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 non vide et $n \in \mathbb{N}^*$.

1 LOIS DE COMPOSITION INTERNES

1.1 MAGMAS

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

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

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 des applications de $\mathbb{N} \times \mathbb{N}$ **DANS** $\mathbb{N}$.
  Plus généralement, si M désigne l'un des ensembles $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$, $(M, +)$ et $(M, \times)$ sont des magmas.
- $(\mathbb{Z}, -)$ est un magma, mais $-$ n'est pas une loi interne sur $\mathbb{N}$ 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 strictement négatifs n'est jamais 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. En revanche, $+$ n'est pas une loi interne sur $\mathrm{GL}_n(\mathbb{K})$ car, par exemple, la somme d'une matrice inversible et de son opposé — également inversible — est la matrice nulle, qui n'est pas inversible.
- $\left(\mathscr{P}(E), \cup\right)$, $\left(\mathscr{P}(E), \cap\right)$ et $\left(E^E, \circ\right)$ sont des magmas car 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.
- Soient $(M, \star)$ un magma et X un ensemble non vide. Pour toutes applications f et g de X dans M, on note $f \star g$ l'application $x \longmapsto f(x) \star g(x)$ de X dans M. Ainsi défini, le couple $\left(M^X, \star\right)$ est un magma. Notez bien ici que le symbole $\star$ désigne deux lois différentes, une sur M et une sur M^X.

  Cet exemple a l'air abstrait ? Mais non ! Êtes-vous surpris d'apprendre qu'on peut définir la somme et le produit de deux fonctions de $\mathbb{R}$ dans $\mathbb{R}$? Au fond, vous savez bien que $\left(\mathbb{R}^{\mathbb{R}}, +\right)$ et $\left(\mathbb{R}^{\mathbb{R}}, \times\right)$ sont des magmas.

La théorie des magmas est ce domaine des mathématiques — immense ! — qu'on appelle l'*algèbre*, et un magma est ce qu'on obtient quand on *structure* un ensemble à l'aide d'une loi interne. Mais qu'est-ce qu'une *structure* exactement ? On emploie souvent ce mot sans lui donner une définition rigoureuse. À l'état brut d'ensemble, $\mathbb{R}$ est une collection d'objets donnés sans ordre, en vrac, sans structure a priori. La relation d'ordre $\leqslant$ apporte 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 d'une *structure algébrique*. Tout un horizon de calculs possibles 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 $M = \{a,b,c\}$ à trois éléments muni d'une loi interne $\star$, on pourra résumer entièrement la structure de M 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 $(M,\star)$ un magma.

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

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 et le résultat est donc 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 $x\in M$ et $n\in\mathbb{N}^*$, on pose $x^n = x\star\ldots\star x$ (n termes).

— **Notation additive :** Pour tous $x\in M$ et $n\in\mathbb{N}^*$, on pose $nx = x\star\ldots\star x$ (n termes). 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 pas le second 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 deux éléments. En effet, par exemple, si x et y sont deux éléments distincts 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 $f\circ g\neq g\circ f$.
- Soient $(M,\star)$ un magma et X un ensemble non vide.
  — Si $(M,\star)$ est commutatif, $\big(M^X,\star\big)$ l'est aussi. En effet, soient $f,g\in M^X$. Alors $f\star g = g\star f$ car pour tout $x\in X$: $(f\star g)(x) = f(x)\star g(x) = g(x)\star f(x) = (g\star f)(x)$.
  — Si $(M,\star)$ est associatif, $\big(M^X,\star\big)$ l'est aussi. En effet, soient $f,g,h\in M^X$. Alors $(f\star g)\star h = f\star(g\star h)$ car pour tout $x\in X$: $\Big((f\star g)\star h\Big)(x) = (f\star g)(x)\star h(x) = \big(f(x)\star g(x)\big)\star h(x) = f(x)\star\big(g(x)\star h(x)\big) = f(x)\star(g\star h)(x) = \Big(f\star(g\star h)\Big)(x)$.
- 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-théorème **(Élément neutre)** Soient $(M,\star)$ un magma et $e\in M$. On dit que e est un *élément neutre de* $(M,\star)$ (ou *pour* $\star$) si : $\forall x\in M,\quad x\star e = e\star x = x$.

S'IL EN EXISTE UN, un tel élément neutre est unique et on parle de L'élément neutre de M plutôt que d'« un » élément neutre de M. On le note généralement 1_M ou 1 en notation multiplicative et 0_M ou 0 en notation additive.

Démonstration Si $e,e'\in M$ sont deux éléments neutres pour $\star$: $e = e\star e' = e'$, donc $e=e'$.

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 $\big(\mathscr{P}(E),\cup\big)$ admet $\varnothing$ pour élément neutre, $\big(\mathscr{P}(E),\cap\big)$ l'ensemble E et $\big(E^E,\circ\big)$ l'identité Id_E.
- Soient $(M,\star)$ un magma et X un ensemble non vide. Si $(M,\star)$ possède un élément neutre 1_M, l'application constante $x\longmapsto 1_M$ est élément neutre du magma $\big(M^X,\star\big)$. Par exemple, la fonction constante $x\longmapsto 0$ est neutre dans le magma $\big(\mathbb{R}^{\mathbb{R}},+\big)$ et la fonction $x\longmapsto 1$ est neutre dans le magma $\big(\mathbb{R}^{\mathbb{R}},\times\big)$.

Dans un magma $(M,\star)$ associatif avec élément neutre, on pose par convention $x^0=1_M$ pour tout $x\in M$ en notation multiplicative et $0\,x=0_M$ en notation additive. Cette convention prolonge les relations bien connues $x^0=1$ et $0\,x=0$ pour tout $x\in\mathbb{C}$. Par exemple, dans le magma $\big(\mathscr{M}_n(\mathbb{K}),\times\big)$: $M^0=I_n$ pour tout $M\in\mathscr{M}_n(\mathbb{K})$, 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 $(M,\star)$ un magma possédant un élément neutre et $x\in M$. On dit que x est *inversible dans* $(M,\star)$ (ou *pour* $\star$) s'il existe $x'\in M$, appelé un *inverse de* x, pour lequel $x\star x'=x'\star x=1_M$.

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

(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 :** $\begin{cases}\text{Si } x\star y=x\star z \text{ et si } x \text{ est inversible :} & y=z.\\ \text{Si } y\star x=z\star x \text{ et si } x \text{ est inversible :} & y=z.\end{cases}$

(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 : $y=1_M\star y=(x^{-1}\star x)\star y=x^{-1}\star(x\star y)=x^{-1}\star(x\star z)=(x^{-1}\star x)\star z=1_M\star z=z$.

Exemple

- Dans $(\mathbb{N},+)$, seul 0 possède un opposé. Dans $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$ et $(\mathbb{C},+)$ au contraire, tout élément possède un opposé. Par exemple, 1 n'a pas d'opposé dans $(\mathbb{N},+)$, mais il admet -1 pour opposé dans $(\mathbb{Z},+)$.

  Attention, donc : Un élément peut posséder un inverse dans un magma, mais pas dans un magma plus petit.
- 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 $\big(\mathscr{M}_n(\mathbb{K}),+\big)$, toute matrice possède un opposé. Dans $\big(\mathscr{M}_n(\mathbb{K}),\times\big)$ au contraire, l'ensemble des matrices inversibles a été noté $\mathrm{GL}_n(\mathbb{K})$ et il n'est pas égal à $\mathscr{M}_n(\mathbb{K})$ tout entier — loin de là.
- On a déjà vu que $\varnothing$ est l'élément 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 $A\cup B=\varnothing$: $A=B=\varnothing$.
  — Seul E possède un inverse pour l'intersection, car pour tous $A,B\in\mathscr{P}(E)$, si $A\cap B=E$: $A=B=E$.
- Les éléments inversibles du magma $\big(E^E,\circ\big)$ 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.
- Soient $(M,\star)$ un magma associatif avec élément neutre 1_M et X un ensemble non vide. Soit $f\in M^X$. À quelle condition nécessaire et suffisante l'application f est-elle inversible dans $\big(M^X,\circ\big)$? Si f est inversible d'inverse g, alors $f\star g=g\star f=(x\longmapsto 1_M)$, donc $f(x)\star g(x)=g(x)\star f(x)=1_M$ pour tout $x\in X$, donc $f(x)$ est inversible d'inverse $g(x)$. En d'autres termes, f est à valeurs dans l'ensemble des éléments inversibles de $(M,\star)$, et la réciproque est vraie.

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 : $\forall x,y,z\in E,\quad x\star(y\square z)=(x\star y)\square(x\star z)\quad$ 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 $(M,\star)$ un magma et A une partie de M.
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 $\star|_{A\times A}$.

Dire que A est stable par $\star$, c'est dire que A fonctionne en vase clos dans M. 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 M.

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.
- Dans $\mathcal{P}(E)$, l'ensemble des parties de E qui ont au plus k éléments est stable par intersection pour tout $k\in\mathbb{N}$. 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 $(M,\star)$ un magma et A une partie de M stable par $\star$. L'intérêt de la stabilité, c'est qu'alors $(A,\star)$ est lui aussi un magma. Cela dit, les propriétés de $(M,\star)$ sont-elles transmises intactes à $(A,\star)$? Réponse : ça dépend.

- Si $(M,\star)$ 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 $x,y\in M$, c'est bien sûr aussi vrai pour tous $x,y\in A$.
- Le même raisonnement vaut pour l'associativité — si $(M,\star)$ est associatif, $(A,\star)$ l'est aussi.
- En revanche, $(M,\star)$ peut posséder un élément neutre sans que $(A,\star)$ en possède un — pensez à $(\mathbb{N},+)$ et $(\mathbb{N}^*,+)$. Pire que ça, $(M,\star)$ et $(A,\star)$ peuvent posséder chacun un élément neutre, mais pas le même. Par exemple, $\left(\mathcal{M}_2(\mathbb{R}),\times\right)$ admet I_2 pour élément neutre, mais si on note A l'ensemble des matrices $\begin{pmatrix}a&0\\0&0\end{pmatrix}$, a décrivant $\mathbb{R}$, A est une partie de $\mathcal{M}_2(\mathbb{R})$ stable par produit et $(A,\times)$ admet $\begin{pmatrix}1&0\\0&0\end{pmatrix}$ pour élément neutre.
- Également, un élément de A peut être inversible dans $(M,\star)$ 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. Le cardinal d'un groupe fini est généralement appelé son *ordre*.

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} : $\quad ab=ac \iff b=c$.

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. En revanche, $\big(\mathrm{GL}_n(\mathbb{K}),\times\big)$ est un groupe, mais non commutatif pour $n\geqslant 2$. Voilà pourquoi on appelle $\mathrm{GL}_n(\mathbb{K})$ un GROUPE linéaire !
- Soient G un groupe et X un ensemble non vide. L'ensemble G^X des applications de X dans G est un groupe d'après nos exemples précédents. Par exemple, $\big(\mathbb{R}^{\mathbb{R}},+\big)$ est un groupe, qui plus est commutatif.

✖ **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, et *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. ∎

Définition **(Produit de groupes)** Soient $G_1,\dots,G_n$ des groupes. On définit une loi de composition interne sur le produit $G_1\times\dots\times G_n$ en posant pour tous $(x_1,\dots,x_n),(y_1,\dots,y_n)\in G_1\times\dots\times G_n$: $\quad (x_1,\dots,x_n)(y_1,\dots,y_n)=(x_1y_1,\dots,x_ny_n)$. Muni cette loi, $G_1\times\dots\times G_n$ est un groupe d'élément neutre $(1_{G_1},\dots,1_{G_n})$ appelé le *groupe produit de $G_1,\dots,G_n$*.

Démonstration Nous nous contenterons du cas $n=2$ par souci de légèreté.

- **Associativité :** Pour tous $(x_1,x_2),(y_1,y_2),(z_1,z_2)\in G_1\times G_2$:

$$\begin{aligned}(x_1,x_2)\Big((y_1,y_2)(z_1,z_2)\Big)&=(x_1,x_2)(y_1z_1,y_2z_2)=\big(x_1(y_1z_1),x_2(y_2z_2)\big)=\big((x_1y_1)z_1,(x_2y_2)z_2\big)\qquad\text{par associativité de } G_1 \text{ et } G_2\\&=(x_1y_1,x_2y_2)(z_2,z_2)=\Big((x_1,x_2)(y_1,y_2)\Big)(z_1,z_2).\end{aligned}$$

- **Élément neutre :** Pour tout $(x_1,x_2)\in G_1\times G_2$: $\quad (1_{G_1},1_{G_2})(x_1,x_2)=\big(1_{G_1}x_1,1_{G_2}x_2\big)=(x_1,x_2)\quad$ et de même $(x_1,x_2)(1_{G_1},1_{G_2})=\big(x_11_{G_1},x_21_{G_2}\big)=(x_1,x_2)$.
- **Inversibles :** Soit $(x_1,x_2)\in G_1\times G_2$. Montrons que (x_1,x_2) est inversible d'inverse $\big(x_1^{-1},x_2^{-1}\big)$.

$(x_1,x_2)\big(x_1^{-1},x_2^{-1}\big)=\big(x_1x_1^{-1},x_2x_2^{-1}\big)=(1_{G_1},1_{G_2})\quad$ et $\quad\big(x_1^{-1},x_2^{-1}\big)(x_1,x_2)=\big(x_1^{-1}x_1,x_2^{-1}x_2\big)=(1_{G_1},1_{G_2})$. ∎

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

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

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.

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 inversion* : $\forall h \in H,\quad h^{-1} \in H$.

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) 1_H est neutre dans H : $1_H 1_H = 1_H$ et 1_G l'est dans G : $1_H 1_G = 1_H$, 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. Aussitôt $h^{-1} = h' \in H$ car : $h^{-1} = h^{-1}1_G = h^{-1}1_H = h^{-1}(hh') = (h^{-1}h)h' = 1_G h' = h'$. ∎

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) $\begin{cases} — & 1_G \in H. \\ — & H \text{ est stable par produit : } \forall h,h' \in H,\quad hh' \in H. \\ — & H \text{ est stable par inversion : } \forall h \in H,\quad h^{-1} \in H. \end{cases}$ (iii) $\begin{cases} — & 1_G \in H. \\ — & H \text{ est stable par produit-inversion : } \\ & \forall h,h' \in H,\quad h^{-1}h' \in H. \end{cases}$

En notation additive, l'assertion (iii) s'écrit ainsi : $\begin{cases} — & 0_G \in H. \\ — & H \text{ est stable par différence : } \forall h,h' \in H,\quad h-h' \in H. \end{cases}$

Démonstration Nous nous contenterons de démontrer l'équivalence des assertions (i) et (iii).

(i) $\Longrightarrow$ (iii) 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.

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

— Comme $1_G \in H$, d'après ♣ : $\forall h \in H,\quad h^{-1} = h^{-1}1_G \in H$, i.e. H est stable par inversion. 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. ∎

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.

Par ailleurs, 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 $\left\{1_G\right\}$ sont deux sous-groupes de G.

Démonstration C'est évident pour G. Pour $\left\{1_G\right\}$, 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 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 appartient à $\mathbb{U}$ car $|1| = 1$. Enfin, pour la stabilité par produit-inversion : $u^{-1}u' \in \mathbb{U}$ pour tous $u,u' \in \mathbb{U}$ car $\left|u^{-1}u'\right| = \dfrac{|u'|}{|u|} = \dfrac{1}{1} = 1$.

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

Démonstration Il est connu que $\mathbb{U}_n \subset \mathbb{U}$. Ensuite, l'élément neutre de $\mathbb{U}$ est 1 et appartient à $\mathbb{U}_n$ car $1^n = 1$. Enfin, pour la stabilité par produit-inversion : $u^{-1}u' \in \mathbb{U}_n$ pour tous $u, u' \in \mathbb{U}_n$ car $\left(u^{-1}u'\right)^n = \dfrac{u'^n}{u^n} = \dfrac{1}{1} = 1$.

Exemple L'ensemble $\mathcal{T}_n(\mathbb{K})$ des matrices triangulaires supérieures de $\mathcal{M}_n(\mathbb{K})$ à coefficients diagonaux non nuls est un groupe pour le produit matriciel.

Démonstration Il nous suffit de montrer que $\mathcal{T}_n(\mathbb{K})$ est un SOUS-groupe de $\mathrm{GL}_n(\mathbb{K})$. Faites l'effort de bien comprendre en quoi chacune des assertions qui suit découle de nos aventures du chapitre « Matrices et systèmes linéaires ». Pour commencer $\mathcal{T}_n(\mathbb{K}) \subset \mathrm{GL}_n(\mathbb{K})$. Ensuite, l'élément neutre de $\mathrm{GL}_n(\mathbb{K})$ est I_n et appartient à $\mathcal{T}_n(\mathbb{K})$. Enfin, pour la stabilité par produit-inversion : $T^{-1}T' \in \mathcal{T}_n(\mathbb{K})$ pour tous $T, T' \in \mathcal{T}_n(\mathbb{K})$.

Exemple Soient E un ensemble non vide et $x \in E$. L'ensemble $\mathrm{Stab}(x) = \left\{\sigma \in S_E \mid \sigma(x) = x\right\}$ 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 $\sigma^{-1}(x) = x$. En outre $\sigma'(x) = x$, donc $\sigma^{-1} \circ \sigma'(x) = \sigma^{-1}(x) = x$.

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

Démonstration Il n'est pas dur de vérifier que $n\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$ pour tout $n \in \mathbb{N}$.

Réciproquement, soit G un sous-groupe de $\mathbb{Z}$. On veut montrer que $G = n\mathbb{Z}$ pour un certain $n \in \mathbb{N}$, mais quel n ? Pour le comprendre, demandons-nous ce que n représente pour $n\mathbb{Z}$. Réponse : n est le plus petit élément de $n\mathbb{Z}$ à droite de 0. Cela nous donne envie de poser $n = \min\left(G \cap \mathbb{N}^*\right)$... si jamais c'est possible.

- Si $G = \{0\}$, alors $G = 0\mathbb{Z}$ et c'est fini.
- Supposons désormais $G \neq \{0\}$. Le sous-groupe G contient donc un élément non nul, mais comme il est stable par passage à l'opposé, il contient forcément un entier naturel non nul. Ainsi, $G \cap \mathbb{N}^*$ est une partie non vide de $\mathbb{N}$, donc possède un plus petit élément n et nous allons montrer que $G = n\mathbb{Z}$.

  L'inclusion $n\mathbb{Z} \subset G$ vient facilement. En effet, G contient n, donc en tant que sous-groupe, il contient aussi toutes les « puissances » de n, i.e. les entiers nk, k décrivant $\mathbb{Z}$, puisque nous travaillons avec la loi + de $\mathbb{Z}$.

  Montrons enfin que $G \subset n\mathbb{Z}$. Soit $g \in G$. Nous voulons montrer que $g \in n\mathbb{Z}$, i.e. que n divise g. La division euclidienne de g par n s'écrit $g = nq + r$ pour certains $q \in \mathbb{Z}$ et $r \in [\![0, n-1]\!]$. L'entier r n'appartient pas seulement à $[\![0, n-1]\!]$, il appartient aussi à G car il s'écrit $r = g - nq$ avec $n\mathbb{Z} \subset G$. On en déduit par minimalité de n que $r = 0$, ce qui achève de montrer que n divise g.

2.3 Morphisme de groupes

Définition (Morphisme de groupes) Soient $(G, \star)$ et $(G', \square)$ deux groupes. On appelle *morphisme (de groupes) de G dans G'* toute application $f : G \longrightarrow G'$ pour laquelle :

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

Si on omet de noter les lois $\star$ et $\square$, cela revient à dire que : $\forall x, y \in G, \quad f(xy) = f(x)f(y)$.

Lorsque $G = G'$, on dit plutôt que f est un *endomorphisme (de groupe) de G*.

Les morphismes de groupes sont une façon de faire communiquer les groupes entre eux alors qu'on s'est contenté jusqu'ici de les observer individuellement. Un morphisme de groupes f de G dans G' transforme toute relation dans G en une relation analogue dans G'. Par exemple, si $x^2yx = y$ dans G pour certains $x, y \in G$, alors $f(x)^2 f(y) f(x) = f(y)$ dans G'.

Exemple Toute phrase du genre « Le machin des trucs est égal au truc des machins » est le signe certain qu'un morphisme de groupes est dans les parages.

- L'exponentielle complexe est un morphisme de groupes de $\mathbb{C}$ dans $\mathbb{C}^*$ car l'exponentielle d'une somme est égal au produit des exponentielles. Le logarithme est un morphisme de groupes de $\mathbb{R}_+^*$ dans $\mathbb{R}$ car le logarithme d'un produit est égal à la somme des logarithmes.
- La fonction module $z \longmapsto |z|$ est un ENDOmorphisme de groupe de $\mathbb{C}^*$ car le module d'un produit est égal au produit des modules.
- Pour tout $z \in \mathbb{C}$, la fonction $k \longmapsto z^k$ est un morphisme de groupes de $\mathbb{Z}$ dans $\mathbb{C}^*$.
- Pour tout $\alpha \in \mathbb{R}$, la fonction puissance $x \longmapsto x^\alpha$ est un ENDOmorphisme de groupe de $\mathbb{R}_+^*$.
- L'application trace $M \longmapsto \mathrm{tr}(M)$ est un morphisme de groupes de $\mathcal{M}_n(\mathbb{K})$ dans $\mathbb{K}$.

Exemple Soient $(G,+)$ un groupe COMMUTATIF et $n\in\mathbb{N}$. L'application $x\longmapsto nx$ est un ENDOmorphisme de groupe de G car la puissance $n^{\text{ème}}$ d'un produit est égal au produit des puissances $n^{\text{èmes}}$.

Démonstration Pour tous $x,y\in G$, sachant que G est COMMUTATIF :

$$n(x+y)=\underbrace{(x+y)+\ldots+(x+y)}_{n\text{ termes}}=\underbrace{x+\ldots+x}_{n\text{ termes}}+\underbrace{y+\ldots+y}_{n\text{ termes}}=nx+ny.$$

Théorème (Propriétés diverses des morphismes de groupes)

(i) **Éléments neutres et inverses :** Soient G et G' deux groupes et $f:G\longrightarrow G'$ un morphisme de groupes. Alors $f(1_G)=1_{G'}$ et pour tout $x\in G$: $f\left(x^{-1}\right)=f(x)^{-1}$.

(ii) **Composition :** Soient G, G' et G'' trois groupes et $f:G\longrightarrow G'$ et $g:G'\longrightarrow G''$ deux morphismes de groupes. Alors $g\circ f$ est un morphisme de groupes de G dans G''.

(iii) **Images directe et réciproque d'un sous-groupe par un morphisme de groupes :** Soient G et G' deux groupes, $f:G\longrightarrow G'$ un morphisme de groupes, H un sous-groupe de G et H' un sous-groupe de G'. Alors $f(H)$ est un sous-groupe de G' et $f^{-1}(H')$ un sous-groupe de G.

Démonstration

(i) Pour commencer : $f(1_G)f(1_G)=f(1_G1_G)=f(1_G)=f(1_G)1_{G'}$, donc après simplification par $f(1_G)$ à gauche : $f(1_G)=1_{G'}$.

Ensuite, pour tout $x\in G$: $f\left(x^{-1}\right)f(x)=f\left(x^{-1}x\right)=f(1_G)=1_{G'}$ et de même $f(x)f\left(x^{-1}\right)=1_{G'}$, donc $f(x)$ et $f\left(x^{-1}\right)$ sont inverses l'un de l'autre.

(ii) Pour tous $x,y\in G$: $g\circ f(xy)=g\big(f(xy)\big)=g\big(f(x)f(y)\big)=g\big(f(x)\big)\,g\big(f(y)\big)=g\circ f(x)\;g\circ f(y)$.

(iii) Montrons que $f(H)$ est un sous-groupe de G'. D'abord $f(H)\subset G'$. Ensuite $1_{G'}=f(1_G)\in f(H)$ car $1_G\in H$. Enfin, pour la stabilité par produit-inversion, pour tous $y,y'\in f(H)$: $y=f(h)$ et $y'=f(h')$ pour certains $h,h'\in H$, donc $y^{-1}y'=f(h)^{-1}f(h')=f\left(h^{-1}h'\right)$, or H est lui-même stable par produit-inversion, donc $h^{-1}h'\in H$, donc $y^{-1}y'\in f(H)$.

Montrons que $f^{-1}(H')$ est un sous-groupe de G. D'abord $f^{-1}(H')\subset G$. Ensuite $f(1_G)=1_{G'}\in H'$, donc $1_G\in f^{-1}(H')$. Enfin, pour tous $x,x'\in f^{-1}(H')$: $f\left(x^{-1}x'\right)=f(x)^{-1}f(x')\in H'$ car H' est lui-même stable par produit-inversion, donc $x^{-1}x'\in f^{-1}(H')$.

Définition-théorème (Image et noyau d'un morphisme de groupes) Soient G et G' deux groupes et $f:G\longrightarrow G'$ un morphisme de groupes.

- **Image :** L'image de f, notée $\operatorname{Im}f$, est un sous-groupe DE G'.
  En outre, f est surjectif de G sur G' si et seulement si $\operatorname{Im}f=G'$.
- **Noyau :** On appelle *noyau de* f le sous-groupe DE G : $\operatorname{Ker}f=f^{-1}\left(\{1_{G'}\}\right)=\left\{x\in G\mid f(x)=1_{G'}\right\}$.
  En outre, f est injectif sur G si et seulement si $\operatorname{Ker}f=\{1_G\}$.

Le noyau de f est l'ensemble des éléments de G qui ne comptent pas aux yeux de f, qu'elle ne voit pas. En effet, pour tous $x\in G$ et $k\in\operatorname{Ker}f$: $f(xk)=f(x)f(k)=f(x)1_{G'}=f(x)$ et de même $f(kx)=f(x)$.

La caractérisation de l'injectivité par le noyau est a priori surprenante. En principe, f est injectif si TOUT élément de G' possède au plus un antécédent par f, mais quand f est un morphisme de groupes, il suffit que ce soit vrai du seul élément $1_{G'}$.

Pour finir, $\operatorname{Ker}f$ contient 1_G en tant que sous-groupe de G, donc pour montrer que f est injective, il est suffisant de montrer l'INCLUSION $\operatorname{Ker}f\subset\{1_G\}$.

Démonstration Pour commencer, $\operatorname{Im}f=f(G)$ est un sous-groupe de G' en tant qu'image directe d'un sous-groupe de G par un morphisme de groupes et $\operatorname{Ker}f$ est un sous-groupe de G' en tant qu'image réciproque d'un sous-groupe de G'.

À présent, si f est injectif, pour tout $x\in\operatorname{Ker}f$: $f(x)=1_{G'}=f(1_G)$, donc $x=1_G$ par injectivité, ce qui montre bien que $\operatorname{Ker}f\subset\{1_G\}$.

Réciproquement, si $\operatorname{Ker}f=\{1_G\}$, montrons que f est injectif. Soient $x,x'\in G$. Si $f(x)=f(x')$:

$$f\left(x^{-1}x'\right)=f(x)^{-1}f(x')=f(x)^{-1}f(x)=1_{G'},\quad\text{donc } x^{-1}x'\in\operatorname{Ker}f=\{1_G\},\text{ i.e. } x=x'.$$

Exemple

- L'exponentielle complexe $z \longmapsto \mathrm{e}^z$ est surjective de $\mathbb{C}$ sur $\mathbb{C}^*$ de noyau $\left\{z \in \mathbb{C} \mid \quad \mathrm{e}^z = 1\right\} = 2\mathrm{i}\pi\mathbb{Z}$.
- Le module $z \longmapsto |z|$ a pour image $\mathbb{R}_+^*$ et pour noyau $\left\{z \in \mathbb{C}^* \mid \quad |z| = 1\right\} = \mathbb{U}$.
- L'exponentielle imaginaire $\theta \longmapsto \mathrm{e}^{\mathrm{i}\theta}$ est surjective de $\mathbb{R}$ sur $\mathbb{U}$ de noyau $2\pi\mathbb{Z}$.
- Soit $n \in \mathbb{N}^*$. On pose $z = \mathrm{e}^{\frac{2\mathrm{i}\pi}{n}}$. Le morphisme de groupes $k \longmapsto z^k$ de $\mathbb{Z}$ dans $\mathbb{C}^*$ a pour image $\mathbb{U}_n$ et pour noyau :
$$\left\{k \in \mathbb{Z} \mid \quad \mathrm{e}^{\frac{2\mathrm{i}k\pi}{n}} = 1\right\} = \left\{k \in \mathbb{Z} \mid \quad \frac{2k\pi}{n} \equiv 0\,[2\pi]\right\} = \left\{k \in \mathbb{Z} \mid \quad k \equiv 0\,[n]\right\} = n\mathbb{Z}.$$

Définition **(Isomorphisme de groupes)** Soient G et G' deux groupes.

- **Isomorphisme de groupes :** On appelle *isomorphisme (de groupes) de G sur G'* tout morphisme de groupes bijectif de G sur G'.

  Lorsque $G = G'$, on parle plutôt d'*automorphisme (de groupe) de G*.
- **Groupes isomorphes :** On dit que G' est *isomorphe à G (en tant groupe)* s'il existe un isomorphisme de groupes de G sur G'.

« Iso-morphe » provient du grec et signifie « de même forme ». Un isomorphisme de groupes de G sur G' est non seulement une bijection de G sur G', autrement dit un dictionnaire, mais c'est aussi un morphisme de groupes. Aux noms près, tout calcul qu'on peut faire dans G a donc son pendant dans G'. En résumé, deux groupes isomorphes G et G' sont absolument identiques en tant que groupes quand bien même les objets qu'ils accueillent n'ont rien de commun d'un point de vue ensembliste.

Exemple

- Les groupes $\mathbb{R}$ et $\mathbb{R}_+^*$ sont isomorphes car l'exponentielle réelle est un isomorphisme de $\mathbb{R}$ sur $\mathbb{R}_+^*$.
- Pour tout $\alpha \in \mathbb{R}^*$, la fonction puissance $x \longmapsto x^\alpha$ est un AUTOmorphisme de $\mathbb{R}_+^*$ — de réciproque $x \longmapsto x^{\frac{1}{\alpha}}$.

Théorème **(Propriétés des isomorphismes de groupes)**

(i) **Composition :** La composée de deux isomorphismes de groupes est un isomorphismes de groupes.

(ii) **Réciproque :** Soient G et G' deux groupes et $f : G \longrightarrow G'$ un isomorphisme de groupes de G sur G'. Alors f^{-1} est un isomorphisme de groupes de G' sur G.

(iii) **Relation d'isomorphisme :** La relation « être isomorphe à » est une relation d'équivalence sur la classe des groupes.

Démonstration

(i) La composée de deux bijections (resp. morphismes) est une bijection (resp. un morphisme).

(ii) Nous savons déjà que f^{-1} est une bijection de G' sur G. Montrons que c'est un morphisme de groupes. Pour tous $y, y' \in G'$:
$$\begin{aligned} f^{-1}(yy') &= f^{-1}\Big(f\big(f^{-1}(y)\big)\,f\big(f^{-1}(y')\big)\Big) = f^{-1}\Big(f\big(f^{-1}(y)f^{-1}(y')\big)\Big) \\ &= f^{-1} \circ f\Big(f^{-1}(y)f^{-1}(y')\Big) = f^{-1}(y)f^{-1}(y'). \end{aligned}$$

(iii) **Réflexivité :** Pour tout groupe G, Id_G est un automorphisme de G car Id_G est bijective de G sur lui-même et pour tous $x, y \in G$: $\mathrm{Id}_G(xy) = xy = \mathrm{Id}_G(x)\mathrm{Id}_G(y)$.

Transitivité : La composée de deux isomorphismes est un isomorphisme.

Symétrie : La réciproque d'un isomorphisme est un isomorphisme. ∎

Exemple Les groupes $\mathbb{U}_4$ et $\mathbb{U}_2^2 = \mathbb{U}_2 \times \mathbb{U}_2$ sont tous deux d'ordre 4, mais pas isomorphes.

Démonstration Pour commencer : $\mathbb{U}_4 = \{1, -1, \mathrm{i}, -\mathrm{i}\}$ et $\mathbb{U}_2^2 = \big\{(1,1),(1,-1),(-1,1),(-1,-1)\big\}$.
Soit f un morphisme de groupes de $\mathbb{U}_2^2$ dans $\mathbb{U}_4$. Pour tout $(u,v) \in \mathbb{U}_2^2$: $(u,v)^2 = \big(u^2, v^2\big) = (1,1)$, donc $f(u,v)^2 = f\big((u,v)^2\big) = f(1,1) = 1$. Comme $\mathrm{i}^2 = -1$, il en découle que f ne prend pas la valeur i, donc n'est pas surjectif. En résumé, aucun morphisme de groupes de $\mathbb{U}_2^2$ dans $\mathbb{U}_4$ ne peut être un isomorphisme, et comme la réciproque d'un isomorphisme est un isomorphisme, il n'existe pas davantage d'isomorphisme de $\mathbb{U}_4$ sur $\mathbb{U}_2^2$.

Question étrange : combien y a-t-il d'ensembles des réels dans la nature mathématique ? « Bah un seul, quelle question ! » Et pourtant… Notons $\oplus$ la loi du groupe produit $\mathbb{R}\times\{0\}$ définie par $(x,0)\oplus(x',0)=(x+x',0)$ pour tous $x,x'\in\mathbb{R}$. Cette relation fait de l'application $x\longmapsto(x,0)$ un morphisme de groupes de $\mathbb{R}$ dans $\mathbb{R}\times\{0\}$, et même un isomorphisme de $\mathbb{R}$ sur $\mathbb{R}\times\{0\}$. Les groupes $\mathbb{R}$ et $\mathbb{R}\times\{0\}$ sont donc absolument identiques du point de vue de leurs additions respectives. Lequel de ces groupes mérite-t-il donc qu'on l'appelle « L'ensemble des réels », comme s'il n'y en avait qu'un ? Les deux se valent. Il y a autant d'ensembles des réels qu'on veut bien se donner la peine d'en construire **À ISOMORPHISME PRÈS**.

Alors bien sûr, le monde $\mathbb{R}$ n'est pas seulement structuré par son addition, il l'est aussi par sa multiplication et sa relation d'ordre, mais cela ne change rien au fond de l'affaire. Nous avons défini l'algèbre comme la théorie des structures algébriques, i.e. des lois internes. Mais quel est son objectif ? L'algèbre entreprend de *classifier* les structures algébriques. En quel sens ? Les groupes $(\mathbb{R},+)$ et $\big(\mathbb{R}\times\{0\},\oplus\big)$ sont différents en tant qu'ensembles mais parfaitement identiques — isomorphes — comme groupes. Ce sont **DEUX** groupes mais **UNE SEULE** structure représentée par sa *classe d'isomorphisme*. La grande question de la théorie des groupes n'est donc pas « Qui sont tous les groupes ? » mais plus finement « Que sont toutes les classes d'isomorphisme de groupes ? » ou encore « Qui sont tous les groupes **À ISOMORPHISME PRÈS** ? »

Définition-théorème **(Groupe des automorphismes d'un groupe)** Soit G un groupe. L'ensemble $\mathrm{Aut}(G)$ des automorphismes de groupe de G est un groupe pour la composition.

Démonstration Il suffit de montrer que $\mathrm{Aut}(G)$ est un **SOUS**-groupe du groupe symétrique S_G. Pour commencer $\mathrm{Aut}(G)\subset S_G$, ensuite $\mathrm{Id}_G\in\mathrm{Aut}(G)$, et la stabilité par produit-inversion découle du théorème précédent. ∎

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 généralement noté 0_A ou 0,

— $(A,\times)$ est un magma associatif possédant un élément neutre généralement 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*.

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 $\times$ dans les calculs.

Par ailleurs, pour tous $a\in A$ et $n\in\mathbb{N}$: $na=a+\ldots+a$ (n termes) et : $a^n=a\times\ldots\times a$ (n termes), et pour tous $a\in A$ et $n\in\mathbb{Z}\setminus\mathbb{N}$: $na=(-a)+\ldots+(-a)$ ($-n$ termes).

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 **NON** commutatif pour $n\geqslant 2$, mais jusqu'où est-il **NON** 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) : $m_{ii}=m_{jj}$. 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 $i,j\in[\![1,n]\!]$: $M=\lambda I_n$ pour $\lambda=m_{11}$.

Exemple Soient A un anneau et X un ensemble non vide. Nous l'avons vu, les propriétés des magmas $(A,+)$ et $(A,\times)$ se transmettent naturellement aux magmas $\left(A^X,+\right)$ et $\left(A^X,\times\right)$. Il en résulte que $\left(A^X,+,\times\right)$ est un anneau. Par exemple, $\mathbb{R}^{\mathbb{R}}$ est un anneau, qui plus est commutatif car l'anneau $\mathbb{R}$ l'est.

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

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 $n\in\mathbb{N}$: $n(ab)=ab+\ldots+ab=a(b+\ldots+b)=a(nb)$.

Pour $n=-1$: $ab+a(-b)=a(b-b)=a\times 0_A\overset{(i)}{=}0_A$, donc $-(ab)=a(-b)$.

Finalement, pour $n\in\mathbb{Z}$ négatif : $-n\in\mathbb{N}$, donc nous pouvons utiliser les cas déjà traités :

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

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

(iv) Même preuve que dans $\mathbb{C}$.

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 $A=\{0_A\}$. Ce genre d'anneau est qualifié d'*anneau nul*. Les anneaux nuls n'ont à peu près aucun intérêt !

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

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

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

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 $a,b,x,y\in A$:

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

Exemple

- Heureusement, les anneaux $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont intègres.
- L'anneau $\mathcal{M}_n(\mathbb{K})$ N'EST PAS intègre pour $n\geqslant 2$ car un produit de matrices non nulles peut être nul — par exemple $\begin{pmatrix}1&0\\0&0\end{pmatrix}\begin{pmatrix}0&0\\1&0\end{pmatrix}=\begin{pmatrix}0&0\\0&0\end{pmatrix}$.

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 $\mathrm{U}(A)$.

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

Par ailleurs, la preuve qui suit est plus subtile qu'il n'y paraît. Un élément a de $\mathrm{U}(A)$ peut être inversible en deux sens a priori. Il peut l'être dans A : $\exists\, a'\in A,\quad aa'=a'a=1_A$ comme il peut l'être dans $\mathrm{U}(A)$: $\exists\, a'\in\mathrm{U}(A),\quad aa'=a'a=1_A$. Par définition, $\mathrm{U}(A)$ est l'ensemble des éléments de A inversibles DANS A.

- Comme le produit de deux inversibles de A est encore un inversible de A, $\mathrm{U}(A)$ est stable par produit, autrement dit $\big(\mathrm{U}(A),\times\big)$ est un magma.
- La multiplication est associative sur A, donc a fortiori sur $\mathrm{U}(A)$ — qui peut le plus peut le moins.
- Ensuite $1_A 1_A = 1_A$, donc 1_A est inversible dans A, donc $\mathrm{U}(A)$ contient 1_A, qui est neutre.
- Pour finir, pour tout $a \in \mathrm{U}(A)$, a est inversible dans A, donc a^{-1} aussi, ce qui signifie que $a^{-1} \in \mathrm{U}(A)$. Il en découle que a possède un inverse dans $\mathrm{U}(A)$, i.e. qu'il est inversible **DANS** $\mathrm{U}(A)$. Bref, tout élément de $\mathrm{U}(A)$ est inversible **DANS** $\mathrm{U}(A)$.

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

3.2 Sous-anneaux

Notons A l'ensemble des matrices $\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$, a décrivant $\mathbb{R}$, inclus dans $\mathscr{M}_2(\mathbb{R})$.

— Pour commencer, A contient 0 et est stable par différence, donc est un sous-groupe **ADDITIF** de $\mathscr{M}_2(\mathbb{R})$.

— Ensuite, A est stable par produit et admet $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ pour élément neutre **MULTIPLICATIF**.

— Enfin, le produit matriciel est distributif sur l'addition dans $\mathscr{M}_2(\mathbb{R})$, donc dans A.

Conclusion : A est un anneau. Et de plus, A est inclus dans $\mathscr{M}_2(\mathbb{R})$, dont il partage les lois. Tout ceci ne fait-il pas de A ce qu'on pourrait appeler un *sous-anneau de* $\mathscr{M}_2(\mathbb{R})$? Eh bien non, car A et $\mathscr{M}_2(\mathbb{R})$ n'ont pas le même élément neutre. A fortiori, leurs inversibles n'ont aucun rapport.

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 : $1_A \in B$ 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 $\mathbb{C}$.
- $\mathscr{M}_n(\mathbb{R})$ est un sous-anneau de $\mathscr{M}_n(\mathbb{C})$.

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

(i) B est un sous-anneau de A.

(ii)
- $1_A \in B$.
- B est stable par différence : $\forall b, b' \in B,\quad b - b' \in B$.
- B est stable par produit : $\forall b, b' \in B,\quad bb' \in B$.

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

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

Exemple L'ensemble $\mathscr{C}(\mathbb{R},\mathbb{R})$ est un sous-anneau de $\mathbb{R}^{\mathbb{R}}$.

Démonstration Pour commencer $\mathscr{C}(\mathbb{R},\mathbb{R}) \subset \mathbb{R}^{\mathbb{R}}$. Ensuite, la fonction constante égale à 1 est continue sur $\mathbb{R}$. Nous savons bien enfin que la différence et le produit de deux fonctions continues sont continues.

Exemple L'ensemble $\mathscr{C}$ des matrices $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$, a et b décrivant $\mathbb{R}$, est un sous-anneau de $\mathscr{M}_2(\mathbb{R})$.

Démonstration Pour commencer $\mathscr{C} \subset \mathscr{M}_2(\mathbb{R})$. Ensuite $I_2 = \begin{pmatrix} 1 & -0 \\ 0 & 1 \end{pmatrix} \in \mathscr{C}$. Enfin, pour la stabilité par différence et produit, soient $M = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}, N = \begin{pmatrix} c & -d \\ d & c \end{pmatrix} \in \mathscr{C}$ avec $a, b, c, d \in \mathbb{R}$. Alors :

$$M - N = \begin{pmatrix} a-c & -(b-d) \\ b-d & a-c \end{pmatrix} \in \mathscr{C} \qquad \text{et} \qquad MN = \begin{pmatrix} ac-bd & -(ad+bc) \\ ad+bc & ac-bd \end{pmatrix} \in \mathscr{C}.$$

✖ **Attention !** Soient A un anneau et B un sous-anneau de A. Quel lien entre $\mathrm{U}(A)$ et $\mathrm{U}(B)$? Tout élément de $\mathrm{U}(B)$ est inversible DANS B, i.e. possède un inverse dans B, donc en possède un dans A a fortiori. Conclusion : $\mathrm{U}(B) \subset \mathrm{U}(A) \cap B$, MAIS LA RÉCIPROQUE EST FAUSSE ! Il ne suffit pas d'être inversible dans A et élément de B pour être inversible dans B. Par exemple, pour $A = \mathbb{R}$ et $B = \mathbb{Z}$, 2 est inversible dans $\mathbb{R}$ et appartient à $\mathbb{Z}$, mais 2 n'est pas inversible dans $\mathbb{Z}$, son inverse $\frac{1}{2}$ dans $\mathbb{R}$ n'appartient pas à $\mathbb{Z}$.

Exemple L'ensemble $\mathcal{T}_n(\mathbb{K})$ des matrices triangulaires supérieures de $\mathcal{M}_n(\mathbb{K})$ est un sous-anneau de $\mathcal{M}_n(\mathbb{K})$ et $\mathrm{U}\big(\mathcal{T}_n(\mathbb{K})\big)$ est l'ensemble des matrices triangulaires supérieures à coefficients diagonaux non nuls de $\mathcal{M}_n(\mathbb{K})$.

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

À présent, $\mathrm{U}\big(\mathcal{T}_n(\mathbb{K})\big)$ est l'ensemble des matrices triangulaires supérieures inversibles de $\mathcal{M}_n(\mathbb{K})$ dont l'inverse est triangulaire supérieure et on conclut de nouveau grâce au 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.

Dans un anneau, on ne peut pas diviser comme on veut par un élément non nul. Dans un corps au contraire, c'est possible, 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.

Il est même autorisé, dans un corps, d'utiliser la notation fractionnaire $\frac{a}{b}$ pour peu que l'élément b soit non nul. La non-nullité de b garantit son inversibilité, mais $\frac{a}{b}$ pourrait désigner deux choses a priori $b^{-1}a$ et ab^{-1}. Les corps étant commutatifs, ces quantités sont égales et on peut les noter $\frac{a}{b}$ sans danger.

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

Exemple L'ensemble $\big\{a + \mathrm{i}b \mid \quad a, b \in \mathbb{Q}\big\}$, noté $\mathbb{Q}(\mathrm{i})$, est un corps.

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

Exemple L'ensemble $\mathscr{C}$ des matrices $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$, a et b décrivant $\mathbb{R}$, est un corps.

Démonstration Nous avons déjà vu que $\mathscr{C}$ est un sous-anneau de $\mathcal{M}_2(\mathbb{R})$, clairement non nul. Ensuite, l'anneau $\mathcal{M}_2(\mathbb{R})$ n'est pas commutatif, mais il n'est pas dur de vérifier que $\mathscr{C}$ l'est. Pour finir, soit $M = \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \in \mathscr{C}^*$ avec $a, b \in \mathbb{R}$. Comme M est non nulle : $\quad a \neq 0 \quad$ ou $\quad b \neq 0, \quad$ donc $\det(M) = a^2 + b^2 > 0$, donc M est inversible… c'est-à-dire inversible DANS $\mathcal{M}_2(\mathbb{R})$, attention ! Sauf qu'en réalité, nous visons l'inversibilité de M DANS $\mathscr{C}$. Il nous faut donc vérifier que l'inverse M^{-1} de M dans $\mathcal{M}_2(\mathbb{R})$ appartient à $\mathscr{C}$. Or tout simplement $M^{-1} = \frac{1}{a^2 + b^2}\begin{pmatrix} a & b \\ -b & a \end{pmatrix} = \begin{pmatrix} a' & -b' \\ b' & a' \end{pmatrix} \in \mathscr{C}$ si on pose $a' = \frac{a}{a^2 + b^2}$ et $b' = -\frac{b}{a^2 + b^2}$.

3.4 Morphisme d'anneaux

Définition (Morphisme d'anneaux) Soient A et B deux anneaux. On appelle *morphisme (d'anneaux) de A dans B* toute application $f : A \longrightarrow B$ pour laquelle : $\boxed{f(1_A) = 1_B}$ et :

$$\forall a, a' \in A, \quad f(a + a') = f(a) + f(a') \quad \text{et} \quad f(aa') = f(a)f(a').$$

Lorsque $A = B$, on dit plutôt que f est un *endomorphisme (d'anneau) de A*.

En particulier, f est un **MORPHISME DE GROUPES POUR L'ADDITION**, donc d'une part $f(0_A) = 0_B$, et d'autre part, pour tout $a \in A$: $f(-a) = -f(a)$.

En revanche, f n'est pas un morphisme de groupes pour la multiplication car A et B ne sont même pas des groupes ! Cela dit, pour tout $a \in \mathrm{U}(A)$: $f(a)f\left(a^{-1}\right) = f\left(aa^{-1}\right) = f(1_A) = 1_B$ et de même $f\left(a^{-1}\right)f(a) = 1_B$, donc $f(a) \in \mathrm{U}(B)$ et $f\left(a^{-1}\right) = f(a)^{-1}$. En résumé : $f_{|\mathrm{U}(A)}$ est un morphisme de groupes de $\mathrm{U}(A)$ dans $\mathrm{U}(B)$.

Comme dans le cas des groupes, la composée de deux morphismes d'anneaux est un morphisme d'anneaux et l'image directe/réciproque d'un sous-anneau par un morphisme d'anneau est un sous-anneau. On définit également les notions d'*isomorphisme d'anneaux*, d'*automorphisme d'anneau* et d'*anneaux isomorphes*. Il reste vrai que la composée de deux isomorphismes est un isomorphismes et que la réciproque d'un isomorphisme est un isomorphisme.

Exemple La conjugaison complexe $z \longmapsto \overline{z}$ est un automorphisme d'anneau de $\mathbb{C}$.

Démonstration La bijectivité est claire car $\overline{\overline{z}} = z$ pour tout $z \in \mathbb{C}$. Ensuite $\overline{1} = 1$, et pour tous $z, z' \in \mathbb{C}$: $\overline{z+z'} = \overline{z} + \overline{z'}$ et $\overline{zz'} = \overline{z}\,\overline{z'}$.

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 et c'est à partir de ce point de vue naïf qu'on vous a généralement présenté les objets mathématiques jusqu'ici. Nombres, objets géométriques, limites de fonctions, 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 a ses vertus quand on débute — à chaque âge ses plaisirs — et il est normal que de telles questions ne soient posées qu'à partir d'un certain niveau mathématique.

D'ailleurs, pourquoi nous posons-nous de telles questions ? Quand vous étiez petits, on vous a d'abord parlé des entiers et les entiers étaient tout pour vous. Plus tard 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 $\aleph$ satisfait la relation : $\aleph \times 0 = 0 \times \aleph = 1$? 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 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 proprement 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 un morphisme injectif d'anneaux de $\mathbb{R}$ dans $\mathcal{M}_2(\mathbb{R})$. Son image $\mathrm{Im}\,\varphi$ est donc un corps isomorphe à $\mathbb{R}$ inclus 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.

On crée ainsi ex nihilo une copie parfaite de $\mathbb{R}$ à l'intérieur de $\mathcal{M}_2(\mathbb{R})$. Le résultat qui suit a été démontré plus haut.

Définition-théorème (Corps $\mathbb{C}$ des nombres complexes) On appelle *nombre complexe* toute matrice $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$ dans laquelle a et b sont deux réels 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. Via l'identification précédente, $\mathbb{R}$ en est un sous-anneau.

On pose alors $\mathrm{i} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, et là, surprise : $\mathrm{i}^2 = -1$. En outre, pour tous $a, b \in \mathbb{R}$: $\begin{pmatrix} a & -b \\ b & a \end{pmatrix} = aI_2 + b\mathrm{i} = a + \mathrm{i}b$.

Ce théorème de construction de $\mathbb{C}$ est vraiment fait pour être oublié. Qu'il y ait un théorème, c'est important d'un point de vue intellectuel, 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 à $\mathbb{C}$ comme avant. D'autres constructions de $\mathbb{C}$ auraient d'ailleurs pu être proposées.

Une petite douceur pour finir. Nous avons déjà observé que : $\begin{pmatrix}\cos\varphi & -\sin\varphi\\ \sin\varphi & \cos\varphi\end{pmatrix}\begin{pmatrix}\cos\psi & -\sin\psi\\ \sin\psi & \cos\psi\end{pmatrix}=\begin{pmatrix}\cos(\varphi+\psi) & -\sin(\varphi+\psi)\\ \sin(\varphi+\psi) & \cos(\varphi+\psi)\end{pmatrix}$ pour tous $\varphi,\psi\in\mathbb{R}$. Dans le cadre de notre construction matricielle de $\mathbb{C}$, cette identité s'écrit aussi $e^{i\varphi}e^{i\psi}=e^{i(\varphi+\psi)}$ si on pose pour tout $\theta\in\mathbb{R}$: $e^{i\theta}=\begin{pmatrix}\cos\theta & -\sin\theta\\ \sin\theta & \cos\theta\end{pmatrix}=\cos\theta+i\sin\theta$.

5 Groupes symétriques

Pour tout $n\in\mathbb{N}^*$, le groupe symétrique de l'ensemble $[\![1,n]\!]$ est noté S_n plutôt que $S_{[\![1,n]\!]}$.

Les éléments de S_n peuvent être représentés de plusieurs façons. La première consiste à écrire toute permutation σ sous la forme d'une matrice $\begin{pmatrix}1 & 2 & \cdots & n\\ \sigma(1) & \sigma(2) & \cdots & \sigma(n)\end{pmatrix}$. Par exemple, la permutation σ de $[\![1,4]\!]$ définie par les égalités : $\sigma(1)=2$, $\sigma(2)=4$, $\sigma(3)=1$ et $\sigma(4)=3$ est notée $\begin{pmatrix}1 & 2 & 3 & 4\\ 2 & 4 & 1 & 3\end{pmatrix}$. Produit et inversion sont faciles à effectuer à partir de cette représentation. Par exemple, dans S_5 :

$$\begin{pmatrix}1&2&3&4&5\\1&4&2&5&3\end{pmatrix}\begin{pmatrix}1&2&3&4&5\\2&1&4&5&3\end{pmatrix}=\begin{pmatrix}1&2&3&4&5\\4&1&5&3&2\end{pmatrix}\qquad\text{et}\qquad\begin{pmatrix}1&2&3&4&5\\3&5&2&4&1\end{pmatrix}^{-1}=\begin{pmatrix}1&2&3&4&5\\5&3&1&4&2\end{pmatrix}.$$

Pour l'inverse, lisez simplement la matrice de σ du bas vers le haut au lieu de la lire du haut vers le bas.

Définition-théorème (Support d'une permutation, permutations disjointes)

- **Support d'une permutation :** Soit $\sigma\in S_n$. On appelle *support de* σ l'ensemble des éléments de $[\![1,n]\!]$ qui NE sont PAS fixés par σ : $\operatorname{supp}(\sigma)=\big\{x\in[\![1,n]\!]\ |\ \sigma(x)\neq x\big\}$.
- **Permutations disjointes :** On dit que deux permutations de $[\![1,n]\!]$ sont *disjointes* si leurs supports sont disjoints.

  Propriété remarquable : Deux permutations disjointes commutent.

Démonstration Soient $\sigma,\sigma'\in S_n$ disjointes et $x\in[\![1,n]\!]$. Montrons que σ et σ' commutent.

— Si $x\notin\operatorname{supp}(\sigma)$ et $x\notin\operatorname{supp}(\sigma')$, alors $\sigma\sigma'(x)=\sigma(x)=x=\sigma'(x)=\sigma'\sigma(x)$.

— Supposons maintenant que $x\in\operatorname{supp}(\sigma)$ — on traiterait de même le cas où $x\in\operatorname{supp}(\sigma')$.
Comme σ et σ' sont disjointes : $x\notin\operatorname{supp}(\sigma')$, donc $\sigma'(x)=x$, donc $\sigma\sigma'(x)=\sigma(x)$.
Ensuite $\sigma(x)\neq x$ et σ est injective, donc $\sigma\big(\sigma(x)\big)\neq\sigma(x)$, donc $\sigma(x)\in\operatorname{supp}(\sigma)$, or σ et σ' sont disjointes, donc $\sigma'\sigma(x)=\sigma(x)$. Finalement $\sigma\sigma'(x)=\sigma(x)=\sigma'\sigma(x)$.

Dans tous les cas $\sigma\sigma'(x)=\sigma'\sigma(x)$, donc comme c'est vrai pour tout $x\in[\![1,n]\!]$: $\sigma\sigma'=\sigma'\sigma$.

Exemple La permutation $\begin{pmatrix}1&2&3&4&5\\2&4&3&1&5\end{pmatrix}$ admet $\{1,2,4\}$ pour support.

Définition (Cycle, transposition)

- **Cycle :** Soit $p\in[\![2,n]\!]$. On appelle *p-cycle de* $[\![1,n]\!]$ ou *cycle de longueur p de* $[\![1,n]\!]$ toute permutation σ de $[\![1,n]\!]$ pour laquelle il existe des éléments distincts $x_1,\dots,x_p$ de $[\![1,n]\!]$ pour lesquels :
$$\sigma(x_1)=x_2,\qquad\sigma(x_2)=x_3,\qquad\dots\qquad\sigma(x_{p-1})=x_p\qquad\text{et}\qquad\sigma(x_p)=x_1$$
$$\text{et}\qquad\sigma(x)=x\qquad\text{si } x\text{ n'est aucun des éléments } x_1,\dots,x_p.$$
  Un tel p-cycle est alors noté $(x_1\ x_2\ \dots\ x_p)$, ou $(x_2\ x_3\ \dots\ x_p\ x_1)$, ou $(x_3\ x_4\ \dots\ x_p\ x_1\ x_2)$, etc.
- **Transposition :** Un 2-cycle de $[\![1,n]\!]$ est aussi appelé une *transposition de* $[\![1,n]\!]$.

Exemple Tâchons de décrire explicitement les groupes S_2 et S_3. Mais pour commencer : $|S_n|=n!$ car construire une permutation σ de $[\![1,n]\!]$ revient à choisir $\sigma(1)$ dans $[\![1,n]\!]$ (n possibilités), puis $\sigma(2)$ dans $[\![1,n]\!]\setminus\{\sigma(1)\}$ ($n-1$ possibilités), puis $\sigma(3)$ dans $[\![1,n]\!]\setminus\{\sigma(1),\sigma(2)\}$ ($n-2$ possibilités), …, et enfin $\sigma(n)$ (une seule possibilité). Et maintenant :
$$S_2=\big\{\mathrm{Id}\ ,\ (1\ 2)\big\},\qquad S_3=\big\{\mathrm{Id}\ ,\ (1\ 2),\ (1\ 3)\ ,\ (2\ 3)\ ,\ (1\ 2\ 3)\ ,\ (3\ 2\ 1)\big\}.$$

En composant des cycles entre eux, on obtient de nouvelles permutations, mais pas forcément des cycles.

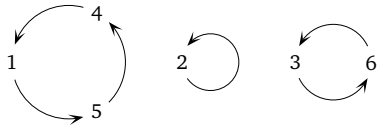
Exemple Dans S_4 : $(2\ 3)\ (4\ 3\ 1)\ (4\ 2\ 3)=\begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix}=(1\ 4\ 3\ 2)$. Ici, on obtient encore un cycle.

Démonstration $\big((2\ 3)\circ(4\ 3\ 1)\circ(4\ 2\ 3)\big)(1)=\big((2\ 3)\circ(4\ 3\ 1)\big)(1)=\big((2\ 3)\big)(4)=4$
et : $\big((2\ 3)\circ(4\ 3\ 1)\circ(4\ 2\ 3)\big)(2)=\big((2\ 3)\circ(4\ 3\ 1)\big)(3)=\big((2\ 3)\big)(1)=1$, etc.

Inversement, toute permutation peut être décomposée comme un produit de cycles disjoints.

Exemple Dans S_6 : $\begin{pmatrix}1&2&3&4&5&6\\5&2&6&1&4&3\end{pmatrix} = (1\ 5\ 4)\ (3\ 6) = (3\ 6)\ (1\ 5\ 4)$ et les cycles $(1\ 5\ 4)$ et $(3\ 6)$ sont disjoints.

Démonstration La permutation de gauche agit circulairement sur certains paquets d'éléments. Elle envoie ainsi 1 sur 5, 5 sur 4 et 4 sur 1, elle fixe 2, et enfin elle envoie 3 sur 6 et 6 sur 3. C'est exactement ce que fait aussi la permutation $(1\ 5\ 4)\ (3\ 6) = (3\ 6)\ (1\ 5\ 4)$ — d'où l'égalité.



Théorème (Décomposition d'une permutation en produit de cycles disjoints) Toute permutation de $[\![1,n]\!]$ peut être décomposée d'une et une seule manière — à l'ordre des facteurs près — comme un produit de cycles disjoints.

Disjoints, les cycles en jeu commutent, donc l'ordre dans lequel on les écrit n'a pas d'importance.

Démonstration Nous prouverons seulement l'existence d'une telle décomposition. Soit $\sigma \in S_n$. On définit une relation $\sim$ sur $[\![1,n]\!]$ de la manière suivante — pour tous $x, y \in [\![1,n]\!]$: $x \sim y \iff \exists k \in \mathbb{Z},\ y = \sigma^k(x)$.

- La relation $\sim$ ainsi définie est une relation d'équivalence. En effet, soient $x, y, z \in [\![1,n]\!]$.
  - **Réflexivité :** $x = \mathrm{Id}(x) = \sigma^0(x)$, donc $x \sim x$.
  - **Symétrie :** Si $x \sim y$, alors $y = \sigma^k(x)$ pour un certain $k \in \mathbb{Z}$, donc $x = \sigma^{-k}(y)$, i.e. $y \sim x$.
  - **Transitivité :** Si $x \sim y$ et $y \sim z$, alors $y = \sigma^k(x)$ et $z = \sigma^l(y)$ pour certains $k, l \in \mathbb{Z}$, donc $z = \sigma^{k+l}(x)$, i.e. $x \sim z$.

  Notons alors $X_1, \dots, X_r$ les classes d'équivalence de $[\![1,n]\!]$ pour $\sim$ et choisissons x_1 dans X_1, …, x_r dans X_r. Par définition, pour tout $i \in [\![1,n]\!]$: $X_i = \left\{\sigma^k(x_i) \mid k \in \mathbb{Z}\right\}$.
- Soit $i \in [\![1,r]\!]$. Comme X_i est un ensemble fini : $\sigma^k(x_i) = \sigma^l(x_i)$ pour certains $k, l \in \mathbb{N}$ pour lesquels $k < l$, et donc $\sigma^{l-k}(x_i) = x_i$. Nous pouvons dès lors noter p_i le plus entier naturel non nul pour lequel $\sigma^{p_i}(x_i) = x_i$. Il n'est alors pas trop dur de se convaincre que $X_i = \left\{x_i, \sigma(x_i), \dots, \sigma^{p_i-1}(x_i)\right\}$ avec $|X_i| = p_i$ — via une petite division euclidienne par p_i.
- Pour tout $i \in [\![1,r]\!]$, notons finalement σ_i le p_i-cycle $\left(x_i\ \sigma(x_i)\ \dots\ \sigma^{p_i-1}(x_i)\right)$ de support X_i. Ce sont là r cycles disjoints et pour tout $i \in [\![1,r]\!]$: $\sigma_i|_{X_i} = \sigma|_{X_i}$ et $\sigma_i|_{[\![1,n]\!]\setminus X_i} = \mathrm{Id}_{[\![1,n]\!]\setminus X_i}$. Il en découle que $\sigma = \sigma_1 \dots \sigma_r$ et c'est bien une telle décomposition qu'on cherchait.

Exemple Quelques exemples sur lesquels vous pouvez vous entraîner : $(1\ 2\ 3\ 4\ 5\ 6)\ (1\ 2\ 4\ 6)\ (1\ 3\ 5) = (1\ 4)\ (2\ 5\ 3\ 6)$, $(1\ 2\ 4\ 6)\ (2\ 5)\ (3\ 4\ 1) = (1\ 3\ 6)\ (2\ 5\ 4)$, $(1\ 3)\ (3\ 2\ 1\ 4)\ (3\ 1\ 4)\ (2\ 1\ 4) = (1\ 2)\ (3\ 4)$, $(4\ 5\ 1\ 2)\ (3\ 4\ 1\ 6)\ (5\ 4\ 1\ 6)\ (4\ 2) = (1\ 3\ 5\ 2\ 6)$.

Théorème (Le groupe symétrique est engendré par ses transpositions) Toute permutation de $[\![1,n]\!]$ peut être décomposée comme un produit de transpositions.

En d'autres termes, quand on doit permuter n objets — quelle que soit la complexité apparente de la permutation — on peut TOUJOURS le faire progressivement par des échanges de deux objets.

Démonstration Grâce au théorème précédent, il nous suffit d'établir le résultat dans le seul cas des cycles. Or tout simplement, pour tous $x_1, \dots, x_p \in [\![1,n]\!]$ distincts : $(x_1\ \dots\ x_p) = (x_1\ x_2)\ (x_2\ x_3)\ \dots\ (x_{p-1}\ x_p)$, donc en effet tout cycle est un produit de transpositions.

Attention, la décomposition d'une permutation en produit de transpositions N'EST PAS DU TOUT unique, par exemple : $(1\ 2\ 3) = (1\ 2)\ (2\ 3) = (1\ 3)\ (1\ 2)$. À défaut d'unicité, cela dit, deux décompositions en produit de transpositions d'une même permutation n'ont-elles rien de commun ? Nous allons voir que si. Deux décompositions de ce genre ne font pas forcément intervenir les mêmes nombres p et p' de transpositions, MAIS p et p' ont TOUJOURS la même parité.

Définition-théorème (Signature)

- **Signature :** Il existe un et un seul morphisme de groupes ε de S_n dans $\left\{-1, 1\right\}$ qui donne à toute transposition la valeur -1. On l'appelle la *signature* de S_n.
- **Permutation paire/impaire :** Pour tout $\sigma \in S_n$, on dit que σ est *paire* si $\varepsilon(\sigma) = 1$ et *impaire* si $\varepsilon(\sigma) = -1$.

En dépit du mystère qui l'entoure, la signature sera pour nous un allié précieux en fin d'année au chapitre « Déterminants ».

Démonstration

- Notons $\mathscr{P}$ l'ensemble des paires $\{i,j\}$ d'entiers $i,j\in[\![1,n]\!]$ distincts, et pour toute permutation $\sigma\in S_n$, μ_σ l'application $\left\{\begin{array}{ccc}\mathscr{P}&\longrightarrow&\mathscr{P}\\ \{i,j\}&\longmapsto&\{\sigma(i),\sigma(j)\}\end{array}\right.$, bijective de réciproque $\mu_{\sigma^{-1}}$. Cette bijectivité nous autorise à effectuer le changement d'indice $\{u,v\}=\mu_\sigma\big(\{i,j\}\big)$: $\displaystyle\prod_{\{i,j\}\in\mathscr{P}}|\sigma(j)-\sigma(i)|=\prod_{\{u,v\}\in\mathscr{P}}|v-u|=\prod_{\{i,j\}\in\mathscr{P}}|j-i|$. Le produit $\displaystyle\prod_{\{i,j\}\in\mathscr{P}}\frac{\sigma(j)-\sigma(i)}{j-i}$ vaut donc ±1, notons-le $\varepsilon(\sigma)$.
- Montrons que ε est un morphisme de groupes. Pour tous $\sigma,\sigma'\in S_n$:

$$\varepsilon(\sigma\sigma')=\prod_{\{i,j\}\in\mathscr{P}}\frac{\sigma\sigma'(j)-\sigma\sigma'(i)}{j-i}=\prod_{\{i,j\}\in\mathscr{P}}\frac{\sigma\sigma'(j)-\sigma\sigma'(i)}{\sigma'(j)-\sigma'(i)}\times\prod_{\{i,j\}\in\mathscr{P}}\frac{\sigma'(j)-\sigma'(i)}{j-i}$$
$$=\prod_{\{u,v\}\in\mathscr{P}}\frac{\sigma(v)-\sigma(u)}{v-u}\times\prod_{\{i,j\}\in\mathscr{P}}\frac{\sigma'(j)-\sigma'(i)}{j-i}=\varepsilon(\sigma)\varepsilon(\sigma')\qquad\text{après le changement d'indice }\{u,v\}=\mu_{\sigma'}\big(\{i,j\}\big).$$

- Soit $\tau=(a\ b)\in S_n$ une transposition avec $a<b$. Pour montrer l'égalité $\varepsilon(\tau)=-1$, nous allons simplement passer en revue les uns après les autres les termes du produit $\varepsilon(\tau)=\displaystyle\prod_{\{i,j\}\in\mathscr{P}}\frac{\tau(j)-\tau(i)}{j-i}$.
  - Si $\{i,j\}\in\mathscr{P}$ ne contient ni a ni b : $\dfrac{\tau(j)-\tau(i)}{j-i}=\dfrac{j-i}{j-i}=1$.
  - Pour tout $i\in[\![1,n]\!]$ distinct de a et b, regroupons les termes d'indices $\{i,a\}$ et $\{i,b\}$. Leur contribution au produit vaut $\dfrac{\tau(a)-\tau(i)}{a-i}\times\dfrac{\tau(b)-\tau(i)}{b-i}=\dfrac{b-i}{a-i}\times\dfrac{a-i}{b-i}=1$.
  - Pour finir, le terme d'indice $\{a,b\}$ vaut -1 car $\dfrac{\tau(b)-\tau(a)}{b-a}=\dfrac{a-b}{b-a}=-1$.

  Conclusion : $\varepsilon(\tau)=-1$ par produit.
- Pour l'unicité de la signature sur S_n, soient η et η' deux applications de S_n dans $\{-1,1\}$ qui satisfont la conclusion du théorème. Pour tout $\sigma\in S_n$, disons $\sigma=\tau_1\dots\tau_p$ où $\tau_1,\dots,\tau_p$ sont des transpositions : $\eta(\sigma)=\eta(\tau_1)\dots\eta(\tau_p)=(-1)^p=\eta'(\tau_1)\dots\eta'(\tau_p)=\eta'(\tau_1\dots\tau_p)=\eta'(\sigma)$, donc $\eta=\eta'$. ∎

Théorème (Signature d'un cycle) Soit $p\in[\![2,n]\!]$. La signature d'un p-cycle de $[\![1,n]\!]$ est $(-1)^{p-1}$.

Démonstration Pour tous $x_1,\dots,x_p\in[\![1,n]\!]$ distincts : $(x_1\ \dots\ x_p)=(x_1\ x_2)\,(x_2\ x_3)\ \dots\ (x_{p-1}\ x_p)$ et cette décomposition fait intervenir $p-1$ transpositions, donc $\varepsilon\big((x_1\ \dots\ x_p)\big)=(-1)^{p-1}$. ∎

Exemple $(1\ 5\ 3)\,(2\ 4\ 6\ 1)\,(3\ 4)$ est une permutation paire.

Démonstration $\varepsilon\big((1\ 5\ 3)\,(2\ 4\ 6\ 1)\,(3\ 4)\big)=\varepsilon\big((1\ 5\ 3)\big)\,\varepsilon\big((2\ 4\ 6\ 1)\big)\,\varepsilon\big((3\ 4)\big)=(-1)^{3-1}(-1)^{4-1}(-1)^{2-1}=1$.

6 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 $n\in\mathbb{N}^*$. La relation $\equiv\ [n]$ est une relation d'équivalence sur $\mathbb{Z}$ et nous noterons $\overline{x}$ la classe d'équivalence de x pour cette relation pour tout $x\in\mathbb{Z}$. Concrètement, pour tous $x,y\in\mathbb{Z}$: $\overline{x}=n\mathbb{Z}+x$, et surtout : $\overline{x}=\overline{y}\iff x\equiv y\ [n]$.

On note alors $\frac{\mathbb{Z}}{n\mathbb{Z}}$ l'ensemble quotient de $\mathbb{Z}$ par $\equiv\ [n]$: $\dfrac{\mathbb{Z}}{n\mathbb{Z}}=\big\{\overline{0},\overline{1},\dots,\overline{n-1}\big\}$, i.e. l'ensemble des classes d'équivalence de $\mathbb{Z}$ pour cette relation. Le résultat est un ensemble de cardinal n.

Pour tous $x_1,x_2,y_2,y_2\in\mathbb{Z}$, si $\overline{x_1}=\overline{x_2}$ et $\overline{y_1}=\overline{y_2}$: $\overline{x_1+y_1}=\overline{x_2+y_2}$ et $\overline{x_1\times y_1}=\overline{x_2\times y_2}$. Ces égalités définissent deux lois internes $+$ et $\times$ sur $\frac{\mathbb{Z}}{n\mathbb{Z}}$ si on pose pour tous $x,y\in\mathbb{Z}$: $\overline{x}+\overline{y}=\overline{x+y}$ et $\overline{x}\times\overline{y}=\overline{x\times y}$. Le triplet $\left(\frac{\mathbb{Z}}{n\mathbb{Z}},+,\times\right)$ est finalement un anneau commutatif d'éléments neutres $\overline{0}$ pour $+$ et $\overline{1}$ pour $\times$.

C'est subtil, mais les relations : $\overline{x_1+y_1}=\overline{x_2+y_2}$ et $\overline{x_1\times y_1}=\overline{x_2\times y_2}$ sont indispensables à la bonne définition des nouvelles lois $+$ et $\times$. Pour définir par exemple $\overline{2}+\overline{3}$ dans $\frac{\mathbb{Z}}{7\mathbb{Z}}$, j'ai bien envie de poser $\overline{2}+\overline{3}=\overline{2+3}=\overline{5}$, mais $\overline{2}$ vaut aussi $\overline{16}$ et $\overline{3}$ vaut aussi $\overline{17}$, alors pourquoi ne pas poser $\overline{2}+\overline{3}=\overline{16+17}=\overline{12}$? Il serait catastrophique que $\overline{2+3}$ et $\overline{16+17}$ ne soient pas égaux. Par chance, la relation $\overline{x_1+y_1}=\overline{x_2+y_2}$ nous dit qu'ils le sont.

La définition des lois de $\frac{\mathbb{Z}}{n\mathbb{Z}}$ signifie que l'application $x\longmapsto\overline{x}$ est un morphisme surjectif d'anneaux de $\mathbb{Z}$ sur $\frac{\mathbb{Z}}{n\mathbb{Z}}$.

Démonstration Nous montrerons seulement que $\left(\frac{\mathbb{Z}}{n\mathbb{Z}},+\right)$ est un groupe commutatif, mais il n'est pas plus difficile de montrer que c'est un anneau commutatif. Fixons une fois pour toutes $x_1,x_2,y_1,y_2,x,y,z\in\mathbb{Z}$.

- **Bonne définition de $+$ et $\times$:** On suppose que $\overline{x_1}=\overline{x_2}$ etd $\overline{y_1}=\overline{y_2}$, i.e. que : $x_1\equiv x_2\ [n]$ et $y_1\equiv y_2\ [n]$. Nous savons bien qu'alors : $x_1+y_1\equiv x_2+y_2\ [n]$ et $x_1\times y_1\equiv x_2\times y_2\ [n]$, i.e. : $\overline{x_1+y_1}=\overline{x_2+y_2}$ et $\overline{x_1\times y_1}=\overline{x_2\times y_2}$.
- **Commutativité de $+$:** $\overline{x}+\overline{y}=\overline{x+y}=\overline{y+x}=\overline{y}+\overline{x}$.
- **Associativité de $+$:** $\left(\overline{x}+\overline{y}\right)+\overline{z}=\overline{x+y}+\overline{z}=\overline{(x+y)+z}=\overline{x+(y+z)}=\overline{x}+\overline{y+z}=\overline{x}+\left(\overline{y}+\overline{z}\right)$.
- **Élément neutre $\overline{0}$ pour $+$:** $\overline{x}+\overline{0}=\overline{x+0}=\overline{x}$ et $\overline{0}+\overline{x}=\overline{0+x}=\overline{x}$.
- **Inversibles pour $+$:** $\overline{x}+\overline{-x}=\overline{x+(-x)}=\overline{0}$ et $\overline{-x}+\overline{x}=\overline{(-x)+x}=\overline{0}$, donc $\overline{x}$ est inversible pour $+$ d'inverse $\overline{-x}$. ■

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 $x\in\mathbb{Z}$: $\quad\overline{x}\in\mathrm{U}\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)\quad\Longleftrightarrow\quad x\wedge n=1.$

Démonstration
$$\overline{x}\in\mathrm{U}\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)\iff\exists\,y\in\mathbb{Z},\ \overline{xy}=\overline{yx}=\overline{1}\iff\exists\,y\in\mathbb{Z},\ xy\equiv1\ [n]$$
$$\iff\exists\,y,z\in\mathbb{Z},\ xy+nz=1\overset{\text{Bézout}}{\iff}x\wedge n=1.$$ ■

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

Par exemple, $\overline{7}$ est inversible dans $\frac{\mathbb{Z}}{10\mathbb{Z}}$ car $7\wedge10=1$. La relation de Bézout $3\times7-2\times10=1$ montre que $\overline{3}\times\overline{7}=\overline{1}$ après réduction modulo 10, i.e. que $\overline{7}^{-1}=\overline{3}$.

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 Plutôt que de passer en revue tous les éléments de $\frac{\mathbb{Z}}{37\mathbb{Z}}$, remarquons que $\overline{2}$ est inversible dans $\frac{\mathbb{Z}}{37\mathbb{Z}}$ car $2\wedge37=1$. En outre $2\times19-37=1$, donc $\overline{2}^{-1}=\overline{19}$. Ainsi, pour tout $x\in\frac{\mathbb{Z}}{37\mathbb{Z}}$:
$$\overline{2}x=\overline{5}\quad\Longleftrightarrow\quad x=\overline{2}^{-1}\overline{5}\quad\Longleftrightarrow\quad x=\overline{19}\times\overline{5}\quad\Longleftrightarrow\quad x=\overline{21}.$$

L'anneau $\frac{\mathbb{Z}}{4\mathbb{Z}}$ n'est pas intègre — donc 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 nécessaire et suffisante $\frac{\mathbb{Z}}{n\mathbb{Z}}$ 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 Soient $p \in \mathbb{P}$ IMPAIR et $a, b, c \in \dfrac{\mathbb{Z}}{p\mathbb{Z}}$ avec $a \neq \overline{0}$. L'équation $ax^2 + bx + c = \overline{0}$ d'inconnue $x \in \dfrac{\mathbb{Z}}{p\mathbb{Z}}$ possède au plus 2 solutions.

Démonstration Comme p est premier, $\dfrac{\mathbb{Z}}{p\mathbb{Z}}$ est un corps, donc est à la fois intègre et commutatif. En outre $2 \wedge p = 1$ car p est impair, donc $\overline{2}$ est inversible dans $\dfrac{\mathbb{Z}}{p\mathbb{Z}}$. Pour tout $x \in \dfrac{\mathbb{Z}}{p\mathbb{Z}}$, la commutativité aidant :

$$ax^2 + bx + c = a\left(\left(x + \frac{b}{\overline{2}}\right)^2 - \frac{\Delta}{\left(\overline{2}a\right)^2}\right) \qquad \text{si on pose } \Delta = b^2 - 4ac,$$

donc : $\quad ax^2 + bc + c = \overline{0} \iff \left(x + \dfrac{b}{\overline{2}}\right)^2 = \dfrac{\Delta}{\left(\overline{2}a\right)^2}$.

— Si Δ N'EST PAS un carré dans $\dfrac{\mathbb{Z}}{p\mathbb{Z}}$, l'équation étudiée n'a pas de solution.

— Si $\Delta = \overline{0}$, l'équation admet pour seule solution l'élément $-\dfrac{b}{\overline{2}}$ par intégrité.

— Si Δ est un carré non nul dans $\dfrac{\mathbb{Z}}{p\mathbb{Z}}$, disons $\Delta = \delta^2$ pour un certain $\delta \in \dfrac{\mathbb{Z}}{p\mathbb{Z}}$ non nul, l'équation étudiée possède deux solutions distinctes par intégrité et commutativité de $\dfrac{\mathbb{Z}}{p\mathbb{Z}}$, en l'occurrence $\dfrac{-b \pm \delta}{\overline{2}a}$.

Ainsi, la situation est exactement la même que dans $\mathbb{R}$ et $\mathbb{C}$, mais on comprend aujourd'hui que l'essentiel n'est pas de connaître le SIGNE du discriminant — cela n'a aucun sens dans $\dfrac{\mathbb{Z}}{p\mathbb{Z}}$ — mais de savoir si le discriminant est un carré ou non. Dans $\mathbb{R}$, il se trouve simplement que les carrés sont exactement les réels positifs.

Le cadre de l'arithmétique modulaire fournit à présent une expression très simple au petit théorème de Fermat.

Théorème (Petit théorème de Fermat) Pour tous $p \in \mathbb{P}$ et $x \in \dfrac{\mathbb{Z}}{p\mathbb{Z}}$: $\quad x^p = x$,
et si $x \neq \overline{0}$: $\quad x^{p-1} = \overline{1}$.

Pour finir, le théorème qui suit est un énoncé classique d'arithmétique dans $\mathbb{Z}$, mais qu'on ne comprend véritablement que lorsqu'on l'interprète dans $\dfrac{\mathbb{Z}}{p\mathbb{Z}}$.

Théorème (Théorème de Wilson) Pour tout $p \in \mathbb{P}$: $\quad (p-1)! \equiv -1\ [p]$.

Démonstration Comme p est premier, $\dfrac{\mathbb{Z}}{p\mathbb{Z}}$ est un corps, donc est à la fois intègre et commutatif, donc pour tout $x \in \dfrac{\mathbb{Z}}{p\mathbb{Z}}$ non nul : $\quad x = x^{-1} \iff x^2 = \overline{1} \iff \left(x - \overline{1}\right)\left(x + \overline{1}\right) = \overline{0} \iff x = \overline{1}$ ou $x = -\overline{1}$.
Ces équivalences montrent que $\overline{1}$ et $-\overline{1}$ sont les seuls éléments non nuls de $\dfrac{\mathbb{Z}}{p\mathbb{Z}}$ égaux à leur inverse.
Nous allons maintenant calculer de deux façons différentes le produit Π de tous les éléments non nuls de $\dfrac{\mathbb{Z}}{p\mathbb{Z}}$. La question de l'ordre dans lequel on multiplie les éléments ne se pose pas ici car $\dfrac{\mathbb{Z}}{p\mathbb{Z}}$ est commutatif.

— **Premier calcul :** $\quad \Pi = \overline{1} \times \overline{2} \times \ldots \times \overline{p-1} = \overline{(p-1)!}$.

— **Deuxième calcul :** Dans Π, tout élément autre que $\overline{1}$ et $-\overline{1}$ est distinct de son inverse, donc disparaît corps et biens de la rencontre de son inverse. Seuls $\overline{1}$ et $-\overline{1}$ réchappent de ce jeu de massacre, et donc $\Pi = -\overline{1}$.

Conclusion : $\quad \overline{(p-1)!} = -\overline{1}, \quad$ donc $(p-1)! \equiv -1\ [p]$. ∎