GROUPES ET ANNEAUX

Dans ce chapitre, $\mathbb{K}$ est l'un des ensembles $\mathbb{R}$ ou $\mathbb{C}$, E un ensemble non vide et n un entier naturel non nul.

1 LOIS INTERNES

1.1 MAGMAS

Définition (Loi interne, magma et partie stable par une loi interne)

- **Loi interne et magma :** Soit M un ensemble. On appelle *loi (de composition) interne sur M* toute application $\star$ de $M\times M$ dans M. Le couple $(M,\star)$ est alors appelé un *magma*.
- **Partie stable par une loi interne :** Soient $(M,\star)$ un magma et A une partie de M. On dit que A est *stable par* $\star$ si : $\forall a,a'\in A,\quad a\star a'\in A$. Il est équivalent de dire que l'application $\star|_{A\times A}$ est une loi interne sur A. Le cas échéant, $\left(A,\star|_{A\times A}\right)$ est lui-même un magma.

Une loi interne sur M, c'est ce que vous avez appelé une opération jusqu'ici, i.e. une manière de transformer deux éléments de M en un troisième élément de M. L'image par $\star$ d'un couple (x,y) est toujours notée $x\star y$ plutôt que $\star(x,y)$.

Dire qu'une partie A de M est stable par $\star$, c'est dire que A fonctionne en vase clos dans M comme un petit monde autonome à l'intérieur d'un plus vaste monde. Les calculs qu'on effectue avec $\star$ sur des éléments de A ne quittent jamais A.

On représente parfois les magmas finis par des tableaux dits *tables de Cayley*. Par exemple, pour un ensemble $M=\{a,b,c\}$ à trois éléments muni d'une loi interne $\star$, la table de Cayley ci-contre résume lisiblement la structure que $\star$ confère à M.

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

Exemple

- Les applications $(x,y)\overset{+}{\longmapsto}x+y$ et $(x,y)\overset{\times}{\longmapsto}xy$ sont des lois internes sur $\mathbb{C}$ et font de $(\mathbb{C},+)$ et $(\mathbb{C},\times)$ deux magmas.
  - Exemples de parties stables par addition : $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, mais aussi $\{0\}$ et $\mathbb{N}^*$.
  - Exemples de parties stables par produit : $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, mais aussi $\mathbb{N}^*$, $\mathbb{Z}^\star$, $\mathbb{Q}^*$, $\mathbb{R}^*$ car le produit de deux complexes non nul est un complexe non nul. Citons également $\mathbb{R}_+$, $\mathbb{Q}_+^*$, $\mathbb{R}_+$ et $\mathbb{R}_+^*$.

  Attention, $\mathbb{R}_-$ n'est pas stable par produit car le produit de deux réels négatifs n'est pas toujours un réel négatif, c'est même rarement le cas.

  L'application $(x,y)\longmapsto x-y$ est elle aussi une loi interne sur $\mathbb{C}$ et les parties $\mathbb{Z}$, $\mathbb{Q}$ et $\mathbb{R}$ sont stables par soustraction, mais ce n'est pas le cas de $\mathbb{N}$.
- Les applications $(M,N)\overset{+}{\longmapsto}M+N$ et $(M,N)\overset{\times}{\longmapsto}MN$ sont des lois internes sur $\mathcal{M}_n(\mathbb{K})$ et font de $\left(\mathcal{M}_n(\mathbb{K}),+\right)$ et $\left(\mathcal{M}_n(\mathbb{K}),\times\right)$ des magmas.
  - Exemples de parties stables par addition : l'ensemble des matrices diagonales, l'ensemble des matrices triangulaires supérieures, l'ensemble des matrices symétriques.
  - Exemples de parties stables par produit : l'ensemble des matrices diagonales, l'ensemble des matrices triangulaires supérieures, et surtout l'ensemble $\mathrm{GL}_n(\mathbb{K})$ des matrices inversibles.

  Attention, $\mathrm{GL}_n(\mathbb{K})$ n'est pas stable par addition car, par exemple, la somme d'une matrice inversible et de son opposé, également inversible, est la matrice nulle, non inversible.

  Avec des matrices de taille quelconque, l'application $(M,N)\overset{+}{\longmapsto}M+N$ est une loi interne sur $\mathcal{M}_{n,p}(\mathbb{K})$.
- Les applications $(A,B)\overset{\cup}{\longmapsto}A\cup B$ et $(A,B)\overset{\cap}{\longmapsto}A\cap B$ sont des lois internes sur $\mathcal{P}(E)$. L'ensemble $\mathcal{P}(E)\setminus\{\varnothing\}$ des parties non vides de E est stable par réunion, de même que l'ensemble des parties de E de cardinal supérieur à 42.
- L'application $(f,g)\overset{\circ}{\longmapsto}f\circ g$ est une loi interne sur E^E. L'ensemble des bijections de E sur E et l'ensemble des applications constantes de E dans E sont stables par composition. Dans $\mathbb{R}^{\mathbb{R}}$, l'ensemble des fonctions croissantes est stable par composition.

La théorie des magmas est ce domaine immense des mathématiques qu'on appelle l'*algèbre*. Un magma, c'est ce qu'on obtient quand on *structure* un ensemble à l'aide d'une loi interne. 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 $\times$ lui apportent 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 la relation $\leqslant$ et les lois internes $+$ et $\times$.

1.2 Commutativité, associativité, distributivité

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

- **Commutativité :** On dit que $(M,\star)$ est *commutatif* ou que $\star$ est *commutative* si : $\forall x,y\in M,\quad x\star y=y\star x$.
- **Associativité :** On dit que $(M,\star)$ est *associatif* ou que $\star$ est *associative* si : $\forall x,y,z\in M,\ (x\star y)\star z=x\star(y\star z)$.
- **Qui peut le plus peut le moins :** Soit A une partie de M stable par $\star$. Si $(M,\star)$ est commutatif (resp. associatif), alors $(A,\star)$ est l'est aussi. Vive les quantificateurs $\forall$!

En cas d'associativité, on néglige tous les parenthésages et on note par exemple $a\star b\star c\star d$ les éléments $(a\star b)\star(c\star d)$ et $a\star\big((b\star c)\star d\big)$ qui se trouvent être égaux : $(a\star b)\star(c\star d)=a\star\big(b\star(c\star d)\big)=a\star\big((b\star c)\star d\big)$. En particulier, le produit de n copies d'un élément $x\in M$ est bien défini pour tout $n\in\mathbb{N}^*$, mais deux notations sont utilisées selon le contexte :

— en *notation multiplicative*, on pose $x^n=x\star\ldots\star x$ (n termes) et on appelle x^n une *puissance de* x,

— en *notation additive*, on pose $nx=x\star\ldots\star x$ (n termes) et on appelle nx un *multiple de* x.

Il ne s'agit là vraiment que d'une affaire de notation. Il n'y a pas les lois multiplicatives d'un côté et les lois additives de l'autre. Les deux points de vue sont toujours possibles pour une loi donnée, mais l'usage veut qu'on choisisse un camp et qu'on s'y tienne. L'idée ne viendrait à personne aujourd'hui d'écrire $5^3=15$ l'égalité $3\times5=5+5+5=15$, mais c'est seulement parce que l'histoire a fixé les conventions.

Exemple Ci-dessous, dès qu'un magma est commutatif ou associatif, les magmas plus petits qu'on peut en tirer par stabilité sont tous eux aussi commutatifs ou associatifs. Qui peut le plus peut le moins !

- Les magmas $(\mathbb{C},+)$ et $(\mathbb{C},\times)$ sont commutatifs et associatifs.
- Les magmas $\big(\mathcal{M}_{n,p}(\mathbb{K}),+\big)$ et $\big(\mathcal{M}_n(\mathbb{K}),\times\big)$ sont associatifs. Le premier est commutatif, mais pas le second pour $n\geqslant2$. Par exemple, les matrices $A=\begin{pmatrix}0&1\\1&0\end{pmatrix}$ et $B=\begin{pmatrix}0&-1\\1&0\end{pmatrix}$ ne commutent pas dans $\mathcal{M}_2(\mathbb{K})$, donc les matrices par blocs $\begin{pmatrix}A&0\\0&I_{n-2}\end{pmatrix}$ et $\begin{pmatrix}B&0\\0&I_{n-2}\end{pmatrix}$ non plus dans $\mathcal{M}_n(\mathbb{K})$.
- Les magmas $\big(\mathscr{P}(E),\cup\big)$ et $\big(\mathscr{P}(E),\cap\big)$ sont commutatifs et associatifs.
- Le magma $\big(E^E,\circ\big)$ est associatif, mais non commutatif si $|E|\geqslant2$. Par exemple, si E contient deux éléments distincts a et b, les applications constantes $x\overset{f}{\longmapsto}a$ et $x\overset{g}{\longmapsto}b$ ne commutent pas car $f\circ g=f\neq g=g\circ f$.
- 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 $3-(1-1)=3$. L'addition, c'est vraiment mieux que la soustraction.

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

Exemple

- Dans $\mathbb{C}$ et $\mathcal{M}_n(\mathbb{K})$, la multiplication est distributive sur l'addition, et de nouveau, qui peut le plus peut le moins grâce aux quantificateurs $\forall$, donc le résultat reste vrai dans $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ et $\mathbb{R}$.
- Réunion et intersection sont distributives l'une sur l'autre dans $\mathscr{P}(E)$. Pour tous $A,B,C\in\mathscr{P}(E)$:
$$A\cup(B\cap C)=(A\cup B)\cap(A\cup C)\quad\text{et}\quad(A\cap B)\cup C=(A\cup C)\cap(B\cup C)\quad\text{(distributivité de }\cup\text{ sur }\cap)$$
et : $A\cap(B\cup C)=(A\cap B)\cup(A\cap C)\quad$ et $\quad(A\cup B)\cap C=(A\cap C)\cup(B\cap C)\quad$ (distributivité de $\cap$ sur $\cup$).

1.3 Élement neutre, 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 : $\forall x\in M,\quad x\star e=e\star x=x$.

Si $(M,\star)$ possède un élément neutre, celui-ci est unique et on le note souvent 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 $\star$, alors $e=e\star e'=e'$, donc $e=e'$.

Exemple

- Les magmas $(\mathbb{C},+)$, $(\mathbb{R},+)$, $(\mathbb{Q},+)$, $(\mathbb{Z},+)$ et $(\mathbb{N},+)$ admettent 0 pour élément neutre et les magmas $(\mathbb{C},\times)$, $(\mathbb{R},\times)$, $(\mathbb{Q},\times)$, $(\mathbb{Z},\times)$ et $(\mathbb{N},\times)$ le nombre 1. Le magma $(\mathbb{N}^*,+)$, en revanche, ne possède pas d'élément neutre.
- Le magma $\big(\mathcal{M}_{n,p}(\mathbb{K}),+\big)$ admet la matrice nulle $0_{n,p}$ 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.

Attention ! Ce qui existe dans un grand monde peut ne pas exister dans un monde plus petit. Ainsi, étant donné un magma $(M,\star)$ et une partie A de M stable par $\star$, $(M,\star)$ 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, $\big(\mathcal{M}_2(\mathbb{R}),\times\big)$ 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.

Dans un magma $(M,\star)$ associatif avec élément neutre, on pose $x^0=1_M$ pour tout $x\in M$ en notation multiplicative et $0x=0_M$ en notation additive. 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-théorème **(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 un élément $x'\in M$, appelé un *inverse de* x, pour lequel $x\star x'=x'\star x=1_M$.

Unicité dans un magma associatif : Si $(M,\star)$ est associatif et si x est inversible, alors x possède un unique inverse. On le note x^{-1} en notation multiplicative et $-x$ en notation additive, auquel cas on parle plutôt de l'*opposé de* x.

Démonstration Si $(M,\star)$ est associatif et si x' et x'' sont deux inverses de x, alors :
$$x'=x'\star 1_M=x'\star(x\star x'')=(x\star x)\star x''=1_M\star x''=x''.$$

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

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

(ii) **Produit :** Si x et y sont inversibles, $x\star y$ l'est aussi et $(x\star y)^{-1}=y^{-1}\star x^{-1}$.

(iii) **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) **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 « Relations binaires et applications ».

Démonstration Mêmes preuves qu'au chapitre « Matrices et systèmes linéaires » pour les assertions (ii), (iii) et (iv). Pour (i), si $a\star x=a\star y$ avec a inversible :
$$x=1_M\star x=\big(a^{-1}\star a\big)\star x=a^{-1}\star(a\star x)=a^{-1}\star(a\star y)=\big(a^{-1}\star a\big)\star y=1_M\star y=y.$$

Exemple

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

  Attention, donc : Un élément peut posséder un inverse dans un magma, mais pas dans un magma plus petit.

- Dans $(\mathbb{C},\times)$, tout le monde est inversible à part 0. Par conséquent, dans $(\mathbb{C}^*,\times)$, qui est bien un magma, tout élément est inversible. En revanche, 1 et -1 sont les seuls inversibles de $(\mathbb{Z},\times)$ et 1 est même le seul inversible de $(\mathbb{N},\times)$.
- 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.
- Rappelons maintenant 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 $A\cup B=\varnothing$, 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 $\big(E^E,\circ\big)$ 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.

1.4 Lois produits

Vous savez depuis longtemps additionner les familles de réels, en géométrie analytique notamment, ainsi que les fonctions de $\mathbb{R}$ dans $\mathbb{R}$. Par exemple, $(2,1,3)+(1,0,-1)=(1,1,2)$ et $\cos+\sin$ est la fonction $x\longmapsto\cos x+\sin x$. On généralise ici les deux procédés.

Définition-théorème **(Produit de magmas)** Soient $(M,\star)$ et $(M',\bullet)$ deux magmas. On définit une loi interne $\square$ sur le produit $M\times M'$ en posant pour tous $(x,x'),(y,y')\in M\times M'$: $(x,x')\square(y,y')=(x\star y\,,\,x'\bullet y')$.

(i) **Commutativité, associativité :** Si $(M,\star)$ et $(M',\bullet)$ sont commutatifs (resp. associatifs), $\big(M\times M',\square\big)$ l'est aussi.

Avec deux lois sur M et deux sur M', un énoncé analogue est vrai en termes de distributivité.

(ii) **Élément neutre :** Si $(M,\star)$ et $(M',\bullet)$ possèdent chacun un élément neutre, $\big(M\times M',\square\big)$ en possède un aussi, et en l'occurrence $1_{M\times M'}=\big(1_M,1_{M'}\big)$.

(iii) **Inversibles :** On suppose $(M,\star)$ et $(M',\bullet)$ associatifs avec élément neutre. Pour tous $x\in M$ inversible pour $\star$ et $x'\in M'$ inversible pour $\bullet$, (x,x') est inversible pour $\square$ et $(x,x')^{-1}=\big(x^{-1},x'^{-1}\big)$.

Cette construction se généralise naturellement au cas d'un nombre quelconque de magmas.

Démonstration

(i) Si $\star$ et $\bullet$ sont commutatives, $\square$ l'est car pour tous $(x,x'),(y,y')\in M\times M'$:
$$(x,x')\square(y,y')=(x\star y,x'\bullet y')=(y\star x,y'\star x')=(y,y')\square(x,x').$$
De même, si $\star$ et $\bullet$ sont associatives, $\square$ l'est car pour tous $(x,x'),(y,y'),(z,z')\in M\times M'$:
$$(x,x')\square\big((y,y')\square(z,z')\big)=(x,x')\square(y\star z,y'\bullet z')=\big(x\star(y\star z),x'\bullet(y'\bullet z')\big)=\big((x\star y)\star z,(x'\bullet y')\bullet z'\big)$$
$$=(x\star y,x'\bullet y')\square(z,z')=\big((x,x')\square(y,y')\big)\square(z,z').$$
(ii) Pour tout $(x,x')\in M\times M'$: $(1_M,1_{M'})\square(x,x')=\big(1_M\star x,1_{M'}\bullet x'\big)=(x,x')$ et idem dans l'autre sens.

(iii) Pour tout $(x,x')\in M\times M'$, (x,x') est inversible pour $\square$ d'inverse $\big(x^{-1},x'^{-1}\big)$ car :
$$(x,x')\square\big(x^{-1},x'^{-1}\big)=\big(x\star x^{-1},x'\bullet x'^{-1}\big)=\big(1_M,1_{M'}\big)$$ et de même dans l'autre sens. ∎

Définition-théorème **(Ensembles d'applications à valeurs dans un magma)** 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 $\left\{\begin{array}{ccc}X&\longrightarrow&M\\x&\longmapsto&f(x)\star g(x).\end{array}\right.$

L'application $(f,g)\longmapsto f\star g$ est alors une loi interne sur l'ensemble M^X des applications de X dans M.

(i) **Commutativité, associativité :** Si $(M,\star)$ est commutatif (resp. associatif), $\big(M^X,\star\big)$ l'est aussi.

(ii) **Élément neutre :** Si $(M,\star)$ possède un élément neutre, $\big(M^X,\star\big)$ en possède un aussi. En l'occurrence, $\mathbb{1}_{M^X}$ est l'application constante $x\longmapsto 1_M$.

(iii) **Inversibles :** On suppose $(M,\star)$ associatif avec élément neutre et on note I l'ensemble de ses inversibles. Pour toute application $f\in M^X$, f est inversible dans $\big(M^X,\star\big)$ si et seulement si f est à valeurs dans I, et le cas échéant, son inverse est l'application $x\longmapsto f(x)^{-1}$.

Démonstration

(i) Supposons $(M,\star)$ commutatif et montrons que $\big(M^X,\star\big)$ l'est. Soient $f,g\in M^X$. Alors $f\star g=g\star f$ car pour tout $x\in X$: $\quad(f\star g)(x)=f(x)\star g(x)=g(x)\star f(x)=(g\star f)(x)$.

Supposons $(M,\star)$ associatif et montrons que $\big(M^X,\star\big)$ l'est. Soient $f,g,h\in M^X$. Alors $(f\star g)\star h=f\star(g\star h)$ car pour tout $x\in X$:
$$\big((f\star g)\star h\big)(x)=(f\star g)(x)\star h(x)=\big(f(x)\star g(x)\big)\star h(x)=f(x)\star\big(g(x)\star h(x)\big)$$
$$=f(x)\star(g\star h)(x)=\big(f\star(g\star h)\big)(x).$$

(iii) Soit $f\in M^X$. Si f est inversible dans $\big(M^X,\star\big)$ d'inverse g, alors $f\star g=g\star f=1_{M^X}=(x\longmapsto 1_M)$, donc $f(x)$ est inversible d'inverse $g(x)$ pour tout $x\in X$ car $f(x)\star g(x)=g(x)\star f(x)=1_M$. Comme voulu, f est à valeurs dans I et son inverse est l'application $x\longmapsto f(x)^{-1}$. Réciproque immédiate. ∎

Exemple Le magma $\big(\mathbb{R}^{\mathbb{R}},+\big)$ est commutatif et associatif, il admet la fonction nulle $x\longmapsto 0$ pour élément neutre et toute fonction $f:\mathbb{R}\longrightarrow\mathbb{R}$ admet la fonction $x\longmapsto -f(x)$ pour opposée.

De son côté, le magma $\big(\mathbb{R}^{\mathbb{R}},\times\big)$ est commutatif et associatif, il admet la fonction constante $x\longmapsto 1$ pour élément neutre et ses inversibles sont les fonctions de $\mathbb{R}$ dans $\mathbb{R}$ qui ne s'annulent pas.

2 Groupes

2.1 Définition et premiers exemples

Définition (Groupe) On appelle *groupe* tout magma associatif possédant un élément neutre et dont tout élément est inversible. Le cardinal d'un groupe fini est généralement appelé son *ordre*.

Dans les exemples concrets, les lois de groupes sont notées multiplicativement ou additivement selon les cas. Dans les situations théoriques abstraites en revanche, les lois de groupes sont toujours notées multiplicativement par convention — sauf mention explicite du contraire. Par ailleurs, quand on introduit un groupe abstrait $(G,\star)$, on omet généralement de mentionner la loi $\star$ pour alléger les notations. On dit simplement « Soit G un groupe » et on note xx' le produit de deux éléments x et x'.

Dans un groupe, on simplifie comme on veut car tout élément est inversible. Par exemple : $\quad ab=ac\quad\Longrightarrow\quad b=c$ après multiplication à gauche par a^{-1}.

Exemple $(\mathbb{C},+)$, $(\mathbb{R},+)$, $(\mathbb{Q},+)$ et $(\mathbb{Z},+)$ sont des groupes commutatifs, de même de $(\mathbb{C}^*,\times)$, $(\mathbb{R}^*,\times)$ et $(\mathbb{Q}^*,\times)$. En revanche, $(\mathbb{Z}^*,\times)$ n'est pas un groupe car 2 n'y est pas inversible par exemple.

Exemple $\big(\mathcal{M}_n(\mathbb{K}),+\big)$ est un groupe, mais pas $\big(\mathcal{M}_n(\mathbb{K}),\times\big)$ car la matrice nulle n'est pas inversible par exemple.
En revanche, le groupe linéaire $\big(\mathrm{GL}_n(\mathbb{K}),\times\big)$ est un groupe comme son nom l'indique, non commutatif si $n\geqslant 2$.

Démonstration Commençons par une subtilité cruciale. Par définition, une matrice $A\in\mathcal{M}_n(\mathbb{K})$ est inversible si : $\quad\exists B\in\mathcal{M}_n(\mathbb{K}),\quad AB=BA=I_n,\quad$ i.e. si elle est inversible dans le magma $\big(\mathcal{M}_n(\mathbb{K}),\times\big)$. Le point important, c'est que l'inverse B de A, qu'on note après coup A^{-1}, est cherché dans $\mathcal{M}_n(\mathbb{K})$ a priori. En d'autres termes, quand on parle de « l'inverse de A », c'est par définition son inverse dans $\mathcal{M}_n(\mathbb{K})$ qu'on désigne.

Montrons maintenant que $\big(\mathrm{GL}_n(\mathbb{K}),\times\big)$ est un groupe. C'est un magma car $\mathrm{GL}_n(\mathbb{K})$ est stable par produit, associatif car $\big(\mathcal{M}_n(\mathbb{K}),\times\big)$ l'est et d'élément neutre I_n. Cela dit, tout élément de $\mathrm{GL}_n(\mathbb{K})$ est-il inversible dans $\big(\mathrm{GL}_n(\mathbb{K}),\times\big)$? En d'autres termes, est-il vrai que pour tout $A\in\mathrm{GL}_n(\mathbb{K})$: $\quad\exists B\in\mathrm{GL}_n(\mathbb{K}),\quad AB=BA=I_n$? Cette fois, l'inverse est cherché dans $\mathrm{GL}_n(\mathbb{K})$, on n'a pas affaire à la même notion d'inversibilité. Nous savons toutefois que l'inverse A^{-1} de A dans $\mathcal{M}_n(\mathbb{K})$ appartient à $\mathrm{GL}_n(\mathbb{K})$. Il est donc exact que A possède un inverse dans le magma $\big(\mathrm{GL}_n(\mathbb{K}),\times\big)$.

Exemple 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 les paragraphes précédents. Par exemple, $\big(\mathbb{R}^{\mathbb{R}},+\big)$ est un groupe commutatif.

✖ **Attention !** $(\mathbb{C},\times)$ n'est pas une groupe car 0 n'y est pas inversible. Par conséquent, quand on parlera désormais du groupe $\mathbb{C}$ sans préciser la loi, il s'agira toujours du groupe $(\mathbb{C},+)$, et quand on parlera du groupe $\mathbb{C}^*$, il s'agira toujours du groupe $(\mathbb{C}^*,\times)$. Idem pour $\mathbb{R}$, $\mathbb{R}^*$, $\mathbb{Q}$ et $\mathbb{Q}^*$. Pour une raison analogue, on parlera désormais du groupe $\mathcal{M}_n(\mathbb{K})$ pour désigner le groupe $\big(\mathcal{M}_n(\mathbb{K}),+\big)$ et du groupe $\mathrm{GL}_n(\mathbb{K})$ pour désigner le groupe $\big(\mathrm{GL}_n(\mathbb{K}),\times\big)$. Ces formulations ne souffrent d'aucune ambiguïté ici et vous devez en être absolument convaincus.

Définition-théorème **(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 S_E des permutations de E. Le magma $(S_E, \circ)$ est un groupe d'élément neutre Id_E.

Démonstration Comme avec $\mathrm{GL}_n(\mathbb{K})$, observons d'abord que par définition, une application $f \in E^E$ est bijective si : $\exists\, g \in E^E, \quad f \circ g = g \circ f = \mathrm{Id}_E$, i.e. si elle est inversible dans le magma $(E^E, \circ)$. L'inverse, qu'on appelle réciproque, est cherché dans E^E a priori.

À présent, $(S_E, \circ)$ est un magma car la composée de deux bijections est une bijection, associatif car $(E^E, \circ)$ l'est et d'élément neutre Id_E. Cela dit, tout élément de S_E est-il inversible dans $(S_E, \circ)$? En d'autres termes, est-il vrai que pour tout $f \in S_E$: $\exists\, g \in S_E, \quad f \circ g = g \circ f = \mathrm{Id}_E$? Cette fois, l'inverse est cherché dans S_E, on n'a pas affaire à la même notion d'inversibilité. Nous savons toutefois que la réciproque f^{-1} de f appartient à S_E. Il est donc exact que f possède un inverse dans le magma $(S_E, \circ)$.

Définition-théorème **(Produit de groupes)** Soient $G_1, \dots, G_n$ des groupes. Muni de la loi produit, $G_1 \times \dots \times G_n$ est un groupe appelé le *groupe produit de $G_1, \dots, G_n$*.

Exemple La loi du groupe $\mathbb{R} \times \mathbb{R}$ est définie par la relation $(x, y) + (x', y') = (x + x', y + y')$ pour tous $(x, y), (x', y') \in \mathbb{R}$. La loi du groupe $\mathbb{R} \times \mathbb{R}^*$ est définie par la relation mixte $(x, y)(x', y') = (x + y, x'y')$ pour tous $(x, y), (x', y') \in \mathbb{R} \times \mathbb{R}^*$.

2.2 Sous-groupes

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

Nous disposons de deux groupes, G et H, dont chacun possède un élément neutre et dans lesquels tout élément est inversible. Deux questions subtiles se posent alors :

— Les groupes 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 ?

Démonstration

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

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

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 Montrons seulement l'équivalence des assertions (i) et (iii).

(i) $\Longrightarrow$ (iii) Si H est un sous-groupe de G, H est stable par produit et nous venons de voir que $1_G \in H$ et H est stable par passage à l'inverse. Ainsi, pour tout $h, h' \in H$, $h^{-1} \in H$ par stabilité par inversion, puis $h^{-1}h' \in H$ par stabilité par produit.

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

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

— Maintenant que H est stable par produit, montrons que c'est un groupe pour la loi de G. Or H est associatif car G l'est et admet 1_G pour élément neutre puisque $1_G \in H$. Enfin, H est stable par inversion, donc tout élément de H est inversible. ∎

C'est toujours ce résultat qu'il faut utiliser pour montrer qu'une partie d'un groupe en est un sous-groupe. Avec la **DÉFINITION** des sous-groupes, on est obligé de parler d'associativité et d'inversibilité. La **CARACTÉRISATION** en fait l'économie.

Par ailleurs, pour montrer qu'un ensemble H muni d'une certaine loi est un groupe, il suffit souvent de montrer que H est un **SOUS-GROUPE** d'un groupe connu. Pas besoin de revenir à la définition des groupes avec associativité, élément neutre et inversibles, la caractérisation des sous-groupes est plus sobre.

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 $\mathbb{C}$. Même chose avec $\mathbb{Q}^*$, $\mathbb{R}^*$ et $\mathbb{C}^*$. Enfin, $\mathbb{R}_+^*$ et $\mathbb{U}$ sont des sous-groupes de $\mathbb{C}^*$.

Démonstration Pour commencer, $\mathbb{R}_+^* \subset \mathbb{C}^*$ et $\mathbb{U} \subset \mathbb{C}^*$. Ensuite, l'élément neutre 1 de $\mathbb{C}^*$ appartient à $\mathbb{R}_+^*$ et $\mathbb{U}$. Pour la stabilité par produit-inversion enfin, $x^{-1}x' = \dfrac{x'}{x} \in \mathbb{R}_+^*$ pour tous $x, x' \in \mathbb{R}_+^*$ et $\left|u^{-1}u'\right| = \dfrac{|u'|}{|u|} = \dfrac{1}{1} = 1$ pour tous $u, u' \in \mathbb{U}$.

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 suffit de montrer que $\mathcal{T}_n(\mathbb{K})$ est un **SOUS-GROUPE** de $\mathrm{GL}_n(\mathbb{K})$, et d'abord $\mathcal{T}_n(\mathbb{K}) \subset \mathrm{GL}_n(\mathbb{K})$ car toute matrice triangulaire à coefficients diagonaux non nuls est inversible. Ensuite, l'élément neutre I_n de $\mathrm{GL}_n(\mathbb{K})$ appartient à $\mathcal{T}_n(\mathbb{K})$. Pour la stabilité par produit, $TT' \in \mathcal{T}_n(\mathbb{K})$ pour tous $T, T' \in \mathcal{T}_n(\mathbb{K})$ car le produit de deux matrices triangulaires supérieures est triangulaire supérieure et $(TT')_{ii} = t_{ii}t'_{ii} \neq 0$ pour tout $i \in [\![1, n]\!]$. Enfin, pour la stabilité par inversion, $T^{-1} \in \mathcal{T}_n(\mathbb{K})$ pour tout $T \in \mathcal{T}_n(\mathbb{K})$ car toute matrice triangulaire supérieure à coefficients diagonaux non nuls est inversible et $\left(T^{-1}\right)_{ii} = \dfrac{1}{t_{ii}} \neq 0$ pour tout $i \in [\![1, n]\!]$.

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

Démonstration Pour commencer, $\mathrm{Stab}(x) \subset S_E$. Ensuite, l'élément neutre Id_E de S_E appartient à $\mathrm{Stab}(x)$ car $\mathrm{Id}_E(x) = x$. Enfin, pour la stabilité par produit-inversion, pour tous $\sigma, \sigma' \in \mathrm{Stab}(x)$, $\sigma(x) = x$ donc $\sigma^{-1}(x) = x$, donc $\sigma^{-1} \circ \sigma'(x) = \sigma^{-1}(x) = x$, i.e. $\sigma^{-1} \circ \sigma' \in \mathrm{Stab}(x)$.

Théorème **(Intersection de sous-groupes)** Soit G un groupe. Toute intersection de sous-groupes de G est un sous-groupe de G.

Démonstration Soit $(H_i)_{i \in I}$ une famille de sous-groupes de G. Montrons que $K = \bigcap_{i \in I} H_i$ est un sous-groupe de G. Pour commencer, $K \subset G$. Ensuite, H_i contient 1_G pour tout $i \in I$ en tant que sous-groupe de G, donc $1_G \in K$. Enfin, pour la stabilité par produit-inversion, soient $x, x' \in K$. Pour tout $i \in I$, H_i contient x et x', donc aussi $x^{-1}x'$ en tant que sous-groupe de G. Par conséquent, $x^{-1}x' \in K$.

Théorème **(Sous-groupes de $\mathbb{Z}$)** Les sous-groupes de $\mathbb{Z}$ sont exactement les $n\mathbb{Z}$, 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 ? Que n représente pour l'ensemble $n\mathbb{Z}$? Réponse : n est le premier élément de $n\mathbb{Z}$ qu'on trouve à droite de 0, i.e. le plus petit élément de $n\mathbb{Z} \cap \mathbb{N}^*$. Cela nous donne envie de poser $n = \min\left(G \cap \mathbb{N}^*\right)$… si jamais c'est possible.

- Si $G = \left\{0\right\}$, alors $G = 0\mathbb{Z}$ et c'est fini.

- Supposons désormais $G \neq \{0\}$. Le sous-groupe G contient alors au moins un élément non nul, mais il contient même forcément un entier NATUREL non nul car il est stable par passage à l'opposé. Partie non vide de $\mathbb{N}$, $G \cap \mathbb{N}^*$ possède ainsi un plus petit élément n et nous allons montrer que $G = n\mathbb{Z}$.

  L'inclusion $n\mathbb{Z} \subset G$ se prouve aisément. En effet, G contient n, donc aussi toutes les multiples nk de n, k décrivant $\mathbb{Z}$, car il est stable par addition et passage à l'opposé.

  Montrons que $G \subset n\mathbb{Z}$. Soit $g \in G$. Nous voulons montrer que $g \in n\mathbb{Z}$, i.e. que $n \mid g$. La division euclidienne de g par n s'écrit $g = nq + r$ pour certains $q \in \mathbb{Z}$ et $r \in [\![0, n-1]\!]$. Ainsi, $r = g - nq \in G$ car $n\mathbb{Z} \subset G$ et G est stable par addition, donc $r \in G \cap [\![0, n-1]\!]$. Il en découle par minimalité de n que $r = 0$, de sorte que $n \mid g$.

Le théorème suivant, simple mais fondamental, est spécifique aux groupes finis.

Théorème **(Théorème de Lagrange)** Soient G un groupe fini et H un sous-groupe de G. L'ordre de H divise l'ordre de G.

Démonstration

- Pour tous $x, y \in G$, on dira que $x \sim y$ si $y = xh$ pour un certain $h \in H$. Montrons que $\sim$ est une relation d'équivalence sur G.

  Réflexivité : Pour tout $x \in G$, $x = x1_G$ avec $1_G \in H$ car H est un sous-groupe de G, donc $x \sim x$.

  Symétrie : Pour tous $x, y \in G$, si $x \sim y$, alors $y = xh$ pour un certain $h \in H$, donc $x = yh^{-1}$ avec $h^{-1} \in H$ car H est stable par inversion, donc $y \sim x$.

  Transitivité : Pour tous $x, y, z \in G$, si $x \sim y$ et $y \sim z$, alors $y = xh$ et $z = yh'$ pour certains $h, h' \in H$, donc $z = x(hh')$ avec $hh' \in H$ car H est stable par produit, donc $x \sim z$.

- À présent, pour tout $x \in G$, la classe d'équivalence de x pour $\sim$ est l'ensemble :
$$\{y \in G \mid \exists h \in H, \quad y = xh\} = \{xh \mid h \in H\} = xH.$$
  En outre, l'application $h \longmapsto xh$ est bijective de H sur xH de réciproque $g \longmapsto x^{-1}g$, donc $|xH| = |H|$. Finalement, en notant $x_1, \dots, x_n$ des représentants des classes d'équivalence de $\sim$:
$$|G| = \left|x_1 H \sqcup \dots \sqcup x_n H\right| = |x_1 H| + \dots + |x_n H| = |H| + \dots + |H| = n|H|, \quad \text{donc } |H| \text{ divise } |G|.$$

2.3 MORPHISMES DE GROUPES

Définition **(Morphisme de groupes)** Soient $(G, \star)$ et $(G', \bullet)$ deux groupes. On appelle *morphisme (de groupes) de G dans G'* toute application $f : G \longrightarrow G'$ pour laquelle :
$$\forall x, y \in G, \quad f(x \star y) = f(x) \bullet f(y).$$
Si on omet de noter les lois $\star$ et $\bullet$, cela revient à dire que : $\forall x, y \in G, \quad f(xy) = f(x)f(y)$.

Quand $G = G'$, 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 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 $\mathbb{K}$.
- Soient G un groupe commutatif et $n \in \mathbb{Z}$. L'application $x \longmapsto x^n$ est un endomorphisme de groupe de G car pour tous $x, y \in G$, $(xy)^n = x^n y^n$ par commutativité.

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 :** Soient G et G' deux groupes et $f : G \longrightarrow G'$ un morphisme de groupes. Pour tout sous-groupe H de G, $f(H)$ est un sous-groupe de G', et pour tout sous-groupe H' de G', $f^{-1}(H')$ en est un de G.

Démonstration

(i) $f(1_G)\,f(1_G) = f(1_G 1_G) = f(1_G) = f(1_G)\,1_{G'}$, donc $f(1_G) = 1_{G'}$ après simplification par $f(1_G)$ à gauche. Ensuite, pour tout $x \in G$: $f\left(x^{-1}\right) f(x) = f\left(x^{-1}x\right) = f(1_G) = 1_{G'}$, donc $f\left(x^{-1}\right) = f(x)^{-1}$ après multiplication par $f(x)^{-1}$ à droite.

(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, $f(H) \subset G'$ et $1_{G'} = f(1_G) \in f(H)$ car $1_G \in H$. Enfin, pour tous $y, y' \in f(H)$, $y = f(h)$ et $y' = f(h')$ pour certains $h, h' \in H$, donc $y^{-1}y' = f\left(h^{-1}h'\right)$, or $h^{-1}h' \in H$ car H est stable par produit-inversion, donc $y^{-1}y' \in f(H)$.

Montrons que $f^{-1}(H')$ est un sous-groupe de G. D'abord, $f^{-1}(H') \subset G$ et $1_G \in f^{-1}(H')$ car $f(1_G) = 1_{G'} \in H'$. 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 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.

(i) **Image :** L'image de f est notée $\operatorname{Im} f$ et c'est un sous-groupe de G'.
En outre, f est surjectif de G sur G' si et seulement si $\operatorname{Im} f = G'$.

(ii) **Noyau :** On appelle *noyau de* f le sous-groupe de G : $\operatorname{Ker} f = f^{-1}\big(\{1_{G'}\}\big) = \big\{x \in G \mid f(x) = 1_{G'}\big\}$.
En outre, f est injectif sur G si et seulement si $\operatorname{Ker} f = \{1_G\}$.

(iii) **Équations $f(x) = y_0$:** Soit $y_0 \in G'$.

— Si $y_0 \notin \operatorname{Im} g$, l'équation $f(x) = y_0$ d'inconnue $x \in G$ n'a pas de solution.

— Si $y_0 \in \operatorname{Im} f$, alors en notant x_0 un antécédent de y_0 par f : $\big\{x \in G \mid f(x) = y_0\big\} = x_0 \operatorname{Ker} f$.

Le noyau de f est l'ensemble des éléments de G qui ne comptent pas aux yeux de f, i.e. qu'elle ne distingue pas de l'élément neutre. 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

(i) $\operatorname{Im} f = f(G)$ est un sous-groupe de G' en tant qu'image d'un sous-groupe par un morphisme de groupes.

(ii) $\operatorname{Ker} f$ est un sous-groupe de G' en tant qu'image réciproque d'un sous-groupe par un morphisme de groupes.

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

Réciproquement, faisons l'hypothèse que $\operatorname{Ker} f = \{1_G\}$ et montrons que f est injectif. Soient $x, x' \in G$. Si $f(x) = f(x')$, alors $f\left(x^{-1}x'\right) = f(x)^{-1}f(x') = f(x)^{-1}f(x) = 1_{G'}$, donc $x^{-1}x' \in \operatorname{Ker} f = \{1_G\}$, i.e. $x = x'$.

(iii) Sous l'hypothèse que $y_0 = f(x_0) \in \operatorname{Im} f$, pour tout $x \in G$:

$$\begin{aligned} f(x) = y_0 &\iff f(x) = f(x_0) \iff f(x_0)^{-1}f(x) = 1_{G'} \\ &\iff f\left(x_0^{-1}x\right) = 1_{G'} \iff x_0^{-1}x \in \operatorname{Ker} f \iff x \in x_0 \operatorname{Ker} f. \end{aligned}$$

Exemple

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

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'.

  Quand $G = G'$, 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 son pendant dans G'. Deux groupes isomorphes 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 groupes de $\mathbb{R}$ sur $\mathbb{R}_+^*$.
- Pour tout $\alpha \in \mathbb{R}^*$, la fonction puissance $x \longmapsto x^\alpha$ est un automorphisme de groupe 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, dont les classes d'équivalence sont appelées les *classes d'isomorphisme*.

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 $x, y \in G$: $\quad \mathrm{Id}_G(xy) = xy = \mathrm{Id}_G(x)\mathrm{Id}_G(y)$.

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 $\mathbb{U}_2^2$ sont tous les deux d'ordre 4, mais pas isomorphes.

Démonstration Pour commencer : $\quad \mathbb{U}_4 = \{1, -1, i, -i\} \quad$ et $\quad \mathbb{U}_2^2 = \big\{(1,1),(1,-1),(-1,1),(-1,-1)\big\}$.
Soit f un morphisme de groupes de $\mathbb{U}_2^2$ dans $\mathbb{U}_4$. Pour tout $(u,v) \in \mathbb{U}_2^2$: $\quad (u,v)^2 = \big(u^2, v^2\big) = (1,1), \quad$ donc $f(u,v)^2 = f\big((u,v)^2\big) = f(1,1) = 1$. Comme $i^2 = -1$, il en découle que f ne prend pas la valeur i, donc n'est pas surjectif. A fortiori, 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… Intéressons-nous au groupe produit $\mathbb{R}\times\{0\}$, dont la loi est définie par $(x,0)+(x',0)=(x+x',0)$ pour tous $x,x'\in\mathbb{R}$. Cette définition fait de l'application $x\longmapsto(x,0)$ un morphisme de groupes de $\mathbb{R}$ dans $\mathbb{R}\times\{0\}$, et même un isomorphisme. Les groupes $\mathbb{R}$ et $\mathbb{R}\times\{0\}$ sont ainsi identiques du point de vue de leurs additions respectives. Pourquoi le groupe $\mathbb{R}$ dont nous sommes partis serait-il plus « l'ensemble des réels » que le groupe $\mathbb{R}\times\{0\}$? Les deux se valent. Il y a autant de groupes des réels qu'on veut bien se donner la peine d'en construire *à isomorphisme près*.

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 magmas, mais avec quel objectif ? L'algèbre entreprend de classifier les structures algébriques. Les groupes $\mathbb{R}$ et $\mathbb{R}\times\{0\}$ sont différents en tant qu'ensembles mais identiques en tant que groupes — isomorphes. Ils appartiennent à la même classe d'isomorphisme. La grande question de la théorie des groupes n'est donc pas « Qui sont tous les groupes ? » mais plus finement « Qui 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, en fait un sous-groupe du groupe symétrique S_G.

Démonstration $\mathrm{Aut}(G)\subset S_G$ et $\mathrm{Id}_G\in\mathrm{Aut}(G)$, et la stabilité par produit-inversion découle du théorème précédent.

Exemple $\mathrm{Aut}(\mathbb{Z})=\{\mathrm{Id}_\mathbb{Z},-\mathrm{Id}_\mathbb{Z}\}$.

Démonstration Pour commencer, $\mathrm{Id}_\mathbb{Z}$ et $-\mathrm{Id}_\mathbb{Z}$ sont bien des automorphismes de groupe de $\mathbb{Z}$. Réciproquement, soit $f\in\mathrm{Aut}(\mathbb{Z})$. La loi de groupe de $\mathbb{Z}$ étant l'addition, pour tout $n\in\mathbb{Z}$: $f(n)=f(n.1)=nf(1)$, donc f est l'application $x\longmapsto\lambda x$ si on pose $\lambda=f(1)$. Cela dit, f est aussi bijective de $\mathbb{Z}$ sur $\mathbb{Z}$, donc $\lambda=\pm1$, donc $f=\mathrm{Id}_\mathbb{Z}$ ou $f=-\mathrm{Id}_\mathbb{Z}$.

2.4 Groupes symétriques

Pour tout $n\in\mathbb{N}^*$, le groupe symétrique de $[\![1,n]\!]$ est noté S_n plutôt que $S_{[\![1,n]\!]}$ et le produit $\sigma\circ\sigma'$ de deux permutations $\sigma,\sigma'\in S_n$ est généralement noté $\sigma\sigma'$.

Rappelons que $|S_n|=n!$ car la donnée d'une permutation σ de S_n est équivalente à la donnée du n-arrangement $\big(\sigma(1),\dots,\sigma(n)\big)$ de $[\![1,n]\!]$. Un vaste monde, donc, dont certaines permutations sont cela dit faciles à décrire.

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 :
$$\sigma(x_1)=x_2,\qquad\sigma(x_2)=x_3,\qquad\dots,\qquad\sigma(x_{p-1})=x_p,\qquad\sigma(x_p)=x_1$$
et $\sigma(x)=x$ si x n'est aucun des éléments $x_1,\dots,x_p$. Un tel p-cycle est noté $(x_1\ x_2\ \dots\ x_p)$ ou $(x_2\ x_3\ \dots\ x_p\ x_1)$ ou $(x_3\ x_4\ \dots\ x_p\ x_1\ x_2)\dots$
- **Transposition :** Un 2-cycle est plutôt appelé une *transposition*.

Attention ! Toute permutation n'est pas un cycle. Par exemple, $(1\ 2)(3\ 4)$ envoie 1 sur 2 et aussitôt 2 sur 1, mais sans fixer 3 et 4, ce n'est donc pas un cycle dans S_4.

Exemple Dans S_4 : $(2\ 3)(4\ 3\ 1)(4\ 2\ 3)=(1\ 4\ 3\ 2)$. Ici, le produit est un cycle, mais c'est par hasard.

Démonstration $\big((2\ 3)(4\ 3\ 1)(4\ 2\ 3)\big)(1)=\big((2\ 3)(4\ 3\ 1)\big)(1)=\big((2\ 3)\big)(4)=4$,
puis : $\big((2\ 3)(4\ 3\ 1)(4\ 2\ 3)\big)(2)=\big((2\ 3)(4\ 3\ 1)\big)(3)=\big((2\ 3)\big)(1)=1$,
et on calcule de même les images de 3 et 4.

Exemple $S_2=\{\mathrm{Id}\ ,\ (1\ 2)\}$ et les tables de Cayley ci-contre montrent que l'application de $\mathbb{U}_2=\{\pm1\}$ dans S_2 qui envoie 1 sur Id et -1 sur $(1\ 2)$ est un isomorphisme de groupes.

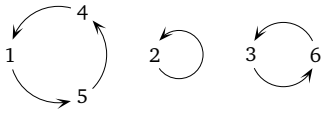
$\times$	1	-1
1	1	-1
-1	-1	1

$\circ$	Id	$(1\,2)$
Id	Id	$(1\,2)$
$(1\,2)$	$(1\,2)$	Id

Exemple $S_3=\{\mathrm{Id}\ ,\ (1\ 2)\ ,\ (1\ 3)\ ,\ (2\ 3)\ ,\ (1\ 2\ 3)\ ,\ (3\ 2\ 1)\}$. En outre, $(1\ 2)(1\ 3)=(1\ 3\ 2)\neq(1\ 2\ 3)=(1\ 3)(1\ 2)$, donc S_3 n'est pas commutatif. Ainsi, les groupes $\mathbb{U}_6$ et S_3 sont tous les deux d'ordre 6, mais pas isomorphes car les isomorphismes préservent la commutativité.

Intéressons-nous à présent à la permutation σ de S_6 définie par le tableau ci-contre. On y observe que σ agit circulairement sur certains paquets d'éléments. Elle envoie 1 sur 5, 5 sur 4 et 4 sur 1, elle fixe 2, et elle envoie enfin 3 sur 6 et 6 sur 3. Or c'est exactement ce que font aussi les permutations $(1\ 5\ 4)(3\ 6)$ et $(3\ 6)(1\ 5\ 4)$, donc $\sigma = (1\ 5\ 4)(3\ 6) = (3\ 6)(1\ 5\ 4)$. En réalité, le phénomène est universel et constitue l'objectif de ce paragraphe.

i	1	2	3	4	5	6
$\sigma(i)$	5	2	6	1	4	3



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 : $\quad \mathrm{supp}(\sigma) = \Big\{x \in [\![1,n]\!] \mid \quad \sigma(x) \neq x\Big\}$.
- **Permutations disjointes :** On dit que deux permutations de $[\![1,n]\!]$ sont *disjointes* si leurs supports sont disjoints.

  Le résultat important, c'est que deux permutations disjointes commutent.

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

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

— Supposons maintenant que $x \in \mathrm{supp}(\sigma)$ — même raisonnement si $x \in \mathrm{supp}(\sigma')$. Ainsi, $x \notin \mathrm{supp}(\sigma')$ car σ et σ' sont disjointes, 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 $\sigma(x) \in \mathrm{supp}(\sigma)$, donc $\sigma'\sigma(x) = \sigma(x)$ car σ et σ' sont disjointes. Finalement, $\sigma\sigma'(x) = \sigma(x) = \sigma'\sigma(x)$.

Dans tous les cas : $\quad \sigma\sigma'(x) = \sigma'\sigma(x)$, $\quad$ et ce pour tout $x \in [\![1,n]\!]$, donc $\sigma\sigma' = \sigma'\sigma$.

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 Montrons seulement l'existence de la décomposition. Soit $\sigma \in S_n$. Pour tous $x, y \in [\![1,n]\!]$, on dira que $x \sim y$ si $y = \sigma^k(x)$ pour un certain $k \in \mathbb{Z}$.

- La relation $\sim$ est une relation d'équivalence sur $[\![1,n]\!]$. En effet, soient $x, y, z \in [\![1,n]\!]$.

  Réflexivité : $x \sim x$ car $x = \mathrm{Id}(x) = \sigma^0(x)$.

  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 à présent $X_1, \dots, X_r$ les classes d'équivalence de $\sim$.
- Fixons $i \in [\![1,n]\!]$ et donnons-nous un élément x_i de X_i. Par finitude de X_i, $\sigma^k(x_i) = \sigma^l(x_i)$ pour certains $k, l \in \mathbb{N}$ pour lesquels $k < l$, donc $\sigma^{l-k}(x_i) = x_i$. Non vide, l'ensemble $\Big\{k \in \mathbb{N}^* \mid \quad \sigma^k(x_i) = x_i\Big\}$ possède ainsi un plus petit élément p_i. Montrons que l'application $k \longmapsto \sigma^k(x_i)$ est bijective de $[\![0, p_i - 1]\!]$ sur X_i.

  Surjectivité : Soit $y \in X_i$, disons $y = \sigma^k(x_i)$ pour un certain $k \in \mathbb{Z}$ par définition de $\sim$. Par division euclidienne, $k = p_i q + r$ pour certains $q \in \mathbb{Z}$ et $r \in [\![0, p_i - 1]\!]$, donc $y = \sigma^{p_i q + r}(x_i) = \sigma^r\big(\sigma^{p_i}\big)^q(x_i) = \sigma^r(x_i)$.

  Injectivité : Soient $k, l \in [\![0, p_i - 1]\!]$. Si $k < l$ et $\sigma^k(x_i) = \sigma^l(x_i)$, alors $l - k \in [\![0, p_i - 1]\!]$ et $\sigma^{l-k}(x_i) = x_i$, donc $l - k = 0$ par minimalité de p_i, i.e. $k = l$.

  La bijectivité obtenue nous autorise à noter σ_i le p_i-cycle $\big(x_i\ \sigma(x_i)\ \dots\ \sigma^{p_i - 1}(x_i)\big)$ de support X_i.
- Les cycles $\sigma_1, \dots, \sigma_r$ sont deux à deux disjoints car leurs supports $X_1, \dots, X_r$ le sont. Par ailleurs, $\sigma_i|_{X_i} = \sigma|_{X_i}$ pour tout $i \in [\![1,r]\!]$, donc $\sigma_1 \dots \sigma_r$ et σ agissent de la même manière sur $[\![1,n]\!]$, donc $\sigma = \sigma_1 \dots \sigma_r$.

Exemple $(1\ 2\ 3\ 4\ 5\ 6)(1\ 2\ 4\ 6)(1\ 3\ 5) = (1\ 4)(2\ 5\ 3\ 6)$ $\quad$ et $\quad (1\ 2\ 4\ 6)(2\ 5)(3\ 4\ 1) = (1\ 3\ 6)(2\ 5\ 4)$.

3 Anneaux

3.1 Définition et premiers exemples

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

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

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

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

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

Les *inversibles de A* sont ses inversibles au sens de la multiplication. Je noterai $\mathrm{U}(A)$ leur ensemble, mais la notation n'a rien d'universel.

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 on omet généralement le $\times$ dans les calculs.

La loi $+$ est commutative par définition, c'est donc toujours de la loi $\times$ qu'on parle quand on précise qu'un anneau est commutatif. De même, les éléments d'un anneau possèdent tous un opposé car tout anneau est un groupe additif, donc c'est toujours à la loi $\times$ qu'on fait référence quand on parle des inversibles d'un anneau.

Deux lois cohabitent dans un anneau A et on peut y calculer à la fois des multiples et des puissances. Pour tous $a\in A$ et $n\in\mathbb{N}$: $\quad na=a+\ldots+a\quad$ (n termes) et : $\quad a^n=a\times\ldots\times a\quad$ (n termes).

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

Exemple $\mathcal{M}_n(\mathbb{K})$ est un anneau, non commutatif pour $n\geqslant 2$, mais non commutatif jusqu'où ? 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, $ME_{ij}=E_{ij}M$ donc :

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

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

En position (i,j) : $\quad m_{ii}=m_{jj}$. 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. Le triplet $\left(A^X,+,\times\right)$ est un anneau car les propriétés des magmas $(A,+)$ et $(A,\times)$ se transmettent à $\left(A^X,+\right)$ et $\left(A^X,\times\right)$. Par exemple, $\mathbb{R}^{\mathbb{R}}$ est un anneau, 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) $\quad a\times 0_A=0_A\times a=0_A$.

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

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

(iv) Pour tout $n\in\mathbb{N}$, si a et b commutent, i.e. si $ab=ba$:

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

Attention ! Dans (iv), l'hypothèse selon laquelle A et B commutent est essentielle, c'est déjà très clair pour $k=2$: $(a+b)^2=(a+b)(a+b)=a^2+ab+ba+b^2\overset{ab=ba}{=}a^2+2ab+b^2\qquad$ 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 : $\quad a\times 0_A+a\times 0_A=a\times(0_A+0_A)=a\times 0_A$, $\quad$ on simplifie par $a\times 0_A$ dans le groupe $(A,+)$: $\quad a\times 0_A=0_A$. 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 $n = -1$: $ab + a(-b) = a(b-b) = a \times 0_A \overset{\text{(i)}}{=} 0_A$, donc $-(ab) = a(-b)$.
Finalement, $-n \in \mathbb{N}$ pour $n \in \mathbb{Z}$ négatif, donc d'après ce qui précède :
$$n(ab) = (-n)\big(-(ab)\big) = (-n)\big((-a)b\big) = \big((-n)(-a)\big)b = (na)b.$$
(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 dans $\mathbb{C}$. ∎

Définition-théorème **(Produit d'anneaux)** Soient $A_1, \ldots, A_n$ des anneaux. Muni de sa loi produit, $A_1 \times \ldots \times A_n$ est un anneau appelé l'*anneau produit de* $A_1, \ldots, A_n$.

À présent, l'égalité $0_A = 1_A$ est-elle possible dans un anneau A ? Le cas échéant, $a = a \times 1_A = a \times 0_A = 0_A$ pour tout $a \in A$, donc $A = \{0_A\}$. Ce genre d'anneau est qualifié d'*anneau nul* et ne présente aucun intérêt.

Définition **(Anneau intègre)** Soit A un anneau. On dit que A est *intègre* si A est NON NUL et si :
$$\forall a, b \in A, \quad \big(ab = 0_A \implies a = 0_A \text{ ou } b = 0_A\big),$$
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 ?
$$ax = ay \not\Longrightarrow a = 0_A \text{ ou } x = y \qquad \text{et} \qquad a^2 = b^2 \not\Longrightarrow a = b \text{ ou } a = -b.$$

Exemple Les anneaux $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$ et $\mathbb{Z}$ sont intègres, mais $\mathcal{M}_n(\mathbb{K})$ ne l'est pas pour $n \geqslant 2$ car un produit de matrices non nulles peut être nul.

Exemple L'anneau produit $A \times A'$ de deux anneaux non nuls A et A' n'est jamais intègre car $(1_A, 0_{A'}) \times (0_A, 1_{A'}) = (0_A, 0_{A'})$ alors que $(1_A, 0_{A'}) \neq (0_A, 0'_A)$ et $(0_A, 1_{A'}) \neq (0_A, 0_{A'})$.

Théorème **(Groupe des inversibles d'un anneau)** Soit A un anneau. L'ensemble $\mathrm{U}(A)$ des inversibles de A est un groupe pour la multiplication.

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.

Attention, un élément a de $\mathrm{U}(A)$ peut être inversible dans A : $\exists\, a' \in A, \quad aa' = a'a = 1_A$ et 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 inversibles de A, i.e. des éléments de A inversibles dans A.

Le produit de deux inversibles de A est un inversible de A, donc $\mathrm{U}(A)$ est stable par produit, ce qui fait du couple $\big(\mathrm{U}(A), \times\big)$ un magma, associatif car $(A, \times)$ l'est et d'élément neutre 1_A car $1_A 1_A = 1_A$. Montrons enfin que tout élément de $\mathrm{U}(A)$ est inversible dans $\mathrm{U}(A)$. Soit $a \in \mathrm{U}(A)$. Par définition, a est inversible dans A, donc a^{-1} aussi, autrement dit $a^{-1} \in \mathrm{U}(A)$. Ainsi, a possède un inverse dans $\mathrm{U}(A)$, i.e. est inversible dans $\mathrm{U}(A)$. ∎

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

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

En particulier, tout corps est un anneau intègre.

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.

Démonstration Tout corps K est un anneau intègre, car pour tous $a, b \in K$, si $ab = 0_K$ avec $a \neq 0_K$, alors $b = 0_K$ après division par a. ∎

La notation fractionnaire $\dfrac{a}{b}$ est autorisée dans un corps pour peu que l'élément b soit non nul. A priori, $\dfrac{a}{b}$ pourrait désigner deux éléments distincts, à savoir $b^{-1}a$ et ab^{-1}, mais ces éléments sont égaux car les corps sont commutatifs.

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

3.2 Sous-anneaux

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

— A contient 0 et il est stable par différence, c'est un sous-groupe additif de $\mathcal{M}_2(\mathbb{R})$.

— A est stable par produit, donc $(A,\times)$ est un magma, qui plus est associatif d'élément neutre $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$.

Enfin, le produit matriciel est distributif sur l'addition, donc A est un anneau inclus dans $\mathcal{M}_2(\mathbb{R})$ pour les mêmes lois. Tout ceci ne fait-il pas de A un *sous-anneau de* $\mathcal{M}_2(\mathbb{R})$? Eh bien non, car A et $\mathcal{M}_2(\mathbb{R})$ n'ont pas le même élément neutre. A fortiori, leurs inversibles n'ont aucun rapport. Dans ces conditions, qu'est-ce qu'un *sous-anneau* ?

Définition **(Sous-anneau, sous-corps)** 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.

Si A et B sont des corps, on dit plutôt que B est un *sous-corps 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 $\mathcal{M}_n(\mathbb{C})$.

En pratique, on utilise la caractérisation suivante pour montrer qu'une partie d'un anneau en est un sous-anneau. On la démontre comme son analogue pour les groupes.

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)
- $1_A \in B$. ← Attention, c'est 1_A, pas 0_A !
- B est stable par différence : $\forall b, b' \in B, \quad b - b' \in B$.
- B est stable par produit : $\forall b, b' \in B, \quad bb' \in B$.

Si A est un corps et si on veut montrer que B en est un sous-corps, il faut vérifier en plus que B^* est stable par inversion : $\forall b \in B^*, \quad b^{-1} \in B$.

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

Démonstration Pour commencer, $\mathscr{C}(\mathbb{R},\mathbb{R}) \subset \mathbb{R}^{\mathbb{R}}$ et la fonction $x \longmapsto 1$ est continue sur $\mathbb{R}$. Ensuite, il est bien connu que $\mathscr{C}(\mathbb{R},\mathbb{R})$ est stable par différence et produit.

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 $\mathrm{U}(B)$ possède un inverse dans B, donc dans A car $B \subset A$. 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 $\mathcal{M}_n(\mathbb{K})$.

Ici : $\mathrm{U}\big(\mathcal{T}_n(\mathbb{K})\big) = \mathrm{GL}_n(\mathbb{K}) \cap \mathcal{T}_n(\mathbb{K}) = \mathrm{U}\big(\mathcal{M}_n(\mathbb{K})\big) \cap \mathcal{T}_n(\mathbb{K})$, mais l'égalité $\mathrm{U}(B) = \mathrm{U}(A) \cap B$ n'a rien de général.

Démonstration Pour commencer, $\mathcal{T}_n(\mathbb{K}) \subset \mathcal{M}_n(\mathbb{K})$ et $I_n \in \mathcal{T}_n(\mathbb{K})$. Ensuite, nous avons déjà vu que $\mathcal{T}_n(\mathbb{K})$ est stable par différence et produit. Pour finir, $\mathrm{U}\big(\mathcal{T}_n(\mathbb{K})\big)$ est l'ensemble des matrices triangulaires supérieures inversibles de $\mathcal{M}_n(\mathbb{K})$ dont l'inverse est triangulaire supérieure. Or nous savons qu'une matrice triangulaire supérieure est inversible si et seulement si ses coefficients diagonaux sont non nuls, et le cas échéant, son inverse est encore triangulaire supérieure. La conclusion en découle.

Exemple L'ensemble $\mathbb{Z}[\mathrm{i}] = \big\{a + \mathrm{i}b \mid \quad a, b \in \mathbb{Z}\big\}$ des *entiers de Gauss* est un sous-anneau de $\mathbb{C}$ et $\mathrm{U}\big(\mathbb{Z}[\mathrm{i}]\big) = \mathbb{U}_4 = \big\{\pm 1, \pm\mathrm{i}\big\}$. De son côté, $\mathbb{Q}(\mathrm{i}) = \big\{a + \mathrm{i}b \mid \quad a, b \in \mathbb{Q}\big\}$ est un sous-corps de $\mathbb{C}$. En particulier, $\mathrm{U}\big(\mathbb{Q}(\mathrm{i})\big) = \mathbb{Q}(\mathrm{i})^*$ donc $\mathrm{U}\big(\mathbb{Z}[\mathrm{i}]\big) \neq \mathrm{U}\big(\mathbb{Q}(\mathrm{i})\big) \cap \mathbb{Z}[\mathrm{i}]$.

Démonstration

- Pour commencer, $\mathbb{Z}[\mathrm{i}] \subset \mathbb{C}$ et $\mathbb{Z}[\mathrm{i}]$ contient 1. Ensuite, pour la stabilité par soustraction et produit, pour tous $z = a + \mathrm{i}b, z' = a' + \mathrm{i}b' \in \mathbb{Z}[\mathrm{i}]$ avec $a, b, a', b' \in \mathbb{Z}$, $z - z'$ et zz' appartiennent à $\mathbb{Z}[\mathrm{i}]$ car :
$$z - z' = \underbrace{(a - a')}_{\in \mathbb{Z}} + \mathrm{i}\underbrace{(b - b')}_{\in \mathbb{Z}} \qquad \text{et} \qquad zz' = \underbrace{(aa' - bb')}_{\in \mathbb{Z}} + \mathrm{i}\underbrace{(ab' + ba')}_{\in \mathbb{Z}}.$$

- Déterminons à présent les inversibles de $\mathbb{Z}[\mathrm{i}]$. Soit $z = a+\mathrm{i}b \in \mathrm{U}\big(\mathbb{Z}[\mathrm{i}]\big)$ avec $a, b \in \mathbb{Z}$. Ainsi, $z^{-1} = a' + \mathrm{i}b'$ pour certains $a', b' \in \mathbb{Z}$, donc $1 = |1|^2 = \left|zz^{-1}\right|^2 = |z|^2\left|z^{-1}\right|^2 = \big(a^2+b^2\big)\big(a'^2+b'^2\big)$, or a^2+b^2 et $a'^2+b'^2$ sont des entiers naturels, donc $a^2+b^2 = 1$. A fortiori, $a^2 \leqslant a^2+b^2 = 1$, donc $|a| \leqslant 1$, et de même $|b| \leqslant 1$. Conclusion : $\quad a, b \in \big\{0, \pm 1\big\}, \quad$ donc $z \in \big\{\pm 1, \pm \mathrm{i}\big\}$. Réciproquement, 1 et -1 sont inversibles dans $\mathbb{Z}[\mathrm{i}]$ d'inverses eux-mêmes, i l'est d'inverse $-\mathrm{i}$ et $-\mathrm{i}$ d'inverse i.
- Comme $\mathbb{Z}[\mathrm{i}]$, $\mathbb{Q}(\mathrm{i})$ est un sous-anneau de $\mathbb{C}$, mais on veut qu'il en soit un sous-corps, il reste donc à montrer que $\mathrm{U}\big(\mathbb{Q}(\mathrm{i})\big) = \mathbb{Q}(\mathrm{i})^*$. Or pour tout $z = a+\mathrm{i}b \in \mathbb{Q}(\mathrm{i})^*$ avec $a, b \in \mathbb{Q}$, l'inverse de z dans $\mathbb{C}$ vaut $z^{-1} = \dfrac{a-\mathrm{i}b}{a^2+b^2}$ et appartient à $\mathbb{Q}(\mathrm{i})$, donc z est inversible dans $\mathbb{Q}(\mathrm{i})$.

3.3 Morphismes d'anneaux

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

$$\forall x, y \in A, \qquad f(x+y) = f(x)+f(y) \quad \text{et} \quad f(xy) = f(x)f(y).$$

Si A et A' sont des corps, on dit plutôt que f est un *morphisme de corps*.

On définit comme pour les groupes les notions d'*endomorphisme d'anneau*, d'*isomorphisme d'anneaux*, d'*automorphisme d'anneau* et d'*anneaux isomorphes*. Idem pour les corps.

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

Exemple Pour tout $P \in \mathrm{GL}_n(\mathbb{K})$, l'application $M \longmapsto PMP^{-1}$ est un automorphisme de corps de $\mathcal{M}_n(\mathbb{K})$.

Démonstration Soit $P \in \mathrm{GL}_n(\mathbb{K})$. Alors $PI_nP^{-1} = I_n$ et pour tous $M, M' \in \mathcal{M}_n(\mathbb{K})$:

$$P(M+M')P^{-1} = PMP^{-1} + PM'P^{-1} \qquad \text{et} \qquad P(MM')P^{-1} = \big(PMP^{-1}\big)\big(PM'P^{-1}\big).$$

Enfin, l'application $M \longmapsto PMP^{-1}$ est bijective de $\mathcal{M}_n(\mathbb{K})$ sur lui-même de réciproque $M \longmapsto P^{-1}MP$.

Les propriétés qui suivent se démontre comme dans le cas des groupes.

Théorème **(Propriétés des morphismes d'anneaux)** Soient A et A' deux anneaux et $f : A \longrightarrow A'$ un morphisme d'anneaux.

(i) **Loi + :** f est un morphisme de groupes additifs de A dans A'.
Ainsi, $f(0_A) = 0_{A'}$ et pour tout $x \in A$: $\quad f(-x) = -f(x)$.

(ii) **Loi × :** $f_{|\mathrm{U}(A)}$ est un morphisme de groupes multiplicatifs de $\mathrm{U}(A)$ dans $\mathrm{U}(A')$.
Ainsi, pour tout $x \in \mathrm{U}(A)$: $\quad f\big(x^{-1}\big) = f(x)^{-1}$.

(iii) **Image :** L'image de f est notée $\mathrm{Im}\, f$ et c'est un sous-anneau de A'.
En outre, f est surjectif de A sur A' si et seulement $\mathrm{Im}\, f = A'$.

(iv) **Noyau :** On appelle *noyau de f* son noyau en tant que morphisme de groupes additifs de A :

$$\mathrm{Ker}\, f = f^{-1}\big(\{0_{A'}\}\big) = \big\{x \in A \mid \quad f(x) = 0_{A'}\big\}.$$

En outre, f est injectif sur A si et seulement si $\mathrm{Ker}\, f = \{0_A\}$.

(iv) **Composition :** La composée de deux morphismes d'anneaux est un morphisme d'anneaux.

(iv) **Isomorphismes :** La composée de deux isomorphismes d'anneaux est un isomorphisme d'anneaux et la réciproque d'un isomorphisme d'anneaux est un isomorphisme d'anneaux.

Attention !

- $\mathrm{Ker}\, f$ est défini à partir de 0_A en référence à la structure additive de A et non pas à partir de 1_A.
- $\mathrm{Ker}\, f$ n'est un sous-anneau de A que s'il coïncide avec A tout entier. En effet, si $\mathrm{Ker}\, f$ contient 1_A, alors pour tout $a \in A$: $f(a) = f(a \times 1_A) = f(a)f(1_A) = f(a) \times 0_{A'} = 0_{A'}$, $\quad$ donc $\mathrm{Ker}\, f = A$.

3.4 Construction matricielle de $\mathbb{C}$

Ensembles de nombres, fonctions usuelles, notions d'intégrale et d'angle… Les objets mathématiques vous ont été présentés jusqu'ici comme s'ils allaient de soi, comme si l'intuition naïve et la parole des profs suffisaient, et ce n'est pas grave ! Oui, on arrive à faire des maths sans savoir de quoi on parle, car l'essentiel n'est pas tant de savoir ce que les objets sont que de savoir les manipuler. À partir d'un certain niveau de formation, cette approche naïve mérite toutefois d'être interrogée.

Pour commencer, faut-il croire ce que les profs racontent ? On vous a demandé de croire en l'existence de $\mathbb{R}$, cette grosse boîte noire pleine d'objets et de règles de calcul. On a re-sollicité votre foi plus récemment et vous croyez en $\mathbb{C}$. Vous croyez aussi en l'exponentielle, mais on croit parfois des bêtises. Dans tous les cas, on vous a dit sans le prouver : « Il existe un objet qui fait ceci-cela » et vous avez cru. Inutile de paniquer, on sait effectivement justifier l'existence des objets mathématiques en les *construisant*. Aujourd'hui, nous allons construire $\mathbb{C}$… mais en admettant l'existence de $\mathbb{R}$, qui demande plus de travail.

Cela dit, pourquoi est-ce important de construire les objets soi-même si on peut se contenter de les manipuler ? Les physiciens sont contents que les mathématiques aient des bases solides, mais ils n'ont pas besoin de connaître les détails pour faire de la physique. Alors pourquoi ? Premièrement, j'espère que ces questions vous intéressent. Deuxièmement, la plupart des objets mathématiques n'ont pas de contact direct avec le monde physique et leur intuition demande du travail. En étudiant soi-même des constructions d'objets, on approfondit sa propre intuition, on gagne en capacités d'abstraction et on s'offre peu à peu un accès à des objets plus fins qu'on n'aurait pas réussi à se représenter sinon.

Allez, assez bavardé, partons de $\mathbb{R}$ et construisons $\mathbb{C}$. Je prétends que $\mathbb{C}$ peut être vu comme une partie bien choisie de $\mathcal{M}_2(\mathbb{R}) = \mathbb{R}^{[\![1,2]\!]\times[\![1,2]\!]}$. En l'occurrence, notons $\mathbb{C}$ l'ensemble des matrices $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$, a et b décrivant $\mathbb{R}$, et posons $\mathrm{i} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. Et là, surprise : $\mathrm{i}^2 = -I_2$. En outre, pour tous $z = \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \in \mathbb{C}$ avec $a, b \in \mathbb{R}$: $z = aI_2 + b\mathrm{i} = \mathrm{Re}(z)\, I_2 + \mathrm{i}\,\mathrm{Im}(z)$ si on pose $\mathrm{Re}(z) = a$ et $\mathrm{Im}(z) = b$.

Montrons maintenant que $\mathbb{C}$ est un sous-anneau de $\mathcal{M}_2(\mathbb{R})$, et même que c'est un corps.

> **Démonstration** Pour commencer, $\mathbb{C} \subset \mathcal{M}_2(\mathbb{R})$ et $I_2 = \begin{pmatrix} 1 & -0 \\ 0 & 1 \end{pmatrix} \in \mathbb{C}$. Ensuite, pour la stabilité par différence et produit, pour tous $M = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}, N = \begin{pmatrix} c & -d \\ d & c \end{pmatrix} \in \mathcal{C}$:
>
> $$M - N = \begin{pmatrix} a-c & -(b-d) \\ b-d & a-c \end{pmatrix} \in \mathbb{C} \qquad \text{et} \qquad MN = \begin{pmatrix} ac-bd & -(ad+bc) \\ ad+bc & ac-bd \end{pmatrix} \in \mathbb{C}.$$
>
> Pour montrer que $\mathbb{C}$ est un corps, il nous reste à montrer qu'il est non nul en tant qu'anneau, commutatif et que ses éléments non nuls sont tous inversibles, i.e. inversibles au sens où leur inverse est encore dans $\mathbb{C}$. Pour commencer, $\mathbb{C}$ est non nul car $I_n \neq 0$. Ensuite, $\mathbb{C}$ est commutatif bien que $\mathcal{M}_2(\mathbb{R})$ ne le soit pas car avec les notations précédentes : $MN = \begin{pmatrix} ac-bd & -(ad+bc) \\ ad+bc & ac-bd \end{pmatrix} = \begin{pmatrix} ca-db & -(cb+da) \\ cb+da & ca-db \end{pmatrix} = NM$.
>
> Pour finir, soit $M = \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \in \mathbb{C}^*$. Par non-nullité de M, a ou b est non nul, donc $\det(M) = a^2 + b^2 > 0$, donc M est inversible dans $\mathcal{M}_2(\mathbb{R})$. Cela dit, $M^{-1} = \dfrac{1}{a^2+b^2}\begin{pmatrix} a & b \\ -b & a \end{pmatrix} = \begin{pmatrix} a' & -b' \\ b' & a' \end{pmatrix} \in \mathbb{C}$ si on pose $a' = \dfrac{a}{a^2+b^2}$ et $b' = -\dfrac{b}{a^2+b^2}$, donc M est inversible dans $\mathbb{C}$ comme voulu.

À ce stade, $\mathbb{C}$ ressemble au corps que nous avions en tête, mais où est $\mathbb{R}$ dans tout ça ? Gros problème ! Nous avons construit $\mathbb{C}$ comme une partie de $\mathcal{M}_2(\mathbb{R})$, donc $\mathbb{C}$ ne contient pas $\mathbb{R}$. Qu'à cela ne tienne, on vérifie aisément que l'application $x \overset{f}{\longmapsto} xI_2$ est un morphisme injectif de corps de $\mathbb{R}$ dans $\mathbb{C}$, donc un isomorphisme de $\mathbb{R}$ sur son image $\mathrm{Im}\, f$. Via cet isomorphisme, $\mathrm{Im}\, f$ est un sous-corps de $\mathbb{C}$ isomorphe à $\mathbb{R}$, i.e. une nouvelle version de $\mathbb{R}$ incluse dans $\mathbb{C}$. Finalement, pour obliger $\mathbb{R}$ à être inclus dans $\mathbb{C}$, privons le corps $\mathbb{R}$ initial du nom $\mathbb{R}$ qui lui était attribué et accordons ce nom à $\mathrm{Im}\, f$. Ça y est, $\mathbb{R}$ est inclus dans $\mathbb{C}$!

Évidemment, on préfère noter 1 la matrice I_2 quand on la voit comme un élément de $\mathbb{C}$, de sorte que pour tout $z \in \mathbb{C}$: $z = \mathrm{Re}(z) + \mathrm{i}\,\mathrm{Im}(z)$. Notre construction de $\mathbb{C}$ est achevée et le chapitre « Nombres complexes » aurait pu commencer ici.

Et finalement, que faut-il retenir de cette construction ? Rien du tout en ce qui concerne $\mathbb{C}$. Imprégnez-vous de la démarche intellectuelle générale de ce paragraphe, mais abstenez-vous impérativement de voir les nombres complexes comme des matrices 2×2. J'ai choisi de vous construire $\mathbb{C}$ matriciellement, mais d'autres constructions sont possibles et tout aussi légitimes. En principe, vous êtes maintenant convaincus que la nature mathématique ne contient pas qu'une seule version des corps $\mathbb{R}$ ou $\mathbb{C}$, mais une infinité qui se valent toutes parce qu'elles sont isomorphes. Ce paragraphe s'achève ainsi comme il a commencé — peu importe ce que les objets sont, l'essentiel est de savoir ce qu'ils nous autorisent à faire d'eux.

4 Anneaux $\mathbb{Z}/n\mathbb{Z}$ et indicatrice d'Euler

Ce paragraphe est hors programme en MPSI, mais au programme en MP.

4.1 Anneaux $\mathbb{Z}/n\mathbb{Z}$

L'anneau $\mathbb{Z}/n\mathbb{Z}$ est le petit monde qu'on obtient quand on décide de raisonner sur les entiers modulo n. Sans le savoir, nous y raisonnions déjà au chapitre « Arithmétique des entiers » quand nous résolvions certaines équations diophantiennes.

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

- **Classes de congruence modulo n :** La relation $\equiv [n]$ est une relation d'équivalence sur $\mathbb{Z}$ et pour tout $x \in \mathbb{Z}$, la classe d'équivalence de x pour cette relation est l'ensemble $\overline{x} = x + n\mathbb{Z}$. En outre, pour tous $x, y \in \mathbb{Z}$:
$$\overline{x} = \overline{y} \iff x \equiv y\ [n].$$
On note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble quotient de $\mathbb{Z}$ par $\equiv [n]$, qui est de cardinal n : $\mathbb{Z}/n\mathbb{Z} = \left\{\overline{0}, \overline{1}, \dots, \overline{n-1}\right\}$.
- **Structure d'anneau :** On définit deux lois internes $+$ et $\times$ sur $\mathbb{Z}/n\mathbb{Z}$ en posant pour tous $x, y \in \mathbb{Z}$:
$$\overline{x} + \overline{y} = \overline{x+y} \quad \text{et} \quad \overline{x} \times \overline{y} = \overline{x \times y}.$$
Le triplet $\left(\mathbb{Z}/n\mathbb{Z}, +, \times\right)$ est un anneau commutatif d'éléments neutres $\overline{0}$ pour $+$ et $\overline{1}$ pour $\times$.
Enfin, l'application $x \longmapsto \overline{x}$ est un morphisme surjectif d'anneaux de $\mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}$ de noyau $n\mathbb{Z}$.

Banale en apparence, la définition des lois internes $+$ et $\times$ sur $\mathbb{Z}/n\mathbb{Z}$ est très problématique en réalité. Pour définir $\overline{x} + \overline{y}$ dans $\mathbb{Z}/n\mathbb{Z}$, il est tentant de poser $\overline{x} + \overline{y} = \overline{x+y}$, mais après tout, $\overline{x} = \overline{x'}$ et $\overline{y} = \overline{y'}$ pour tout un tas d'autres entiers x' et y', donc pourquoi ne pas poser $\overline{x} + \overline{y} = \overline{x'+y'}$? À cause de cette marge de manœuvre sur le choix des représentants, on est peut-être en train d'attribuer plusieurs valeurs différentes à la notation $\overline{x} + \overline{y}$. La bonne nouvelle, c'est que $\overline{x+y}$ ne dépend pas des représentants de $\overline{x}$ et $\overline{y}$ choisis pour le calculer : $\forall x, x', y, y' \in \mathbb{Z},\ \left(\overline{x} = \overline{x'} \text{ et } \overline{y} = \overline{y'}\right) \implies \overline{x+y} = \overline{x'+y'}$ car l'addition est *compatible avec la relation* $\equiv [n]$:
$$\forall x, x', y, y' \in \mathbb{Z},\quad \left(x \equiv x'\ [n] \text{ et } y \equiv y'\ [n]\right) \implies x + y \equiv x' + y'\ [n].$$
Grâce à cette implication, on ne commet pas d'hérésie en notant $\overline{x} + \overline{y}$ l'élément $\overline{x+y}$. Le même raisonnement vaut pour la loi $\times$ car la multiplication est elle aussi compatible avec la relation $\equiv [n]$.

Démonstration Je montrerai seulement que $\left(\mathbb{Z}/n\mathbb{Z}, +\right)$ est un groupe commutatif, mais il n'est pas plus difficile de montrer que c'est un anneau commutatif. Soient $x, y, z \in \mathbb{Z}$.

- **Commutativité :** $\overline{x} + \overline{y} = \overline{x+y} = \overline{y+x} = \overline{y} + \overline{x}$.
- **Associativité :** $\left(\overline{x} + \overline{y}\right) + \overline{z} = \overline{x+y} + \overline{z} = \overline{(x+y)+z} = \overline{x+(y+z)} = \overline{x} + \overline{y+z} = \overline{x} + \left(\overline{y} + \overline{z}\right)$.
- **Élément neutre additif :** $\overline{x} + \overline{0} = \overline{x+0} = \overline{x}$ et $\overline{0} + \overline{x} = \overline{0+x} = \overline{x}$.
- **Opposés :** $\overline{x} + \overline{-x} = \overline{x + (-x)} = \overline{0}$ et idem dans l'autre sens, donc $\overline{x}$ est inversible pour $+$ d'opposé $\overline{-x}$.

Concernant l'application $x \overset{f}{\longmapsto} \overline{x}$, elle est surjective de $\mathbb{Z}$ sur $\mathbb{Z}/n\mathbb{Z}$ par définition de $\mathbb{Z}/n\mathbb{Z}$ et c'est un morphisme d'anneaux par définition des lois $+$ et $\times$, sachant que $f(1) = \overline{1}$ où 1 est l'élément neutre multiplicatif de $\mathbb{Z}$ et $\overline{1}$ celui de $\mathbb{Z}/n\mathbb{Z}$. Enfin, pour tout $x \in \mathbb{Z}$: $x \in \operatorname{Ker} f \iff \overline{x} = \overline{0} \iff x \equiv 0\ [n] \iff x \in n\mathbb{Z}$. ■

Exemple L'équation $\overline{3}\,x = \overline{2}$ d'inconnue $x \in \mathbb{Z}/n\mathbb{Z}$ n'a pas de solution si $n = 6$ et admet $\overline{3}$ pour seule solution si $n = 7$. À ce stade, on s'en convainc aisément en testant un par un les éléments de $\mathbb{Z}/6\mathbb{Z}$ et $\mathbb{Z}/7\mathbb{Z}$.

Exemple L'équation diophantienne $3x^2 - y^2 = 1$ d'inconnue $(x, y) \in \mathbb{Z}^2$ n'a pas de solution.

Démonstration Si l'équation possède une solution (x, y), alors dans $\mathbb{Z}/3\mathbb{Z}$: $\overline{3}\,\overline{x}^2 - \overline{y}^2 = \overline{1}$, donc $\overline{y}^2 = -\overline{1}$, mais cette égalité est contradictoire car aucun carré ne vaut $-\overline{1}$ dans $\mathbb{Z}/3\mathbb{Z}$: $\overline{0}^2 = \overline{0}$, $\overline{1}^2 = \overline{1}$ et $\overline{2}^2 = \overline{1}$.

✖ **Attention !** En général, $\mathbb{Z}/n\mathbb{Z}$ n'est pas un corps, ni même un anneau intègre. Par exemple, $\overline{2} \times \overline{2} = \overline{0}$ dans $\mathbb{Z}/4\mathbb{Z}$ alors que $\overline{2} \neq \overline{0}$. En particulier, $\overline{2}$ n'est pas inversible dans $\mathbb{Z}/4\mathbb{Z}$.

Théorème (Inversibles de $\mathbb{Z}/n\mathbb{Z}$ et intégrité) Soit $n \in \mathbb{N}^*$.

(i) **Groupe des inversibles :** $\mathrm{U}\left(\mathbb{Z}/n\mathbb{Z}\right) = \left\{\overline{x} \mid \quad x \in [\![1, n-1]\!], \quad x \wedge n = 1\right\}$.

En d'autres termes, pour tout $x \in \mathbb{Z}$: $\quad \overline{x} \in \mathrm{U}\left(\mathbb{Z}/n\mathbb{Z}\right) \iff x \wedge n = 1$.

En outre, tout calcul d'inverse dans $\mathbb{Z}/n\mathbb{Z}$ se ramène à la recherche d'une relation de Bézout. Pour tout $x \in \mathbb{Z}$, tout entier $u \in \mathbb{Z}$ pour lequel $ux \equiv 1\ [n]$ est appelé UN *inverse de x modulo n*. Le cas échéant, $\overline{u}$ est l'inverse, le seul, de x dans $\mathbb{Z}/n\mathbb{Z}$.

(ii) **Intégrité :** Les assertions suivantes sont équivalentes :

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

Pour $n = p$ premier, le corps $\mathbb{Z}/p\mathbb{Z}$ est souvent noté $\mathbb{F}_p$.

Au chapitre « Arithmétique des entiers », nous avons vu que pour tous $a, b, m \in \mathbb{Z}$, si $ma \equiv mb\ [n]$ et $m \wedge n = 1$, alors $a \equiv b\ [n]$. Après coup, ce résultat raconte juste que $\overline{m}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$.

Démonstration

(i) $\overline{x} \in \mathrm{U}\left(\mathbb{Z}/n\mathbb{Z}\right) \iff \exists u \in \mathbb{Z}, \quad \overline{x}\,\overline{u} = \overline{u}\,\overline{x} = \overline{1} \iff \exists u \in \mathbb{Z}, \quad ux \equiv 1\ [n]$

$\iff \exists u, v \in \mathbb{Z}, \quad ux + nv = 1 \overset{\text{Bézout}}{\iff} x \wedge n = 1.$

(ii) Trois implications à montrer.

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

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

(ii–iii) $\Longrightarrow$ (ii–i) Si n est premier, tout élément de $[\![1, n-1]\!]$ est premier à n, donc $\mathrm{U}\left(\mathbb{Z}/n\mathbb{Z}\right) = \left(\mathbb{Z}/n\mathbb{Z}\right)^*$ d'après (i), donc $\mathbb{Z}/n\mathbb{Z}$ est un corps.

Une fois qu'on sait inverser dans $\mathbb{Z}/n\mathbb{Z}$, on sait résoudre l'équation $ax = b$ d'inconnue $x \in \mathbb{Z}/n\mathbb{Z}$ pour tous $a, b \in \mathbb{Z}/n\mathbb{Z}$ et l'équation $ax \equiv b\ [n]$ d'inconnue $x \in \mathbb{Z}$ pour tous $a, b \in \mathbb{Z}$. Précisons la situation dans le cas d'une résolution dans $\mathbb{Z}$.

— Si $a \wedge n = 1$, $\overline{a}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$, disons d'inverse $\overline{u}$, donc pour tout $x \in \mathbb{Z}$: $\quad ax \equiv b\ [n] \iff x \equiv ub\ [n]$.

— Et si $a \wedge n \neq 1$? Toute relation de la forme $ax \equiv b\ [n]$ implique que $a \wedge n$ divise b, donc l'équation $ax \equiv b\ [n]$ n'a pas de solution si $a \wedge n$ ne divise pas b. Si au contraire $a \wedge n$ divise b, alors pour tout $x \in \mathbb{Z}$: $\quad ax \equiv b\ [n] \iff a'x \equiv b'\ [n']$ si on pose $a' = \dfrac{a}{a \wedge n}$, $b' = \dfrac{b}{a \wedge n}$ et $n' = \dfrac{n}{a \wedge n}$. D'une équation modulo n, on est ramené à une équation modulo n'.

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

Démonstration $\overline{2}$ est inversible dans $\mathbb{Z}/37\mathbb{Z}$ car $2 \wedge 37 = 1$. Plus précisément, $2 \times 19 - 37 = 1$ donc $\overline{2}^{-1} = \overline{19}$. Dès lors, pour tout $x \in \mathbb{Z}/37\mathbb{Z}$: $\quad \overline{2}\,x = \overline{5} \iff x = \overline{2}^{-1}\,\overline{5} = \overline{19} \times \overline{5} = \overline{21}$.

Exemple L'équation $\overline{3}\,x = \overline{2}$ d'inconnue $x \in \mathbb{Z}/6\mathbb{Z}$ n'a pas de solution.

Démonstration Pour tout $x \in \mathbb{Z}$: $\quad \overline{3}\,\overline{x} = \overline{2} \iff 3x \equiv 2\ [6]$ et cette équation n'a pas de solution car 3 ne divise pas 2.

Exemple L'équation $\overline{6}\,x = \overline{4}$ d'inconnue $x \in \mathbb{Z}/16\mathbb{Z}$ admet $\overline{6}$ et $-\overline{2}$ pour solutions.

Démonstration Pour tout $x \in \mathbb{Z}$:

$$\begin{aligned}\overline{6}\,\overline{x} = \overline{4} &\iff 6x \equiv 4\ [16] \iff 3x \equiv 2\ [8]\\ &\iff x \equiv 3 \times 2 \equiv 6\ [8] \quad \text{car 3 est un inverse de 3 modulo 8}\\ &\iff x \equiv 6\ [16] \quad \text{ou} \quad x \equiv 14\ [16] \iff \overline{x} \in \left\{\overline{6}, -\overline{2}\right\}.\end{aligned}$$

Pourquoi deux solutions finalement ? On est passé d'une équation modulo 16 à une équation modulo 8 en divisant par 2, puis on a résolu l'équation modulo 8 et le retour modulo 16 a dédoublé la solution. Le principe est général. À méditer !

Après ces résolutions d'équations $ax \equiv b\ [n]$ d'inconnue $x \in \mathbb{Z}$, intéressons-nous maintenant à des systèmes d'équations. Le cas le plus simple est celui des systèmes $\begin{cases} x \equiv a\ [m] \\ x \equiv b\ [n] \end{cases}$ avec $m, n \in \mathbb{N}^*$ premiers entre eux et $a, b \in \mathbb{Z}$.

Cherchons-en d'abord une solution particulière. Sachant que $m \wedge n = 1$, m est inversible modulo n et n l'est modulo m, donc nous pouvons nous donner un inverse u de m modulo n et un inverse v de n modulo m. Bref, $nv \equiv 1\ [m]$ et $mu \equiv 1\ [n]$, donc $anv \equiv a\ [m]$ et $bmu \equiv b\ [n]$, donc $x_{\text{part}} = bmu + anv$ est solution du système étudié. Au-delà, pour tout $x \in \mathbb{Z}$:

$$\begin{cases} x \equiv a\ [m] \\ x \equiv b\ [n] \end{cases} \iff \begin{cases} x \equiv x_{\text{part}}\ [m] \\ x \equiv x_{\text{part}}\ [n] \end{cases} \iff m \mid (x - x_{\text{part}}) \quad \text{et} \quad n \mid (x - x_{\text{part}})$$
$$\overset{m \wedge n = 1}{\iff} \quad mn \mid (x - x_{\text{part}}) \iff x \equiv x_{\text{part}}\ [mn].$$

En résumé, la résolution d'un système mixte modulo m/modulo n avec $m \wedge n = 1$ nous a ramenés à un ensemble de solutions modulo mn. C'est exactement ce que le *théorème chinois* exprime dans le langage de l'algèbre.

Théorème **(Théorème chinois)** Soient $m, n \in \mathbb{N}^*$. Pour tout $x \in \mathbb{Z}$, on note ici $\overline{x}$ la classe de congruence de x modulo mn, $\widehat{x}$ sa classe modulo m et $\widetilde{x}$ sa classe modulo n.

Si $m \wedge n = 1$, l'application $\overline{x} \longmapsto \left(\widehat{x}, \widetilde{x}\right)$ est bien définie de $\mathbb{Z}/mn\mathbb{Z}$ dans $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ et c'est un isomorphisme d'anneaux.

Plus généralement, les anneaux $\mathbb{Z}/n_1 \dots n_r\mathbb{Z}$ et $\mathbb{Z}/n_1\mathbb{Z} \times \dots \times \mathbb{Z}/n_r\mathbb{Z}$ sont isomorphes pour tous $n_1, \dots, n_r \in \mathbb{Z}$ premiers entre eux **deux à deux**. En particulier, les anneaux $\mathbb{Z}/n\mathbb{Z}$ et $\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \times \dots \times \mathbb{Z}/p_r^{\alpha_r}\mathbb{Z}$ sont isomorphes si la factorisation première de n s'écrit $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$.

Démonstration Notons f l'application $x \longmapsto \left(\widehat{x}, \widetilde{x}\right)$ de $\mathbb{Z}$ dans $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Nous devons transformer f en une application $\overline{f}$ de $\mathbb{Z}/m\mathbb{Z}$ dans $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.

- Pour tous $x, x' \in \mathbb{Z}$:

$$f(x) = f(x') \iff \left(\widehat{x}, \widetilde{x}\right) = \left(\widehat{y}, \widetilde{x'}\right) \iff \widehat{x} = \widehat{x'} \quad \text{et} \quad \widetilde{x} = \widetilde{x'}$$
$$\iff x \equiv x'\ [m] \quad \text{et} \quad x \equiv x'\ [n] \iff m \mid (x - x') \quad \text{et} \quad n \mid (x - x')$$
$$\overset{m \wedge n = 1}{\iff} mn \mid (x - x') \iff x \equiv x'\ [mn] \iff \overline{x} = \overline{x'}.$$

  Bref : $\forall x, x' \in \mathbb{Z}, \quad \overline{x} = \overline{x'} \implies f(x) = f(x')$. Ainsi, f est incapable de distinguer les éléments d'une même classe de congruence modulo mn, elle donne la même image à tous les éléments de $\overline{x}$. Cette indifférence de f aux éléments de $\overline{x}$ nous permet de poser $\overline{f}\left(\overline{x}\right) = f(x)$ pour tout $x \in \mathbb{Z}$. On définit ainsi une nouvelle application $\overline{f}$ de $\mathbb{Z}/mn\mathbb{Z}$ dans $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, injective par construction car pour tous $x, x' \in \mathbb{Z}$, si $\overline{f}\left(\overline{x}\right) = \overline{f}\left(\overline{x'}\right)$, alors $f(x) = f(x')$, donc $\overline{x} = \overline{x'}$.

- Montrons que $\overline{f}$ est un morphisme d'anneaux. Or $\overline{f}\left(\overline{1}\right) = f(1) = \left(\widehat{1}, \widetilde{1}\right)$ et pour tous $x, y \in \mathbb{Z}$:
  $$\overline{f}\left(\overline{x+y}\right) = f(x+y) = \left(\widehat{x+y}, \widetilde{x+y}\right) = \left(\widehat{x} + \widehat{y}, \widetilde{x} + \widetilde{y}\right) = \left(\widehat{x}, \widetilde{x}\right) + \left(\widehat{y}, \widetilde{y}\right) = f(x) + f(y) = \overline{f}\left(\overline{x}\right) + \overline{f}\left(\overline{y}\right)$$
  et de même, $\overline{f}\left(\overline{xy}\right) = \overline{f}\left(\overline{x}\right)\overline{f}\left(\overline{y}\right)$.

- À ce stade, $\overline{f}$ est injective de $\mathbb{Z}/mn\mathbb{Z}$ dans $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, mais $\left|\mathbb{Z}/mn\mathbb{Z}\right| = mn = \left|\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}\right|$, donc $\overline{f}$ est en fait bijective. On aurait cela dit pu montrer la surjectivité à la main, c'est exactement ce que nous avons fait en résolvant plus haut le système $\begin{cases} x \equiv a\ [m] \\ x \equiv b\ [n], \end{cases}$ qu'on peut écrire $\overline{f}\left(\overline{x}\right) = \left(\widehat{a}, \widetilde{b}\right)$.

Exemple En particulier, $\mathbb{Z}/6\mathbb{Z}$ et $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ sont isomorphes en tant que groupes additifs.

4.2 Indicatrice d'Euler

Définition-théorème **(Indicatrice d'Euler)** On pose pour tout $n \in \mathbb{N}^*$:

$$\varphi(n) = \left|\mathrm{U}\left(\mathbb{Z}/n\mathbb{Z}\right)\right| = \left|\left\{k \in [\![1, n-1]\!] \mid \quad k \wedge n = 1\right\}\right|.$$

La fonction φ ainsi définie est appelée l'*indicatrice d'Euler*.

(i) Pour tous $m, n \in \mathbb{N}^*$ premiers entre eux : $\quad \varphi(mn) = \varphi(m)\,\varphi(n)$.

(ii) Pour tout $n \in \mathbb{N}^*$: $\quad \varphi(n) = \prod_{p \mid n} p^{v_p(n)-1}(p-1)$ où l'indice p est un nombre premier.

(iii) Pour tout $n \in \mathbb{N}^*$: $\quad n = \sum_{d \mid n} \varphi(d)$ où l'entier d est positif.

Par exemple : $\quad \varphi(360) = \varphi\left(2^3 \times 3^2 \times 5\right) = 2^{3-1}(2-1) \times 3^{2-1}(3-1) \times 5^{1-1}(5-1) = 4 \times 6 \times 4 = 96.$

Démonstration

(i) Soient $m,n\in\mathbb{N}^*$ premiers entre eux. Le théorème chinois nous fournit un isomorphisme d'anneaux f de $\mathbb{Z}/mn\mathbb{Z}$ sur $\mathbb{Z}/m\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}$. Par restriction, nous en tirons un isomorphisme de groupes de $\mathrm{U}\left(\mathbb{Z}/mn\mathbb{Z}\right)$ sur $\mathrm{U}\left(\mathbb{Z}/m\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}\right)=\mathrm{U}\left(\mathbb{Z}/m\mathbb{Z}\right)\times\mathrm{U}\left(\mathbb{Z}/n\mathbb{Z}\right)$. En particulier :

$$\varphi(mn)=\left|\mathrm{U}\left(\mathbb{Z}/mn\right)\right|=\left|\mathrm{U}\left(\mathbb{Z}/m\mathbb{Z}\right)\times\mathrm{U}\left(\mathbb{Z}/n\mathbb{Z}\right)\right|=\left|\mathrm{U}\left(\mathbb{Z}/m\mathbb{Z}\right)\right|\times\left|\mathrm{U}\left(\mathbb{Z}/n\mathbb{Z}\right)\right|=\varphi(m)\varphi(n).$$

(ii) Pour commencer, pour tous $p\in\mathbb{P}$ et $\alpha\in\mathbb{N}^*$:

$$\varphi\left(p^\alpha\right)=\left|\mathrm{U}\left(\mathbb{Z}/p^\alpha\mathbb{Z}\right)\right|=\left|\left\{x\in[\![1,p^\alpha-1]\!]\ \middle|\ x\wedge p^\alpha=1\right\}\right|\overset{p\in\mathbb{P}}{=}\left|\left\{x\in[\![1,p^\alpha-1]\!]\ \middle|\ p\not| x\right\}\right|,$$

or $[\![1,p^\alpha-1]\!]$ contient $p^\alpha-1$ éléments en tout, dont $p^{\alpha-1}-1$ exactement sont divisibles par p — les entiers pk, k décrivant $[\![1,p^{\alpha-1}-1]\!]$ — donc par différence : $\varphi\left(p^\alpha\right)=(p^\alpha-1)-(p^{\alpha-1}-1)=p^{\alpha-1}(p-1)$.

En retour, pour tout $n\in\mathbb{N}^*$: $\varphi(n)=\varphi\left(\prod_{p\mid n}p^{v_p(n)}\right)\overset{\text{(i)}}{=}\prod_{p\mid n}\varphi\left(p^{v_p(n)}\right)=\prod_{p\mid n}p^{v_p(n)-1}(p-1)$.

(iii) Soit $n\in\mathbb{N}^*$. Intéressons-nous à l'application $x\overset{f}{\longmapsto}x\wedge n$ de $[\![1,n]\!]$ dans $\mathbb{N}^*$. Son image est l'ensemble des diviseurs positifs de n. Groupons alors les éléments de $[\![1,n]\!]$ en fonction de la valeur que f leur attribue : $[\![1,n]\!]=\bigsqcup_{d\mid n}f^{-1}\left(\{d\}\right)$. En particulier : $n=\sum_{d\mid n}\left|f^{-1}\left(\{d\}\right)\right|$.

Or pour tout diviseur positif d de n et tout $x\in[\![1,n]\!]$:

$$x\in f^{-1}\left(\{d\}\right)\iff f(x)=d\iff x\wedge n=d\iff d\mid x\quad\text{et}\quad\frac{x}{d}\wedge\frac{n}{d}=1.$$

L'application $x\longmapsto\dfrac{x}{d}$ est ainsi bijective de $f^{-1}\left(\{d\}\right)$ sur $\left\{y\in\left[\!\left[1,\dfrac{n}{d}\right]\!\right]\ \middle|\ y\wedge\dfrac{n}{d}=1\right\}$ — réfléchissez-y calmement. En particulier, $\left|f^{-1}\left(\{d\}\right)\right|=\varphi\left(\dfrac{n}{d}\right)$.

Finalement, l'application $d\longmapsto\dfrac{n}{d}$ étant bijective de l'ensemble des diviseurs positifs de n sur lui-même — de réciproque elle-même : $n=\sum_{d\mid n}\varphi\left(\dfrac{n}{d}\right)\overset{d'=\frac{n}{d}}{=}\sum_{d'\mid n}\varphi(d')$. ∎

5 Groupes monogènes et ordre d'un élément

5.1 Parties génératrices et groupes monogènes

Définition **(Sous-groupe engendré par une partie, groupe monogène)** Soient G un groupe et X une partie de G.

- **Sous-groupe engendré :** L'intersection de tous les sous-groupes de G contenant X est appelée le *sous-groupe de G engendré par X* et noté $\langle X\rangle$. À ce titre, $\langle X\rangle$ est le plus petit sous-groupe de G contenant X.

  En particulier, tout sous-groupe de G qui contient X contient $\langle X\rangle$.

  Plus concrètement, $\langle X\rangle$ est aussi l'ensemble de tous les produits qu'on peut former à partir des éléments de X et de leurs inverses, i.e. l'ensemble des produits $x_1^{\varepsilon_1}\dots x_n^{\varepsilon_n}$, n décrivant $\mathbb{N}$, $x_1,\dots,x_n$ décrivant X et $\varepsilon_1,\dots,\varepsilon_n$ valant ±1. Pour $n=0$, le produit vide vaut 1_G.

- **Partie génératrice, groupe monogène :**
  - On dit que X est une *partie génératrice de G* ou que X *engendre G* si $G=\langle X\rangle$.
  - On dit que G est *monogène* s'il est engendré par un seul élément, i.e. si $G=\langle x\rangle$ pour un certain $x\in G$. Le cas échéant, un tel x est appelé un *générateur de G*.
  - On dit que G est *cyclique* s'il est à la fois monogène et fini.

Si G est monogène engendré par x, alors $G=\langle x\rangle=\left\{x^k\ \middle|\ k\in\mathbb{Z}\right\}$. En particulier, G est commutatif car pour tous $m,n\in\mathbb{Z}$: $x^mx^n=x^nx^m$.

Si X est une paire $\{x,y\}$, le sous-groupe $\langle X\rangle=\langle x,y\rangle$ contient tous les x^k et y^k, k décrivant $\mathbb{Z}$, mais aussi tous les x^iy^j et y^jx^i, i et j décrivant $\mathbb{Z}$, mais aussi encore beaucoup de monde : $x^2y^4x^{-1}$, $yx^{-2}y^4x$, $xy^2x^{-3}y^{13}x^5\dots$ Si jamais x et y commutent, alors $\langle x,y\rangle=\left\{x^iy^j\ \middle|\ i,j\in\mathbb{Z}\right\}$, mais dans le cas général, $\langle x,y\rangle$ est plus compliqué à décrire.

Si G est commutatif de loi notée additivement, alors pour tous $x, y \in G$: $\langle x\rangle = \{kx \mid k \in \mathbb{Z}\}$ et $\langle x, y\rangle = \{ix + jy \mid i, j \in \mathbb{Z}\}$.

Démonstration

- En tant qu'intersection de sous-groupes, $\langle X\rangle$ est un sous-groupe de G, et bien sûr il contient X. Ensuite, pour tout sous-groupe H de G contenant X, H contient $\langle X\rangle$ par définition de $\langle X\rangle$. Ainsi, $\langle X\rangle$ est le plus petit sous-groupe de G contenant X.
- Notons H l'ensemble des produits $x_1^{\varepsilon_1}\dots x_n^{\varepsilon_n}$. Il s'agit de montrer que $\langle X\rangle = H$. Or d'emblée, $\langle X\rangle$ est stable par produit-inversion et contient X, donc il contient H.

  Pour montrer l'inclusion réciproque $\langle X\rangle \subset H$, il nous suffit de montrer que H est un sous-groupe de G contenant X. Pour commencer, $H \subset G$ et $1_G \in H$ par convention du produit vide. Ensuite, H contient X car pour tout $x \in X$, $x = x_1^{\varepsilon_1}$ pour $x_1 = x$ et $\varepsilon_1 = 1$. Enfin, H est stable par produit-inversion car il est clair que le produit de deux éléments $x_1^{\varepsilon_1}\dots x_n^{\varepsilon_n}$ et l'inverse d'un tel élément sont encore de la forme $x_1^{\varepsilon_1}\dots x_n^{\varepsilon_n}$. ∎

Exemple Pour tout groupe G : $\langle 1_G\rangle = \{1_G\}$.

Exemple $\mathbb{Z}$ est monogène car $\mathbb{Z} = \langle 1\rangle$. Pour tout $n \in \mathbb{N}^*$, $\mathbb{U}_n$ et $\mathbb{Z}/n\mathbb{Z}$ sont cycliques d'ordre n car $\mathbb{U}_n = \left\langle e^{\frac{2i\pi}{n}}\right\rangle$ et $\mathbb{Z}/n\mathbb{Z} = \langle \overline{1}\rangle$.

Exemple $\left(\mathbb{Z}/2\mathbb{Z}\right)^2 = \{(\overline{0},\overline{0}),(\overline{1},\overline{0}),(\overline{0},\overline{1}),(\overline{1},\overline{1})\}$ n'est pas monogène car aucun de ses éléments ne l'engendre. Par exemple : $\langle(\overline{1},\overline{0})\rangle = \{(\overline{0},\overline{0}),(\overline{1},\overline{0})\}$. En revanche, $\{(\overline{1},\overline{0}),(\overline{0},\overline{1})\}$ est une partie génératrice de $\left(\mathbb{Z}/2\mathbb{Z}\right)^2$ car $(\overline{1},\overline{1}) = (\overline{1},\overline{0}) + (\overline{0},\overline{1})$.

Exemple S_n est engendré par ses cycles d'après l'existence de la décomposition en produit de cycles disjoints.

Le théorème suivant offre une classification complète à isomorphisme près de tous les groupes monogènes.

Théorème **(Classification des groupes monogènes)** Soit G un groupe monogène de générateur x.

- Si G est infini, l'application $k \longmapsto x^k$ est un isomorphisme de $\mathbb{Z}$ sur G.
- Si G est cyclique d'ordre n, l'application $\overline{k} \longmapsto x^k$ est bien définie de $\mathbb{Z}/n\mathbb{Z}$ dans G et c'est un isomorphisme de groupes. En outre : $G = \{1_G, x, x^2, \dots, x^{n-1}\}$ et pour tous $i, j \in \mathbb{Z}$: $x^i = x^j \iff i \equiv j\ [n]$.

En résumé, les groupes additifs $\mathbb{Z}$ et $\mathbb{Z}/n\mathbb{Z}$, n décrivant $\mathbb{N}^*$, sont les seuls groupes monogènes à isomorphisme près.

Démonstration L'application $k \overset{f}{\longmapsto} x^k$ est un morphisme de groupes de $\mathbb{Z}$ dans G, surjectif par définition de x. Son noyau est un sous-groupe de $\mathbb{Z}$, donc de la forme $\operatorname{Ker} f = m\mathbb{Z}$ pour un unique entier $m \in \mathbb{N}$.

- Si $m = 0$, f est injective car $\operatorname{Ker} f = \{0\}$, c'est un isomorphisme de $\mathbb{Z}$ sur G. En particulier, G est infini.
- Si $m \in \mathbb{N}^*$, tâchons de transformer f en une application de $\mathbb{Z}/m\mathbb{Z}$ dans G. Pour tous $k, k' \in \mathbb{Z}$:

$$f(k) = f(k') \iff f(k-k') = 1_G \iff k - k' \in \operatorname{Ker} f = m\mathbb{Z} \iff k \equiv k'\ [m] \iff \overline{k} = \overline{k'}.$$

  Ainsi, f donne la même image à tous les éléments d'une même classe de congruence modulo m. Cette indifférence de f aux éléments de $\overline{k}$ nous permet de poser $\overline{f}(\overline{k}) = f(k) = x^k$ pour tout $k \in \mathbb{Z}$. L'application $\overline{f}$ ainsi définie de $\mathbb{Z}/m\mathbb{Z}$ dans G est surjective par définition du générateur x, et injective par construction car pour tous $k, k' \in \mathbb{Z}$, si $\overline{f}(\overline{k}) = \overline{f}(\overline{k'})$, alors $f(k) = f(k')$, donc $\overline{k} = \overline{k'}$. En particulier, G est fini par bijectivité et $m = \left|\mathbb{Z}/m\mathbb{Z}\right| = |G| = n$.

  En réalité, $\overline{f}$ est même un isomorphisme de groupes de $\mathbb{Z}/n\mathbb{Z}$ sur G car pour tous $k, k' \in \mathbb{Z}$:

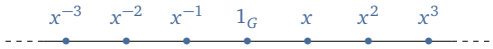
$$\overline{f}(\overline{k} + \overline{k'}) = \overline{f}(\overline{k+k'}) = x^{k+k'} = x^k x^{k'} = \overline{f}(\overline{k})\,\overline{f}(\overline{k'}).$$

  Pour finir, l'équivalence : $x^k = x^{k'} \iff k \equiv k'\ [n]$ montre que :

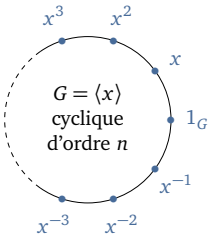
$$G = \langle x\rangle = \{x^k \mid k \in \mathbb{Z}\} = \{1_G, x, x^2, \dots, x^{n-1}\}.$$ ∎

Exemple Pour tout $n \in \mathbb{N}^*$, $\mathbb{U}_n$ est cyclique d'ordre n, donc isomorphe à $\mathbb{Z}/n\mathbb{Z}$ d'après le théorème précédent. Concrètement, l'application $\overline{k} \longmapsto e^{\frac{2ik\pi}{n}}$ est bien définie et c'est un isomorphisme de $\mathbb{Z}/n\mathbb{Z}$ sur $\mathbb{U}_n$.

Les groupes monogènes sont faciles à représenter graphiquement. Au fond, $\mathbb{Z}/n\mathbb{Z}$ et $\mathbb{U}_n$ ne sont jamais qu'une horloge à n graduations.



$G = \langle x \rangle$ monogène infini



Théorème **(Générateurs d'un groupe monogène)**

(i) $\mathbb{Z}$ n'a que deux générateurs, à savoir 1 et -1.

(ii) Pour tout $n \in \mathbb{N}^*$, les générateurs du groupe additif $\mathbb{Z}/n\mathbb{Z}$ sont les $\overline{x}$ pour lesquels $x \in [\![1, n-1]\!]$ et $x \wedge n = 1$, i.e. les inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$.

J'ai énoncé le résultat dans le seul cas des groupes $\mathbb{Z}$ et $\mathbb{Z}/n\mathbb{Z}$, mais par isomorphisme, un groupe monogène $\langle x \rangle$ admet x et x^{-1} pour seuls générateurs s'il est infini, et s'il est cyclique d'ordre n, ses générateurs sont les x^k pour lesquels $k \wedge n = 1$.

Démonstration

(i) $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$, et pour tout $x \in \mathbb{Z}$ autre que 1 et -1 : $\langle x \rangle = x\mathbb{Z} \neq \mathbb{Z}$.

(ii) Soit $n \in \mathbb{N}^*$. Pour tout $x \in \mathbb{Z}$:

$$\begin{aligned}
\langle \overline{x} \rangle = \mathbb{Z}/n\mathbb{Z} &\iff \langle \overline{x} \rangle = \left\langle \overline{1} \right\rangle \\
&\iff \overline{1} \in \langle \overline{x} \rangle \quad \text{car } \left\langle \overline{1} \right\rangle \text{ est le plus petit sous-groupe de } \mathbb{Z}/n\mathbb{Z} \text{ contenant } \overline{1} \\
&\iff \exists u \in \mathbb{Z},\ \overline{1} = u\overline{x} \iff \exists u \in \mathbb{Z},\ \overline{u}\,\overline{x} = \overline{x}\,\overline{u} = \overline{1} \\
&\iff \overline{x} \in \mathrm{U}\left(\mathbb{Z}/n\mathbb{Z}\right) \iff x \wedge n = 1.
\end{aligned}$$

5.2 Ordre d'un élément

Définition-théorème **(Ordre d'un élément)** Soient G un groupe et $x \in G$. On appelle *ordre de x* l'ordre du sous-groupe $\langle x \rangle$ — éventuellement $+\infty$. Je le noterai $|x|$, mais cette notation n'est pas universelle.

Cas d'un élément d'ordre fini : Si x est d'ordre fini, alors $\langle x \rangle = \left\{1_G, x, x^2, \dots, x^{|x|-1}\right\}$ et $|x|$ est le plus petit entier $k \in \mathbb{N}^*$ pour lequel $x^k = 1_G$. Plus précisément, pour tout $k \in \mathbb{Z}$: $x^k = 1_G \iff |x|$ divise k.

Théorème de Lagrange : Si G est fini, alors $|x|$ divise $|G|$, autrement dit $x^{|G|} = 1_G$.

Démonstration Supposons G fini. D'après le théorème de Lagrange général pour les sous-groupes, l'ordre de $\langle x \rangle$ divise alors celui de G. Ainsi, $|G| = k \times |x|$ pour un certain $k \in \mathbb{N}^*$, donc $x^{|G|} = \left(x^{|x|}\right)^k = 1_G^k = 1_G$.

Exemple

- Dans tout groupe G, l'élément neutre 1_G est d'ordre 1.
- Dans $\mathbb{C}$, tout élément x autre que 0 est d'ordre infini car $\langle x \rangle = x\mathbb{Z}$ est infini.
- Dans $\mathbb{C}^*$, $e^{\frac{2i\pi}{n}}$ est d'ordre n pour tout $n \in \mathbb{N}^*$ car $\left\langle e^{\frac{2i\pi}{n}} \right\rangle = \mathbb{U}_n$ est d'ordre n.
- Dans $\left(\mathbb{Z}/2\mathbb{Z}\right)^2$, tout élément autre que $\left(\overline{0}, \overline{0}\right)$ est d'ordre 2 car $\left\langle \left(\overline{1}, \overline{0}\right) \right\rangle = \left\{\left(\overline{0}, \overline{0}\right), \left(\overline{1}, \overline{0}\right)\right\}$.
- Dans $\mathbb{Z}/6\mathbb{Z}$, $\overline{1}$ et $\overline{5}$ sont d'ordre 6 en tant que générateurs — 1 et 5 sont premiers à 6 — mais $\overline{2}$ est d'ordre 3 et $\overline{3}$ d'ordre 2 car $\left\langle \overline{2} \right\rangle = \left\{\overline{0}, \overline{2}, \overline{4}\right\}$ et $\left\langle \overline{3} \right\rangle = \left\{\overline{0}, \overline{3}\right\}$.
- On a déjà vu que les groupes $\mathbb{U}_6$ et S_3 ne sont pas isomorphes car l'un est commutatif et l'autre non. A fortiori, $\mathbb{Z}/6\mathbb{Z}$ et S_3 ne sont pas isomorphes et on peut le comprendre autrement. Tout simplement, les isomorphismes préservent l'ordre, or $\mathbb{Z}/6\mathbb{Z}$ contient un élément d'ordre 6 alors que S_3 ne contient que des éléments d'ordre 1, 2 ou 3.

Théorème **(Théorème d'Euler et petit théorème de Fermat)**

(i) **Théorème d'Euler :** Pour tous $n \in \mathbb{N}^*$ et $x \in \mathbb{Z}$ premier à n : $x^{\varphi(n)} \equiv 1\ [n]$, i.e. $\overline{x}^{\varphi(n)} = \overline{1}$ dans $\mathbb{Z}/n\mathbb{Z}$.

(ii) **Petit théorème de Fermat :** Pour tous $p \in \mathbb{P}$ et $x \in \mathbb{Z}$: $x^p \equiv x\ [p]$, i.e. $\overline{x}^p = \overline{x}$ dans $\mathbb{Z}/p\mathbb{Z}$.

Pour tous $n \in \mathbb{N}^*$ et $x \in \mathbb{Z}$ premier à n, l'ordre de $\overline{x}$ dans le groupe multiplicatif $\mathrm{U}\left(\mathbb{Z}/n\mathbb{Z}\right)$ est appelé l'*ordre de x modulo n*.

Démonstration

(i) Dans le groupe multiplicatif $\mathrm{U}\left(\mathbb{Z}/n\mathbb{Z}\right)$, qui est d'ordre $\varphi(n)$, le théorème de Lagrange énonce que $\overline{x}^{\varphi(n)} = \overline{1}$.

(ii) Si p divise x, alors $x^p \equiv 0 \equiv x\ [p]$. Dans le cas contraire, $x \wedge p = 1$ car p est premier, donc $\overline{x}^{p-1} = \overline{x}^{\varphi(p)} = \overline{1}$ d'après le théorème d'Euler, donc $\overline{x}^p \equiv \overline{x}$ après multiplication par $\overline{x}$. ∎

Exemple Pour tout $n \geqslant 2$, n ne divise pas $2^n - 1$.

Démonstration Soit $n \geqslant 2$. Supposons par l'absurde que n divise $2^n - 1$ et notons p le plus petit diviseur premier de n, puis k l'ordre de 2 modulo p. En particulier, p divise $2^n - 1$, donc $\overline{2}^n = \overline{1}$ dans $\mathbb{Z}/p\mathbb{Z}$, donc k divise n. Cela dit, $\overline{2}^{p-1} = \overline{1}$ d'après le théorème d'Euler, donc k divise $p - 1$. Ainsi, k est un diviseur de n strictement inférieur au plus petit diviseur premier de n. Forcément $k = 1$, autrement dit $\overline{2} = \overline{1}$ — contradiction.

Théorème (Quelques propriétés de l'ordre d'un élément) Soient G un groupe et $x, y \in G$ d'ordres finis.

(i) **Conjugaison :** Pour tout $g \in G$: $\left|gxg^{-1}\right| = |x|$. Les éléments gxg^{-1} sont appelés les *conjugués de x*.

(ii) **Puissances :** Pour tout $k \in \mathbb{Z}$ premier à $|x|$: $\left|x^k\right| = |x|$ et pour tout diviseur d de $|x|$: $\left|x^d\right| = \dfrac{|x|}{d}$.

(iii) **Cas particulier de produit :** Si x et y commutent et si $|x| \wedge |y| = 1$, alors $|xy| = |x| \times |y|$.

Attention ! L'hypothèse de commutation est essentielle dans l'assertion (ii). Dans S_3, $(1\ 2)$ est d'ordre 2 et $(1\ 2\ 3)$ d'ordre 3, mais $(1\ 2)(1\ 2\ 3) = (2\ 3)$ est d'ordre 2.

Démonstration

(i) Pour tous $g \in G$ et $k \in \mathbb{Z}$: $\left(gxg^{-1}\right)^k = \left(gxg^{-1}\right)\ldots\left(gxg^{-1}\right) = gx^kg^{-1}$, donc :

$$\left(gxg^{-1}\right)^k = 1_G \iff gx^kg^{-1} = 1_G \iff x^k = 1_G,$$

donc x et gxg^{-1} ont le même ordre.

(ii) Pour tout $k \in \mathbb{Z}$ premier à $|x|$, x^k est un générateur de $\langle x\rangle$, donc $\left\langle x^k\right\rangle = \langle x\rangle$, donc x^k est d'ordre $|x|$.

À présent, soit d un diviseur de $|x|$. L'entier $\left|x^d\right|$ divise $\dfrac{|x|}{d}$ car $\left(x^d\right)^{\frac{|x|}{d}} = x^{|x|} = 1_G$. Inversement, $|x|$ divise $d \times \left|x^d\right|$ car $x^{d\times|x^d|} = \left(x^d\right)^{|x^d|} = 1_G$. A fortiori, $\dfrac{|x|}{d}$ divise $\left|x^d\right|$, donc $\left|x^d\right| = \dfrac{|x|}{d}$.

(iii) Sachant que x et y commutent, $(xy)^{|x|\times|y|} = \left(x^{|x|}\right)^{|y|}\left(y^{|y|}\right)^{|x|} = 1_G$, donc $|xy|$ divise $|x| \times |y|$.

Inversement, toujours parce que x et y commutent, $x^{|xy|}y^{|xy|} = (xy)^{|xy|} = 1_G$, donc $x^{|xy|} = y^{-|xy|}$, puis $x^{|y|\times|xy|} = \left(y^{|y|}\right)^{-|xy|} = 1_G^{-|xy|} = 1_G$. Conclusion : $|x|$ divise $|y| \times |xy|$, or $|x| \wedge |y| = 1$, donc $|x|$ divise $|xy|$ d'après le théorème de Gauss. A fortiori, $|y|$ divise $|xy|$ par symétrie des rôles de x et y. Il en découle comme voulu que $|x| \times |y|$ divise $|xy|$, toujours parce que $|x| \times |y| = 1$. ∎

Exemple Soit G un groupe cyclique d'ordre 21 de générateur x. D'après le théorème précédent, x^4 est d'ordre 21 car $4 \wedge 21 = 1$ et x^7 est d'ordre $\dfrac{21}{7} = 3$, mais qu'en est-il de x^{15} ? Coupons simplement 15 en deux en lui arrachant son PGCD avec 21 : $15 = 3 \times 5$. Ainsi, x^3 est d'ordre $\dfrac{21}{3} = 7$, et ensuite, $x^{15} = \left(x^3\right)^5$ reste d'ordre 7 car $5 \wedge 7 = 1$.

Intéressons-nous maintenant aux sous-groupes d'un groupe monogène. Les sous-groupes de $\mathbb{Z}$ sont les $n\mathbb{Z}$, n décrivant $\mathbb{N}$, donc les sous-groupes d'un groupe monogène infini $\langle x\rangle$ sont les $\langle x^n\rangle$, n décrivant $\mathbb{N}$. Et pour les groupes cycliques ?

Théorème (Sous-groupes d'un groupe cyclique) Soit G un groupe cyclique d'ordre n de générateur x. Pour tout diviseur positif d de n, on note G_d l'ensemble des éléments de G d'ordre un diviseur de d : $G_d = \left\{g \in G \mid g^d = 1_G\right\}$.

(i) Les sous-groupes de G sont exactement les G_d. En outre, pour tout diviseur positif d de n, G_d est le seul sous-groupe d'ordre d de G et $G_d = \left\langle x^{\frac{n}{d}}\right\rangle$.

(ii) Pour tous diviseurs positifs a et b de n : $G_a \subset G_b \iff a \mid b$.

Si $G = \mathbb{U}_n$, alors $G_d = \mathbb{U}_d$ pour tout diviseur positif d de n, et si $G = \mathbb{Z}/n\mathbb{Z}$, alors $G_d = \left\langle \dfrac{\overline{n}}{d} \right\rangle$ — notation additive ici !

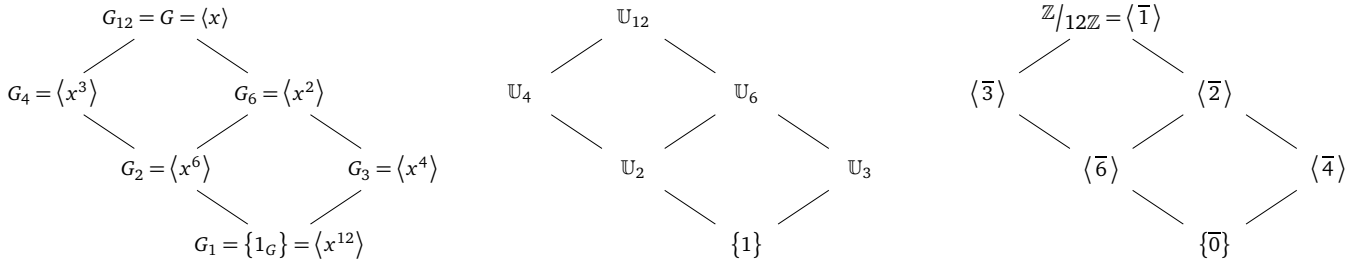
Démonstration

(i) Pour tout diviseur positif d de n, $\left\langle x^{\frac{n}{d}}\right\rangle$ est un sous-groupe d'ordre $\dfrac{n}{n/d} = d$ de G. Ensuite, $x^{\frac{n}{d}} \in G_d$ donc $\left\langle x^{\frac{n}{d}}\right\rangle \subset G_d$. Inversement, pour tout $g = x^k \in G_d$ avec $k \in \mathbb{Z}$, $x^{kd} = g^d = 1_G$, donc n divise kd d'après le théorème de Lagrange, donc $\dfrac{n}{d}$ divise k, donc $g \in \left\langle x^{\frac{n}{d}}\right\rangle$. Conclusion : $\left\langle x^{\frac{n}{d}}\right\rangle = G_d$.

Réciproquement, soit H un sous-groupe d'ordre d de G. L'application $k \overset{f}{\longmapsto} x^k$ est un morphisme de groupes de $\mathbb{Z}$ dans G, donc $f^{-1}(H)$ est un sous-groupe de $\mathbb{Z}$, donc $\left\{k \in \mathbb{Z} \mid \quad x^k \in H\right\} = f^{-1}(H) = m\mathbb{Z}$ pour un certain $m \in \mathbb{N}$. Cela dit, tout élément de H est une puissance de x car $G = \langle x\rangle$, donc $H = \left\{x^k \mid \quad k \in m\mathbb{Z}\right\} = \langle x^m\rangle$. Par ailleurs, $x^n = 1_G \in H$ donc $n \in f^{-1}(H) = m\mathbb{Z}$, i.e. m divise n. En retour, $d = |H| = \left|\langle x^m\rangle\right| = \dfrac{n}{m}$, donc d divise n, $m = \dfrac{n}{d}$ et $H = \left\langle x^{\frac{n}{d}}\right\rangle$.

(ii) $$\begin{aligned} G_a \subset G_b &\iff \left\langle x^{\frac{n}{a}}\right\rangle \subset G_b \\ &\iff x^{\frac{n}{a}} \in G_b \qquad \text{car } \left\langle x^{\frac{n}{a}}\right\rangle \text{ est le plus petit sous-groupe de } G \text{ contenant } x^{\frac{n}{a}} \\ &\iff x^{\frac{nb}{a}} = 1_G \iff n \,\Big|\, \frac{nb}{a} \iff a \mid b. \end{aligned}$$

Les figures ci-dessous représentent, pour $n = 12$, les sous-groupes de G, $\mathbb{U}_{12}$ et $\mathbb{Z}/12\mathbb{Z}$ ainsi que leur emboîtement les uns dans les autres.



Et en guise de bouquet final, une caractérisation simple du groupe S_3.

Exemple Soit G un groupe engendré par un élément r d'ordre 3 et un élément s d'ordre 2 pour lesquels $srs^{-1} = r^{-1}$. Alors G est isomorphe à S_3.

Démonstration La relation $srs^{-1} = r^{-1}$ signifie qu'en conjuguant r par s, on inverse r, mais dans la preuve qui suit, nous l'utiliserons plutôt sous la forme $sr = r^{-1}s = r^2s$.

Tout élément de G est le produit d'un certain nombre de r, s, r^{-1} et s^{-1}, mais ici $r^{-1} = r^2$ et $s^{-1} = s$, donc tout élément de G est le produit d'un certain nombre de r et s. Cela dit, la relation $sr = r^2s$ permet de déplacer de proche en proche vers la droite toutes les occurrences de s dans un tel produit, donc :

$$G = \left\{r^i s^j \mid \quad i \in [\![0,2]\!], \quad j \in \{0,1\}\right\} = \left\{1_G, r, r^2, s, rs, r^2s\right\}.$$

En particulier, $|G| \leqslant 6$. Cela dit, les éléments 1_G, r, r^2 et s sont distincts et il n'est pas dur de se convaincre que rs n'est aucun d'entre eux. Par exemple, $rs \neq 1_G$ sans quoi on aurait $r = s^{-1} = s$. De même, r^2s est distinct des 5 précédents, donc $|G| = 6$.

Dans S_3, posons à présent $\rho = (1\ 2\ 3)$ et $\sigma = (1\ 2)$. Un simple calcul montre que $S_3 = \left\{\mathrm{Id}, \rho, \rho^2, \sigma, \rho\sigma, \rho\sigma^2\right\}$. Tiens tiens ! Pour montrer que G et S_3 sont isomorphes, dressons finalement leurs tables de Cayley. Elles coïncident pour peu qu'on associe 1_G à Id, r à ρ, r^2 à ρ^2, etc. L'application sous-jacente est un isomorphisme de G sur S_3.

	1_G	r	r^2	s	rs	r^2s
1_G	1_G	r	r^2	s	rs	r^2s
r	r	r^2	1_G	rs	r^2s	s
r^2	r^2	1_G	r	r^2s	s	rs
s	s	r^2s	rs	1_G	r^2	r
rs	rs	s	r^2s	r	1_G	r^2
r^2s	r^2s	rs	s	r^2	r	1_G

	1_G	ρ	ρ^2	σ	$\rho\sigma$	$\rho^2\sigma$
1_G	1_G	ρ	ρ^2	σ	$\rho\sigma$	$\rho^2\sigma$
ρ	ρ	ρ^2	1_G	$\rho\sigma$	$\rho^2\sigma$	σ
ρ^2	ρ^2	1_G	ρ	$\rho^2\sigma$	σ	$\rho\sigma$
σ	σ	$\rho^2\sigma$	$\rho\sigma$	1_G	ρ^2	ρ
$\rho\sigma$	$\rho\sigma$	σ	$\rho^2\sigma$	ρ	1_G	ρ^2
$\rho^2\sigma$	$\rho^2\sigma$	$\rho\sigma$	σ	ρ^2	ρ	1_G