Chapitre 6

Groupes - Anneaux - Corps

6.1 Lois de compositions

6.1.1 Définitions

Une **loi de composition interne** [1] sur un ensemble E est une application

$$(*) : \begin{cases} E \times E & \to & E \\ (x,y) & \mapsto & x*y \end{cases}$$

- Remarquer que la notation habituelle " $*(x,y)$ "
  est remplacée par " $x*y$ " qui est plus commode.
- Les symboles les plus utilisés sont $*$, $\cdot$, $+$, Δ, $\perp$, $\top$, $\vee, \wedge$, etc.
- Tout symbole peut être utilisé.
  Cependant, l'usage en limite parfois l'utilisation
  (par exemple, "$+$" et "$\cdot$" seront évitées si la loi n'est pas commutative.)

Un **magma** [2] est un couple $(E,*)$, où $*$ est une **LCI** sur l'ensemble E.

Une **loi de composition externe** sur un ensemble E, à opérateurs dans un ensemble F est une application [3] $(\cdot) : \begin{cases} F \times E & \to & E \\ (\alpha,x) & \mapsto & \alpha \cdot x \end{cases}$

Nous utiliserons les sigles **LCI** *et* **LCE** *pour désigner de telles lois.*

Test 132

Les "opérations suivantes sont-elles des LCI ou des LCE :
1 : le produit scalaire sur les vecteurs du plan ?
2 : l'opération "milieu de" sur les points du plan ?
3 : l'opération "moyenne" sur les entiers ?

6.1.2 Qualités usuelles d'une LCI

$*$ et $\vee$ sont deux **LCI** sur E.

Associativité :
$*$ est une **LCI** associative ssi

$$\forall\, x,y,z \in E,\ x*(y*z) = (x*y)*z$$

On parle alors de "magma associatif".

Commutativité :
$*$ est une **LCI** commutative ssi

$$\forall\, x,y \in E,\quad x*y = y*x$$

1. Ceci correspond à la notion **d'opération** sur un ensemble
2. Vocabulaire peu utilisé qui permet d'alléger certains énoncés.
3. On peut éventuellement changer l'ordre de E et F : $E \times F \to E$.

On parle alors de "magma commutatif".

Élément neutre :
$e \in E$ est élément neutre pour la loi $*$ [4] ssi

$$\forall\, x \in E, \qquad x * e = x \qquad \textit{(neutre à droite)}$$
$$\text{et} \qquad e * x = x \qquad \textit{(neutre à gauche)}$$

On parle alors de "magma **unifère** " ou de "magma **unitaire** ".

Élément inversible : si $e \in E$ est élément neutre pour $*$, alors,

$\exists\, y \in E,\ y * x = e$ signifie que *x est inversible à gauche*
$\exists\, y \in E,\ x * y = e$ signifie que *x est inversible à droite*
$\exists\, y \in E,\ x * y = y * x = e$ signifie que *x est inversible*

L'élément inverse est généralement noté x^{-1}.

Élément régulier : [5] $a \in E$ est régulier pour la loi $*$ ssi

$$\forall\, x, y \in E, \qquad x * a = y * a \Rightarrow x = y \qquad \textit{(régulier à droite)}$$
$$\text{et} \qquad a * x = a * y \Rightarrow x = y \qquad \textit{(régulier à gauche)}$$

Élément absorbant : $a \in E$ est absorbant pour la loi $*$ ssi

$$\forall\, x \in E, \qquad x * a = a \qquad \textit{(absorbant à droite)}$$
$$\text{et} \qquad a * x = a \qquad \textit{(absorbant à gauche)}$$

Distributivité : la loi $\vee$ est distributive par rapport à $*$ ssi

$$\forall\, x, y, z \in E, \qquad x \vee (y * z) = (x \vee y) * (x \vee z) \qquad \textit{(à gauche)}$$
$$\text{et} \qquad (x * y) \vee z = (x \vee z) * (y \vee z) \qquad \textit{(à droite)}$$

Test 133 Montrer que la loi $*$ définie sur $\mathbb{R}$ par : $x * y = x + y + x\,y$ est une **LCI** commutative, associative, ayant un élément neutre et telle que tout élément différent de (-1) est inversible.

Test 134 Montre que $\vee$ définie sur $\mathcal{P}(E)$ par : $A \vee B = A \quad (E \neq \varnothing)$ est une **LCI** associative, non commutative et ne possédant pas d'élément neutre.

6.1.3 Quelques propriétés élémentaires

- S'il existe, l'élément neutre est unique
- Dans un magma associatif unifère :
  - Tout élément inversible à droite est régulier à droite (idem à gauche)

    Attention : la réciproque est fausse.
  - Si $x \in E$ admet un inverse à droite et à gauche, ces inverses sont égaux.
  - S'il existe, le symétrique est unique.
  - si x est symétrisable de symétrique x^{-1},

    alors x^{-1} est symétrisable et $\boxed{\left(x^{-1}\right)^{-1} = x}$
  - si x et y sont symétrisables,

    alors $x * y$ est symétrisable et $\boxed{(x * y)^{-1} = y^{-1} * x^{-1}}$

6.1.4 Itérés d'un élément

Notation multiplicative :
E est muni d'une **LCI** associative notée $*$ et possédant un élément neutre e.
Pour $x \in E$ et $n \in \mathbb{N}$, l'élément :

$$x^n = \underbrace{x * x * \cdots * x}_{n \text{ fois}}$$

appelé **itéré** n-ième de x est défini par récurrence :

$$x^0 = e \qquad \text{et} \qquad \forall n \in \mathbb{N} \quad x^{n+1} = x * (x^n)$$

4. Attention : s'il existe, l'élément neutre dépend de la loi **et** de l'ensemble
5. On peut dire "simplifiable".

On a de plus pour tout $(p,q) \in \mathbb{N}^2$:

$$x^{p+q} = x^p * x^q \qquad \text{et} \qquad (x^p)^q = x^{pq}$$

Si x est inversible, ces relations sont vraies pour tout $(p,q) \in \mathbb{Z}^2$.

Exemple | Dans $(E,\circ)$, f^2 désignera $f \circ f$, à ne pas confondre avec la multiplication dans $\mathbb{R}$ ou $\mathbb{C}$.

Notation additive :
Lorsque la loi est notée additivement, l'itéré n-ième d'un élément x de E est noté $n \cdot x$ ou nx au lieu de x^n pour $n \in \mathbb{N}$ (ou $n \in \mathbb{Z}$ si x est inversible).

ATTENTION : en général, $(x*y)^n \neq x^n * y^n$ sauf si $*$ est commutative.

6.1.5 Morphismes

$(E,*)$ et (F,Δ) sont deux magmas, et $f : E \to F$ une application.
f est un **homomorphisme** [6] de $(E,*)$ vers (F,Δ) ssi

□ **Homomorphisme**

$$\forall\, x,y \in E, \quad f(x*y) = f(x)\Delta f(y)$$

Un **isomorphisme** est un homomorphisme bijectif.
Un **endomorphisme** de $(E,*)$ est un homomorphisme de $(E,*)$ vers $(E,*)$.
Un **automorphisme** est un endomorphisme bijectif.

Exemples | Id est un endomorphisme pour tout magma $E,*$
ln est un homomorphisme de $(R_+^*,\times)$ vers $(\mathbb{R},+)$
exp est un homomorphisme de $(\mathbb{R},+)$ vers $(R_+^*,\times)$
La dérivation est un homomorphisme de $(\mathcal{D}(I,\mathbb{R}),+)$ vers $(\mathcal{F}(I,\mathbb{R}),+)$

Test 135 | La dérivation est-elle un morphisme pour la multiplication ?

Propriétés des morphismes
- Si $f : (E,*) \to (F,\Delta)$ et $g : (F,\Delta) \to (H,\top)$ sont deux homomorphismes, alors $g \circ f : (E,*) \to (H,\top)$ et un homomorphisme.
- Si $f : (E,*) \to (F,\Delta)$ est un isomorphismes, alors $f^{-1} : (F,\Delta) \to (E,*)$ et un isomorphisme.

(On retrouve ici le fait que Id est un endomorphisme)

Th. ▷ **Utilisation des morphismes surjectifs**

Si $f : (E,*) \to (F,\Delta)$ est un homomorphisme surjectif, alors :
- $*$ associative $\Rightarrow \Delta$ associative
- $*$ commutative $\Rightarrow \Delta$ commutative
- e neutre dans $(E,*) \Rightarrow f(e)$ neutre dans (F,Δ)
- x^{-1} symétrique de x dans E $\Rightarrow f(x^{-1})$ est le symétrique de $f(x)$ dans F

(On note abusivement $f(x^{-1}) = \big(f(x)\big)^{-1}$.)

Remarques :
- Pour la dernière propriété, la surjection est inutile.
- **Attention :** la régularité ne se transmet pas...

Test 136 | Utiliser un morphisme surjectif pour montrer que $\mathbb{R} - \{-1\}$ muni de la loi $*$ du test **??** page **??** est un groupe abélien. (on retrouvera le neutre et le symétrique.)

6. On abrège souvent en "**morphisme**".

6.2 Groupes

6.2.1 Définition

Un **groupe** est un magma associatif unifère, dans lequel
tout élément admet un symétrique.

Le groupe est **commutatif** (ou **abélien**) [7] quand $*$ est commutative.

En résumé : $(E,*)$ est un groupe ssi
- ▶ $*$ est une **LCI** dans E
- ▶ $*$ est associative
- ▶ $\exists\, e \in E,\ \forall\, x \in E, \quad x*e = e*x = x$
- ▶ $\forall\, x \in E, \quad \exists\, x^{-1} \in E, \quad x*x^{-1} = x^{-1}*x = e$

Conséquence immédiate : dans un groupe, tout élément est régulier

Exemples
$\mathbb{Z}, \mathbb{Q}, \mathbb{D}, \mathbb{R}, \mathbb{C}$ sont des groupes abéliens pour l'addition.
$\mathcal{F}(I,\mathbb{R})$, $\mathbb{R}[X]$, $\mathbb{R}_n[X]$ aussi.
L'ensemble $\mathcal{U}$ des complexes de module 1, et l'ensemble des racines n^{emes} de l'unité sont des groupes multiplicatifs.

Test 137
Important : dans un magma associatif unifère $(E,*)$, l'ensemble E^* des éléments inversibles est un groupe, vérifiez-le !.
(En fait, $\mathbb{R}^*$ désigne les éléments inversibles de $\mathbb{R}$ pour la multiplication, etc.)

6.2.2 Sous-groupe

Soit un magma $(E,*)$.
$A \subset E$ est **stable** pour $*$ ssi $\quad \forall\, x,y \quad (x,y) \in A^2 \Rightarrow x*y \in A$.

Dans ces conditions, la restriction de $*$ à A est une **LCI** .
$(A,*)$ [8] est un magma. On parle de la **loi induite** par $*$ sur A.

$A \subset E$ est un **sous-groupe** du groupe $(E,*)$ si et seulement si
$*$ induit sur A une structure de groupe.

Exemples
$\mathbb{Z} \subset \mathbb{D} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$.
Chaque ensemble est un sous-groupe du suivant (pour $+$)
$\{e\}$ est le plus petit sous-groupe de $(E,*)$ ("plus petit" pour l'inclusion)
E est le plus grand sous-groupe de $(E,*)$ ("plus grand" pour l'inclusion)

Test 138
Un sous-groupe d'un groupe abélien est-il abélien ?
Un sous-groupe d'un groupe non abélien est-il non abélien ?

Première propriété : [9] si A est un sous-groupe de E,
alors A et E ont le même élément neutre.

Th. ▷ **Caractérisation d'un sous-groupe**

$A \subset E$ est un sous-groupe de $(E,*)$ ssi $\begin{cases} A \neq \varnothing \\ A \text{ est stable pour } * \\ \forall\, x \quad x \in A \Rightarrow x^{-1} \in A \end{cases}$

Th. ▷ **Autre caractérisation d'un sous-groupe**

$A \subset E$ est un sous-groupe de $(E,*)$ ssi $\begin{cases} A \neq \varnothing \\ \forall\, (x,y) \in A^2, \quad x*y^{-1} \in A \end{cases}$

7. Niels Abel (1802-1829) mathématicien norvégien, dont les travaux ont été sous-estimés par ses pairs. Par ses conditions de vie précaires, il décèdera de tuberculose à 27 ans. Ce sont Jacobi et Galois qui mettront en avant les découvertes d'Abel.

8. Normalement, il faudrait changer de notation, par exemple utiliser $\overline{*}$, car $*$ et $\overline{*}$ n'ont pas le même ensemble de définition.

9. Vraie pour les groupes, cette propriété est est généralement fausse avec des magmas associatifs unifères.

Test 139 Montrer que $\mathcal{U}$ est un groupe en tant que sous-groupe de $\mathbb{C}^*$.

Th. ▷ **Intersection - réunion de sous-groupes**

• Toute intersection d'une famille quelconque de sous groupes de $(E,*)$ est un sous groupe de E :

$$\forall\, i \in I,\ A_i \text{ sous-groupe de } E \Rightarrow \bigcap_{i\in I} A_i \text{ sous-groupe de } E$$

• Par contre : la réunion de deux sous-groupes n'est pas un sous-groupe, **sauf** si l'un d'eux est inclus dans l'autre

Point Méthode : Il est souvent plus facile de montrer qu'un ensemble muni d'une **LCI** est un groupe en montrant qu'il est un sous-groupe d'un groupe connu.

Exemples
$(\mathbb{Q}^*,\times)$ est un sous-groupe de $(\mathbb{R}^*,\times)$, lui-même sous-groupe de $(\mathbb{C}^*,\times)$.
$(\mathbb{U}_n,\times)$ est un sous-groupe de $(\mathbb{U},\times)$

6.2.3 Groupe produit

Soient G_1 et G_2 deux groupes.
Désignons par $G_1 \times G_2$ leur produit cartésien.
On peut définir sur $G_1 \times G_2$ une loi de composition $\star$ composante par composante :

$$(x_1,x_2)\star(y_1,y_2) = (x_1y_1, x_2y_2)$$

Le produit x_1y_1 apparaissant dans le second membre étant calculé dans G_1 et le produit x_2y_2 dans G_2.

Th. ▷ **Groupe produit**

Cette loi de composition munit $G_1\times G_2$ d'une structure de groupe. Ce groupe est appelé **produit des groupes** G_1 et G_2 et noté $G_1 \times G_2$.

Si e_1 et e_2 désignent respectivement les neutres de G_1 et de G_2, le neutre de $G_1\times G_2$ est (e_1,e_2).
Le symétrique d'un élément (x_1,x_2) de $G_1\times G_2$ est l'élément (x_1^{-1},x_2^{-1}).

6.2.4 Morphisme de groupes

C'est un homomorphisme du groupe $(E,*)$ vers le groupe (F,Δ).
Nous avons donc les propriétés du morphisme de magmas,
mais il est inutile ici de supposer la surjection. [10]

Si $f:(E,*)\to(F,\Delta)$ est un morphisme de groupes, alors
- $f(e_E) = e_F$
- $\forall\, x\in E,\quad f(x^{-1}) = \big(f(x)\big)^{-1}$

Test 140
On considère la loi $\top$ définie sur $\mathbb{R}$ par $x\top y = \sqrt[3]{x^3+y^3}$.
Montrer que $(\mathbb{R},\top)$ est un groupe abélien
1 : directement
2 : en utilisant un isomorphisme

6.2.5 Image, Noyau

Rappel Soit $f:E\to F$ une application quelconque [a] :
$\forall\, A\subset E$: l'**image de A par f** est l'ensemble

$$f(A) = \big\{y\in F \mid \exists\, x\in A,\ y=f(x)\big\}$$

$\forall\, B\subset F$: l'**image réciproque de B par f** est l'ensemble

$$\overset{\vee}{f}(B) = \big\{x\in E \mid f(x)\in B\big\}$$

a. voir 2.3.2 page 32

10. Il faut savoir que les deux ensembles sont des groupes... Si ce n'est pas le cas, ne pas oublier que la surjection peut permettre de montrer que (F,Δ) est un groupe.

Soit $f : (E, *) \to (F, \Delta)$ un morphisme de groupes.
L'**image de f** est l'image par f de E

$$y \in \mathrm{Im}\,(f) \Leftrightarrow \exists\, x \in E, \quad y = f(x)$$

Le **noyau de f** est l'image réciproque par f du singleton $\{e_F\}$

$$x \in \mathrm{Ker}\,(f) \Leftrightarrow f(x) = e_F$$

Th. ▷ **Image directe et réciproque d'un sous-groupe**

Si $f : (E, *) \to (F, \Delta)$ est un morphisme de groupes, alors
- L'image d'un sous-groupe de E est un sous-groupe de F
- En particulier : $\mathrm{Im}\,(f)$ est un sous-groupe de F
- L'image réciproque d'un sous-groupe de F est un sous-groupe de E
- En particulier : $\mathrm{Ker}\,(f)$ est un sous-groupe de E

Test 141 Utiliser ce qui précède pour montrer que $\mathcal{U}$ est un groupe.

Th. ▷ **Caractérisation des morphismes injectifs ou surjectifs**

Si $f : (E, *) \to (F, \Delta)$ est un morphisme de groupes, alors
- f est injectif si et seulement si $\mathrm{Ker\,(f)} = \{e_E\}$
- f est surjectif si et seulement si $\mathrm{Im\,(f)} = \mathrm{F}$

6.3 Anneaux

6.3.1 Définition

Un groupe n'étant muni que d'une seule opération, nous allons munir l'ensemble d'une deuxième loi, en imposant des conditions pour que ces lois puissent facilement "travailler ensemble"...

$(E, +, \cdot)$ est un **anneau** si et seulement si
- ▶ $(E, +)$ est un groupe abélien
- ▶ " $\cdot$ " est une **LCI** sur E qui est :
  - ▷ associative
  - ▷ il existe dans E un élément neutre pour $\cdot$

    [appelé **élément unité**, souvent noté 1 ou 1_E]
  - ▷ distributive à droite et à gauche par rapport $+$

Ne pas oublier le mot "élément" de "élément unité" [11].

L'anneau est **commutatif** si la loi "$\cdot$" est commutative.

Exemples Munis de "$+$" et "$\cdot$", $\mathbb{Z}$, $\mathbb{D}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ sont des anneaux commutatifs, $\left(\mathcal{F}(I, \mathbb{R}), +, \cdot\right)$, $\left(\mathbb{R}[X], +, \cdot\right)$ également.

Test 142 Dire pourquoi $\left(\mathbb{R}_n[X], +, \cdot\right)$ n'a pas une structure d'anneau. Comme précédemment, $+$ et $\cdot$ représentent l'addition et la multiplication des polynômes.

Test 143 Montrer que dans un anneau $(E, +, \cdot)$ l'élément unité 1_E est unique. (On pourra en prendre deux et montrer qu'il sont égaux.)

11. Utilisé seul, le mot "unité" désigne un élément inversible pour la deuxième loi de l'anneau.

6.3.2 Règles de calculs dans un anneau

ATTENTION : **il ne faut pas généraliser toutes les règles habituelles.**

Beaucoup de ces règles semblent naturelles car ce sont les celles utilisées pour les calculs dans $\mathbb{R}$ ou $\mathbb{C}$, voire même avec les fonctions et les polynômes. Mais, certaines de ces propriétés usuelles ont une autre origine que "la structure d'anneau" et ne seront pas valable dans tous les cas...

Dans l'anneau $(E,+,\cdot)$, d'éléments neutres 0_E et 1_E :

- $\forall\, x \in E, \quad 0_E \cdot x = x \cdot 0_E = 0_E$ (0_E est absorbant pour $\cdot$)

  Attention : la réciproque est fausse (voir 6.3.3 page 88 l'intégrité)
- $\forall\, x \in E, \quad x \cdot (-1_E) = (-1_E) \cdot x = -x$
- $\forall\, x, y \in E, \quad x \cdot (-y) = (-x) \cdot y = -(x \cdot y)$ (règle des signes)
- d'où la distributivité par rapport à "-" :

$$\forall\, x, y, z \in E, \quad \begin{cases} x \cdot (y - z) = x \cdot y - x \cdot z \\ (x - y) \cdot z = x \cdot z - y \cdot z \end{cases}$$

Test 144 Un **Anneau nul** est un anneau dans lequel $(0_A = 1_A)$.
Montrer que, si A est un anneau nul, alors A est un singleton $A = \{0_A\}$.
Conclusion : dans un anneau contenant au moins deux éléments : $0_A \neq 1_A$

Utilisation du symbole $\sum$ (dans le cas d'une somme finie)

$\sum$ est une notation : $a_1 + a_2 + \cdots + a_n = \sum_{k=1}^{n} a_k$.

La définition mathématique de $\sum_{k=1}^{n} a_k$ est **récursive** [12]

$$\sum_{k=1}^{1} a_k = a_1 \quad \text{et} \quad \forall\, n \geqslant 2, \quad \sum_{k=1}^{n} a_k = \sum_{k=1}^{n-1} a_k + a_n$$

Dans un anneau, la distributivité (à droite et à gauche) se généralise à toute somme finie : $\forall\, a, a_1, a_2, \cdots, a_k \in E$,

$$a \cdot \left(\sum_{k=1}^{n} a_k\right) = \sum_{k=1}^{n} (a \cdot a_k) \quad \text{et} \quad \left(\sum_{k=1}^{n} a_k\right) \cdot a = \sum_{k=1}^{n} (a_k \cdot a)$$

Test 145 Développer $\left(\sum_{k=1}^{n} a_k\right) \cdot \left(\sum_{k=1}^{m} b_k\right)$ (Attention : il y a un petit piège !)

Th. ▷ **Formule du binôme de Newton**

Si a et b commutent dans l'anneau $(E,+,\cdot)$: $\forall\, n \in \mathbb{N}$,

$$a \cdot b = b \cdot a \;\Rightarrow\; (a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k \cdot b^{n-k}$$

Attention : ceci n'est valable que si a et b commutent.

Th. ▷ **Factorisation $x^n - y^n$**

Si x et y commutent dans l'anneau $(E,+,\cdot)$, $\forall\, n \in \mathbb{N}^*$:

$$x^n - y^n = (x - y) \cdot \left(x^{n-1} + x^{n-2} \cdot y + x^{n-3} \cdot y^2 + \cdots + y^{n-1}\right)$$

(S'adapte à $x^n + y^n$ si n est impair.)

Test 146 Écrire cette factorisation en utilisant le symbole $\sum$

12. c'est une expression qui se définit par rapport à elle même.

6.3.3 L'intégrité

Dans ce paragraphe, nous supposons l'anneau **commutatif**[13].

Diviseur de zéro : dans l'anneau commutatif $(A,+,\cdot)$, a est un diviseur de zéro ssi $\begin{cases} a \neq 0_A \\ \exists\, b \in A, \quad b \neq 0_A \text{ et } a \cdot b = 0_A \end{cases}$

Anneau intègre : anneau non nul[14], commutatif et sans diviseur de zéro.

Ainsi, dans un anneau intègre $(A,+,\cdot)$:

$$x \cdot y = 0_A \Leftrightarrow x = 0_A \text{ ou } y = 0_A$$
$$x \neq 0_A \text{ et } y \neq 0_A \Leftrightarrow x \cdot y \neq 0_A$$

Exemples $\mathbb{Z}$, $\mathbb{D}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{R}[X]$ sont des anneaux intègres.
$\mathcal{F}(\mathbb{R},\mathbb{R})$ est un anneau non intègre.

Test 147 Dans $\mathbb{R}^2$ on définit les lois $\begin{cases} (x,y)+(x',y') = (x+x', y+y') \\ (x,y)\cdot(x',y') = (x\,x', y\,y') \end{cases}$
Montrer que $(\mathbb{R}^2,+,\cdot)$ est un anneau. Est-il intègre ?

Th. ▷ **Lien entre intégrité et régularité**

Pour un élément a non nul d'un anneau, on a l'équivalence
a est régulier pour $\cdot \quad \Leftrightarrow \quad a$ n'est pas diviseur de zéro

6.3.4 Groupe des inversibles

Groupe des inversibles d'un anneau :
Soit A un anneau commutatif.
L'ensemble des éléments inversibles de A forment un groupe G multiplicatif.

Test 148 Montrer la proposition précédente

6.3.5 Sous-anneau

Sous-anneau :
Soit A un anneau.
Dire que S est un sous-anneau de A signifie que $S \subset A$ et que les lois de A confère à S la structure d'anneau.

Th. ▷ **Sous-Anneau**

S est un sous-anneau de A si et seulement si
- ▷ stable par addition,
- ▷ stable par passage au symétrique pour la loi additive,
- ▷ stable par multiplication,
- ▷ contenant le neutre pour la multiplication.

Test 149 Montrer le théorème précédent.

6.3.6 Morphisme d'anneaux

Morphisme d'anneaux :
application d'un anneau $(A,+,\cdot)$ vers un anneau $(B,\oplus,\odot)$ qui vérifie

$$\forall\, (x,y) \in A^2 \quad \begin{cases} f(x+y) = f(x) \oplus f(y) \\ f(x\cdot y) = f(x) \odot f(y) \\ f(1_A) = 1_B \end{cases}$$

13. On se limite aux anneaux commutatifs pour ne pas avoir à distinguer l'intégrité à droite et à gauche.
14. Voir le test 6.3.2 page 87

6.4 Corps

Corps : $(E,+,\cdot)$ est un corps ssi $\begin{cases} (E,+,\cdot) \text{ est un anneau} \\ 0_E \neq 1_E \quad \text{(anneau non nul)} \\ \forall\, x \in E, \quad x \neq 0_E \Rightarrow x \text{ inversible} \end{cases}$

Le corps $(E,+,\cdot)$ est un **corps commutatif** si la loi "$\cdot$" est commutative[15].

$A \subset E$ est un **sous-corps** de E ssi $\begin{cases} A \text{ est un sous-anneau de } E \\ \forall\, x \in A, x \neq 0_E \Rightarrow x^{-1} \in A \end{cases}$

Exemples
- $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ sont des corps commutatifs.
- $\mathbb{R}[X]$ n'est pas un corps, mais $\mathbb{R}(X)$ est son corps des fractions...
- $\left(\mathbb{Z}/2\mathbb{Z},+,\cdot\right)$ est un corps.

Lien avec l'intégrité : $\mathbb{K}$ corps commutatif $\Rightarrow$ $\mathbb{K}$ anneau intègre.

Attention : la réciproque est fausse.

Test 150 **Somme des termes d'une suite géométrique :**

Montrer que, dans tout corps $\mathbb{K}$: $x \neq 1_{\mathbb{K}} \Rightarrow \sum_{k=0}^{n} x^k = \dfrac{1_{\mathbb{K}} - x^{n+1}}{1_{\mathbb{K}} - x}$

(L'usage de la notation "fraction" est-il légitime ?)

Théorème admis

Le corps des fractions d'un anneau commutatif intègre :
Pour tout anneau commutatif intègre A, il existe un corps C tel que
- A est un sous-anneau de C
- tout élément de $x \in C$ se met sous la forme $x = \dfrac{a}{b}, \quad (a,b) \in A^2,\ b \neq 0_A$

C est appelé le **corps des fractions** de A.

Exemples
- $\mathbb{Q}$ est le corps des fractions de $\mathbb{Z}$.
- $\mathbb{R}(X)$ est le corps des fractions de $R[X]$

Test 151 $\mathbb{Z}$ est un sous-anneau du corps $\mathbb{R}$. $\mathbb{R}$ est-il le corps des fractions de $\mathbb{Z}$?

6.5 Application aux calculs dans $\mathbb{C}$

6.5.1 Calcul de sommes

Proposition (Sommes remarquables)
Soit $n \in \mathbb{N}^*$. Alors on a les égalités suivantes :

1. $\displaystyle\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$.
2. $\displaystyle\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$.

15. Le programme se limite au cas des corps commutatifs

3. $\displaystyle\sum_{k=1}^{n} k^3 = \frac{n^2(n+1)^2}{4}$.
4. *pour tout nombre réel q différent de 1, on a*

$$\sum_{k=0}^{n} q^k = \frac{1-q^{n+1}}{1-q}$$

Point Méthode :

1. Calculons $\displaystyle\sum_{k=1}^{10}\left(5k^2+10k+5\right)$.

$$\begin{aligned}
\sum_{k=1}^{10}\left(5k^2+10k+5\right) &= 5\sum_{k=1}^{10}k^2+10\sum_{k=1}^{10}k+\sum_{k=1}^{10}5\\
\sum_{k=1}^{10}\left(5k^2+10k+5\right) &= 5\frac{(10)\,(10+1)\,(2\times 10+1)}{6}+10\frac{10\,(10+1)}{2}+5\times 10\\
\sum_{k=1}^{10}\left(5k^2+10k+5\right) &= 1425
\end{aligned}$$

2. Soit $n\in\mathbb{N}$, calculons $\displaystyle\sum_{k=0}^{n}\left(\frac{2^k}{3^{2k+1}}\right)$.

$$\begin{aligned}
\sum_{k=0}^{n}\left(\frac{2^k}{3^{2k+1}}\right) &= \sum_{k=0}^{n}\left(\frac{2}{3^2}\right)^k\times\left(\frac{1}{3}\right)\\
\sum_{k=0}^{n}\left(\frac{2^k}{3^{2k+1}}\right) &= \left(\frac{1}{3}\right)\times\sum_{k=0}^{n}\left(\frac{2}{9}\right)^k\\
\sum_{k=0}^{n}\left(\frac{2^k}{3^{2k+1}}\right) &= \left(\frac{1}{3}\right)\times\frac{1-\left(\frac{2}{9}\right)^{n+1}}{1-\frac{2}{9}}\\
\sum_{k=0}^{n}\left(\frac{2^k}{3^{2k+1}}\right) &= \left(\frac{3}{7}\right)\times\left(1-\left(\frac{2}{9}\right)^{n+1}\right)
\end{aligned}$$

3. Soit $n\in\mathbb{N}^*$, calculons $\displaystyle\sum_{k=n}^{2n}k^3$.

$$\begin{aligned}
\sum_{k=n}^{2n}k^3 &= \sum_{k=1}^{2n}k^3-\sum_{k=1}^{n-1}k^3\\
\sum_{k=n}^{2n}k^3 &= \frac{(2n)^2((2n)+1)^2}{4}-\frac{(n-1)^2((n-1)+1)^2}{4}\\
\sum_{k=n}^{2n}k^3 &= \frac{4n^2(2n+1)^2}{4}-\frac{(n-1)^2n^2}{4}\\
\sum_{k=n}^{2n}k^3 &= n^2\left((2n+1)^2-\frac{1}{4}(n-1)^2\right)\\
\sum_{k=n}^{2n}k^3 &= n^2\left(\frac{15}{4}n^2+\frac{9}{2}n+\frac{3}{4}\right)
\end{aligned}$$

Remarque : On remarque que $\displaystyle\sum_{k=l}^{n}a_k=\sum_{j=l}^{n}a_j=\sum_{\alpha=l}^{n}a_\alpha$. "Les entiers" k, j, l sont des indices de sommation autrement dit ce sont des variables muettes que l'on peut inter-changer.

Point Méthode : Simplifions $\displaystyle\sum_{k=3}^{10}\frac{k^2-k-2}{k-2}$. Posons $j=k-2$ alors $k=j+2$.

Quand $k=3$, alors $j=1$

Quand $k = 10$ alors $j = 8$.
On obtient

$$\sum_{k=3}^{10} \frac{k^2-k-2}{k-2} = \sum_{j=1}^{8} \frac{(j+2)^2-(j+2)-2}{(j+2)-2}$$

$$\sum_{k=3}^{10} \frac{k^2-k-2}{k-2} = \sum_{j=1}^{8} \frac{j^2+3j}{j}$$

$$\sum_{k=3}^{10} \frac{k^2-k-2}{k-2} = \sum_{j=1}^{8} (j+3)$$

Point Méthode : Montrons par récurrence que $\forall n \in \mathbb{N}^*$, $\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$.

Initialisation : Montrons que cette égalité est vraie au rang $n = 1$.

Le membre de gauche de l'égalité est égal à 1 et le membre de droite est égal à $\frac{1 \times 2}{2} = 1$.
Donc l'égalité est vraie au rang 1.

Hérédité : Supposons qu'à un rang n, on a $\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$.

Montrons alors qu'au rang $n+1$, on a $\sum_{k=1}^{n+1} k = \frac{(n+1)((n+1)+1)}{2}$.

$$1 + .. + n + (n+1) = \frac{n(n+1)}{2} + (n+1) = (n+1)(\frac{n}{2}+1) = \frac{(n+1)(n+2)}{2}$$

Par conséquent $1 + 2 + .. + n + (n+1) = \frac{(n+1)((n+1)+1)}{2}$.
L'hérédité est démontrée.

Conclusion Finalement, par le principe de récurrence, $\forall n \in \mathbb{N}^*$, $1 + 2 + .. + n = \frac{n(n+1)}{2}$.

6.5.2 Sommes doubles

On appelle somme double toute somme du type

$$\sum_{i=1}^{n} \sum_{j=1}^{p} a_{i,j}$$

Attention, les bornes de la deuxième somme peuvent dépendre de l'indice de la première somme. Par exemple,

$$\sum_{i=1}^{n} \sum_{j=1}^{i} a_{i,j}$$

Mais l'inverse n'arrive JAMAIS ou alors on a fait une erreur !

Ce sont les mêmes règles de calcul que pour une somme simple. Remarquons que l'on peut mettre en facteur dans la deuxième somme toute expression qui ne dépend pas du deuxième indice.

$$\sum_{i=1}^{n} \sum_{j=1}^{p} a_i b_{i,j} = \sum_{i=1}^{n} \left(a_i \sum_{j=1}^{p} b_{i,j} \right)$$

Cette dernière remarque nous permet de factoriser une double somme lorsqu'on peut séparer les indices :

$$\sum_{i=1}^{n} \sum_{j=1}^{p} a_i b_j = \left(\sum_{i=1}^{n} a_i \right) \left(\sum_{j=1}^{p} b_j \right)$$

Test 152 Calculer $\sum_{i=0}^{n}\sum_{j=0}^{n} 2^{2i-j}$

Si les bornes ne dépendent pas des indices, on peut intervertir les signes sans se poser de questions.

Sinon, les choses sont un peu plus délicates et on visualise souvent mieux la situation au moyen d'un tableau.

Point Méthode : Interversion au moyen d'un tableau Dans le tableau ci-contre, on peut faire la somme des éléments ligne par ligne ou colonne par colonne.

i/j	1	2	3
1	$a_{1,1}$		
2	$a_{2,1}$	$a_{2,2}$	
3	$a_{3,1}$	$a_{3,2}$	$a_{3,3}$

On obtient l'égalité de sommes suivante :

$$\sum_{i=1}^{n}\sum_{j=1}^{i} a_{i,j} = \sum_{1\leq j\leq i\leq n} a_{i,j} = \sum_{j=1}^{n}\sum_{i=j}^{n} a_{i,j}$$

Test 153 Ecrire de deux manières différentes

$$\sum_{1\leq i\leq j\leq n} a_{i,j}$$

Test 154 Vérifier que

$$\sum_{k=1}^{n} k2^k = \sum_{k=1}^{n}\sum_{l=1}^{k} 2^k$$

et donner une expression simple de cette somme en intervertissant l'ordre de sommation.

Exercices

Groupes

Exercice 1

$(G, *)$ est un groupe non commutatif, et a un élément de G.

1. Montrer que $\Gamma_a = \{x \in G \mid x * a = a * x\}$ est un sous-groupe de G.
2. On appelle "centre de G", l'ensemble noté $C(G)$ des éléments qui commutent avec tout élément de G : $t \in C(G) \Leftrightarrow \forall\, x \in G, \quad t * x = x * t$.
   (a) Comment relier $C(G)$ aux ensembles Γ_a précédents ?
   (b) Montrer que $C(G)$ est un sous-groupe de G.

Exercice 2

Les ensembles (munis de lois) suivants sont-ils des groupes ?

$$(\mathbb{N}, +) \qquad (\mathbb{Z}^*, +) \qquad (\mathbb{Z}^*, \times) \qquad (\mathbb{R}^*, +)$$

Exercice 3

On définit la loi $\triangle$ sur $\mathbb{R}^2$ par $\forall (x_1, y_1), (x_2, y_2) \in \mathbb{R}^2$, $(x_1, y_1) \triangle (x_2, y_2) = \big(x_1 + x_2,\, y_1 + e^{x_1} y_2\big)$.
Montrer que $(\mathbb{R}^2, \triangle)$ est un groupe non commutatif.

Exercice 4

Soit E un ensemble fini muni d'une loi de composition interne associative (notée multiplicativement). Montrer qu'il existe $x \in E$ tel que $x^2 = x$.
(Indice : pour $x \in E$, $\left\{x^{(2^n)},\ n \in \mathbb{N}^*\right\}$ ne peut être formé d'éléments 2 à 2 distincts.)

Exercice 5

Soit $(G, \diamond)$ un groupe d'élément neutre e, tel que $\forall x \in G, \qquad x \diamond x = e$.
Montrer que G est un groupe abélien.

Exercice 6

Soit $n \in \mathbb{N}$, montrer que $(n\mathbb{Z}, +)$ est un groupe.
(On note $n\mathbb{Z}$ l'ensemble des nombres nk avec $k \in \mathbb{Z}$).

Morphismes

Exercice 7

Traduire en termes de morphismes de groupes les propriétés bien connues suivantes (dont le domaine de validité a volontairement été omis) :

1. $ln(xy) = ln(x) + ln(y)$;
2. $|zz'| = |z| \times |z'|$;
3. $\sqrt{xy} = \sqrt{x}\sqrt{y}$;
4. $e^{x+y} = e^x e^y$;

Exercice 8

Justifier que exp est un morphisme de $(\mathbb{C}, +)$ dans $(\mathbb{C}^*, \times)$.
Quel est son image ? Son noyau ?

Exercice 9

[Automorphismes intérieurs] Soit $(G, \times)$ un groupe. Pour $a \in G$, on note $\tau_a : G \to G$ défini par $\tau_a(x) = axa^{-1}$.

1. Démontrer que τ_a est un endomorphisme de G.
2. Vérifier que, pour tout couple $(a, b) \in G$, on a $\tau_a \circ \tau_b = \tau_{ab}$.
3. Montrer que τ_a est bijective et déterminer son inverse.
4. En déduire que $\Theta = \{\tau_a \text{ avec } a \in G\}$ muni du produit de composition est un groupe.

Anneaux

Exercice 10

Si $\mathbb{A}$ est un sous-anneau de $\mathbb{C}$, on note $\mathbb{A}[\sqrt{2}] = \{x \in \mathbb{C} \,|\, \exists (a, b) \in \mathbb{A}^2, x = a + b\sqrt{2}\}$.

1. Montrer que $\mathbb{Z}[\sqrt{2}]$ est un anneau intègre.
2. Soient a, b deux entiers. Montrer que $a + b\sqrt{2}$ est inversible dans l'anneau $\mathbb{Z}[\sqrt{2}]$ si et seulement si $a^2 - 2b^2 \in \{-1; 1\}$.
3. Montrer que $\mathbb{Q}[\sqrt{2}]$ est un corps.

Exercice 11

Eléments nilpotents d'un anneau

Soit A un anneau. Un élément $a \in A$ est dit nilpotent s'il existe $n \in \mathbb{N}^*$ tel que $a^n = 0_A$.

1. Un élément nilpotent peut-il être inversible ?
2. Soit a un élément nilpotent de A. Montrer que $1_A - a$ est inversible, et calculer son inverse.
3. Soient a et b deux éléments qui commutent. On suppose que a est nilpotent. Montrer que ab est nilpotent.

Exercice 12

On définit sur $\mathbb{Z}^2$ deux lois de compositions internes notées $+$ et $\star$ par :

$$(a, b) + (c, d) = (a + c, b + d) \text{ et } (a, b) \star (c, d) = (ac, ad + bc)$$

a) Montrer que $(\mathbb{Z}^2, +, \star)$ est un anneau commutatif.
b) Montrer que $A = \{(a, 0)/a \in \mathbb{Z}\}$ est un sous-anneau de $(\mathbb{Z}^2, +, \star)$.

Sommes et Produits

Exercice 13

Ecrire sans le symbole $\sum$ les expressions $\displaystyle\sum_{k=1}^{5} k^2$ et $\displaystyle\sum_{j=3}^{8} \frac{j}{3^j}$.

Ecrire les sommes suivantes avec le symbole $\sum$

1. $2^5 + 3^5 + 4^5 + .. + n^5$ avec $n \in \mathbb{N}$, $n \geq 2$.
2. $\dfrac{a^2}{2} + \dfrac{a^4}{4} + \dfrac{a^6}{6} + ... + \dfrac{a^{2n}}{2n}$ avec $a \in \mathbb{R}$.

Exercice 14

Soit $n \in \mathbb{N}^*$, calculer les sommes suivantes :

1. $A_n = \displaystyle\sum_{k=0}^{n} (5k + 2)$
2. $B_n = \displaystyle\sum_{k=0}^{n} (4k^2 - 4k + 2)$
3. $C_n = \displaystyle\sum_{k=0}^{n} (6k^2 - 2k + 1)$

4. $D_n = \sum_{k=0}^{n}(3k^3 - 5k + 1)$
5. $E_n = \sum_{k=0}^{n} \frac{2^k}{3^{k+1}}$
6. $F_n = \sum_{k=2}^{n} \left(\frac{1}{3}\right)^k$
7. $G_n = \sum_{k=1}^{n}(2^k + 3^{2k})$
8. Soit $p \in \mathbb{N}^*$, $H_p = \sum_{k=0}^{p}(k^3 - 6 \times 2^k)$

Exercice 15

Principe des dominos ou téléscopage

1. Déterminer deux réels a et b tels que $\forall k \in \mathbb{N}^*,\ \frac{1}{k(k+1)} = \frac{a}{k} + \frac{b}{k+1}$.
2. En déduire $\sum_{k=1}^{100} \frac{1}{k(k+1)}$

Exercice 16

Sommes doubles

Calculer pour $n \in \mathbb{N}^*$, $S = \sum_{i=1}^{n}\sum_{j=1}^{n} i2^j$.

6.6 Exercices Complémentaires

Exercice 1

Les ensembles (munis de lois) suivants sont-ils des groupes ?

1. $(\mathbb{R}^*, \times)$.
2. $(\mathbb{C}, +)$.
3. $(a\mathbb{Z}, +)$, $a \in \mathbb{C}$.
4. $(a\mathbb{Z}, \times)$, $a \in \mathbb{C}^*$.
5. $(\mathcal{U}, +)$.
6. $(\mathcal{U}, \times)$.

Exercice 2

Soit $(G, \diamond)$ un groupe. Soit a un élément fixé de G. On définit une loi interne $*$ sur G par la formule

$$x * y = x \diamond a \diamond y$$

Montrer que $(G, *)$ est un groupe.

Exercice 3

Montrer que $(\mathcal{P}(E), \Delta)$ est un groupe, avec $F \Delta G = (F \cap \overline{G}) \cup (G \cap \overline{F})$.

Exercice 4

On note $\mathbb{Z}/2\mathbb{Z}$ l'ensemble $\{\overline{0}\ ;\ \overline{1}\}$ muni des lois $\overline{+}$ et $\overline{\times}$ définies par les tables suivantes :

$\overline{+}$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{1}$
$\overline{1}$	$\overline{1}$	$\overline{0}$

$\overline{\times}$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$

Montrer que $(\mathbb{Z}/2\mathbb{Z}, \overline{+}, \overline{\times})$ est un corps

Exercice 5

Symbole de sommation

Soit $n \in \mathbb{N}^*$, calculer les sommes suivantes :

1. $I_n = \sum_{k=0}^{n} \left(\frac{2^{k+3}}{3^{k+1}} \right)$
2. Soit $p \in \mathbb{N}^*$, $J_p = \sum_{k=2}^{3p} (2k+1)$
3. $K_n = \sum_{k=n}^{2n} (k^2)$ avec $n \geq 2$.
4. Soit $p \in \mathbb{N}$, $p \geq 3$, $L_p = \sum_{k=3}^{p} (3k^2 + 2k + 2)$
5. Soit $n \in \mathbb{N}^*$, $M_n = \sum_{k=2}^{2n+1} (k^3 + 3^{k+1})$
6. Soit $p \in \mathbb{N}^*$, $N_p = \sum_{k=p}^{2p} (2k^2 + k^3)$
7. Soit $p \in \mathbb{N}$, $O_p = \sum_{k=p}^{p+2} (2)$

Exercice 6

On pose $u_0 = 0$ et, $\forall n \in \mathbb{N}$,

$$u_{n+1} = u_n + n$$

$$v_n = u_{n+1} - u_n$$

1. Exprimer, $\forall n \in \mathbb{N}^*$,
$$\sum_{k=0}^{n-1} v_k$$
en fonction de u_n.
2. Exprimer, $\forall n \in \mathbb{N}^*$, u_n en fonction de n.

Exercice 7
Sommes doubles
Calculer pour $n \in \mathbb{N}^*$,
$$S = \sum_{i=1}^{n} \sum_{j=0}^{n} (1 - 2^i) 2^{ij}$$

Exercice 8
Sommes doubles
Calculer pour $n \in \mathbb{N}^*$,
$$S = \sum_{i=1}^{n} \sum_{j=i}^{n} \frac{1}{j}$$