Chapitre 13

Groupes, anneaux, corps

I Lois de composition interne

Dans tout le chapitre, E désigne un ensemble non vide, et $\mathbb{K}$ désigne $\mathbb{R}$ ou $\mathbb{C}$.

1. Définitions

Définition - Loi de composition interne, magma

On appelle *loi de composition interne*, ou *loi interne* sur E une application $\star : E \times E \to E$. On appelle alors *magma* et on note $(E, \star)$ l'ensemble E muni de sa loi de composition interne $\star$.

Remarques.

- Si $(E, \star)$ est un magma, on note $x \star y$ l'image de $(x, y) \in E^2$ par l'application $\star$.
- Les lois internes sont souvent notées de manière additive : $x + y$ ou de manière multiplicative : $x \times y$ ou xy. Il s'agit d'un choix arbitraire qui dépend du contexte, la seule contrainte est de se tenir au choix effectué.

Exemples.

- L'addition $+$ et la multiplication $\times$ sont des lois internes sur les ensembles $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.
- L'addition est une loi interne sur $\mathscr{M}_{n,p}(\mathbb{K})$, le produit matriciel est une loi interne sur $\mathscr{M}_n(\mathbb{K})$.
- L'addition $+$ et la multiplication $\times$ sur $\mathscr{F}(E, \mathbb{R})$ sont des lois internes, on dit qu'elles sont induites par les lois $+$ et $\times$ sur $\mathbb{R}$.
- La composition $\circ$ est une loi interne sur $\mathscr{F}(E, E)$.
- L'union $\cup$ et l'intersection $\cap$ sont des lois internes sur l'ensemble $\mathscr{P}(E)$ des parties de E.

Définition - Commutativité, associativité

Soit $(E, \star)$ un magma. On dit que la loi $\star$ est :

- *commutative* si : $\forall x, y \in E, \quad x \star y = y \star x$.
- *associative* si : $\forall x, y, z \in E, \quad x \star (y \star z) = (x \star y) \star z$.

Remarque. Si $\star$ est associative, on omet les parenthèses, qui deviennent inutiles : $x \star y \star z = x \star (y \star z) = (x \star y) \star z$. En notation multiplicative, on note $x^n = \underbrace{x \star \ldots \star x}_{n \text{ termes}}$, et en notation additive, on note $nx = \underbrace{x \star \ldots \star x}_{n \text{ termes}}$.

Exemples.

- Les lois $+$ et $\times$ sur $\mathbb{R}$ sont commutatives et associatives.
- Les lois $+$ et $\times$ sur $\mathscr{M}_n(\mathbb{K})$ sont associatives, mais $\times$ n'est pas commutative.
- La loi $\circ$ sur $\mathscr{F}(E, E)$ est associative mais non commutative.
- La soustraction $-$ est une loi interne sur $\mathbb{Z}$ qui est non associative et non commutative (on a par exemple $3 - (2 - 1) \neq (3 - 2) - 1$ et $2 - 1 \neq 1 - 2$).

Définition - Distributivité

Si $\star$ et $\diamond$ sont deux lois internes sur E, on dit que $\star$ est *distributive par rapport* à $\diamond$ si

$$\forall x, y, z \in E, \quad x \star (y \diamond z) = (x \star y) \diamond (x \star z) \quad \text{et} \quad (y \diamond z) \star x = (y \star x) \diamond (z \star x).$$

Exemples.

- Dans $\mathbb{R}$, la loi $\times$ est distributive par rapport à la loi $+$.
- Dans $\mathscr{P}(E)$, la loi $\cup$ est distributive par rapport à la loi $\cap$, et la loi $\cap$ distributive par rapport à la loi $\cup$.

Définition-théorème - Élément neutre

Si $(E,\star)$ est un magma et $e\in E$, on dit que e est un élément neutre de $(E,\star)$ (ou pour la loi $\star$) si

$$\forall x\in E,\quad x\star e \;=\; e\star x \;=\; x.$$

S'il existe un élément neutre pour la loi $\star$, alors il est unique.

Démonstration. Si e et e' sont deux éléments neutres pour $\star$, alors $e=e\star e'=e'$, donc $e=e'$. □

Remarque. S'il existe, l'élément neutre est souvent noté 0_E ou 0 en notation additive, et 1_E ou 1 en notation multiplicative.

Exemples.

1. $(\mathbb{R},+)$ admet 0 pour élément neutre, et $(\mathbb{R},\times)$ admet 1 pour élément neutre.
2. $(\mathscr{F}(E,\mathbb{R}),+)$ a pour élément neutre la fonction nulle, et $(\mathscr{F}(E,\mathbb{R}),\times)$ a pour élément neutre la fonction constante égale à 1.
3. $(\mathscr{M}_n(\mathbb{K}),+)$ a pour élément neutre la matrice nulle, et $(\mathscr{M}_n(\mathbb{K}),\times)$ a pour élément neutre I_n.
4. $(\mathscr{F}(E,E),\circ)$ a pour élément neutre la fonction Id_E.

Exercice 1. Quel est l'élément neutre de $(\mathscr{P}(E),\cup)$? L'élément neutre de $(\mathscr{P}(E),\cap)$?

Définition-théorème - Élément inversible, inverse

Si $(E,\star)$ a pour élément neutre e, on dit que $x\in E$ est *inversible* s'il existe un élément $y\in E$ appelé *inverse* de x tel que $x\star y \;=\; y\star x \;=\; e$.

Si $(E,\star)$ est associatif et si $x\in E$ admet un inverse, alors il est unique. On le note x^{-1} (si la notation est multiplicative), ou $-x$ (si la notation est additive).

Démonstration. Si y et z sont des inverses de x, alors par associativité $y\star x\star z \;=\; (y\star x)\star z \;=\; e\star z=z$, et $y\star x\star z \;=\; y\star(x\star z) \;=\; y\star e=y$, donc $y=z$. □

Remarque. On peut construire un exemple de magma non associatif tel qu'un élément a deux inverses : si E est un ensemble à trois éléments $1_E,a,b$ et si la loi interne $\star$ est décrite par

$\star$	1_E	a	b
1_E	1_E	a	b
a	a	1_E	1_E
b	b	1_E	1_E

alors $a\star a=a\star b=b\star a=1_E$, donc a et b sont deux inverses distincts de E. Comme $(a\star a)\star b=b$ et $a\star(a\star b)=a$, la loi $\star$ n'est en effet pas associative.

Exemples.

– Dans $(\mathbb{Z},+)$, tout élément est inversible, mais pas dans $(\mathbb{N},+)$ ou seul 0 admet un inverse.
– Dans $(\mathbb{R}^\star,\times)$, tout élément est inversible, mais pas dans $(\mathbb{R},\times)$ où 0 n'est pas inversible.
– Dans $(\mathscr{M}_n(\mathbb{K}),+)$, tout élément est inversible, mais dans $(\mathscr{M}_n(\mathbb{K}),\times)$, seules les matrices de $A\in\mathrm{GL}_n(\mathbb{K})$ admettent un inverse pour la loi $\times$, il s'agit bien sûr de la matrice inverse A^{-1}.
– Dans $(\mathscr{F}(E,\mathbb{R}),+)$ tout élément est inversible, mais dans $(\mathscr{F}(E,\mathbb{R}),\times)$, seules les fonctions qui ne s'annulent pas admettent un inverse.
– Dans $(\mathscr{F}(E,E),\circ)$, le éléments inversibles sont les fonctions f bijectives, d'inverse leur bijection réciproque f^{-1}.

Théorème - Inverse et opérations

Si $(E,\star)$ est un magma associatif possédant un élément neutre 1_E, alors

– Si $x\in E$ est inversible, alors x^{-1} est inversible et $(x^{-1})^{-1}=x$.
– Si $x\in E$ est inversible et $n\in\mathbb{N}$, alors x^n est inversible, et $(x^n)^{-1}=(x^{-1})^n$. On note cet élément x^{-n}.
– Si $x,y\in E$ sont inversibles, alors $x\star y$ est inversible et $(x\star y)^{-1}=y^{-1}\star x^{-1}$.

Remarques.

- En notation additive : – si x est inversible alors $-x$ l'est aussi et $-(-x) = x$,
  – si x est inversible alors nx l'est aussi et $-(nx) = n(-x)$, qu'on note $-nx$.
- On retrouve par exemple les propriétés déjà rencontrées pour $(\mathscr{M}_n(\mathbb{K}), \times)$.

Démonstration. Ce résultat a déjà été montré dans le cas de $\mathscr{M}_n(\mathbb{K})$. Les preuves sont les mêmes dans ce cas plus général. □

Définition - Partie stable

Si $(E, \star)$ est un magma et $F \subset E$, on dit que F est *stable* par $\star$ si

$$\forall x, y \in F, \quad x \star y \in F.$$

Dans ce cas, $(F, \star)$ est un magma. On dit que la loi $\star$ induit une loi interne sur F.

Exemples.

- Dans $(\mathbb{R}, \times)$: $\mathbb{R}_+$ est une partie stable par $\times$, mais pas $\mathbb{R}_-$.
- Dans $(\mathscr{M}_n(\mathbb{K}), +)$: les ensembles $\mathscr{S}_n(\mathbb{K})$, $\mathscr{T}_n^+(\mathbb{K})$, $\mathscr{D}_n(\mathbb{K})$ sont stables par $+$, mais pas $\mathrm{GL}_n(\mathbb{K})$.
- Dans $(\mathscr{M}_n(\mathbb{K}), \times)$: les ensembles $\mathscr{S}_n(\mathbb{K})$, $\mathscr{T}_n^+(\mathbb{K})$, $\mathscr{D}_n(\mathbb{K})$, $\mathrm{GL}_n(\mathbb{K})$ sont stables par $\times$.
- Dans $\mathscr{F}(\mathbb{R}, \mathbb{R}), \circ)$: l'ensemble des fonctions croisantes est stable par $\circ$.

II Structure de groupe

1. Groupes

Définition - Groupe

On dit qu'un magma associatif $(G, \star)$ est un *groupe* si :

- ◇ G possède un élément neutre,
- ◇ tout élément de G est inversible.

Si de plus $\star$ est commutative, on dit que $(G, \star)$ est un groupe *commutatif*, ou *abélien*.

Remarque. Si $(G, .)$ est un groupe et $x \in G$, alors toutes ses puissances appartiennent à G : pour tout $n \in \mathbb{Z}$, $x^n \in G$.
En notation additive, ceci s'écrit : si $(G, +)$ est un groupe et $x \in G$, alors pour tout $n \in \mathbb{Z}$, $nx \in G$.

Exemples.

1. $(\mathbb{C}, +)$, $(\mathbb{R}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{Z}, +)$ sont des groupes abéliens.
2. $(\mathbb{C}^\star, \times)$, $(\mathbb{R}^\star, \times)$ et $(\mathbb{Q}^\star, \times)$ sont des groupes abéliens. En revanche, $(\mathbb{C}, \times)$, $(\mathbb{R}, \times)$, $(\mathbb{Q}, \times)$ ne sont pas des groupes : 0 n'est pas inversible dans ces magmas.
3. $(\mathbb{Z}^\star, \times)$ n'est pas un groupe : par exemple, 2 n'a pas d'inverse dans $\mathbb{Z}^\star$.
4. $(\mathscr{M}_n(\mathbb{K}), +)$ est un groupe, mais $(\mathscr{M}_n(\mathbb{K}), \times)$ n'en est pas un (par exemple, la matrice nulle n'est pas inversible).
   Plus généralement, $(\mathscr{M}_{n,p}(\mathbb{K}), +)$ est un groupe.
5. $(\mathrm{GL}_n(\mathbb{K}), \times)$ est un groupe : si $A \in \mathrm{GL}_n(\mathbb{K})$, alors A possède un inverse dans $\mathrm{GL}_n(\mathbb{K})$, qui est A^{-1}.
   $(\mathrm{GL}_n(\mathbb{K}), +)$ n'est pas un groupe : on a vu que $\mathrm{GL}_n(\mathbb{K})$ n'est pas stable par la loi $+$.
6. L'ensemble des bijections de E dans E, noté $\mathfrak{S}_E$ ou $\mathfrak{S}(E)$, forme un groupe pour la loi $\circ$, qu'on appelle *groupe symétrique* de E et qu'on note $(\mathfrak{S}_E, \circ)$.

   En effet, si $f \in \mathfrak{S}_E$, alors sa bijection réciproque f^{-1} est encore un élément de $\mathfrak{S}_E$, donc tout élément de $\mathfrak{S}_E$ admet un inverse dans $\mathfrak{S}_E$.

Remarque. Il arrive fréquemment qu'on omette de préciser la loi du groupe lorsque le contexte est clair : par exemple, le groupe $\mathbb{C}$ désigne le groupe $(\mathbb{C}, +)$, et le groupe $\mathbb{C}^\star$ désigne le groupe $(\mathbb{C}^\star, \times)$. De même pour $\mathbb{R}, \mathbb{Q}, \mathbb{Z}, \mathbb{R}^\star, \mathbb{Q}^\star$, mais aussi $\mathscr{M}_n(\mathbb{K})$, $\mathrm{GL}_n(\mathbb{K})$. D'après ce qui précède, il n'y a pas d'ambiguïté.

Lorsqu'on travaille avec un groupe G quelconque de manière théorique, il arrive qu'on ne précise pas la loi, et qu'on utilise par défaut la notation multiplicative : on note 1_G ou 1 l'élément neutre de G et xy pour $x \star y$.

Définition-théorème - Groupe et régularité

Si $(G,\star)$ est un groupe, alors tout élément $x\in G$ est *régulier*, c'est-à-dire :

$$\forall a,b\in G,\quad x\star a = x\star b \Rightarrow a=b \quad \text{et} \quad a\star x = b\star x \Rightarrow a=b.$$

On dit aussi qu'on peut simplifier (à gauche ou à droite) par tout élément de G.

Démonstration. Soient $a,b\in G$ tels que $x\star a = x\star b$. Comme x est inversible dans G, d'inverse noté x^{-1}, on a $x^{-1}\star x\star a = x^{-1}\star x\star b$, donc $a=b$. De même pour le deuxième cas. □

Définition-théorème - Groupe produit

Si $(G,\star)$ et $(H,\diamond)$ sont des groupes, alors $(G\times H,\bullet)$ est un groupe, où la loi $\bullet$ est donnée par :

$$\forall (x,y),(x',y')\in G\times H,\quad (x,y)\bullet(x',y') = (x\star x', y\diamond y').$$

On dit que $G\times H$ est le groupe produit associé à G et H. On généralise cette définition au produit $G_1\times\ldots\times G_n$ de n groupes $G_1,\ldots,G_n$.

Démonstration. Il est clair que $\bullet$ est une loi interne associative sur G. Par ailleurs, si on note 1_G et 1_H les éléments neutres respectifs de G et H, alors $(1_G,1_H)$ est élément neutre de $G\times H$. Pour finir, si $(x,y)\in G\times H$, alors en notant x^{-1} (resp. y^{-1}) l'inverse de x dans G (resp. de y dans H), le couple (x^{-1},y^{-1}) est inverse de (x,y) dans $G\times H$. □

Exemple. La loi du groupe produit $\mathbb{R}\times\mathbb{R}$ est donnée par : $((x,y),(x',y')) \mapsto (x+x', y+y')$.

2. Sous-groupes

Définition - Sous-groupe

Soient $(G,\star)$ un groupe et H une partie de G stable par $\star$. On dit que H est un *sous-groupe* de G si $(H,\star)$ est lui-même un groupe.

Exemples.

1. Un groupe G a toujours pour sous-groupe $\{e\}$ (ou e désigne l'élément neutre de G), et G. On dit que ces deux sous-groupes sont *triviaux*.
2. $\mathbb{Z}$ est un sous-groupe de $\mathbb{R}$, et $\mathbb{R}$ est un sous-groupe de $\mathbb{C}$ (muni de la loi $+$), $\mathbb{R}^\star$ est un sous-groupe de $\mathbb{C}^\star$ (muni de la loi $\times$).

Théorème - Caractérisation des sous-groupes

Si $(G,.)$ est un groupe et $H\subset G$, alors :

$$H \text{ est un sous-groupe de } G \iff \begin{cases} 1_G\in H \\ H \text{ est stable par la loi de } G : \ \forall x,y\in H,\ xy\in H \\ H \text{ est stable par passage à l'inverse} : \ \forall x\in H,\ x^{-1}\in H \end{cases}$$

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

Remarques.

– Le résultat ci-dessus est écrit en notation multiplicative. En notation additive, ceci devient : $H\subset G$ est un sous-groupe de $(G,+)$ si et seulement si $0_G\in H$ et pour tous $x,y\in H$, $x-y\in H$.

– On peut remplacer la vérification de $1_G\in H$ par : “H est non vide”.

Démonstration. On montre que H est un sous-groupe de G ssi $1_G\in H$ et $\forall x,y\in H,\ xy^{-1}\in H$, le reste est analogue.

– Si H est un sous-groupe de G, notons 1_H son élément neutre. On a alors $1_H 1_G = 1_H$ car $1_H\in G$, et $1_H1_H = 1_H$, donc $1_H1_G = 1_H1_H$, ce qui donne $1_H = 1_G$ car 1_H est régulier.

Soient $x,y\in H$. On note y_G^{-1} l'inverse de y dans G et y_H^{-1} son inverse dans H. On a $y_G^{-1} = y_H^{-1}$ car y est régulier dans G et $y_G^{-1}y = y_H^{-1}y = 1_H = 1_G$. Ainsi, par stabilité de H par la loi de G, on a $xy^{-1}\in H$.

– Supposons que $1_G \in H$ et $\forall x, y \in H,\ xy^{-1} \in H$. Si $y \in H$, alors $1_G y^{-1} \in H$, donc $y^{-1} \in H$, donc y est inversible dans H. Par ailleurs, si $x, y \in H$, alors $xy = x(y^{-1})^{-1} \in H$, donc H est stable par la loi de G. Comme par ailleurs la loi de G est associative, on en déduit que $(H, .)$ est un groupe. □

Remarques.

– Dans la pratique, on utilisera toujours le résultat ci-dessus pour montrer que H est un sous-groupe de G.
– Lorsqu'on souhaite montrer que $(H, .)$ est un groupe, il sera souvent très utile de montrer qu'il s'agit d'un sous-groupe d'un groupe $(G, .)$ qu'on identifiera. De cette manière, on pourra s'affranchir de la vérification de l'associativité, l'élément neutre et l'existence d'inverse : ces propriétés seront directement héritées de celles de la loi . sur G.

Exemples.

1. Si $n \in \mathbb{N}$, alors $n\mathbb{Z} = \{kn,\ k \in \mathbb{Z}\}$ est un sous-groupe de $\mathbb{Z}$ (muni de la loi $+$).

   En effet, on a d'abord $n\mathbb{Z} \subset \mathbb{Z}$. Par ailleurs, 0 est un multiple de n, donc $0 \in n\mathbb{Z}$, et si $x, y \in n\mathbb{Z}$, alors $x - y$ est un multiple de n donc $x - y \in n\mathbb{Z}$.

2. Si $a, b \in \mathbb{Z}$, alors $a\mathbb{Z} + b\mathbb{Z} = \{au + bv,\ u, v \in \mathbb{Z}\}$ est un sous-groupe de $\mathbb{Z}$.

   Si on note $G = a\mathbb{Z} + b\mathbb{Z}$, alors on a $0 \in G$ et si $n, m \in G$, il existe $k, l, k', l' \in \mathbb{Z}$ tels que $n = ka + lb$, $m = k'a + l'b$, donc $n - m = (k - k')a + (l - l')b \in G$.

3. $\mathbb{R}_+^\star$ est un sous-groupe de $(\mathbb{R}^\star, \times)$.
4. L'ensemble $\mathbb{U} = \{z \in \mathbb{C},\ |z| = 1\}$ est un sous-groupe de $\mathbb{C}^\star$ (muni de la loi $\times$).

   En effet, on a $\mathbb{U} \subset \mathbb{C}^\star$ et $1 \in \mathbb{U}$. Par ailleurs, si $z, z' \in \mathbb{U}$, alors $|zz'^{-1}| = \frac{|z|}{|z'|} = 1$, donc $zz'^{-1} \in \mathbb{U}$.

5. Si I est un intervalle de $\mathbb{R}$, alors $\mathscr{C}^0(I, \mathbb{R})$ est un sous-groupe de $(\mathscr{F}(I, \mathbb{R}), +)$.

Exercice 2.

1. Montrer que $S = \{z \mapsto az + b,\ (a, b) \in \mathbb{C}^\star \times \mathbb{C}\}$ est un sous-groupe de $\mathfrak{S}_\mathbb{C}$ (muni de la loi $\circ$).
2. Montrer que $T = \{A \in \mathscr{T}_n^+(\mathbb{K}),\ \forall i \in [\![1, n]\!],\ a_{i,i} \neq 0\}$ est un sous-groupe de $\mathrm{GL}_n(\mathbb{K})$ (muni de la loi $\times$).

Théorème - Intersection de sous-groupes

Si G est un groupe et H, H' sont des sous-groupes de G, alors $H \cap H'$ est un sous-groupe de G.
Plus généralement, si $(H_i)_{i \in I}$ est une famille de sous-groupes de G, alors $\bigcap_{i \in I} H_i$ est un sous-groupe de G.

Démonstration. Traitons le cas de deux sous-groupes, le cas général est identique. On a $H \cap H' \subset G$, $1_G \in H \cap H'$, et si $x, y \in H \cap H'$, alors $xy^{-1} \in H$ et $xy^{-1} \in H'$ car H et H' sont des sous-groupes, donc $xy^{-1} \in H \cap H'$. □

Exemple. Si $a, b \in \mathbb{Z}$, alors l'ensemble $a\mathbb{Z} \cap b\mathbb{Z}$ des multiples communs à a et b est un sous-groupe de $\mathbb{Z}$.

⚠ L'union de deux sous-groupes de G n'est pas un sous-groupe en général.

Par exemple, $2\mathbb{Z}$ et $3\mathbb{Z}$ sont des sous-groupes de $\mathbb{Z}$, mais $H = 2\mathbb{Z} \cup 3\mathbb{Z}$ n'est pas un sous-groupe de $\mathbb{Z}$: $2, 3 \in H$ mais $2 + 3 \notin H$.

On retiendra le résultat suivant, montré en TD : si H et H' sont des sous-groupes de G, alors $H \cup H'$ est un sous-groupe de G si et seulement si l'un des sous-groupes H, H' est inclus dans l'autre.

Théorème - Sous-groupes de $\mathbb{Z}$

Les sous-groupes de $\mathbb{Z}$ sont exactement les ensembles $n\mathbb{Z}$, où $n \in \mathbb{N}$.

Démonstration. On sait déjà que les ensembles de la forme $n\mathbb{Z}$ sont des sous-groupes de $\mathbb{Z}$. Si maintenant G est un sous-groupe de $\mathbb{Z}$, il s'agit de montrer que G est de la forme $n\mathbb{Z}$ pour $n \in \mathbb{N}$.

– Si $G = \{0\}$, alors $G = 0\mathbb{Z}$.
– Si $G \neq \{0\}$, alors il existe $k \neq 0$ tel que $k \in G$, et donc $-k \in G$. Ceci entraîne que $G \cap \mathbb{N}^\star$ est une partie non vide de $\mathbb{N}$. On pose alors $n = \min G \cap \mathbb{N}^\star$, et on va montrer que $G = n\mathbb{Z}$.

- On a $n\mathbb{Z} \subset G$: on sait que $n \in G$, et comme G est stable par $+$, on a aussi $kn \in G$ pour tout $k \in \mathbb{Z}$.
- On a $G \subset n\mathbb{Z}$: si $x \in G$, on écrit $x = nq + r$ la division euclidienne de x par n, on a alors $r \in [\![0, n-1]\!]$. Comme $nq \in n\mathbb{Z}$, on a aussi $nq \in G$. Ainsi, $r = x - nq \in G$. Comme $r \in G \cap \mathbb{N}$ et $r < n$, on a a alors $r = 0$, et $x \in n\mathbb{Z}$. □

Remarque. Soient $a, b \in \mathbb{Z}$.

- ◇ On retrouve le fait que $a\mathbb{Z} \cap b\mathbb{Z}$ est de la forme $m\mathbb{Z}$ avec $m \in \mathbb{N}$, en tant que sous-groupe de $\mathbb{Z}$. Nous avons déjà vu d'ailleurs que $a\mathbb{Z} \cap b\mathbb{Z} = (a \vee b)\mathbb{Z}$.
- ◇ On retrouve également que $a\mathbb{Z} + b\mathbb{Z}$ est de la forme $d\mathbb{Z}$ avec $d \in \mathbb{N}$, en tant que sous-groupe de $\mathbb{Z}$. Nous avons déjà vu d'ailleurs que $a\mathbb{Z} + b\mathbb{Z} = (a \wedge b)\mathbb{Z}$.

3. Morphismes de groupes

Définition - Morphisme de groupes

Soient $(G, \star)$ et $(G', \diamond)$ deux groupes. On dit qu'une application $f : G \to G'$ est un *morphisme de groupes* si

$$\forall x, y \in G, \quad f(x \star y) = f(x) \diamond f(y).$$

Remarque. En notation multiplicative pour les deux groupes G, G', ceci se récrit : $\forall x, y \in G, \ f(xy) = f(x)f(y)$.

Exemples.

- La fonction exp est un morphisme de groupes de $(\mathbb{R}, +)$ dans $(\mathbb{R}_+^\star, \times)$.
- La fonction ln est un morphisme de groupes de $(\mathbb{R}_+^\star, \times)$ dans $(\mathbb{R}, +)$.
- Si $a \in \mathbb{R}$, la fonction $f : x \mapsto ax$ définit un morphisme de groupes de $(\mathbb{R}, +)$ dans $(\mathbb{R}, +)$.
- L'application $\varphi : f \mapsto \int_0^1 f(t)\,dt$ définit un morphisme de groupes de $(\mathscr{C}^0([0,1], \mathbb{R}), +)$ dans $(\mathbb{R}, +)$.
- L'application transposition $f : A \mapsto A^\top$ définit un morphisme de groupes de $\mathscr{M}_n(\mathbb{K})$ dans lui-même.
- L'application $A \mapsto \operatorname{tr} A$ définit un morphisme de groupes de $\mathscr{M}_n(\mathbb{K})$ dans $\mathbb{K}$.
- Si $A \in \mathscr{M}_{n,p}(\mathbb{K})$, alors l'application $X \mapsto AX$ définit un morphisme de groupes de $\mathscr{M}_{p,1}(\mathbb{K})$ dans $\mathscr{M}_{n,1}(\mathbb{K})$.

Théorème - Morphismes, éléments neutres et inverses

Si $f : G \to G'$ est un morphisme de groupes, alors $f(1_G) = 1_{G'}$ et pour tout $x \in G$, $f(x^{-1}) = f(x)^{-1}$.

Démonstration. On a $f(1_G) = f(1_G 1_G) = f(1_G)f(1_G)$. En multipliant à droite par $f(1_G)^{-1}$, on obtient $1_{G'} = f(1_G)$. Si $x \in G$, on a $f(x)f(x^{-1}) = f(xx^{-1}) = 1_{G'}$. En multipliant à gauche par $f(x)^{-1}$, on obtient $f(x^{-1}) = f(x)^{-1}$. □

Remarque. Avec la notation additive, ceci d'écrit $f(0_G) = 0_{G'}$, et pour tout $x \in G$, $f(-x) = -f(x)$.

Théorème - Composition de morphismes

Soient $f : (G, \star) \to (G', \diamond)$ et $g : (G', \diamond) \to (G'', \bullet)$ des morphismes de groupes. Alors, $g \circ f : (G, \star) \to (G'', \bullet)$ est un morphisme de groupes.

Démonstration. Soient $x, y \in G$, on a $g(f(x \star y)) = g(f(x) \diamond f(y)) = g(f(x)) \bullet g(f(y))$. □

Théorème - Image directe, image réciproque d'un sous-groupe

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

- L'image directe d'un sous-groupe de G est un sous-groupe de G'.
- L'image réciproque d'un sous-groupe de G' est un sous-groupe de G.

Démonstration. On choisit une notation multiplicative pour G et G' pour plus de clarté.

- Soit H un sous-groupe, montrons que $f(H) = \{f(x), \ x \in H\}$ est un sous-groupe de G'. On a tout d'abord $1_{G'} \in f(H)$ car $1_G \in H$ et $f(1_G) = 1_{G'}$. Ensuite, si $y, y' \in f(H)$, alors il existe $x, x' \in H$ tels que $y = f(x)$ et $y' = f(x')$. Ainsi, $yy'^{-1} = f(x)f(x')^{-1} = f(x)f(x'^{-1}) = f(xx'^{-1}) \in f(H)$.

– Soit H' un sous-groupe de G', montrons que $f^{-1}(H') = \{x \in G,\ f(x) \in H'\}$ est un sous-groupe de G. On a $f(1_G) = 1_{G'} \in H'$, donc $1_G \in f^{-1}(H')$. Par ailleurs, si $x, x' \in f^{-1}(H')$, alors $f(x), f(x') \in H'$, donc $f(xx'^{-1}) = f(x)f(x')^{-1} \in H'$, donc $xx'^{-1} \in f^{-1}(H')$. □

4. Noyau et image d'un morphisme de groupes

Les cas particuliers suivants d'images directes et réciproques de sous-groupes joueront un grand rôle dans la suite.

Définition - Image et noyau d'un morphisme

Soient $f : G \to G'$ un morphisme de groupes et e' l'élément neutre de G'. On appelle

– *image* de f, et on note $\operatorname{Im} f$ le sous-groupe $f(G) = \{f(x),\ x \in G\}$ de G',
– *noyau* de f, et on note $\operatorname{Ker} f$ le sous-groupe $f^{-1}(\{e'\}) = \{x \in G,\ f(x) = e'\}$ de G.

Exemples.

– L'application $f : \theta \mapsto \mathrm{e}^{\mathrm{i}\theta}$ définit un morphisme de groupes de $(\mathbb{R}, +)$ dans $(\mathbb{U}, \times)$. On a :
  ◇ $\operatorname{Im} f = \{f(\theta),\ \theta \in \mathbb{R}\} = \{\mathrm{e}^{\mathrm{i}\theta},\ \theta \in \mathbb{R}\} = \mathbb{U}$,
  ◇ $\operatorname{Ker} f = \{\theta \in \mathbb{R},\ f(\theta) = 0\} = \{2k\pi,\ k \in \mathbb{Z}\} = 2\pi\mathbb{Z}$.
– Si $A \in \mathscr{M}_{n,p}(\mathbb{K})$, on a vu que $f_A : X \mapsto AX$ définit un morphisme de groupes de $\mathscr{M}_{p,1}(\mathbb{K})$ dans $\mathscr{M}_{n,1}(\mathbb{K})$. Ainsi,

$$\operatorname{Ker} f_A = f_A^{-1}(\{0_{n,1}\}) = \{X \in \mathscr{M}_{p,1}(\mathbb{K}),\ AX = 0_{n,1}\}$$

  On remarque que, dans ce cas, il s'agit exactement de la notion de noyau de la matrice A, rencontrée dans le chapitre Matrices et systèmes linéaires.

Remarque. On peut alors montrer qu'un ensemble définit un sous-groupe en montrant qu'on peut le voir comme le noyau ou l'image d'un morphisme de groupes.

Théorème - Noyau, image, injectivité et surjectivité

Si $f : G \to G'$ un morphisme de groupes et e est l'élément neutre de G, alors

◇ f est surjectif si et seulement si $\operatorname{Im} f = G'$,
◇ f est injectif si et seulement si $\operatorname{Ker} f = \{e\}$.

Démonstration.

◇ Il s'agit de la définition de la surjectivité de l'application $f : G \to G'$.
◇ Supposons que f est injectif, et montrons $\operatorname{Ker} f = \{e\}$. Comme $e \in \operatorname{Ker} f$, il suffit que montrer que $\operatorname{Ker} f \subset \{e\}$. Si $x \in \operatorname{Ker} f$, alors $f(x) = e' = f(e)$. Par injective, on a alors $x = e$, ce qui conclut.
  Réciproquement, si $\operatorname{Ker} f = \{e\}$, on considère $x, y \in G$ tels que $f(x) = f(y)$. On a alors $f(x)f(y)^{-1} = e'$, donc $f(xy^{-1}) = e'$ et $xy^{-1} \in \operatorname{Ker} f$. Ainsi, on a $xy^{-1} = e$, ce qui donne $x = y$. □

Remarque. Nous avons choisi la notation multiplicative dans la preuve ci-dessus, mais nous aurions aussi bien pu écrire le raisonnement en notation additive : si $f(x) = f(y)$, alors $f(x) - f(y) = e'$, donc $f(x-y) = e'$, et $x - y \in \operatorname{Ker} f$.

Exemple. Le morphisme $f : \theta \mapsto \mathrm{e}^{\mathrm{i}\theta}$ est surjectif, car $\operatorname{Im} f = \mathbb{U}$, mais pas injectif, car $\operatorname{Ker} f \neq \{0\}$.

5. Isomorphismes, automorphismes

Définition - Isomorphisme de groupes, groupes isomorphes

On dit qu'un morphisme de groupe $f : G \to G'$ est un *isomorphisme de groupes* si f est bijectif. On dit alors que G et G' sont des groupes isomorphes.

Dans le cas où $G = G'$, on appelle *automorphisme* de G un isomorphisme $f : G \to G$. On note $\operatorname{Aut}(G)$ l'ensemble des automorphismes de G.

Exemple. Les groupes $\mathbb{R}$ et $\mathbb{R}_+^\star$ sont isomorphes : la fonction $\exp : \mathbb{R} \to \mathbb{R}_+^\star$ définit un isomorphisme du groupe $\mathbb{R}$ dans le groupe $\mathbb{R}_+^\star$.

Théorème - Isomorphismes et composition, réciproque

Soient $f : G \to G'$ et $g : G' \to G''$ des isomorphismes de groupes.

- La composition $g \circ f$ est un isomorphisme de groupes de G dans G''.
- La réciproque f^{-1} est un isomorphisme de groupes de G' dans G.

Démonstration.

- On sait qu'une composée de morphismes est un morphisme, et qu'une composée de bijections est une bijection.
- On sait déjà que f^{-1} est une bijection, il reste à voir que c'est un morphisme. Soient $y, y' \in G'$ et $x, x' \in G$ tels que $f(x) = y$ et $f(x') = y'$. On a alors $f(xx') = f(x)f(x') = yy'$, donc $xx' = f^{-1}(yy')$. Ceci entraîne que $f^{-1}(yy') = xx' = f^{-1}(y)f^{-1}(y')$, donc f^{-1} est un morphisme. □

Théorème - Groupe des automorphismes

Si G est un groupe, alors $(\mathrm{Aut}(G), \circ)$ est un groupe. On parle du groupe des automorphismes de G.

Démonstration. $(\mathrm{Aut}(G), \circ)$ est un sous-groupe de $(\mathfrak{S}(G), \circ)$. En effet, $\mathrm{Id}_G \in \mathrm{Aut}(G)$, et $\sigma \circ \tau^{-1} \in \mathrm{Aut}(G)$ pour tous $\sigma, \tau \in \mathrm{Aut}(G)$: τ^{-1} est un isomorphisme, donc $\sigma \circ \tau$ est un isomorphisme de G dans G. □

Exercice 3. Déterminer tous les automorphismes de $\mathbb{Z}$.

III Structure d'anneau, structure de corps

1. Définitions

Définition - Anneau

Si A est un ensemble muni de deux lois de composition internes $+$ et $\times$, on dit que $(A, +, \times)$ est un anneau si

- $(A, +)$ est un groupe abélien,
- la loi $\times$ est associative, distributive par rapport à $+$, et A admet un élément neutre pour $\times$.

Si de plus la loi $\times$ est commutative, on dit que A est un anneau commutatif.

Exemples.

1. $(\mathbb{Z}, +, \times)$, $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$, $(\mathbb{C}, +, \times)$ sont des anneaux commutatifs.
2. $(\mathscr{F}(E, \mathbb{R}), +, \times)$ est un anneau commutatif.
3. $(\mathscr{M}_n(\mathbb{K}), +, \times)$ est un anneau, qui est non commutatif si $n \geqslant 2$.

Remarques.

- Il arrive fréquemment qu'on ne précise pas les lois d'un anneau lorsque le contexte est clair : on évoquera par exemple l'anneau $\mathbb{Z}$, l'anneau $\mathscr{M}_n(\mathbb{K})$.
- Dans un anneau A, l'élément neutre pour $+$ est généralement noté 0_A ou 0, et l'élément neutre pour $\times$ est généralement noté 1_A ou 1.
- Si A est un anneau, $a \in A$ et $n \in \mathbb{N}$, les éléments na et a^n existent, et désignent respectivement $a + a + \ldots + a$ et $a \times a \times \ldots \times a$.
- Tout élément a d'un anneau a toujours un inverse pour la loi $+$, noté $-a$, mais n'a pas toujours un inverse pour la loi $\times$. Lorsqu'on parle d'un élément inversible d'un anneau, on l'entend donc toujours pour la loi $\times$.

Théorème - Règles de calcul dans un anneau

Soient A un anneau et $a, b \in A$. On a :

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

◇ $(-a)\,b = a\,(-b) = -ab$ et $(-a)\,(-b) = ab$. Plus généralement pour $n \in \mathbb{Z}$, $(na)\,b = a\,(nb) = n\,ab$.

Démonstration.

- ◇ On a $0_A \times a = (0_A + 0_A) \times a = 0_A \times a + 0_A \times a$ par distributivité. Il suffit de simplifier [1] par $0_A \times a$, et on obtient $0_A \times A = 0_A$.
- ◇ On a $(-a+a)b = 0_A b = 0_A$ d'après le point précédent. Ainsi, par distributivité, on a $(-a)b + ab = 0_A$, ce qui donne $(-a)b = -ab$. L'autre cas est similaire. On déduit de ceci que $(-a)(-b) = -(a(-b)) = -(-ab) = ab$.

  On en déduit le dernier point par récurrence immédiate le résultat pour $n \in \mathbb{N}$, puis ce sui précède montre qu'il est vrai pour $n \in \mathbb{Z}$. □

Remarques.

- En particulier, $(-1_A)\,a = a\,(-1_A) = -a$, et $(-1_A)^2 = 1_A$.
- Il est possible d'avoir $1_A = 0_A$. Dans ce cas, on a $A = \{0_A\}$: en effet, on a alors $a = 1_A a = 0_A a = 0_A$ pour tout $a \in A$. L'anneau A est alors appelé l'*anneau nul*.

Théorème - Formule du binôme, formule de Bernoulli

Si A est un anneau et $a, b \in A$ commutent, *i.e.* $ab = ba$, alors pour tout $n \in \mathbb{N}$,

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k\, b^{n-k}, \qquad a^n - b^n = (b-a) \sum_{k=0}^{n-1} a^k\, b^{n-1-k}.$$

Démonstration. Mêmes preuves que dans $\mathbb{R}$. □

Théorème et définition - Groupe des inversibles d'un anneau

Soit A un anneau, on note $A^\times$ l'ensemble des éléments inversibles de A. $(A^\times, \times)$ est un groupe, appelé *groupe des inversibles* de A.

Démonstration. On sait déjà que $\times$ est associative, et l'élément neutre 1_A appartient à $A^\times$ car $1_A^2 = 1_A$. Par ailleurs, $\times$ est une loi interne sur $A^\times$ car un produit d'éléments inversibles de A est également inversible. Pour finir, tout élément de $A^\times$ est inversible dans $A^\times$: si $x \in A^\times$, alors $x^{-1} \in A^\times$. □

Exemples.
- ◇ $\mathbb{C}^\times = \mathbb{C}^\star$, $\mathbb{R}^\times = \mathbb{R}^\star$,
- ◇ $\mathbb{Z}^\times = \{-1, 1\}$,
- ◇ $\mathscr{F}(\mathbb{R}, \mathbb{R})^\times = \{f : \mathbb{R} \to \mathbb{R},\ f \text{ ne s'annule pas}\}$.

Définition - Anneau intègre

On dit qu'un anneau A non nul est *intègre* si

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

Autrement dit, le produit de deux éléments non nuls est non nul.

Exemples.
- Les anneaux $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ sont intègres.
- L'anneau $\mathscr{M}_n(\mathbb{K})$ n'est pas intègre si $n \geqslant 2$: par exemple, ${E_{1,n}}^2 = 0_{\mathscr{M}_n(\mathbb{K})}$.

Exercice 4. L'anneau $\mathscr{F}([0,1], \mathbb{R})$ est-il intègre ?

Définition-théorème - Anneau produit

Si $(A, +, \times)$ et $(B, +, \times)$ sont deux anneaux, alors $(A \times B, +, \times)$ est un anneau, où les lois de $A \times B$ sont données par :

$$\forall (x, y), (x', y') \in A \times B, \quad (x, y) + (x', y') = (x + x', y + y') \quad \text{et} \quad (x, y)\,(x', y') = (xx', yy').$$

1. $(A, +)$ est un groupe, donc on peut simplifier par tout élément.

Exemple. $\mathbb{Z}^2$ est un anneau, muni des lois : $(x, y) + (x', y') = (x + x', y + y')$, et $(x, y)\,(x', y') = (xx', yy')$.

2. Sous-anneaux

De même que pour les groupes, nous allons introduire la notion de sous-anneaux. Ici encore, il sera plus commode pour montrer qu'un ensemble est un anneaux de l'identifier comme sous-anneau d'un anneau de référence.

Définition - Sous-anneau

Soient $(A, +, \times)$ un anneau et B une partie de A. On dit que B est un *sous-anneau* de A si

- B est stable par les lois $+$ et $\times$,
- $1_A \in B$,
- $(B, +, \times)$ est un anneau.

Exemples. $\mathbb{Z}$ est un sous-anneau de $\mathbb{Q}$, qui est un sous-anneau de $\mathbb{R}$, qui est un sous-anneau de $\mathbb{C}$.

Théorème - Caractérisation des sous-anneaux

Si A est un anneau et $B \subset A$, alors B est un sous-anneau de A si et seulement si

- $1_A \in B$,
- B est stable par différence : $\forall x, y \in B,\ x - y \in B$,
- B est stable par produit : $\forall x, y \in B,\ xy \in B$.

Démonstration. La preuve est analogue à celle pour les groupes, et est laissée en exercice. □

Exemples.

– Si I est un intervalle de $\mathbb{R}$, $(\mathscr{C}^k(I), \mathbb{R})$ est un sous-anneau de $\mathscr{F}(I, \mathbb{R})$.

En effet, la fonction $x \in I \mapsto 1$ est bien de classe $\mathscr{C}^k$, et on sait que $\mathscr{C}^k(I, \mathbb{R})$ est stable par différence et par produit.

– L'ensemble $\mathscr{T}_n^+(\mathbb{K})$ des matrices triangulaires supérieures de $\mathscr{M}_n(\mathbb{K})$ est un sous-anneau de $\mathscr{M}_n(\mathbb{K})$.

En effet, $I_n \in \mathscr{T}_n^+(\mathbb{K})$ et on sait que $\mathscr{T}_n^+(\mathbb{K})$ est stable par différence et par produit matriciel.

3. Morphismes d'anneaux

Définition - Morphisme d'anneaux

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

- $f(1_A) = 1_{A'}$,
- $\forall x, y \in A, \quad f(x + y) = f(x) + f(y)$,
- $\forall x, y \in A, \quad f(xy) = f(x)\,f(y)$.

Si f est un morphisme d'anneaux bijectif, on dit que f est un *isomorphisme*, et si de plus $A = A'$, on dit que f est un *automorphisme*.

Exemples.

– L'application $f : z \mapsto \bar{z}$ est un morphisme d'anneaux de $\mathbb{C}$ dans $\mathbb{C}$.

On a $\bar{1} = 1$, et on sait que si $z, z' \in \mathbb{C}$, alors $\overline{z + z'} = \bar{z} + \bar{z}$ et $\overline{zz'} = z\bar{z}$.

– Si $P \in \mathrm{GL}_n(\mathbb{K})$, alors l'application $\varphi_P : A \mapsto PAP^{-1}$ est un morphisme d'anneaux de $\mathscr{M}_n(\mathbb{K})$ dans $\mathscr{M}_n(\mathbb{K})$.

On a $\varphi_P(I_n) = I_n$, et si $A, B \in \mathscr{M}_n(\mathbb{K})$, alors $\varphi_P(A + B) = PAP^{-1} + PBP^{-1} = \varphi_P(A) + \varphi_P(B)$, et $\varphi_p(AB) = PAP^{-1}PBP^{-1} = \varphi_P(A)\,\varphi_P(B)$.

Ces deux exemples sont en fait des automorphismes d'anneaux.

Théorème - Propriétés des morphismes d'anneaux

– Si $f : A \to A'$ est un morphisme d'anneaux, alors :
  - $f(0_A) = 0_{A'}$,
  - pour tout $x \in A$, $f(-x) = -f(x)$
  - pour tout $x \in A^\times$, $f(x^{-1}) = f(x)^{-1}$.

– La composition $g \circ f$ de deux morphismes d'anneaux $f : A \to A'$ et $g : A' \to A''$ est un morphisme d'anneaux de A dans A''.

– L'image réciproque d'un sous-anneau de A' est un sous-anneau de A, l'image directe d'un sous-anneau de A est un sous-anneau de A'.

– Si $f : A \to A'$ est un morphisme d'anneaux, on définit comme pour les morphismes de groupes :

$$\operatorname{Im} f = f(A) = \{f(x),\ x \in A\}, \qquad \operatorname{Ker} f = f^{-1}(\{0_{A'}\}) = \{x \in A,\ f(x) = 0_{A'}\}.$$

On a toujours : f est surjectif si et seulement si $\operatorname{Im} f = A'$ et f est injectif si et seulement si $\operatorname{Ker} f = \{0_A\}$.

Démonstration. Les preuves sont similaires aux preuves des résultats sur les morphismes de groupes, et sont laissées en exercice. □

⚠ Le noyau d'un morphisme d'anneau est toujours défini en choisissant l'élément neutre 0_A (pour la loi $+$).

4. Corps

Définition - Corps

On appelle *corps* tout anneau commutatif non nul tel que tout élément non nul est inversible.

Exemple. $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont des corps. $\mathbb{Z}$ n'est pas un corps.

Remarques.

– Si K est un corps, on note $K^\star = K \backslash \{0_K\}$. On a alors $K^\star = K^\times$.
– Si $x \in K$ et $y \in K^\star$, alors on note $\frac{x}{y} = y^{-1}x = xy^{-1}$. Cette notation n'est pas ambiguë car K est commutatif. On retiendra qu'un corps est un anneau dans lequel on peut diviser par tout élément, sauf 0.
– Tout corps K est intègre : si $x, y \in K$ et $xy = 0_K$ avec $x \neq 0_K$, alors $y = \frac{xy}{x} = 0_K$.

On introduit la notion de sous-corps, similaire à la notion de sous-anneau, et on donne une caractérisation analogue à celle rencontrée pour les sous-anneaux.

Définition - Sous-corps

Soient $(K, +, \times)$ un anneau et L une partie de K. On dit que L est un *sous-corps* de A si

- L est stable par les lois $+$ et $\times$,
- $1_K \in L$,
- $(L, +, \times)$ est un corps.

Théorème - Caractérisation des sous-corps

Si K est un corps et $L \subset K$, alors L est un sous-corps de K si et seulement si

- $1_K \in L$,
- L est stable par différence : $\forall x, y \in L,\ x - y \in L$,
- L est stable par quotient : $\forall (x, y) \in L \times L^\star,\ \frac{x}{y} \in L$.

Remarque. Un sous-corps L de K est donc un sous-anneau de K stable par passage à l'inverse : $\forall x \in L^\star,\ x^{-1} \in L$.