Christophe Bertault

Une introduction aux structures quotients en MPSI

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 orthodoxes 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 $\frac{\mathbb{Z}}{n\mathbb{Z}}$.

1 Lois quotients

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 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 la loi de E* si pour tous $x, y, x', y' \in E$: $\big(x \mathcal{R} x' \quad \text{et} \quad y \mathcal{R} y'\big) \implies xy \mathcal{R} x'y'$.

On peut définir dans ces conditions une loi interne sur l'ensemble quotient $E\big/\mathcal{R}$, dite *loi quotient*, en posant $\overline{x} \star \overline{y} = \overline{xy}$ pour tous $x, y \in E$.

(i) **Propriétés transmises à la loi quotient :** Si E est associatif (resp. commutatif), $E\big/\mathcal{R}$ l'est aussi.

Si E possède un élément neutre 1, $E\big/\mathcal{R}$ admet $\overline{1}$ pour élément neutre. De plus, dans ce cas, pour tout $x \in E$ inversible, $\overline{x}$ est inversible dans $E\big/\mathcal{R}$ et $\overline{x}^{-1} = \overline{x^{-1}}$.

(ii) **Cas des groupes :** Si E est un groupe, $E\big/\mathcal{R}$ en est un aussi et l'application $x \longmapsto \overline{x}$ est un morphisme de groupes de E dans $E\big/\mathcal{R}$.

En outre, il existe un sous-groupe H de G pour lequel pour tous $x, y \in G$: $x \mathcal{R} y \iff xy^{-1} \in H$.

La relation $\overline{x} \star \overline{y} = \overline{xy}$ 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. Pourtant, 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 $x \mathcal{R} x'$. La compatibilité de $\mathcal{R}$ avec la loi de E est précisément là pour garantir l'indépendance de $\overline{xy}$ vis-à-vis des choix divers qu'on peut faire de x et y. En cas de compatibilité, $\overline{xy}$ dépend de $\overline{x}$ et $\overline{y}$, mais pas vraiment du choix des éléments x et y.

La fin de l'assertion (ii) montre que les relations compatibles avec une loi de groupe n'ont vraiment pas n'importe quelle tête, elles sont fortement liées aux sous-groupes de E — mais pas n'importe lesquels, comme nous le verrons bientôt.

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

(i) Si E est associatif, alors pour tous $x, y, z \in E$: $\overline{x} \star \big(\overline{y} \star \overline{z}\big) = \overline{x} \star \overline{yz} = \overline{x(yz)} = \overline{(xy)z}$
$= \overline{xy} \star \overline{z} = \big(\overline{x} \star \overline{y}\big) \star \overline{z}$.

De même, si E est commutatif, alors pour tous $x, y \in E$: $\overline{x} \star \overline{y} = \overline{xy} = \overline{yx} = \overline{y} \star \overline{x}$. Enfin, si E possède un élément neutre e, alors pour tout $x \in E$: $\overline{x} \star \overline{e} = \overline{xe} = \overline{x}$ et $\overline{e} \star \overline{x} = \overline{ex} = \overline{x}$, donc $\overline{e}$ est neutre dans $E\big/\mathcal{R}$, et pour tout $x \in E$ inversible : $\overline{x} \star \overline{x^{-1}} = \overline{xx^{-1}} = \overline{e}$ et $\overline{x^{-1}} \star \overline{x} = \overline{x^{-1}x} = \overline{e}$, donc $\overline{x}$ est inversible dans $E\big/\mathcal{R}$ et $\overline{x}^{-1} = \overline{x^{-1}}$.

(ii) L'application $x \longmapsto \overline{x}$ est un morphisme de groupes par simple définition de la loi quotient. Son noyau H est dès lors un sous-groupe de E, et en l'occurrence $H = \Big\{x \in E \mid \overline{x} = \overline{1}\Big\} = \Big\{x \in E \mid x \mathcal{R} 1\Big\} = \overline{1}$.
Enfin, pour tous $x, y \in E$, par compatibilité de $\mathcal{R}$ avec la loi de E, sachant que $y^{-1} \mathcal{R} y^{-1}$ pour l'implication directe et $y \mathcal{R} y$ pour la réciproque :

$$x \mathcal{R} y \iff xy^{-1} \mathcal{R} yy'^{-1} \iff xy^{-1} \mathcal{R} 1 \iff xy^{-1} \in \overline{1} = H. \qquad \blacksquare$$

2 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 :
$$x \equiv y\ [n] \quad \Longleftrightarrow \quad x - y \in n\mathbb{Z}$$
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 :
$$\overline{x} = \left\{ y \in \mathbb{Z} \mid \quad y \equiv x\ [n] \right\} = \left\{ x + nk \mid \quad k \in \mathbb{Z} \right\} = x + n\mathbb{Z}.$$
Par conséquent : $\frac{\mathbb{Z}}{n\mathbb{Z}} = \left\{ \overline{x} \mid \quad x \in \mathbb{Z} \right\} = \left\{ x + n\mathbb{Z} \mid \quad x \in \mathbb{Z} \right\}$. 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 : $7 \equiv -5\ [12]$ dans $\mathbb{Z}$, donc $\overline{7} = \overline{-5}$ dans $\frac{\mathbb{Z}}{12\mathbb{Z}}$. Les entiers distincts 7 et -5 deviennent ainsi un objet unique dans $\frac{\mathbb{Z}}{12\mathbb{Z}}$. On peut également 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 $\frac{\mathbb{Z}}{n\mathbb{Z}} = \left\{ \overline{x} \mid \quad x \in [\![0, n-1]\!] \right\}$.

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

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

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 comme $7 \times 10 - 3 \times 23 = 1$: $7 \times 10 = 1$ dans $\frac{\mathbb{Z}}{23\mathbb{Z}}$, donc $10^{-1} = 7$.

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 $x \in \frac{\mathbb{Z}}{11\mathbb{Z}}$: $x^2 - 3x + 7 = \big(x - 2^{-1}3\big)^2 - \big(2^{-1}3\big)^2 + 7 = \big(x - 6 \times 3\big)^2 - (6 \times 3)^2 + 7 = (x-7)^2 - 9$, donc :

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

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 $x \in \frac{\mathbb{Z}}{p\mathbb{Z}}$: $x^p = x$, et si $x \neq 0$, alors $x^{p-1} = 1$.

Démonstration Nous allons donner de ce résultat une preuve plus typique de $\frac{\mathbb{Z}}{p\mathbb{Z}}$ que celle qu'on en donne généralement dans $\mathbb{Z}$. Fixons $x \in \frac{\mathbb{Z}}{p\mathbb{Z}} \setminus \{0\}$, inversible car $\frac{\mathbb{Z}}{p\mathbb{Z}}$ est un CORPS, et notons π le produit $\prod_{y \neq 0} y$ de tous les éléments non nuls de $\frac{\mathbb{Z}}{p\mathbb{Z}}$, 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 $\frac{\mathbb{Z}}{p\mathbb{Z}} \setminus \{0\}$ sur lui-même de réciproque $z \longmapsto xz$. Ainsi : $\pi \overset{z = x^{-1}y}{=} \prod_{z \neq 0} (xz) = \prod_{z \neq 0} x \prod_{z \neq 0} z = x^{p-1}\pi$. Divisons par π, qui est non nul : $x^{p-1} = 1$.

Voici pour finir un résultat moins important mais dont la jolie 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 $p \in \mathbb{P}$: $(p-1)! = -1$ dans $\frac{\mathbb{Z}}{p\mathbb{Z}}$.
En outre, si p est impair : $\left(\frac{p-1}{2}\right)!^2 = (-1)^{\frac{p+1}{2}}$.

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 $\frac{\mathbb{Z}}{p\mathbb{Z}}$, donc tout élément inversible de $\frac{\mathbb{Z}}{p\mathbb{Z}}$ figure dans ce produit avec son inverse. Or certains éléments coïncident peut-être avec leur inverse, mais lesquels ? Pour tout $x \in \frac{\mathbb{Z}}{p\mathbb{Z}} \setminus \{0\}$:

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

Regroupons ainsi tout élément avec son inverse dans le produit $(p-1)!$: $(p-1)! = 1 \times (-1) = -1$. Le théorème de Wilson est démontré. Pour le deuxième point, p étant impair, $n = \frac{p-1}{2}$ est un entier et :

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

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

Exemple Soit $p \in \mathbb{P}$. On suppose $p \equiv 1\ [4]$ et on s'intéresse à l'équation $x^2 + 2x + 2 = 0$ d'inconnue $x \in \frac{\mathbb{Z}}{p\mathbb{Z}}$. Comme $\frac{p+1}{2} \equiv 1\ [2]$, d'après le corollaire du théorème de Wilson : $\left(\frac{p-1}{2}\right)!^2 \equiv (-1)^{p+1} = -1$. Ainsi, pour tout $x \in \frac{\mathbb{Z}}{p\mathbb{Z}}$: $x^2 + 2x + 2 = (x+1)^2 + 1 = (x+1)^2 - \left(\frac{p-1}{2}\right)!^2$, donc :

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

3 Espaces vectoriels quotients

Dans ce paragraphe, $\mathbb{K}$ désigne un corps quelconque, typiquement $\mathbb{R}$ ou $\mathbb{C}$, mais pourquoi pas $\frac{\mathbb{Z}}{p\mathbb{Z}}$ 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 :

$$x \equiv y\ [F] \iff x - y \in F.$$

Cette relation $\equiv\ [F]$ est une relation d'équivalence sur E. On note $\frac{E}{F}$ 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*.

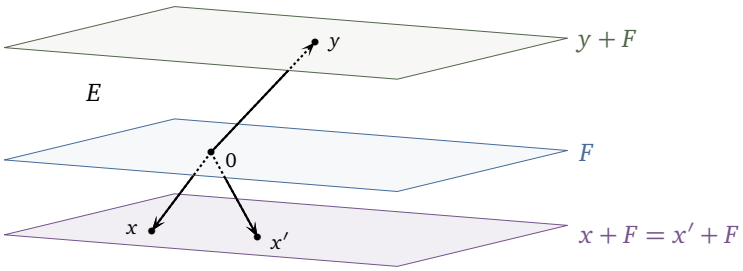
Pour tout $x \in E$, $\overline{x}$ n'est jamais que le sous-espace affine de E de direction F passant par x.

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 $x \equiv y\ [F]$: $x - y \in F$, 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 $x \in E$: $\overline{x} = \left\{y \in E \mid y \equiv x\ [F]\right\} = \left\{x + f \mid f \in F\right\} = x + F$.

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 $\frac{E}{F}$. Tout simplement, alors que E est la réunion des sous-espaces affines $x + F$, x décrivant E, $\frac{E}{F}$ 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 $\frac{E}{F}$.



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

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.

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

Muni de ces opérations, $\frac{E}{F}$ 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

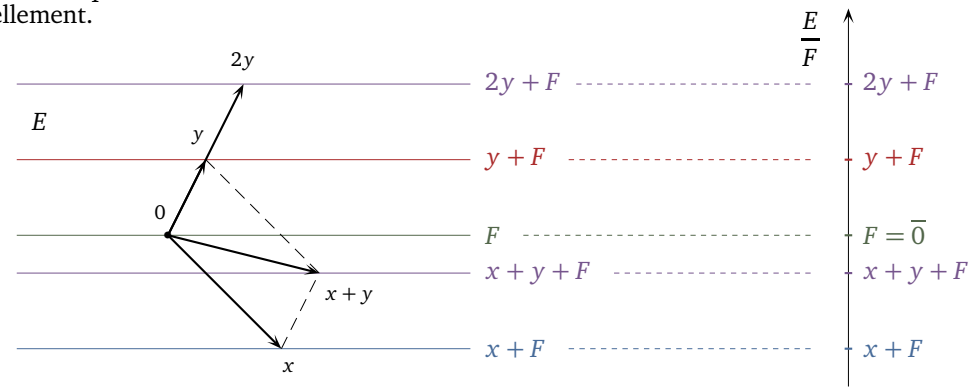
- **Loi additive :** Soient $x, y, x', y' \in E$. Si $x \equiv x'\ [F]$ et $y \equiv y'\ [F]$, alors $x - x' \in F$ et $y - y' \in F$, donc F étant stable par addition : $\quad (x+y) - (x'+y') \in F, \quad$ autrement dit $x + y \equiv x' + y'\ [F]$.
- **Loi externe :** Soient $x, x' \in E$ et $\lambda \in \mathbb{K}$. Si $x \equiv x'\ [F]$: $\quad x - x' \in F, \quad$ donc F étant stable par multiplication par un scalaire : $\quad \lambda \cdot x - \lambda \cdot x' = \lambda \cdot (x - x') \in F, \quad$ 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 $\lambda, \mu \in \mathbb{K}$: $\quad 1 \cdot \overline{x} = \overline{1 \cdot x} = \overline{x} \quad$ et :

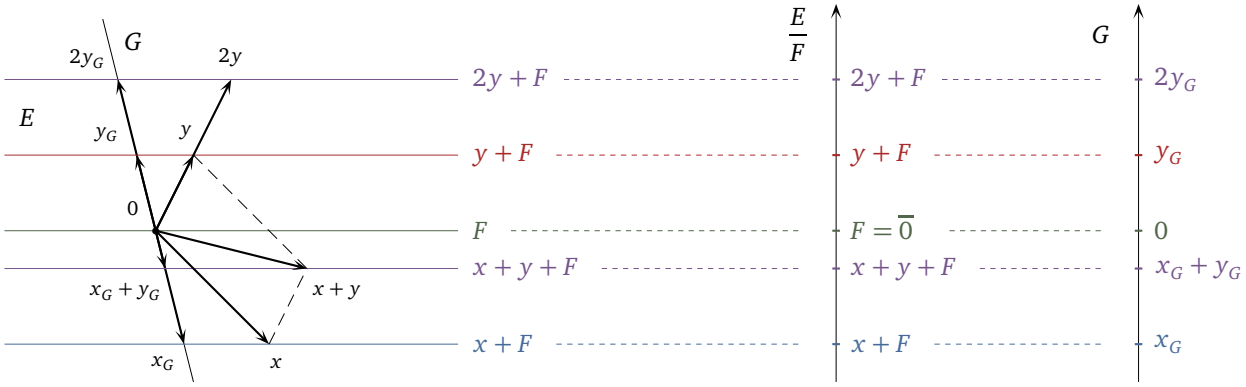
$$\lambda \cdot \left(\overline{x} + \overline{y}\right) = \lambda \cdot \overline{x+y} = \overline{\lambda \cdot (x+y)} = \overline{\lambda \cdot x + \lambda \cdot y} = \overline{\lambda \cdot x} + \overline{\lambda \cdot y} = \lambda \cdot \overline{x} + \lambda \cdot \overline{y},$$

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

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 $\frac{E}{F}$, 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 $\frac{E}{F}$. Ainsi, si E est de dimension finie : $\dim \frac{E}{F} = \dim E - \dim F$.

La supplémentarité de F et G dans E fait ici écho au théorème de la division euclidienne dans le contexte des anneaux $\frac{\mathbb{Z}}{n\mathbb{Z}}$. 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* $A + B = \{a + b \mid \quad a \in A \quad \text{et} \quad b \in B\}$. 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 $\frac{\mathbb{Z}}{n\mathbb{Z}}$, l'égalité $E = F \oplus G$ nous fournit à présent une bijection π de G sur $\frac{E}{F}$.

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 $\frac{E}{F}$. Sa linéarité est une autre manière d'énoncer la compatibilité des opérations $+$ et $\cdot$ avec la relation $\equiv \ [F]$. Enfin, pour tout $x \in E$: $\quad x \in \operatorname{Ker} \pi \iff \overline{x} = \overline{0} \iff x \equiv 0 \ [F] \iff x \in F$. ∎

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 $x \equiv y \ [\operatorname{Ker} f]$: $x - y \in \operatorname{Ker} f$, $\quad$ donc $f(x-y) = 0$, i.e. $f(x) = f(y)$. En d'autres termes, pour tous $x, y \in E$: $\quad \overline{x} = \overline{y} \implies f(x) = f(y)$. Cette *compatibilité de la relation* $\equiv \ [\operatorname{Ker} f]$ *avec* f nous permet de poser sans ambiguïté $\overline{f}(\overline{x}) = f(x)$ pour tout $x \in E$. On définit ainsi une application $\overline{f}$ de $\frac{E}{F}$ 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 $\equiv \ [\operatorname{Ker} f]$ est compatible avec f au sens où pour tout $x, y \in E$: $\quad x \equiv x' \ [\operatorname{Ker} f] \implies f(x) = f(x')$. On définit donc une application $\overline{f}$ en posant $\overline{f}(\overline{x}) = f(x)$ pour tout $x \in E$.

Cette application $\overline{f}$ est alors un isomorphisme $\overline{f}$ de $\frac{E}{\operatorname{Ker} f}$ sur $\operatorname{Im} f$. On dit que f *induit par quotient* un isomorphisme $\overline{f}$ de $\frac{E}{\operatorname{Ker} f}$ sur $\operatorname{Im} f$.

Théorème du rang usuel : Si E est de dimension finie, $\frac{E}{\operatorname{Ker} f}$ est de dimension finie et : $\quad \dim \frac{E}{\operatorname{Ker} f} = \dim \operatorname{Im} f$, $\quad$ ce qui nous ramène à la forme usuelle du théorème du rang : $\quad \dim E = \dim \operatorname{Ker} f + \dim \operatorname{Im} f$.

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 $\operatorname{Im} f$. 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 distinguer 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 :** $\operatorname{Im}\overline{f} = \left\{\overline{f}(y) \;\middle|\; y \in \dfrac{E}{F}\right\} = \big\{\overline{f}\big(\overline{x}\big) \mid x \in E\big\} = \big\{f(x) \mid x \in E\big\} = \operatorname{Im} f.$
- **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 $\operatorname{Ker} f$.

4 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 ne sont qu'un exemple parmi tant d'autres de groupes quotients, et nous n'avons commencé par eux que parce que les espaces vectoriels sont à l'honneur en MPSI, contrairement aux groupes. Dans les livres de mathématiques, les groupes quotients sont toujours la première structure quotient 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 :
$$x \equiv y\ [H] \iff xy^{-1} \in H.$$
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 $x \equiv y\ [H]$: $xy^{-1} \in H$, mais H est stable par inversion, donc $yx^{-1} = \big(xy^{-1}\big)^{-1} \in H$, 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 : $xz^{-1} = \big(xy^{-1}\big)\big(yz^{-1}\big) \in H$, i.e. $x \equiv z\ [H]$.
- **Classes d'équivalence :** Pour tout $x \in G$: $\overline{x} = \big\{y \in G \mid y \equiv x\ [H]\big\} = \big\{hx \mid h \in H\big\} = Hx.$

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 $\big|G:H\big|$ le cardinal — peut-être infini — de l'ensemble quotient G/H.

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

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 $|Hx| = |H|$. 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 : $\quad G = \big|G:H\big| \times |H|$.

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 qu'un ensemble à ce stade et non un groupe. La relation $\equiv\ [H]$ est-elle compatible avec la loi de G ? Eh bien 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.

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

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

(ii) **Groupe quotient :** Les assertions suivantes sont équivalentes :

— H est distingué dans G.

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

On définit dans ce cas une loi sur G/H en posant pour tous $x, y \in G$: $\quad \overline{x}\,\overline{y} = \overline{xy}$. 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*.
Enfin, l'application $x \longmapsto \overline{x}$ est un morphisme de groupes surjectif de G sur $\dfrac{G}{H}$ de noyau H.

Dire que H est distingué dans G, c'est dire que pour tout $x \in G$: $\quad Hx = xH$, $\quad$ 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. Pour commencer $1 = x^{-1}1x \in x^{-1}Hx$. 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 que $x \equiv x'\ [H]$ et $y \equiv y'\ [H]$, i.e. que $xx'^{-1} \in H$ et $yy'^{-1} \in H$. Comme H est distingué dans G, on peut aussi affirmer que : $\quad x\big(yy'\big)^{-1}x^{-1} \in xHx^{-1} = H$, $\quad$ mais du coup : $(xy)(x'y')^{-1} = \underbrace{x\big(yy'^{-1}\big)x^{-1}}_{\in H}\underbrace{\big(xx'^{-1}\big)}_{\in H} \in H$, $\quad$ donc $xy \equiv x'y'\ [H]$.

Réciproquement, supposons $\equiv\ [H]$ 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 $hx \equiv x\ [H]$, $\quad$ donc par compatibilité de $\equiv\ [H]$ avec la loi de G : $\quad x^{-1}(hx) \equiv x^{-1}x\ [H]$, $\quad$ i.e. $x^{-1}hx \equiv 1\ [H]$, ou encore $x^{-1}hx \in H$. Conclusion : $\quad x^{-1}Hx \subset H$. A fortiori, en remplaçant x par x^{-1} : $\quad xHx^{-1} \subset H$, $\quad$ donc $H \subset x^{-1}Hx$, et enfin $x^{-1}Hx = H$.

Pour finir, notons π le morphisme de groupes $x \longmapsto \overline{x}$ de G dans $\dfrac{G}{H}$. Ce morphisme est surjectif par définition de $\dfrac{G}{H}$ et pour tout $x \in G$: $\quad x \in \operatorname{Ker}\pi \iff \overline{x} = \overline{1} \iff x \equiv 1\,[H] \iff x \in H.$ ∎

En pratique, on vient de voir dans cette preuve 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 $\dfrac{G}{\{1\}} = \Big\{\{x\} \mid \quad x \in G\Big\}$ 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 $n = 0$, $\dfrac{\mathbb{Z}}{0\mathbb{Z}}$ est infini et 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 $r \in [\![0, n-1]\!]$, donc comme G contient $n\mathbb{Z}$: $\quad r = g - nq \in G$. $\quad$ Ainsi r appartient à $G \cap \mathbb{N}$ et $r < n$, donc $r = 0$ par minimalité de n, i.e. $g = nq$. Conclusion : $\quad G \subset n\mathbb{Z}$.

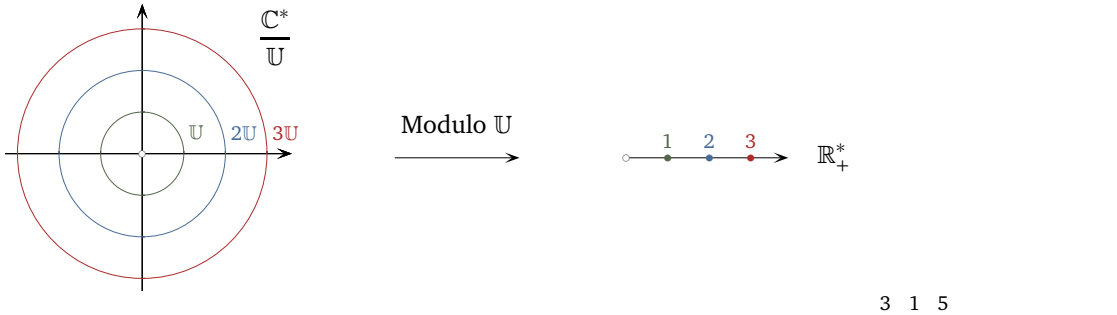
Exemple $\mathbb{R}_+^*$ est un sous-groupe distingué du groupe abélien $\mathbb{R}^*$ et :

$$\frac{\mathbb{R}^*}{\mathbb{R}_+^*} = \Big\{x\mathbb{R}_+^* \mid \quad x \in \mathbb{R}^*\Big\} = \Big\{\mathbb{R}_+^*, \mathbb{R}_-^*\Big\} = \Big\{\overline{1}, \overline{-1}\Big\}.$$

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

La table du groupe $\dfrac{\mathbb{R}^*}{\mathbb{R}_+^*}$ n'est rien d'autre que la traditionnelle règle des signes, mais 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. Le groupe $\dfrac{\mathbb{Z}}{2\mathbb{Z}}$ ayant la même table, l'application de $\dfrac{\mathbb{Z}}{2\mathbb{Z}} = \{0, 1\}$ dans $\dfrac{\mathbb{R}^*}{\mathbb{R}_+^*}$ qui envoie 0 sur $\overline{1}$ et 1 sur $\overline{-1}$ est un isomorphisme.

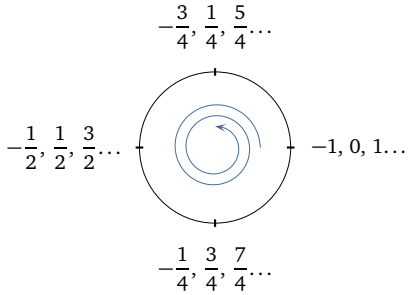
Exemple $\mathbb{U}$ est un sous-groupe distingué du groupe abélien $\mathbb{C}^*$ et $\dfrac{\mathbb{C}^*}{\mathbb{U}} = \Big\{z\mathbb{U} \mid \quad z \in \mathbb{C}^*\Big\} = \Big\{r\mathbb{U} \mid \quad r > 0\Big\}$, un peu comme si $\dfrac{\mathbb{C}^*}{\mathbb{U}}$ pouvait être assimilé à $\mathbb{R}_+^*$. Nous donnerons bientôt un sens plus 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 :

$$\frac{\mathbb{R}}{\mathbb{Z}} = \Big\{x + \mathbb{Z} \mid \quad x \in \mathbb{R}\Big\} = \Big\{x + \mathbb{Z} \mid \quad x \in [0, 1[\Big\},$$

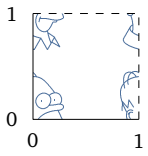
un peu comme si $\dfrac{\mathbb{R}}{\mathbb{Z}}$ pouvait être assimilé à $[0, 1[$. L'ensemble $[0, 1[$ gagne cela dit à être perçu comme un cercle plutôt que comme une intervalle. La congruence $1 \equiv 0\,[1]$ lui permet de se refermer sur lui-même en quelque sorte. Nous donnerons plus tard à cette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



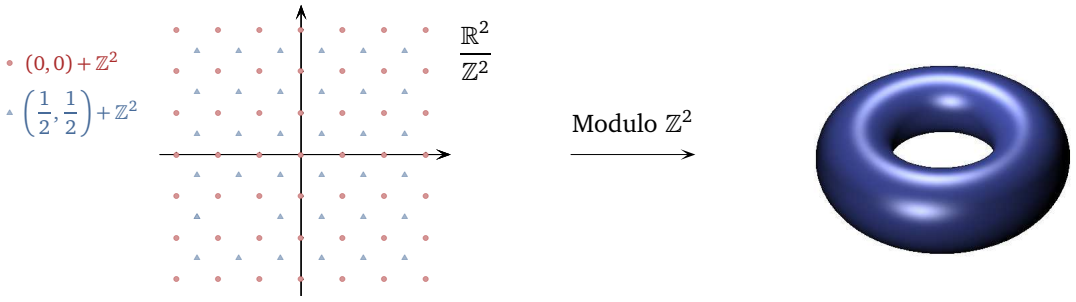
Exemple $\mathbb{Z}^2$ est un sous-groupe distingué du groupe abélien $\mathbb{R}^2$ et :

$$\frac{\mathbb{R}^2}{\mathbb{Z}^2} = \Big\{(x,y)+\mathbb{Z}^2 \mid \quad x,y\in\mathbb{R}\Big\} = \Big\{(x,y)+\mathbb{Z}^2 \mid \quad x,y\in[0,1[\Big\},$$

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 comme un tore plutôt 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 !



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



Théorème **(Sous-groupes d'indice 2)** Soient G un groupe et H un sous-groupe de G.
Si $\big|G:H\big| = 2$, H est distingué dans G et le groupe $\dfrac{G}{H}$ est isomorphe à $\dfrac{\mathbb{Z}}{2\mathbb{Z}}$.

Démonstration

- Montrons que H est distingué dans G. 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 $G = H\sqcup Hx$, or $x^{-1}hx\notin Hx$ — sans quoi x serait élément de H — donc $x^{-1}hx\in H$.
- Fixons maintenant $x\in G$. D'après le point précédent : $G = H\sqcup Hx$, donc $G = Gx = Hx\sqcup Hx^2$ car l'application $t\longmapsto tx$ est une permutation de G, donc $Hx^2 = G\setminus H = H$. Ainsi, si on note d'une barre les classes d'équivalence de G modulo H : $\dfrac{G}{H} = \{\overline{1},\overline{x}\}$ avec les relations : $\overline{1}^2=\overline{1}$, $\overline{1}\,\overline{x}=\overline{x}$, $\overline{x}\,\overline{1}=\overline{x}$ et $\overline{x}^2=\overline{1}$. Les groupes $\dfrac{\mathbb{Z}}{2\mathbb{Z}}$ et $\dfrac{G}{H}$ ont donc la même table, ils sont isomorphes.

Le théorème qui suit constitue en dépit de sa trivialité l'une des idées de base les plus importantes de l'algèbre.

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 $\operatorname{Ker} f$.

(i) Le sous-groupe $\operatorname{Ker} f$ est distingué dans G.

(ii) La relation $\equiv\ [\operatorname{Ker} f]$ est compatible avec f au sens où : $x\equiv x'\ [\operatorname{Ker} f] \implies f(x)=f(x')$ pour tous $x,x'\in E$. On définit donc une application $\overline{f}$ en posant $\overline{f}\big(\overline{x}\big)=f(x)$ pour tout $x\in E$.

Cette application $\overline{f}$ 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 $\big|G:\operatorname{Ker} f\big| = \big|\operatorname{Im} f\big|$.

Démonstration

(i) 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 $f\big(x^{-1}kx\big) = f(x)^{-1}f(k)f(x) = f(x)^{-1}f(x) = 1$.

(ii) Même preuve que celle du « vrai » théorème du rang !

Exemple Soit $n\in\mathbb{N}^*$. Le morphisme de groupes $k\longmapsto e^{\frac{2ik\pi}{n}}$ de $\mathbb{Z}$ dans $\mathbb{C}^*$ admet $\mathbb{U}_n$ pour image et $n\mathbb{Z}$ pour noyau. Il induit donc par quotient un isomorphisme de $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ sur $\mathbb{U}_n$. Cet isomorphisme ne devrait pas vous étonner car 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 $x \longmapsto \dfrac{x}{|x|}$ de $\mathbb{R}^*$ admet $\{\pm 1\}$ pour image et $\mathbb{R}_+^*$ pour noyau. Il induit donc par quotient un isomorphisme de $\dfrac{\mathbb{R}^*}{\mathbb{R}_+^*}$ sur $\{\pm 1\}$. De nouveau la fameuse règle des signes !

Exemple L'endomorphisme de groupe $z \longmapsto |z|$ de $\mathbb{C}^*$ admet $\mathbb{R}_+^*$ pour image et $\mathbb{U}$ pour noyau. Il induit donc 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 $x \longmapsto e^{2i\pi x}$ de $\mathbb{R}$ dans $\mathbb{C}^*$ admet $\mathbb{U}$ pour image et $\mathbb{Z}$ pour noyau. Il induit donc 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 à la manière d'un cercle, mais la notion d'isomorphisme fournit à cette circularité un sens plus rigoureux.

Exemple Soit $n \in \mathbb{N}^*$. La signature ε est un morphisme de groupes surjectif de S_n sur $\{\pm 1\}$. Son noyau est l'ensemble des permutations paires de S_n, noté A_n et appelé le *groupe alterné de degré n*. La signature induit donc 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 ? Plus grand-chose, seulement les valeurs possibles de la signature.

Exemple Soient $\mathbb{K}$ un corps et $n \in \mathbb{N}^*$. Le déterminant est un morphisme de groupes de $\mathrm{GL}_n(\mathbb{K})$ dans $\mathbb{K}^*$, surjectif car pour tout $\lambda \in \mathbb{K}^*$: $\det\big(\mathrm{diag}(\lambda, 1, \dots, 1)\big) = \lambda$. Son noyau est l'ensemble des matrices de déterminant 1 de $\mathscr{M}_n(\mathbb{K})$, noté $\mathrm{SL}_n(\mathbb{K})$ et appelé le *groupe spécial linéaire de degré n sur* $\mathbb{K}$. Le déterminant induit donc 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 ? Plus grand-chose, seulement les valeurs possibles du déterminant.

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

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 $\mathbb{U}_n = \langle e^{\frac{2i\pi}{n}} \rangle$.

Définition-théorème **(Ordre d'un élément et théorème de Lagrange)** Soient G un groupe et $x \in G$. L'ordre du groupe $\langle x \rangle$ est aussi appelé l'*ordre de x* et noté $|x|$.

(i) **Cas infini :** Si x est d'ordre infini, l'application $k \longmapsto x^k$ est un isomorphisme de $\mathbb{Z}$ sur $\langle x \rangle$.

(ii) **Cas fini :** On suppose x d'ordre fini. L'application $k \longmapsto x^k$ est alors un morphisme de groupes surjectif de $\mathbb{Z}$ sur $\langle x \rangle$ de noyau $|x|\mathbb{Z}$, donc induit par quotient un isomorphisme de $\dfrac{\mathbb{Z}}{|x|\mathbb{Z}}$ sur $\langle x \rangle$.
Concrètement : $\langle x \rangle = \{x^k \mid k \in [\![0, |x|-1]\!]\}$, et pour tout $k \in \mathbb{Z}$, $x^k = 1$ si et seulement si $|x|$ divise k.
Théorème de Lagrange : $|x|$ divise $|G|$, autrement dit $x^{|G|} = 1$.

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

Démonstration Dans tous les cas, l'application $k \xrightarrow{\rho} x^k$ est un morphisme de groupes surjectif de $\mathbb{Z}$ sur $\langle x \rangle$ de noyau $\mathrm{Ker}\,\rho = \{k \in \mathbb{Z} \mid x^k = 1\}$. En tant que sous-groupe de $\mathbb{Z}$: $\mathrm{Ker}\,\rho = n\mathbb{Z}$ pour un certain $n \in \mathbb{N}$, donc ρ induit par quotient un isomorphisme de $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ sur $\langle x \rangle$. Ainsi, si x est d'ordre infini, le groupe $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ est infini, donc $n = 0$, donc ρ est un isomorphisme.

Supposons désormais x d'ordre fini. Par isomorphisme : $n = \left|\dfrac{\mathbb{Z}}{n\mathbb{Z}}\right| = \big|\langle x\rangle\big| = |x|$. En retour, pour tout $k \in \mathbb{Z}$: $x^k = 1 \iff k \in \operatorname{Ker}\rho \iff k \in |x|\mathbb{Z} \iff |x| \text{ divise } k$ et le théorème de Lagrange n'est qu'un cas particulier de cette équivalence. Pour finir $\langle x\rangle \subset \left\{x^k \mid k \in [\![0, |x|-1]\!]\right\}$ 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 $r \in [\![0, |x|-1]\!]$: $x^k = \big(x^n\big)^q x^r = 1^q x^r = x^r$. ■

L'énoncé qui suit n'est qu'une reformulation du précédent. En résumé, $\mathbb{Z}$ et ses quotients sont à isomorphisme près les seuls groupes monogènes.

Théorème **(Classification des groupes monogènes à isomorphisme près)** Soit G un groupe monogène.

- Si G est infini, G est isomorphe à $\mathbb{Z}$.
- Si G est fini d'ordre n, G est isomorphe à $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$. On dit que G est *cyclique*.

Le théorème d'isomorphisme et la notion d'ordre d'un élément nous permettent à présent d'approfondir notre compréhension des anneaux $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$.

Définition-théorème **(Indicatrice 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 $x \wedge n = 1$: $x^{\varphi(n)} \equiv 1\ [n]$.

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

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

(iv) Pour tout $n \in \mathbb{N}^*$: $\varphi(n) = \displaystyle\prod_{p\in\mathbb{P}} p^{v_p(n)-1}(p-1)$.

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

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

Démonstration

(i) L'ensemble $\mathrm{U}\left(\dfrac{\mathbb{Z}}{n\mathbb{Z}}\right)$ des inversibles de l'anneau $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ est un groupe multiplicatif et nous avons vu que $\mathrm{U}\left(\dfrac{\mathbb{Z}}{n\mathbb{Z}}\right) = \left\{\overline{a} \mid a \in \mathbb{Z} \text{ et } a \wedge n = 1\right\}$, donc d'après le théorème de Lagrange : $\overline{a}^{\varphi(n)} = 1$ pour tout $a \in \mathbb{Z}$ premier avec n, autrement dit $a^{\varphi(n)} \equiv 1\ [n]$.

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

(iii) 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. Il est facile de vérifier que f est un morphisme de groupes additifs. Calculons son noyau. Pour tout $x \in \mathbb{Z}$:

$$x \in \operatorname{Ker} f \iff \overline{x} = \overline{0} \text{ et } \widehat{x} = \widehat{0} \underset{m\wedge n = 1}{\iff} x \text{ est divisible par } m \text{ et } n \iff x \text{ est divisible par } mn \iff x \in mn\mathbb{Z}.$$

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 le même cardinal fini, F est un isomorphisme. Pour tout $x \in \mathbb{Z}$, nous noterons $\widetilde{x}$ la classe de congruence de x modulo mn. À présent, pour tout $x \in \mathbb{Z}$:

$$\widetilde{x} \in \mathrm{U}\left(\frac{\mathbb{Z}}{mn\mathbb{Z}}\right) \iff x \wedge (mn) = 1 \iff x \wedge m = x \wedge n = 1 \iff F\big(\widetilde{x}\big) = \big(\overline{x}, \widehat{x}\big) \in \mathrm{U}\left(\frac{\mathbb{Z}}{m\mathbb{Z}}\right) \times \mathrm{U}\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right),$$

donc F est bijective de $\mathrm{U}\left(\dfrac{\mathbb{Z}}{mn\mathbb{Z}}\right)$ sur $\mathrm{U}\left(\dfrac{\mathbb{Z}}{m\mathbb{Z}}\right) \times \mathrm{U}\left(\dfrac{\mathbb{Z}}{n\mathbb{Z}}\right)$. Conclusion :

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

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

On étudie en détail dans les deux exemples qui suivent les sous-groupes distingués et les quotients du groupe symétrique S_3 et du *groupe des quaternions* Q_8.

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

- 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 : $\langle \mathrm{Id}\rangle = \{\mathrm{Id}\}$, $\big\langle (1\,2)\big\rangle = \{\mathrm{Id}, (1\,2)\}$, $\big\langle (1\,3)\big\rangle = \{\mathrm{Id}, (1\,3)\}$, $\big\langle (2\,3)\big\rangle = \{\mathrm{Id}, (2\,3)\}$ et $A_3 = \big\langle (1\,2\,3)\big\rangle = \{\mathrm{Id}, (1\,2\,3), (1\,3\,2)\}$. Tout sous-groupe strictement plus grand est alors déjà égal à S_3 pour une raison de cardinal.
- 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 : $(1\,3)^{-1}\big\langle (1\,2)\big\rangle (1\,3) = \big\langle (1\,3)^{-1}(1\,2)\,(1\,2)\big\rangle = \big\langle (2\,3)\big\rangle \neq \big\langle (1\,2)\big\rangle$.

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 quelques relations simples. Pour commencer : $\mathrm{i}^2 = \mathrm{j}^2 = \mathrm{k}^2 = -1$, donc i, j et k sont d'ordre 4 alors que -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 $\frac{Q_8}{\langle \mathrm{i}\rangle}$, $\frac{Q_8}{\langle \mathrm{j}\rangle}$ et $\frac{Q_8}{\langle \mathrm{k}\rangle}$ sont de simples copies de $\frac{\mathbb{Z}}{2\mathbb{Z}}$, mais qu'en est-il du quotient $\frac{Q_8}{\langle -1\rangle}$ d'ordre 4 ? En notant d'une barre les quotients par $\langle -1\rangle$: $\frac{Q_8}{\langle -1\rangle} = \big\{ \{\pm 1\}, \{\pm \mathrm{i}\}, \{\pm \mathrm{j}\}, \{\pm \mathrm{k}\} \big\} = \big\{\overline{1}, \overline{\mathrm{i}}, \overline{\mathrm{j}}, \overline{\mathrm{k}}\big\}$, 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 $\overline{\mathrm{k}}\;\overline{\mathrm{i}} = \overline{\mathrm{j}}$. Il se trouve que ces relations sont les mêmes que celles qui définissent le groupe produit $\frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}}$:
$$(1,0)^2 = (0,1)^2 = (1,1)^2 = (0,0), \qquad (1,0)+(0,1) = (1,1), \qquad (0,1)+(1,1) = (1,0) \qquad \text{et} \qquad (1,1)+(1,0) = (0,1).$$
Les tables qui suivent montrent ainsi que les groupes $\frac{Q_8}{\langle -1\rangle}$ et $\frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}}$ sont isomorphes.

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

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

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

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 $|x| = p$. Il en découle pour une raison de cardinal que $G = \langle x \rangle$. Comme voulu, G est cyclique d'ordre p, i.e. isomorphe à $\frac{\mathbb{Z}}{p\mathbb{Z}}$.

Exemple Peut-on déterminer de même les groupes d'ordre 4 à isomorphisme près ? Nous en connaissons déjà deux : $\frac{\mathbb{Z}}{4\mathbb{Z}}$ et $\frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}}$, 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 $\frac{\mathbb{Z}}{4\mathbb{Z}}$ contient des éléments d'ordre 4 alors que $\frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}}$ n'en contient pas.
Soit G un groupe d'ordre 4. Si G est cyclique, G est isomorphe à $\frac{\mathbb{Z}}{4\mathbb{Z}}$. 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. Bref, $x^2 = 1$ pour tout $x \in G$, donc pour tous $x, y \in G$: $x^2y^2 = 1 = (xy)^2$, donc $xy = yx$ après simplification. Conclusion : 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 $\frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}}$ que nous avons déjà détaillée plus haut. Conclusion : G est isomorphe à $\frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}}$.

$\times$	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. En particulier, pour tout $x \in G \setminus \{1\}$: $\langle x \rangle = G$, donc G est isomorphe à $\mathbb{Z}$ ou à $\frac{\mathbb{Z}}{|x|\mathbb{Z}}$, mais comme $\mathbb{Z}$ a plus que deux sous-groupes, G est fini isomorphe à $\frac{\mathbb{Z}}{|x|\mathbb{Z}}$. Retenons-en que tout élément de $G \setminus \{1\}$ est d'ordre $|G|$.

Or fixons justement x dans $G \setminus \{1\}$ et notons p un diviseur premier de $|x|$. L'égalité $\left(x^p\right)^{\frac{|x|}{p}} = x^{|x|} = 1$ montre que x^p est d'ordre un diviseur strict de $\dfrac{|x|}{p}$ donc de $|G|$. Ainsi $x^p = 1$, donc $|x| = p$.

La classification des groupes simples abéliens est donc facile à obtenir, 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 $i \in [\![0, n-1]\!]$,

— $\dfrac{H_{i+1}}{H_i}$ 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 $\left(H'_0, \dots, H'_{n'}\right)$ 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 $\dfrac{H_{i+1}}{H_i}$ et $\dfrac{H'_{\sigma(i)+1}}{H'_{\sigma(i)}}$ 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 $\dfrac{G}{H}$, mais on ne connaît pas G entièrement. La manière dont $\dfrac{G}{H}$ 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 $\dfrac{\mathbb{Z}}{p\mathbb{Z}}$ 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. Tout groupe fini d'ordre impair est donc un empilement de groupes $\dfrac{\mathbb{Z}}{p\mathbb{Z}}$ avec $p \in \mathbb{P}$. En théorie des groupes, le nombre premier 2 est toujours un peu à part.