Christophe Bertault

UNE INTRODUCTION AUX STRUCTURES QUOTIENTS EN MPSI

Une théorie mathématique de l'oubli.

Hors programme en MPSI, les structures quotients requièrent peu de matériel pour être introduites et éclairent de nombreuses situations mathématiques étudiées immédiatement après le bac. Ce texte se propose d'en exposer les charmes à un niveau d'utilisation élémentaire. J'ai tenté de mettre sur l'accent sur la représentation intuitive des structures quotients sur des exemples variés plus que sur leurs usages avancés.

Les formalistes m'en voudront peut-être, mais je ne commencerai pas par les groupes quotients car le programme de MPSI ne valorise pas cette structure. Après une rapide présentation des anneaux $\frac{\mathbb{Z}}{n\mathbb{Z}}$, j'introduirai directement les espaces vectoriels quotients et la représentation qu'on peut s'en donner en lien avec le théorème du rang. Les groupes quotients ne seront étudiés qu'ensuite. Je ne parlerai pas d'anneaux quotients en revanche au-delà de l'exemple des anneaux $\frac{\mathbb{Z}}{n\mathbb{Z}}$.

La définition qui suit décrit le cadre général des structures quotients que nous nous apprêtons à explorer.

Définition-théorème **(Relation d'équivalence compatible avec une loi et loi quotient)** Soient $(E,\star)$ un magma et $\mathcal{R}$ une relation d'équivalence sur E. Pour tout $x\in E$, on note $\overline{x}$ la classe d'équivalence de x pour $\mathcal{R}$.

On dit que $\mathcal{R}$ est *compatible avec* $\star$ si pour tous $x,y,x',y'\in E$: $\quad\Big(x\mathcal{R}x' \quad\text{et}\quad y\mathcal{R}y'\Big) \quad\Longrightarrow\quad (x\star y)\mathcal{R}(x'\star y')$.

On définit dans ce cas une loi interne sur l'ensemble quotient $E\big/\mathcal{R}$ en posant pour tous $x,y\in E$: $\quad\overline{x}\star\overline{y}=\overline{x\star y}$, appelée la *loi quotient de* $\star$ *par* $\mathcal{R}$.

- Si le magma $(E,\star)$ est associatif (resp. commutatif), le magma $\big(E\big/\mathcal{R},\star\big)$ l'est aussi.
- Si le magma $(E,\star)$ possède un élément neutre e, le magma $\big(E\big/\mathcal{R}\big)$ admet $\overline{e}$ pour élément neutre. De plus, dans ce cas, si un élément x de E est inversible dans le magma $(E,\star)$, $\overline{x}$ l'est dans le magma $\big(E\big/\mathcal{R}\big)$ et : $\quad\overline{x}^{\,-1}=\overline{x^{-1}}$.
- En particulier, si $(E,\star)$ est un groupe, $\big(E\big/\mathcal{R},\star\big)$ en est un aussi.

La relation : $\quad\overline{x}\star\overline{y}=\overline{x\star y}\quad$ définit le produit des deux classes d'équivalence $\overline{x}$ et $\overline{y}$ à partir de la donnée d'UN SEUL de leurs membres, en l'occurrence x et y. Or x et y ne jouent a priori aucun rôle privilégié dans $\overline{x}$ et $\overline{y}$. La classe $\overline{x}$ coïncide avec la classe $\overline{x'}$ pour tout élément x' de E pour lequel : $\quad x\mathcal{R}x'$. La compatibilité de $\mathcal{R}$ avec $\star$ est précisément là pour garantir l'indépendance de $\overline{x\star y}$ vis-à-vis des choix divers qu'on peut faire de x et y. En cas de compatibilité, $\overline{x\star y}$ dépend de $\overline{x}$ et $\overline{y}$, mais pas vraiment du choix des éléments x et y.

Démonstration Par définition de $E\big/\mathcal{R}$, tout élément de $E\big/\mathcal{R}$ est de la forme $\overline{x}$ pour un certain $x\in E$.

- Si $(E,\star)$ est associatif, alors pour tous $x,y,z\in E$:
$$\overline{x}\star\big(\overline{y}\star\overline{z}\big)=\overline{x}\star\overline{y\star z}=\overline{x\star(y\star z)}=\overline{(x\star y)\star z}=\overline{x\star y}\star\overline{z}=\big(\overline{x}\star\overline{y}\big)\star\overline{z}.$$
- Si $(E,\star)$ est commutatif, alors pour tous $x,y\in E$: $\quad\overline{x}\star\overline{y}=\overline{x\star y}=\overline{y\star x}=\overline{y}\star\overline{x}$.
- Si $(E,\star)$ possède un élément neutre e, alors pour tout $x\in E$: $\quad\overline{x}\star\overline{e}=\overline{x\star e}=\overline{x}\quad$ et $\quad\overline{e}\star\overline{x}=\overline{e\star x}=\overline{x}$. En outre, si x est inversible dans $(E,\star)$: $\quad\overline{x}\star\overline{x^{-1}}=\overline{x\star x^{-1}}=\overline{e}\quad$ et $\quad\overline{x^{-1}}\star\overline{x}=\overline{x^{-1}\star x}=\overline{e}$, donc $\overline{x}$ est inversible dans $\big(E\big/\mathcal{R}\big)$ et : $\quad\overline{x}^{\,-1}=\overline{x^{-1}}$. ■

1 L'exemple des anneaux $\frac{\mathbb{Z}}{n\mathbb{Z}}$

- **Définition :** Soit $n \in \mathbb{N}^*$. La relation de congruence modulo n sur $\mathbb{Z}$ définie pour tous $x, y \in \mathbb{Z}$ par :

$$x \equiv y\ [n] \qquad \Longleftrightarrow \qquad x - y \in n\mathbb{Z}$$

est une relation d'équivalence dont l'ensemble quotient est généralement noté $\frac{\mathbb{Z}}{n\mathbb{Z}}$. Explicitement, pour tout $x \in \mathbb{Z}$, la classe d'équivalence de x, que nous noterons $\overline{x}$ ou parfois simplement x, est l'ensemble :

$$\overline{x} = \left\{ y \in \mathbb{Z} / \quad y \equiv x\ [n] \right\} = \left\{ x + nk \right\}_{k \in \mathbb{Z}} = x + n\mathbb{Z}.$$

Par conséquent : $\frac{\mathbb{Z}}{n\mathbb{Z}} = \left\{ \overline{x} \right\}_{x \in \mathbb{Z}} = \left\{ x + n\mathbb{Z} \right\}_{x \in \mathbb{Z}}$. Intuitivement, $\frac{\mathbb{Z}}{n\mathbb{Z}}$ est le monde qu'on obtient à partir de $\mathbb{Z}$ quand on décide d'y négliger, au sens de l'addition, l'ensemble $n\mathbb{Z}$ des multiples de n. En ce sens, quotienter c'est oublier. Quand on sait de quoi on parle, i.e. quand on sait dans quel monde on se trouve, à savoir $\mathbb{Z}$ ou $\frac{\mathbb{Z}}{n\mathbb{Z}}$, la confusion des notations x et $\overline{x}$ allège les calculs sans occasionner d'erreur.

Par exemple, dans $\mathbb{Z}$: $7 \equiv -5\ [12]$, donc dans $\frac{\mathbb{Z}}{12\mathbb{Z}}$: $\overline{7} = \overline{-5}$. Les deux entiers distincts 7 et -5 deviennent un objet unique dans $\frac{\mathbb{Z}}{12\mathbb{Z}}$. On peut aussi affirmer que : $7 = -5$, mais seulement si on garde en tête que cette égalité est une égalité dans $\frac{\mathbb{Z}}{12\mathbb{Z}}$ et non dans $\mathbb{Z}$!

- **Cardinal :** Indexé par l'ensemble infini $\mathbb{Z}$, $\frac{\mathbb{Z}}{n\mathbb{Z}}$ n'est pas pour autant lui-même un ensemble infini. Il faut évoquer le théorème de la division euclidienne pour le comprendre :

$$\forall x \in \mathbb{Z}, \quad \exists\,!\,(q,r) \in \mathbb{Z} \times \mathbb{Z} / \quad x = nq + r \quad \text{et} \quad 0 \leqslant r < n,$$

qu'on peut aussi écrire : $\forall x \in \mathbb{Z}, \quad \exists\,!\, r \in [\![0, n-1]\!] / \quad x \equiv r\ [n]$, et même : $\forall x \in \mathbb{Z}, \quad \exists\,!\, r \in [\![0, n-1]\!] / \quad \overline{x} = \overline{r}$. Or cette proposition n'est rien d'autre que la bijectivité de l'application $r \longmapsto \overline{r}$ de $[\![0, n-1]\!]$ dans $\frac{\mathbb{Z}}{n\mathbb{Z}}$. Il en découle que : $\left| \frac{\mathbb{Z}}{n\mathbb{Z}} \right| = n$, et plus précisément que : $\frac{\mathbb{Z}}{n\mathbb{Z}} = \left\{ \overline{x} \right\}_{x \in [\![0, n-1]\!]}$.

- **Structure d'anneau :** À ce stade, $\frac{\mathbb{Z}}{n\mathbb{Z}}$ n'est qu'un ensemble, autrement dit un désert, et nous ne pouvons rien en faire. Les choses commenceront à être amusantes quand nous pourrons y mener des calculs. Or il est bien connu que la relation d'équivalence $\equiv\ [n]$ est compatible avec les lois d'addition et de multiplication sur $\mathbb{Z}$. Cette compatibilité nous permet de définir deux lois internes sur $\frac{\mathbb{Z}}{n\mathbb{Z}}$ en posant pour tous $x, y \in \mathbb{Z}$: $\overline{x} + \overline{y} = \overline{x + y}$ et $\overline{x} \times \overline{y} = \overline{x \times y}$. Muni de ces lois, $\frac{\mathbb{Z}}{n\mathbb{Z}}$ est un anneau commutatif d'élément neutre additif $\overline{0}$ et d'élément neutre multiplicatif $\overline{1}$.

En résumé :

Théorème (Anneaux $\frac{\mathbb{Z}}{n\mathbb{Z}}$) Pour tout $n \in \mathbb{N}^*$, $\frac{\mathbb{Z}}{n\mathbb{Z}}$ est un anneau de cardinal n.

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

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

Pour de plus grandes valeurs de n, la résolution des équations de la forme : $ax = b$ d'inconnue $x \in \frac{\mathbb{Z}}{n\mathbb{Z}}$ avec $a, b \in \frac{\mathbb{Z}}{n\mathbb{Z}}$ requiert qu'on sache diviser si possible dans $\frac{\mathbb{Z}}{n\mathbb{Z}}$ comme on le fait dans les anneaux $\mathbb{C}$ ou $\mathcal{M}_n(\mathbb{C})$. Dans $\mathbb{C}$ qui est un corps, le seul élément non inversible est 0. La description des matrices inversibles de $\mathcal{M}_n(\mathbb{C})$ est plus complexe, mais l'algorithme du pivot est sans faille. Et dans $\frac{\mathbb{Z}}{n\mathbb{Z}}$?

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

Démonstration $\overline{x}\in \mathrm{U}\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right) \iff \exists\, y\in\mathbb{Z}/\quad \overline{x}\,\overline{y}=\overline{y}\,\overline{x}=\overline{1} \iff \exists\, y\in\mathbb{Z}/\quad xy\equiv 1\,[n]$

$\iff \exists\, y,z\in\mathbb{Z}/\quad xy+nz=1 \overset{\text{Bézout}}{\iff} x\wedge n=1.$ ■

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

Par exemple, 10 est inversible dans $\frac{\mathbb{Z}}{23\mathbb{Z}}$ car : $10\wedge 23=1$, et après calcul : $7\times 10-3\times 23=1$, donc dans $\frac{\mathbb{Z}}{23\mathbb{Z}}$: $7\times 10=1$. Conclusion : $10^{-1}=7$.

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

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

Le théorème qui précède montre que $\frac{\mathbb{Z}}{n\mathbb{Z}}$ n'est pas un corps en général, on ne peut donc pas y mener les calculs avec autant de facilité que dans $\mathbb{C}$. Par exemple, l'anneau $\frac{\mathbb{Z}}{4\mathbb{Z}}$ n'est pas intègre, donc ce n'est pas non plus un corps car : $2\times 2=0$ alors que : $2\neq 0$. À quelle condition $\frac{\mathbb{Z}}{n\mathbb{Z}}$ est-il un anneau intègre, voire un corps ?

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

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

Démonstration

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

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

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

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

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

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

Le petit théorème de Fermat trouve quant à lui une expression très simple dans le cadre de l'arithmétique modulaire. Nous y reviendrons davantage quand nous aurons introduit les groupes quotients.

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

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

Démonstration Nous allons donner de ce résultat une preuve plus typique de $\dfrac{\mathbb{Z}}{p\mathbb{Z}}$ que celle qu'on en donne généralement dans $\mathbb{Z}$. Fixons $x \in \dfrac{\mathbb{Z}}{p\mathbb{Z}} \setminus \{0\}$, inversible car $\dfrac{\mathbb{Z}}{p\mathbb{Z}}$ est un CORPS, et notons π le produit $\prod_{y \neq 0} y$ de tous les éléments non nuls de $\dfrac{\mathbb{Z}}{p\mathbb{Z}}$, que nous pouvons définir ici sans nous soucier de l'ordre dans lequel les termes sont multipliés. L'application $y \longmapsto x^{-1}y$ peut nous servir à y réaliser un changement d'indice car elle est bijective de $\dfrac{\mathbb{Z}}{p\mathbb{Z}} \setminus \{0\}$ sur lui-même de réciproque $z \longmapsto xz$. Ainsi : $\quad \pi \overset{z=x^{-1}y}{=} \prod_{z \neq 0} (xz) = \prod_{z \neq 0} x \prod_{z \neq 0} z = x^{p-1}\pi.$ Divisons par π, qui est non nul : $\quad x^{p-1} = 1.$ ∎

Voici pour finir un résultat moins important mais non moins joli dont la preuve ne se comprend bien que dans le cadre de l'arithmétique modulaire. Des deux congruences qui suivent, seule la première est à proprement parler le *théorème de Wilson*.

Théorème **(Théorème de Wilson)** Pour tout $p \in \mathbb{P}$: $\quad (p-1)! = -1 \quad$ dans $\dfrac{\mathbb{Z}}{p\mathbb{Z}}$.

En outre, si p est impair : $\quad \left(\dfrac{p-1}{2}\right)!^2 = (-1)^{\frac{p+1}{2}}.$

Démonstration Pour le premier point, $(p-1)! = 1 \times 2 \times \ldots \times (p-1)$ est le produit de tous les éléments non nuls de $\dfrac{\mathbb{Z}}{p\mathbb{Z}}$, donc tout élément inversible de $\dfrac{\mathbb{Z}}{p\mathbb{Z}}$ figure dans ce produit avec son inverse. Or certains éléments coïncident peut-être avec leur inverse, mais lesquels ? Pour tout $x \in \dfrac{\mathbb{Z}}{p\mathbb{Z}} \setminus \{0\}$:

$$x = x^{-1} \iff x^2 = 1 \overset{\text{Intégrité}}{\iff} x = 1 \quad \text{ou} \quad x = -1.$$

Regroupons ainsi tout élément avec son inverse dans le produit $(p-1)!$: $\quad (p-1)! = 1 \times (-1) = -1.$ Le théorème de Wilson est démontré. Pour le deuxième point, p étant impair :

$$(p-1)! = \prod_{k=1}^{p-1} k = \prod_{k=1}^{\frac{p-1}{2}} k \prod_{k=\frac{p+1}{2}}^{p-1} k \overset{l=p-k}{=} \prod_{k=1}^{\frac{p-1}{2}} k \prod_{l=1}^{\frac{p-1}{2}} (-l) = (-1)^{\frac{p-1}{2}} \left(\prod_{k=1}^{\frac{p-1}{2}} k\right)^2 = (-1)^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)!^2,$$

et donc d'après le théorème de Wilson : $\quad \left(\dfrac{p-1}{2}\right)!^2 = (-1)^{\frac{p+1}{2}}.$ ∎

Exemple Soit $p \in \mathbb{P}$. On s'intéresse à l'équation : $\quad x^2 + 2x + 2 = 0 \quad$ d'inconnue $x \in \dfrac{\mathbb{Z}}{p\mathbb{Z}}$ sous l'hypothèse que : $\quad p \equiv 1\ [4].$

Ainsi, par hypothèse : $\quad \dfrac{p+1}{2} \equiv 1\ [2], \quad$ donc d'après le corollaire du théorème de Wilson : $\quad \left(\dfrac{p-1}{2}\right)!^2 \equiv (-1)^{p+1} = -1.$

Ainsi, pour tout $x \in \dfrac{\mathbb{Z}}{p\mathbb{Z}}$: $\quad x^2 + 2x + 2 = (x+1)^2 + 1 = (x+1))^2 - \left(\dfrac{p-1}{2}\right)!^2, \quad$ donc :

$$x^2 + 2x + 2 = 0 \overset{\text{Intégrité}}{\iff} x = -1 + \left(\frac{p-1}{2}\right)! \quad \text{ou} \quad x = -1 - \left(\frac{p-1}{2}\right)!.$$

2 Espaces vectoriels quotients

Dans ce paragraphe, $\mathbb{K}$ désigne un corps quelconque, typiquement $\mathbb{R}$ ou $\mathbb{C}$, mais pourquoi pas $\dfrac{\mathbb{Z}}{p\mathbb{Z}}$ pour tout $p \in \mathbb{P}$.

Définition-théorème (Congruence modulo un sous-espace vectoriel) Soient E un $\mathbb{K}$-espace vectoriel et F un sous-espace vectoriel de E. On appelle *relation de congruence modulo F sur E* la relation définie pour tous $x, y \in E$ par :

$$x \equiv y\ [F] \quad \Longleftrightarrow \quad x - y \in F.$$

Cette relation $\equiv\ [F]$ est une relation d'équivalence sur E. On note $\dfrac{E}{F}$ l'ensemble quotient associé, et généralement, pour tout $x \in E$, $\overline{x}$ la classe d'équivalence de x : $\overline{x} = x + F$, aussi appelée la *classe de x modulo F*.

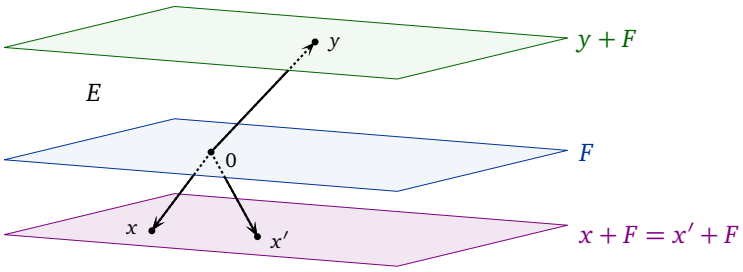
Pour tout $x \in E$, $\overline{x}$ n'est jamais que le sous-espace affine de E de direction F passant par x.

Démonstration

- **Réflexivité :** Pour tout $x \in E$: $x - x = 0 \in F$, donc : $x \equiv x\ [F]$.
- **Symétrie :** Pour tous $x, y \in E$, si : $x \equiv y\ [F]$, alors : $x - y \in F$, mais F est stable par passage à l'opposé, donc : $y - x \in F$, i.e. : $y \equiv x\ [F]$.
- **Transitivité :** Pour tous $x, y, z \in E$, si : $x \equiv y\ [F]$ et $y \equiv z\ [F]$, alors : $x - y \in F$ et $y - z \in F$, mais F est stable par addition, donc : $x - z = (x - y) + (y - z) \in F$, i.e. : $x \equiv z\ [F]$.
- **Classes d'équivalence :** Pour tout $x \in E$: $\overline{x} = \left\{ y \in E /\quad y \equiv x\ [F] \right\} = \left\{ x + f \right\}_{f \in F} = x + F$. ■

Quelles propriétés du sous-espace vectoriel F avons-nous finalement utilisé pour démontrer ce théorème ? Pour la réflexivité, le fait que F contienne 0. Pour la symétrie, le fait qu'il soit stable par passage à l'opposé. Et pour la transitivité, le fait qu'il soit stable par somme. En résumé, nous avons seulement eu besoin de savoir que F est un **sous-groupe de E**. Cette remarque éclaire en retour l'exemple arithmétique des relations $\equiv\ [n]$ sur $\mathbb{Z}$, définies à partir de l'ensemble $n\mathbb{Z}$ qui a le bon goût lui aussi d'être un sous-groupe de $\mathbb{Z}$. La notion de congruence ne nécessite ni plus ni moins qu'un sous-groupe.

Tâchons à présent de nous représenter géométriquement l'ensemble quotient $\dfrac{E}{F}$. Tout simplement, alors que E est la réunion des sous-espaces affines $x + F$, x décrivant E, $\dfrac{E}{F}$ est l'ensemble dont les éléments sont ces sous-espaces. En d'autres termes, les sous-espaces affines $x + F$ sont des parties de E, mais des éléments de $\dfrac{E}{F}$.



$$\frac{E}{F} = \left\{ \underset{x+F}{\square},\ \underset{F}{\square},\ \underset{y+F}{\square},\ \dots \right\}.$$

Définition-théorème (Espace vectoriel quotient) Soient E un $\mathbb{K}$-espace vectoriel et F un sous-espace vectoriel de E. Pour tout $x \in E$, on note $\overline{x}$ la classe de x modulo F.

- La relation d'équivalence $\equiv\ [F]$ est compatible avec l'addition. On définit donc une loi interne sur $\dfrac{E}{F}$ en posant pour tous $x, y \in E$: $\overline{x} + \overline{y} = \overline{x + y}$.
- La relation d'équivalence $\equiv\ [F]$ est compatible avec la loi externe au sens où pour tous $x, x' \in E$ et $\lambda \in \mathbb{K}$:

$$x \equiv x'\ [F] \quad \Longrightarrow \quad \lambda \cdot x \equiv \lambda \cdot x'\ [F].$$

  On peut ainsi définir une loi externe sur $\dfrac{E}{F}$ en posant pour tous $x \in E$ et $\lambda \in \mathbb{K}$: $\lambda \cdot \overline{x} = \overline{\lambda \cdot x}$.

Muni de ces opérations, $\dfrac{E}{F}$ est un $\mathbb{K}$-espace vectoriel de vecteur nul $\overline{0} = F$ appelé le *quotient de E par F*.

La nouveauté de ce théorème, c'est que les sous-espaces affines $x+F$, x décrivant E, peuvent être vus comme des VECTEURS dans $\frac{E}{F}$. On peut les additionner et les multiplier par un scalaire.

Démonstration

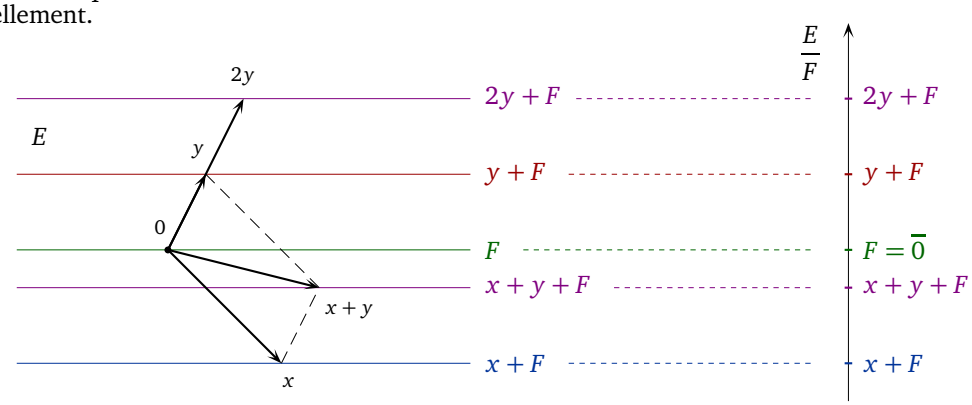
- **Compatibilité avec l'addition :** Soient $x,y,x',y' \in E$. Si : $x \equiv x'\ [F]$ et $y \equiv y'\ [F]$, alors : $x-x' \in F$ et $y-y' \in F$, donc F étant stable par addition : $(x+y)-(x'+y') \in F$, autrement dit : $x+y \equiv x'+y'\ [F]$.
- **Compatibilité avec la multiplication par un scalaire :** Soient $x,x' \in E$ et $\lambda \in \mathbb{K}$. Si : $x \equiv x'\ [F]$, alors : $x-x' \in F$, donc F étant stable par multiplication par un scalaire : $\lambda \cdot x - \lambda \cdot x' = \lambda \cdot (x-x') \in F$, autrement dit : $\lambda \cdot x \equiv \lambda \cdot x'\ [F]$.

  Les axiomes de la loi externe $\cdot$ de $\frac{E}{F}$ qui en font un $\mathbb{K}$-espace vectoriel sont maintenant faciles à vérifier. Pour tous $x,y \in E$ et $\lambda,\mu \in \mathbb{K}$: $1 \cdot \overline{x} = \overline{1 \cdot x} = \overline{x}$ et :

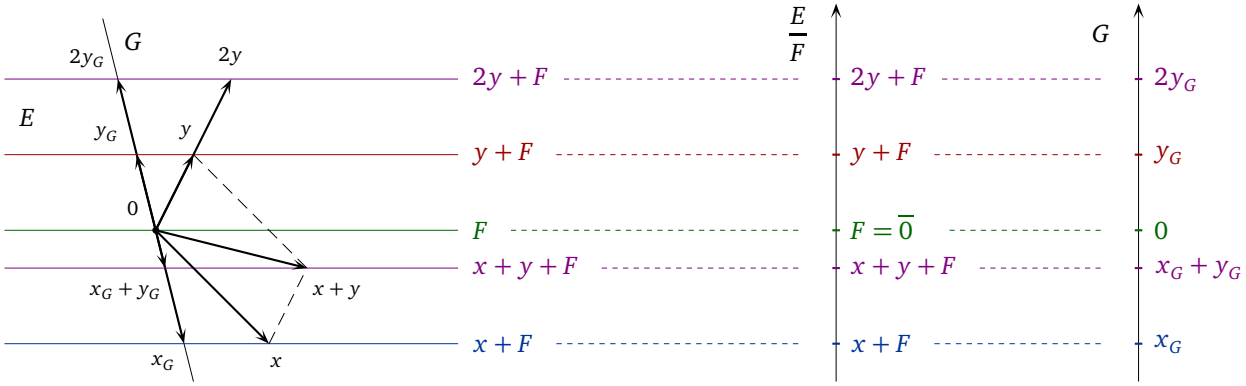
$$\lambda \cdot \left(\overline{x}+\overline{y}\right) = \lambda \cdot \overline{x+y} = \overline{\lambda \cdot (x+y)} = \overline{\lambda \cdot x + \lambda \cdot y} = \overline{\lambda \cdot x} + \overline{\lambda \cdot y} = \lambda \cdot \overline{x} + \lambda \cdot \overline{y},$$

  et on prouve de même que : $(\lambda+\mu) \cdot \overline{x} = \lambda \cdot \overline{x} + \mu \cdot \overline{x}$ et $\lambda \cdot \left(\mu \cdot \overline{x}\right) = (\lambda\mu) \cdot \overline{x}$. ■

Plaçons-nous à présent, à des fins d'illustration, dans le cas d'un $\mathbb{K}$-espace vectoriel E de dimension 2 et d'un sous-espace vectoriel F de dimension 1. Nous avons proposé précédemment une représentation de l'ENSEMBLE $\frac{E}{F}$, mais de quelle manière pouvons-nous maintenant nous le représenter comme ESPACE VECTORIEL ? On voit bien, sur la double figure qui suit, de quelle manière $\frac{E}{F}$ peut être vu comme une droite. L'addition des vecteurs et leur multiplication par un scalaire s'y calculent naturellement.



Complétons cette figure en y représentant un supplémentaire G quelconque de F dans E. Tout élément x de E est d'une unique façon la somme d'un élément x_F de F et d'un élément x_G de G, et on peut aussi dire que x_G est l'unique point d'intersection des droites $x+F$ et G. Relativement au vecteur x, oublier F revient à ne percevoir de lui que sa composante x_G dans G. De cette façon, l'espace vectoriel quotient $\frac{E}{F}$ peut être identifié au supplémentaire G de F dans E.



Le théorème qui suit formalise l'intention des figures précédentes.

Définition-théorème (Surjection canonique et supplémentarité) Soient E un $\mathbb{K}$-espace vectoriel et F un sous-espace vectoriel de E. Pour tout $x \in E$, on note $\overline{x}$ la classe de x modulo F. On suppose que F possède un supplémentaire G dans E et on note π l'application $x \longmapsto \overline{x}$ de E dans $\dfrac{E}{F}$, appelée la *surjection canonique du quotient de E par F*.

(i) L'application π est linéaire surjective de noyau F.

(ii) L'application π est un isomorphisme de G sur $\dfrac{E}{F}$.

En particulier, si E est de dimension finie : $\dim \dfrac{E}{F} = \dim E - \dim F$.

La supplémentarité de F et G dans E fait ici écho au théorème de la division euclidienne dans le contexte des anneaux $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$. Le théorème de la division euclidienne pourrait d'ailleurs être écrit ainsi : $\mathbb{Z} = n\mathbb{Z} \oplus [\![0, n-1]\!]$. Pour deux parties A et B quelconques de $\mathbb{Z}$, on sait en effet toujours définir la *somme* $A+B = \{a+b\}_{a\in A, b\in B}$. On dit qu'elle est *directe* et on la note $A \oplus B$ si tout élément de $A+B$ s'écrit d'une seule manière sous forme $a+b$ avec $a \in A$ et $b \in B$.

Alors que l'égalité : $\mathbb{Z} = n\mathbb{Z} \oplus [\![0, n-1]\!]$ nous a donné une bijection de $[\![0, n-1]\!]$ sur $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$, l'égalité : $E = F \oplus G$ nous fournit à présent une bijection π de G sur $\dfrac{E}{F}$.

Démonstration L'assertion (ii) découle de l'assertion (i) d'après la forme géométrique du théorème du rang, G étant un supplémentaire du noyau de π dans E. Pour l'assertion (i), la surjectivité de π est immédiate par définition de $\dfrac{E}{F}$. Sa linéarité est une autre manière d'énoncer la compatibilité des opérations $+$ et $\cdot$ avec la relation $\equiv\ [F]$. Enfin, pour tout $x \in E$: $x \in \operatorname{Ker}\pi \iff \overline{x} = \overline{0} \iff x \equiv 0\ [F] \iff x \in F$. ■

Nous venons d'exploiter la forme géométrique du théorème du rang, mais les espaces vectoriels quotients éclairent en retour d'une lumière nouvelle le théorème du rang en général. Donnons-nous pour le comprendre deux $\mathbb{K}$-espaces vectoriels E et F et $f \in \mathscr{L}(E,F)$. Pour tout $x \in E$, notons $\overline{x}$ la classe de x modulo $\operatorname{Ker} f$. Par définition du noyau, les éléments de $\operatorname{Ker} f$ sont totalement transparents pour f, qui les envoie tous sur 0. A fortiori, pour tous $x, y \in E$, si : $x \equiv y\ [\operatorname{Ker} f]$, alors : $x - y \in \operatorname{Ker} f$, donc : $f(x-y) = 0$, i.e. : $f(x) = f(y)$. En d'autres termes, pour tous $x, y \in E$:

$$\overline{x} = \overline{y} \quad \Longrightarrow \quad f(x) = f(y).$$

Cette *compatibilité de la relation d'équivalence* $\equiv\ [\operatorname{Ker} f]$ *avec* f nous permet de poser sans ambiguïté pour tout $x \in E$: $\overline{f}\big(\overline{x}\big) = f(x)$. On définit ainsi une application $\overline{f}$ de $\dfrac{E}{F}$ dans F. Il faut bien comprendre qu'a priori, $f(x)$ dépend de x et non de $\overline{x}$. On peut ici envoyer $\overline{x}$ sur $f(x)$ précisément parce que f donne la même valeur à tous les éléments de la classe $\overline{x}$.

Le théorème qui suit décrit les propriétés de l'application $\overline{f}$.

Théorème (Le « vrai » théorème du rang) Soient E et F deux $\mathbb{K}$-espaces vectoriels et $f \in \mathscr{L}(E,F)$. Pour tout $x \in E$, on note $\overline{x}$ la classe de x modulo $\operatorname{Ker} f$.

- La relation d'équivalence $\equiv\ [\operatorname{Ker} f]$ est compatible avec f au sens où pour tout $x, y \in E$:

$$x \equiv x'\ [\operatorname{Ker} f] \quad \Longrightarrow \quad f(x) = f(x').$$

  On peut ainsi définir une application $\overline{f}$ en posant pour tout $x \in E$: $\overline{f}\big(\overline{x}\big) = f(x)$.
- L'application $\overline{f}$ ainsi définie est alors un isomorphisme $\overline{f}$ de $\dfrac{E}{\operatorname{Ker} f}$ sur $\operatorname{Im} f$. On dit que f *induit par quotient* un isomorphisme $\overline{f}$ de $\dfrac{E}{\operatorname{Ker} f}$ sur $\operatorname{Im} f$.
- En particulier, si E est de dimension finie, $\dfrac{E}{\operatorname{Ker} f}$ est de dimension finie et : $\dim \dfrac{E}{\operatorname{Ker} f} = \dim\ \operatorname{Im} f$, ou encore :

$$\dim E = \dim \operatorname{Ker} f + \dim \operatorname{Im} f.$$

Dans ce nouveau théorème du rang, $\overline{f}$ est en quelque sorte la version parfaite de f, sa version purifiée. En quel sens ? Classiquement, s'il est faux en général que f est surjective de E sur F, il est au moins vrai qu'elle l'est de E sur son image

Im f. De façon analogue, s'il est faux en général que f est injective sur E, il est possible de la rendre injective en acceptant une autre forme de restriction, cette fois sur l'ensemble de départ. Sauf qu'il ne s'agit pas d'une vraie restriction. Rendre f injective, c'est l'obliger à discerner tous les éléments de son ensemble de départ, c'est donc tuer dans E tout ce qu'il recèle d'indiscernables vis-à-vis de f. Or pour tuer les indiscernables, il suffit de les identifier, i.e. de considérer qu'ils sont égaux, i.e. de quotienter par $\operatorname{Ker} f$.

Démonstration

- **Linéarité :** Pour tous $x, y \in E$ et $\lambda, \mu \in \mathbb{K}$:
$$\overline{f}\big(\lambda\overline{x}+\mu\overline{y}\big) = \overline{f}\big(\overline{\lambda x+\mu y}\big) = f(\lambda x+\mu y) = \lambda f(x)+\mu f(y) = \lambda\overline{f}\big(\overline{x}\big)+\mu\overline{f}\big(\overline{y}\big).$$
- **Image :** $\operatorname{Im}\overline{f} = \Big\{\overline{f}(y)\Big\}_{y\in\frac{E}{F}} = \Big\{\overline{f}\big(\overline{x}\big)\Big\}_{x\in E} = \big\{f(x)\big\}_{x\in E} = \operatorname{Im} f$.
- **Noyau :** Pour tout $x \in E$:
$$\overline{x} \in \operatorname{Ker}\overline{f} \iff \overline{f}\big(\overline{x}\big) = 0 \iff f(x) = 0 \iff x \in \operatorname{Ker} f \iff \overline{x} = \overline{0}.$$ ■

Pourquoi ce nouveau théorème du rang est-il le « vrai » théorème du rang ? La forme géométrique du théorème du rang énonce que si $\operatorname{Ker} f$ possède un supplémentaire I dans E, alors $f_{|I}$ est un isomorphisme de I sur $\operatorname{Im} f$. Or on a déjà vu plus haut que I et $\dfrac{E}{\operatorname{Ker} f}$ sont isomorphes via l'application $x \longmapsto \overline{x}$ de I dans $\dfrac{E}{\operatorname{Ker} f}$. Le nouveau théorème du rang est meilleur en ceci qu'il est **CANONIQUE**, i.e. ne dépend d'aucun choix annexe. Il n'est pas nécessaire de **CHOISIR** un supplémentaire de $\operatorname{Ker} f$ dans E pour rendre f bijective, il est suffisant pour cela d'effectuer une autre forme de restriction de l'ensemble de départ, en l'occurrence en le quotientant par $\operatorname{Ker} f$.

Nous achèverons cette partie par un exemple naturel d'espaces vectoriels quotients que vous manipulez depuis quelques temps en analyse asymptotique sans le soupçonner le moins du monde. Je noterai exceptionnellement (u_n) la suite $(u_n)_{n\in\mathbb{N}^*}$ pour alléger un peu les notations. Pour toute suite $(a_n) \in \mathbb{R}^{\mathbb{N}^*}$ qui ne s'annule pas à partir d'un certain rang, posons :
$$\mathrm{o}(a_n) = \left\{(u_n) \in \mathbb{R}^{\mathbb{N}^*} \Big/ \quad \lim_{n\to+\infty} \frac{u_n}{a_n} = 0\right\}.$$
Il est clair que $\mathrm{o}(a_n)$ est un sous-espace vectoriel du $\mathbb{R}$-espace vectoriel $\mathbb{R}^{\mathbb{N}^*}$ des suites réelles. Eh bien il se trouve que lorsqu'on raisonne à $\mathrm{o}(a_n)$ près en analyse asymptotique, on mène en fait des calculs dans l'espace vectoriel quotient $\dfrac{\mathbb{R}^{\mathbb{N}^*}}{\mathrm{o}(a_n)}$. Est-il étonnant cela dit que la relation de négligeabilité ait un rapport avec le concept d'oubli, ou plus formellement avec les structures quotients ? Par exemple, quand on écrit que : $\sqrt{n+1} \underset{n\to+\infty}{=} \sqrt{n} + \dfrac{1}{2\sqrt{n}} + \mathrm{o}\left(\dfrac{1}{\sqrt{n}}\right)$, cela revient à dire que :
$$\left(\sqrt{n+1}\right) \equiv \left(\sqrt{n} + \frac{1}{2\sqrt{n}}\right)\left[\mathrm{o}\left(\frac{1}{\sqrt{n}}\right)\right].$$
Vous avez pu trouver curieux au départ ce symbole d'égalité « $\underset{n\to+\infty}{=}$ » qui n'en est pas une. De fait, il ne s'agit là vraiment pas d'un symbole d'égalité mais d'un symbole de congruence, et il arrive, comme en arithmétique, qu'on jongle avec plusieurs symboles de congruence au sein d'un même calcul. Par exemple : $\sqrt{n+1} \underset{n\to+\infty}{=} \sqrt{n} + \dfrac{1}{2\sqrt{n}} + \mathrm{o}\left(\dfrac{1}{\sqrt{n}}\right) \underset{n\to+\infty}{=} \sqrt{n} + \mathrm{o}(1)$ signifie que : $\left(\sqrt{n+1}\right) \equiv \left(\sqrt{n} + \dfrac{1}{2\sqrt{n}}\right)\left[\mathrm{o}\left(\dfrac{1}{\sqrt{n}}\right)\right] \equiv \left(\sqrt{n}\right)\big[\mathrm{o}(1)\big]$. Le fond de l'affaire dans cet enchaînement est une simple inclusion de sous-espaces vectoriels : $\mathrm{o}\left(\dfrac{1}{\sqrt{n}}\right) \subset \mathrm{o}(1)$, mais c'est parce que l'inclusion est stricte que la lecture de l'enchaînement permise de la gauche vers la droite seulement.

Pour finir, un calcul du genre : $u_n \underset{n\to+\infty}{=} \dfrac{1}{n} + \mathrm{o}\left(\dfrac{1}{n}\right) + \dfrac{1}{n^2} + \mathrm{o}\left(\dfrac{1}{n^2}\right) \underset{n\to+\infty}{=} \dfrac{1}{n} + \mathrm{o}\left(\dfrac{1}{n}\right)$ cache les congruences suivantes :
$$(u_n) \equiv \frac{1}{n} + \frac{1}{n^2}\left[\mathrm{o}\left(\frac{1}{n}\right) + \mathrm{o}\left(\frac{1}{n^2}\right)\right] \equiv \frac{1}{n} + \frac{1}{n^2}\left[\mathrm{o}\left(\frac{1}{n}\right)\right],$$
et cette fois, c'est l'inclusion : $\mathrm{o}\left(\dfrac{1}{n^2}\right) \subset \mathrm{o}\left(\dfrac{1}{n}\right)$ qui fait marcher les choses, que l'on peut aussi traduire par une égalité suivante entre sous-espaces vectoriels : $\mathrm{o}\left(\dfrac{1}{n}\right) + \mathrm{o}\left(\dfrac{1}{n^2}\right) = \mathrm{o}\left(\dfrac{1}{n}\right)$.

3 GROUPES QUOTIENTS

On s'intéresse à présent à la structure quotient la plus fondamentale envisageable, celle de *groupe quotient*. Les espaces vectoriels étant des groupes additifs, les espaces vectoriels quotients seront un exemple particulier de groupe quotient. Nous n'avons commencé par ces quotients particuliers que parce qu'en MPSI, les espaces vectoriels sont à l'honneur, ce qui n'est pas le cas des groupes. Dans les livres de mathématiques, les groupes quotients sont au contraire toujours la première structure présentée.

En théorie des groupes, on dit généralement qu'un groupe est *abélien* pour dire qu'il est *commutatif* et nous nous conformerons désormais à cet usage. On parle aussi de l'*ordre* d'un groupe plutôt que de son cardinal.

Définition-théorème **(Congruence modulo un sous-groupe)** Soient G un groupe et H un sous-groupe de G. On appelle *relation de congruence à droite modulo H sur G* la relation définie pour tous $x, y \in H$ par :

$$x \equiv y\ [H] \qquad \Longleftrightarrow \qquad xy^{-1} \in H.$$

Cette relation $\equiv\ [H]$ est une relation d'équivalence sur G. On note G/H l'ensemble quotient associé, et généralement, pour tout $x \in H$, $\overline{x}$ la classe d'équivalence de x : $\overline{x} = Hx$, aussi appelée la *classe à droite de x modulo H*.

En tant que groupes additifs, $\mathbb{Z}$ et les espaces vectoriels que nous avons rencontrés jusqu'ici étaient tous commutatifs. Il était ainsi équivalent d'écrire « $x - y \in F$ » et « $-y + x \in F$ ». Dans le cas d'un groupe non abélien, on dispose au contraire de deux relations de congruence distinctes, l'une à gauche, l'autre à droite. Il est suffisant de n'en étudier qu'une cela dit, comme je vais le faire à présent. Pour la relation à gauche, il convient juste de remplacer ci-dessus « $xy^{-1} \in H$ » par « $x^{-1}y \in H$ ».

Démonstration Comme nous l'avons déjà observé, le fait que H soit un sous-groupe de G est exactement ce qui fait de la relation $\equiv\ [H]$ une relation d'équivalence.

- **Réflexivité :** Pour tout $x \in G$: $xx^{-1} = 1 \in H$, donc : $x \equiv x\ [H]$.
- **Symétrie :** Pour tous $x, y \in G$, si : $x \equiv y\ [H]$, alors : $xy^{-1} \in H$, mais H est stable par inversion, donc : $yx^{-1} = \left(xy^{-1}\right)^{-1} \in H$, i.e. : $y \equiv x\ [H]$.
- **Transitivité :** Pour tous $x, y, z \in G$, si : $x \equiv y\ [H]$ et $y \equiv z\ [H]$, alors : $xy^{-1} \in H$ et $yz^{-1} \in H$, mais H est stable par addition, donc : $xz^{-1} = \left(xy^{-1}\right)\left(yz^{-1}\right) \in H$, i.e. : $x \equiv z\ [H]$.
- **Classes d'équivalence :** Pour tout $x \in G$: $\overline{x} = \left\{y \in G /\quad y \equiv x\ [H]\right\} = \left\{hx\right\}_{h \in H} = Hx$. ■

Définition-théorème **(Indice d'un sous-groupe et théorème de Lagrange)** Soient G un groupe et H un sous-groupe de G. On appelle *indice de H dans G* et on note $\left|G : H\right|$ le cardinal — peut-être infini — de l'ensemble quotient G/H.

Théorème de Lagrange : Si G est fini, $|H|$ divise $|G|$ et : $\left|G : H\right| = \dfrac{|G|}{|H|}$.

Démonstration Pour tout $x \in G$, l'application $\left\{\begin{array}{ccc} H & \longrightarrow & Hx \\ h & \longmapsto & hx \end{array}\right.$ est bijective de réciproque $\left\{\begin{array}{ccc} Hx & \longrightarrow & H \\ t & \longmapsto & tx^{-1} \end{array}\right.$, donc en particulier : $|Hx| = |H|$. En d'autres termes, les classes de congruence de G modulo H sont toutes de cardinal $|H|$, et comme G n'est autre que leur réunion disjointe : $G = \left|G : H\right| \times |H|$. ■

Nous avons associé précédemment à TOUT sous-espace vectoriel F d'un espace vectoriel E un espace vectoriel quotient $\dfrac{E}{F}$, mais dans le cas des groupes, l'ensemble G/H des classes à gauche du groupe G modulo le sous-groupe H n'est encore qu'un ensemble à ce stade, et non un groupe. La relation d'équivalence $\equiv\ [H]$ est-elle compatible avec la loi de G ? Eh bien il se trouve que non, pas toujours. Nous ne pourrons pas associer un groupe quotient à TOUT sous-groupe d'un groupe. C'est dommage et cela rend la théorie des groupes bien plus compliquée que l'algèbre linéaire, mais ce qui complique une théorie est aussi parfois ce qui en fait le sel et l'exotisme. La théorie des groupes est le règne du multiple et l'algèbre linéaire le règne de l'un. Le monde des espaces vectoriels est beau et puissant — mais un peu plat, tout le monde ressemble à tout le monde et aucune tête ne dépasse.

Définition-théorème **(Sous-groupe distingué et groupe quotient)** Soient G un groupe et H un sous-groupe de G. Pour tout $x \in G$, on note $\overline{x}$ la classe à gauche de x modulo H.

(i) Pour tout $x \in G$, l'ensemble $x^{-1}Hx = \{x^{-1}hx\}_{h \in H}$ est un sous-groupe de G appelé le *conjugué de H par x*. On dit que H est *distingué dans G* si pour tout $x \in G$: $x^{-1}Hx = H$.

En particulier, si G est abélien, H est distingué dans G.

(ii) Les assertions suivantes sont équivalentes :

— H est distingué dans G.

— La relation d'équivalence $\equiv\ [H]$ est compatible avec la loi de G.

On définit dans ce cas une loi sur G/H en posant pour tous $x, y \in G$: $\overline{x}\,\overline{y} = \overline{xy}$. Le groupe quotient G/H ainsi défini est un groupe d'élément neutre $\overline{1} = H$, noté plutôt $\dfrac{G}{H}$ et appelé le *quotient de G par H*.

Dire que H est distingué dans G, c'est dire que pour tout $x \in G$: $Hx = xH$, autrement dit que H, comme partie de G, « commute » avec tout élément de G. Une telle condition ne suffit pas à rendre G abélien, mais elle explique aisément que tout sous-groupe d'un groupe abélien soit distingué. On peut dire en quelque sorte que l'ensemble G/H n'est un groupe que si G est « suffisamment abélien ».

Pour un sous-groupe H NON distingué dans G, on continuera de noter au besoin G/H l'ensemble des classes à gauche de G modulo H. La notation $\dfrac{G}{H}$ ne sera quant à elle utilisée que dans le cas où H est distingué dans G et désignera donc toujours un groupe.

Démonstration

(i) Soit $x \in G$ fixé. Montrons que $x^{-1}Hx$ est un sous-groupe de G. Or d'abord : $1 = x^{-1}1x \in x^{-1}Hx$, et ensuite pour tous $g, g' \in x^{-1}Hx$, disons : $g = x^{-1}hx$ et $g' = x^{-1}h'x$ avec $h, h' \in H$:

$$g^{-1}g' = \big(x^{-1}hx\big)^{-1}x^{-1}h'x = x^{-1}h^{-1}xx^{-1}h'x = x^{-1}\big(\underbrace{h^{-1}h'}_{\in H}\big)x \in x^{-1}Hx.$$

(ii) Supposons H distingué dans G et montrons que la relation $\equiv\ [H]$ est compatible avec la loi de G. Soient $x, y, x', y' \in G$. On suppose : $x \equiv x'\ [H]$ et $y \equiv y'\ [H]$, i.e. : $xx'^{-1} \in H$ et $yy'^{-1} \in H$. Comme H est distingué dans G, on peut aussi dire que : $x\big(yy'\big)^{-1}x^{-1} \in xHx^{-1} = H$, mais du coup : $(xy)(x'y')^{-1} = \underbrace{x\big(yy'^{-1}\big)x^{-1}}_{\in H}\underbrace{\big(xx'^{-1}\big)}_{\in H} \in H$, donc : $xy \equiv x'y'\ [H]$.

Réciproquement, faisons l'hypothèse que la relation $\equiv\ [H]$ est compatible avec la loi de G et montrons que H est distingué dans G. Soient $x \in G$ et $h \in H$. Alors : $(hx)x^{-1} \in H$, donc : $hx \equiv x\ [H]$, donc par compatibilité de $\equiv\ [H]$ avec la loi de G : $x^{-1}(hx) \equiv x^{-1}x\ [H]$, i.e. : $x^{-1}hx \equiv 1\ [H]$, ou encore : $x^{-1}hx \in H$. Conclusion : $x^{-1}Hx \subset H$. A fortiori, en remplaçant x par x^{-1} : $xHx^{-1} \subset H$, donc : $H \subset x^{-1}Hx$, et enfin comme voulu : $x^{-1}Hx = H$. ■

✎ **En pratique** ✎ Les deux dernières lignes de cette preuve sont importantes en pratique. Elles montrent qu'il est suffisant de montrer l'INCLUSION : $x^{-1}Hx \subset H$ pour tout $x \in G$ pour montrer que H est distingué dans G.

Exemple Soit G un groupe. Les sous-groupes $\{1\}$ et G de G sont distingués dans G car : $x^{-1}\{1\}x = \{x^{-1}1x\} = \{1\}$ et $x^{-1}Gx \subset G$ pour tout $x \in G$, mais aucun des quotients associés n'est très intéressant. Le quotient $\dfrac{G}{\{1\}} = \big\{\{x\}\big\}_{x \in G}$ n'est en effet jamais qu'une vulgaire copie de G dans laquelle on a remplacé tout élément x de G par le singleton $\{x\}$ et dont la loi reproduit bêtement celle de G. Le quotient $\dfrac{G}{G} = \{G\}$ est quant à lui trivial d'ordre 1.

Exemple Les sous-groupes du groupe $\mathbb{Z}$ sont exactement les ensembles $n\mathbb{Z}$, n décrivant $\mathbb{N}$, et comme $\mathbb{Z}$ est abélien, ils sont tous distingués. En d'autres termes, $\mathbb{Z}$ n'a pas d'autres quotients que les groupes $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ que nous avons déjà rencontrés. Pour $n = 0$, $\dfrac{\mathbb{Z}}{0\mathbb{Z}}$ peut être vu comme une copie de $\mathbb{Z}$ d'après l'exemple précédent.

Démonstration Les ensembles $n\mathbb{Z}$, n décrivant $\mathbb{N}$, sont clairement des sous-groupes de $\mathbb{Z}$. Réciproquement, soit G un sous-groupe de $\mathbb{Z}$. Si : $G = \{0\}$, alors : $G = 0\mathbb{Z}$. Dans le cas contraire, G étant stable par inversion,

i.e. ici par passage à l'opposé, $G\cap\mathbb{N}^*$ est une partie non vide de $\mathbb{N}$, donc possède un plus petit élément n. Il reste à montrer qu'alors : $G=n\mathbb{Z}$.

— Or G contient n et est stable par addition et passage à l'opposé, donc : $n\mathbb{Z}\subset G$.

— Inversement, soit $g\in G$. La division euclidienne de g par n s'écrit : $g=nq+r$ pour certains $q\in\mathbb{Z}$ et $r\in[\![0,n-1]\!]$, et comme G contient $n\mathbb{Z}$: $r=g-nq\in G$. Ainsi : $r\in G\cap\mathbb{N}$ et $r<n$, donc par minimalité de n : $r=0$, i.e. : $g=nq$. Conclusion : $G\subset n\mathbb{Z}$.

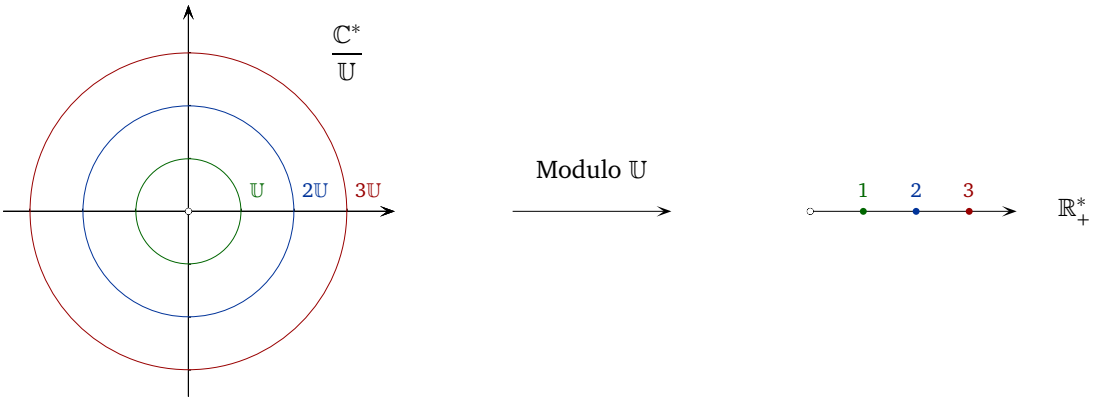
Exemple $\mathbb{R}_+^*$ est un sous-groupe distingué du groupe abélien $\mathbb{R}^*$ et :

$$\frac{\mathbb{R}^*}{\mathbb{R}_+^*}=\left\{x\mathbb{R}_+^*\right\}_{x\in\mathbb{R}^*}=\left\{\mathbb{R}_+^*,\mathbb{R}_-^*\right\}=\left\{\overline{1},\overline{-1}\right\}.$$

$\times$	$\overline{1}$	$\overline{1}$
$\overline{1}$	$\overline{1}$	$\overline{-1}$
$\overline{-1}$	$\overline{-1}$	$\overline{1}$

La table du groupe $\dfrac{\mathbb{R}^*}{\mathbb{R}_+^*}$ n'est rien d'autre que la traditionnelle *règle des signes*. Quoi d'étonnant ? Raisonner modulo $\mathbb{R}_+^*$, c'est oublier des réels non nuls tout ce qu'il y a de positif en eux — leur valeur absolue — pour n'en retenir que le signe.

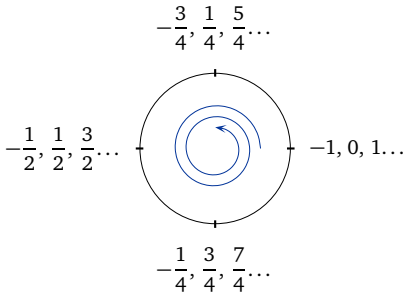
Exemple $\mathbb{U}$ est un sous-groupe distingué du groupe abélien $\mathbb{C}^*$ et : $\dfrac{\mathbb{C}^*}{\mathbb{U}}=\left\{z\mathbb{U}\right\}_{z\in\mathbb{C}^*}=\left\{r\mathbb{U}\right\}_{r>0}$, un peu comme si $\dfrac{\mathbb{C}^*}{\mathbb{U}}$ pouvait être assimilé à $\mathbb{R}_+^*$. Nous donnerons bientôt un sens précis à cette idée. En attendant, $r\mathbb{U}$ est géométriquement le cercle de centre 0 et de rayon r pour tout $r>0$. En résumé, tout nombre complexe non nul peut être ramené modulo $\mathbb{U}$ à son seul module.



Exemple $\mathbb{Z}$ est un sous-groupe distingué du groupe abélien $\mathbb{R}$ et :

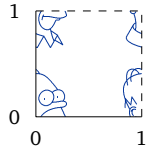
$$\frac{\mathbb{R}}{\mathbb{Z}}=\left\{x+\mathbb{Z}\right\}_{x\in\mathbb{R}}=\left\{x+\mathbb{Z}\right\}_{x\in[0,1[},$$

un peu comme si $\dfrac{\mathbb{R}}{\mathbb{Z}}$ pouvait être assimilé à $[0,1[$. L'ensemble $[0,1[$ gagne cela dit à être perçu ici davantage comme un cercle que comme une intervalle. La congruence : $1\equiv 0\,[1]$ lui permet de se refermer sur lui-même en quelque sorte. Nous donnerons plus tard à cette idée un contenu rigoureux.



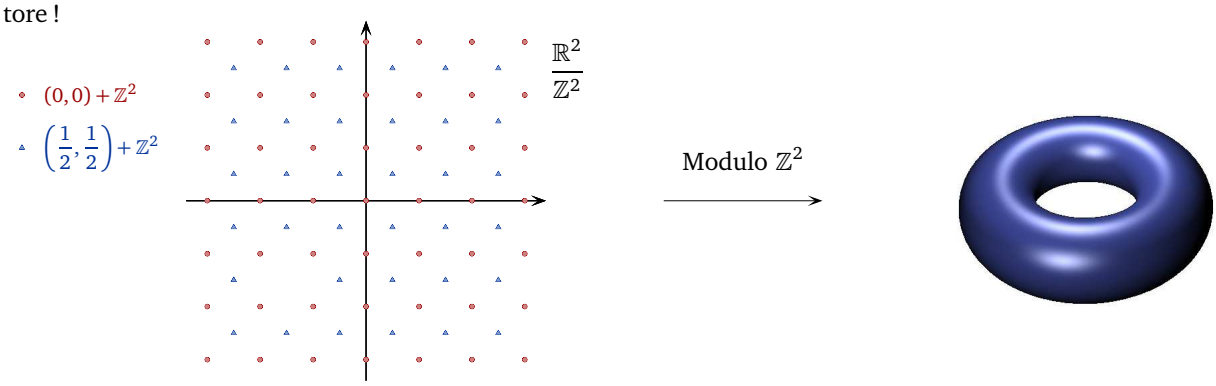
Exemple $\mathbb{Z}^2$ est un sous-groupe distingué du groupe abélien $\mathbb{R}^2$ et :

$$\frac{\mathbb{R}^2}{\mathbb{Z}^2}=\left\{(x,y)+\mathbb{Z}^2\right\}_{x,y\in\mathbb{R}}=\left\{(x,y)+\mathbb{Z}^2\right\}_{x,y\in[0,1[},$$



Homer Simpson modulo $\mathbb{Z}^2$

un peu comme si $\dfrac{\mathbb{R}^2}{\mathbb{Z}^2}$ pouvait être assimilé à $[0,1[\times[0,1[$. L'ensemble $[0,1[\times[0,1[$ gagne cela dit à être perçu ici davantage comme un tore que comme un carré, car qu'est-ce qu'un carré dont on rabat les côtés opposés les uns sur les autres ? C'est un tore !



Théorème **(Sous-groupes d'indice 2)** Soient G un groupe et H un sous-groupe de G.

Si : $\big|G:H\big| = 2$, alors H est distingué dans G.

Dans ce cas : $\dfrac{G}{H} = \big\{H, G\setminus H\big\}$ et la loi de $\dfrac{G}{H}$ est décrite par la table suivante,

qui coïncide avec la table du groupe $\dfrac{\mathbb{Z}}{2\mathbb{Z}}$ au nom près des objets :

$\times$	H	$G\setminus H$
H	H	$G\setminus H$
$G\setminus H$	$G\setminus H$	H

Démonstration Soient $x\in G$ et $h\in H$. Si : $x\in H$, évidemment : $x^{-1}hx\in H$.

Supposons désormais que : $x = x1^{-1}\notin H$. Dans ce cas, x et 1 ne sont pas dans la même classe à droite modulo H, autrement dit : $Hx\neq H$. Comme : $\big|G:H\big| = 2$, il en découle que : $G/H = \big\{H, Hx\big\}$ et $Hx = G\setminus H$. Or : $x^{-1}hx\notin Hx$ — sans quoi x serait élément de H — donc : $x^{-1}hx\in H$.

Dans tous les cas : $x^{-1}hx\in H$, donc H est distingué dans G. ■

Nos prochains exemples seront plus faciles à présenter après la définition suivante.

Définition-théorème **(Sous-groupe engendré par une partie)** Soient G un groupe et X une partie de G. L'ensemble de tous les produits qu'on peut former à partir des éléments de X ou de leurs inverses est un sous-groupe de G contenant X noté $\langle X\rangle$ et appelé le *sous-groupe de G engendré par X*.

Tout sous-groupe de G qui contient X contient aussi $\langle X\rangle$.

Si X est un singleton $\big\{x\big\}$, le groupe $\langle X\rangle$ est dit *monogène* et on le note plutôt $\langle x\rangle$. Concrètement : $\langle x\rangle = \big\{x^k\big\}_{k\in\mathbb{Z}}$.

Démonstration Montrons que $\langle X\rangle$ est un sous-groupe de G contenant X. Il est à vrai dire évident que $\langle X\rangle$ contient X, mais aussi qu'il est stable par produit et inversion. Enfin, par convention du produit vide : $1\in\langle X\rangle$.

Tout sous-groupe de G qui contient X contient d'abord tous les inverses des éléments de X par stabilité par inversion, mais du coup aussi $\langle X\rangle$ tout entier par stabilité par produit. ■

Exemple

- Le groupe $n\mathbb{Z}$ est monogène pour tout $n\in\mathbb{N}$ car : $n\mathbb{Z} = \langle n\rangle$.
- Le groupe $\mathbb{U}_n$ est monogène pour tout $n\in\mathbb{N}^*$ car : $\mathbb{U}_n = \big\langle \mathrm{e}^{\frac{2\mathrm{i}\pi}{n}}\big\rangle$.

Définition-théorème **(Ordre d'un élément et théorème de Lagrange)** Soient G un groupe et $x\in G$.

- Si $\langle x\rangle$ est infini, on dit que x est *d'ordre infini*.
- Si $\langle x\rangle$ est fini, on dit que x est *d'ordre fini*. Il existe alors un entier naturel non nul noté $|x|$ et appelé l'*ordre de x* pour lequel : $\Big\{k\in\mathbb{Z}/\quad x^k = 1\Big\} = |x|\mathbb{Z}$. Ainsi, pour tout $k\in\mathbb{Z}$: $x^k = 1$ si et seulement si $|x|$ divise k.

  Dans ce cas : $\langle x\rangle = \big\{x^k\big\}_{0\leqslant k\leqslant |x|-1}$ et $\big|\langle x\rangle\big| = |x|$.

  Théorème de Lagrange : $|x|$ divise $|G|$, autrement dit : $x^{|G|} = 1$.

En particulier, 1 est le seul élément de G d'ordre 1.

Démonstration Supposons x d'ordre fini.

- L'ensemble $E = \Big\{k\in\mathbb{Z}/\quad x^k = 1\Big\}$ est un sous-groupe de $\mathbb{Z}$ car : $x^0 = 1$ et pour tous $i,j\in\mathbb{Z}$, si : $x^i = x^j = 1$, alors : $x^{j-i} = x^j\big(x^i\big)^{-1} = 1$. Ainsi, pour un certain $n\in\mathbb{N}$: $E = n\mathbb{Z}$.

  Se peut-il que n soit nul ? Comme $\langle x\rangle$ est fini, l'application $k\longmapsto x^k$ de $\mathbb{Z}$ dans $\langle x\rangle$ ne peut pas être injective, donc : $x^i = x^j$ pour certains $i,j\in\mathbb{Z}$ avec : $i<j$. Aussitôt : $x^{j-i} = 1$ avec : $j-i\in\mathbb{N}^*$, donc $E = n\mathbb{Z}$ contient un élément autre que 0, ce qui montre bien que : $n\neq 0$.
- Montrons que l'application $k\overset{\varphi}{\longmapsto} x^k$ est bijective de $[\![0,n-1]\!]$ sur $\langle x\rangle$. Cela montrera en particulier que : $\big|\langle x\rangle\big| = n$, donc que $|x|$ divise $|G|$ d'après le théorème de Lagrange. On pourra alors affirmer en particulier que : $x^{|G|} = \big(x^n\big)^{|G:\langle x\rangle|} = 1^{|G:\langle x\rangle|} = 1$.

L'application φ est surjective car pour tout $k \in \mathbb{Z}$, en notant : $k = nq+r$ la division euclidienne de k par $|x|$ avec $q \in \mathbb{Z}$ et $r \in [\![0, n-1]\!]$: $x^k = \left(x^n\right)^q x^r = 1^q x^r = x^r = \varphi(r)$. L'application φ est ensuite injective car pour tous $i, j \in [\![0, n-1]\!]$, si : $x^i = x^j$, alors : $x^{j-i} = 1$, donc : $j - i \in E \cap [\![0, n-1]\!] = \{0\}$, i.e. : $i = j$. ■

Le *théorème d'Euler* suivant est à la fois une généralisation du petit théorème de Fermat et un simple cas particulier du théorème de Lagrange.

Définition-théorème **(Indicatrice d'Euler et théorème d'Euler)** On appelle *indicatrice d'Euler* la fonction φ définie pour tout $n \in \mathbb{N}^*$ par : $\varphi(n) = \left|\mathrm{U}\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)\right|$.

(i) **Théorème d'Euler :** Pour tout $n \in \mathbb{N}^*$ et $x \in \mathbb{Z}$, si : $x \wedge n = 1$, alors : $x^{\varphi(n)} \equiv 1\ [n]$.

(ii) Pour tous $p \in \mathbb{P}$ et $r \in \mathbb{N}^*$: $\varphi\left(p^r\right) = p^{r-1}(p-1)$.

Pour tout $p \in \mathbb{P}$: $\varphi(p) = p - 1$ car $\frac{\mathbb{Z}}{p\mathbb{Z}}$ est un corps, donc pour tout $x \in \mathbb{Z}$ non divisible par p : $x^p \equiv 1\ [p]$ conformément au petit théorème de Fermat. Nous calculerons plus tard les valeurs de la fonction φ de façon générale.

Démonstration

(i) Il est bien connu que l'ensemble $\mathrm{U}\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)$ des inversibles de l'anneau $\frac{\mathbb{Z}}{n\mathbb{Z}}$ est un groupe multiplicatif. En outre : $\mathrm{U}\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right) = \left\{\overline{a}\right\}_{a \in \mathbb{Z},\ a \wedge n = 1}$, donc d'après le théorème de Lagrange, pour tout $a \in \mathbb{Z}$, si : $a \wedge n = 1$, alors : $\overline{a}^{\varphi(n)} = 1$, i.e. : $a^{\varphi(n)} \equiv 1\ [n]$.

(ii) Par définition : $\varphi\left(p^r\right) = \left|\mathrm{U}\left(\frac{\mathbb{Z}}{p^r\mathbb{Z}}\right)\right| = \left|\left\{x \in [\![0, p^r - 1]\!] / \quad x \wedge p^r = 1\right\}\right| = \left|\left\{x \in [\![0, p^r - 1]\!] / \quad p \not| x\right\}\right|$.
Or $[\![0, p^r - 1]\!]$ contient p^r éléments en tout dont p^{r-1} qui sont divisibles par p, donc par différence : $\varphi\left(p^r\right) = p^r - p^{r-1} = p^{r-1}(p-1)$. ■

On étudie à présent en détail les sous-groupes distingués du groupe symétrique S_3 et du *groupe des quaternions* Q_8.

Exemple Le groupe symétrique S_3 a pour éléments : $\overbrace{\mathrm{Id},}^{\text{d'ordre 1}}$ $\overbrace{(1\ 2),\quad (1\ 3),\quad (2\ 3),}^{\text{d'ordre 2}}$ $\overbrace{(1\ 2\ 3),\quad (1\ 3\ 2).}^{\text{d'ordre 3}}$

- La liste de ses sous-groupes est facile à dresser. Ils sont d'ordre 1, 2, 3 ou 6 d'après le théorème de Lagrange, et parmi eux, les sous-groupes monogènes sont : $\langle \mathrm{Id} \rangle = \{\mathrm{Id}\}$, $\langle (1\ 2) \rangle = \{\mathrm{Id}, (1\ 2)\}$, $\langle (1\ 3) \rangle = \{\mathrm{Id}, (1\ 3)\}$, $\langle (2\ 3) \rangle = \{\mathrm{Id}, (2\ 3)\}$ et $A_3 = \langle (1\ 2\ 3) \rangle = \{\mathrm{Id}, (1\ 2\ 3), (1\ 3\ 2)\}$. Comme on peut le vérifier ensuite, le produit de deux transpositions distinctes de S_3 est toujours un 3-cycle et le produit d'une transposition et d'un 3-cycle est toujours une transposition, donc le seul sous-groupe d'ordre 1, 2, 3 ou 6 que nous n'avons pas encore évoqué est le groupe S_3 lui-même. Par exemple : $(1\ 2)\,(1\ 3) = (1\ 3\ 2)$ et $(1\ 2\ 3)\,(1\ 2) = (1\ 3)$.
- En plus de $\langle \mathrm{Id} \rangle$ et S_3, le sous-groupe A_3 est distingué dans S_3 car il y est d'indice 2 et le quotient $\frac{S_3}{A_3}$ est une copie de $\frac{\mathbb{Z}}{2\mathbb{Z}}$. Les sous-groupes d'ordre 2 de S_3 ne sont en revanche pas distingués dans S_3 et ne donnent donc lieu à aucun groupe quotient. Par exemple : $(1\ 3)^{-1}\langle (1\ 2) \rangle (1\ 3) = \langle (1\ 3)^{-1}(1\ 2)\ (1\ 2) \rangle = \langle (2\ 3) \rangle \neq \langle (1\ 2) \rangle$.

Exemple Dans le groupe $\mathrm{GL}_2(\mathbb{C})$, on pose : $1 = I_2$, $\mathrm{i} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, $\mathrm{j} = \begin{pmatrix} 0 & \mathrm{i} \\ \mathrm{i} & 0 \end{pmatrix}$ et $\mathrm{k} = \begin{pmatrix} -\mathrm{i} & 0 \\ 0 & \mathrm{i} \end{pmatrix}$. Ce choix de notations peut paraître étrange, mais il est à peu près universel.

- Les matrices ainsi définies satisfont entre elles quelques relations simples. Pour commencer : $\mathrm{i}^2 = \mathrm{j}^2 = \mathrm{k}^2 = -1$, donc i, j et k sont d'ordre 4. Évidemment, -1 est d'ordre 2. Par ailleurs :

$$\mathrm{ij} = \mathrm{k} \quad \text{et} \quad \mathrm{ji} = -\mathrm{k}, \qquad \mathrm{jk} = \mathrm{i} \quad \text{et} \quad \mathrm{kj} = -\mathrm{i}, \qquad \mathrm{ki} = \mathrm{j} \quad \text{et} \quad \mathrm{ik} = -\mathrm{j}.$$

Ces relations montrent que : $\langle \mathrm{i}, \mathrm{j} \rangle = \{\pm 1, \pm\mathrm{i}, \pm\mathrm{j}, \pm\mathrm{k}\}$. Nous noterons Q_8 ce sous-groupe de $\mathrm{GL}_2(\mathbb{C})$ et nous l'appellerons le *groupe des quaternions*. Il est préférable à vrai dire d'oublier qu'on a construit Q_8 comme un groupe de matrices. Voyez plutôt Q_8 comme une boîte noire de 8 objets soumis seulement à quelques relations simples.

- La liste des sous-groupes de Q_8 est facile à dresser. Ses sous-groupes monogènes sont :

  $$\langle 1\rangle = \{1\}, \qquad \langle -1\rangle = \{\pm 1\}, \qquad \langle \mathrm{i}\rangle = \langle -\mathrm{i}\rangle = \{\pm 1, \pm \mathrm{i}\}, \qquad \langle \mathrm{j}\rangle = \langle -\mathrm{j}\rangle = \{\pm 1, \pm \mathrm{j}\}, \qquad \langle \mathrm{k}\rangle = \langle -\mathrm{k}\rangle = \{\pm 1, \pm \mathrm{k}\}$$

  et le seul sous-groupe non monogène de Q_8 est Q_8 lui-même. D'indice 2 dans Q_8, $\langle \mathrm{i}\rangle$, $\langle \mathrm{j}\rangle$ et $\langle \mathrm{k}\rangle$ sont distingués dans Q_8. C'est aussi le cas de $\langle -1\rangle$ car -1 commute à tout élément de Q_8. Les sous-groupes de Q_8 sont ainsi tous distingués dans Q_8.
- Les quotients $\dfrac{Q_8}{\langle \mathrm{i}\rangle}$, $\dfrac{Q_8}{\langle \mathrm{j}\rangle}$ et $\dfrac{Q_8}{\langle \mathrm{k}\rangle}$ sont de simples copies de $\dfrac{\mathbb{Z}}{2\mathbb{Z}}$, mais qu'en est-il du quotient $\dfrac{Q_8}{\langle -1\rangle}$ d'ordre 4 ? En notant d'une barre les quotients par $\langle -1\rangle$: $\dfrac{Q_8}{\langle -1\rangle} = \Big\{ \{\pm 1\}, \{\pm \mathrm{i}\}, \{\pm \mathrm{j}\}, \{\pm \mathrm{k}\} \Big\} = \big\{\overline{1}, \overline{\mathrm{i}}, \overline{\mathrm{j}}, \overline{\mathrm{k}}\big\}$, et les relations qu'on a listées ci-dessus sur i, j et k deviennent : $\overline{\mathrm{i}}^2 = \overline{\mathrm{j}}^2 = \overline{\mathrm{k}}^2 = \overline{1}$, $\overline{\mathrm{i}}\,\overline{\mathrm{j}} = \overline{\mathrm{k}}$, $\overline{\mathrm{j}}\,\overline{\mathrm{k}} = \overline{\mathrm{i}}$ et $\overline{\mathrm{k}}\,\overline{\mathrm{i}} = \overline{\mathrm{j}}$. Or ces relations sont les mêmes que celles qui définissent le groupe produit $\dfrac{\mathbb{Z}}{2\mathbb{Z}} \times \dfrac{\mathbb{Z}}{2\mathbb{Z}}$:

  $$(1,0)^2 = (0,1)^2 = (1,1)^2 = (0,0), \qquad (1,0)+(0,1) = (1,1), \qquad (0,1)+(1,1) = (1,0) \qquad \text{et} \qquad (1,1)+(1,0) = (0,1).$$

  Les lois des groupes $\dfrac{Q_8}{\langle -1\rangle}$ et $\dfrac{\mathbb{Z}}{2\mathbb{Z}} \times \dfrac{\mathbb{Z}}{2\mathbb{Z}}$ sont ainsi décrites par les mêmes tables au nom près des objets.

$\times$	$\overline{1}$	$\overline{\mathrm{i}}$	$\overline{\mathrm{j}}$	$\overline{\mathrm{k}}$
$\overline{1}$	$\overline{1}$	$\overline{\mathrm{i}}$	$\overline{\mathrm{j}}$	$\overline{\mathrm{k}}$
$\overline{\mathrm{i}}$	$\overline{\mathrm{i}}$	$\overline{1}$	$\overline{\mathrm{k}}$	$\overline{\mathrm{j}}$
$\overline{\mathrm{j}}$	$\overline{\mathrm{j}}$	$\overline{\mathrm{k}}$	$\overline{1}$	$\overline{\mathrm{i}}$
$\overline{\mathrm{k}}$	$\overline{\mathrm{k}}$	$\overline{\mathrm{j}}$	$\overline{\mathrm{i}}$	$\overline{1}$

$+$	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$
$(0,0)$	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$
$(1,0)$	$(1,0)$	$(0,0)$	$(1,1)$	$(0,1)$
$(0,1)$	$(0,1)$	$(1,1)$	$(0,0)$	$(1,0)$
$(1,1)$	$(1,1)$	$(0,1)$	$(1,0)$	$(0,0)$

- Une remarque pour finir. Les sous-groupes de Q_8 sont tous distingués alors que Q_8 n'est pas abélien, mais une telle situation est vraiment très rare et on peut montrer que les groupes concernés sont tous en un sens très proches de Q_8.

4 Morphismes de groupes

Les *morphismes de groupes* sont aux groupes ce que les applications linéaires sont aux espaces vectoriels. Les applications linéaires pourraient d'ailleurs être appelées des *morphismes d'espaces vectoriels*.

Définition **(Morphisme de groupes)** Soient G et Γ deux groupes.

- On appelle *morphisme* (*de groupes*) *de G dans Γ* toute application $f : G \longrightarrow \Gamma$ pour laquelle pour tous $x, y \in G$:
$$f(xy) = f(x)f(y).$$
- On appelle *isomorphisme* (*de groupes*) *de G sur Γ* tout morphisme de groupes bijectif de G sur Γ, et on dit que Γ est *isomorphe à G* (*comme groupe*) s'il existe un isomorphisme de G sur Γ.

On définit comme en algèbre linéaire les notions d'*endomorphisme* et d'*automorphisme*. Avec les notations qui précèdent, il n'est pas dur de vérifier que : $\boxed{f(1) = 1}$ après simplification par $f(1)$ dans la relation : $f(1) = f\big(1^2\big) = f(1)^2$, et que pour tout $x \in G$: $\boxed{f\big(x^{-1}\big) = f(x)^{-1}}$ car : $f(x)f\big(x^{-1}\big) = f\big(xx^{-1}\big) = f(1) = 1$.

Exemple Toute phrase du genre : « Le machin des trucs est égal au truc des machins » est le signe sûr qu'un morphisme de groupes n'est pas loin.

- Toute application linéaire entre deux espaces vectoriels est en particulier un morphisme de groupes additifs.
- La fonction $z \longmapsto |z|$ est un endomorphisme de $\mathbb{C}^*$ car le module d'un produit est égal aux produit des modules.

- La fonction logarithme est un isomorphisme de $\mathbb{R}_+^*$ dans $\mathbb{R}$ car le logarithme d'un produit est égal à la somme des logarithmes.
- La fonction $z \longmapsto e^z$ est un morphisme de $\mathbb{C}$ dans $\mathbb{C}^*$ car l'exponentielle d'une somme est égale au produit des exponentielles.
- La fonction $\theta \longmapsto e^{i\theta}$ est un morphisme de $\mathbb{R}$ dans $\mathbb{U}$.
- La fonction $x \longmapsto x^\alpha$ est un automorphisme de $\mathbb{R}_+^*$ pour tout $\alpha \in \mathbb{R}^*$.
- La fonction $k \longmapsto z^k$ est un morphisme de $\mathbb{Z}$ dans $\mathbb{C}^*$ pour tout $z \in \mathbb{C}^*$.
- La signature ε est un morphisme du groupe symétrique S_n dans le groupe $\{\pm 1\}$ pour tout $n \in \mathbb{N}^*$.
- Le déterminant est un morphisme de $GL_n(\mathbb{K})$ dans $\mathbb{K}^*$ pour tout corps $\mathbb{K}$ et pour tout $n \in \mathbb{N}^*$.

Exemple Soient G un groupe et H un sous-groupe de G. On suppose que : $\big|G : H\big| = 2$. Nous avons vu que H est alors distingué dans G et que la table de $\dfrac{G}{H}$ est une copie de celle de $\dfrac{\mathbb{Z}}{2\mathbb{Z}}$. Plus rigoureusement, il vaut mieux dire maintenant que l'application qui envoie 0 sur H et 1 sur $G \setminus H$ est un isomorphisme de $\dfrac{\mathbb{Z}}{2\mathbb{Z}}$ sur $\dfrac{G}{H}$.

Exemple Nous avons montré sans le dire à la fin du paragraphe précédent que les groupes $\dfrac{Q_8}{\langle -1\rangle}$ et $\dfrac{\mathbb{Z}}{2\mathbb{Z}} \times \dfrac{\mathbb{Z}}{2\mathbb{Z}}$ sont isomorphes.

Exemple Soit $p \in \mathbb{P}$. La valuation p-adique v_p est définie sur $\mathbb{Z} \setminus \{0\}$ en MPSI, mais rien n'empêche qu'on la définisse sur $\mathbb{Q}^*$. On a bien envie de poser pour tout $r = \dfrac{a}{b} \in \mathbb{Q}^*$ avec $a \in \mathbb{Z}, b \in \mathbb{Z} \setminus \{0\}$: $v_p(r) = v_p(a) - v_p(b)$, mais $\dfrac{a}{b}$ n'est QU'UNE écriture fractionnaire de r parmi une infinité. La quantité $v_p(a) - v_p(b)$ dépend-elle vraiment de a et b ou bien ne dépend-elle que de r indépendamment de l'écriture fractionnaire choisie ? En d'autres termes, est-il vrai que pour tous $a, b, a'b' \in \mathbb{Z} \setminus \{0\}$: $\dfrac{a}{b} = \dfrac{a'}{b'} \implies v_p(a) - v_p(b) = v_p(a') - v_p(b')$? Or si : $\dfrac{a}{b} = \dfrac{a'}{b'}$, alors dans $\mathbb{Z}$: $ab' = ba'$, donc : $v_p(a) + v_p(b') = v_p(b) + v_p(a')$, et donc en effet : $v_p(a) - v_p(b) = v_p(a') - v_p(b')$.

Nous venons ainsi de définir une fonction v_p de $\mathbb{Q}^*$ dans $\mathbb{Z}$, mais est-il bien raisonnable de la nommer v_p ? La nouvelle fonction v_p coïncide-t-elle avec l'ancienne sur $\mathbb{Z} \setminus \{0\}$? Il se trouve que oui car : $v_p(1) = 0$, donc pour tout $n \in \mathbb{Z} \setminus \{0\}$: $v_p(n) - v_p(1) = v_p(n)$. La nouvelle fonction v_p prolonge ainsi notre valuation p-adique classique à $\mathbb{Q}^*$ tout entier.

Pour finir, v_p est un morphisme de groupes de $\mathbb{Q}^*$ dans $\mathbb{Z}$ car pour tous $r = \dfrac{a}{b}, r' = \dfrac{a'}{b'} \in \mathbb{Q}^*$ avec $a, b, a', b' \in \mathbb{Z} \setminus \{0\}$:

$$v_p(rr') = v_p\left(\frac{aa'}{bb'}\right) = v_p(aa') - v_p(bb') = v_p(a) + v_p(a') - v_p(b) - v_p(b') = v_p\left(\frac{a}{b}\right) + v_p\left(\frac{a'}{b'}\right) = v_p(r) + v_p(r').$$

Pour en revenir à des généralités, il n'est pas difficile de montrer que la composée de deux morphismes de groupes est encore un morphisme de groupes et que la réciproque d'un isomorphisme de groupes est encore un isomorphisme de groupes. Il en découle que la relation « être isomorphe à » entre groupes est une relation d'équivalence.

Définition-théorème (Noyau et image d'un morphisme de groupes) Soient G et Γ deux groupes et f un morphisme de groupes de G dans Γ.

(i) L'image $\operatorname{Im} f$ de f est un sous-groupe de Γ.

(ii) On appelle *noyau de* f l'ensemble : $\operatorname{Ker} f = \big\{x \in G / \quad f(x) = 1\big\}$, qui est un sous-groupe distingué de G.
En outre, f est injectif sur G si et seulement si : $\operatorname{Ker} f = \{1\}$.

La notion de noyau est une notion propre à la théorie des groupes et n'est exploitée en algèbre linéaire que parce que les espaces vectoriels sont des groupes additifs.

Démonstration

(i) Pour commencer : $1 = f(1) \in \operatorname{Im} f$. Ensuite, pour tous $y, y' \in \operatorname{Im} f$, disons : $y = f(x)$ et $y' = f(x')$ avec $x, x' \in G$: $y^{-1}y' = f(x)^{-1}f(x') = f\big(x^{-1}x'\big) \in \operatorname{Im} f$.

(ii) Montrons que $\operatorname{Ker} f$ est un sous-groupe de G. Pour commencer : $1 \in \operatorname{Ker} f$ car : $f(1) = 1$. Ensuite, pour tous $x, x' \in \operatorname{Ker} f$: $x^{-1}x' \in \operatorname{Ker} f$ car : $f\left(x^{-1}x'\right) = f(x)^{-1}f(x') = 1$.

Montrons que $\operatorname{Ker} f$ est distingué dans G, i.e. que pour tout $x \in G$: $x^{-1}(\operatorname{Ker} f)x \subset \operatorname{Ker} f$. Or pour tout $x \in G$ et $k \in \operatorname{Ker} f$: $x^{-1}kx \in \operatorname{Ker} f$ car : $f\left(x^{-1}kx\right) = f(x)^{-1}f(k)f(x) = f(x)^{-1}f(x) = 1$.

À présent, si f est injectif, alors pour tout $x \in \operatorname{Ker} f$: $f(x) = 1 = f(1)$, donc : $x = 1$ par injectivité. Comme on a toujours : $f(1) = 1$, il en découle que : $\operatorname{Ker} f = \{1\}$.

Réciproquement, si : $\operatorname{Ker} f = \{1\}$, montrons que f est injectif. Soient $x, x' \in G$. On suppose que : $f(x) = f(x')$. Aussitôt : $f\left(x^{-1}x'\right) = f(x)^{-1}f(x') = 1$, donc : $x^{-1}x' \in \operatorname{Ker} f = \{1\}$, donc : $x = x'$. ■

Exemple

- Le morphisme $z \longmapsto |z|$ de $\mathbb{C}^*$ dans $\mathbb{C}^*$ a pour image $\mathbb{R}_+^*$ et pour noyau $\mathbb{U}$.
- Le morphisme $z \longmapsto \mathrm{e}^z$ de $\mathbb{C}$ dans $\mathbb{C}^*$ a pour image $\mathbb{C}^*$ et pour noyau $2\mathrm{i}\pi\mathbb{Z}$.
- Le morphisme $\theta \longmapsto \mathrm{e}^{\mathrm{i}\theta}$ de $\mathbb{R}$ dans $\mathbb{U}$ est surjectif de noyau $2\pi\mathbb{Z}$.
- Soit $n \in \mathbb{N}^*$. On pose : $z = \mathrm{e}^{\frac{2\mathrm{i}\pi}{n}}$. Le morphisme $k \longmapsto z^k$ de $\mathbb{Z}$ dans $\mathbb{C}^*$ a pour image $\mathbb{U}_n$ et pour noyau $n\mathbb{Z}$.
- Pour tout $n \in \mathbb{N}^*$, la signature ε est un morphisme de groupes surjectif du groupe symétrique S_n sur $\{\pm 1\}$, car : $\varepsilon(\mathrm{Id}) = 1$ et $\varepsilon\big((1\ 2)\big) = -1$. Son noyau, l'ensemble des permutations paires de $[\![1, n]\!]$, est noté A_n et appelé le *groupe alterné de degré n*. Nous avions déjà observé plus haut que le sous-groupe A_3 est distingué dans A_3.
- Pour tout corps $\mathbb{K}$ et pour tout $n \in \mathbb{N}^*$, le déterminant est un morphisme de groupes surjectif de $\mathrm{GL}_n(\mathbb{K})$ sur $\mathbb{K}^*$, car pour tout $\lambda \in \mathbb{K}^*$: $\begin{pmatrix} I_{n-1} & 0 \\ 0 & \lambda \end{pmatrix} = \lambda$. Son noyau, noté $\mathrm{SL}_n(\mathbb{K})$, est appelé le *groupe spécial linéaire de degré n sur* $\mathbb{K}$.

Le théorème qui suit, en dépit de sa trivialité, énonce l'une des idées de base les plus importantes de l'algèbre. On l'appelle souvent le *premier théorème d'isomorphisme*, mais je ne présenterai pas les deux autres théorèmes d'isomorphisme qu'on lui accole d'ordinaire.

Théorème (Théorème d'isomorphisme) Soient G et Γ deux groupes et f un morphisme de groupes de G dans Γ. Pour tout $x \in G$, on note $\overline{x}$ la classe de x modulo $\operatorname{Ker} f$.

- La relation $\equiv\ [\operatorname{Ker} f]$ est compatible avec f au sens où pour tous $x, x' \in E$:
$$x \equiv x'\ [\operatorname{Ker} f] \quad \Longrightarrow \quad f(x) = f(y).$$
On peut ainsi définir une application $\overline{f}$ en posant pour tout $x \in E$: $\overline{f}\left(\overline{x}\right) = f(x)$.
- L'application $\overline{f}$ ainsi définie est alors un isomorphisme $\overline{f}$ de $\dfrac{G}{\operatorname{Ker} f}$ sur $\operatorname{Im} f$. On dit que f *induit par quotient* un isomorphisme $\overline{f}$ de $\dfrac{G}{\operatorname{Ker} f}$ sur $\operatorname{Im} f$.
- En particulier, si G est fini, $\dfrac{G}{\operatorname{Ker} f}$ l'est aussi et : $\left|G : \operatorname{Ker} f\right| = \left|\operatorname{Im} f\right|$.

Ce théorème fondamental est très clairement l'analogue du théorème du rang en théorie des groupes. Il se démontre de la même manière que l'énoncé que nous en avons donné plus haut dans le cadre des espaces vectoriels quotients.

Exemple Pour tout $n \in \mathbb{N}^*$, le morphisme de groupes $k \longmapsto \mathrm{e}^{\frac{2\mathrm{i}k\pi}{n}}$ de $\mathbb{Z}$ dans $\mathbb{C}^*$ induit par quotient un isomorphisme de $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ sur $\mathbb{U}_n$. Cet isomorphisme ne devrait pas vous étonner, car après tout, nous nous représentons tous $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ et $\mathbb{U}_n$ de la même manière, à savoir comme une sorte d'horloge à n graduations.

Exemple L'endomorphisme de groupe $z \longmapsto |z|$ de $\mathbb{C}^*$ induit par quotient un isomorphisme de $\dfrac{\mathbb{C}^*}{\mathbb{U}}$ sur $\mathbb{R}_+^*$. Nous avions déjà observé que $\dfrac{\mathbb{C}^*}{\mathbb{U}}$ pouvait être assimilé à $\mathbb{R}_+^*$, mais de façon floue seulement. Cette « assimilation » est à proprement parler un isomorphisme.

Exemple Le morphisme de groupes $x \longmapsto \mathrm{e}^{2\mathrm{i}\pi x}$ de $\mathbb{R}$ dans $\mathbb{C}^*$ induit par quotient un isomorphisme de $\dfrac{\mathbb{R}}{\mathbb{Z}}$ sur $\mathbb{U}$. Nous avions déjà vaguement compris que $\dfrac{\mathbb{R}}{\mathbb{Z}}$ se refermait sur lui-même en quelque sorte, mais la notion d'isomorphisme fournit à cette circularité un sens plus rigoureux.

Exemple Pour tout $n \in \mathbb{N}^*$, la signature ε induit par quotient un isomorphisme de $\dfrac{S_n}{A_n}$ sur $\{\pm 1\}$. En résumé, que reste-t-il de S_n quand on y rend les permutations paires indiscernables ? Il ne reste plus grand-chose justement, seulement les valeurs possibles de la signature.

Exemple Pour tout corps $\mathbb{K}$ et pour tout $n \in \mathbb{N}^*$, le déterminant induit par quotient un isomorphisme de $\dfrac{\mathrm{GL}_n(\mathbb{K})}{\mathrm{SL}_n(\mathbb{K})}$ sur $\mathbb{K}^*$. En résumé, que reste-t-il de $\mathrm{GL}_n(\mathbb{K})$ quand on y rend les matrices de déterminant 1 indiscernables ? Il ne reste plus grand-chose justement, seulement les valeurs possibles du déterminant.

Le théorème d'isomorphisme va nous permettre de calculer les valeurs de l'indicatrice d'Euler avec une certaine élégance.

Théorème (Calcul des valeurs de 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 $n \in \mathbb{N}^*$: $\quad \varphi(n) = \displaystyle\prod_{p \in \mathbb{P}} p^{v_p(n)-1}(p-1)$.

Par exemple : $\quad \varphi(360) = \varphi\big(2^3 \times 3^2 \times 5\big) = 2^{3-1}(2-1) \times 3^{2-1}(3-1) \times 5^{1-1}(5-1) = 4 \times 6 \times 4 = 96$, $\quad$ donc d'après le théorème d'Euler, pour tout $x \in \mathbb{Z}$ non divisible par 2, 3 ou 5 : $\quad x^{96} \equiv 1\ [360]$.

Démonstration

(i) Soient $m, n \in \mathbb{N}^*$ premiers entre eux. Notons f l'application $x \longmapsto \big(\overline{x}, \widehat{x}\big)$ de $\mathbb{Z}$ dans $\dfrac{\mathbb{Z}}{m\mathbb{Z}} \times \dfrac{\mathbb{Z}}{n\mathbb{Z}}$ dans laquelle $\overline{x}$ désigne la classe de congruence de x modulo m et $\widehat{x}$ sa classe de congruence modulo n. Cette application f est un morphisme de groupes additifs, car pour tous $x, y \in \mathbb{Z}$: $\quad f(x+y) = f(x) + f(y)$ $\quad$ comme on le vérifie aisément. Le noyau de f est également facile à calculer. Pour tout $x \in \mathbb{Z}$:

$$\begin{aligned} x \in \operatorname{Ker} f \quad &\Longleftrightarrow \quad \overline{x} = \overline{0} \quad \text{et} \quad \widehat{x} = \widehat{0} \quad \Longleftrightarrow \quad x \text{ est divisible par } m \text{ et } n \\ &\overset{m \wedge n = 1}{\Longleftrightarrow} \quad x \text{ est divisible par } mn \quad \Longleftrightarrow \quad x \in mn\mathbb{Z}. \end{aligned}$$

Ainsi, f induit par quotient un morphisme de groupes injectif F de $\dfrac{\mathbb{Z}}{mn\mathbb{Z}}$ dans $\dfrac{\mathbb{Z}}{m\mathbb{Z}} \times \dfrac{\mathbb{Z}}{n\mathbb{Z}}$, mais comme les ensembles de départ et d'arrivée ont ici même cardinal fini, F est en fait un isomorphisme. Pour tout $x \in \mathbb{Z}$, nous noterons $\widetilde{x}$ la classe de congruence de x modulo mn. À présent, pour tout $x \in \mathbb{Z}$:

$$\begin{aligned} \widetilde{x} \in \mathrm{U}\Big(\frac{\mathbb{Z}}{mn\mathbb{Z}}\Big) \quad &\Longleftrightarrow \quad x \wedge (mn) = 1 \quad \Longleftrightarrow \quad x \wedge m = x \wedge n = 1 \\ &\Longleftrightarrow \quad F\big(\widetilde{x}\big) = \big(\overline{x}, \widehat{x}\big) \in \mathrm{U}\Big(\frac{\mathbb{Z}}{m\mathbb{Z}}\Big) \times \mathrm{U}\Big(\frac{\mathbb{Z}}{n\mathbb{Z}}\Big), \end{aligned}$$

donc F est bijective de $\mathrm{U}\Big(\dfrac{\mathbb{Z}}{mn\mathbb{Z}}\Big)$ sur $\mathrm{U}\Big(\dfrac{\mathbb{Z}}{m\mathbb{Z}}\Big) \times \mathrm{U}\Big(\dfrac{\mathbb{Z}}{n\mathbb{Z}}\Big)$. Or f n'est pas seulement un morphisme de groupes additifs, c'est aussi un morphisme de magmas multiplicatifs en ce sens que pour tous $x, y \in \mathbb{Z}$: $f(x \times y) = f(x) \times f(y)$, $\quad$ et donc : $\quad F\big(\widetilde{x} \times \widetilde{y}\big) = F\big(\widetilde{x \times y}\big) = f(x \times y) = f(x) \times f(y) = F\big(\widetilde{x}\big) \times F\big(\widetilde{y}\big)$. Conclusion : F est un isomorphisme de groupes de $\mathrm{U}\Big(\dfrac{\mathbb{Z}}{mn\mathbb{Z}}\Big)$ sur $\mathrm{U}\Big(\dfrac{\mathbb{Z}}{m\mathbb{Z}}\Big) \times \mathrm{U}\Big(\dfrac{\mathbb{Z}}{n\mathbb{Z}}\Big)$, $\quad$ donc comme voulu :

$$\varphi(mn) = \Big|\mathrm{U}\Big(\frac{\mathbb{Z}}{mn\mathbb{Z}}\Big)\Big| = \Big|\mathrm{U}\Big(\frac{\mathbb{Z}}{m\mathbb{Z}}\Big) \times \mathrm{U}\Big(\frac{\mathbb{Z}}{n\mathbb{Z}}\Big)\Big| = \Big|\mathrm{U}\Big(\frac{\mathbb{Z}}{m\mathbb{Z}}\Big)\Big| \times \Big|\mathrm{U}\Big(\frac{\mathbb{Z}}{n\mathbb{Z}}\Big)\Big| = \varphi(m)\,\varphi(n).$$

(ii) D'après (i), pour tout $n \in \mathbb{N}^*$: $\quad \varphi(n) = \varphi\left(\displaystyle\prod_{p \in \mathbb{P}} p^{v_p(n)}\right) = \displaystyle\prod_{p \in \mathbb{P}} \varphi\big(p^{v_p(n)}\big)$ $\quad$ et nous avons déjà montré que : $\varphi\big(p^{v_p(n)}\big) = p^{v_p(n)-1}(p-1)$. ∎

Le théorème d'isomorphisme éclaire également les groupes monogènes d'une lumière nouvelle.

Théorème (Classification des groupes monogènes à isomorphisme près) Soit G un groupe monogène engendré par un certain élément x.

- Si G est infini, l'application $k \longmapsto x^k$ est un isomorphisme de $\mathbb{Z}$ sur G.
- Si G est fini, l'application $k \longmapsto x^k$ de $\mathbb{Z}$ dans G induit par quotient un isomorphisme de $\dfrac{\mathbb{Z}}{|x|\mathbb{Z}}$ sur G. On dit que G est *cyclique* (*d'ordre* $|x|$).

En résumé, $\mathbb{Z}$ et ses quotients sont à isomorphisme près les seuls groupes monogènes.

Démonstration L'application $k \overset{\varphi}{\longmapsto} x^k$ est un morphisme de groupes surjectif de $\mathbb{Z}$ sur $G = \langle x \rangle$ et induit par quotient un isomorphisme de $\dfrac{\mathbb{Z}}{\operatorname{Ker}\varphi}$ sur G. Si G est fini, x est d'ordre fini et par définition de $|x|$: $\operatorname{Ker}\varphi = |x|\mathbb{Z}$. Si au contraire G est infini, il en est de même du quotient $\dfrac{\mathbb{Z}}{\operatorname{Ker}\varphi}$, donc : $\operatorname{Ker}\varphi = 0\mathbb{Z} = \{0\}$, mais dans ce cas, φ est injective, donc est un isomorphisme de $\mathbb{Z}$ sur G. ■

Théorème (Classification des groupes d'ordre premier à isomorphisme près) Soit $p \in \mathbb{P}$. Tout groupe d'ordre p est isomorphe à $\dfrac{\mathbb{Z}}{p\mathbb{Z}}$ — donc abélien en particulier.

Démonstration Soit G un groupe d'ordre p. Donnons-nous un élément quelconque x de $G \setminus \{1\}$. D'après le théorème de Lagrange, $|x|$ divise p, or ici : $x \neq 1$, donc : $|x| = p$. Enfin, d'après le théorème précédent, l'application $k \longmapsto x^k$ induit par quotient un isomorphisme de $\dfrac{\mathbb{Z}}{p\mathbb{Z}}$ sur G. ■

Exemple Peut-on déterminer de même les groupes d'ordre 4 à isomorphisme près ? Nous en connaissons déjà deux : $\dfrac{\mathbb{Z}}{4\mathbb{Z}}$ et $\dfrac{\mathbb{Z}}{2\mathbb{Z}} \times \dfrac{\mathbb{Z}}{2\mathbb{Z}}$, en l'occurrence abéliens, et nous allons montrer qu'il n'y en a pas d'autres à isomorphisme près. Ces deux groupes sont bien non isomorphes car $\dfrac{\mathbb{Z}}{4\mathbb{Z}}$ contient des éléments d'ordre 4 alors que $\dfrac{\mathbb{Z}}{2\mathbb{Z}} \times \dfrac{\mathbb{Z}}{2\mathbb{Z}}$ n'en contient pas.
Soit G un groupe d'ordre 4. Si G est cyclique, G est isomorphe à $\dfrac{\mathbb{Z}}{4\mathbb{Z}}$. Supposons-le non cyclique.

- Dans ce cas, aucun élément de G n'est d'ordre 4, donc d'après le théorème de Lagrange, tout élément non trivial de G est d'ordre 2. En d'autres termes : $x^2 = 1$ pour tout $x \in G$, donc pour tous $x, y \in G$: $x^2y^2 = 1 = (xy)^2$, puis après simplification : $xy = yx$. Ainsi, G est abélien et tout élément de G est égal à son inverse.
- Introduisons les éléments de G : $G = \{1, a, b, c\}$. Le produit ab ne peut valoir ni 1, ni a, ni b, donc : $ab = ba = c$. On calcule de même tout autre produit de deux éléments de G, ce dont découle la table ci-dessous, qui coïncide avec la table de $\dfrac{\mathbb{Z}}{2\mathbb{Z}} \times \dfrac{\mathbb{Z}}{2\mathbb{Z}}$ que nous avons déjà détaillée plus haut. Conclusion : G est isomorphe à $\dfrac{\mathbb{Z}}{2\mathbb{Z}} \times \dfrac{\mathbb{Z}}{2\mathbb{Z}}$.

$\times$	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

La classification des groupes à isomorphisme près est l'alpha et l'oméga de la théorie des groupes, mais le monde des groupes est trop riche et nul ne pense qu'une telle classification est possible, même pour les seuls groupes finis. Les espaces

vectoriels de dimension finie sont tellement plus reposants ! Leur classification à isomorphisme près est non seulement possible, mais elle est surtout très simple. Un seul entier suffit à les distinguer — la dimension. Pour tout $n \in \mathbb{N}$, il existe un et un seul espace vectoriel de dimension n. La théorie des groupes se heurte à une complexité inouïe en comparaison.

Tout espoir n'est pas perdu cela dit grâce au *théorème de Jordan-Hölder* que nous allons juste évoquer à titre culturel. Mais d'abord, une définition.

Définition **(Groupe simple)** Soit G un groupe. On dit que G est *simple* si : $G \neq \{1\}$ et si ses seuls sous-groupes distingués sont $\{1\}$ et G.

Les groupes simples sont un peu à la théorie des groupes ce que les nombres premiers sont à l'arithmétique comme on va le comprendre dans un instant. Dans le lot, certains sont abéliens, que nous connaissons bien.

Théorème **(Groupes simples abéliens)** À isomorphisme près, les groupes simples abéliens sont exactement les groupes $\frac{\mathbb{Z}}{p\mathbb{Z}}$, p décrivant $\mathbb{P}$.

Démonstration

- Pour commencer, soit $p \in \mathbb{P}$ D'après le théorème de Lagrange, $\frac{\mathbb{Z}}{p\mathbb{Z}}$ ne possède que deux sous-groupes en tout : $\{0\}$ et lui-même, distingués. Conclusion : $\frac{\mathbb{Z}}{p\mathbb{Z}}$ est simple — et abélien.
- Réciproquement, soit G un groupe simple abélien. Comme G est abélien, ses sous-groupes sont tous distingués, mais du coup en retour, G étant simple, il ne possède que deux sous-groupes, à savoir $\{1\}$ et lui-même.

  Fixons x dans $G \setminus \{1\}$. Comme $\langle x\rangle$ est un sous-groupe de G autre que $\{1\}$: $G = \langle x\rangle$, donc G est isomorphe à $\mathbb{Z}$ ou à $\frac{\mathbb{Z}}{|x|\mathbb{Z}}$. Or $\mathbb{Z}$ a plus que deux sous-groupes, donc G est fini isomorphe à $\frac{\mathbb{Z}}{|x|\mathbb{Z}}$.

  Il nous reste à montrer que $|x|$ est un nombre premier. Notons pour cela p l'un de ses diviseurs premiers. L'égalité : $\left(x^{\frac{|x|}{p}}\right)^p = x^{|x|} = 1$ montre que $x^{\frac{|x|}{p}}$ est d'ordre un diviseur de p, mais comme x est d'ordre $|x|$ et : $\frac{|x|}{p} < |x|$, forcément : $|x| = p$. ∎

La classification des groupes simples abéliens est finalement on ne peut plus facile, mais il existe des groupes simples non abéliens, certains finis, d'autres infinis. On peut montrer par exemple que pour tout $n \geqslant 5$, le groupe alterné A_n est simple. Dans le cas des groupes finis, l'intérêt des groupes simples est énoncé en des termes très clairs par le *théorème de Jordan-Hölder*.

Théorème **(Théorème de Jordan-Hölder)** Soit G un groupe fini. On appelle *suite de Jordan-Hölder de G* toute famille $(H_0, \dots, H_n)$ de sous-groupes de G pour lesquels :

— $H_0 = \{1\}$ et $H_n = G$,

— H_i est un sous-groupe distingué de H_{i+1} pour tout $i \in [\![0, n-1]\!]$,

— $\frac{H_{i+1}}{H_i}$ est un groupe simple pour tout $i \in [\![0, n-1]\!]$.

De telles suites existent toujours — ça, c'est facile à comprendre. Ce qui l'est moins, c'est que si $(H_0, \dots, H_n)$ et $(H'_0, \dots, H'_{n'})$ sont deux suites de Jordan-Hölder de G, alors d'une part : $n = n'$, mais d'autre part il existe une permutation σ de $[\![1, n]\!]$ pour laquelle pour tout $i \in [\![0, n-1]\!]$, les groupes $\frac{H_{i+1}}{H_i}$ et $\frac{H'_{\sigma(i)+1}}{H'_{\sigma(i)}}$ sont isomorphes.

Tout groupe fini peut être ainsi vu comme un assemblage de groupes finis simples dont le nombre et la nature à isomorphisme près sont entièrement fixés. Le théorème de Jordan-Hölder est en quelque sorte le théorème de factorisation première

de la théorie des groupes finis. La différence, c'est qu'il n'y a qu'une seule manière de multiplier deux entiers entre eux alors qu'il y a tout un tas de manières d'empiler deux groupes l'un sur l'autre. On connaît relativement bien un groupe G quand on connaît l'un de ses sous-groupes distingué H ainsi que le quotient $\frac{G}{H}$, mais on ne connaît pas G entièrement. La manière dont $\frac{G}{H}$ est empilé sur H est déterminante et les empilements sont variés. Deux questions se posent alors au théoricien des groupes :

— qui sont exactement les groupes simples, et notamment les groupes finis simples ?

— à quelles conditions un assemblage de groupes simples est-il possible ?

La deuxième question est encore ouverte et il est probable qu'on n'arrivera pas à lui donner une réponse exhaustive définitive. La première a quant à elle fait l'objet d'intenses recherches depuis la fin du $19^{\text{ème}}$ siècle avec un pic d'activité pendant toute la deuxième moitié du $20^{\text{ème}}$ siècle. Il en est sorti un théorème, un théorème fascinant mais monstrueux qu'on appelle la *classification des groupes finis simples* et qui court, dit-on, sur des milliers de pages, sans doute au moins 10 000. Un seul théorème, vraiment ? Il faut plutôt voir ce résultat comme un foisonnement d'articles éparpillés dans des dizaines de revues, même si un gros effort de synthèse a été fourni depuis les années 1980 pour alléger l'ensemble. En résumé, la classification des groupes finis simples énonce que tout groupe fini simple est :

— soit l'un des groupes cycliques $\frac{\mathbb{Z}}{p\mathbb{Z}}$ pour un certain $p \in \mathbb{P}$,

— soit l'un des groupes alternés A_n pour un certain $n \geqslant 5$,

— soit un groupe appartenant à certaines familles classiques de groupes finis — construits à partir des groupes linéaires $\mathrm{GL}_n(\mathbb{K})$ par exemple,

— soit l'une des 26 exceptions qu'on appelle les *groupes sporadiques* et dont le plus volumineux, dit *le monstre*, a pour ordre : $2^{46} \times 3^{20} \times 5^9 \times 7^6 \times 11^2 \times 13^3 \times 17 \times 19 \times 23 \times 29 \times 31 \times 41 \times 47 \times 59 \times 71$
$= 808\,017\,424\,794\,512\,875\,886\,459\,904\,961\,710\,757\,005\,754\,368\,000\,000\,000.$

Les groupes finis simples sont finalement assez divers, mais le *théorème de Feit-Thompson*, démontré en 1963 et qui a en quelque sorte lancé la classification des groupes finis simples, énonce que tout groupe fini simple **non abélien** est d'ordre pair. En d'autres termes, tout groupe fini d'ordre impair est un empilement de groupes $\frac{\mathbb{Z}}{p\mathbb{Z}}$ avec $p \in \mathbb{P}$. En théorie des groupes, le nombre premier 2 est toujours un peu à part.