)$ un groupe et $a \in E$.*
>
> *Les applications définies de E vers E par $x \mapsto a*x$ et $x \mapsto x*a$ sont des bijections, respectivement appelées translation à gauche et à droite d'élément a.*

8▶

THÉORÈME DÉFINITION :

> *Soit E un ensemble. On note $\mathcal{S}_E$ l'ensemble des bijections de E dans E.*
>
> *Alors $(\mathcal{S}_E,\circ)$ forme un groupe, appelé* **groupe des permutations de** *E ou* **groupe symétrique de** *E, dont l'élément neutre est Id_E.*

9▶

Pratique 4 :

Donner les tables des groupes $(\mathcal{S}_2,\circ)$ et $(\mathcal{S}_3,\circ)$.

II.2 Sous-groupe

DÉFINITION

> *Soit $(E,*)$ un groupe.*
>
> *Un sous-groupe de $(E,*)$ est une partie H de E telle que $(H,*)$ forme un groupe.*

10▶

THÉORÈME (CARACTÉRISATION DES SOUS-GROUPES) :

> *Soit $(E,*)$ un groupe et H une partie de E.*
>
> *H est un sous-groupe de $(E,*)$ si et seulement si :*
>
> *1) e_E appartient à H (qui est donc non vide), et*
>
> *2) H est stable par $*$ et par passage à l'inverse, c'est-à-dire : $\forall(x,y)\in H^2$, $x*y^{-1}\in H$*

11▶

Pratique 5 :

1. Montrer que pour $n \in \mathbb{N}^*$, $\mathbb{U}_n$ est un sous-groupe de $(\mathbb{U}, \times)$.

2. Soit E un ensemble non vide et a un élément de E. Montrer que l'ensemble des bijections de E laissant invariant a forme un sous-groupe du groupe des permutations de E.

3. Soit $(E, *)$ un groupe. On appelle centre de ce groupe l'ensemble C des éléments de E qui commutent avec tous les éléments de E. Montrer que C forme un sous-groupe de $(E, *)$.

PROPOSITION

Soit $(E, *)$ un groupe.

1) Soit $(H_i)_{i\in I}$ une famille de sous-groupes de E. Alors $\bigcap\limits_{i\in \mathrm{i}} H_i$ est un sous-groupe de $(E, *)$.

2) En particulier, pour toute partie H de E, il existe un plus petit sous-groupe de $(E, *)$ au sens de l'inclusion qui contient H, c'est l'intersection de tous les sous-groupes de $(E, *)$ qui contiennent H. On l'appelle : **sous-groupe engendré** *par H, noté $Gr(H)$ ou $<H>$.*

12▶

La réunion de deux sous-groupes n'en est pas un en général !

II.3 Morphismes de groupes

DÉFINITION

Soit $(G_1, *)$ et $(G_2, \bullet)$ deux groupes.

Une application f de G_1 vers G_2 est un **morphisme de groupes** *si :*

$$\forall (x, y) \in G_1 \times G_1, \quad f(x * y) = f(x) \bullet f(y)$$

Si de plus f est bijectif, on dit que f est un **isomorphisme de groupes**, *et les deux groupes sont dits isomorphes.*

On appelle **endomorphisme de groupes** *un morphisme de groupes de $(G, *)$ vers lui-même.*

S'il est de plus bijectif, c'est un **automorphisme de groupes**.

Calculs dans le cadre de la définition

a) $f(e_1) = e_2$ où e_1 est le neutre de G_1, e_2 celui de G_2

b) $\forall x \in G_1$, $f(x^{-1}) = (f(x))^{-1}$

c) $\forall x \in G_1$, $\forall n \in \mathbb{Z}$, $f(x^n) = (f(x))^n$

13▶

Pratique 6 :

1. Vérifier que l'exponentielle réalise un morphisme de groupes de $(\mathbb{R}, +)$ vers $(\mathbb{R}_+^*, \times)$.
Est-ce un isomorphisme de groupes ?

2. Vérifier que $\theta \mapsto e^{i\theta}$ est un morphisme de groupes entre $(\mathbb{R}, +)$ et $(\mathbb{C}^*, \times)$.
Est-ce un isomorphisme de groupes ?

Proposition

Soit K_1 un sous-groupe du groupe $(G_1, *)$, K_2 un sous-groupe du groupe $(G_2, \bullet)$, et f un morphisme de groupe entre les deux groupes.

Alors $f(K_1)$ est un sous-groupe de $(G_2, \bullet)$ et $f^{-1}(K_2)$ un sous-groupe de $(G_1, *)$.
(Pour faire vite, l'image directe ou réciproque d'un sous-groupe par un morphisme de groupes est un sous-groupe).

En particulier, si e_2 désigne le neutre de $(G_2, \bullet)$:
$*$ $\mathrm{Ker}(f) = f^{-1}(\{e_2\}) = \{x \in G_1 \mid f(x) = e_2\}$ *est un sous-groupe de* $(G_1, *)$
$*$ $f(G_1) = \mathrm{Im}\, f$ *est un sous-groupe de* $(G_2, \bullet)$

14▶

Pratique 7 :

Identifier les noyaux et images des deux morphismes de groupes de la pratique précédente.

III Structure d'anneau

Définition

Un ensemble A muni de deux lois de composition internes $+$ et $*$ est un **anneau** *si :*

1) $(A, +)$ est un groupe commutatif

2) la loi $*$ est associative

3) la loi $*$ est distributive par rapport à la loi $+$:
$\forall (x, y, z) \in A^3$, $x * (y + z) = (x * y) + (x * z)$ *et* $(x + y) * z = (x * z) + (y * z)$
4) il existe un élément neutre pour $*$, noté 1_A (ou 1).

Si de plus $*$ est commutative, on dit que l'anneau est commutatif.

15▶

Calculs dans un anneau $(A, +, *)$ de neutre 0 pour $+$ et 1 pour $*$

a) $\forall a \in A$, $a * 0 = 0 * a = 0$ (on dit que 0 est absorbant)

b) $\forall (a, b) \in A^2$, $(-a) * b = -(a * b) = a * (-b)$ et $(-a) * (-b) = a * b$

c) Si a est inversible, $(-a)$ l'est aussi et $(-a)^{-1} = -a^{-1}$

d) Si a et b sont inversibles, alors $(a * b)^{-1} = b^{-1} * a^{-1}$

e) **Binôme de Newton** : <u>si $a * b = b * a$</u>, pour $n \in \mathbb{N}$, $(a + b)^n = \sum_{k=0}^{n} \binom{n}{k} (a^k * b^{n-k})$

f) <u>Si $a * b = b * a$</u> et pour $n \in \mathbb{N}$: $a^n - b^n = (a - b) * (\sum_{k=0}^{n-1} (a^k * b^{n-1-k}))$, et en particulier : $1 - a^n = (1 - a) * (1 + a + a^2 + \ldots + a^{n-1})$

16▶

Proposition

Soit $(A,+,*)$ un anneau. L'ensemble A^* formé des inversibles pour $*$, et muni de $*$, forme un groupe, appelé le groupe des unités de A.

17▶

⚠ Dans un anneau $(A,+,*)$, l'équation $a*b=0$ n'implique pas en général $a=0$ ou $b=0$! !

IV Structure de corps

Définition

Un corps est un anneau distinct de $\{0\}$ dont tout élément non nul est inversible.

18▶

Pratique 8 :

Montrer que $\mathbb{Q}(\mathrm{i})=\{a+\mathrm{i}b \mid (a,b)\in\mathbb{Q}^2\}$ muni de l'addition et de la multiplication usuelles forme un corps.

SAVOIR...

(1) *... parfaitement les définitions de groupe, anneau et corps*

2) *... calculer dans un anneau (puissances, calculs d'inverses, formule du binôme)*

3) *... que l'équation $a*b=0$ dans un anneau n'implique pas $a=0$ ou $b=0$*

4) *... que l'équation $a*x=b$ ne se résout simplement que lorsque a est inversible...*

THÉORÈMES et PROPOSITIONS...	**... OUTILS pour ...**
Unicité de l'élément neutre, de l'inverse, règles de calcul	*Calculs avec une loi*
Les inversibles sont simplifiables	*Résolutions d'équations*
Bijectivité des translations droites et gauches	*Descriptions des éléments, calculs*
Théorème-Définition du groupe des permutations	*Exemples de groupes*
Théorème de caractérisation des sous-groupes	*Montrer qu'un (sous-)ensemble forme un groupe*
Théorème du sous-groupe engendré	*Recherche de sous-groupes, d'éléments générateurs*
Image directe et récriproque d'un sous-groupe par une morphisme de groupes	*Noyaux, images*
Groupe des inversibles d'un anneau	*Résolution d'équations dans un anneau*