Espaces quotients

Philosophie du document : Plutôt que d'énoncer directement la définition d'un espace quotient puis d'en étudier les applications, ce document propose de suivre le chemin des écoliers : nous partirons à chaque fois du cas particulier pour approcher le cas général de façon la plus intuitive possible.

Le lecteur pressé d'obtenir des définitions claires et définitives peut donc fermer ce document et en chercher un autre plus succinct.

Notre idée est de partir de considérations concrètes : construire des bijections.
Cet objectif conduit très naturellement aux espaces quotients et nous proposerons alors quelques mises en oeuvre classiques en algèbre pour voir la puissance de cet outil, et ouvrir les perspectives.

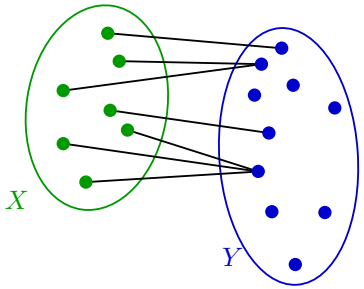
Public visé : étudiant de MPSI ou de MP.

Prérequis : définition d'une application, injectivité, surjectivité, bijectivité. Notion de relation d'équivalence et des classes d'équivalence.
Certaines parties demandent d'autres connaissances listées au début de celles-ci.

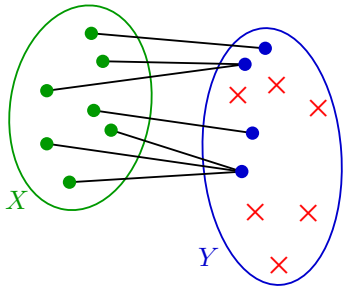
1 Fabriquer des bijections

Dans cette partie, nous voulons transformer une application quelconque en une bijection.
On s'intéresse donc à une application f entre deux ensembles X et Y.

$$f : X \to Y.$$

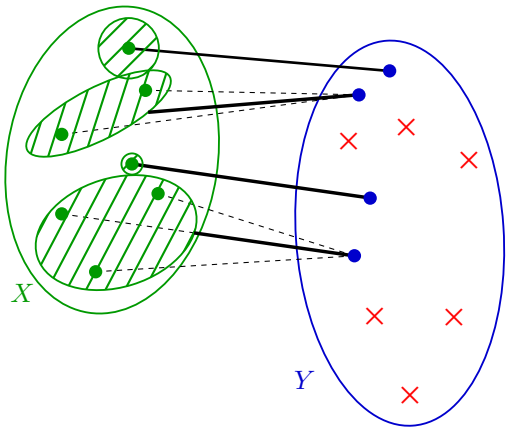


On veut la rendre bijective :

1. *Surjectivité*
   Rendre cette application surjective est très facile : il suffit de ne considérer que les élements qui ont un antécédent, c'est-à-dire de corestreindre à $\mathrm{Im}\,(f) \subset Y$.
   On remplace f par
   $$f : X \to \mathrm{Im}\,(f).$$
   

2. *Injectivité*
   Pour rendre l'application injective, on pourrait restreindre l'ensemble de départ, de sorte à ne choisir qu'un seul antécédent lorsqu'il y en a plusieurs.
   Mais cela nécessiterait d'être capable de choisir à chaque fois un antécédent particulier que l'on conserverait, et d'écarter tous les autres. Outre la difficulté de choisir un tel objet, cette méthode repose sur un choix arbitraire et ne donne donc pas de solution unique. Deux personnes différentes construiraient alors des applications injectives différentes.

   On dispose d'une autre idée très proche, mais plus facile à mettre en oeuvre : on « fusionne » tous les antécédents d'un même y en un seul objet.



Formellement, cela revient à créer une relation d'équivalence : deux objets sont équivalents s'ils ont la même image.

$$\forall (x, x') \in X^2,\ x \sim x' \iff f(x) = f(x').$$

On vérifie sans difficulté qu'il s'agit d'une relation d'équivalence, et on remplace donc chaque élément x par sa classe d'équivalence modulo $\sim$.
Ainsi, deux éléments qui ont la même image sont fusionnés : le nouvel objet issu de cette fusion est leur classe d'équivalence.

L'ensemble des classes d'équivalence est appelé **espace quotient** et noté $X/\sim$.

On construit donc la nouvelle application

$$\widetilde{f} : \left\{ \begin{array}{ccc} X/\sim & \to & \mathrm{Im}\,(f) \\ \dot{x} & \mapsto & f(x). \end{array} \right.$$

Cette application est injective par construction.

Assurance contre les casse-pieds : on vérifie que si x et x' sont dans la même classe, ils donnent bien la même valeur $f(x) = f(x')$. Ceci justifie que la fonction $\widetilde{f}$ est bien définie.

Définition 1.1 *(Espace quotient)*

Soit X un ensemble, et $\sim$ une relation d'équivalence sur X.
L'**espace quotient** $X/\sim$ est défini comme l'ensemble des classes d'équivalence de X modulo $\sim$.
Il forme une partition de X.

Voir sur ce site le cours sur les nombres réels où sont introduites les relations binaires.

Propriété 1.2 *(Diagramme commutatif)*

Toute application $f : X \to Y$ peut être *factorisée* à l'aide du diagramme commutatif suivant :

$$\begin{array}{ccc} X & \xrightarrow{f} & Y \\ {\scriptstyle s}\downarrow & & \uparrow{\scriptstyle i} \\ X/\sim & \xrightarrow{\widetilde{f}} & \mathrm{Im}\,(f) \end{array}$$

Explications

- L'application $s : X \to X/\sim$ est une surjection qui envoie chaque $x \in X$ sur sa classe $\dot{x} \in X/\sim$.
- L'application $i : \mathrm{Im}\,(f) \to Y$ est une injection qui envoie chaque $y \in \mathrm{Im}\,(f)$ sur lui-même.
- L'application f est celle de départ, et l'application $\widetilde{f}$ est l'application bijective obtenue.

Le diagramme est dit *commutatif* car les deux « chemins » donnent le même résultat :

$$f = i \circ \widetilde{f} \circ s.$$

2 Application aux morphismes de groupes

Prérequis : définition d'un groupe, d'un morphisme de groupe, sous groupes de $\mathbf{Z}$.
Les sous parties se suivent et sont à lire dans l'ordre.

A Ordre d'un groupe

Définition du morphisme. Pour prouver qu'un élément x d'un groupe fini G admet un ordre fini, on s'intéresse aux puissances de x, ce qui revient à étudier le morphisme :

$$f : \left\{ \begin{array}{ccc} \mathbf{Z} & \to & G \\ k & \mapsto & x^k. \end{array} \right.$$

Pour construire ce morphisme de groupes, on part évidemment de $\mathbf{Z}$ (et non de $\mathbf{N}$ qui n'est pas un groupe).
Il est clair que f est un morphisme de groupes[1] :

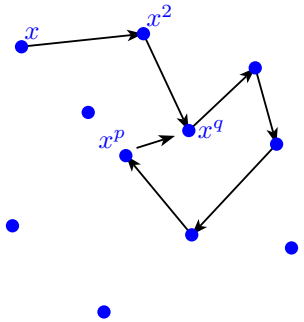
$$\forall (p,\, q) \in \mathbf{Z}^2,\ f\,(p+q) = f(p) f(q).$$

⚠ Le groupe $\mathbf{Z}$ est un groupe additif alors que G a été noté multiplicativement.

Non injectivité du morphisme. On remarque que $\mathbf{Z}$ est un ensemble infini, alors que G est fini. L'application f n'est donc pas injective et il existe deux puissances différentes $p < q$ telles que $x^p = x^q$.

> En effet, si par l'absurde f est injective alors deux éléments différents de $\mathbf{Z}$ ont des images différentes dans G, ce qui implique que G contient « plus d'éléments[2] » que $\mathbf{Z}$, et il en a donc une infinité, ce qui est contradictoire avec l'hypothèse.

Si on trace un circuit qui relie les puissances successives de x, alors la non injectivité indique l'existence d'une boucle.



Factorisation du morphisme. Deux puissances qui donnent le même élément sur la boucle peuvent être assimilées, ce qui revient à considérer la relation d'équivalence :

$$\forall (p,\, q) \in \mathbf{Z}^2,\ p \sim q \iff x^p = x^q.$$

C'est la même relation d'équivalence qu'à la partie précédente :

$$\forall (p,\, q) \in \mathbf{Z}^2,\ p \sim q \iff f(p) = f(q).$$

Mais ici, on peut aller plus loin :

$$\begin{aligned} \forall (p,\, q) \in \mathbf{Z}^2,\ p \sim q &\iff f(p) = f(q) \\ &\iff f(p)\,(f(q))^{-1} = e \\ &\iff f(p-q) = e \\ &\iff p - q \in \ker(f). \end{aligned}$$

Cas du morphisme de groupes

Pour un morphisme de groupes, toutes les classes d'équivalence sont sur le même modèle : ce sont les translatées de $\ker(f)$ par une constante.

$$\dot{p} = p + \ker(f).$$

On factorise donc l'application avec le diagramme commutatif :

$$\begin{array}{ccc} \mathbf{Z} & \xrightarrow{\ f\ } & G \\ {\scriptstyle s}\downarrow & & \uparrow{\scriptstyle i} \\ \mathbf{Z}/\ker(f) & \xrightarrow[\tilde{f}]{} & \mathrm{Im}\,(f) =< x > \end{array}$$

Étude du groupe quotient. Montrons $\mathbf{Z}/\ker(f)$ est bien un groupe.
Pour cela on définit l'opération $+$ par

$$\forall (\dot{p},\, \dot{q}) \in \left(\mathbf{Z}/\ker(f)\right)^2,\ \dot{p} + \dot{q} = \dot{\overbrace{p+q}}.$$

Comme lors de « l'assurance contre les casse-pieds » à la page 2, le plus important est de vérifier que la relation d'équivalence est *compatible* avec l'addition. En effet, si on choisit q' dans la classe de q et p' dans la classe de p alors

$$f(p+q) = f(p)f(q) = f(p')f(q') = f(p'+q').$$

Ainsi $p'+q' \sim p+q$ ce qui justifie que $\dot{\overbrace{p'+q'}} = \dot{\overbrace{p+q}}$ et que le résultat ne dépend pas des représentants choisis.
L'élément neutre est la classe d'équivalence de 0 et les autres axiomes de groupe s'obtiennent sans problème.
La preuve complète est donnée pour le cas général à la page 6 dans la section 4.

Finalement, l'étude de $\mathrm{Im}\,(f) =< x >$, se ramène, via l'isomorphisme, à l'étude du groupe $\mathbf{Z}/\ker(f)$.

1. On retrouve l'équation fonctionnelle des fonctions puissances. En particulier l'exponentielle est elle-même un morphisme de $(\mathbf{R},\, +)$ dans $\left(\mathbf{R}_+^*,\, \times\right)$.
2. Voir le cours sur le dénombrement, pour avoir les notions plus précises.

À quoi ressemble $\mathbf{Z}/\ker(f)$?

$\ker(f)$ est un sous-groupe de $\mathbf{Z}$, et on sait (ou on saura) que tous les sous-groupes de $\mathbf{Z}$ sont de la forme $n\mathbf{Z}$ pour $n \in \mathbf{N}$.
On obtient donc qu'il existe $n \in \mathbf{N}$ tel que

$$\forall (p,\, q) \in \mathbf{Z}^2,\ p \sim q \iff p - q \in n\mathbf{Z} \iff p \equiv q\ [n].$$

La relation d'équivalence est donc la congruence.

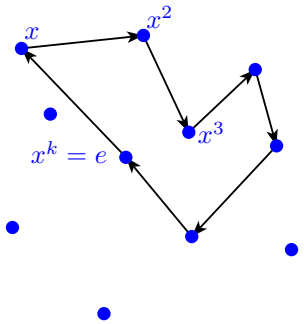
Ici $\ker(f) = n\mathbf{Z}$ désigne la classe d'équivalence de 0, c'est-à-dire tous les entiers k tels que $x^k = x^0 = \mathrm{e}$.

Définition 2.1 *(Ordre d'un élément)*

n est le plus petit entier positif non nul[3] de $\ker(f)$, c'est-à-dire le plus petit entier positif qui est solution de $x^n = \mathrm{e}$.

n est **l'ordre** de x.

Il représente la « taille » de la boucle dont on sait à présent qu'elle a cette forme :



On obtient de surcroît que pour tout élément x d'un groupe fini G, le groupe engendré $< x >$ est isomorphe à $\mathbf{Z}/n\mathbf{Z}$ pour un certain $n \in \mathbf{N}^*$.

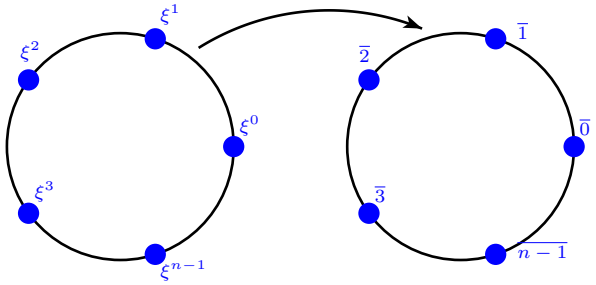
Réminiscences & analogies : La factorisation du morphisme a fait apparaître une boucle dans G.

Or, la boucle $\mathrm{Im}\,(f) =< x >$ et $\mathbf{Z}/\ker(f)$ sont isomorphes et ils ont donc la même « forme ». Ainsi, la factorisation du morphisme a enroulé $\mathbf{Z}$ sur lui-même.

On se souvient que lors de l'étude sur les racines n-ièmes de l'unité dans le cours sur les complexes, nous avions exactement le même phénomène qui nous avait aussi conduit à la congruence modulo n sur $\mathbf{Z}$:

$$\forall \xi \in \mathbf{U}_n,\ \xi^p = \xi^q \iff p \equiv q\ [n].$$

3. Il est évident que $\ker(f)$ ne peut être réduit à 0 car f n'est pas injective.



Sans le dire, nous avions factorisé le morphisme : $\left\{ \begin{array}{ccc} \mathbf{Z} & \to & \mathbf{U}_n \\ k & \mapsto & \xi^k. \end{array} \right.$

Ici, on remplace les puissances de ξ par les puissances de x : c'est exactement pareil.

B Caractérisation des groupes monogènes

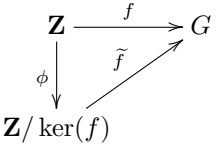
Ce qui a été fait avec l'ordre d'un élément (c'est-à-dire avec le groupe qu'il engendre), se généralise facilement à tous les groupes monogènes (groupes engendrés par un seul élément).

On considère donc $(G, \star)$ un groupe monogène.
On note $x \in G$, un générateur de G.
On pose

$$f : \left\{ \begin{array}{ccc} \mathbf{Z} & \to & G \\ x & \mapsto & x^k. \end{array} \right.$$

Par hypothèse sur x, f est déjà surjective.

On factorise le morphisme :



$\ker(f)$ est un sous-groupe de $\mathbf{Z}$, donc il existe $n \in \mathbf{N}$ tel que $\ker(f) = n\mathbf{Z}$.

- Si $n = 0$, alors $\ker(f) = \{0\}$: le morphisme est injectif et les classes d'équivalence ne contiennent chacune qu'un seul élément.
  On peut alors identifier $\mathbf{Z}$ et $\mathbf{Z}/\ker(\mathbf{Z})$: G est isomorphe à $\mathbf{Z}$ (et donc infini).
- Si $n \geqslant 1$, alors G est isomorphe à $\mathbf{Z}/n\mathbf{Z}$ et contient exactement n éléments distincts qui sont
  $$G = \left\{ \mathrm{e},\, x,\, x^2,\, \cdots,\, x^{n-1} \right\}.$$
  G est donc un groupe monogène fini : il est cyclique[4].
  Si on préfère, on peut aussi dire que G est isomorphe à $\mathbf{U}_n$.

4. On voit bien avec les représentations précédentes qu'il réalise une boucle.

Théorème 2.2

- Tout groupe monogène infini est isomorphe à $\mathbf{Z}$.
- Tout groupe monogène fini est isomorphe à $\mathbf{Z}/n\mathbf{Z}$ où $n = \#G$.

Remarque : On reparlera des groupes $\mathbf{Z}/n\mathbf{Z}$ un peu plus loin à la page 10 : ils constituent l'exemple (voire le modèle) le plus naturel pour les quotients de groupes.

Le théorème amène un corollaire très remarquable :

Corollaire 2.3

Tout groupe monogène est commutatif.

3 Application aux actions de groupes

Prérequis : définition d'une action de groupe.

On considère une action de groupe de G sur E.
Pour $x \in E$ fixé, on étudie l'application orbitale

$$f : \left\{ \begin{array}{ccc} G & \to & \mathscr{O}_x \\ g & \mapsto & g \cdot x. \end{array} \right.$$

Par définition de l'orbite $\mathscr{O}_x$, f est surjective.
Pour factoriser, il suffit donc de quotienter par la relation d'équivalence :

$$\forall (g,\, g') \in G^2, \quad g \sim g' \iff g \cdot x = g' \cdot x.$$

Comme il s'agit d'une action de groupe, on peut faire agir g^{-1} :

$$\forall (g,\, g') \in G^2, \quad g \sim g' \iff x = (g^{-1}g') \cdot x.$$

On retrouve la définition du stabilisateur de x, il joue le rôle qui était dévolu au noyau pour les morphismes de groupes.

$$\forall (g,\, g') \in G^2, \quad g \sim g' \iff g^{-1}g' \in \mathrm{Stab}(x) \iff g' \in g\,\mathrm{Stab}(x).$$

La classe d'équivalence de g s'écrit $g\,\mathrm{Stab}(x)$.

On suppose à présent que G est un groupe fini, donc $\mathrm{Stab}(x)$ est lui-même un ensemble fini (partie de G).
Toutes les classes d'équivalence ont le même nombre d'éléments qui est $\#\mathrm{Stab}(x)$.
Le nombre de classes d'équivalence est donc $\frac{\#G}{\#\mathrm{Stab}(x)}$.
La bijection entre deux ensembles donne que $\mathscr{O}_x$ est lui-même fini et de cardinal

$$\#\mathscr{O}_x = \frac{\#G}{\#\mathrm{Stab}(x)}.$$

On peut donc écrire la formule des classes :

Théorème 3.1 *(Formule des classes)*

Soit $(G, \star)$ un groupe *fini* qui agit sur un ensemble E.

$$\forall x \in E,\ (\#\mathscr{O}_x) \times (\#\mathrm{Stab}(x)) = \#G.$$

Remarque : Les orbites forment une partition de E, alors que les stabilisateurs sont des parties du groupe G on parle donc d'objets de natures totalement différentes.

4 Quotient de groupes

Prérequis : groupes et morphismes de groupes.
Cette partie reprend et généralise ce qui a été fait page 3 pour l'ordre d'un élément dans un groupe fini. Il est donc conseillé de d'avoir lu avant.

A Quotient par le noyau d'un morphisme

Loi additive : Pour tout morphisme de groupes : $f : G \to G'$, l'injectivité s'obtient en quotientant par le noyau.
En effet, si on note G additivement, la relation d'équivalence s'écrit :

$$\forall (x,\, x') \in G^2, \quad f(x) = f(x') \iff x - x' \in \ker(f).$$

Ainsi, on obtient toujours un diagramme du type :

$$\begin{array}{ccc} G & \xrightarrow{\quad f \quad} & G' \\ {\scriptstyle s}\downarrow & & \uparrow{\scriptstyle i} \\ G/\ker(f) & \xrightarrow[\widetilde{f}]{} & \mathrm{Im}\,(f) \end{array}$$

La structure de groupe de G se transmet naturellement à $G/\ker(f)$.

Preuve

On rappelle que $G/\ker(f)$ représente l'ensemble des classes d'équivalence « modulo $\ker(f)$. »
Ainsi, la classe d'équivalence de x est $x + \ker(f) = \{x + u,\, u \in \ker(f)\}$ si on note G additivement.
Pour s'en rappeler, il faut garder l'idée de $\mathbf{Z}/n\mathbf{Z}$ où la classe de x est l'ensemble des entiers qui sont congrus à x modulo n, c'est-à-dire

$$\dot{x} = \{k \in \mathbf{N},\, k \equiv x\ [n]\} = \{k \in \mathbf{N},\, k - x \in n\mathbf{Z}\} = x + n\mathbf{Z}.$$

Dans le cas présent, Pour obtenir une structure de groupe, on définit l'opération interne $+$ sur $G/\ker(f)$ par

$$\forall (x,\, y) \in G^2,\, \overline{x} + \overline{y} = \overline{x+y}.$$

- On vérifie que cette définition est valide, c'est-à-dire que $\overline{x+y}$ ne dépend pas du représentant choisi dans la classe de x, ni dans celle de y.
  Si $x' \in \overline{x} = x + \ker(f)$ et $y' \in \overline{y} = y + \ker(f)$, alors $(x'+y') - (x+y) = x' - x + y' - y$.
  Or $x' - x \in \ker(f)$ et $y' - y \in \ker(f)$.
  On sait de plus que $\ker(f)$ est un sous-groupe de G, donc il est stable par somme.
  Ainsi $(x'+y') - (x+y) \in \ker(f)$, c'est-à-dire $x'+y' \in (x+y) + \ker(f) = \overline{x+y}$.
  On vient donc de montrer que

  $$\overline{x'+y'} = \overline{x+y}.$$

  Ceci justifie que l'opération $+$ est bien définie sur $G/\ker(f)$.
- Reste à prouver que l'on obtient un groupe :
  - $+$ est internet et associative,
  - $\ker(f)$ est l'élément neutre de $G/\ker(f)$.
  - si $\overline{x} \in G/\ker(f)$, alors $\overline{-x}$ est son opposé.
    En effet $\overline{x} + \overline{-x} = \overline{0} = \ker(f)$.

  On a donc bien prouvé que $G/\ker(f)$ est un groupe. ■

Loi multiplicative : prenons à présent une loi multiplicative, pour laquelle on ne suppose pas la commutativité.
On reprend alors les raisonnements précédents que l'on adapte à cette situation.
La relation d'équivalence est donnée par

$$\begin{aligned} \forall (x,\, x') \in G^2, \quad x \sim x' &\iff f(x) = f(x') \\ &\iff 1 = f(x^{-1}x') \\ &\iff x^{-1}x' \in \ker(f) \\ &\iff x' \in x\ker(f). \end{aligned}$$

La classe d'équivalence de x s'écrit donc

$$x\ker(f) = \{xu,\, u \in \ker(f)\}.$$

On définit l'opération interne $\times$ sur $G/\ker(f)$ par

$$\forall (x,\, y) \in G^2,\, \overline{x} \times \overline{y} = \overline{xy}.$$

On vérifie que cette définition ne dépend pas des représentants choisis.
Si $x' \in \overline{x} = x\ker(f)$ et $y' \in \overline{y} = y\ker(f)$,
Il existe $a,\, b \in \ker(f)$ tels que $x' = xa$ et $y' = yb$.
Vérifions que $(xy)^{-1}(x'y') \in \ker(f)$.
Or

$$(xy)^{-1}(x'y') = y^{-1}x^{-1}xayb = y^{-1}ayb.$$

Ici, on se heurte au problème de commutativité : il n'y a acune raison que a et y commutent.
Mais le fait de travailler avec le noyau va nous sauver :

$$\begin{aligned} f(y^{-1}ayb) = f(y^{-1})f(a)f(y)f(b) &= f(y^{-1}) \times 1 \times f(y) \times 1 \\ &= f(y^{-1}) \times f(y) \\ &= f(y^{-1}y) \\ &= f(1) = 1. \end{aligned}$$

Donc $(xy)^{-1}(x'y') = y^{-1}ayb \in \ker(f)$ ce qui nous assure que $x'y' \in \overline{xy}$ et donc que l'opération $\times$ est bien définie sur $G/\ker(f)$.

La vérification des axiomes de groupe est ensuite évidente.

B Le groupe distingué fait son entrée

Les morphismes nous ont conduits aux quotient par $\ker(f)$, mais on peut imaginer quotienter par un autre ensemble H.

Voyons ce que ça donne. On définit une nouvelle relation $\mathscr{R}$ par

$$\forall (x,\, y) \in G^2,\ x\mathscr{R}y \iff x^{-1}y \in H.$$

Est-ce une relation d'équivalence ?

- *Réflexivité :*
  Soit $x \in G$, $x\mathscr{R}x \iff x^{-1}x \in H \iff 1 \in H$.
  On voit donc qu'il est nécessaire que H contienne l'élément neutre.

- *Symétrie :*
  Soit $(x,\, y) \in G^2$, on suppose que $x\mathscr{R}y$ c'est-à-dire que $x^{-1}y \in H$.
  On voit alors que $y\mathscr{R}x \iff y^{-1}x \in H$.
  Or $y^{-1}x = \left(x^{-1}y\right)^{-1}$.
  Donc, il est nécessaire que si $x^{-1}y \in H$, alors son inverse $\left(x^{-1}y\right)^{-1} \in H$.
  Lorsque H est stable par passage à l'inverse, cette relation est vérifiée.
  Montrons que c'est même nécessaire.
  En effet, si $x \in H$, alors $1^{-1}x \in H$, donc $1\mathscr{R}x$ et par symétrie, $x\mathscr{R}1$.
  On a donc $x^{-1} \in H$.
  Il est donc nécessaire est suffisant que H soit stable par passage à l'inverse pour avoir la symétrie.

- *Transitivité :*
  Soit $(x,\, y,\, z) \in G^3$, on suppose que $x\mathscr{R}y$ et $y\mathscr{R}z$ c'est-à-dire que $x^{-1}y \in H$ et $y^{-1}z \in H$.
  $x\mathscr{R}z \iff x^{-1}z \in H \iff (x^{-1}y)(y^{-1}z) \in H$.
  Lorsque H est stable par produit, alors cette relation est satisfaite.
  Montrons alors que cette condition est même nécessaire.
  Si $(x,\, y) \in H^2$, alors $x \times 1 \in H$ et $1 \times y \in H$.
  Donc $x^{-1}\mathscr{R}1$ et $1\mathscr{R}y$, et par transitivité $x^{-1}\mathscr{R}y$, donc $xy \in H$.

On vient donc de démontrer que :

> $\mathscr{R}$ est une relation d'équivalence si, et seulement si H est un sous groupe de G.
> On ne peut pas quotienter par autre chose que par un groupe.

On souhaite à présent que le quotient G/H puisse hériter de la structure de groupe de G comme avec le noyau.
Pour cela, on vérifie que l'opération suivante a un sens :

$$\forall (x,\, y) \in H^2,\ \overline{x} \times \overline{y} = \overline{xy}.$$

On reprend les calculs réalisés pour le noyau.
Soit $x' \in \overline{x} = xH$ et $y' \in \overline{y} = yH$,
Donc il existe $a,\, b \in H$ tels que $x' = xa$ et $y' = yb$.

$$\begin{aligned}
\overline{xy} = \overline{x'y'} &\iff x'y' \in \overline{xy} \\
&\iff (xy)^{-1}(x'y') \in H \\
&\iff y^{-1}x^{-1}xayb \in H \\
&\iff y^{-1}ayb \in H \\
&\iff y^{-1}ay \in H \qquad \text{car } b \in H.
\end{aligned}$$

Ainsi, on voit qu'il est nécessaire et suffisant que

$$\forall y \in G,\ \forall a \in H,\ y^{-1}ay \in H.$$

Quitte à prendre $g = y^{-1}$ quelconque dans G, on reconnaît ici l' automorphisme (de conjugaison) intérieur

$$\forall g \in G,\ f_g : \left\{ \begin{array}{ccc} G & \to & G \\ x & \mapsto & gxg^{-1}. \end{array} \right.$$

H doit donc être stable par les automorphismes intérieurs.
Dans ce cas, les axiomes du groupe se vérifient sans difficulté pour G/H.

On a donné un nom aux sous-groupes qui permettent le quotient : les **sous-groupes distingués.**

Définition 4.1 *(Sous-groupe distingué)*

Soient $(G,\, \times)$ un groupe et H un sous-groupe de G.
H est un **sous-groupe distingué** si, et seulement si

$$\forall g \in G,\ gHg^{-1} \subset H.$$

C'est-à-dire

$$\forall g \in G,\ \forall h \in H,\ ghg^{-1} \in H.$$

Si H est un sous-groupe distingué de G, on note $K \triangleleft G$.

Le sous-groupe distingué est aussi appelé **sous-groupe normal.**

Propriété 4.2

Soit G un groupe et H un sous-groupe de G.
H est un sous-groupe distingué de G si, et seulement s'il est stable par tout automorphisme intérieur de G.

Exemple

Si $f : G \to H$ est un morphisme de groupes, alors $\ker(f) \triangleleft G$.

Théorème 4.3

Soit (G, x) un groupe, et H un sous-groupe distingué de G.
On munit G/H de la loi $\times$ définie par

$$\forall(\overline{x}, \overline{y}) \in (G/H)^2, \ \overline{x} \times \overline{y} = \overline{xy}.$$

Cette opération est bien définie ; et muni de cette loi, G/H est un groupe.

Ainsi, dans un groupe commutatif, tout sous-groupe est distingué.
La notion n'a d'intérêt que si le groupe **n'est pas commutatif.**
Elle supplée au défaut de commutativité.

5 Construction de corps

A Construction des rationnels

La construction des rationnels est très simple :

$$\mathbf{Q} = \left\{ \frac{p}{q}, \ (p, q) \in \mathbf{Z} \times \mathbf{N}^* \right\}.$$

On remarque que l'on peut toujours choisir le dénominateur positif et faire porter le signe de la fraction au numérateur.
Intervient ici une difficulté assez subtile :

$$\text{On ne } \textit{sait pas ce que veut dire } \frac{p}{q}.$$

En effet, si on connaissait déjà ce que sont les nombres réels, alors, de facto, on connaîtrait les rationnels. Il ne s'agirait donc pas tant de les *construire*, que de les identifier parmi les nombres réels.
Ici le problème est autre : on connaît les nombres entiers naturels (Péano, Von Neumann par exemple) et les relatifs par symétrisation. Mais rien d'autre.
Ainsi, dès que q ne divise par p, la fraction $\frac{p}{q}$ n'a aucune signification pour nous.

Pour obtenir une définition qui nous convienne, revenons alors à l'idée initiale des fractions.

$$\text{Que désigne la fraction } \frac{1}{2} \ ?$$

Il s'agit simplement de couper une totalité en deux parties identiques. Ainsi, le rassemblement des deux parties redonne la totalité :

$$\frac{1}{2} \text{ est donc l'unique solution } x \text{ de } 2x = 1.$$

Comme une telle solution ne peut pas être un nombre entier, il convient de définir un nouvel ensemble de nombres qui corresponde à toutes les solutions du type

$$qx = p, \ \text{ pour } (p, q) \in \mathbf{Z} \times \mathbf{N}^*.$$

Une fraction $\frac{p}{q}$ serait donc naturellement codée par le couple $(p, q) \in \mathbf{Z} \times \mathbf{N}^*$.
Mais voici le problème d'unicité qui intervient.
En effet, on voit bien qu'il existe plusieurs fractions équivalentes. Ce que vous écriviez sous la forme $\frac{1}{2} = \frac{2}{4} = \frac{3}{6} \cdots$ peut aussi se dire

$$2x = 1 \iff 4x = 2 \iff 6x = 3 \cdots$$

Il faut donc trouver un moyen de s'assurer que ces différents couples $(1, 2)$ et $(2, 4)$,... soient associés au même nombre.
Pour cela on définit la relation d'équivalence pour identifier les couples qui donnent les mêmes solutions.
Ces couples équivalents sont exactement les couples proportionnels :
$\forall\big((p, q), (p', q')\big) \in (\mathbf{Z} \times \mathbf{N}^*)^2$,

$$(p, q) \mathscr{R} (p', q') \iff \exists a \in \mathbf{Z}^*, \ (p', q') = a(q, q) \text{ ou } (p, q) = a(p', q').$$

Remarque : il faut bien écrire les deux formes car pour $a \notin \{-1, 1\}$, on se sait pas diviser par a.
Cette relation d'équivalence est plus simple à rédiger en utilisant le produit en croix :

$$\forall (p, q), (p', q') \in (\mathbf{Z} \times \mathbf{N}^*)^2, (p, q) \mathscr{R} (p', q') \iff pq' = p'q.$$

On obtient alors une définition qui ne fait intervenir que des objets que l'on connaît. L'ensemble des rationnels est donc défini comme l'espace quotient

$$\mathbf{Q} = (\mathbf{Z} \times \mathbf{N}^*) / \mathscr{R}.$$

Reste ensuite à bien définir les sommes, produits et quotients sur ce nouvel ensemble, à partir des sommes et produits définis sur $\mathbf{Z}$. Ce travail est sans difficulté et n'est pas mené ici pour ne pas distraire le lecteur de l'essentiel.

Remarque : la construction de $\mathbf{R}$ à partir de $\mathbf{Q}$ relève de considérations radicalement différentes.

B Construction de C

Prérequis : nombres complexes, polynômes. Si possibles les idéaux d'un anneau commutatif.
Le corps des nombres complexes est traditionnellement défini à partir de l'écriture algébrique :

$$\mathbf{C} = \left\{ a + ib, (a, b) \in \mathbf{R}^2 \right\}.$$

Mais comme i n'a aucune existence a priori, il convient plutôt de définir $\mathbf{C}$ comme $\mathbf{R}^2$ muni de lois bien choisies. Le couple (a, b) étant ensuite plus commodément noté $a + ib$.
Pour plus de détails, voir le cours sur les nombres complexes.

Cette construction est tout à fait valable, mais n'est qu'un artifice pour créer ce nombre *imaginaire* i qui doit être solution de $i^2 = -1$.

On peut donc prendre le problème à rebours et partir du polynôme $X^2 + 1$ et chercher à l'annuler (ce qui revient à lui donner – au moins – une racine).
Une solution assez radicale est de ramener ce polynôme à 0 : dire qu'il est nul.

On revient alors à la même idée que la construction de $\mathbf{Z}/n\mathbf{Z}$ avec les congruences dont l'idée était de « ramener » n à 0.
Pour cela, on avait construit la relation d'équivalence :

$$\forall (p, q) \in \mathbf{Z}^2, p \mathscr{R} q \iff (p - q) \in n\mathbf{Z}.$$

On avait ensuite quotienté $\mathbf{Z}$ par cette relation d'équivalence pour obtenir $\mathbf{Z}/n\mathbf{Z}$.
Ici, on fait pareil, et on définit la relation d'équivalence :

$$\forall (P, Q) \in (\mathbf{R}[X])^2, P \mathscr{R} Q \iff P - Q \in (X^2 + 1)\mathbf{R}[X]$$

où $(X^2+1)\mathbf{R}[X]$ désigne l'ensemble des multiples de X^2+1 dans $\mathbf{R}[X]$, et noté plus succinctement $(X^2 + 1)$ avec les parenthèses.

$$(X^2 + 1) = \left\{ (X^2 + 1)P, P \in \mathbf{R}[X] \right\}.$$

On reconnaît l'idéal engendré par $X^2 + 1$.
On note alors $K = \mathbf{R}[X]/(X^2 + 1)$ l'espace quotient.

Voyons en résumé ce qu'on peut en obtenir (et les notions que cela amènerait à étudier) :

- Comme cette relation d'équivalence est compatible avec l'addition et le produit sur $\mathbf{R}[X]$ on obtient une structure d'anneau.
  $\to$ c'est un des principaux intérêts de la notion d'idéal dans un anneau.
- Comme $X^2 + 1$ est irréductible sur $\mathbf{R}$, on peut montrer que K est un corps.
  $\to$ l'idéal (X^2+1) est un idéal *maximal* de $\mathbf{R}[X]$, donc le quotient $\mathbf{R}[X]/(X^2+1)$ est un corps.
- Le corps $K = \mathbf{R}[X]/(X^2 + 1)$ forme un $\mathbf{R}$-espace vectoriel de dimension 2.
  Une base de K vu comme $\mathbf{R}$-espace vectoriel est $(\dot{1}, \dot{X})$ les classes d'équivalence de 1 et de X.
  On note cette seconde i et on voit aisément que $i^2 = -1$ dans le corps.
  On a bien construit $\mathbf{C}$.

On dit que $\mathbf{C}$ est le corps de décomposition de $X^2 + 1$ sur $\mathbf{R}$.
Cette méthode se généralise dès que l'on veut donner des racines à un polynôme irréductible.

6 Les groupes $\mathbf{Z}/n\mathbf{Z}$

Cette partie est une simple reprise de ce qui a été fait dans la section 2-A page 4.

Les groupes[5] $\mathbf{Z}/n\mathbf{Z}$ sont des **modèles** d'espaces quotients, et nous nous permettons donc d'insister lourdement à leur sujet (quitte à nous répéter).

$\mathbf{Z}/n\mathbf{Z}$ représente les entiers modulo n :

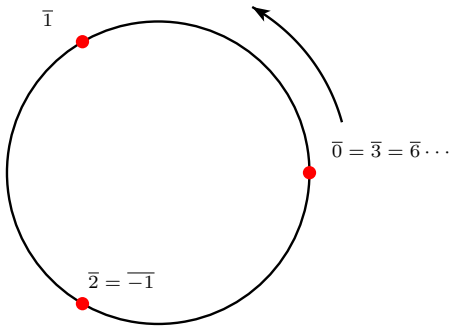
$$\left\{\overline{0}, \overline{1}, \cdots, \overline{n-1}\right\}.$$

Lorsqu'il n'y a pas d'ambigüité, on n'écrit pas les barres au dessus des valeurs.

Par exemple pour $\mathbf{Z}/3\mathbf{Z}$, on obtient la table d'opération suivante

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Dans $\mathbf{Z}/3\mathbf{Z}$: $\overline{-6} = \overline{-3} = \overline{0} = \overline{3} = \overline{36}$... ce qui revient à compter le long du cercle :



Dans $\mathbf{Z}/n\mathbf{Z}$, les nombres divisibles par n sont ramenés à 0 et plus généralement chaque nombre est ramené à son reste modulo n.

Quotienter par $n\mathbf{Z}$, c'est identifier les objets modulo n, ce qui revient à « enrouler » la droite des entiers relatifs. Ainsi tous les entiers séparés par $n\mathbf{Z}$ se superposent, ils sont dans la même classe d'équivalence, donc identifiés.

Quotienter par $I \triangleleft G$ **:** c'est « tuer » I, ce qui revient à assimiler I à 0.

Cette image a été utilisée pour la construction de $\mathbf{C}$.

L'enroulement de $\mathbf{Z}$ était ce que nous avions réalisé page 4 avec le morphisme :

$$f : \left\{ \begin{array}{ccc} (\mathbf{Z}, +) & \to & (\mathbf{U}_n, \times) \\ k & \mapsto & \mathrm{e}^{\frac{2ik\pi}{n}} \end{array} \right.$$

Ce morphisme n'est pas injectif car $\mathbf{U}_n$ est de cardinal fini n alors que $\mathbf{Z}$ est infini. On peut factoriser f par le noyau $\ker(f)$.

$$f(k) = 1 \iff k \equiv 0\ [n] \iff k \in n\mathbf{Z}.$$

Ainsi $\ker(f) = n\mathbf{Z}$ et l'isomorphisme en découle :

$$\widetilde{f} : \left\{ \begin{array}{ccc} (\mathbf{Z}/n\mathbf{Z}, +) & \to & (\mathbf{U}_n, \times) \\ \overline{k} & \mapsto & \mathrm{e}^{\frac{2ik\pi}{n}} \end{array} \right.$$

On pourrait en dire beaucoup plus sur $\mathbf{Z}/n\mathbf{Z}$*, mais ce n'est pas le but ici.*

Exercice

Montrer que tout groupe cyclique (engendré par un seul élément) est isomorphe à $\mathbf{Z}$ s'il est infini, ou à $\mathbf{Z}/n\mathbf{Z}$ s'il est fini de cardinal n.

Solution :

Soit $G =< x >$ un groupe cylique engendré par x (et noté multiplicativement).
On définit le morphisme

$$f : \left\{ \begin{array}{ccc} (\mathbf{Z}, +) & \to & (G, \times) \\ k & \mapsto & x^k \end{array} \right.$$

Par définition d'un groupe cyclique, f est surjective.
On peut donc factoriser f par son noyau pour obtenir un isomorphisme.
Or $\ker(f) \triangleleft \mathbf{Z}$: il existe $n \in \mathbf{N}$ tel que $\ker(f) = n\mathbf{Z}$.
Donc G est isomorphe à $\mathbf{Z}/n\mathbf{Z}$.
Si $n = 0$, alors $\mathbf{Z}/n\mathbf{Z}$ correspond à $\mathbf{Z}$ et G est un groupe cyclique infini isomorphe à $\mathbf{Z}$.
Sinon, $\mathrm{Card}\,(G) = \mathrm{Card}\,(\mathbf{Z}/n\mathbf{Z}) = n$.

5. On peut munir $\mathbf{Z}/n\mathbf{Z}$ d'une structure d'anneau.