STRUCTURES DE GROUPE ET D'ANNEAU

L'*algèbre* ou théorie des *structures algébriques* est un pan complet des mathématiques, un champ énorme et, pour vous, une vraie nouveauté. L'objectif de ce chapitre est très mince cela dit car il ne contient pratiquement que des définitions. Vous ne saurez pour ainsi dire rien de la théorie des groupes et de la théorie des anneaux en fin de MPSI, ni même en fin de MP si vous allez en MP. Vous saurez en revanche « presque tout » d'une branche importante de l'algèbre qu'on appelle l'*algèbre linéaire*, exclue du présent chapitre mais qui nous occupera longuement par la suite.

Dans tout ce chapitre, $\mathbb{K}$ est l'un des ensembles $\mathbb{R}$ ou $\mathbb{C}$, E est un ensemble quelconque, et $n \in \mathbb{N}^*$.

1 LOIS DE COMPOSITION INTERNES

1.1 MAGMAS

Définition (Loi de composition interne et magma) Soit E un ensemble.

- On appelle *loi (de composition) interne sur E*, ou simplement *loi sur E* toute application de $E \times E$ dans E.
- On appelle *magma* tout couple $(E, \star)$ constitué d'un ensemble E et d'une loi interne $\star$ sur E.

Explication Une loi interne, c'est ce que vous avez souvent appelé une « opération » jusqu'ici, une manière de transformer deux objets d'un certain ensemble en un troisième objet du même ensemble.

Exemple

- $(\mathbb{N}, +)$ et $(\mathbb{N}, \times)$ sont des magmas car l'addition et la multiplication sont bien des applications de $\mathbb{N} \times \mathbb{N}$ DANS $\mathbb{N}$. Plus généralement, si E désigne l'un des ensembles $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$, $(E, +)$ et $(E, \times)$ sont des magmas.
- $(\mathbb{Z}, -)$ est un magma mais pas $(\mathbb{N}, -)$ car la différence de deux entiers naturels n'est pas forcément un entier NATUREL.
- $\left(\mathbb{R}_+^*, \times\right)$ est un magma mais pas $\left(\mathbb{R}_-^*, \times\right)$ car le produit de deux réels négatifs n'est pas un réel négatif.
- $\left(\mathcal{M}_n(\mathbb{K}), +\right)$ et $\left(\mathcal{M}_n(\mathbb{K}), \times\right)$ sont deux magmas car la somme et le produit de deux matrices carrées de taille n est encore une matrice carrée de taille n. Également, $\left(\mathrm{GL}_n(\mathbb{K}), \times\right)$ est un magma car le produit de deux matrices inversibles est encore une matrice inversible — mais ce résultat étant faux pour l'addition, $\left(\mathrm{GL}_n(\mathbb{K}), +\right)$ n'est pas un magma.
- $\left(\mathscr{P}(E), \cup\right)$, $\left(\mathscr{P}(E), \cap\right)$ et $\left(E^E, \circ\right)$ sont trois magmas. En effet, la réunion et l'intersection de deux parties de E sont des parties de E, et la composée de deux applications de E dans E est une application de E dans E.

Explication

- La théorie des magmas est ce domaine des mathématiques — immense ! — qu'on appelle l'*algèbre*, et un magma, c'est ce qu'on obtient quand on *structure* un ensemble à l'aide d'une loi de composition interne. Mais une *structure* c'est quoi exactement ? On emploie souvent ce mot sans lui donner jamais une définition rigoureuse. À l'état brut d'ensemble, par exemple, $\mathbb{R}$ est une collection d'objets donnés sans ordre, en vrac, sans *structure* a priori. La relation d'ordre $\leqslant$ apporte déjà à $\mathbb{R}$ un premier niveau de *structure*, elle en fait un ensemble ordonné. C'est grâce à cette *structure* ordonnée qu'on a coutume de se représenter $\mathbb{R}$ comme une droite. Les opérations $+$ et $\times$ apportent quant à elles à $\mathbb{R}$ un autre type de *structure*, elles le munissent, comme on dit, d'une *structure algébrique*. C'est tout un horizon de calculs possibles qui se trouve ouvert dès lors qu'on s'autorise à additionner et multiplier les réels. Cet ensemble de calculs possibles, c'est cela en quelque sorte qu'on appelle la *structure algébrique* de $\mathbb{R}$. L'ensemble $\mathbb{R}$ serait désertique s'il n'était qu'un ensemble, si aucun calcul n'y était rendu possible par $\leqslant$, $+$ et $\times$.
- On représente parfois les magmas FINIS par des tableaux. Par exemple, pour un ensemble $E = \{a, b, c\}$ à trois éléments muni d'une loi interne $\star$, on pourra résumer entièrement la structure de E par $\star$ au moyen du tableau suivant :

$\star$	a	b	c
a	$a \star a$	$a \star b$	$a \star c$
b	$b \star a$	$b \star b$	$b \star c$
c	$c \star a$	$c \star b$	$c \star c$

1.2 Commutativité et associativité

Définition **(Commutativité et associativité)** Soit $(E,\star)$ un magma.

- On dit que $(E,\star)$ est *associatif* ou que $\star$ est *associative* si : $\forall x,y,z\in E,\quad (x\star y)\star z = x\star(y\star z)$.
- On dit que $(E,\star)$ est *commutatif* ou que $\star$ est *commutative* si : $\forall x,y\in E,\quad x\star y = y\star x$.

Explication

- L'associativité permet d'oublier les parenthésages. Ainsi, calculer : $\big((a\star b)\star(c\star d)\big)\star e$ ou $a\star\Big(\big((b\star c)\star d\big)\star e\Big)$, c'est la même chose, raison pour laquelle le résultat sera simplement noté : $a\star b\star c\star d\star e$.
- L'associativité permet en particulier la définition des *puissances*. Deux notations sont utilisées selon le contexte :
  - **Notation multiplicative :** Pour tous $x\in E$ et $n\in\mathbb{N}^*$, on pose : $x^n = \overbrace{x\star\ldots\star x}^{n\text{ fois}}$.
  - **Notation additive :** Pour tous $x\in E$ et $n\in\mathbb{N}^*$, on pose : $nx = \overbrace{x\star\ldots\star x}^{n\text{ fois}}$. On préfère ici souvent le mot « *multiple* » au mot « puissance », mais c'est au fond la même chose.

  Il ne s'agit là bien sûr que d'une question de NOTATION. Il n'y a pas les lois multiplicatives d'un côté et les lois additives de l'autre. Il y a seulement un point de vue multiplicatif et un point de vue additif sur une même loi donnée. Les deux points de vue sont toujours possibles, mais l'usage veut qu'on en choisisse un et qu'on s'y tienne.

Exemple

- Les magmas $(\mathbb{N},+)$, $(\mathbb{N},\times)$, $(\mathbb{Z},+)$, $(\mathbb{Z},\times)$, $(\mathbb{Q},+)$, $(\mathbb{Q},\times)$, $(\mathbb{R},+)$, $(\mathbb{R},\times)$, $(\mathbb{C},+)$ et $(\mathbb{C},\times)$ sont commutatifs et associatifs.
- Les magmas $\big(\mathcal{M}_n(\mathbb{K}),+\big)$ et $\big(\mathcal{M}_n(\mathbb{K}),\times\big)$ sont associatifs. Le premier est commutatif, mais le second non pour $n\geqslant 2$.
- Les magmas $\big(\mathcal{P}(E),\cup\big)$ et $\big(\mathcal{P}(E),\cap\big)$ sont commutatifs et associatifs.
- Le magma $\big(E^E,\circ\big)$ est associatif, mais non commutatif si E possède au moins eux éléments. En effet, par exemple, si x et y sont deux éléments distints de E et si $f : E\longrightarrow E$ est l'application constante égale à x et $g : E\longrightarrow E$ l'application constante égale à y, alors $f\circ g$ est constante égale à x et $g\circ f$ constante égale à y, donc : $f\circ g\neq g\circ f$.
- Le magma $(\mathbb{Z},-)$ n'est ni commutatif ni associatif car par exemple : $3-1=2$ alors que : $1-3=-1$, et : $(3-1)-1=1$ alors que : $3-(1-1)=3$.

1.3 Élement neutre et éléments inversibles

Définition **(Élément neutre)** Soient $(E,\star)$ un magma et $e\in E$. On dit que e est un *élément neutre de* $(E,\star)$ (ou *pour* $\star$) si : $\forall x\in E,\quad x\star e = e\star x = x$.

Théorème **(Unicité de l'élément neutre)** Soit $(E,\star)$ un magma. Alors E possède au plus un élément neutre.

On peut donc parler, QUAND IL EXISTE, de L'élément neutre de E plutôt que d'« un » élément neutre de E. On le note généralement 1_E ou 1 en notation multiplicative et 0_E ou 0 en notation additive.

Démonstration Si $e,e'\in E$ sont deux éléments neutres pour $\star$, alors : $e = e\star e' = e'$, i.e. $e=e'$. ■

Exemple

- Les magmas $(\mathbb{N},+)$, $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$ et $(\mathbb{C},+)$ admettent 0 pour élément neutre et les magmas $(\mathbb{N},\times)$, $(\mathbb{Z},\times)$, $(\mathbb{Q},\times)$, $(\mathbb{R},\times)$ et $(\mathbb{C},\times)$ le nombre 1. Le magma $(\mathbb{N}^*,+)$, en revanche, ne possède pas d'élément neutre.
- Le magma $\big(\mathcal{M}_n(\mathbb{K}),+\big)$ admet la matrice nulle $0_{n,n}$ pour élément neutre et le magma $\big(\mathcal{M}_n(\mathbb{K}),\times\big)$ la matrice I_n.
- Le magma $\big(\mathcal{P}(E),\cup\big)$ admet $\varnothing$ pour élément neutre, $\big(\mathcal{P}(E),\cap\big)$ l'ensemble E et $\big(E^E,\circ\big)$ l'identité Id_E.

✌ **Explication** ✌ Dans un magma $(E,\star)$ avec élément neutre e, on pose par convention : $x^0 = e$ pour tout $x \in E$ en notation multiplicative et : $0\,x = e$ en notation additive. Cette convention prolonge les relations bien connues : $x^0 = 1$ et $0\,x = 0$ sur les nombres complexes. Par exemple, dans le magma $\big(\mathcal{M}_n(\mathbb{K}),\times\big)$: $M^0 = I_n$ pour tout $M \in \mathcal{M}_n(\mathbb{K})$, et dans le magma $\big(E^E,\circ\big)$: $f^0 = \mathrm{Id}_E$ pour toute application $f : E \longrightarrow E$.

Définition **(Élément inversible)** Soient $(E,\star)$ un magma possédant un élément neutre e et $x \in E$. On dit que x est *inversible dans* $(E,\star)$ (ou *pour* $\star$) s'il existe $x' \in E$, appelé un *inverse de* x, tel que : $x \star x' = x' \star x = e$.

Théorème **(Inversibilité dans un magma associatif avec élément neutre)** Soient $(E,\star)$ un magma associatif possédant un élément neutre e et $x,y,z \in E$.

(i) **Unicité de l'inverse :** Si x est inversible, alors x possède un unique inverse.

On peut donc parler de L'*inverse de* x plutôt que d'« un » inverse. On le note x^{-1} en notation multiplicative et $-x$ en notation additive — on parle plutôt de L'*opposé de* x dans ce cas.

(ii) **Simplification par un élément inversible :** $\begin{cases} \text{Si : } x \star y = x \star z \text{ et si } x \text{ est inversible, alors : } y = z. \\ \text{Si : } y \star x = z \star x \text{ et si } x \text{ est inversible, alors : } y = z. \end{cases}$

(iii) **Inversibilité d'un produit :** Si x et y sont inversibles, $x \star y$ l'est aussi et : $(x \star y)^{-1} = y^{-1} \star x^{-1}$.

(iv) **Puissances négatives :** Pour tout $n \in \mathbb{N}$, si x est inversible alors x^n l'est aussi et : $\big(x^n\big)^{-1} = \big(x^{-1}\big)^n$.
Cet élément est noté x^{-n}. La notation x^k a donc un sens pour tout $k \in \mathbb{Z}$.

(v) **Inversibilité de l'inverse :** Si x est inversible, alors x^{-1} l'est aussi et : $\big(x^{-1}\big)^{-1} = x$.

✖ **Attention !** ✖ Dans l'assertion (iii), si x et y ne commutent pas, il est faux que : $(x\star y)^{-1} = x^{-1}\star y^{-1}$. Rappelez-vous l'histoire du trésor du chapitre « Injections, surjections, bijections » !

Démonstration Les assertions (i), (iii), (iv) et (v) ont été prouvées dans le cas des matrices au chapitre « Matrices et systèmes linéaires » et les preuves ici sont les mêmes. Pour (ii), si : $x \star y = x \star z$ avec x inversible : $y = e \star y = (x^{-1} \star x) \star y = x^{-1} \star (x \star y) = x^{-1} \star (x \star z) = (x^{-1} \star x) \star z = e \star z = z$. ■

Exemple

- Dans $(\mathbb{N},+)$, seul 0 possède un inverse — ou plutôt un opposé. On pourrait se dire que 1 possède aussi un opposé, à savoir -1, mais : $-1 \notin \mathbb{N}$. Dans le monde $(\mathbb{N},+)$, 1 n'a pas d'opposé.
  Dans $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$ et $(\mathbb{C},+)$ au contraire, tout élément possède un opposé.

  Attention, donc : Un élément peut posséder un inverse dans un contexte, mais pas dans un contexte plus restrictif.
- Dans $(\mathbb{N},\times)$, seul 1 possède un inverse. Dans $(\mathbb{Z},\times)$, seuls 1 et -1. Dans $(\mathbb{C},\times)$, tout le monde sauf 0. Dans $(\mathbb{C}^*,\times)$ en revanche, qui est bien un magma, tout élément possède un inverse.
- Dans $\big(\mathcal{M}_n(\mathbb{K}),+\big)$, toute matrice possède un opposé. Dans $\big(\mathcal{M}_n(\mathbb{K}),\times\big)$ au contraire, l'ensemble des matrices inversibles a été noté $\mathrm{GL}_n(\mathbb{K})$ et il n'est pas égal à $\mathcal{M}_n(\mathbb{K})$ tout entier — loin de là.
- On a déjà vu que $\varnothing$ est l'élement neutre de $\big(\mathscr{P}(E),\cup\big)$ et E celui de $\big(\mathscr{P}(E),\cap\big)$.
  - Seul $\varnothing$ possède un inverse pour la réunion, car pour tous $A,B \in \mathscr{P}(E)$, si : $A \cup B = \varnothing$, alors : $A = B = \varnothing$.
  - Seul E possède un inverse pour l'intersection, car pour tous $A,B \in \mathscr{P}(E)$, si : $A \cap B = E$, alors : $A = B = E$.
- Les éléments inversibles du magma $(E^E,\circ)$ sont exactement les bijections de E sur E. Pourquoi ? Être bijectif c'est posséder une réciproque, et une réciproque n'est rien de plus qu'un inverse pour la composition.

1.4 Distributivité d'une loi sur une autre

Définition (Distributivité) Soient E un ensemble et $\star$ et $\square$ deux lois internes sur E. On dit que $\star$ est *distributive sur* $\square$ si :
$$\forall x,y,z\in E,\quad x\star(y\square z)=(x\star y)\square(x\star z)\quad\text{et}\quad(y\square z)\star x=(y\star x)\square(z\star x).$$

Exemple

- Dans $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ et $\mathcal{M}_n(\mathbb{K})$, la multiplication est distributive sur l'addition.
- Réunion et intersection sont distributives l'une sur l'autre dans $\mathcal{P}(E)$. Pour tous $A,B,C\in\mathcal{P}(E)$:
$$A\cup(B\cap C)=(A\cup B)\cap(A\cup C)\quad\text{et}\quad(A\cap B)\cup C=(A\cup C)\cap(B\cup C)\quad\text{(distributivité de }\cup\text{ sur }\cap)$$
$$\text{et}\quad A\cap(B\cup C)=(A\cap B)\cup(A\cap C)\quad\text{et}\quad(A\cup B)\cap C=(A\cap C)\cup(B\cap C)\quad\text{(distributivité de }\cap\text{ sur }\cup).$$

1.5 Parties stables par une loi

Définition (Partie stable par une loi) Soient $(E,\star)$ un magma et A une partie de E. On dit que A est *stable par* $\star$ si :
$$\forall a,a'\in A,\quad a\star a'\in A.$$
Dans ces conditions, $(A,\star)$ est lui-même un magma, si l'on note encore $\star$ la restriction de $\star$ à $A\times A$.

✌ **Explication** ✌ Dire que A est stable par $\star$, c'est dire que A fonctionne en vase clos dans E. Les calculs qu'on effectue via $\star$ sur des éléments de A ne sortent jamais de A, A est comme un sous-monde autonome à l'intérieur de E.

Exemple

- Dans $\mathbb{C}$, les parties $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ et $\mathbb{R}$ sont à la fois stables par addition et stables par produit.
- Dans $\mathcal{M}_n(\mathbb{K})$, nous avons vu que l'ensemble des matrices diagonales, l'ensemble des matrices triangulaires supérieures et l'ensemble $\mathrm{GL}_n(\mathbb{K})$ des matrices inversibles sont tous trois stables par produit.
- Soit $k\in\mathbb{N}$. Dans $\mathcal{P}(E)$, l'ensemble des parties de E qui ont au plus k éléments est stable par intersection. Également, l'ensemble $\mathcal{P}(E)\setminus\{\varnothing\}$ des parties non vides de E est stable par réunion.
- Dans E^E, l'ensemble des applications constantes est stable par composition. Dans $\mathbb{R}^{\mathbb{R}}$, l'ensemble des fonctions croissantes est stable par composition.

✖ **Attention !** ✖ Soient $(E,\star)$ un magma et A une partie de E stable par $\star$. L'intérêt de la stabilité, c'est qu'alors $(A,\star)$ est lui aussi un magma. Cela dit, les propriétés de $(E,\star)$ sont-elles transmises intactes à $(A,\star)$? Réponse : ça dépend.

- Si $(E,\star)$ est commutatif, alors oui, $(A,\star)$ l'est aussi car qui peut le plus peut le moins — s'il est vrai que : $x\star y=y\star x$ pour **tous** $x,y\in E$, c'est bien sûr aussi vrai pour tous $x,y\in A$.
- Le même raisonnement vaut pour l'associativité — si $(E,\star)$ est associatif, $(A,\star)$ l'est aussi.
- Attention en revanche, $(E,\star)$ peut posséder un élément neutre sans que $(A,\star)$ en possède un — pensez à $(\mathbb{N},+)$ et $(\mathbb{N}^*,+)$.
- Également, un élément de A peut être inversible dans $(E,\star)$ sans l'être dans $(A,\star)$ — pensez à 2 dans $(\mathbb{Q},\times)$ et $(\mathbb{Z},\times)$.

2 Structure de groupe

2.1 Groupe

Définition (Groupe) On appelle *groupe* tout magma associatif possédant un élément neutre et dans lequel tout élément est inversible.

🐰 **Explication** 🐰

- Généralement, quand on introduit un groupe $(G,\star)$ abstrait, on omet volontairement de mentionner la loi $\star$ pour alléger les notations. On dit alors simplement : « Soit G un groupe ». Par convention, on note alors généralement multiplicativement la loi de G, et même on se contente de noter xx' le produit de x et x'.
- Dans un groupe, tout élément étant inversible, on peut toujours simplifier facilement. Par exemple, en vertu d'une multiplication à gauche par a^{-1} : $\quad ab=ac \quad\Longrightarrow\quad b=c$.

Exemple

- $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$ et $(\mathbb{C},+)$ sont des groupes commutatifs, de même de $(\mathbb{Q}^*,\times)$, $(\mathbb{R}^*,\times)$, $(\mathbb{C}^*,\times)$, $(\mathbb{Q}_+^*,\times)$ et $(\mathbb{R}_+^*,\times)$. En revanche, $(\mathbb{Z}^*,\times)$ n'est pas un groupe car 2 par exemple n'a pas d'inverse ENTIER.
- $\big(\mathcal{M}_n(\mathbb{K}),+\big)$ est un groupe commutatif, mais pas $\big(\mathcal{M}_n(\mathbb{K}),\times\big)$ car toute matrice n'y est pas inversible. Le magma $\big(\mathrm{GL}_n(\mathbb{K}),\times\big)$, en revanche, est quant à lui un groupe, mais non commutatif si $n\geqslant 2$. Voilà pourquoi on appelle $\mathrm{GL}_n(\mathbb{K})$ un GROUPE linéaire !

✖ ATTENTION ! ✖ $(\mathbb{Q},\times)$, $(\mathbb{R},\times)$ et $(\mathbb{C},\times)$ ne sont pas des groupes car 0 n'est pas inversible pour la multiplication. Désormais, quand on parlera du groupe $\mathbb{C}$, il s'agira toujours du groupe $(\mathbb{C},+)$, et quand on parlera du groupe $\mathbb{C}^*$, il s'agira toujours du groupe $(\mathbb{C}^*,\times)$ — même chose avec $\mathbb{R}$ et $\mathbb{Q}$. De la même manière, quand on parlera du groupe $\mathcal{M}_n(\mathbb{K})$, il s'agira toujours du groupe $\big(\mathcal{M}_n(\mathbb{K}),+\big)$, et quand on parlera du groupe $\mathrm{GL}_n(\mathbb{K})$, il s'agira toujours du groupe $\big(\mathrm{GL}_n(\mathbb{K}),\times\big)$. IL N'Y A AUCUNE AMBIGUÏTÉ ICI ET VOUS DEVEZ EN ÊTRE ABSOLUMENT CONVAINCUS.

Définition (Permutation, groupe symétrique) Soit E un ensemble non vide.

- On appelle *permutation de E* toute bijection de E sur E.
- On appelle *groupe symétrique de E* l'ensemble des permutations de E, noté S_E. Le magma $\big(S_E,\circ\big)$ est un groupe d'élément neutre Id_E.

Démonstration Conséquence des propriétés du magma $\big(E^E,\circ\big)$ démontrées dans les exemples précédents. ■

2.2 Sous-groupe

Définition (Sous-groupe) Soient G un groupe et H une partie de G STABLE PAR PRODUIT. On dit que H est un *sous-groupe de G* si H est un groupe pour la loi de G.

🐰 **Explication** 🐰 Un sous-groupe, c'est un groupe dans un autre groupe — pour la même loi.

Théorème (Élément neutre et inverses dans un sous-groupe) Soient G un groupe et H un sous-groupe de G.

(i) $1_G\in H$. (ii) H est *stable par passage à l'inverse* : $\forall h\in H,\quad h^{-1}\in H$.

✌ **Explication** ✌ Ce théorème répond à un problème un peu subtil. Nous disposons de deux groupes, G et H, dont chacun possède un élément neutre et dans lesquels tout élément est inversible. Deux questions se posent alors :

— H et G ont-ils le même élément neutre ? On pourrait très bien imaginer que non, que : $1_G \notin H$ et que 1_H est neutre vis-à-vis des éléments de H mais pas de tous les éléments de G.

— Pour tout $h \in H$, l'inverse de h dans H et son inverse dans G coïncident-ils ? On pourrait là aussi imaginer que ce n'est pas obligatoire.

Démonstration

(i) Comme 1_H est neutre dans H : $1_H 1_H = 1_H$. Mais 1_G est neutre dans G, donc : $1_H 1_G = 1_H$, donc : $1_H 1_H = 1_H 1_G$. Or on peut simplifier par 1_H car G est un groupe, donc : $1_H = 1_G$, et enfin : $1_G \in H$.

(ii) Soit $h \in H$. Notons h' l'inverse de h dans H pour le distinguer de l'inverse h^{-1} de h dans G. Alors : $h' = h^{-1}$ car : $h' = 1_G h' = (h^{-1}h)h' = h^{-1}(hh') = h^{-1}1_H = h^{-1}1_G = h^{-1}$, donc : $h^{-1} \in H$. ■

Théorème (Caractérisation des sous-groupes) Soient G un groupe et H une partie de G. Les assertions suivantes sont équivalentes :

(i) H est un sous-groupe de G.

(ii)
— $1_G \in H$.
— H est stable par produit et passage à l'inverse, i.e. en résumé : $\forall h, h' \in H, \quad h^{-1}h' \in H$.

✌ **Explication** ✌ En notation additive, l'assertion (ii) s'écrit ainsi :
— $0_G \in H$.
— H est stable par différence, i.e. en résumé : $\forall h, h' \in H, \quad h - h' \in H$.

Démonstration

(i) $\Longrightarrow$ (ii) Si H est un sous-groupe de G, alors H est stable par produit et nous avons vu en outre que : $1_G \in H$ et que H est stable par passage à l'inverse. Bref, pour tout $h, h' \in H$: $h^{-1} \in H$ par stabilité par passage à l'inverse, puis : $h^{-1}h' \in H$ par stabilité par produit.

(ii) $\Longrightarrow$ (i) Faisons l'hypothèse que : $1_G \in H$ et que : $\forall h, h' \in H, \quad h^{-1}h' \in H$ ♣.

— Comme : $1_G \in H$, alors d'après ♣ : $\forall h \in H, \quad h^{-1} = h^{-1}1_G \in H$, i.e. H est stable par passage à l'inverse. En retour, toujours d'après ♣ : $\forall h, h' \in H, \quad hh' = \left(h^{-1}\right)^{-1}h' \in H$, i.e. H est stable par produit.

— Maintenant que H est stable par produit, il nous reste à montrer que H est un groupe pour la loi de G. L'associativité de G est transmise intacte à H — qui peut le plus peut le moins. Ensuite H possède un élément neutre en la personne de 1_G puisque : $1_G \in H$. Enfin tout élément de H est inversible puisque H est stable par passage à l'inverse. ■

✎ **En pratique** ✎

- C'est **TOUJOURS** le résultat précédent qu'il faut utiliser pour montrer qu'une partie d'un groupe en est un sous-groupe. Si on utilisait la **DÉFINITION** des sous-groupes, on serait obligé de parler d'associativité et d'inversibilité à chaque fois, alors que la **CARACTÉRISATION** en fait l'économie.
- Pour montrer qu'un certain ensemble H muni d'une certaine loi est un groupe, il suffit souvent de montrer que H est un **SOUS**-groupe d'un autre groupe connu. Pas besoin donc de revenir à la définition des groupes avec associativité, élément neutre et inversibles, la caractérisation des sous-groupes est plus économique.

Exemple Pour tout groupe G, G lui-même et $\{1_G\}$ sont deux sous-groupes de G.

Démonstration C'est évident pour G. Pour $\{1_G\}$, cela découle de l'égalité : $1_G 1_G = 1_G$, qui vérifie à elle seule tous les points de la caractérisation des sous-groupes.

Exemple $(\mathbb{Z}, +)$ est un sous-groupe de $(\mathbb{Q}, +)$, qui est lui-même un sous-groupe de $(\mathbb{R}, +)$, qui est lui-même un sous-groupe de $(\mathbb{C}, +)$. De même, $(\mathbb{Q}^*, \times)$ est un sous-groupe de $(\mathbb{R}^*, \times)$, qui est lui-même un sous-groupe de $(\mathbb{C}^*, \times)$.

Exemple $(\mathbb{U},\times)$ est un groupe.

Démonstration Il nous suffit de montrer que $\mathbb{U}$ est un sous-groupe de $\mathbb{C}^*$.

- Pour commencer : $\mathbb{U}\subset\mathbb{C}^*$.
- Ensuite, l'élément neutre de $\mathbb{C}^*$ est 1 et : $|1|=1$, donc : $1\in\mathbb{U}$.
- Enfin, pour tous $u,u'\in\mathbb{U}$: $\left|u^{-1}u'\right|=\left|\dfrac{u'}{u}\right|=\dfrac{|u'|}{|u|}=\dfrac{1}{1}=1$, donc : $u^{-1}u'\in\mathbb{U}$.

Exemple $\mathbb{U}_n$ est un sous-groupe de $\mathbb{U}$.

Démonstration

- Pour commencer : $\mathbb{U}_n\subset\mathbb{U}$, c'est bien connu.
- Ensuite, l'élément neutre de $\mathbb{U}$ est 1 et : $1\in\mathbb{U}_n$.
- Enfin, pour tous $u,u'\in\mathbb{U}_n$: $\left(u^{-1}u'\right)^n=\left(\dfrac{u'}{u}\right)^n=\dfrac{u'^n}{u^n}=\dfrac{1}{1}=1$, donc : $u^{-1}u'\in\mathbb{U}_n$.

Exemple L'ensemble $\mathcal{T}^+$ des matrices triangulaires supérieures de $\mathcal{M}_n(\mathbb{K})$ à coefficients diagonaux non nuls est un sous-groupe de $\mathrm{GL}_n(\mathbb{K})$.

Démonstration

- Pour commencer : $\mathcal{T}^+\subset\mathrm{GL}_n(\mathbb{K})$, c'est bien connu.
- Ensuite, l'élément neutre de $\mathrm{GL}_n(\mathbb{K})$ est I_n et : $I_n\in\mathcal{T}^+$.
- Enfin, pour tous $T,T'\in\mathcal{T}^+$: $T^{-1}T'\in\mathcal{T}^+$ — conséquence de deux théorèmes importants du chapitre « Matrices et systèmes linéaires ».

Exemple Soient E un ensemble non vide et $x\in E$. L'ensemble $\mathrm{Stab}(x)=\left\{\sigma\in S_E/\ \sigma(x)=x\right\}$ est un sous-groupe de S_E.

Démonstration

- Pour commencer : $\mathrm{Stab}(x)\subset S_E$.
- Ensuite, Id_E est l'élément neutre de S_E et : $\mathrm{Id}_E(x)=x$, donc : $\mathrm{Id}_E\in\mathrm{Stab}(x)$.
- Enfin, soient $\sigma,\sigma'\in\mathrm{Stab}(x)$. Montrons que : $\sigma^{-1}\circ\sigma'\in\mathrm{Stab}(x)$. Or : $\sigma(x)=x$, donc : $\sigma^{-1}(x)=x$. Comme $\sigma'(x)=x$: $\sigma^{-1}\circ\sigma'(x)=\sigma^{-1}(x)=x$, donc en effet : $\sigma^{-1}\circ\sigma'\in\mathrm{Stab}(x)$.

2.3 Groupe produit

Définition (Groupe produit) Soient G_1 et G_2 deux groupes. On définit une loi de composition interne sur l'ensemble $G_1\times G_2$ en posant pour tous $(x_1,x_2),(x_1',x_2')\in G_1\times G_2$: $(x_1,x_2)(x_1',x_2')=(x_1x_1',x_2x_2')$. Muni cette loi, $G_1\times G_2$ est un groupe d'élément neutre $(1_{G_1},1_{G_2})$ appelé le *groupe produit de G_1 et G_2*.

Le principe de cette construction se généralise sans difficulté au produit d'une famille quelconque de groupes.

Démonstration

- **Associativité :** Pour tous $(x_1,x_2),(x_1',x_2'),(x_1'',x_2'')\in G_1\times G_2$:

$$(x_1,x_2)\Big((x_1',x_2')(x_1'',x_2'')\Big)=(x_1,x_2)(x_1'x_1'',x_2'x_2'')=(x_1x_1'x_1'',x_2x_2'x_2'')=(x_1x_1',x_2x_2')(x_2'',x_2'')=\Big((x_1,x_2)(x_1',x_2')\Big)(x_1'',x_2'').$$

- **Élément neutre :** Pour tout $(x_1,x_2)\in G_1\times G_2$:

$$(1_{G_1},1_{G_2})(x_1,x_2)=\left(1_{G_1}x_1,1_{G_2}x_2\right)=(x_1,x_2)\quad\text{et}\quad(x_1,x_2)(1_{G_1},1_{G_2})=\left(x_11_{G_1},x_21_{G_2}\right)=(x_1,x_2).$$

- **Inversibles :** Soit $(x_1,x_2)\in G_1\times G_2$. Montrons que (x_1,x_2) est inversible d'inverse $\left(x_1^{-1},x_2^{-1}\right)$.

$$(x_1,x_2)\left(x_1^{-1},x_2^{-1}\right)=\left(x_1x_1^{-1},x_2x_2^{-1}\right)=(1_{G_1},1_{G_2})\quad\text{et}\quad\left(x_1^{-1},x_2^{-1}\right)(x_1,x_2)=\left(x_1^{-1}x_1,x_2^{-1}x_2\right)=(1_{G_1},1_{G_2}).$$ ■

Exemple Le produit de deux éléments (x,u) et (x',u') dans le groupe produit $\mathbb{R}\times\mathbb{U}$ est donné par la relation suivante :

$$(x,u)(x',u')=(x+x',uu')\qquad\text{car }\mathbb{R}\text{ est un groupe pour la loi }+\text{ et }\mathbb{U}\text{ un groupe pour la loi }\times.$$

3 Structure d'anneau

3.1 Anneau

Définition (Anneau) On appelle *anneau* tout triplet $(A,+,\times)$ constitué d'un ensemble A et de deux lois de composition internes sur A — une loi $+$ appelée *addition* et une loi $\times$ appelée *multiplication* — soumises aux conditions suivantes :

— $(A,+)$ est un groupe commutatif dont l'élément neutre est traditionnellement noté 0_A ou 0,

— $(A,\times)$ est un magma associatif possédant un élément neutre traditionnellement noté 1_A ou 1,

— la multiplication $\times$ est distributive par rapport à l'addition $+$.

Si le magma $(A,\times)$ est commutatif, on dit en outre que l'anneau $(A,+,\times)$ est *commutatif*.

✌ **Explication** ✌ Comme avec les groupes, on allège souvent les notations. Quand on écrit « Soit A un anneau », il est sous-entendu que l'addition est notée $+$ et la multiplication $\times$ — mais souvent on omet le $\times$. Pour tout $a\in A$, rappelons que : $na=\underbrace{a+\ldots+a}_{n\text{ fois}}$ et $a^n=\underbrace{a\times\ldots\times a}_{n\text{ fois}}$ si $n\in\mathbb{N}$, et $na=\underbrace{(-a)+\ldots+(-a)}_{-n\text{ fois}}$ si $n\in\mathbb{Z}\setminus\mathbb{N}$.

Exemple $(\mathbb{Z},+,\times)$, $(\mathbb{Q},+,\times)$, $(\mathbb{R},+,\times)$ et $(\mathbb{C},+,\times)$ sont des anneaux commutatifs.

Exemple $\big(\mathcal{M}_n(\mathbb{K}),+,\times\big)$ est un anneau. Nous savons que cet anneau n'est pas commutatif pour $n\geqslant 2$, mais jusqu'où n'est-il pas commutatif ? Réponse : les matrices *scalaires*, i.e. de la forme λI_n avec $\lambda\in\mathbb{K}$, sont les seules de $\mathcal{M}_n(\mathbb{K})$ qui commutent à TOUTE matrice de $\mathcal{M}_n(\mathbb{K})$.

Démonstration Les matrices scalaires commutent à toute matrice. Réciproquement, soit $M\in\mathcal{M}_n(\mathbb{K})$ une matrice qui commute à toute matrice. Pour tous $i,j\in[\![1,n]\!]$, notons E_{ij} la matrice dont les coefficients sont tous nuls sauf le coefficient de position (i,j), égal à 1. Par hypothèse sur M : $ME_{ij}=E_{ij}M$, donc après calcul :

$$\begin{pmatrix} & m_{1i} & \\ & \vdots & \\ 0 & m_{ii} & 0 \\ & \vdots & \\ & m_{ni} & \end{pmatrix}=\begin{pmatrix} & 0 & \\ & \vdots & \\ m_{j1} & m_{jj} & m_{jn} \\ & \vdots & \\ & 0 & \end{pmatrix},$$

égalité matricielle dans laquelle on n'a représenté que la $i^{\text{ème}}$ ligne et la $j^{\text{ème}}$ colonne.

En position (i,j), on obtient : $m_{ii}=m_{jj}$. Les autres positions montrent que la $j^{\text{ème}}$ ligne et la $i^{\text{ème}}$ colonne de M sont nulles sauf éventuellement sur la diagonale. Comme c'est vrai pour tous $i,j\in[\![1,n]\!]$, on a bien montré que : $M=\lambda I_n$ avec : $\lambda=m_{11}$ par exemple.

Théorème (Règles de calcul dans un anneau) Soient A un anneau et $a,b\in A$.

(i) $a\times 0_A=0_A\times a=0_A$.

(ii) Pour tout $n\in\mathbb{Z}$: $n(ab)=(na)b=a(nb)$. En particulier : $-(ab)=(-a)b=a(-b)$.

(iii) $(-a)(-b)=ab$. En particulier : $(-1_A)^2=1_A$.

(iv) Pour tout $n\in\mathbb{N}$, si a et b COMMUTENT :

$$(a+b)^n=\sum_{k=0}^{n}\binom{n}{k}a^kb^{n-k}\quad\text{(formule du binôme)}\qquad\text{et}\qquad a^n-b^n=(a-b)\sum_{k=0}^{n-1}a^kb^{n-k-1}.$$

✖ **Attention !** ✖ Dans (iv), l'hypothèse selon laquelle A et B commutent est essentielle, c'est déjà très clair pour $k=2$:

$$(a+b)^2=(a+b)(a+b)=a^2+ab+ba+b^2\overset{ab=ba}{=}a^2+2ab+b^2\qquad\text{et}\qquad(a+b)(a-b)=a^2-ab+ba-b^2\overset{ab=ba}{=}a^2-b^2.$$

Démonstration

(i) Partant de la relation : $a\times 0_A+a\times 0_A=a\times(0_A+0_A)=a\times 0_A$, on simplifie par $a\times 0_A$ dans le groupe $(A,+)$: $a\times 0_A=0_A$. De même : $0_A\times a=0_A$.

(ii) Conséquence de la distributivité pour $n \in \mathbb{N}$: $n(ab) = \overbrace{ab + \ldots + ab}^{n \text{ fois}} = a\left(\overbrace{b + \ldots + b}^{n \text{ fois}}\right) = a(nb)$.
Pour $n = -1$: $ab + a(-b) = a(b-b) = a \times 0_A \overset{\text{(i)}}{=} 0_A$, donc : $-(ab) = a(-b)$.
Finalement, pour $n \in \mathbb{Z}$ négatif, nous pouvons utiliser les cas déjà traité puisque $-n \in \mathbb{N}$:

$$n(ab) = (-n)\big(-(ab)\big) = (-n)\big((-a)b\big) = \big((-n)(-a)\big)b = (na)b.$$

(iii) $(-a)(-b) - (ab) \overset{\text{(ii)}}{=} (-a)(-b) + (-a)b = (-a)(-b+b) = (-a) \times 0_A \overset{\text{(i)}}{=} 0_A$.

(iv) Même preuve que lorsqu'on travaille avec des nombres complexes. ■

Dans un anneau A, est-il possible d'avoir : $0_A = 1_A$? Si c'est le cas, pour tout $a \in A$: $a = a \times 1_A = a \times 0_A = 0_A$, donc : $A = \{0_A\}$. Un tel anneau est qualifié d'*anneau nul*. Ce sont là les anneaux les moins intéressants des mathématiques.

Définition **(Anneau intègre)** Soit A un anneau. On dit que A est *intègre* si A est NON NUL et si :

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

ou encore, par contraposition, si : $\forall a, b \in A, \quad \big(a \neq 0_A \text{ et } b \neq 0_A \implies ab \neq 0_A\big)$.

✖ ATTENTION ! ✖ Tout anneau n'est pas intègre. Et que se passe-t-il quand un anneau N'EST PAS intègre ? Il N'EST alors PAS forcément vrai que pour tous $a, b, x, y \in A$:

$$ax = ay \implies a = 0_A \text{ ou } x = y \qquad \text{NI que :} \qquad a^2 = b^2 \implies a = b \text{ ou } a = -b.$$

Exemple

- Les anneaux $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$, heureusement, sont intègres.
- L'anneau $\mathcal{M}_n(\mathbb{K})$ en revanche, hélas, ne l'est pas pour $n \geqslant 2$. Nous savons en effet que le produit de matrices non nulles peut être nul — par exemple : $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$.

Par définition, tout anneau est en particulier un groupe pour son addition, donc quand on parle des éléments inversibles d'un anneau, c'est toujours aux ÉLÉMENTS INVERSIBLES POUR LA MULTIPLICATION qu'on fait référence.

Théorème **(Groupe des inversibles d'un anneau)** Soit A un anneau. L'ensemble des éléments inversibles de A est un groupe pour la multiplication, souvent noté $U(A)$.

Démonstration Pour une fois, nous ne pouvons pas montrer que $U(A)$ est un SOUS-groupe d'un groupe connu plus gros car nous n'avons pas de groupe connu plus gros à proposer.

- Comme le produit de deux inversibles de A est encore un inversible de A, $U(A)$ est stable par produit. En résumé, $\big(U(A), \times\big)$ est un magma.
- La multiplication est associative sur A, donc a fortiori sur $U(A)$ — qui peut le plus peut le moins.
- Ensuite : $1_A 1_A = 1_A$, donc 1_A est inversible dans A, donc $U(A)$ contient 1_A — élément neutre.
- L'inverse d'un inversible de A étant inversible dans A, tout élément de $U(A)$ est inversible DANS $U(A)$. ■

Exemple $U(\mathbb{Z}) = \{-1, 1\}$, $U(\mathbb{Q}) = \mathbb{Q}^*$, $U(\mathbb{R}) = \mathbb{R}^*$, $U(\mathbb{C}) = \mathbb{C}^*$ et $U\big(\mathcal{M}_n(\mathbb{K})\big) = \mathrm{GL}_n(\mathbb{K})$.

3.2 Sous-anneaux

Définition (Sous-anneau) Soient A un anneau et B une partie de A **stable par addition et produit**. On dit que B est un *sous-anneau de A* si B **contient** 1_A et si B est un anneau pour les lois de A.

Exemple

- Pour tout anneau A, A est un sous-anneau de A.
- $\mathbb{Z}$ est un sous-anneau de $\mathbb{Q}$, qui est lui-même un sous-anneau de $\mathbb{R}$, qui est lui-même un sous-anneau de $\mathbb{C}$.
- $\mathcal{M}_n(\mathbb{R})$ est un sous-anneau de $\mathcal{M}_n(\mathbb{C})$.

Théorème (Caractérisation des sous-anneaux) Soient A un anneau et B une partie de A. Les assertions suivantes sont équivalentes :

- B est un sous-anneau de A.
- $\left\{\begin{array}{l} — \ 1_A \in B. \\ — \ B \text{ est stable par différence.} \\ — \ B \text{ est stable par produit.} \end{array}\right.$

Exemple L'ensemble $\{a+ib\}_{a,b\in\mathbb{Z}}$, noté $\mathbb{Z}[i]$, est un sous-anneau de $\mathbb{C}$ appelé l'*anneau des entiers de Gauss*.

Démonstration

- Pour commencer : $\mathbb{Z}[i] \subset \mathbb{C}$.
- Ensuite, $\mathbb{Z}[i]$ contient 1 car : $1 = 1 + 0.i$.
- Pour la stabilité par soustraction et produit, soient $x, x' \in \mathbb{Z}[i]$ donnés sous la forme $x = a+ib$ et $x' = a'+ib'$ avec $a, b, a', b' \in \mathbb{Z}$. Alors : $x'-x \in \mathbb{Z}[i]$ et $xx' \in \mathbb{Z}[i]$ car :
$$x'-x = \underbrace{(a'-a)}_{\in\mathbb{Z}} + i\underbrace{(b'-b)}_{\in\mathbb{Z}} \quad \text{et} \quad xx' = \underbrace{(aa''-bb')}_{\in\mathbb{Z}} + i\underbrace{(ab'+ba')}_{\in\mathbb{Z}}.$$

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

Démonstration Pour commencer : $\mathcal{T} \subset \mathcal{M}_n(\mathbb{K})$. Ensuite : $I_n \in \mathcal{T}$. Enfin, la stabilité par soustraction et produit est un théorème du chapitre « Matrices et systèmes linéaires ».

3.3 Corps

Rappelons encore une fois que les inversibles d'un anneau sont ses inversibles **au sens de la multiplication**.

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

🐰 **Explication** 🐰 L'énorme différence entre un anneau et un corps, c'est que dans un anneau on ne peut pas diviser comme on veut par un élément non nul. Dans un corps c'est possible, en résumé « tout » marche bien, on peut additionner, soustraire, multiplier et diviser — sauf par 0. En particulier, tout corps est un anneau **intègre**, car si : $ab = 0_A$ avec : $a \neq 0_A$, alors : $b = 0_A$ après division par a.

Exemple Les anneaux $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont des corps, mais pas $\mathbb{Z}$ car : $U(\mathbb{Z}) = \{-1, 1\} \neq \mathbb{Z}^*$.

Exemple L'ensemble $\{a+ib\}_{a,b\in\mathbb{Q}}$, noté $\mathbb{Q}(i)$, est un corps.

Démonstration

- On montre que $\mathbb{Q}(i)$ est un sous-anneau de $\mathbb{C}$ — non nul et commutatif — comme on l'a fait pour $\mathbb{Z}[i]$.
- Ensuite, soit $x = a+ib \in \mathbb{Q}(i)$ non nul avec $a, b \in \mathbb{Q}$. L'inverse de x **dans** $\mathbb{C}$ est $x^{-1} = \dfrac{a-ib}{a^2+b^2}$, et comme cet inverse appartient à $\mathbb{Q}(i)$, en fait x est inversible **dans** $\mathbb{Q}(i)$.

4 Construction matricielle du corps des nombres complexes

Nous avons adopté en début d'année un point de vue naïf sur les nombres complexes en acceptant leur existence sans discussion. Ce point de vue naïf est le point de vue à partir duquel on vous a généralement présenté les objets mathématiques jusqu'ici. Qu'il s'agisse de nombres, d'objets géométriques, de limites de fonctions ou d'intégrales, on vous a présenté ces objets comme s'ils allaient de soi en s'appuyant sur votre intuition **sans jamais interroger leur existence**. Ce point de vue naïf n'est en rien critiquable — à chaque âge ses plaisirs — et il est normal que de telles questions ne soient posées qu'à partir d'un certain niveau mathématique.

Il faut d'ailleurs pour commencer bien comprendre pourquoi nous nous posons de telles questions. On vous a d'abord parlé des entiers, les entiers étaient alors tout pour vous. Ensuite vinrent les « nombres à virgule » et les fractions, les nombres négatifs, les réels. Les règles de calcul se sont succédées sans justification, dogmatiques. On vous a répété ensuite que le carré d'un réel était toujours positif, et puis finalement on vous a parlé des nombres complexes, avec qui un carré peut être négatif et même pire. Et si je vous disais aujourd'hui qu'il existe un corps $\mathbb{B}$ plus grand que $\mathbb{C}$ dans lequel un certain élément $\aleph$ vérifie : $\aleph \times 0 = 0 \times \aleph = 1$? Je pourrais vous faire un chapitre entier sur le corps $\mathbb{B}$ sans que vous y trouviez rien à redire dans un premier temps… Tôt ou tard cependant, l'un ou l'une d'entre vous finirait par apercevoir la supercherie, car en réalité le corps $\mathbb{B}$ est **contradictoire** : $0 = 0 \times 1 = 0 \times (0 \times \aleph) = (0 \times 0) \times \aleph = 0 \times \aleph = 1$. Conclusion : le corps $\mathbb{B}$ n'existe pas. En d'autres termes, il ne suffit pas d'annoncer l'existence d'un monde pour que ce monde existe, encore faut-il lui donner vie, le construire effectivement pour lui éviter les affres de la contradiction.

Pour nous aujourd'hui, le point de départ ce sera le corps $\mathbb{R}$, dont nous admettrons qu'il existe sans contradiction avec toutes les propriétés que vous lui connaissez. Sur cette base, nous allons **construire** un corps plus grand $\mathbb{C}$ dans lequel vous reconnaîtrez aisément notre bien-aimé corps des complexes.

Théorème (Une copie matricielle de $\mathbb{R}$ dans $\mathcal{M}_2(\mathbb{R})$)

- L'application $x \overset{\varphi}{\longmapsto} \begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix}$ est une injection de $\mathbb{R}$ dans $\mathcal{M}_2(\mathbb{R})$ et pour tous $x, y \in \mathbb{R}$: $\varphi(x+y) = \varphi(x) + \varphi(y)$ et $\varphi(xy) = \varphi(x)\varphi(y)$, avec de plus : $\varphi(1) = I_2$.
- Muni de ses lois d'addition et de multiplication matricielles, l'image de φ est alors une copie parfaite de $\mathbb{R}$ dans $\mathcal{M}_2(\mathbb{R})$. On identifiera dans la suite de ce paragraphe tout réel x à la matrice $\varphi(x)$, donc en particulier 1 à I_2.

Explication Aussi étonnant que cela puisse paraître, il n'existe pas qu'**un** corps des réels mais déjà **deux** — et en fait une infinité ! L'application φ du théorème est comme un dictionnaire parfait entre le monde $\mathbb{R}$ et un autre petit monde à l'intérieur de $\mathcal{M}_2(\mathbb{R})$. Ce dictionnaire ne nous permet pas d'affirmer que $\mathbb{R}$ coïncide comme ensemble avec son image par φ, mais les règles de transformation de l'addition et de la multiplication par φ montrent que du point de vue de ces lois, tout calcul dans $\mathbb{R}$ a son analogue dans l'image de φ et vice versa. En résumé, $\mathbb{R}$ et son image par φ sont **deux incarnations de la même structure de corps**. À travers φ, le corps $\mathbb{R}$ et son image sont parfaitement interchangeables et c'est cela que nous appelons *identification* quand nous disons que tout réel x peut être identifié à la matrice $\varphi(x)$.

Définition-théorème (Corps $\mathbb{C}$ des nombres complexes)

- On appelle *nombre complexe* toute matrice de la forme $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$ pour certains réels a et b appelés respectivement *partie réelle* et *partie imaginaire*.
- L'ensemble des nombres complexes, noté $\mathbb{C}$, est un sous-anneau de $\mathcal{M}_2(\mathbb{R})$ et même un corps appelé le *corps des nombres complexes*. Via l'identification précédente, $\mathbb{C}$ contient par ailleurs $\mathbb{R}$ comme sous-anneau.
- On pose en particulier : $\mathrm{i} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, et là, surprise : $\mathrm{i}^2 = -1$.
  Avec cette notation, pour tous $a, b \in \mathbb{R}$: $\begin{pmatrix} a & -b \\ b & a \end{pmatrix} = aI_2 + b\mathrm{i} = a + \mathrm{i}b$.

Explication Ce théorème de construction de $\mathbb{C}$ est vraiment fait pour être oublié. Qu'il y ait un théorème, c'est important, c'est cela qui nous garantit l'existence du corps $\mathbb{C}$. Le caractère matriciel de sa construction ne présente en revanche aucun intérêt et nous continuerons de penser $\mathbb{C}$ seulement en termes de forme algébrique « $a + \mathrm{i}b$ ».

Démonstration Nous allons montrer que $\mathbb{C}$ est un sous-anneau de $\mathcal{M}_2(\mathbb{R})$. Pour montrer que c'est même un corps, nous aurons à prouver en plus la commutativité de la loi $\times$ sur $\mathbb{C}$ et l'inversibilité pour cette loi de tout élément non nul.

- Pour commencer : $\mathbb{C} \subset \mathcal{M}_2(\mathbb{R})$.

- Ensuite, $\mathbb{C}$ contient $I_2 = \begin{pmatrix} 1 & -0 \\ 0 & 1 \end{pmatrix}$.
- Pour la stabilité par différence et produit, soient $M = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}, N = \begin{pmatrix} c & -d \\ d & c \end{pmatrix} \in \mathbb{C}$ avec $a,b,c,d \in \mathbb{R}$.
  Alors : $M - N = \begin{pmatrix} a-c & -(b-d) \\ b-d & a-c \end{pmatrix} \in \mathbb{C}$ et $MN = \begin{pmatrix} ac-bd & -(ad+bc) \\ ad+bc & ac-bd \end{pmatrix} \in \mathbb{C}$.
  Pour la commutativité de $\times$, il n'est pas dur de vérifier que : $MN = NM$.
- Soit enfin $M = \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \in \mathbb{C} \setminus \{0\}$ avec $a,b \in \mathbb{R}$. Comme $M \neq 0$: $a \neq 0$ ou $b \neq 0$, donc : $\det(M) = a^2 + b^2 > 0$, ce qui montre l'inversibilité de M **dans** $\mathcal{M}_2(\mathbb{R})$. Or nous voulons l'inversibilité de M **dans** $\mathbb{C}$, il nous faut donc vérifier que l'inverse M^{-1} de M dans $\mathcal{M}_2(\mathbb{R})$ est élément de $\mathbb{C}$. Tout simplement : $M^{-1} = \dfrac{1}{a^2+b^2}\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in \mathbb{C}$. ■

Exemple Pour tout $\theta \in \mathbb{R}$, l'exponentielle $e^{i\theta}$ s'écrit matriciellement : $e^{i\theta} = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$. Il est alors intéressant d'observer que pour tous $\varphi, \psi \in \mathbb{R}$, l'identité : $e^{i(\varphi+\psi)} = e^{i\varphi}e^{i\psi}$ a pour traduction matricielle :

$$\begin{pmatrix} \cos(\varphi+\psi) & -\sin(\varphi+\psi) \\ \sin(\varphi+\psi) & \cos(\varphi+\psi) \end{pmatrix} = \begin{pmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{pmatrix}\begin{pmatrix} \cos\psi & -\sin\psi \\ \sin\psi & \cos\psi \end{pmatrix}.$$

5 Introduction à l'arithmétique modulaire

Le contenu de ce paragraphe est tout à fait hors programme — vous y reviendrez en MP si vous allez en MP — mais si vous n'avez pas été convaincus par le charme de l'algèbre après le peu de choses que nous en avons dites, un peu d'exotisme ne vous fera pas de mal.

Définition (Anneau $\frac{\mathbb{Z}}{n\mathbb{Z}}$) Soit $n \in \mathbb{N}^*$.

- On note $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ l'ensemble quotient de $\mathbb{Z}$ par la relation d'équivalence $\equiv\ [n]$, i.e. l'ensemble des classes d'équivalence de $\mathbb{Z}$ pour cette relation : $\dfrac{\mathbb{Z}}{n\mathbb{Z}} = \Big\{n\mathbb{Z}, n\mathbb{Z}+1, \dots, n\mathbb{Z}+n-1\Big\}$, ensemble à n éléments.
  Pour tout $x \in \mathbb{Z}$, la classe d'équivalence de x sera notée $\overline{x}$ plutôt que $n\mathbb{Z}+x$.
- Pour tous $x,y,x',y' \in \mathbb{Z}$, si : $\overline{x} = \overline{x'}$ et $\overline{y} = \overline{y'}$, alors : $\overline{x+y} = \overline{x'+y'}$ et $\overline{x \times y} = \overline{x' \times y'}$. Ces égalités montrent qu'on définit deux lois internes $+$ et $\times$ sur $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ en posant : $\overline{x}+\overline{y} = \overline{x+y}$ et $\overline{x} \times \overline{y} = \overline{x \times y}$.
  Alors $\left(\dfrac{\mathbb{Z}}{n\mathbb{Z}}, +, \times\right)$ est un anneau commutatif d'éléments neutres $\overline{0}$ pour $+$ et $\overline{1}$ pour $\times$.

Explication

- Les relations : $\overline{x+y} = \overline{x'+y'}$ et $\overline{x \times y} = \overline{x' \times y'}$ sont indispensables à la bonne définition des nouvelles lois $+$ et $\times$. En effet, pour définir par exemple $\overline{2}+\overline{3}$ dans $\dfrac{\mathbb{Z}}{7\mathbb{Z}}$, j'ai bien envie de poser sans réfléchir : $\overline{2}+\overline{3} = \overline{2+3} = \overline{5}$, sauf que $\overline{2}$ vaut aussi $\overline{16}$ et $\overline{3}$ vaut aussi $\overline{-4}$, alors pourquoi ne pas poser aussi : $\overline{2}+\overline{3} = \overline{16+(-4)} = \overline{12}$? Il serait ici catastrophique que $\overline{2+3}$ et $\overline{16+(-4)}$ ne soient pas égaux, mais ouf, la relation : $\overline{x+y} = \overline{x'+y'}$ nous dit qu'ils le sont.
- Géométriquement, $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ est ce qu'on obtient quand on enroule $\mathbb{Z}$ sur une bobine de périmètre n — les points qui diffèrent d'un multiple de n se trouvent alors placés au même endroit sur la bobine.

Démonstration

- **Bonne définition de $+$ et $\times$:** Soient $x,y,x',y' \in \mathbb{Z}$ tels que : $\overline{x} = \overline{x'}$ et $\overline{y} = \overline{y'}$, i.e. : $x \equiv x'\ [n]$ et $y \equiv y'\ [n]$. Nous savons bien qu'alors : $x+y \equiv x'+y'\ [n]$ et $x \times y \equiv x' \times y'\ [n]$, i.e. : $\overline{x+y} = \overline{x'+y'}$ et $\overline{x \times y} = \overline{x' \times y'}$.

- **Commutativité de $+$:** Pour tous $x,y\in\mathbb{Z}$: $x+y=y+x$ donc : $x+y\equiv y+x\ [n]$, donc : $\overline{x+y}=\overline{y+x}$, i.e. : $\overline{x}+\overline{y}=\overline{y}+\overline{x}$.
- **Associativité de $+$:** Pour tous $x,y,z\in\mathbb{Z}$: $(x+y)+z=x+(y+z)$ donc : $(x+y)+z\equiv x+(y+z)\ [n]$, donc : $\overline{(x+y)+z}=\overline{x+(y+z)}$, i.e. : $(\overline{x}+\overline{y})+\overline{z}=\overline{x}+(\overline{y}+\overline{z})$.
- **Élément neutre pour $+$:** Pour tout $x\in\mathbb{Z}$: $x+0=0+x=x$ donc : $x+0\equiv 0+x\equiv x\ [n]$, donc : $\overline{x+0}=\overline{0+x}=\overline{x}$, i.e. : $\overline{x}+\overline{0}=\overline{0}+\overline{x}=\overline{x}$.
- **Inversibles pour $+$:** Pour tout $x\in\mathbb{Z}$: $x+(-x)=(-x)+x=0$ donc : $x+(-x)\equiv(-x)+x\equiv 0\ [n]$, donc : $\overline{x+(-x)}=\overline{(-x)+x}=\overline{0}$, i.e. : $\overline{x}+\overline{-x}=\overline{-x}+\overline{x}=\overline{0}$. Bref, $\overline{x}$ est inversible pour $+$ d'inverse $\overline{-x}$.

Tout ceci montre que $\left(\frac{\mathbb{Z}}{n\mathbb{Z}},+\right)$ est un groupe commutatif. On procède de même pour montrer que $\left(\frac{\mathbb{Z}}{n\mathbb{Z}},+,\times\right)$ est un anneau commutatif. ■

Exemple L'équation : $\overline{3}x+\overline{2}=\overline{0}$ d'inconnue x admet $\overline{4}$ pour seule solution dans $\frac{\mathbb{Z}}{7\mathbb{Z}}$, et aucune dans $\frac{\mathbb{Z}}{6\mathbb{Z}}$.

Démonstration À ce stade, le plus simple consiste à passer simplement en revue les éléments de $\frac{\mathbb{Z}}{7\mathbb{Z}}$ et $\frac{\mathbb{Z}}{6\mathbb{Z}}$ pour voir lesquels sont solutions et lesquels ne le sont pas.

Théorème (Inversibles de $\frac{\mathbb{Z}}{n\mathbb{Z}}$) Pour tous $n\in\mathbb{N}^*$ et $x\in\mathbb{Z}$: $\overline{x}\in U\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)\iff x\wedge n=1$.

Démonstration
$$\overline{x}\in U\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)\iff\exists\,y\in\mathbb{Z}/\quad\overline{xy}=\overline{yx}=\overline{1}\iff\exists\,y\in\mathbb{Z}/\quad xy\equiv 1\ [n]$$
$$\iff\exists\,y,z\in\mathbb{Z}/\quad xy+nz=1\overset{\text{Bézout}}{\iff}x\wedge n=1.$$ ■

✎ **En pratique** ✎ À retenir : Inverser un élément dans $\frac{\mathbb{Z}}{n\mathbb{Z}}$ revient à calculer une relation de Bézout.

Par exemple, $\overline{8}$ est inversible dans $\frac{\mathbb{Z}}{21\mathbb{Z}}$ car : $8\wedge 21=1$, et par exemple, après calcul : $8\times 8-3\times 21=1$. Réduisons modulo 21 : $\overline{8}\times\overline{8}=\overline{1}$, autrement dit : $\overline{8}^{-1}=\overline{8}$.

Exemple L'équation : $\overline{2}x=\overline{5}$ d'inconnue $x\in\frac{\mathbb{Z}}{37\mathbb{Z}}$ admet $\overline{21}$ pour seule solution.

Démonstration Tâchons ici de ne pas simplement passer en revue tous les éléments de $\frac{\mathbb{Z}}{37\mathbb{Z}}$. Or $\overline{2}$ est inversible dans $\frac{\mathbb{Z}}{37\mathbb{Z}}$ car : $2\wedge 37=1$, et comme $2\times 19-37=1$: $\overline{2}^{-1}=\overline{19}$. Du coup, pour tout $x\in\frac{\mathbb{Z}}{37\mathbb{Z}}$:
$$\overline{2}x=\overline{5}\iff x=\overline{2}^{-1}\overline{5}\iff x=\overline{19}\times\overline{5}\iff x=\overline{21}.$$

L'anneau $\frac{\mathbb{Z}}{4\mathbb{Z}}$ n'est pas intègre, donc ce n'est pas non plus un corps, car : $\overline{2}\times\overline{2}=\overline{0}$ alors que : $\overline{2}\neq\overline{0}$. À quelle condition $\frac{\mathbb{Z}}{n\mathbb{Z}}$ est-il intègre ? est-il un corps ?

Théorème (Intégrité de $\frac{\mathbb{Z}}{n\mathbb{Z}}$) Les assertions suivantes sont équivalentes :

(i) $\frac{\mathbb{Z}}{n\mathbb{Z}}$ est un corps. (ii) $\frac{\mathbb{Z}}{n\mathbb{Z}}$ est intègre. (iii) n est premier.

Démonstration

(i) $\Longrightarrow$ (ii) Tout corps est intègre.

(ii) $\Longrightarrow$ (iii) Par contraposition, montrons que si n n'est pas premier, $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ n'est pas intègre. Or par hypothèse : $n = ab$ pour certains $a, b \in [\![2, n-1]\!]$, donc : $\overline{a}\,\overline{b} = \overline{0}$ alors que : $\overline{a} \neq \overline{0}$ et $\overline{b} \neq \overline{0}$.

(iii) $\Longrightarrow$ (i) Si n est premier, tous les éléments de $[\![1, n-1]\!]$ sont premiers à n, donc seul $\overline{0}$ n'est pas inversible dans $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$. Conclusion : $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ est un corps. ■

Exemple L'équation : $x^2 - \overline{3}x + \overline{7} = \overline{0}$ d'inconnue $x \in \dfrac{\mathbb{Z}}{11\mathbb{Z}}$ admet $-\overline{1}$ et $\overline{4}$ pour solutions.

Démonstration Comme 11 est premier, $\dfrac{\mathbb{Z}}{11\mathbb{Z}}$ est un corps donc un anneau intègre, et : $\overline{2}^{-1} = \overline{6}$. Or pour tout $x \in \dfrac{\mathbb{Z}}{11\mathbb{Z}}$: $x^2 - \overline{3}x + \overline{7} = \left(x - \overline{2}^{-1}\overline{3}\right)^2 - \left(\overline{2}^{-1}\overline{3}\right)^2 + \overline{7} = \left(x - \overline{6}\times\overline{3}\right)^2 - \left(\overline{6}\times\overline{3}\right)^2 + \overline{7} = \left(x - \overline{7}\right)^2 - \overline{9}$, donc :

$$x^2 - \overline{3}x + \overline{7} = \overline{0} \iff \left(x - \overline{7}\right)^2 = \overline{9} \overset{\text{Intégrité}}{\iff} x - \overline{7} = \overline{3} \text{ ou } x - \overline{7} = -\overline{3} \iff x = -\overline{1} \text{ ou } x = \overline{4}.$$

Pour finir, le petit théorème de Fermat a maintenant une expression très simple dans le cadre de l'arithmétique modulaire.

Théorème (Petit théorème de Fermat) Pour tous $p \in \mathbb{P}$ et $x \in \dfrac{\mathbb{Z}}{p\mathbb{Z}}$: $x^p = x$,

et si : $x \neq \overline{0}$, alors : $x^{p-1} = \overline{1}$.