Mathématiques pures

ALGÈBRE UNIVERSELLE

UN PETIT PEU D'ENSEMBLES POUR LES CONCOURS

Un petit peu d'ensembles pour les concours

On suppose connus les fondements sur les ensembles de la première année de classe préparatoire.

Quelques références sûres pour ces notions :

- ▷ Le cours de B. Rivet ;
- ▷ *Les mathématiques dévoilées*, Vincent Rohart, Ellipses (deux chapitres sur les ensembles) ;
- ▷ *Mathématiques. Tout-en-un pour la licence, Niveau 1*, Jean-Pierre Ramis et André Warusfel, Dunod ;
- ▷ *Mathématiques : tout-en-un* chez Dunod, le premier volume pour le chapitre sur les ensembles (MPSI) et le second (MP), dans le chapitre « Familles sommables » pour la dénombrabilité.

Exercice 1

1. Montrer que $\{0,1\}^{\mathbb{N}}$ est bijection avec $\mathcal{P}(\mathbb{N})$.

2. Montrer que tout intervalle non trivial est en bijection avec $\mathbb{R}$.

3. Montrer que $\mathcal{P}(\mathbb{N})$ et $\mathbb{R}$ sont en bijection.

1 Cardinaux : les lacunes du cours

Nous ne nous donnons pas en objet de former ici un cours complet sur les cardinaux dénombrables, mais seulement un complément de cours rudimentaire : deux démonstrations non seulement au programme, mais dont les méthodes sont réutilisables. On rappelle d'abord une convention fluctuante.

Définition. *(Dénombrabilité)*

Deux définitions coexistent pour la dénombrabilité :

- La convention faible : un ensemble est *dénombrable* par définition si et seulement s'il est en bijection avec une partie de $\mathbb{N}$, ou, ce qui est équivalent, s'il s'injecte dans $\mathbb{N}$. Dans ce cas, *infini dénombrable* signifie exactement « en bijection avec $\mathbb{N}$ ». Un ensemble dénombrable est donc soit fini (un ensemble est fini si et seulement s'il est en bijection avec un certain $[\![1,n]\!]$, $n \in \mathbb{N}$) soit infini dénombrable.
- La convention forte : *dénombrable* signifie maintenant « en bijection avec $\mathbb{N}$ » et le terme *au plus dénombrable* couvre les ensembles finis ou dénombrables au sens fort. *Infini dénombrable* est alors un pléonasme. **C'est la convention du programme donc nous nous efforcerons de nous y soumettre.**

Dans les deux cas, on réserve le mot *indénombrable* pour les cardinaux plus grands que $\mathbb{N}$ (on dit qu'un cardinal A est plus grand que B si l'ensemble B s'injecte dans A).

Exercice 2

Montrer que $\mathbb{Q}$ est dénombrable.

Remarque. Un ensemble est infini si et seulement s'il n'est pas fini. On dit qu'un ensemble est *infini au sens de Dedekind* s'il est équipotent à l'une de ses parties strictes, ou, ce qui est équivalent, s'il est plus grand que $\mathbb{N}$, c'est-à-dire s'il contient une partie infinie dénombrable. Dans la théorie des ensembles classiques, tout ensemble infini au sens de Dedekind est infini. La réciproque n'est pas démontrable dans le système ZF où ne figure pas l'axiome du choix, mais dès lors qu'on l'y rajoute (ou du moins sa forme dite dénombrable), les deux notions sont équivalentes. Dans ce cas, un ensemble est infini si et seulement s'il en existe une suite d'éléments deux à deux distincts (c'est alors une injection de $\mathbb{N}$ dans cet ensemble), et $\mathbb{N}$ est le plus petit infini (*i. e.* $\mathbb{N}$ s'injecte dans tout ensemble infini).

Exercice 3

Montrer que le complémentaire d'un ensemble fini dans un ensemble infini est infini.

Exercice 4

1. *(Théorème de Cantor)* Soit E un ensemble. Montrer que E et $\mathcal{P}(E)$ ne peuvent être en bijection.

2. Quel est le cardinal de l'ensemble des parties d'un ensemble fini ?

3. Montrer qu'il n'existe pas d'ensemble des parties d'aucun ensemble qui soit infini dénombrable.

Exercice 5

On admet le résultat de cours de la partie suivante.

1. Montrer qu'un ensemble E est infini au sens de Dedekind, si et seulement si $\mathbb{N} \hookrightarrow E$ (que l'on formule : $\mathbb{N}$ s'injecte dans E, ou encore E contient une copie de $\mathbb{N}$).

2. Établir que cette condition est équivalente à ce qu'il existe une suite d'éléments de E deux à deux distincts.

3. Montrer que tout ensemble infini au sens de Dedekind est infini au sens classique.

4. L'axiome du choix dénombrable annonce que si $(E_n)_{n\in\mathbb{N}}$ sont des ensembles non vides, il existe une suite x telle que pour tout n, $x_n \in E_n$. Montrer que modulo cet axiome, tout ensemble infini est infini au sens de Dedekind.

5. En déduire que $\mathbb{N}$ est le plus petit ensemble infini.

1.1 Parties de $\mathbb{N}$

Le théorème suivant, explicitement au programme, permet de décrire le cardinal de toutes les parties de $\mathbb{N}$, dont on a vu qu'il était le premier infini : elles sont soient finies, soit automa-

tiquement dénombrables dans la convention que nous avons fixé. On verra brièvement qu'une telle taxonomie n'est généralement plus possible entre les parties des cardinaux infinis.

Exercice 6

Montrer qu'une partie de $\mathbb{N}$ est infinie si et seulement si elle est non majorée.

Propriété. *(Axiome du bon ordre de $\mathbb{N}$)*
Toute partie non vide de $\mathbb{N}$ a un minimum.

▷ Tout dépend de ce que l'on pose comme axiome de $\mathbb{N}$. ■

Propriété. *(Cardinal des parties de $\mathbb{N}$)*
Toute partie de $\mathbb{N}$ est au plus dénombrable, autrement dit, toute partie de $\mathbb{N}$ est soit finie, soit infinie dénombrable, ou encore, tout partie infinie de $\mathbb{N}$ est en bijection avec $\mathbb{N}$.

▷ On choisit cette dernière formulation. Soit A une partie infinie de $\mathbb{N}$. On veut former une bijection de $\mathbb{N}$ sur A, c'est-à-dire une suite bijective. On la définit par récurrence de la manière suivante : on pose $u_0 = \min(A)$ et $u_0, ..., u_n$ étant déjà construits, on pose $u_{n+1} = \min\{x \in A \mid x > u_n\}$. Montrons que cette suite est bien définie, à valeurs dans A, injective et surjective.

- La suite est bien définie, car u_n n'est pas un majorant de A : en effet, si c'était le cas, A serait majorée et une partie de $\mathbb{N}$ est finie si et seulement si elle est majorée. Ainsi $\{x \in A \mid x > u_n\}$ est une partie non vide de A, partie de $\mathbb{N}$, donc par axiome, elle admet un plus petit élément. Remarquons que par construction $u_{n+1} > u_n$ $(*)$.
- Le minimum d'une partie lui appartient, donc u_n appartient à la partie de A définie ci-dessus donc à A. De même u_0 est dans A, donc la suite est bien définie en image également.
- D'après la remarque $(*)$, u est strictement croissante donc en particulier injective.
- Il reste à montrer que u est surjective. Soit $a \in A$. On considère $A_0 = \{a_n \mid n \in \mathbb{N}^*\}$. Par injectivité, cette partie de $\mathbb{N}$ est infinie donc non majorée, en particulier non majroée par a. L'ensemble A_1 des majorants de A_0 est donc une partie non vide de $\mathbb{N}$ et admet donc par axiome un plus petit élément que nous noterons $a_n = \min(A_1)$. Alors par définition du minimum, $a_n > a$ et $a_{n-1} \leqslant a$. Supposons un instant que cette dernière inégalité soit stricte. Alors par construction, $a_n = \min\{x \in A \mid x > a_{n-1}\}$ et par cette dernière hypothèse, $a_n \leqslant a$ par définition du minimum et $a \in A$ appartenant à ce dernier ensemble. C'est absurde avec $a_n > a$, donc il y a égalité : $a = a_{n-1}$ ce qui donne un antécédent par la suite $a : n - 1$.

Ceci conclut la démonstration. ■

Remarques.

1. Cette méthode est exactement la même que celle qui permet de montrer ce résultat souvent passé sous silence : étant donnés $x_1, ..., x_n$ n réels deux à deux distincts, il existe une unique permutation $\sigma \in \mathfrak{S}_n$ telle que $x_{\sigma(1)}, ..., x_{\sigma(n)}$ les ordonne dans l'ordre croissant.

2. Des arguments semblables permettent de montrer ce que nous appelons personnellement *lemme de recouvrement croissant*[1] : étant donné I un ensemble et $(J_n)_{n\in\mathbb{N}}$ un recouvrement ($\bigcup_{n\in\mathbb{N}} J_n \supseteq I$) de parties de I (il y a donc égalité dans le recouvrement) croissant ($J_n \subseteq J_{n+1}$ pour tout $n \in \mathbb{N}$), la suite des couronnes définie par $I_0 = J_0$ et pour tout $n \geqslant 1$, $I_n = J_n \setminus J_{n-1}$ forme une partition à parties éventuellement vides (*i. e.* un partage) de I.

Exercice 7

1. Quel est le cardinal de l'ensemble des parties finies de $\mathbb{N}$?

2. Quel est le cardinal de l'ensemble des parties infinies de $\mathbb{N}$?

Exemple. L'ensemble des nombres premiers $\mathcal{P}$ est infini : en effet, si $p_1, ..., p_n$ sont les seuls nombres premiers, alors $n = p_1...p_n + 1$ est encore premier, mais distinct de tous les autres... Puisque $\mathcal{P}$ est une partie de $\mathbb{N}$, elle est infinie dénombrable et l'on peut, d'après la preuve précédente, former la suite croissante des nombres premiers $(p_n)_{n\in\mathbb{N}}$. On peut par exemple montrer que $\sum \frac{1}{p_n}$ diverge, et que plus généralement $\sum \frac{1}{p_n^\alpha}$ a le même critère de convergence que celui de Riemann.

Exercice 8

Soit (u_n) une suite réelle et A une partie de $\mathbb{N}$. À quelle condition la quantité $\sum_{n\in A} u_n$ est-elle définie ?

Les cardinaux

Le cardinal est la notion intuitive de nombre d'éléments, et notamment dans le cas des ensembles finis où la notion est plus élémentaire. Cependant, dans le cas des ensembles finis, elle mène à de nombreux paradoxes et notamment à celui donnant que des ensembles peuvent avoir exactement le même nombre d'éléments (et donc, le même cardinal) que leurs parties strictes : par exemple, l'ensemble des entiers naturels et l'ensemble des entiers naturels pairs, propriété qui vient d'après ce que l'on a dit précédemment caractériser justement les ensembles infinis.

On dit que deux ensembles ont le même cardinal s'ils sont en bijection. Ceci définit une relation d'équivalence sur la classe de tous les ensembles (qui n'est pas un ensemble !) dont les classes ont pour représentants des ensembles typiques, qui sont habituellement : $\emptyset$, les $[\![1, n]\!]$,

[1] Ceci est utilisé dans le cadre du programme comme lemme des théorèmes de limite monotone en probabilités discrètes. Il sert aussi à démontrer un corollaire du théorème de sommation par paquets, que l'on utilise notamment dans une preuve par récurrence de l'identité d'Euler.

$n \in \mathbb{N}$, $\mathbb{N}$, $\mathcal{P}(\mathbb{N}) \simeq \mathbb{R}$, puis $\mathcal{P}(\mathcal{P}(\mathbb{N}))$, etc. Et encore, tous les cardinaux ne sont pas représentés par cette suite, strictement croissante pour l'ordre cardinal.

C'est Gottlob Frege et Georg Cantor qui définissent ces notions, posant les fondements de la théorie des ensembles à partir des années 1880, que ce dernier décrit comme l'étude de l'infini. Celle-ci est profondément liée à la logique théorique, deux branches mathématiques tout à fait co-dépendantes.

1.2 Réunion dénombrable de dénombrables

Lorsqu'on sait que pour tout $k \in \mathbb{N}$, $\mathbb{N}^k$ est dénombrable (voir ci-après), il est facile d'établir qu'une réunion finie d'ensembles finis est dénombrable. En effet, si les $A_1, ..., A_k$ sont des ensembles, leur réunion s'injecte trivialement dans $\prod_{i=1}^{k} A_i$. La question se pose différemment dans le cas d'une réunion au plus dénombrable. Dans la suite, on utilisera le fait dû à l'axiome du choix qu'un ensemble *non vide* s'injecte dans un autre si et seulement s'il existe une surjection en sens inverse.

Exercice 9

(Grille de Cantor) Montrer que $(p, q) \longmapsto \frac{(p+q)(p+q+1)}{2} + q$ est une bijection de $\mathbb{N}^2$ sur $\mathbb{N}$, sans nécessairement expliciter la bijection réciproque.

Théorème. *(Dénombrabilité des réunions dénombrables de dénombrables)*

Si I est au plus dénombrable et $(A_i)_{i\in I}$ une famille d'ensembles au plus dénombrables, alors leur réunion est encore au plus dénombrable. Le théorème est encore vrai en remplaçant par *dénombrable* à chaque occurrence de *au plus dénombrable*.

▷ On a vu le cas I fini ; ne considérons plus que I infini dénombrable. On peut donc prendre $(A_n)_{n\in\mathbb{N}}$ une famille d'ensembles tous au plus dénombrables. Ainsi, pour tout $n \in \mathbb{N}$, il existe une surjection $f_n : N \twoheadrightarrow A_n$. Considérons l'application $f : \mathbb{N} \times \mathbb{N} \longrightarrow \bigcup_{i\in\mathbb{N}} A_i$ qui à un couple (n, k) fait correspondre $f_n(k)$: l'existence d'une telle fonction est garantie par l'**axiome du choix**. Cette application est une surjection par définition de la réunion puis surjectivité des f_n : pour tout $x \in \bigcup_{i\in\mathbb{N}} A_i$, il existe k tel que $x \in A_k$ puis $n \in \mathbb{N}$ tel que $x = f_n(k)$. Or $\mathbb{N}^2$ est au plus dénombrable (voir ci-après), donc $\bigcup_{i\in\mathbb{N}} A_i$ (son cardinal est plus petit que $\mathbb{N}$). Enfin, dans le cas de la dénombrabilité forte, il suffit de remarquer que A_0 s'injecte dans $\cup_{i\in\mathbb{N}} A_i$ pour avoir l'*infinie* dénombrabilité. ■

Remarque. La dernière phrase est inutile si l'on convient de la dénombrabilité faible, comme expliqué ci-haut, ce qui lui donne tout son intérêt. Mais en pratique, il est trivial de

vérifier qu'une opération sur ensembles infinis est infinie.

Exercice 10

1. Un nombre réel est *algébrique*, s'il est racine d'un polynôme non nul à coefficients rationnels. Partitionner intelligemment $\mathbb{Q}[X]$ pour trouver le cardinal de l'ensemble des nombres algébriques.

2. *(Théorème de Liouville)* En déduire qu'il existe au moins un réel transcendant, c'est-à-dire non algébrique.

Il ne faut pas confondre ce dernier résultat théorématique avec celui sur les produits cartésiens, qui présente une dissymétrie. En effet, un produit cartésien fini d'ensembles au plus dénombrables est au plus dénombrable, mais c'est faux pour un produit cartésien infini, même dénombrable : on a vu que $\{0,1\}^{\mathbb{N}}$ était indénombrable dans le premier exercice.
Justifions cette première affirmation. Soit k un entier naturel (non nul, le produit cartésien vide étant vide), et $p_1, ..., p_k$ k nombres premiers. Alors l'application de $\mathbb{N}^k$ dans $\mathbb{N}$ qui à $(n_1, ..., n_k)$ fait correspondre $p_1^{n_1} \times ... \times p_k^{n_k}$ est injective d'après le théorème fondamental de d'Alembert, ce qui donne la dénombrabilité de $\mathbb{N}^k$, et à une bijection près celle d'un produit cartésien fini d'au plus dénombrables (une manière beaucoup plus rapide que celle de la grille de Cantor).

Exercice 11

Montrer que $\mathbb{R}^n$, en tant que $\mathbb{Q}$-espace vectoriel, est de dimension infinie. *Une base de* $\mathbb{R}$ *vu comme un* $\mathbb{Q}$*-espace vectoriel est appelée base de Hamel.*

Un ensemble a la puissance du continu, par définition, s'il est en bijection avec $\mathbb{R}$, qui est en bijection avec $\mathcal{P}(\mathbb{N})$. La fameuse *hypothèse du continu*, dont il a été démontré (Kurt Gödel en 1938 puis Paul Cohen en 1963 avec sa célèbre méthode du *forcing*) qu'elle était indécidable, à savoir démontrable et de négation démontrable, dans le cadre usuel de la théorie des ensembles, stipule qu'il n'existe pas de cardinal strictement compris entre $\mathbb{N}$ et $\mathcal{P}(\mathbb{N})$, autrement dit, que toute partie de $\mathbb{R}$ est au plus dénombrable ou a la puissance du continu. Cette affirmation rompt la continuité du théorème sur les parties de $\mathbb{N}$ établi à la partie précédente à laquelle on pouvait s'attendre.

Propriété. *(Cardinal des réunions dénombrables de puissances du continu)* **HP**
Si $(A_n)_{n\in\mathbb{N}}$ est une famille d'ensembles ayant la puissance du continu, alors leur réunion est encore dénombrable.

▷ À faire en exercice, de façon tout à fait similaire à la démonstration précédente. ■

Remarque. Si l'on s'aperçoit que $\mathbb{R}^2$ et $\mathbb{R}$ sont équipotents[2] (*i. e.* en bijection), on peut démontrer qu'une réunion de puissances de continu sur un ensemble ayant la puissance de continu a la puissance du continu. Plus généralement, si l'on sait montrer que tout ensemble infini est équipotent à son carré, ce qui n'est pas évident, mais vrai, alors on peut démontrer pareillement que si $(A_i)_{i\in E}$ est une famille dont tous les éléments sont de cardinal E, leur réunion a pour cardinal E au plus.

Exercice 12

En informatique théorique, on considère des *alphabets* finis, c'est-à-dire ensembles finis, prenons-en un $\mathcal{A}$, dont les éléments sont appelés *lettres*. Un *mot fini* sur $\mathcal{A}$ est un n-uplet d'éléments de $\mathcal{A}$. L'ensemble des *langages* sur $\mathcal{A}$ est défini comme $\mathcal{P}(\mathcal{A}^*)$. On dit qu'un langage $\mathcal{L} \subseteq \mathcal{A}^*$ est *reconnu par un algorithme* s'il existe un programme informatique ayant pour entrées les $u \in \mathcal{A}^*$ et qui calcule la fonction caractéristique de $\mathcal{L}$. Montrer qu'il existe des langages indécidables, c'est-à-dire qui ne sont pas reconnus par des algorithmes.

2 Quotients d'ensembles

Ces notions sont complètement hors programme. Toutefois, elles permettent de s'éclaircir grandement les idées sur certaines notions en théorie des groupes mais également en algèbre linéaire comme nous l'allons voir. De plus, elle permet de clore la théorie élémentaire des opérations ensemblistes : la somme (réunion), la différence (différence ensembliste, différence symétrique), le produit (cartésien ou intersection), sont complétés par le quotient, qu'il faut introduire au moyen d'un objet à première vue retors : la relation d'équivalence.

Ne nous leurrons pas pourtant : lorsqu'il s'agit d'ensembles simplement, il n'y a pas de notion de quotient de deux ensembles, mais seulement d'*ensemble quotient par une relation*

[2] Montrons ce résultat à l'aide du théorème de Cantor-Bernstein, théorème dont la preuve, quoique difficile, permet d'établir que si deux ensembles s'injectent l'un dans l'autre réciproquement, ils sont en bijection. $\mathbb{R}$ s'injecte dans $\mathbb{R}^2$ par l'application canonique $x \longmapsto (x, 0)$. Réciproquement, exhibons une injection de $\mathbb{R}^2$ dans $\mathbb{R}$. Pour ça, il suffit d'exhiber une bijection de $[0,1[^2$ dans $[0,1[$, puisque comme c'est un intervalle non trivial, $[0,1[$ est en bijection avec $\mathbb{R}^2$. Posons l'application qui à deux éléments de $[0,1[$ associe l'entrelacement des décimales de leurs développements illimités propres, définie par :

$$\begin{array}{rccl} \varphi : & [0,1[^2 & \longrightarrow & [0,1[\\ & (0, a_1a_2a_3...; 0, b_1b_2b_3...) & \longmapsto & 0, a_1b_1a_2b_2a_3b_3... \end{array}$$

Cette fonction est bien définie d'après l'existence et l'unicité du développement illimité propre d'un réel, c'est-à-dire qu'on ne peut choisir qu'une unique suite de décimales non stationnaire à 9 qui représente un réel donné. Montrons son injectivité. Soient $(0, a_1a_2a_3...; 0, b_1b_2b_3...)$, $(0, a'_1a'_2a'_3...; 0, b'_1b'_2b'_3...) \in [0,1[$, les représentations ici étant des développements illimités propres. Supposons que $\varphi(0, a_1a_2a_3...; 0, b_1b_2b_3...) = \varphi(0, a'_1a'_2a'_3...; 0, b'_1b'_2b'_3...)$, c'est-à-dire $0, a_1b_1a_2b_2a_3b_3... = 0, a'_1b'_1a'_2b'_2a'_3b'_3...$, alors ces écritures ne sont pas des développements impropres. En effet, si $a_1b_1a_2b_2a_3b_3$ est stationnaire à 9, alors à partir d'un certain rang N, $(a_n, b_n) = (9, 9)$ pour tous $n \geqslant N$. En particulier, (a_n) est stationnaire à 9, ce qui est exclu. De même pour l'écriture de droite. Or il y a unicité du développement décimal propre, ce qui impose : $a_1 = a'_1$ sur la première décimale, puis $b_1 = b'_1$, puis $a_2 = a'_2$, etc., de sorte que $0, a_1a_2a_3... = 0, a'_1a'_2a'_3...$ d'une part et $0, b_1b_2b_3... = 0, b'_1b'_2b'_3...$ d'autre part, ce qui montre l'injectivité de φ.

d'équivalence. On ne pourra définir la notion de quotient d'ensembles par l'une de ses parties, et encore il les faudra structurées (sous-groupe pour un groupe, sous-espace vectoriel, etc., ce qui correspondra à la notion de diviseur) que dans de telles structures.

2.1 Ensembles sans structure donnée

On rappelle un résultat de mathématiques supérieures dans sa totalité.

Théorème. *(Théorème fondamental des relations d'équivalence)*
Soit E un ensemble. L'application $\mathcal{R} \longmapsto \{\overline{x}_{\mathcal{R}} \mid x \in E\}$ est une bijection de l'ensemble des relations d'équivalence sur E dans l'ensemble des partitions de E.

▷ Il s'agit démontrer d'abord que cette application est bien définie, c'est-à-dire que les classes d'une relation d'équivalence partitionnent l'ensemble sur lequel elle est définie, ce qui est un résultat de sup (le refaire !). On vérifie facilement qu'à toute partition de E, on peut faire correspondre une relation d'équivalence définie par l'appartenance de deux éléments à la même partie de la partition. Ces deux applications sont alors bijections réciproques. ■

Exercice 13

Le n-ième nombre de Bell, noté B_n, est le nombre de relations d'équivalence sur un ensemble à n éléments.

1. *(Relation d'Aitken)* Montrer que $B_{n+1} = \sum_{k=0}^{n} \binom{n}{k} B_k$.

2. *(Formule de Dobinski)* En déduire que $B_n = \frac{1}{e} \sum_{k=0}^{+\infty} \frac{k^n}{k!}$ le n-ième moment de la Poisson de moyenne $\lambda = 1$.

3. *(Congruence de Touchard)* Montrer que si p est premier, alors $B_{n+p} \equiv B_n + B_{n+1} \bmod(p)$.

Exemple. Si l'on partitionne $\mathbb{R}^*$ en ses deux composantes connexes, on obtient la relation « avoir le même signe ».

Propriété. Soit $\mathcal{R}$ une relation d'équivalence sur un ensemble E. Alors pour tous $x, y \in E$, $x\mathcal{R}y \Leftrightarrow \overline{x} = \overline{y}$.

▷ En exercice. ■

Définition. *(Ensemble quotient par une relation d'équivalence)*
Soit E un ensemble et $\mathcal{R}$ une relation d'équivalence sur E. Alors on note $E/\mathcal{R}$ l'*ensemble quotient par* $\mathcal{R}$ défini par $E/\mathcal{R} = \{\overline{x}_{\mathcal{R}} \mid x \in E\}$.

⟶ **Convention.** On aurait aussi pu définir, de manière équivalente, l'ensemble quotient par un système de représentants de $\mathcal{R}$, c'est-à-dire un élément de la classe de x et un seul dans l'ensemble quotient pour tout x de E. Cependant, nous fixons la construction de la preuve précédente.

Fixons maintenant E un ensemble, $\mathcal{R}$ une relation d'équivalence sur E. On se permet de la noter $\sim$. Pour rappel, on peut noter indifféremment $\overline{x}_{\mathcal{R}} = \overline{x}_{\sim} = \overline{x} = cl(x)$ quand il n'y a pas d'ambiguïté la classe d'équivalence de l'élément $x \in E$.

Définition et propriété. *(Projection canonique)*
L'application $\pi : E \longrightarrow E/\mathcal{R}$ qui à x fait correspondre la classe de x par $\mathcal{R}$, notée $\overline{x}_{\mathcal{R}}$, est une surjection appelée *projection canonique.*

▷ La surjectivité vient de la réflexivité de $\mathcal{R}$. ■

Propriété. Pour tout $a \in E/\mathcal{R}$, $\pi^{-1}(a) = cl(x)$ où x est un antécédent de a par π (il en existe au moins un d'après la proposition précédente).

▷ Évident. ■

A priori, bien sûr, l'ensemble et l'ensemble des classes d'équivalence par $\mathcal{R}$ n'ont pas le même cardinal.

Exercice 14

Montrer que la projection canonique est une bijection si et seulement si $\mathcal{R}$ égale la relation d'égalité sur E, notée $=_E$.

Heuristique. L'introduction de la notion d'ensemble quotient débrouille la perplexité initiale devant l'idée d'appeler quotient un ensemble formée des classes d'une relation : la surjectivité permet tout d'abord d'avoir que, dans tous les cas, même en milieu infini, $\text{card}(E) \geqslant \text{card}(E/\mathcal{R})$, ce qui permet d'assimiler $\mathcal{R}$ à, par exemple, un nombre supérieur à 1, dans le cas E non vide, par l'artifice frauduleux ci-dessous :

$$\text{card}(E) \geqslant \text{card}(E/\mathcal{R}) = \frac{\text{card}(E)}{\text{card}(\mathcal{R})} \text{ donc } \text{card}(\mathcal{R})\text{card}(E) \geqslant \text{card}(E) \text{ donc } \text{card}(\mathcal{R}) \geqslant 1,$$

nombre qui diviserait E en autant parties disjointes. L'important dans la suite sera double : d'une part que la structure quotientée soit préservée (ce qui sera à peu près toujours le cas, et constituera à chaque section la première partie sur la compatibilité de la structure avec la relation d'équivalence : sous-groupe distingué, linéarité de la projection, continuité en topologie...), d'autre part, l'établissement de théorèmes de factorisation et d'isomorphisme à propos des morphismes partant de structures quotientées dont on verra que, par cet effet, ils sont, sous certaines hypothèses, « simplifiables » en applications quotients.

Exercice 15

Une relation d'équivalence sur $\mathbb{R}$ permet de définir l'argument principal d'un complexe : quel est le cardinal de l'ensemble quotient par elle ?

Les théorèmes sur les ensembles quotients sont très bien résumés par les diagrammes. Nous introduisons d'ores et déjà celui qui sert de base à tous les autres avec les propriétés précédentes. On rappelle que parmi les applications qui sont des flèches $\longrightarrow$, les injections sont notées $\hookrightarrow$, les surjections sont notées $\twoheadrightarrow$, et les bijections sont notées $\simeq$ ou comme la conjonction d'une injection et d'une surjection.

$$\begin{array}{c} E \\ {\scriptstyle\pi}\big\downarrow \\ E/\mathcal{R} \end{array}$$

Exercice 16

Pour se débarbouiller l'esprit sur le raisonnement par analyse-synthèse, montrer que :

1. Toute fonction de $\mathbb{R}$ dans $\mathbb{R}$ se décompose de façon unique comme somme d'une fonction paire et d'une fonction impaire.

2. Toute matrice à coefficients dans un corps de caractéristique différente de 2 ($2 \neq 0$) se décompose de façon unique comme somme d'une matrice symétrique et d'une matrice antisymétrique.

3. Pour toute base $(e_1, ..., e_n)$ d'un espace vectoriel de dimension finie, il existe une unique base de son dual, base duale, notée $(e_i^*)_{i\in[\![1,n]\!]}$ telle que pour tous $i, j \in [\![1, n]\!]$, $e_i^*(e_j) = \delta_i^j$.

Théorème. *(Théorème de factorisation pour les applications)*

Soit F un ensemble quelconque et f une application de E dans F. Alors f est compatible avec $\mathcal{R}$ (*i. e.* $\forall x, y \in E \quad x \sim y \Rightarrow f(x) = f(y)$) si et seulement s'il existe une unique application $\tilde{f}$ telle que $f = \tilde{f} \circ \pi$ (se qui se réécrit $f(x) = \tilde{f}(\overline{x})$ pour tout $x \in E$). Dans ce cas de compatibilité, on dit qu'on *passe au quotient* dans l'application f.

▷ La preuve est très facile si l'on se focalise sur le choix des bons arguments.

▶ Dans le sens direct, on suppose que f est compatible avec la relation $\mathcal{R}$. On montre l'unicité et l'existence de $\tilde{f}$ par analyse-synthèse. Supposons que pour tout $x \in E$, puisque par définition $\pi(x) = \overline{x}$, $\tilde{f}(\overline{x}) = f(x)$: ceci définit de manière explicite et donc unique l'application $\tilde{f}$, ce qui termine l'analyse. Le point crucial est que **cette écriture a un sens**, vu que $f(x)$ ne dépend pas du représentant choisi de $\overline{x}$ *ce qui est exactement ce que signifie la condition de compatibilité.* Pour la synthèse, c'est encore plus immédiat : pour tout $x \in E$, $\overline{x} = \pi(x)$ donc $\tilde{f}(\overline{x}) = \tilde{f} \circ \pi(x)$. Mais l'hypothèse de synthèse définit ce que l'analyse conclut, soit $\tilde{f}(\overline{x}) = f(x)$, d'où $f(x) = \tilde{f} \circ \pi(x)$ ce qui signifie par définition de l'égalité des fonctions que $f = \tilde{f} \circ \pi$.

▶ Réciproquement, si l'on suppose que f se factorise en $\tilde{f} \circ \pi$ (de façon unique, mais on ne s'en sert pas), soient $x \sim y$ deux éléments de E. Alors $\pi(x) = \pi(y)$ par définition de π. Ainsi $\tilde{f} \circ \pi(x) = \tilde{f} \circ \pi(y)$ puisque $\tilde{f}$ est une application, et par hypothèse ces deux quantités égalent $f(x) = f(y)$, et donc f est compatible avec $\mathcal{R}$.

Ainsi f est compatible si et seulement elle se factorise, ce qu'il fallait démontrer. ■

La situation se présente comme suit :

$$\begin{array}{ccc} E & \xrightarrow{\quad f \quad} & F \\ {\scriptstyle \pi}\downarrow & \nearrow_{\tilde{f}} & \\ E/\mathcal{R} & & \end{array}$$

Le théorème de factorisation établit donc la commutation de ce diagramme.

Exemple fondamental. Soit $(\mathbb{A}, +, \times)$ un anneau et

$$\begin{array}{rccc} f: & \mathbb{Z} & \longrightarrow & \mathbb{A} \\ & k & \longmapsto & k.1_{\mathbb{A}} \end{array}$$

(l'unique) morphisme de l'anneau $\mathbb{Z}$ dans $\mathbb{A}$. Si $\mathbb{A}$ est fini, $\mathrm{Ker}(f)$ étant un idéal de $\mathbb{Z}$, il est de la forme $p\mathbb{Z}$ où p est pris minimal, $p \neq 0$ puisque f ne peut être injective par cardinalité. Dans ce cas, f est compatible avec la relation de congruence modulo p sur les entiers, et l'on peut définir

$$\begin{array}{rccc} \tilde{f}: & \mathbb{Z}/p\mathbb{Z} & \longrightarrow & \mathbb{A} \\ & \overline{k} & \longmapsto & k.1_{\mathbb{A}}. \end{array}$$

Il faut remarquer que c'est bien la compatibilité et elle seule (équivalence dans le théorème de factorisation) qui permet de définir ce nouveau morphisme, même il faut vérifier indépendamment que l'application est un morphisme : ce n'est pas dur mais ce sera systématique dans la partie suivante. Si $\mathbb{A}$ est intègre, et l'on peut montrer qu'un anneau fini est intègre si et seulement si c'est un corps, alors on vérifie que p est premier. Dans ce cas, $\tilde{f}$ est injectif car c'est un morphisme de corps, ce qui nous donne notamment que tout corps fini de cardinal premier p est isomorphe à $\mathbb{Z}/p\mathbb{Z}$ et que tout corps fini a pour cardinal p^d où d est un certain entier : la dimension sur $\mathrm{Im}(\tilde{f})$ de $\mathbb{K}$ vu comme $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel.

Exercice 17

Fournir un exemple où une application ne passe pas au quotient par une relation d'équivalence donnée.

Méthode. Recette pour passer au quotient dans les applications

J'ai une application φ d'un ensemble quotient Q dans F un ensemble quelconque.

1. J'identifie la relation d'équivalence qui quotiente : $Q = E/\mathcal{R}$ et E l'ensemble initial.
2. Je vérifie que $\mathcal{R}$ est une relation d'équivalence pour justifier mon propos.
3. Je pose une application f de E dans F définie sans aucun problème et qui devra, une fois passée au quotient, retomber sur φ.
4. Je montre que pour tous éléments x, y de E, si $x\mathcal{R}y$, alors $f(x)$ et $f(y)$ sont égaux.
5. Je peux maintenant définir une application $\varphi = \tilde{f} : Q \longrightarrow F$ sans trouble, telle que pour tout $\overline{x} \in Q$, $\tilde{f}(\overline{x}) = f(x)$, et j'insiste bien sur ce que cette construction n'est possible que grâce à la compatibilité vérifiée précédemment.

Si je veux une propriété d'injectivité, de surjectivité, voire de bijectivité pour mon application, je me réfère au résultat de l'exercice suivant.

Un corollaire d'intérêt principalement formel.

Théorème. *(Théorème de factorisation carré pour les applications)*

Soit F un ensemble muni d'une relation d'équivalence $\mathcal{S}$ que l'on se permet de noter $\equiv$, ses classes $\widehat{\cdot}$ et f une application de E dans F. Alors f est compatible avec $\mathcal{R}$ modulo $\mathcal{S}$ (*i. e.* $\forall x, y \in E \quad x \sim y \Rightarrow f(x) \equiv f(y)$) si et seulement s'il existe une unique application $\tilde{f}$ telle que $\chi \circ f = \tilde{f} \circ \pi$ (se qui se réécrit $\widehat{f(x)} = \tilde{f}(\overline{x})$ pour tout $x \in E$). Dans le cas de compatibilité, on dit encore qu'on passe au quotient dans f.

▷ On applique le théorème de factorisation à l'application $\chi \circ f$, l'ensemble F étant maintenant $F/\mathcal{S}$. Il suffit de vérifier alors que la compatibilité de $\chi \circ f$ avec $\mathcal{R}$ est équivalente à la compatibilité de f avec $\mathcal{R}$ modulo $\mathcal{S}$, ce qui est immédiat par définition de cette dernière notion. ■

Le diagramme correspondant est le suivant :

$$\begin{array}{ccc} E & \xrightarrow{\quad f \quad} & F \\ {\scriptstyle \pi}\downarrow & & \downarrow{\scriptstyle \chi} \\ E/\mathcal{R} & \xrightarrow[\tilde{f}]{} & F/\mathcal{S} \end{array}$$

Exercice 18

Dans chacun des deux théorèmes précédents, montrer que :

1. $\tilde{f}$ est injective si et seulement si $\forall x, y \in E \quad x \sim y \Leftrightarrow f(x) = f(y)$ (respectivement $\forall x, y \in E \quad x \sim y \Leftrightarrow f(x) \equiv f(y)$) ;

2. $\tilde{f}$ est surjective si et seulement si f est surjective ;

3. $\tilde{f}$ est bijective si et seulement si f est surjective et $\forall x, y \in E \quad x \sim y \Leftrightarrow f(x) = f(y)$ (respectivement f est surjective et $\forall x, y \in E \quad x \sim y \Leftrightarrow f(x) \equiv f(y)$).

Méthode. Recette pour passer au quotient dans les applications entre deux espaces quotients

C'est exactement la même que précédemment : **la structure quotient de l'espace d'arrivée n'intervient pas**. Pour une illustration, voir dans la section suivante sur les magmas.

On examine enfin un cas particulier important, celle de la relation $x \sim y \Leftrightarrow f(x) = f(y)$ qui est définie sur tout ensemble étant donné une application f partant de cet ensemble, dont les classes sont parfois appelées *fibres*. Le théorème de factorisation appliqué à f donne un résultat intéressant.

Théorème. *(Théorème d'isomorphisme ensembliste, théorème de bijection quotient)*

Soit f une application de E dans F deux ensembles quelconques. On considère la relation d'équivalence $\mathcal{R}$ sur E définie par $x \sim y \Leftrightarrow f(x) = f(y)$. Dans ce cas, f est compatible avec $\mathcal{R}$ et l'application quotient de f par cette relation réalise une bijection de $E/\mathcal{R}$ sur $\mathrm{Im}(f)$.

▷ Encore une fois, le théorème ne consiste qu'en des astuces de langage. Procédons par étapes claires et distinctes pour rasséréner les esprits malades. D'abord, on vérifie aisément que la relation des fibres $\mathcal{R}$ est bien une relation d'équivalence : la réflexivité est tautologique, la transitivité vient de ce que deux choses égales à un même sont égales, et la symétrie de celle de la relation d'égalité même. Dans ce cas, $E/\mathcal{R} = \{f^{-1}(y) \mid y \in \mathrm{Im}(f)\}$.

Pour pouvoir avoir seulement l'audace de rêver du théorème de factorisation, il nous faut vérifier la compatibilité de f avec $\mathcal{R}$. Nous laissons aux cerveaux fatigués le soin de découvrir par eux-mêmes, pourquoi c'est évident. La relation d'équivalence des fibres est également la relation d'équivalence associée à l'application f, définissable sur tout ensemble dont elle part par « avoir la même image par f ». Cette compatibilité exprime que cette relation est moins fine que la relation définie dans le théorème.

La remarque du paragraphe surprécédent donne en particulier, ayant introduit l'application quotient $\tilde{f}$ par $\mathcal{R}$, que $\boxed{\tilde{f}[f^{-1}(y)] = y}$. En effet

Soient deux éléments de $E/\mathcal{R}$; d'après l'expression de l'ensemble quotient ci-dessus, il existe $y, y' \in \mathrm{Im}(f)$ tels que ces éléments s'écrivent $f^{-1}(y)$, $f^{-1}(y')$. Si $\tilde{f}(f^{-1}(y)) = \tilde{f}(f^{-1}(y'))$, alors d'après ce qui précède $y = y'$ (c'est tout simplement une réécriture des deux termes), d'où $f^{-1}(y) = f^{-1}(y')$, et donc $\tilde{f}$ est injective.

De surcroît, $\mathrm{Im}(f) = \mathrm{Im}(\tilde{f})$. En effet, $\mathrm{Im}(\tilde{f}) = \{\tilde{f}(f^{-1}(y)) \mid f^{-1}(y) \in E/\mathcal{R}\} = \{\tilde{f}(f^{-1}(y)) \mid y \in \mathrm{Im}(f)\}$ d'après l'égalité encadrée et encore d'après l'égalité encadrée ceci égale $\{y \mid y \in \mathrm{Im}(f)\} = \mathrm{Im}(f)$.

Ainsi $\tilde{f}$ est une bijection de $E/\mathcal{R}$ sur $\mathrm{Im}(\tilde{f}) = \mathrm{Im}(f)$, ce qui termine la démonstration. ■

Ceci constitue un résultat théorique : l'utilité de la relation d'équivalence associée à f est factice ; il permet seulement d'établir que l'image d'une application est isomorphe, au sens

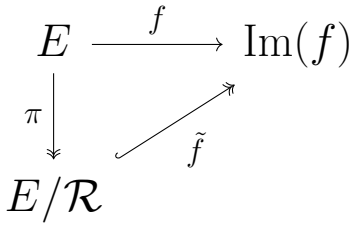
ensembliste (c'est-à-dire en bijection) avec l'espace des fibres par f, ce qui se récrit : $\mathrm{Im}(f) \simeq \{f^{-1}(y) \mid y \in \mathrm{Im}(f)\}$. Remarquons qu'on aurait pu l'établir plus élémentairement.

Exercice 19

1. Démontrer que, pour dénombrer son troupeau, un berger peut se « contenter » de compter les pattes puis diviser par quatre.

2. *(Lemme des bergers)* Soit f une surjection de A dans B deux ensembles finis, telle que pour tout y dans B, y ait exactement k antécédents par f. Montrer qu'alors $\mathrm{card}(E) = k.\mathrm{card}(F)$ et retrouver ce qui précède[3].

A picture is worth a thousand words.



2.2 Algèbre générale. Magmas

Quelques petits rappels terminologiques pour la fluidité du discours qui suit.

Définition. *(Magma)*
Un *magma* est un ensemble muni d'une loi de composition interne.

Définition. *(Magma associatif, commutatif)*
Un *magma associatif* est un magma dont la loi de composition est associative. Un *magma commutatif* est un magma dont la loi de composition est commutative.

Définition. *(Magma unifère (latéral))*
Un *magma unifère* est un magma admettant un élément neutre. Un *magma unifère à gauche* est un magma admettant un élément neutre à gauche. Un *magma unifère à droite* est un magma admettant un élément neutre à droite.

Définition. *(Élément absorbant (latéral))*
Dans un magma unifère (à gauche), un *élément absorbant (à gauche)* est un élément dont le produit (à gauche) avec un élément quelconque vaut toujours le neutre.

[3] *O fortunatos nimium, sua si bona norint, agricolas...*

Exercice 20

1. Montrer qu'un élément neutre d'un magma unifère est unique.

2. Un magma peut-il être unifère à gauche et à droite mais pour deux éléments neutres distincts ?

3. Que dire pour un élément absorbant ?

Définition. *(Inverse (latéral))*

Dans un magma unifère (latéral), un *inverse (à gauche)* d'un élément est un élément dont le produit (à gauche) avec cet élément vaut toujours le neutre.

Remarque. On peut également définir des éléments absorbants ou des inverses à droite, même si le magma est unifère est gauche.

Exercice 21

1. Montrer que les inverses dans un magma unifère sont uniques pour un élément fixé.

2. Peut-on trouver plusieurs inverses à droite dans un magma unifère ?

3. Donner un exemple d'inverse seulement à droite dans un magma unifère seulement à gauche.

4. Peut-on trouver à la fois plusieurs inverses à droite et plusieurs inverses à gauche dans un magma unifère, qui soient distincts les uns les autres ? Et dans un magma unifère à gauche et à droite d'éléments neutres distincts (voir exercice précédent) ?

Définition. *(Monoïde)*

Un *monoïde* est un magma unifère associatif.

Exercice 22

Un *demi-groupe* est un magma associatif. Donner des exemples de demi-groupes et de monoïdes non simplifiables à gauche.

Exercice 23

(Axiomes faibles du groupe) Soit un magma unifère à gauche (resp. à droite) tel que tout élément admette au moins un inverse à gauche (resp. à droite). Montrer que c'est un groupe.

On introduit maintenant les mêmes concepts que précédemment, avec la notion algébrique de loi en supplément. On se rend compte que cela ne change rien aux résultats, et qu'ils sont très stables même compte tenu de l'absence de structure élaborée pour les espaces considérés. Tout d'abord, une équivalence peu utile en pratique mais structurellement fondamentale.

Propriété. *(Compatibilité d'une loi à une relation et morphisme projection)*
Soit $(E, *)$ un magma qui soit également de façon sous-jacente un ensemble muni d'une relation d'équivalence $\mathcal{R}$. Alors $*$ est compatible avec $\mathcal{R}$ (*i. e.* pour tous éléments $x, y, x', y' \in E, (x \sim x' \text{ ET } y \sim y') \Rightarrow x * y \sim x' * y'$) si et seulement s'il existe une unique loi dite *loi quotient* notée ici $\diamond$ telle que π soit un morphisme de $(E, *)$ dans $(E/\mathcal{R}, \diamond)$.

▷ On va plus rapidement que pour le théorème de factorisation, puisque les arguments sont les mêmes. D'une part, si la loi $*$ est compatible, alors pour analyse, on doit poser pour tous $x, y \in E$ $\overline{x} \diamond \overline{y} = \overline{x * y}$ (expression de ce que π soit morphisme), ce qui est licite par compatibilité même de la loi pour la relation d'équivalence et définit de manière unique $\diamond$ sur $E/\mathcal{R}$. La synthèse est immédiate comme précédemment. Réciproquement, s'il existe (une unique) loi quotient qui rende la projection π un morphisme, alors si l'on prend dans E $x \sim x'$ et $y \sim y'$ quatre éléments, on a $\pi(x) = \pi(x')$ et $\pi(y) = \pi(y')$ par définition de la projection canonique puis $\pi(x * y) = \pi(x) \diamond \pi(y) = \pi(x') \diamond \pi(y') = \pi(x' * y')$, les première et dernière égalité étant la propriété hypothétique de morphisme. Ainsi $x * y \sim x' * y'$, donc $*$ est compatible avec $\mathcal{R}$ par définition. ■

Vocabulaire. On dit aussi que la relation compatible est une *congruence*.

Exercice 24

Que connaissez-vous comme famille dénombrable de relations compatibles avec les deux lois de l'anneau $\mathbb{Z}$?

Heuristique. Il faut tenter de ne pas mettre au même ordre cette propriété avec celle du théorème de factorisation, mais plutôt avec la définition de la projection canonique, quoiqu'elle ne soit pas théorème de son côté.

On précise la notion de compatibilité par une subtilité qui ne sera utile que dans la section suivante.

Définition. *(Compatibilité à gauche, à droite d'une loi à une relation)*
Soit $(E, *)$ un magma qui soit également de façon sous-jacente un ensemble muni d'une relation d'équivalence $\mathcal{R}$. On dit que $*$ est *compatible à gauche* avec $\mathcal{R}$ si pour tous éléments $x, y, y' \in E, y \sim y' \Rightarrow x * y \sim x * y'$. On définit de même la compatibilité à droite.

Propriété. *(Compatibilité et compatibilité latérale)*
Une loi est compatible avec une relation d'équivalence si et seulement si elle est compatible à gauche et à droite avec cette relation.

▷ Ce n'est pas aussi évident que certaines choses... D'abord, il est clair qu'une relation compatible est latéralement compatible, par réflexivité : si $x \sim x'$, $y \sim y$ donc la compatibilité donne

$x * y \sim x' \sim y$, de même à gauche. Réciproquement, supposons que la relation soit compatible à gauche et compatible à droite. Soient $x \sim x'$ et $y \sim y'$ quatre éléments de E. Alors par compatibilité à gauche, $x*y \sim x'*y$ et par compatibilité à droite, $x'*y \sim x'*y'$. Par transitivité, on a $x*y \sim x'*y'$. ■

Remarque. Dans le cas d'une loi de magma commutative, ces compatibilité latérales partielles sont équivalentes et donc équivalentes chacune à la compatibilité tout court, ce qui permet d'affaiblir légèrement les hypothèses.

Exercice 25

Soit $\equiv$ une relation d'équivalence sur $\mathbb{M}$. On suppose que $(\mathbb{M}, \cdot)$ est un magma et que la relation est compatible avec la loi interne (où seulement compatible à gauche, voir ce qui précède).

1. Démontrer que, pour tous $x \equiv y$ dans $\mathbb{M}$, pour tout $n \in \mathbb{N}^*$, $x^n \equiv y^n$.

2. On suppose ce magma unifère à gauche. Soient x, y deux éléments équivalents admettant des inverses à gauche. Montrer que $-x \equiv -y$.

3. *(Peu utile)* Que dire de cette dernière propriété si la loi n'avait été que compatible à droite ?

Propriété. *(Héritage des lois quotients)*

Si la loi de base a pour propriétés ou éléments caractéristiques les suivants, la loi quotient également, et dans ce dernier cas pour les classes de ces éléments :

- l'associativité ;
- la commutativité ;
- les éléments neutres (latéraux) ;
- les éléments absorbants (latéraux) ;
- les inverses (latéraux) ;
- en présence d'un magmas muni de deux lois dont l'une est distributive par rapport à l'autre, la distributivité ;
- le quotient d'un monoïde est un monoïde, d'un groupe, d'un anneau est un monoïde, un groupe, un anneau, d'un corps, d'une algèbre, est un anneau, un corps, une algèbre.

▷ En faire quelques-uns soi-même est un bon exercice de clarté mentale. ■

La régularité seule n'est pas conservée dans la loi quotient. Par exemple, si 2 est bien régulier dans $(\mathbb{Z}, \times)$, il ne l'est plus dans $(\mathbb{Z}/4\mathbb{Z}, \times)$ muni de la loi quotient, que l'on note de la même manière abusivement.

La dernière propriété et la relativement grande stabilité des quotients algébriques semble de loin terminer la théorie des espaces quotients. C'est vrai, en ce sens qu'elle la permet ; mais

les sections suivantes vont préciser la nature des relations d'équivalence compatibles pour les lois algébriques : modulo un sous-groupe distingué pour les groupes, pour un idéal dans un anneau unitaire, par exemple.

Semblablement à la section précédente, on peut représenter les théorèmes par des diagrammes commutatifs, en précisant profitablement les lois impliquées.

$$\begin{array}{c} (E, *) \\ \pi \big\downarrow \\ (E/\mathcal{R}, \overline{*}) \end{array}$$

Des diagrammes comme thème universel

En 1942, dans leur essai *General theory of natural equivalences*, les chercheurs Samuel Eilenberg and Saunders MacLane introduisent les notions de catégorie, de foncteur, de transformation naturelle dans le cadre de leurs travaux en topologie algébrique. Ces constructions étaient la suite logique de celle de sa professeur Emmy Noether, notamment connue pour ses travaux en algèbre abstraite (les anneaux noethériens portent son nom). Le mathématicien Stanislaw Ulam écrit que de telles idées germaient déjà en Pologne dans les années 1930. Il semble, plus généralement, que la formalisation de la théorie des catégories ait été en partie une réaction aux vacillations de la théorie des ensembles à cette époque, quoiqu'elle ait davantage servie à justifier une assise globale des domaines mathématiques qu'à leurs résolutions.

Maintenant, on énonce le parallèle du théorème de factorisation, non plus seulement pour les applications, mais pour les morphismes de magmas, définis exactement de la même manière que les morphismes de groupe du cours. Pour fixer les notations, $(E, *)$ est un magma qui soit également de façon sous-jacente un ensemble muni d'une relation d'équivalence $\mathcal{R}$; on suppose que la loi est compatible avec la relation (sinon, on ne peut rien faire comme on l'a vu) et que la loi quotient est notée $\overline{*}$. On introduit également un autre magma quelconque $(F, \diamond)$.

Théorème. *(Théorème de factorisation pour les morphismes)*

Soit f un **morphisme** de E dans F. Alors f est compatible **avec** $\mathcal{R}$ au même sens que dans la section ensembliste si et seulement s'il existe un unique **morphisme** $\tilde{f}$ tel que $f = \tilde{f} \circ \pi$ (se qui se réécrit $f(x) = \tilde{f}(\overline{x})$ pour tout $x \in E$). Dans ce cas de compatibilité, on dit toujours qu'on *passe au quotient* dans le morphisme f.

▷ Par rapport au théorème de factorisation pour les applications, il suffit de vérifier que l'application quotient est un morphisme et on établit les connexions logiques annoncées automatiquement avec ce seul annexe. Or : $\tilde{f}(\overline{x}*\overline{y}) = \tilde{f}(\overline{x*y}) = f(x*y) = f(x)\diamond f(y) = \tilde{f}(\overline{x})\diamond\tilde{f}(\overline{y})$. ■

Remarque. Ne mélangeons pas tout. Il faut prendre garde par exemple à ne pas confondre compatibilité de l'application avec la relation sur l'espace de départ et celle de la loi de l'espace de départ avec cette relation également.

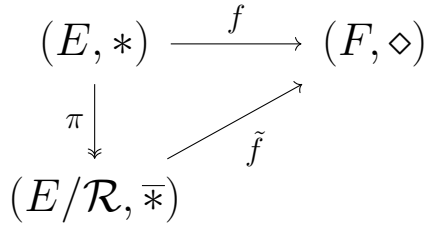
Méthode. Recette pour passer au quotient dans les morphismes

J'ai un morphisme φ d'une structure quotient Q dans F une même structure quelconque.

1. J'identifie la relation d'équivalence qui quotiente : $Q = E/\mathcal{R}$ et E la structure initiale.
2. Je vérifie que $\mathcal{R}$ est une relation d'équivalence pour justifier mon propos.
3. **Je vérifie que la loi de E structuré est compatible avec $\mathcal{R}$.**
4. Je pose un morphisme f de E dans F définie sans aucun problème et qui devra, une fois passée au quotient, retomber sur φ.
5. Je montre que pour tous éléments x, y de E, si $x\mathcal{R}y$, alors $f(x)$ et $f(y)$ sont égaux.
6. Je peux maintenant définir un morphisme $\varphi = \tilde{f} : Q \longrightarrow F$ sans trouble, telle que pour tout $\overline{x} \in Q$, $\tilde{f}(\overline{x}) = f(x)$, et j'insiste bien sur ce que cette construction n'est possible que grâce aux deux compatibilités vérifiées précédemment.

Si je veux une propriété d'injectivité, de surjectivité, voire de bijectivité pour mon application, je me réfère au résultat de l'exercice déjà étudié.

Voilà le diagramme correspond à ce nouveau théorème de factorisation dans sa version algébrique. Par rapport au précédent, on précise les lois pour garder les idées claires. Par contre, on ne précise pas que les flèches sont toutes des morphismes de magmas, ce qui est automatique lorsqu'on se donne de tracer de tels diagrammes. Ceux-ci prennent essor dans la théorie des catégories : dans la catégorie des ensembles, où les objets sont les ensembles, les flèches sont tout simplement les applications ; dans la catégorie des magmas, où les objets sont les magmas, les flèches sont les morphismes de magmas.



Le théorème de factorisation pour les morphismes établit à son tour la commutation de ce diagramme. Notons par surcroît que les caractérisations de monomorphisme, épimorphisme,

isomorphisme (morphismes injectifs, surjectifs, bijectifs), sont les mêmes que dans l'exercice sur ce sujet de la section précédente ; de même pour le théorème qui suit.

De la même manière, on dispose d'un théorème carré corollaire, encore moins excitant que le premier. Là, le magma d'arrivée du morphisme $(F, \diamond)$ est muni de façon sous-jacente d'une relation d'équivalence $\mathcal{S}$ que l'on note aussi $\equiv$, ses classes $\widehat{\cdot}$, compatible avec la loi de magma et l'on note χ le morphisme projection canonique.

Théorème. *(Théorème de factorisation carré pour les morphismes)*
Soit f un morphisme de E dans F. Alors f est compatible avec $\mathcal{R}$ au même sens que dans la section ensembliste si et seulement s'il existe un unique morphisme $\tilde{f}$ tel que $\chi \circ f = \tilde{f} \circ \pi$ (se qui se réécrit $\widehat{f(x)} = \tilde{f}(\overline{x})$ pour tout $x \in E$). Dans le cas de compatibilité, on dit encore qu'on passe au quotient dans f.

▷ C'est tout simplement la conjonction du théorème carré de factorisation pour les applications et du théorème de factorisation pour les morphismes. ■

$$\begin{array}{ccc} (E, *) & \xrightarrow{\quad f \quad} & (F, \diamond) \\ \pi \big\downarrow & & \big\downarrow \chi \\ (E/\mathcal{R}, \overline{*}) & \xrightarrow[\tilde{f}]{} & (F/\mathcal{S}, \overline{\diamond}) \end{array}$$

Le diagramme illustratif est similaire a ce qui a déjà été vu.

Exemple fondamental. Soient n, m deux entiers premiers entre eux et l'application

$$\begin{array}{rccc} f : & \mathbb{Z}/nm\mathbb{Z} & \longrightarrow & \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \\ & \overline{k}_{\equiv_{nm}} & \longmapsto & (\overline{k}_{\equiv_n}, \overline{k}_{\equiv_m}). \end{array}$$

On vérifie que c'est une bijection : en effet, par cardinalité, il suffit de montrer l'injectivité qui découle de la primalité relative de n et m. En réalité, nous devons montrer d'abord que f est bien définie, ce qui découle de la compatibilité de f avec la congruence modulo mn : en effet, si $k \equiv k' \ [nm]$, $k = k' + qnm$ donc $k \equiv k' \ [n]$ et $k \equiv k' \ [m]$ ce qui donne le même couple $f(k) = f(k') = (\overline{k}_{\equiv_n}, \overline{k}_{\equiv_m}) = (\overline{k'}_{\equiv_n}, \overline{k'}_{\equiv_m})$. De plus, l'application quotient est encore un morphisme donc l'application f est un isomorphisme, ce qui constitue le théorème chinois. Pour titre de compréhension, la relation $\mathcal{S}$ en reprenant les notations précédentes, qui n'intervient pas dans aucune hypothèse, est la relation produit $\equiv_n \times \equiv_m$ sur $\mathbb{Z}^2$ le groupe produit[4].

Ce n'est pas parce qu'on établit l'existence d'un isomorphisme qu'il faut confondre cet exemple avec le théorème d'isomorphisme qui suit !

Théorème. *(Théorème d'isomorphisme pour les magmas)*

Soit f une application de $(E, *)$ dans $(F, \diamond)$ deux magmas quelconques. On considère la relation d'équivalence $\mathcal{R}$ sur E définie par $x \sim y \Leftrightarrow f(x) = f(y)$. Dans ce cas, f est compatible avec $\mathcal{R}$, $(\mathrm{Im}(f), \diamond)$ est un magma et l'application quotient de f par cette relation réalise un isomorphisme de $(E/\mathcal{R}, \overline{*})$ sur $(\mathrm{Im}(f), \diamond)$.

▷ Il n'y a pas grand-chose à faire. Précisons toutefois pour être rigoureux :

- La compatibilité de l'application f avec la relation d'équivalence des fibres a déjà été établie dans le théorème de bijection quotient. On se rappelle son extrême trivialité.
- Le théorème de bijection quotient établit que l'application quotient est une bijection sur $\mathrm{Im}(f)$.
- La bijection quotient est un morphisme d'après le théorème de factorisation pour les morphismes (de magmas).
- Il faut seulement montrer que $(\mathrm{Im}(f), \diamond)$ est un magma, c'est-à-dire que la partie $\mathrm{Im}(f)$ est stable sous la loi $\diamond$ dont on note la restriction à $\mathrm{Im}(f) \times \mathrm{Im}(f)$ de la même manière abusivement. C'est facile : si $y, y' \in \mathrm{Im}(f)$, $y = f(x)$ et $y' = f(x')$ et f est un morphisme donc $f(x * x') = f(x) \diamond f(x') = y \diamond y' \in \mathrm{Im}(f)$, car $x * x' \in E$, $(E, *)$ étant stable par $*$ en tant que magma.

Ainsi $\tilde{f}$ est un isomorphisme de magmas de $(E/\mathcal{R}, \overline{*})$ dans $(\mathrm{Im}(f), \diamond)$. ■

$$\begin{array}{ccc} (E, *) & \xrightarrow{\quad f \quad} & \mathrm{Im}(f) \\ {\scriptstyle \pi}\downarrow & \nearrow_{\tilde{f}} & \\ (E/\mathcal{R}, \overline{*}) & & \end{array}$$

D'après la propriété d'héritage de la structure de monoïde et de groupe, on établit les deux mêmes théorèmes pour des monoïdes et des groupes. Il est en fait un peu moins trivial de les vérifier pour des morphismes de monoïdes, qui sont définis non seulement par la préservation de la loi mais aussi par l'image du neutre qui doit être le neutre d'arrivée, ce qui n'est pas automatique comme dans le cas connu des morphismes de groupe.

Exercice 26

1. Énoncer et justifier ces trois derniers théorèmes pour des groupes.

2. Énoncer et justifier ces trois derniers théorèmes pour des monoïdes.

[4] On laisse le soin au lecteur de se rendre compte à partir de la définition pourquoi le produit de deux relations sur un produit cartésien est une relation (*ouf*, murmure le SQL).

Principe. *(Théorèmes de factorisation)*

Le phénomène général est celui-ci : étant donné une structure aussi munie d'une relation d'équivalence, si la structure quotientée est également structurée (compatibilité de la structure avec la relation d'équivalence), alors un morphisme quotient partant de cette structure est compatible avec la relation d'équivalence si et seulement s'il se quotiente en morphisme.

Principe. *(Théorèmes d'isomorphisme)*

Étant donné une structure, étant donné un morphisme quelconque partant de cette structure, son image, qui a systématiquement la même structure, est isomorphe à la structure quotient par la relation d'équivalence des fibres (sa structuration étant systématique).

2.3 Groupes

L'austérité de la section précédente doit s'effacer devant une partie plus sexy sur les quotients de groupe. On doit introduire d'abord la notion adjacente de sous-groupe distingué, aussi appelé sous-groupe normal. On rappelle aussi cette propriété claire de la partie précédente :

Propriété. *(Groupe quotient)*

Si $(G, \times)$ est un groupe, $\mathcal{R}$ une relation d'équivalence sur G compatible avec $\times$, alors $G/\mathcal{R}$ muni de la loi quotient est un groupe d'élément neutre $\overline{e}$; si $x \in G$, $\overline{x}^{-1} = \overline{x^{-1}}$.

▷ On pouvait voir aussi que le quotient est l'image d'un groupe π, surjective, qui est un morphisme de magmas. ■

2.3.1 Distinction de sous-groupes

2.3.1.1 Notion de distinction ou normalité

On introduit une relation d'équivalence dans les groupes, très utile, liée au concept de conjugaison : deux éléments a et b d'un groupe sont dits *conjugués* s'il existe g dans ce groupe tel que $gag^{-1} = b$, ou autrement dit $ga = bg$. Pour toute la suite, on se fixe $(G, \times)$ un groupe, non nécessairement commutatif. Soit H un sous-groupe de G muni de sa loi induite.

Propriété. *(Classes à gauches, classes à droite)*

Les relations $\sim_d$ et $\sim_g$ définies sur G par $a \sim_g b \Leftrightarrow a^{-1}b \in H \Leftrightarrow b \in aH$ et $a \sim_d b \Leftrightarrow ba^{-1} \in H \Leftrightarrow b \in Ha$ sont deux relations d'équivalences. Leurs classes sont respectivement appelées *classes à gauche modulo* H et *classes à droite modulo* H.

▷ Facile (le faire !). ■

⟶ **Remarque.** On ne considère plus que les classes à gauche, quitte à considérer le groupe opposé : $(G, \times')$ où pour tous $x, y \in G$, $x \times' y = y \times x$. La relation d'équivalence des classes à droite pour le groupe G est alors celle des classes à gauche sur son groupe opposé. Cette relation d'équivalence, on pourra appeler systématiquement *relation d'équivalence des classes à gauche*, l'autre, *relation d'équivalence des classes à droite*. Lorsque les classes à gauche et les classes à droite coïncident, on dira tout simplement *classes*, ce dont on va voir que cela correspond exactement au cas où le sous-groupe modulo est distingué. Ce n'est pas la même relation que la conjugaison évoquée plus haut.

Exercice 27

1. Montrer que toutes les classes à gauche par H sont équipotentes à H.

2. *(Théorème de Lagrange)* On suppose G fini. Montrer que $\mathrm{card}(H)$ divise $\mathrm{card}(G)$. *La quantité* $\frac{\mathrm{card}(G)}{\mathrm{card}(H)}$*, notée* $[G : H]$*, est appelée indice de* H *dans* G *; elle peut être définie même si le groupe n'est pas fini.*

Exercice 28

Soit $(u_n)_{n\in\mathbb{N}}$ une suite dans un espace métrique et p un entier naturel. Justifier de deux manières que $(u_n)_{n\in\mathbb{N}}$ converge si et seulement si pour tout $k \in [\![0, p-1]\!]$, les $(u_{np+k})_{n\in\mathbb{N}}$ convergent vers la même limite.

Avant de poursuivre, il est conseillé de reprendre la notion succincte de compatibilité latérale.

Propriété. *(Caractérisation des relations d'équivalence compatibles à gauche avec les lois de groupe)*

La relation d'équivalence des classes à gauche est compatible à gauche avec la loi de groupe $\times$. Réciproquement, toute relation d'équivalence compatible avec elle est une relation de classes à gauche modulo un certain sous-groupe.

▷ On fait systématiquement l'abus de ne pas préciser les lois de groupe, puisqu'il n'y en a qu'une et ses restrictions. Soit G un groupe et H un sous-groupe, $\sim$ la relation d'équivalence des classes à gauche. Montrons qu'elle est compatible à gauche : soient x, y, y' dans G tels que $y \sim y'$, et montrons $xy \sim xy'$. L'hypothèse se récrit $y^{-1}y' \in H$, et montrons $(xy)^{-1}xy' \in H$, soit $y^{-1}x^{-1}xy' \in H$ par inverse d'un produit ; ces notations sont univoques par associativité. Or $x^{-1}x = e$ donc cela revient à montrer $y^{-1}y' \in H$, ce qui exactement l'hypothèse, donc c'est immédiat.

Réciproquement, soit $\sim$ une relation d'équivalence sur G compatible à gauche avec la loi de groupe. On pose $H = \overline{e}$ comme on s'y attend. Dans ce cas, $a \sim b \iff a^{-1}a \sim a^{-1}b \iff e \sim a^{-1}b \iff a^{-1}b \in \overline{e} \iff a^{-1}b \in H$; justifions la première équivalence : le sens direct est la compatibilité à gauche, le sens réciproque est la régularité dans le groupe G. Enfin, il faut vérifier que H est bien un

sous-groupe (et oui, petit scarabée). Il contient le neutre par réflexivité, il est stable par circularité de $\sim$ (conjonction de la transitivité et de la symétrie) et stable par passage à l'inverse, car si $x \in H$, $\overline{x} = \overline{e}$ et l'on a justifié que $\overline{x^{-1}} = \overline{e^{-1}} = \overline{e}$ soit $x^{-1} \in H$. ■

Exercice 29

Donner un exemple de groupe et de sous-groupe où les classes à gauche et les classes à droite ne coïncident pas.

⟶ **Notation.** Étant donné une relation d'équivalence G compatible avec la loi de groupe, on note H le sous-groupe dont elle est relation d'équivalence des classes à gauche ; il existe toujours d'après ce qui précède. On note alors G/H le groupe quotient de G par ladite relation. Pour les classes à droite, ce qui consiste à remplacer par le mot *droite* toutes les occurrences de *gauche* dans le théorème précédent, on note $H \setminus G$.

Exercice 30

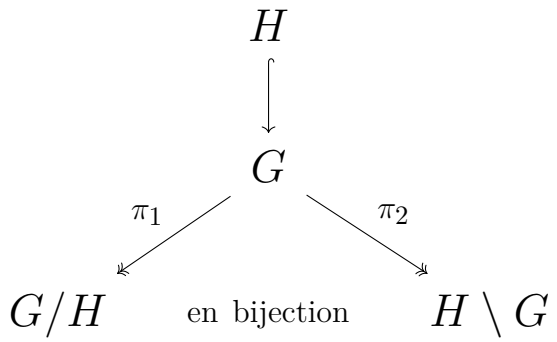
Cette notation est-elle raisonnable ?

Propriété. *(Dénombrement des classes à gauche et à droite)*

Pour tout groupe G, pour tout sous-groupe H de G, G/H et $H \setminus G$ ont le même cardinal.

▷ La bijection à exhiber est celle qui à une partie de G, associe la partie composée des inverses d'éléments de G : $X \longmapsto X^{-1} = \{x^{-1} \mid x \in X\}$. ■

Pour l'instant, on dispose seulement du schéma suivant :



L'injection de H dans G est canonique, car c'est même une inclusion.

Exercice 31

1. Montrer que pour tout $a \in G$, $aH = H$ si et seulement si $a \in H$.

2. Montrer que pour tous $a, b \in G$, $aH = bH$ si et seulement si $aH \subseteq bH$ et que cette condition est elle-même équivalente à l'équivalence de a et b.

3. Montrer que pour tous $a, b \in G$, $aH = Hb$ si et seulement si $aH \subseteq Hb$. Cette condition est elle équivalente à l'équivalence de a et b ?

L'origine des classes à gauche et classes à droite

La théorie des groupes est élaborée en grande partie dans la première moitié du XIX^e siècle par Évariste Galois, mathématicien français, élève au lycée Louis-le-Grand, deux fois emprisonné, mort en 1832 à vingt ans à la suite d'un duel causé par « une infâme coquette ». La veille, le 29 mai, il écrit un lettre adressée à Auguste Chevalier qui constitue son testament mathématique. Il lui demande en fin d'article : « Tu prieras publiquement Jacobi ou Gauss de donner leur avis, non sur la vérité mais sur l'importance des théorèmes. » Dans cette lettre, centrée sur la résolution des équations, il écrit :

> *Dans les deux cas, le groupe de l'équation se partage par l'adjonction en groupes tels, que l'on passe de l'un à l'autre par une même substitution ; mais la condition que ces groupes aient les mêmes substitutions n'a lieu certainement que dans le second cas. Cela s'appelle la décomposition propre.*
>
> *En d'autre termes, quand un groupe G en contient un autre H, le groupe G peut se partager en groupes, que l'on obtient chacun en opérant sur les permutations de H une même substitution ; en sorte que*
>
> $$G = H + HS + HS' + ...$$
>
> *Et aussi il peut se décomposer en groupes qui ont tous les mêmes substitutions, en sorte que*
>
> $$G = H + TH + T'H + ...$$
>
> *Ces deux genres de composition ne coïncident pas ordinairement. Quand ils coïncident, la décomposition est dite* propre.[5]

On introduit maintenant la terminologie fondamentale de cette partie.

[5] Et l'on voit combien le groupe Bourbaki a apporté au formalisme mathématique dans les années 1940.

Définition. *(Sous-groupe normal, sous-groupe distingué)*

Un sous-groupe H du groupe G est dit *normal*, ou *distingué*, ou *invariant*, s'il est stable par automorphismes intérieurs (ou actions par conjugaison, pour tous les élements de G). On note alors $H \triangleleft G$.

Remarques.

1. Par définition, $H \triangleleft G \Leftrightarrow \forall a \in G\ aHa^{-1} \subseteq H$, ou ce qui est équivalent (dire pourquoi), $a^{-1}Ha \subseteq H$.
2. On dit sous-groupe normal, ou sous-groupe distingué de façon tout à fait indistincte, comme on dit abélien et commutatif indifféremment. On dit plutôt *invariant* dans la théorie des représentations.

Propriété. *(Caractérisations des sous-groupes normaux)*

Les conditions suivantes sont équivalentes :
(i) $H \triangleleft G$;
(ii) pour tout $a \in G$, $aHa^{-1} = H$ (H est son seul conjugué) ;
(iii) pour tout $a \in G$, $a^{-1}Ha = H$;
(iv) pour tout $a \in G$, $aH = Ha$;
(v) $\sim_d = \sim_g$;
(vi) la relation d'équivalence des classes à gauche modulo H est compatible avec la loi de groupe de G ;
(vii) il existe une loi $\diamond$ définie sur G/H telle que pour tous $a, b \in G$, $aH \diamond bH = (ab)H$.

▷ Les conditions *(ii)* et *(iii)* sont équivalentes, comme on a demandé au lecteur de le justifier précédemment. Cela vient de ce que $G = \{a^{-1} \mid a \in G\}$, la symétrisation étant une permutation dans un groupe. On établit facilement par double inclusion l'équivalence entre *(ii)* et *(iv)*. Pour établir l'équivalence de *(i)* et *(ii)*, il suffit de montrer l'implication $aHa^{-1} \subseteq H \Rightarrow aHa^{-1} = H$ pour tout a dans G. Elle est bien vraie, car l'inclusion $H \subseteq aHa^{-1}$ est toujours vraie si $aHa^{-1} \subseteq H$; en effet, si $h \in H$, alors cette hypothèse appliqué à a^{-1} donne $a^{-1}ha \in H$. On pose donc $h' = a^{-1}ha$ et dans ce cas $h = ah'a^{-1} \in aHa^{-1}$ (avouons qu'il faut avoir la tête reposée).

Les conditions *(v)* et *(vi)* sont équivalentes. En effet, si $\sim_d = \sim_g$, alors $\sim_g$ est compatible à gauche en tant que relation de classes à gauche mais également à droite puisqu'elle égale $\sim_d$; elle est donc compatible. Réciproquement, si $\sim_g$ est compatible, elle est compatible à droite et l'on peut prendre un sous-groupe H' dont elle est relation modulo à droite. Or on a vu dans la preuve que H' était la classe du neutre, et le neutre à gauche égale le neutre à droite dans un groupe, donc $H = H'$. D'autre part, l'équivalence *(vi)* $\Leftrightarrow$ *(vii)* est l'expression du théorème de factorisation : on a vu que l'unicité de la loi quotient était superfétatoire dans l'équivalence, et l'identité $aH \diamond bH = (ab)H$ exprime que la projection est un morphisme.

Il ne reste plus qu'à faire le lien entre ces deux groupes de propositions équivalentes. On le

fait par *(iv)* $\Leftrightarrow$ *(v)*. Si les classes à gauche égalent les classes à droite pour le même élément, la partition par les classes à gauche et les classes à droite est la même, et donc définit la même relation d'équivalence, soit $\sim_d = \sim_g$. Réciproquement, si $\sim_d = \sim_g$ et $a \in G$, $aH = \overline{a}_{\sim_g} = \overline{a}_{\sim_d} = Ha$. ■

Remarque. Pour la loi $\diamond$, on a alors également pour tous $a, b \in G$,

$$aH \diamond bH = \{x \times y \mid x \in aH, y \in bH\} \ .$$

C'est très commode. Le lecteur avancé pourra remarquer que les classes à gauche sont aussi les orbites pour l'action de translation à droite de H sur G. Comme on appelle parfois *transversale* un système de représentants, une *transversale d'un sous-groupe* est une transversale de la relation d'équivalence des classes à gauche.

▷ Il faut et suffit donc de montrer : pour tous $a, b \in G$, $(ab)H = \{ahbh' \mid h, h' \in H\}$. Puisque H est distingué dans G, $Hb = bH$ donc cet ensemble se récrit $\{abhh' \mid h, h' \in H\}$. Or on vérifier par double inclusion facile que $H = \{hh' \,|h, h' \in H\}$ (l'une est la stabilité magmatique, l'autre la présence du neutre) et l'on peut récrire cet ensemble $(ab)H$, ce que l'on voulait. ■

Mise au point. Nous avons montré que les relations d'équivalences compatibles avoir la loi dans le cas des groupes étaient celles définies par classes modulo un sous-groupe, ce qui est spécifique à la catégorie des groupes et permet de reformuler les théorèmes de quotient. Avec la caractérisation précédente, on montre que la relation d'équivalence de classes à gauche est compatible si et seulement si le sous-groupe considéré est distingué. La conjonction de ses deux résultats permet de réduire l'étude des groupes quotients à celle des quotients par sous-groupes distingués. Étant donné $H \lhd G$, G/H est donc un groupe muni de la loi quotient et la projection canonique est un morphisme de groupes (et si H n'est pas normal, ces deux dernières propositions sont aussi infirmées).

Le schéma triangulaire de tout à l'heure peut donc se simplifier, mais dans le cas seul des sous-groupes distingués :

$$H \overset{\lhd}{\hookrightarrow} G \overset{\pi}{\twoheadrightarrow} G/H = H \setminus G$$

2.3.1.2 Sous-groupes distingués classiques et théorèmes opératoires

Exemples. Les quelques propriétés suivantes, quoique capitales, ne sont pas essentielles. On peut donc se référer au chapeau de la section suivante sur les groupes quotients pour se clarifier l'esprit.

Les **sous-groupes triviaux sont distingués** dans G. On peut donc noter $\{e\} \lhd G$ et $G \lhd G$. Les relations d'équivalence des classes latérales (classes à gauches, classes à droite) sont donc compatibles avec la loi de groupe, mais c'était facilement prévisibles, car ce sont res-

pectivement (le re-vérifier) la relation d'égalité et la relation pleine, c'est-à-dire pour laquelle tous les points du groupe sont en relation.

On en déduit que $G/G = \{G\}$ et que $G/\{e\} = \{\{g\} \mid g \in G\}$. Si l'on avait choisi de représenter les ensembles quotients par des systèmes de représentants (*confer* la remarque associée), on aurait eu $G/\{e\} = G$. Dans les deux cas, $[G : G] = \mathrm{card}(G)$ et $[G : \{e\}] = 1$.

Un **sous-groupe caractéristique** est un sous-groupe qui soit un point fixe de l'action canonique de Aut(G) sur G (voir section sur les actions de groupe plus bas), autrement dit un sous-groupe stable par tout automorphisme de G. Puisque les automorphismes intérieurs sont des automorphismes, tout sous-groupe caractéristique est distingué. De surcroît, on peut aisément se convaincre que tout sous-groupe caractéristique d'un sous-groupe normal est normal dans l'absolu. La caractérisation est bien sûr transitive pour l'inclusion des sous-groupes.

Exercice 32

On considère Φ l'ensemble des sous-groupes de G et la relation $\triangleleft$ définie sur Φ. Montrer que c'est un relation réflexive antisymétrique partielle. Quelle est sa clôture transitive ? Est-ce un ordre total ?

Propriété. *(Intercalation de distinction)*
Soient K un sous-groupe de H un sous-groupe de G. Si $K \triangleleft G$, alors $K \triangleleft H$.

▷ C'est une simple manipulation de la définition. ■

On donnera davantage de théorèmes d'opérations, qui sont peu nombreux. Pour l'instant, on peut retenir que **la distinction n'est pas transitive** mais que **tout sous-groupe intermédiaire dans une relation de distinction en induit une**. De plus, la distinction ne s'étend pas : en général, si $K \triangleleft H$, on n'a pas $K \triangleleft G$ (contre-exemple classique : $\{id, (1,2)(3,4)\}$,$\mathfrak{A}_4$, $\mathfrak{S}_4$).

Propriété. *(Sous-groupes distingués d'un groupe commutatif)*
Tout sous-groupe d'une groupe commutatif est distingué dans ce groupe.

▷ La relation d'équivalence des classes à gauche a la même expression que celle des classes à droite, ce qui permet d'utiliser la caractérisation $\sim_d = \sim_g$. ■

Cette remarque ne rend pas caduque la notion de groupe quotient dans le cas commutatif, mais elle la simplifie considérablement : tous les sous-groupes sont des sous-groupes distingués ce qui permet de définir systématiquement la relation d'équivalence modulo ce sous-groupe de façon univoque. De plus, on avait que les compatibilités opératoires sont équivalentes aux compatibilités latérales, et de toute façon vraies par distinction.

Exemple. On considère le groupe $(\mathbb{Z}, +)$. Soit $n \in \mathbb{N}$, alors $n\mathbb{Z}$ est un sous-groupe additif de $\mathbb{Z}$. De plus, $n\mathbb{Z} \triangleleft \mathbb{Z}$ automatiquement puisque $(\mathbb{Z}, +)$ est commutatif. On peut donc définir le groupe quotient $\mathbb{Z}/n\mathbb{Z}$ de façon unique ; une classe (à gauche, mais le concept est exactement le même qu'à droite par commutativité) selon $n\mathbb{Z}$ est un élément de la forme $k+n\mathbb{Z}$ où $k \in \mathbb{Z}$, ce qui correspond bien aux classes de congruences déjà connues et à la description du cours : $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, ..., \overline{n-1}\}$. Ne pas confondre la notation $n\mathbb{Z}$, qui correspond au « H » des développements précédents, et le $k+H$ qui correspond au « aH » mais en notation additive.

Exercice 33

On appelle *groupe de Dedekind* un groupe dans lequel tout sous-groupe est distingué. On appelle *groupe hamiltonien* un groupe de Dedekind non abélien.

1. Pourquoi introduire le concept de groupe hamiltonien ?

2. Montrer que le groupe des quaternions $Q = \{1, -1, i, -i, j, -j, k, -k\}$, où les quatre premiers sont complexes et $i^2 = j^2 = k^2 = ijk = -1$, est hamiltonien.

Certains sous-groupes classiques généralement définis dans les groupes sont automatiquement distingués. On en voit quelques-uns.

Propriété. *(Distinction des centres)*
Le centre d'un groupe en est un sous-groupe distingué[1].

▷ On peut plus fortement montrer qu'il est caractéristique. Le centre du groupe G est $\mathcal{Z}(G) = \{x \in G \ \ \forall g \in G \ gx = xg\} = \{x \in G \ \ \forall g \in G \ gx = xg\}$, l'ensemble des éléments du groupe qui commutent avec tous les autres ; on laisse au lecteur le soin de montrer que c'est bien un sous-groupe de G. Soit $\phi \in \mathrm{Aut}(G)$. Soit $x \in \mathcal{Z}(G)$. Soit $g \in G$. $g\phi(x)g^{-1} = \phi(t)\phi(x)\phi(t^{-1})$, car ϕ est un automorphisme donc surjectif. Par morphisme, on le récrit $g\phi(x)g^{-1} = \phi(txt^{-1}) = \phi(x)$, car x est central, ce qui conclut. ■

Propriété. *(Distinction des cœurs)*
Le cœur d'un sous-groupe d'un groupe est un sous-groupe distingué de ce dernier.

▷ Pour un sous-groupe H de G, son cœur dans G est $cr_G(H) = H_G = \bigcap_{g \in G} gHg^{-1}$; on laisse au lecteur le soin de montrer que c'est bien un sous-groupe de G. Il est contenu dans H, car cette intersection est contenue dans son terme pour $g = e$ qui est H. Montrons maintenant la distinction dans G, dont découle par ailleurs la distinction dans H. Soit $a \in H$. Alors : $aH_Ga^{-1} = a \bigcap_{g \in G} gHg^{-1}a^{-1} = \{ata^{-1} \mid t \in \bigcap_{g \in G} gHg^{-1}\} = \{ata^{-1} \mid t \in G, \forall g \in G \ t \in gHg^{-1}\} = \{ata^{-1} \mid t \in G, \forall g \in G \ t \in agHg^{-1}a^{-1}\} = \{t \in G \mid \forall g \in G \ t \in gHg^{-1}\} = \bigcap_{g \in G} gHg^{-1}$. L'avant-dernière

[6] Ou, plus généralement, tout sous-groupe du centre d'un groupe est distingué. Dans la même veine : le centralisateur d'un sous-groupe en est un sous-groupe distingué.

égalité vient de ce que $(g \longmapsto ag) \in S(G)$. Ainsi $H_G \lhd G$. ■

On peut définir plus généralement le cœur d'une partie d'un groupe. Le cœur d'un sous-groupe est doté de propriétés encore meilleures[7]. Enfin, un exemple de haute importance, puisqu'on va voir dans la suite qu'il donne exactement les sous-groupes distingués. C'est par lui que nous formulerons en particulier le théorème de factorisation pour les groupes.

Propriété. *(Distinction des noyaux)*
Le noyau d'un morphisme de groupe est un sous-groupe distingué du groupe de départ.

▷ On le vérifie très aisément : si $x \in \mathrm{Ker}(f)$ un morphisme de G dans G' deux groupes quelconques, si $g \in G$, alors $f(gxg^{-1}) = f(g)f(x)f(g^{-1}) = f(g)e_{G'}f(g^{-1}) = f(g)f(g^{-1}) = f(gg^{-1}) = f(e_G) = e_{G'}$, donc $\mathrm{Ker}(f)$ est stable par automorphismes intérieurs soit $\mathrm{Ker}(f) \lhd G$. ■

Exemples fondamentaux.

1. On retrouve que les centres sont distingués en tant qu'intersection des noyaux de tous les automorphismes intérieurs de G.
2. $\mathcal{SL}_n(\mathbb{K}) = \mathrm{Ker}(\det) \lhd \mathcal{GL}_n(\mathbb{K})$ où $(\mathbb{K}, +, \times)$ est corps commutatif ; de même pour un espace vectoriel de dimension finie ;
3. $\mathcal{SO}_n = \mathrm{Ker}(\det) \lhd \mathcal{O}_n(\mathbb{R})$ (bien sûr le morphisme déterminant n'est plus défini sur le même groupe) ; de même pour un espace vectoriel réel de dimension finie ;
4. $SU_n = \mathrm{Ker}(\det) \lhd U(n)$; de même pour un espace vectoriel complexe de dimension finie ;
5. $\mathfrak{A}_n = \mathrm{Ker}(\varepsilon) \lhd \mathfrak{S}_n$; de même pour les permutations d'un ensemble fini.

On se souvient que si K est un sous-groupe de H, et $K \lhd G$, alors $K \lhd H$. N'allez pas pourtant écrire que la première propriété découle de $\mathcal{SL}_n(\mathbb{K}) \lhd \mathfrak{M}_n(\mathbb{K})$, ce qui n'a aucun sens puisque $\mathfrak{M}_n(\mathbb{K})$ n'a pas de structure de groupe. Pour plus d'informations, appelez l'exercice de la section 4.1 sur le sujet.

On a cette dernière caractérisation des sous-groupes normaux, moins pratique, mais qui donne une première importance aux Ker parmi les sous-groupes.

[7] Quelques suppléments intéressants. D'abord, remarquons que le cœur d'un sous-groupe H de G contient tous les sous-groupes que H qui sont normaux dans G ; en effet, si K est un sous-groupe de H normal dans G, si $g \in G$, $K = gKg^{-1} \subseteq gHg^{-1}$ donc $K \subseteq H_G$. C'est donc le plus grand sous-groupe normal dans G contenu dans H au sens de l'inclusion.

Théorème. *(Structure du quotient par le cœur)*
Soit H un sous-groupe quelconque de G. Alors G/H_G est isomorphe à un sous-groupe de $S(G/H)$.

▷ G opère à gauche sur G/H par $(g, X) \longmapsto gX$. Le noyau de cette action est le cœur de H dans G. Ainsi, d'après le théorème de factorisation pour les groupes, son quotient est injectif. Sa co-restriction est donc un isomorphisme sur un sous-groupe de $S(G/H)$. ■

Propriété. *(Caractérisation de la normalité par noyaux)*
Un sous-groupe d'un groupe est distingué si et seulement si c'est le noyau d'un morphisme de groupes.

▷ On a déjà vu dans la propriété précédente la proposition réciproque. Soit maintenant $H \triangleleft G$. Alors le groupe quotient G/H est défini de manière univoque et c'est bien un groupe. On pose $\pi : G \longrightarrow G/H$ le morphisme projection canonique. Alors $\mathrm{Ker}(\pi) = \{x \in G \mid \pi(x) = \overline{x} = \overline{e}\} = \{x \in G \mid x \in \overline{e} = H\} = H$. ■

Exercice 34

(Groupe dérivé) On appelle *groupe dérivé* d'un groupe, le groupe engendré par les commutateurs d'éléments de G (on dit qu'un élément est commutateur s'il s'écrit sous la forme $aba^{-1}b^{-1}$ où $a, b \in G$). Montrer que le groupe dérivé est caractéristique et que c'est le plus petit sous-groupe normal au sens de l'inclusion pour lequel le groupe quotient est abélien. *Ce groupe quotient est appelé l'abélianisé de G.*

Pour clore cette partie, quelques théorèmes opératoires sur la normalité, dont on rappelle le caractère intrinsèque.

Exercice 35

Soit H sous-groupe normal de G. Donner un sous-groupe de H ni normal dans G, ni normal dans H.

Propriété. *(Intersection de sous-groupes normaux)*
Une intersection quelconque de sous-groupes normaux est sous-groupe normal.

▷ On considère G un groupe et $(G_i)_{i\in I}$ une famille quelconque de ses sous-groupes distingués. Il n'est pas forcé de distinguer le cas I vide, quoique évident. Soit $x \in \bigcap_{i\in I} G_i$. Soit $g \in G$. Pour tout $i \in I$, $x \in G_i$ donc $gxg^{-1} \in G_i$ par distinction de G_1 donc $gxg^{-1} \in \bigcap_{i\in I} G_i$ et c'est terminé. ■

Remarque. La borne inférieure pour l'ordre inclusif étant l'intersection, on peut donc définir le sous-groupe distingué engendré par une partie d'un groupe, comme l'intersection de tous les sous-groupes distingués contenant cette partie. C'est exactement le même raisonnement que pour un sous-groupe engendré, une tribu engendré, un sous-espace vectoriel engendré, l'adhérence d'une partie d'un espace topologique... Le phénomène général est seulement lié à la stabilité par intersection : si un truc est stable par intersection quelconque, alors on peut définir le truc engendré par un machin.

Exercice 36

Que dire d'une réunion de sous-groupes normaux ?

Propriété. *(Génération par des sous-groupes normaux)*
Un sous-groupe engendré par une famille quelconque de sous-groupes normaux est sous-groupe normal.

▷ Soit $(G_i)_{i\in I}$ une famille quelconque de groupes normaux dans G. Soit H le groupe généré par elle. Soit $x \in H : x = a_1...a_n$ avec les a_i dans les G_j. Si $g \in G$, $gxg^{-1} = ga_1...a_ng^{-1} = (ga_1g^{-1})(ga_2g^{-1})(ga_3...g^{-1})(ga_ng^{-1})$, car $gg^{-1} = e$. Or chacun des termes ainsi parenthésés de ce produit est dans l'un des G_j puisque ceux-ci sont normaux. Le produit est donc dans le groupe généré par eux, ce qui conclut. ■

Exercice 37
Que dire du produit direct de deux sous-groupes normaux ?

Exercice 38
Quel est le sous-groupe normal engendré par les $(i, i+2)$ dans $\mathfrak{S}_{2n+1}$?

Exercice 39
Montrer que si H_1, H_2 sont deux sous-groupes normaux de G, H_1H_2 est normal dans G. La normalité d'un seul suffit-elle ?

Propriété. *(Image directe d'un sous-groupe normal par un morphisme)*
Soient G, G' deux groupes munis de lois quelconques et f un morphisme de G dans G'. Si H est distingué dans G, alors $f(H)$ est $\boxed{\text{distingué dans } f(G)}$.

▷ Soit $y \in f(H)$, d'où $y = f(x), x \in G$ et $g \in f(G)$. Dans ce cas $g = f(t), t \in G$ et $g^{-1} = f(t^{-1}$. Alors $gyg^{-1} = f(t)f(x)f(t^{-1} = f(txt^{-1})$ par morphisme. Mais H est distingué dans G donc $txt^{-1} \in H$, d'où $gyg^{-1} \in f(H)$ ce qui termine la preuve. ■

Remarque. C'est faux si l'on remplace $f(G)$ par G' dans la proposition précédente. On laisse le lecteur faire l'effort fort formateur de produire un contre-exemple.

Propriété. *(Image réciproque d'un sous-groupe normal par un morphisme)*
Soient G, G' deux groupes munis de lois quelconques et f un morphisme de G dans G'. Si H est $\boxed{\text{distingué dans } f(G)}$, alors $f^{-1}(H)$ est distingué dans G.

▷ Soit $x \in f^{-1}(H')$. Soit $g \in G$. Alors $f(gxg^{-1}) = f(g)f(x)f(g^{-1})$ par morphisme. Mais $f(x) \in H'$ par hypothèse et $f(g) \in f(G)$ donc comme H' est normal dans $f(G)$, ce triple produit appartient encore à H'. ainsi $gxg^{-1} \in f^{-1}(H')$, ce qui termine la preuve. ■

Exercice 40

Montrer que pour tout $n \in \mathbb{N}^*$, un groupe de type fini, c'est-à-dire généré par une partie finie, n'a qu'un nombre fini de sous-groupes normaux d'indice n.

Propriété. *(Distinction par un conjugué du sous-groupe)*
Soit H un sous-groupe de G. H est distingué dans G si et seulement l'un de ses conjugués est distingué dans G.

▷ Et même si et seulement si tous ses conjugués sont distingués dans G. (Un conjugué d'un sous-groupe H est un sous-groupe gHg^{-1}, parfois noté H^g, pour un élément g de G donné.) En effet, on traite l'équivalence en se rappelant la caractérisation : un sous-groupe est distingué si et seulement s'il est son seul conjugué. De plus, H fait partie de ses conjugués par l'action de e. ■

Exercice 41

On appelle *sous-groupe normal minimal*, un élément minimal pour l'inclusion de l'ensemble des sous-groupes normaux non triviaux de G. On rappelle qu'un élément minimal d'un ensemble ordonnée $(E, \leq)$ est un élément m tel que $\forall x \in E\ (x \leq m \Rightarrow x = m)$. Montrer que tout groupe fini non trivial admet au moins un sous-groupe normal minimal. Que dire dans un groupe quelconque ? Discuter le cas des sous-groupes normaux maximaux.

2.3.2 Groupes quotients

On peut, avec toutes les considérations précédentes, fixer les notations du cadre le plus général possible : on prend $(G, \times)$ un groupe et H un sous-groupe distingué dans G. On note $\mathcal{R}$ la relation d'équivalence des classes à gauche modulo H, aussi notée $\equiv$ et appelée congruence modulo H ; dans ce cas, $G/\mathcal{R} = G/H$, et c'est le même ensemble si l'on avait pris les classes à droite, ce qui permet de noter aussi $\overline{G}$ ou $\frac{G}{H}$. De plus, la projection canonique π est un morphisme d'après la section précédente sur les magmas. Muni de la loi quotient, que l'on note multiplicativement, G/H a la structure de groupe. Son élément neutre est $\overline{e} = eH = H$ et si aH est un élément de G/H, où l'on a pris $a \in G$, son inverse est $a^{-1}H$: on peut le reformuler en voyant que $a^{-1}H \cdot aH = (aa^{-1})H = eH = H$ et de même $aH \cdot a^{-1}H = H$. Enfin, ce cadre est justifié par ce qu'il n'existe de groupe quotient (pour lequel la projection canonique soit quotient, ce que l'on veut à chaque fois) que si la relation d'équivalence considérée est compatible avec la loi de groupe, et ces relations sont exactement les relations de classes, indifféremment prises à gauche ou à droite, modulo les sous-groupes distingués.

Exercice 42

Test : quelles sont les parties X de G telles que G/X, muni de la loi quotient, soit un groupe ?

Pour clarté mentale, on énonce le théorème de factorisation établi plus haut en exercice avec sa formulation nouvelle.

Propriété. *(Théorème de factorisation pour les groupes, version mal dite)*
Soit f un morphisme de groupes de G dans G' un autre groupe quelconque muni d'une loi passée sous silence. Alors l'application f est compatible avec la congruence modulo H si et seulement s'il existe un unique morphisme $\tilde{f}$ tel que $f = \tilde{f} \circ \pi$ (se qui se réécrit $f(g) = \tilde{f}(\overline{g})$ pour tout $g \in G$). Dans ce cas de compatibilité, on dit toujours qu'on *passe au quotient* dans le morphisme f.

▷ Normalement, c'est déjà fait. ■

$$\begin{array}{ccccc} (H,\times) & \xhookrightarrow{\triangleleft} & (G,\times) & \xrightarrow{f} & (G',\times') \\ \pi' \big\downarrow & & \pi \big\downarrow & \nearrow_{\tilde{f}} & \\ (\{H\},\overline{\times}) & \xhookrightarrow[\triangleleft]{} & (G/H,\overline{\times}) & & \end{array}$$

Dans le diagramme ci-dessous, l'application π', inutile, est la restriction à H de π. Elle est donc constamment égale à $H = \overline{e} = \overline{h}$ pour tout $h \in H$. Le groupe en bas à gauche est distingué dans le groupe quotient puisque c'est son sous-groupe trivial.

Exercice 43
(Insolite) π' peut-elle être la dérivée de π ?

Propriété. Si G est un groupe abélien et $H \triangleleft G$, G/H est abélien.

▷ C'est une conséquence directe de l'expression de la loi quotient établie en remarque précédemment : pour tous $a, b \in G$, $aH \cdot bH = (ab)H = (ba)H = bH \cdot aH$. ■

Propriété. *(Monogénéité du groupe quotient)*
Si G est un groupe monogène et $H \triangleleft G$, G/H est monogène.

▷ Il s'agit simplement de remarquer que le caractère de générateur est conservé par passage à la structure quotient ; c'est au lecteur de le vérifier. ■

Remarque. Plus généralement : si g génère G, $\overline{g}$ génère G/H ; si G est généré par A, G/H est généré par $\pi(A)$; en particulier, si G est de type fini, G/H également.

Propriété. *(Cyclicité du groupe quotient)*
Si G est un groupe cyclique et $H \triangleleft G$, G/H est cyclique.

▷ Puisqu'un groupe est cyclique si et seulement s'il est monogène et fini, par rapport à la propriété précédente, il n'y a qu'à justifier que le groupe quotient est également fini si G est fini. C'est le cas, par surjectivité de la projection canonique, $\text{card}(G/H) \leqslant \text{card}(G) < \infty$. ■

Remarque. Plus généralement : si G est fini, G/H est fini, de cardinal inférieur. Peut-être doit-on rappeler que, dans tous les cas, fondamentalement, $\text{card}(E/\mathcal{R}) \leqslant \text{card}(E)$, et donc si E est fini, tout quotient de E est également fini. De plus, il y a égalité des cardinaux, dans le cas fini, si et seulement si $\mathcal{R}$ est l'égalité de E.

Théorème. *(Commutativité d'un groupe quotient)*
Un groupe quotient selon un groupe distingué est commutatif si et seulement si celui-ci contient tous les commutateurs.

▷ Voir l'exercice sur les groupes dérivés de la partie précédente. ■

Exercice 44

Soit $n \neq 4$. Quels sont les sous-groupes distingués des $\mathfrak{S}_n$?

Après ces quelques remarques structurelles, il est temps de passer aux choses sérieuses. On introduit un groupe $(G', *)$.

Théorème. *(Théorème de factorisation pour les groupes)*
Soit f un morphisme de groupes de G dans G'. H est dans $\text{Ker}(f)$ si et seulement s'il existe un unique morphisme $\tilde{f}$ tel que $f = \tilde{f} \circ \pi$ (se qui se réécrit $f(g) = \tilde{f}(\overline{g})$ pour tout $g \in G$).

▷ D'abord, la condition $H \subseteq \text{Ker}(f)$ équivaut à la compatibilité de f avec la relation d'équivalence des classes à gauche, c'est-à-dire : $\forall a, b \in G \quad a^{-1}b \in H \Rightarrow f(a) = f(b)$. En effet, si f est un morphisme, $\forall x \in H \Rightarrow \text{Ker}(f) \Leftrightarrow \forall a^{-1}b \in H \ f(a^{-1}b) = e_{G'}$: les éléments de H sont exactement les éléments de la forme $a^{-1}b$ qui sont dans H, équivalence logique qui se montre aisément comme on a déjà pu le faire, et $f(a^{-1}b) = e_{G'} \Leftrightarrow f(a)^{-1}f(b) = e_{G'} \Leftrightarrow f(a) = f(b)$. C'est donc une reformulation du théorème de factorisation. ■

Exercice 45

Donner un exemple de cas où un sous-groupe distingué n'est pas inclus dans le noyau.

Exercice 46

Peut-on trouver un contre-exemple où le sous-groupe n'est pas distingué, et où il y aurait factorisation sans inclusion dans le noyau ?

Exercice 47

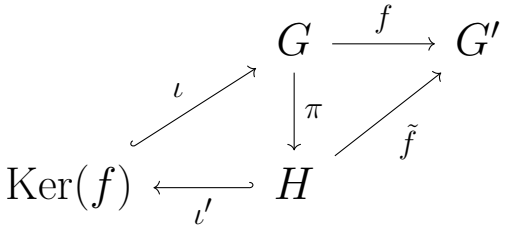
Dans le théorème précédent, montrer que :

1. $\tilde{f}$ est injective si et seulement si $H = \mathrm{Ker}(f)$;

2. $\tilde{f}$ est surjective si et seulement si f est surjective ;

3. $\tilde{f}$ est un isomorphisme si et seulement si f est surjective et $H = \mathrm{Ker}(f)$.

Une illustration du théorème de factorisation.



Méthode. Recette pour passer au quotient dans les morphismes de groupes

1. Je vérifie que je dispose de deux groupes G, G', d'un morphisme f entre les deux, et d'un sous-groupe H du groupe de départ G.

2. Je vérifie que H est distingué dans G. J'en déduis cette affirmation, que le quotient existe dans toute sa splendeur d'ensemble quotient univoquement défini par une relation de congruence et a la structure de groupe.

3. Je vérifie maintenant que H est inclus dans $\mathrm{Ker}(f)$. Si je veux, pour crâner, je précise que c'est une condition nécessaire et suffisante à la compatibilité de f avec la congruence, car je connais même la preuve de mon théorème de factorisation sur les groupes.

4. Je peux maintenant définir un morphisme $= \tilde{f} : G/H \longrightarrow G'$ sans trouble, telle que pour tout $\overline{g} \in G/H$, $\tilde{f}(\overline{g}) = f(g)$, et j'insiste bien sur ce que cette construction n'est possible que grâce aux deux hypothèses vérifiées précédemment.

Si je veux une propriété d'injectivité, de surjectivité, voire de bijectivité pour mon application, je me réfère aux résultats habituels que nous avons déjà vus.

Exercice 48

Expliquer pourquoi, pour tout morphisme d'un groupe G dans un groupe abélien G', on peut le factoriser en un morphisme de l'abélianisé de G dans G'.

Exercice 49

(Rigolo) Soient H, K deux sous-groupes d'un groupe. Montrer que $HK = KH$ si et seulement si $H = K$ ou $H = -K$.

Maintenant, nous énonçons les trois théorèmes d'isomorphisme pour les groupes qui sont l'adaptation du théorème d'isomorphisme pour la structure magmatique, dont découle ensuite deux corollaires. On peut avoir à l'esprit que c'en sont toujours des cas particuliers.

Avec eux, nous retrouvons des « règles de calcul », avec lesquelles il faut bien sûr être toujours très prudent de ne pas écrire d'absurdités, mais qui rendent la notion de quotient bien plus intuitive qu'elle ne l'a été depuis une vingtaine de pages : on fait le quotient de groupes par des groupes, même si ce doivent être des sous-groupes, et distingués, et ils présentent des isomorphismes à la place des identités algébriques élémentaires des petites classes.

Théorème. *(Premier théorème d'isomorphisme)*

Soit f un morphisme de groupes de G dans G', deux groupes quelconques. Alors $\mathrm{Ker}(f)$ est distingué dans G et $G/\mathrm{Ker}(f)$ est isomorphe à $\mathrm{Im}(f)$. Plus précisément, il existe un unique isomorphisme de groupes qui pour tout élément de x de G, applique la classe de x selon $\mathrm{Ker}(f)$ sur $f(x) \in \mathrm{Im}(f)$.

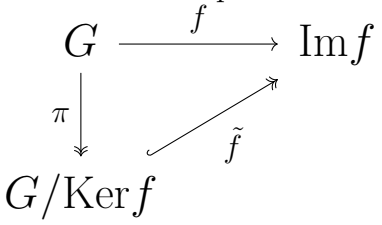
▷ Tout est déjà fait, et l'on voit que c'est la formulation du théorème d'isomorphisme pour les magmas, pour les groupes. L'isomorphisme est bien sûr la corestriction du morphisme quotient $\tilde{f}$, et tout cela est possible, car $\mathrm{Ker}(f)$ est distingué. On peut voir que l'injectivité vient de ce que $\mathrm{Ker}(\tilde{f})$ est $\mathrm{Ker}(f)$ (pourquoi ?) qui est l'élément neutre du groupe quotient $G/\mathrm{Ker}(f)$, ce qui caractérise l'injectivité pour les morphismes. ■

Ce théorème est fondamental ; sa preuve n'est pas pour autant compliquée, comme on demande de s'en rendre compte dans l'exercice suivant : la longueur relative des développements faits, l'accumulation des concepts et du vocabulaire, ne doit pas occulter que ce résultat n'a que l'apparence de l'écueil. L'empêtrement précédent n'est dû qu'à la volonté d'exhaustivité, quitte à étudier ce qui n'est pas fondamental. Nous pensons que le lecteur saura voir ce qui l'est.

Exercice 50

Redémontrer le théorème d'isomorphisme calmement, en allant droit au but.

Voilà en images le premier théorème d'isomorphisme.



On trouve parfois la précision suivante, ι étant l'injection canonique qui retranscrit une inclusion. Le symbole ι pour une injection canonique est très classique.

$$\begin{array}{ccc} G & \xrightarrow{\quad f \quad} & G' \\ {\scriptstyle\pi}\downarrow & & \uparrow{\scriptstyle\iota} \\ G/\mathrm{Ker}f & \xrightarrow[\tilde{f}]{} & \mathrm{Im}f \end{array}$$

Exercice 51

Montrer que, H étant un groupe quelconque, il existe un homomorphisme surjectif de G sur H si et seulement si H est un quotient de G (c'est-à-dire : H est isomorphe à un quotient de G).

Exercice 52

Soit f un morphisme de groupes de G dans G'. On suppose que G est de cardinal fini. On veut montrer que $\mathrm{card}(G) = \mathrm{card}(\mathrm{Ker}(f)).\mathrm{card}(\mathrm{Im}(f))$; en particulier, l'ordre de $\mathrm{Im}(f)$ divise l'ordre de G, ce que ne fournit pas le théorème de Lagrange.

1. Déduire ce résultat du théorème d'isomorphisme.

2. Le redémontrer naïvement grâce au lemme des bergers.

D'après le théorème d'isomorphisme, nous avons donc l'opportunité, dans tous les cas, d'exhiber un groupe isomorphe à un groupe quotient donné G/H. En effet, tout sous-groupe distingué (ici H) est le noyau d'un morphisme de groupe f, et en appliquant le théorème d'isomorphisme, on obtient que G/H est isomorphe à $\mathrm{Im}(f)$.

Exercice 53

1. Donner un groupe facile isomorphe à $\mathcal{GL}_n(\mathbb{K})/\mathcal{SL}_n(\mathbb{K})$.

2. Donner un groupe facile isomorphe à $\mathcal{O}_n(\mathbb{R})/\mathcal{SO}_n$.

3. Donner un groupe facile isomorphe à $\mathfrak{S}_n/\mathfrak{A}_n$.

4. Donner des groupes faciles isomorphes à $\mathbb{R}/\mathbb{Z}$, sa torsion (voir ci-bas), puis $\mathbb{R}/\mathbb{Q}$.

5. À quel groupe est isomorphe $G/Z(G)$?

Exercice 54

Un exemple récréatif, les groupes de torsion : un élément d'un groupe est dit *de torsion* s'il est d'ordre fini ; la *torsion* d'un groupe est l'ensemble de ses éléments de torsion.

1. Montrer que la torsion d'un groupe abélien en est un sous-groupe. Donner un contre-exemple dans le cas non commutatif.

2. Donner un exemple de groupe *sans torsion*, c'est-à-dire dont la torsion est réduite au neutre.

3. Quelle est la torsion de $\mathbb{R}/\mathbb{Z}$?

4. Un *groupe de torsion* est un groupe égal à sa torsion. Donner un exemple de groupe de torsion infini.

Exercice 55

Soit H un sous-groupe distingué de G et X une partie de G. Soit K un sous-groupe de G contenant H.

1. Montrer que $\pi^{-1}(\pi(X)) = XH$.

2. Montrer que $\pi^{-1}(\pi(K)) = K$.

Nous énonçons à présent le théorème de correspondance, résultat intermédiaire aux théorèmes d'isomorphisme, très riche puisque composé de beaucoup de propositions. Nous préférons le donner dans sa forme complexe classique plutôt que d'en délier les parties, avec la contrepartie d'enjoindre le lecteur de s'y attarder pesamment ainsi que sa preuve.

Propriété. *(Théorème de correspondance)*

Soit H un sous-groupe distingué de G. Alors $K \longmapsto K/H$ définit une bijection de l'ensemble des sous-groupes de G contenant H sur l'ensemble des sous-groupes de G/H ; elle applique les sous-groupes normaux de G contenant H sur les sous-groupes normaux de G/H ; elle est croissante pour l'inclusion, de réciproque également croissante, préserve l'indice, et enfin, A est normal dans B si et seulement si l'image de A est normale dans l'image de B.

▷ Procédons point par point.

► On considère l'application $K \longmapsto K/H$ définie sur E l'ensemble des sous-groupes de G contenant H. Soit K un sous-groupe de G contenant H, H étant distingué dans G. Alors la propriété d'intercalation de sous-groupe distingué donne que H est distingué dans K, donc K/H existe, et c'est un sous-groupe de G/H : en effet, la loi sur K/H est induite de celle sur G/H, car si $a, b \in K$ ont peut classes deux éléments aH, bH, ce sont des éléments de G qui ont pour classes ces mêmes. L'application est donc bien à valeurs dans F l'ensemble des sous-groupes du groupe quotient.

► On peut donner une autre expression à cette application : c'est tout simplement π, l'application projection qui est définie sur l'ensemble des parties de G (pour toute application de E dans

F, on peut canoniquement définir une application de $\mathcal{P}(E)$ dans $\mathcal{P}(F)$). Comme c'est au sens strict du terme, une autre application, nous la notons Π. Vérifions que si G' est un sous-groupe de G contenant H, alors $\Pi(G') = \pi(G') = \{\overline{x} \mid x \in G'\} = G'/H$. C'est en fait immédiat, car l'ensemble défini précédemment est G'/H par surjection de la projection canonique (et on rappelle bien que le point précédent nous donne la possibilité de parler de groupe quotient pour la congruence modulo H, pour G').

Remarque. Dans la littérature, on voit $\Pi(G') = \overline{G'}$. Cette notation est tout à fait licite, car la barre supérieure est l'une des notations (notation infixe) de la projection canonique. Cependant, nous sommes convaincus que c'est un pas en arrière dans la compréhension du concept : la quantité $\pi(G')$ est une image directe et non pas l'image de G' par une application, mais nous pouvons définir l'application Π sur une partie de l'ensemble des parties de G, en l'occurrence l'ensemble des sous-groupes contenant H, et dans ce cas $\pi(G')$ désigne aussi, incidemment, l'image d'un élément par une application, Π. Il est également très important que comprendre que Π n'est pas un morphisme, il n'est pas même défini sur une structure algébrique !

- ▶ Montrons que l'application Π est une bijection ; pour cela, on exhibe sa bijection réciproque Φ qui à tout sous-groupe de G/H, prenons en un G', envoie $\pi^{-1}(G')$, qui est un sous-groupe de G contenant H. En effet, si $h \in H$, alors $\pi(h) = \overline{e}$ est le neutre de G/H qui appartient à G' puisque c'est un sous-groupe, donc $\pi^{-1}(G')$ contient H. La structure de groupe vient de celle d'image réciproque par un morphisme. Montrons que $\Pi \circ \Phi = id_F$ et que $\Phi \circ \Pi = id_E$.
  - Soit G' un sous-groupe de G contenant H. L'inclusion $G' \subseteq \pi^{-1}(\pi(G'))$ est vérifiée pour toute partie de G' quelle que soit même π, soit $G' \subseteq \Phi \circ \Pi(G')$. Montrons l'inclusion réciproque. Soit $x \in \pi^{-1}(\pi(G'))$, c'est-à-dire tel que $\pi(x) = \overline{x} \in \pi(G')$. Cela signifie qu'il existe $x' \in G'$ tel que $pi(x) = p(x')$. Mais d'après un résultat anonyme que l'on a pris soin de rappeler en même temps que la notion de relation d'équivalence, on a donc $x \sim x'$, soit $xx'^{-1} = h \in H$. Ainsi $x = hx'$ produit de deux éléments de G', car H est dans G', donc x est dans G'. On en déduit $G' = \pi^{-1}(\pi(G'))$ pour tout G' dans E, d'où $\Phi \circ \Pi = id_E$.
  - Soit B un sous-groupe de G/H. Il est connu (puisqu'on a demandé au tout début de revoir les bases sur les ensembles, et notamment sur les opérations entre images et images réciproques) que puisque π est surjective, l'égalité $B = \pi \circ \pi^{-1}(B)$ est vérifiée pour en fait n'importe quelle partie de B. On a donc $\Pi \circ \Phi = id_F$. Ceci conclut pour la bijectivité de Π, de bijection réciproque Φ.
- ▶ Justifions que Π est un isomorphisme d'ensembles ordonnés, c'est-à-dire une bijection croissante dont la réciproque est également croissante, pour les ordres partiels d'inclusion sur E et F. Avec l'expression de Π par π et de Φ par π^{-1}, c'est une propriété de cours : en effet, image et image réciproque sont deux applications croissantes sur les ensembles de parties du départ et de l'arrivée. C'est inchangé par restriction et corestriction.
- ▶ Vérifions que Π préserve l'indice, c'est-à-dire que l'indice de A dans B est l'indice de $f(A)$ dans $f(B)$. D'abord, ceci a du sens, car $\Pi(A) = A/H$ et $\Pi(B) = B/H$ sont des images de groupes par le morphisme π donc des groupes, et $\Pi(A) \subseteq \Pi(B)$ donc $\Pi(A)$ est un sous-groupe $\Pi(B)$[8]. Il s'agit de montrer que $[B/H : A/H] = [B : A]$, c'est-à-dire que $\text{card}\left(\frac{A/H}{B/H}\right) = \text{card}\left(\frac{A}{B}\right)$. C'est

[8] Rappelons que, pour définir l'indice, il n'y a besoin que de la structure de sous-groupe et pas forcément de sous-groupe distingué, car de toute manière, l'indice à gauche et l'indice à droite coïncident.

une conséquence du troisième théorème d'isomorphisme, puisque $\frac{A/H}{B/H}$ et $\frac{A}{B}$ sont isomorphes donc en particulier ils ont le même cardinal ; on laisse le soin au lecteur de vérifier que le troisième théorème d'isomorphisme n'utilise pas de résultat découlant de cette affirmation.

- ▶ Montrons que pour tous A, B sous-groupes de G contenant H, $\Pi(A) = \pi(A) = A/H$ est normal dans $\Pi(B) = \pi(B) = B/H$ si et seulement si A est normal dans B. D'une part, si $A \triangleleft B$, alors si $x \in B/H$, si $a \in A/H$, $xax^{-1} \in A/H$; pour s'en convaincre, il suffit d'écrire ces classes comme des représentants et tout s'illumine. D'autre part, si $A/H \triangleleft B/H$, alors si $a \in A$ et $x \in B$, $xax^{-1} \in A$. En effet, de même que précédemment, en passant aux classes, $\overline{xax^{-1}} = \overline{x}.\overline{a}.\overline{x^{-1}} \in A/H$ par distinction, d'où $a \in A$ par définition.
- ▶ Nous devons enfin justifier que la restriction de l'application aux sous-groupes normaux dans G a pour image l'ensemble des sous-groupes normaux de G/H. D'une part, si G' (contenant H toujours) est normal dans G, alors $f(G')$ est normal dans $f(G) = G/H$ par surjectivité. D'autre part, si un sous-groupe B de G/H en est un sous-groupe distingué, alors par surjectivité il existe G' dans G contenant H un sous-groupe (c'est-à-dire un élément de E) tel que $\Pi(G') = B$, et $\Pi(G')$ est normal dans $\Pi(G) = G/H$ donc d'après l'équivalence du paragraphe précédent, G' est normal dans G, et il contient H. Ainsi Π envoie l'ensemble des sous-groupes normaux de G contenant H sur l'ensemble des sous-groupes normaux de G/H exactement ; cette restriction et corestriction est donc bien évidemment surjective, et injective en tant que restriction d'une injection ; ces deux ensembles sont en bijection.

Tout a ainsi été justifié. ■

Le théorème de correspondance donne un peu de licence pour travailler sur le groupe quotient, en voyant ses opérations comme des projections de celles sur le groupe d'origine, par l'intermédiaire de la projection canonique. Notamment, elle donne un moyen d'expliciter les sous-groupes d'un groupe quotient en fonction de ceux du groupe de départ : pour un exemple concret, le lecteur peut se référer à la section suivante.

Exercice 56

Si H est distingué dans G, et K un sous-groupe de H distingué dans G, G/K est-il un sous-groupe de G/H ?

Exercice 57

(Une conséquence du théorème de correspondance) Montrer que, si H est normal dans G, H est un sous-groupe normal maximal si et seulement si G/H est simple.

Corollaire. *(Correspondance des sous-groupes normaux avec ceux du quotient)*

Soit H un sous-groupe distingué de G. Alors il existe une bijection explicite entre les sous-groupes normaux de G contenant H et les sous-groupes normaux de G/H.

▷ Relire les dernières lignes de la démonstration du théorème de correspondance. ■

Exercice 58

Soient H, K deux sous-groupes d'un groupe.

1. Montrer que HK est un sous-groupe du groupe si et seulement si $HK = KH$.

2. Montrer qu'il suffit que H soit normal dans le groupe.

3. Sous quelle condition HK est-il normal ?

Théorème. *(Second théorème d'isomorphisme)*

Soient G un groupe, $K \triangleleft G$ et H un sous-groupe de G. Alors $K \cap H \triangleleft H$, HK est un groupe et $K \triangleleft HK$, et $\frac{H}{K \cap H} \simeq \frac{HK}{K}$. Plus précisément, il existe un unique isomorphisme de $H/(H \cap K)$ sur HK/K tel que pour tout élément x de H, $f(x(H \cap K)) = xK$.

▷ On a déjà montré dans l'exercice précédent que HK est un sous-groupe de G, l'un des deux, à savoir K, étant normal dans G. De plus, si $x \in H \cap K$, alors si $a \in H$, $axa^{-1} \in H$ comme produit d'éléments de H et appartient à K, car K est distingué dans G, et $a \in G$: on a donc la distinction de $H \cap K$ dans H. D'autre part, si $x \in K$, si $a = hk \in HK$, alors $axa^{-1} = hkx(hk)^{-1} = h(kxk{-}1)h{-}1$. Or K est distingué dans H donc $kxk{-}1 = k' \in K$. Ainsi $axa^{-1} = hk'h^{-1} \in K$, car K est distingué dans H ; ainsi, K est distingué dans HK ; nous sommes donc tranquilles pour passer à la partie intéressante du théorème. K étant distingué dans G, on considère la projection canonique $\varphi : G \longrightarrow G/K$. Note ψ la restriction de φ à H. (Le noyau de ψ est $H \cap K$ et l'on retrouve que $H \cap K$ est distingué dans H.) L'image de ψ est l'ensemble des classes d'éléments de H suivant K par définition de la projection et de la restriction. On remarque que cet ensemble est HK/K, sous-groupe de G/K. L'énoncé résulte donc du premier théorème d'isomorphisme appliqué à ψ. ■

Remarque importante. Nous enjoignons le lecteur à vérifier que le second théorème d'isomorphisme se généralise légèrement en changeant l'hypothèse « $K \triangleleft G$ » par « H normalise K » (voir les compléments deux sections plus bas).

Exercice 59

1. Quels sont les sous-groupes de $\mathcal{GL}_n(\mathbb{K})$, $\mathbb{K}$ un corps, contenant $\mathcal{SL}_n(\mathbb{K})$?

2. Quels sont les sous-groupes de $\mathfrak{S}_n$ contenant $\mathfrak{A}_n$?

Exercice 60

(Identité de Dedekind) Soient G un groupe, U et V deux parties de G telles que $UV = G$. Soient H un sous-groupe de G contenant U et K un sous-groupe de G contenant V. Montrer que $H = U(V \cap H)$ et que $K = (U \cap K)V$.

Le troisième théorème d'isomorphisme établit une égalité qui rappelle la simplification en haut et en bas des numérateur et dénominateur d'une fraction.

Théorème. *(Troisième théorème d'isomorphisme)*
Soient G un groupe, H un sous-groupe de G, K un sous-groupe de H, avec H, K normaux dans G. Alors $H/K \triangleleft G/K$ et $\frac{G/K}{H/K} \simeq \frac{G}{H}$.

▷ Premier réflexe : K est normal dans H (par intercalation). Ainsi, on a $K \triangleleft H \triangleleft G$ et $K \triangleleft G$, ce qui permet de parler de H/K, de G/K et de G/H. Nous savons déjà également que H/K est un sous-groupe distingué de G/H : on l'a montré dans le théorème de correspondance (et ce n'est pas ce pourquoi l'on a appelé le troisième théorème d'isomorphisme dans la même preuve !). Or, toute classe X de G suivant K est contenue dans une et une seule classe selon H : en effet, X est de la forme xK, $x \in G$, donc $X = xK \subseteq xH$ classe suivant H, et la classe de x suivant H qui contient X est unique, par disjonction des classes d'équivalence. À toute classe X selon K, faisons correspondre cette unique classe selon H contenant X par une application f de G/K dans G/H. Ainsi, pour tout élément $x \in G$, $f(xK) = xH$. On vérifie très vite que f est un morphisme de groupes surjectif de noyau H/K. (On retrouve que H/K est distingué dans G/K.) On conclut par premier théorème d'isomorphisme. ■

Exercice 61
En déduire (mais c'était déjà conséquence du premier théorème d'isomorphisme) que la relation $A \preccurlyeq B \Leftrightarrow A$ est isomorphe à un quotient de B est un ordre.

Exercice 62
Deux sous-groupes isomorphes d'un même groupe sont-ils nécessairement égaux ?

Avant de terminer sur les quotients de groupe, une variante du premier théorème d'isomorphisme.

Propriété. *(Quatrième théorème d'isomorphisme)*
Soient G un groupe, H un autre groupe et L un sous-groupe normal de G. On note π la surjection canonique de G sur G/L. Alors $\mathrm{Hom}(G/L, H)$ est en bijection avec l'ensemble des morphismes de G dans H dont le noyau contient L, par l'application $g \longmapsto g \circ \pi$.

▷ C'est une reformulation du théorème de factorisation pour les groupes ! On peut la voir, au choix, de cette manière, ou comme une généralisation du premier théorème d'isomorphisme, ou encore étudier $G/N \to G/K \to H$ où le premier morphisme est défini comme dans la démonstration du troisième théorème d'isomorphisme. De cette façon, on voit l'intrication des quatre théorèmes précédents. ■

Nous énonçons un résultat connexe, qui introduit pudiquement la notion de suite exacte.

Propriété. Si $f : G \longrightarrow G'$ est un morphisme de groupes, G, G' deux groupes quelconques, alors il existe une suite exacte (c'est-à-dire une suite de morphismes dont l'image de l'un est égale au noyau du suivant) donnée par $G \to G' \to G'/\mathrm{Im}(f) \to 1$.

▷ Les morphismes à considérer sont, dans l'ordre : f, la projection canonique sur $\mathrm{Im}(f)$, le morphisme trivial toujours égal au neutre. ■

2.3.3 Application : le cas des anneaux modulaires

On appelle anneaux modulaires, les $\mathbb{Z}/n\mathbb{Z}$ pour n parcourant l'ensemble des entiers naturels. Comme on le sait depuis le lycée, ce sont des anneaux unitaires, mais on peut se contenter pour l'instant de considérer la structure de groupe additif qui renferme déjà beaucoup des subtilités de la structure. Nous proposons au lecteur de démontrer les quelques résultats suivants en exercice : ce sont des conséquences du théorème de correspondance.

Exercice 63

Montrer que si G est un groupe et H un sous-groupe de G d'indice fini n. Soit $x \in G$. Montrer que $x^n \in H$.

Exercice 64

1. Montrer que, si G est un groupe cyclique, alors tout sous-groupe de G est lui-même cyclique (exercice classique de spé).

2. Justifier que tout groupe monogène est isomorphe à $\mathbb{Z}$ ou à un certain $\mathbb{Z}/n\mathbb{Z}$, pour $n \in \mathbb{N}^*$. En déduire que tout sous-groupe d'un groupe monogène est monogène.

3. Soit $n \in \mathbb{N}^*$. Montrer que $\mathbb{Z}/n\mathbb{Z}$ est fini, de cardinal n.

4. Montrer que les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ sont exactement les $d\mathbb{Z}/n\mathbb{Z}$, pour d diviseur de n, et qu'il y en a donc $\varphi(n)$.

5. Quel est le cardinal de $d\mathbb{Z}/n\mathbb{Z}$, pour d divisant n ? En déduire qu'il est isomorphe à $\mathbb{Z}/l\mathbb{Z}$, où l est le diviseur associé à d de n.

6. Montrer que $\frac{\mathbb{Z}/n\mathbb{Z}}{d\mathbb{Z}/n\mathbb{Z}}$ est isomorphe à $\mathbb{Z}/d\mathbb{Z}$.

7. Soit G un groupe cyclique d'ordre n. Montrer que pour tout diviseur d de n, G admet un unique sous-groupe d'ordre d, que tous les sous-groupes de G sont ainsi décrits, que ce groupe H est cyclique, et que G/H est également cyclique.

8. Montrer que, si G est un groupe cyclique d'ordre n et d un diviseur naturel de n, le sous-groupe d'ordre d de n est l'ensemble des éléments x de G tels que $x^d = 1$.

Exercice 65

On souhaite montrer que le groupe multiplicatif d'un corps $\mathbb{K}$ est cyclique. On note, pour tout entier naturel a, l'endomorphisme de $\mathbb{K}^*$ défini par $f_a : x \longmapsto x^a$. Soient a, b deux entiers naturels tels que $ab = n - 1$. On note $N_a = \text{card}(\text{Ker}(f_a))$.

1. Expliquer pourquoi $N_a \leqslant a$.

2. Montrer que $\text{Im}(f_a) \subseteq \text{Ker}(f_b)$.

3. En déduire que $N_a = a$ et $N_b = b$.

4. Montrer par récurrence sur a, diviseur de $n-1$, que le nombre d'éléments de $\mathbb{K}^*$ d'ordre a est égal à $\varphi(a)$.

5. Conclure.

2.3.4 Retour post-traumatique sur la distinction

Exercice 66

On rappelle qu'un sous-groupe maximal est un élément maximal pour l'inclusion de l'ensemble des sous-groupes propres d'un groupe.

1. Redémontrer la formule des indices.

2. Montrer que tout sous-groupe d'indice fini premier d'un groupe est maximal.

3. Montrer que, dans un groupe fini, tout sous-groupe propre est contenu dans au moins un sous-groupe maximal.

4. Montrer que le résultat persiste dans un groupe de type fini. Qu'a-t-on utilisé ?

5. Montrer que tout sous-groupe maximal aussi normal est d'indice fini premier.

6. Montrer qu'un sous-groupe est divisible si et seulement s'il n'a pas de sous-groupe maximal.

Définition. *(Normalisateur)*

Si H est un sous-groupe de G, on dit qu'un élément g de G normalise H si $gHg^{-1} = H$, ou, ce qui est équivalent (le vérifier), $g^{-1}Hg = H$ (ou encore avec seule l'inclusion directe). L'ensemble des normalisateurs de H est appelé *normalisateur* de H et est noté $N_G(H)$.

Propriété. *(Structure du normalisateur)*

Si H est un sous-groupe de G, $N_G(H)$ est le plus grand sous-groupe de G contenant H dans lequel H est normal.

▷ Les vérifications sont simples, et laissées au lecteur. Il s'agit de voir, successivement que : le normalisateur est un groupe, qu'il contient H, qu'il est normal, et qu'il contient tout sous-groupe de G dans lequel H est normal. ■

Corollaire. *(Caractérisation de la normalité par le normalisateur)*
Si H est un sous-groupe de G, H est distingué dans G si et seulement s'il égale son normalisateur.

▷ C'est trivial avec ce qui précède. ■

Exercice 67

On généralise un résultat démontré en exercice en préambule du second théorème d'isomorphisme. Soit H un sous-groupe de G et K un sous-groupe de G normalisant H, c'est-à-dire inclus dans son normalisateur.

1. Montrer que HK est un sous-groupe.

2. Montrer que $H \cap K$ est distingué dans H. L'est-il dans K ?

Remarque. Le normalisateur d'un sous-groupe H dans G contient le centralisateur de H dans G, donc *a fortiori*, le centre de G. Pour se rendre compte de ce fait, le lecteur peut se reporter aux définitions de centralité sur les actions de groupe.

Propriété. *(Caractérisation des normalisateurs par génératrices)*
Si H est un sous-groupe de G généré par une partie X, un élément g de G normalise H si et seulement si $g^{-1}Xg$ et gXg^{-1} sont tous deux contenus dans H.

▷ En exercice. ■

On termine avec un résultat important. Dans son *Group theory*, William Raymond Scott, docteur mathématicien diplômé en 1947 de l'Université de l'État de l'Ohio, écrit que ce théorème, presque trivial, est d'une grande importance dans la théorie des groupes en général.

Propriété. *(Lemme N/C)*
Soient G un groupe, H un sous-groupe de G. Alors $C_G(H) \triangleleft N_G(H)$ et $N_G(H)/C_G(H)$ est isomorphe à un sous-groupe de $\mathrm{Aut}(G)$.

▷ Montrons d'abord la distinction, pour pouvoir parler de groupe quotient. Soit g un élément de $N_G(H)$. $f_g : x \longmapsto gxg^{-1}$ induit un automorphisme sur H par définition du normalisateur. On définit donc un morphisme (le vérifier) φ de $N_G(H)$ dans $\mathrm{Aut}(H)$ qui à g fait correspondre f_g. Or le noyau de ce morphisme est $C_G(H)$, qui est donc distingué dans $N_H(G)$. Enfin, d'après le premier théorème d'isomorphisme, $C_G(H) \triangleleft N_G(H)$ et $N_G(H)/C_G(H)$ est isomorphe à un sous-groupe de $\mathrm{Aut}(G)$; c'est $\mathrm{Im}(\varphi)$. ■

2.4 Anneaux quotients par des idéaux

On rappelle quelque chose de dit plus haut dans notre composition.

Propriété. *(Anneau quotient)*
Si $(\mathbb{A}, +, \times)$ est un groupe, $\mathcal{R}$ une relation d'équivalence sur $\mathbb{A}$ compatible avec $+$ et avec $\times$, alors $\mathbb{A}/\mathcal{R}$ muni des deux lois quotients est un anneau d'éléments neutres $\overline{0}$ et $\overline{1}$.

Avant de préparer la suite, on conseille de revoir les choses suivantes du cours de mathématiques : définition d'un idéal, ce que l'on dit d'un idéal contenant 1 ou un inversible, noyaux de morphismes d'anneaux, condition nécessaire et suffisante pour qu'un anneau soit un corps avec les idéaux, idéaux classiques, intersection et somme d'idéaux.

Exercice 68

Pourquoi les corps quotients ne vont-ils pas nous intéresser ?

Nous remarquons qu'un anneau, un sous-anneau et un idéal étant en particulier des sous-groupes additifs, les quotients intéressants vont devoir, comme on l'a montré précédemment, vérifier au moins les propriétés analogues à celles des sous-groupes distingués (ce doivent être donc des congruences modulo un sous-groupe). Nous voyons qu'il faut et qu'il suffit que ce soient des congruences modulo un idéal bilatère.

Soit $(\mathbb{A}, +, \times)$ un anneau unitaire, non nécessairement commutatif. On aurait pu considérer seulement les pseudo-anneaux. On rappelle qu'un idéal est dit *bilatère*, s'il est idéal à gauche et idéal à droite.

Propriété. *(Congruences compatibles avec la structure d'anneau)*
Si I est un idéal bilatère de $\mathbb{A}$, alors la congruence modulo le sous-groupe I est compatible avec les lois de $\mathbb{A}$, et réciproquement, toute relation d'équivalence compatible avec les deux lois de $\mathbb{A}$ est la congruence modulo un idéal bilatère (à savoir la classe de 0).

▷ Soit $\sim$ la congruence modulo l'idéal bilatère I, définie par $a \sim b \Leftrightarrow a - b \in I$. Comme le groupe additif d'un anneau est commutatif par axiome, I est un sous-groupe distingué du groupe additif de $\mathbb{A}$. Il ne reste qu'à montrer la compatibilité multiplicative. Elle provient tout simplement de la définition de stabilité globale de l'idéal : si $a \sim b$ et c est quelconque, alors $c(a-b) \in I$, donc $ca - cb \in I$, donc $ca \sim cb$. La loi est compatible à gauche. On montre de même la compatibilité à la droite, d'où la compatibilité avec la multiplication. Réciproquement, si $\sim$ est une relation d'équivalence compatible avec l'addition et la multiplication, alors on sait déjà, d'après la partie sur les groupes, que $\overline{0} = I$ est un sous-groupe de $\mathbb{A}$ et que $\sim$ est la congruence modulo I. Il reste seulement à montrer que I est un idéal bilatère. Cela vient tout simplement du caractère absorbant (à gauche et à droite, car il y a distributivité à gauche et à droite) de 0. Cela termine la preuve. ■

⟶ **Convention.** Dans le contexte des anneaux quotients par des idéaux, on parle de *réduction modulo I de a*, pour parler de la classe de a modulo I.

Remarque. À l'instar des groupes, on pouvait montrer un résultat plus précis (se référer à la preuve) : une relation est compatible à gauche avec la loi multiplicative si et seulement si c'est celle associée à un idéal à gauche, puisque la loi additive n'a aucun intérêt, on l'a vu, pour les quotients d'anneaux.

Le lecteur aura soin de revoir la partie sur les quotients de magma pour se convaincre que les idéaux bilatère, à l'instar des sous-groupes distingués, sont le cadre le plus général pour quotienter des anneaux. Remarquons qu'alors, l'anneau quotient est bien un anneau (ouf !) et que la projection canonique, que l'on appellera donc quelquefois *réduction*, est un morphisme d'anneaux. (Pour vérifier cela, il suffit de considérer le magma $(\mathbb{A}, \times)$.)

Propriété. *(Anneau commutatif quotient)*
Soient A un anneau et I un idéal bilatère de A. Si A est commutatif, alors A/I est commutatif.

▷ C'est déjà vu avec les magmas. ■

Exercice 69
Si A est principal, décrire tous ses quotients.

Exemples fondamentaux. Pour $A = \mathbb{Z}$, les idéaux $n\mathbb{Z}$ sont bilatères, car l'anneau A est commutatif. Ainsi les anneaux modulaires... sont bien des anneaux (commutatifs).

Voilà le schéma général pour les quotients d'anneaux (par des idéaux).

$$\begin{array}{ccc} I & \xhookrightarrow{\ \iota\ } & A \\ & & \downarrow{\scriptstyle \pi} \\ & & A/I \end{array}$$

Exercice 70

1. *(Symétrisation de monoïde)* Expliquer comment on construit un groupe à partir d'un monoïde M grâce à la relation d'équivalence sur $M \times M$: $(a,b) \sim (a',b') \Leftrightarrow \exists k,\ a+b'+k = a'+b+k$. Que représente (a,b) ?

2. *(Corps des fractions)* Expliquer comment on construit un corps à partir d'un anneau intègre A grâce à la relation d'équivalence sur $A \times A$: $(a,b) \sim (a',b') \Leftrightarrow ab' = a'b$. Que représente (a,b) ?

Maintenant, on peut énoncer les théorèmes de factorisation et d'isomorphisme pour les anneaux. Ils sont très semblables à ceux pour les groupes ; pour la plupart, ce n'en est que reformulation et vérification que les propriétés multiplicatives sont encore vérifiées, ce qui est le cas systématiquement, sachant que maintenant, le cadre général a été réduit aux idéaux, et non plus seulement aux sous-groupes distingués (les idéaux sont bien sûr des sous-groupes distingués additifs par commutativité).

Théorème. *(Théorème de factorisation pour les anneaux)*

Soit f un morphisme d'anneaux de A dans A'. I est dans $\mathrm{Ker}(f)$ si et seulement s'il existe un unique morphisme $\tilde{f}$ tel que $f = \tilde{f} \circ \pi$ (se qui se réécrit $f(x) = \tilde{f}(\overline{x})$ pour tout $x \in A$).

▷ C'est une adaptation du théorème de factorisation pour les groupes. Il ne reste qu'à vérifier que $\tilde{f}$ est un morphisme pour la multiplication, et que l'image de $\overline{1_A}$ est $1_{A'}$. ■

Méthode. RECETTE POUR PASSER AU QUOTIENT DANS LES MORPHISMES D'ANNEAUX

1. Je vérifie que je dispose de deux anneaux A, A', d'un morphisme f entre les deux, et d'une partie I de A.
2. **Je vérifie que I est un idéal bilatère de A.** J'en déduis cette affirmation, que le quotient existe dans toute sa splendeur d'ensemble quotient univoquement défini par une relation de congruence et a la structure d'anneau.
3. **Je vérifie maintenant que I est inclus dans $\mathrm{Ker}(f)$.** Si je veux, pour crâner, je précise que c'est une condition nécessaire et suffisante à la compatibilité de f avec la congruence, car je connais même la preuve de mon théorème de factorisation sur les groupes.
4. Je peux maintenant définir un morphisme $= \tilde{f} : A/I \longrightarrow A'$ sans trouble, telle que pour tout $\overline{x} \in A/I$, $\tilde{f}(\overline{x}) = f(x)$, et j'insiste bien sur ce que cette construction n'est possible que grâce aux deux hypothèses vérifiées précédemment.

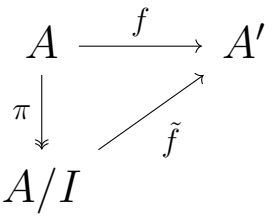
Si je veux une propriété d'injectivité, de surjectivité, voire de bijectivité pour mon application, je me réfère aux résultats de l'exercice précédent.

De la même façon que dans la section sur les groupes quotients, il est tout à fait inutile d'énoncer un théorème de factorisation carré (il aurait exactement le même énoncé que le théorème de factorisation simple !). Toutefois, on dispose d'un corollaire intéressant.

Exercice 71

Dans le théorème précédent, montrer que :
1. $\tilde{f}$ est injective si et seulement si $I = \mathrm{Ker}(f)$;
2. $\tilde{f}$ est surjective si et seulement si f est surjective ;
3. $\tilde{f}$ est un isomorphisme si et seulement si f est surjective et $I = \mathrm{Ker}(f)$.

Une illustration du théorème de factorisation. Le lecteur ayant l'habitude, on ne précise plus les lois des anneaux.



Corollaire. Soit f un morphisme d'anneaux de A dans B et J un idéal de B. Alors $f^{-1}(J)$ est un idéal de A et l'on a un morphisme injectif $A/f^{-1}(J) \longrightarrow B/J$.

▷ On compose le morphisme $A \longrightarrow B \longrightarrow B/J$ en $\pi \circ f$, morphisme d'anneaux. Son noyau est $f^{-1}(J)$, c'est donc un idéal. Le reste est corollaire du théorème et de l'exercice précédents. ■

Corollaire. Si $A \subseteq B$, J un idéal de B, alors $A \cap J$ est une idéal de A et l'on a un morphisme injectif : $A/(A \cap J) \longrightarrow B/J$.

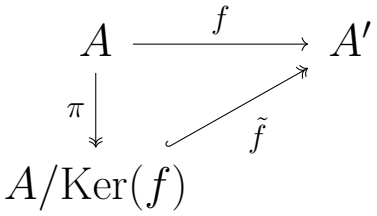
▷ C'est un cas particulier du corollaire précédent. ■

Maintenant, nous énonçons les théorèmes d'isomorphisme pour les anneaux, tout à fait semblables à leurs cousins pour les groupes.

Théorème. *(Premier théorème d'isomorphisme pour les anneaux)*
On considère l'anneau A. Soit A' un autre anneau, et $f : A \longmapsto A'$ un morphisme d'anneaux. Alors les anneaux $A/\mathrm{Ker}(f)$ et $\mathrm{Im}(f)$ sont isomorphes par le morphisme $\tilde{f}$.

▷ On invoque le théorème d'isomorphisme pour les groupes ; il ne reste qu'à vérifier que $\tilde{f}$ est bien un morphisme pour la multiplication, ce qui est facile. ■

Nous pouvons, encore une fois, l'illustrer par un diagramme :



Le théorème de correspondance est prolongé dans les anneaux de façon immédiate.

Propriété. *(Théorème de correspondance pour les anneaux)*
Soit I un idéal bilatère de A. Alors $J \longmapsto J/I$ définit une bijection de l'ensemble des idéaux de A contenant I sur l'ensemble des sous-groupes de A/I ; c'est un isomorphisme d'ensembles ordonnés.

▷ Il n'y a rien à faire. ■

On peut encore énoncer les autres théorèmes d'isomorphismes. Il suffit alors de vérifier que les constructions correspondantes pour les sous-groupes distingués sont bien compatibles avec la multiplication, ce qui est facile, et laissé au lecteur déterminé.

Théorème. *(Deuxième théorème d'isomorphisme pour les anneaux)*
Si J est un idéal de A contenant I, I est un idéal de J, J/I est un idéal de A/I, alors $\frac{A/I}{J/I} \simeq \frac{A}{J}$.

▷ On doit seulement dire pourquoi si J est un idéal de A contenant I, I est un idéal de J. ■

Remarquons simplement qu'il n'y a pas de traduction du deuxième théorème d'isomorphisme (le lecteur attentif aura remarqué que c'était la traduction du troisième théorème d'isomorphisme). Le deuxième théorème pour les groupes fait intervenir la notion de produit direct HK, qui est bien un groupe si H est normal, mais le produit de deux idéaux n'est ni un sous-anneau, ni un idéal.

Exercice 72

On appelle idéal produit de I et J, l'idéal engendré par IJ. Le deuxième théorème d'isomorphisme pour les groupes se généralise-t-il aux anneaux en remplaçant les produits directs de groupes par cette définition sur les idéaux ?

Exercice 73

Quels sont les idéaux de $\mathbb{Z}/n\mathbb{Z}$ et les quotients correspondants ?

2.5 Espaces vectoriels quotients

Nous terminons nos considérations avec le cas des espaces vectoriels quotients. Celui-ci est d'autant plus intéressants que les deux précédents pour les groupes et les anneaux, car, non seulement nous l'utilisons pour donner de nouvelles preuves de résultats au programme, mais mieux encore, il est la façon naturelle d'introduire le concept de codimension (c'est d'ailleurs de cette manière que, sans vergogne, Xavier Gourdon la définit dans *Les maths en tête*, collection censée être un ouvrage manuel pour les classes préparatoires... bien que la notion de quotient soit sortie des programmes au cours d'un autre millénaire). La co-dimension (que l'on sait être la dimension commune à tous les supplémentaires d'un sous-espace vectoriel) d'un sous-espace vectoriel F est également la dimension de l'espace quotient E/F.

Exercice 74

Soient A, B, C des matrices.

1. *(Inégalité de Frobenius)* Montrer que $\mathrm{rg}(AB) + \mathrm{rg}(BC) \leqslant \mathrm{rg}(ABC) + \mathrm{rg}(B)$.

2. *(Inégalité de Sylvester)* En déduire, pour des matrices carrées A, B de taille n, $\mathrm{rg}(A) + \mathrm{rg}(B) - n \leqslant \mathrm{rg}(AB)$.

L'inégalité de Frobenius ne se montre qu'au moyen des espaces vectoriels quotients, que nous allons voir. Cependant, l'inégalité de Sylvester est un grand classique des classes préparatoires.

Nous recommençons le procédé habituel pour la structure des espaces vectoriels. Le théorème de compatibilité est facilité par ce que, comme pour les anneaux, les sous-espaces vectoriels sont automatiquement des sous-groupes distingués, puisqu'en milieu commutatif, et il n'y a pas question de bilatéralité (la loi externe n'est défini que dans un sens bien sûr !).

Soit V un espace vectoriel sur un corps K. Soit W un sous-espace vectoriel de V.

Théorème. *(Congruences compatibles avec la structure d'espace vectoriel)*

(On définit la compatibilité avec la loi externe par : $\overrightarrow{u} \simeq \overrightarrow{v} \Rightarrow \forall \lambda \in K,\ \lambda.\overrightarrow{u} \simeq \lambda.\overrightarrow{v}$.) Toute relation des classes à gauche (ou à droite, peu importe) selon un sous-espace vectoriel est compatible avec l'addition et la loi externe, et réciproquement, toute relation ainsi compatible est relation de classes à gauche (ou à droite) modulo un sous-espace vectoriel.

▷ En exercice. ■

Théorème. *(Espace vectoriel quotient)*

Le groupe V/W admet une unique structure d'espace vectoriel sur K telle que la projection canonique $\pi : V \longrightarrow V/W$ soit une application linéaire.

▷ On veut avoir, par définition de la notion d'application linéaire, $\pi(\lambda x) = \lambda\pi(x)$ et $\pi(x+y) = \pi(x) + \pi(y)$ pour tous $x, y \in V$ et $\lambda \in K$. La première identité définit univoquement la loi externe sur V/W en tant que K-espace vectoriel : pour $a \in V/W$, si x est un représentant de a, on doit donc poser $\lambda a = \overline{\lambda x}$ et cette définition ne dépend pas du choix du représentant x de a, puisque si $x \sim x'$, $x - x' \in W$, donc $\lambda x - \lambda x' \in W$, donc $\lambda x \sim \lambda x'$. Cela signifie de plus que la relation $\sim$ sur V est compatible avec la loi externe. On vérifie alors aisément que, ceci dit, on a un espace vectoriel (la loi additive est déjà déterminée par le groupe commutatif V, avec $\overline{x+y} = \overline{x} + \overline{y}$). Par analyse-synthèse, on a existence et unicité de la structure d'espace vectoriel sur le quotient. ■

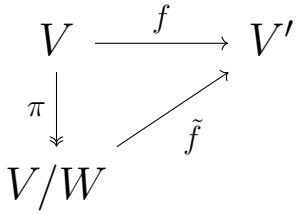
On retient la définition des lois sur le quotient, très intuitive : pour tous $\overline{x}, \overline{y} \in V/W$, pour tout $\lambda \in K$,

$$\overline{x} +' \overline{y} = \overline{x+y} \text{ et } \lambda .' \overline{x} = \overline{\lambda . x}.$$

Dans ce qui suit, les théorèmes concernant les quotients d'espaces vectoriels découlent de deux choses très simples : l'application des théorèmes sur les groupes pour la loi additive, qui est immédiate sachant que tous les sous-groupes (c'est-à-dire ici, sous-espaces vectoriels) additifs sont tous distingués, le groupe additif étant commutatif par axiome ; d'autre part, la vérification chaque fois des compatibilités avec la loi externe, comme nous venons de le faire. Nous ne détaillons pas celle-ci.

Théorème. *(Théorème de factorisation pour les espaces vectoriels)*
Soit f une application linéaire entre deux espaces vectoriels V vers V'. Soit W un sous-espace vectoriel de V. W est dans $\mathrm{Ker}(f)$ si et seulement s'il existe un unique morphisme $\tilde{f}$ tel que $f = \tilde{f} \circ \pi$ (se qui se réécrit $f(u) = \tilde{f}(\overline{u})$ pour tout $u \in V$), en notant π la projection canonique (linéaire) de V dans V/W.

Une petite illustration des familles :



Le théorème de factorisation carré s'applique également (nous invitons le lecteur à l'énoncer). Dans le cas où le départ et l'arrivée sont les mêmes, on obtient un corollaire intéressant.

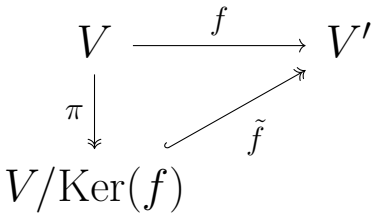
Corollaire. Si f est un endomorphisme de V et W un sous-espace vectoriel stable par f, l'application linéaire quotient est un endomorphisme de V/W.

Les deux théorèmes d'isomorphismes repris pour les anneaux s'énoncent pour les espaces vectoriels. Le deuxième théorème d'isomorphisme pour les groupes proprement dit n'admet

pas de généralisation, puisqu'aucune opérateur multiplicative n'est possible entre sous-espaces vectoriels à part l'addition. On reprend les notations précédentes.

Théorème. *(Premier théorème d'isomorphisme pour les espaces vectoriels)*
Soit $f : V \longrightarrow V'$ une application linéaire. Les espaces vectoriels $V/\mathrm{Ker}(f)$ et $\mathrm{Im}(f) \subseteq V'$ sont isomorphes par l'application linéaire quotient, qui est un isomorphisme.

Ceci s'exprime synthétiquement :



D'autre part :

Théorème. *(Deuxième théorème d'isomorphisme pour les espaces vectoriels)*
Soient $G \subset F \subset E$ des sous-espaces vectoriels. Alors F/G est un sous-espace vectoriel de E/G et $\frac{E/G}{F/G} \simeq \frac{E}{F}$.

Exercice 75

Peut-on énoncer un théorème d'isomorphisme pour les algèbres ?

Nous terminons avec la seule justification de tout ce chapitre dans le cas des classes préparatoires (lol). Il faut s'attarder sur la preuve, quoique très succincte, car elle est la clef, comme d'habitude.

Théorème. *(Théorème fondamental de la codimension)*
Soit W un sous-espace vectoriel de V ; soit W' un supplémentaire de W dans V. Alors W' est isomorphe à V/W.

▷ L'isomorphisme à exhiber est la restriction à W' de la projection canonique de V sur V/W. Celle-ci est linéaire par restriction, d'une application linéaire. Reste à montrer qu'elle est injective et surjective. Pour l'injectivité, on utilise la caractérisation par le noyau : l'ensemble des $x \in W'$ tels que $\pi(x) = W$ le neutre de V/W est réduit à l'élément neutre, car ils sont dans W' ainsi que dans le noyau de π qui est W, et $W \cap W'$ est réduit au neutre car deux espaces supplémentaires sont indépendants. Pour la surjectivité, on a l'image de cette restriction qui égale exactement $\pi(W') = \pi(W) + \pi(W')$, car $\pi(W)$ est le neutre dans V/W. Par linéarité (prolongée sur les parties), $\pi(W) + \pi(W') = \pi(W + W')$ et $W + W' = V$ par complémentarité, donc $\pi(W') = pi(V) = V/W$ par surjectivité de la projection canonique en entier. Et c'est tout. ■

On en déduit ce qui suit, tant attendu :

Corollaire. *(Unicité de la codimension)*
Soit W un sous-espace vectoriel de V, alors tous les supplémentaires de W dans V (il en existe au moins un, d'après le théorème de la base incomplète) sont isomorphes. En particulier, ceux-ci ont la même dimension, appelée *codimension* de W, notée $\mathrm{codim}_V(W)$ qui égale $\dim_K(V/W)$.

Comme la dimension, la codimension dépend tout à fait de l'espace ambiant, d'où la précision dans la notation.

On termine avec quelques propriétés faciles qui en découlent.

Définition. *(Hyperplan)*
Un hyperplan est un sous-espace vectoriel de codimension 1.

Propriété. *(Majoration de la codimension d'une intersection)*
Soient W_1, W_2 deux sous-espaces vectoriels de V de codimensions finies. Alors $\mathrm{codim}(W_1 \cap W_2) \leqslant \mathrm{codim}(W_1) + \mathrm{codim}(W_2)$.

Propriété. *(Majoration de l'intersection d'hyperplans)*
L'intersection de k hyperplans est un sous-espace vectoriel de codimension inférieur ou égale à k.

Propriété. *(Majoration de l'intersection d'hyperplans)*
L'intersection de k hyperplans est un sous-espace vectoriel de codimension inférieur ou égale à k.

Propriété. *(Lien noyau-image pour la codimension)*
Soit $f : V \longrightarrow V'$ une application linéaire. $\mathrm{Ker}(f)$ est de codimension finie si et seulement si $\mathrm{Im}(f)$ est de dimension finie, et dans ce cas, $\mathrm{codim}(\mathrm{Ker}(f)) = \dim(\mathrm{Im}(f))$.

Propriété. Si V' est de dimension finie, $\mathrm{Ker}(f)$ est de dimension finie et $\mathrm{codim}(\mathrm{Ker}(f)) \leqslant \dim(V')$, avec l'égalité dans le cas seul où f est surjective.

2.6 Fenêtre : espaces topologiques

Il n'y a rien de compliqué, une fois qu'on a défini la topologie quotient (voir sur Wikipédia). Une *quotient map*, le terme n'ayant pas d'équivalent en français, est une application continue et ouverte : une application est ouverte, si l'image de tout ouvert est ouverte.

2.7 Tableau récapitulatif

Catégorie	Quotient par...	Théorèmes de factorisation	Théorèmes d'isomorphisme
Ensembles	Relation d'équivalence $\mathcal{R}$	f est compatible avec $\mathcal{R}$ ssi $\exists! \tilde{f} \quad f = \tilde{f} \circ \pi$	Pour $\mathcal{R} : x \sim y \Leftrightarrow f(x) = f(y)$, $E/\mathcal{R} \simeq \operatorname{Im} f$ (par $\tilde{f}$)
Magmas	Relation d'équivalence $\mathcal{R}$ avec laquelle la loi de magma est compatible	φ morph. est compatible avec $\mathcal{R}$ ssi $\exists! \tilde{\varphi}$ morph. $\quad \varphi = \tilde{\varphi} \circ \pi$	Pour $\mathcal{R} : x \sim y \Leftrightarrow \varphi(x) = \varphi(y)$, $E/\mathcal{R} \simeq \operatorname{Im} \varphi$ (par $\tilde{\varphi}$)
Monoïdes, groupes (naïvement)	Idem	Idem	Idem
Groupes	Sous-groupe distingué H	$H \subseteq \operatorname{Ker}(f)$ ssi $\exists! \tilde{f}$ morph. $\quad f = \tilde{f} \circ \pi$	$G/\operatorname{Ker}(f) \simeq \operatorname{Im} f$
Anneaux	Idéal I	$I \subseteq \operatorname{Ker}(f)$ ssi $\exists! \tilde{f}$ morph. $\quad f = \tilde{f} \circ \pi$	$A/\operatorname{Ker}(f) \simeq \operatorname{Im} f$
Espaces vectoriels	Sous-espace vectoriel V	$V \subseteq \operatorname{Ker}(f)$ ssi $\exists! \tilde{f}$ lin. $\quad f = \tilde{f} \circ \pi$	$E/\operatorname{Ker}(f) \simeq \operatorname{Im} f$
Espaces topologiques	Relation d'équivalence $\mathcal{R}$, quotient muni de la topologie quotient	f C^0 est compatible avec $\mathcal{R}$ ssi $\exists! \tilde{f}$ C^0 $\quad f = \tilde{f} \circ \pi$	Pour $\mathcal{R} : x \sim y \Leftrightarrow f(x) = f(y)$, f continue et ouverte (*quotient map*), $E/\mathcal{R} \simeq \operatorname{Im} f$ (par $\tilde{f}$)

FIGURE 1. — *Tableau récapitulatif des phénomènes de factorisation et d'isomorphisme dans les structures quotients selon les catégories.* Il est très beau.

3 Compléments amusants

3.1 Quelques exercices

Exercice 76

Montrer qu'un ensemble E non vide est infini si et seulement si l'on a conjointement $E^E \simeq \mathcal{P}(E)$ et $\operatorname{card}(E) \neq 2$.

Exercice 77

1. Montrer que $\sum \frac{\sin(n)}{n}$ est semi-convergente.

2. En admettant le théorème de Cantor-Bernstein, montrer que $\mathfrak{S}(\mathbb{N})$ a exactement la puissance du continu.

Exercice 78

On appelle *groupe de* $\mathfrak{M}_n(\mathbb{K})$, $\mathbb{K}$ un corps commutatif, ou *groupe de matrices* toute partie de $\mathfrak{M}_n(\mathbb{K})$ stable pour la loi multiplicative induite et qui, muni d'elle, soit un groupe.

1. Montrer que tout groupe de $\mathfrak{M}_n(\mathbb{K})$ dans $\mathcal{GL}_n(\mathbb{K})$ est un sous-groupe de ce dernier.

2. Y a-t-il d'autres groupes de $\mathfrak{M}_n(\mathbb{K})$ que ceux-ci ?

3. Justifier que tout groupe de matrices est un sous-groupe du groupe linéaire ou est constitué uniquement de matrices non inversibles.

4. Montrer que les groupes de $\mathfrak{M}_n(\mathbb{K})$ sont exactement les sous-groupes des conjugués des groupes de la forme : $\left\{ \begin{pmatrix} M & O_{n-r} \\ O_{n-r} & O_{n-r} \end{pmatrix} \mid M \in \mathcal{GL}_r(\mathbb{K}) \right\}$, $r \in [\![0, n]\!]$.

5. Quels sont les éléments neutres des groupes de $\mathfrak{M}_n(\mathbb{K})$?

Exercice 79

Montrer qu'un sous-groupe non trivial d'un groupe est d'indice 2 si et seulement s'il respecte la règle des signes. En déduire qu'un tel sous-groupe est toujours normal.

Exercice 80

1. Quel est le conjugué d'un cycle par une permutation σ ?

2. *Cette question utilise l'exercice précédent.* Montrer que pour tout $n \in \mathbb{N}$, $\mathfrak{A}_n$ est le seul sous-groupe de $\mathfrak{S}_n$ de cardinal $\frac{n!}{2}$.

3. Montrer que ε est le seul morphisme de groupe de $(\mathfrak{S}_n, \circ)$ dans $(\mathbb{C}^*, \times)$.

Exercice 81

Montrer que le groupe diédral d'ordre 3 noté D_6 (groupe des isométries du plan qui conservent les 3-gones, c'est-à-dire les triangles) est isomorphe au groupe symétrique $\mathfrak{S}_3$.

Exercice 82

Un groupe est *simple*, si tous ses sous-groupes distingués sont triviaux.

1. Quels sont les groupes commutatifs simples ?

2. Montrer que $\mathcal{SO}_n(\mathbb{R})$ est simple si et seulement si n est impair.

3. *(Thème pour l'agrégation : simplicité du groupe alterné)* Montrer que $\mathfrak{A}_n$ est simple si et seulement si $n \neq 2$ ou 4 .

Exercice 83

1. Montrer que $\mathfrak{A}_n$ est son propre dérivé.

2. Montrer que $\mathfrak{A}_n$ est le dérivé du groupe symétrique d'ordre n.

Exercice 84

Un sous-groupe d'un groupe est *strictement caractéristique* s'il est stable par tout endomorphisme caractéristique. Il est *pleinement caractéristique* s'il est stable par tout endomorphisme. Caractériser la caractérisation du centre d'un groupe.

3.2 Une preuve constructive du théorème de Cantor-Bernstein

Propriété. *(Théorème de Cantor-Schröder-Bernstein)*

Soient A et B deux ensembles. S'il existe une injection de A dans B, et s'il existe une injection de B dans A, alors A et B sont en bijection. Autrement dit, la relation $\hookrightarrow$ est antisymétrique.

Il existe un grand nombre de preuves du théorème de Cantor-Bernstein ; nous en donnons une constructive et qui ne fait pas recours à l'axiome du choix. Soient A et B deux ensembles, dont on suppose qu'il existe une application injective $f : A \longrightarrow B$, et d'autre part qu'il existe une application $g : B \longrightarrow A$ injective. Ce sont des applications, c'est-à-dire que tout élément de leur départ admet une image.

Remarquons que la corestriction $\tilde{g} : B \longrightarrow \mathcal{I}m(g) \subseteq A$, qui à un élément de B fait correspondre son image par g, est toujours injective, et surjective par construction. C'est donc une bijection. Si l'on exhibe une bijection $h : A \longrightarrow \mathcal{I}m(g)$, c'est-à-dire un bijection de A sur son sous-ensemble $\mathcal{I}m(g)$ a priori strict, alors la fonction $h^{-1} \circ \tilde{g} : B \longrightarrow A$ est une bijection de B dans A et A et B sont en bijection.

Pour construire h, on introduit la suite $(A_n)_{n\in\mathbb{N}}$ de parties de A en posant $A_0 = \complement_A \mathcal{I}m(g)$, et pour tout $n \in \mathbb{N}^*$, $A_{n+1} = g \circ f(A_n)$. De façon immédiate, on a, pour tout entier naturel n, $A_n = (g \circ f)^n(A_0)$. Démontrons d'abord que les A_n sont toutes deux à deux disjointes. Si i est un entier naturel non nul, alors $A_i = (g \circ f)^i(A_0) = g(f \circ (g \circ f)^{i-1})(A_0)$. Par suite, $A_i \subseteq \complement_A A_0$, ce qui signifie exactement que A_i et A_0 sont disjoints. Soit maintenant un entier naturel n. Par composition, $g \circ f$ est une injection, puis encore $(g \circ f)^n$ est injective. En composant l'intersection $A_0 \cap A_i = \emptyset$ par une injection, on obtient l'inclusion $(g \circ f)^n(A_0) \cap (g \circ f)^n(A_i) \subseteq g \circ f(\emptyset) = \emptyset$, l'image de l'ensemble vide par une application étant toujours vide. Ainsi $(g \circ f)^n(A_0) \cap (g \circ f)^n(A_i) = \emptyset$. Or $(g \circ f)^n(A_0) = A_n$ et $(g \circ f)^n(A_i) = A_{n+i}$, donc A_n est disjoint de A_{n+i} pour tous $n \geq 0, i > 0$. Par conséquent, les $A_n, n \in \mathbb{N}$, sont deux à deux disjoints.

Cette construction permet d'écrire que : $g \circ f(\bigcup_{n=0}^{+\infty} A_n) = \bigcup_{n=0}^{+\infty} g \circ f(A_n) = \bigcup_{n=1}^{+\infty} A_n$. (Le caractère injectif n'intervient pas dans cette égalité.)

Définissons la fonction h par :

$$\begin{array}{rcl} h : A & \longrightarrow & \mathcal{I}m(g) \\ a & \longmapsto & \begin{cases} g \circ f(a) \text{ si } a \in \bigcup\limits_{n=0}^{+\infty} A_n, \\ a \text{ sinon.} \end{cases} \end{array}$$

Vérifions que h est une application bijective.

- ▷ Elle est bien définie partout sur son ensemble de définition.
- ▷ Elle est aussi à valeurs dans $\mathcal{I}m(g)$, puisque par construction, $g \circ f$ envoie $\bigcup\limits_{n=0}^{+\infty} A_n$ sur $\bigcup\limits_{n=1}^{+\infty} A_n \subseteq \mathcal{I}m(g)$, et que si $a \notin \bigcup\limits_{n=0}^{+\infty} A_n$, alors en particulier $a \notin A_0 = \complement_A \mathcal{I}m(g)$ donc $a = h(a) \in \mathcal{I}m(g)$.
- ▷ L'injectivité provient de ce que d'abord $g \circ f$ est une injection. Par suite, $id_{|\complement_A \bigcup\limits_{n=0}^{+\infty} A_n}$ et les $(g \circ f)_{|A_n}$ sont des injections, par restriction. De plus, ces injections sont à images disjointes d'après ce que nous avons montré précédemment, car les $A_0, ..., A_n, ...$ sont deux à deux disjointes et toutes dans $\bigcup\limits_{n=0}^{+\infty} A_n$ qui est disjoint de $\complement_A \bigcup\limits_{n=0}^{+\infty} A_n$.
- ▷ D'autre part, on a dit que $g \circ f$ envoie $\bigcup\limits_{n=0}^{+\infty} A_n$ sur $\bigcup\limits_{n=1}^{+\infty} A_n$, ce qui garantit la surjectivité. En effet, si $y \in \mathcal{I}m(g)$, alors $y \notin A_0$, et l'on a :

  1er cas. $y \in \bigcup\limits_{n=1}^{+\infty} A_n$. Alors la remarque précédente donne l'existence d'un antécédent dans $\bigcup\limits_{n=0}^{+\infty} A_n \subseteq A$.

  2e cas. $y \notin \bigcup\limits_{n=1}^{+\infty} A_n$. Alors $y \notin \bigcup\limits_{n=0}^{+\infty} A_n$, donc $h(y) = y$ et l'antécédent y convient.

Ainsi h est une bijection, ce qui permet de conclure.

3.3 Axiome de fondation

Un petit développement sur l'axiome de fondation, axiome supplémentaire de la théorie des ensembles classiques (au même titre que l'axiome du choix) et qui n'est pas du tout utile. C'est pourquoi les discussions à propos de son adoption ne sont pas véhémentes, et l'on peut considérer des théories tout à fait semblables en termes des mathématiques que nous connaissons munies soit d'un axiome de fondation, soit d'un axiome d'anti-fondation. Le principe général de l'axiome de fondation est d'interdire la construction d'ensembles qui s'appartiennent eux-mêmes.

3.3.1 Retour sur la relation d'appartenance

En théorie naïve des ensembles, on pose qu'il existe des objets, appelés *ensembles*, liés par une relation dite d'appartenance, et notée $\in$, et dont les règles de construction sont regroupées en une liste d'axiomes. Tout ce que nous appelons *élément* est ensemble, et réciproquement tout ensemble peut-être vu comme un élément[9]. Ce que sont les ensembles n'est pas précisé. Plus

[9] En effet, si E : Ens, *i.e.* « E est un ensemble », alors d'après l'axiome de la paire, $E \in F$ en posant $F = \{E\}$.

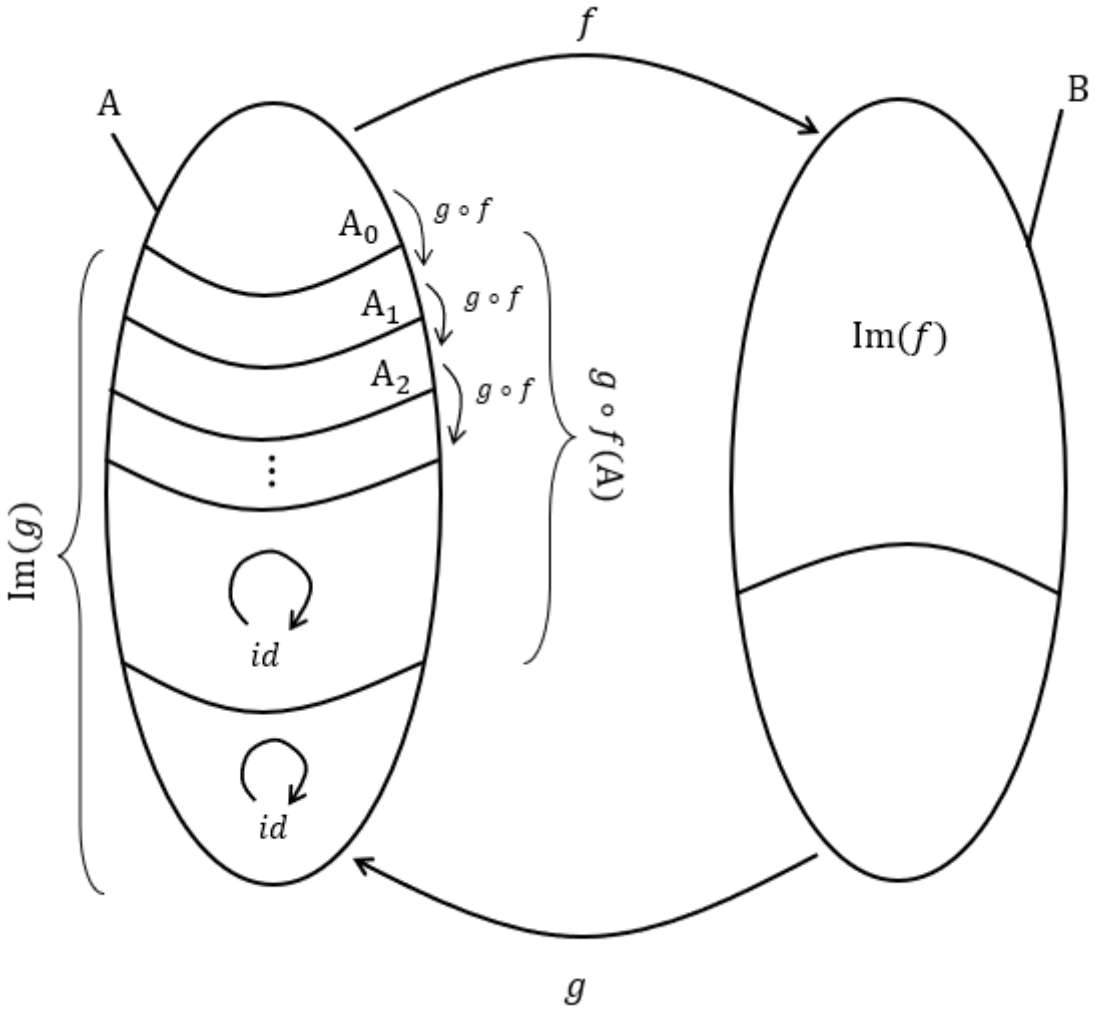


FIGURE 2. — *Illustration de la preuve du théorème de Cantor-Bernstein*

généralement, on regroupe le concept intuitif de collection d'objets sous le terme de *classe*, de sorte que tout ensemble soit une classe, mais ce n'est pas réciproque : par exemple, la classe regroupant tous les ensembles n'est pas un ensemble (paradoxe de Russell) ; elle est dite impropre.

La liste des axiomes choisis constitue les fondements de la théorie ; si quelques axiomes semblent essentiels à la construction d'une théorie des ensembles pertinente, pour d'autres, la communauté n'est pas décidée, tant qu'ils sont indépendants (aucun axiome n'est conséquence logique des autres), c'est en particulier le cas pour l'axiome du choix. Ceci mène à l'élaboration de différents *modèles* d'une théorie, à laquelle nous associons les noms de leur créateur, avec plus ou moins de précision : Z pour Zermelo, ZF pour Zermelo et Fraenkel, ZFC pour ce système d'axiomes additionné de l'axiome du choix.

Ainsi les axiomes, qui sont admis obtusément, ont pour but primaire de régir les règles de construction d'ensembles et relatives à la relation d'appartenance notée $\in$, en hommage au ϵ grec, pour le verbe « est » en latin. Le but de cette section est de donner de la relation

d'appartenance quelques propriétés importances, avec pour conséquence notable la construction véritable des entiers naturels.

3.3.1.1 Notion intuitive d'appartenance

Axiome. *(Relation d'appartenance)*
Sur la classe des ensembles, il existe une relation notée $\in$, c'est-à-dire une partie (impropre) de Ens $\times$ Ens.

Exemples.

1. $1, 2, 3 \in \mathbb{N}$;
2. $-1 \notin \mathbb{N}$;
3. $-1, 1 \in \mathbb{Z}$;
4. $(-1, 1) \notin \mathbb{N}$;
5. $(-1, 1) \in \mathbb{Z} \times \mathbb{N}$;
6. $(-1, 1) \in \{-1\{\times\{1\}, \{-1, 1\}^2$;
7. $\mathbb{N} \in \{\mathbb{N}, \mathbb{Z}, \mathbb{Q}\}$;
8. $\mathbb{R} \notin \mathbb{R}^2$;
9. $\mathbb{N} \notin \mathbb{R}$;
10. $\emptyset \in \{\emptyset\}$;
11. $\emptyset \notin \emptyset$;
12. $\{1, 2, 3\} \subseteq \{1, 2, 3, 4\}$;
13. $\{1, 2, 3\} \notin \{1, 2, 3, 4\}$;
14. $\left\{^{\{1,2,3\} \in \{\{1,2,3\},1,2,3,4\}}\right\}$;
15. $\mathbb{N} \subseteq \mathbb{N} \cup \{-1\}$;
16. $\{\emptyset\} \notin \emptyset$.

Quelques propriétés très intuitives.

Propriété. *(Non-transitivité de l'appartenance)*
La relation d'appartenance n'est pas transitive (mais pas intransitive).

▷ Il suffit de prendre pour exemples : $1 \in \{1, 2\} \in \{\{1, 2\}, 2\}$, mais $1 \notin \{\{1, 2\}, 2\}$. La construction et structure des ensembles entiers naturels sera justifiée plus tard. ■

Propriété. *(Non-totalité de l'appartenance)*
La relation d'appartenance est partielle.

▷ On a $\emptyset \notin \{\{\emptyset\}\}$ et $\{\{\emptyset\}\} \notin \emptyset$ (le vérifier soi-même). ■

Remarques.

1. Par essence de la théorie des ensembles, tout objet est ensemble. Un problème émerge : il n'y a pas de distinction absolue entre les ensembles et leurs éléments. On comprend que $\mathbb{N}$, $\mathbb{Z}$,..., $\mathbb{R}$, soient des ensembles, mais on conçoit mal que $1, 2, \pi, x \longmapsto x^2, \mathbb{P}, \int_1^2 e^{it}\mathrm{d}t, \int_1^{+\infty} e^t \mathrm{d}t$ le soient également. C'est pourtant le cas.
2. L'axiome de fondation, noté AF dans la suite, répond aux questions suivantes : $\in$ est-elle réflexive ? et $\in$ est-elle symétrique, antisymétrique ? On propose au lecteur de se poser la question lui-même avant de trouver la réponse dans la suite.

Exercice 85

Expliciter les ensembles $1, 2, \pi, x \longmapsto x^2, \mathbb{P}, \int_1^2 e^{it}\mathrm{d}t$.

3.3.1.2 Axiomes déjà connus quant à $\in$

Axiome. *(Principe d'extensionnalité)*
Pour tous A, B : Ens, $(A = B) \Leftrightarrow (\forall x\ (x \in A \Leftrightarrow x \in B))$.

Remarques.

1. C'est le premier axiome.
2. C'est en fait une définition, celle de « $=$ » . Cette relation d'égalité est définie entre les ensembles, et l'on peut garder en mémoire que toutes les relations d'égalités utilisées quotidiennement sont des *restrictions* de cette relation définie sur une classe impropre.
3. Le syntagme « $\forall x$ » seul apparaissant dans la formulation de l'axiome n'est pas un abus, mais la notation la plus correcte pour : « pour tout ensemble x... » . Quand on note, $\forall x \in \mathbb{R},\ \mathrm{Re}(x) = x$, on raccourcit la plus correcte : $(\forall x, x \in \mathbb{R} \Rightarrow \mathrm{Re}(x) = x)$.

Un petit rappel qui ne fait pas de mal.

Définition. *(Inclusion)*
Pour tous A, B : Ens, on dit que $A \subseteq B$ si $\forall x,\ x \in A \Rightarrow x \in B$.

Remarque. L'idée fondamentale de l'inclusion est son rapport avec l'appartenance : l'appartenance $\in$ est un notion locale, alors que l'inclusion $\subseteq$ est une notion globale.

On donne quelques applications du principe d'extensionnalité, sachant qu'un peu de raisonnement axiomatique n'est pas luxueux. Dans le théorème suivant, l'existence d'un ensemble des parties en conséquence de l'axiome d'existence d'ensemble des parties. Nous ne donnons pas tous les axiomes, au risque de faire inventaire. Le lecteur intéressé peut les trouver à l'adresse : http ://math.univ-lyon1.fr/ melleray/AnnexeA.pdf.

Théorème. *(Identité d'ensembles par les ensembles des parties)*
Pour tous A, B : Ens, $A = B \Leftrightarrow \mathcal{P}(A) = \mathcal{P}(B)$.

▷ Si $A = B$, $\forall x\ x \in A \Leftrightarrow x \in B$. Or $\forall X\ X \subseteq A \Leftrightarrow \forall x \in X\ x \in A$, donc on vérifie : $\forall X\ X \subseteq A \Leftrightarrow X \subseteq B$, soit par définition $\mathcal{P}(A) = \mathcal{P}(B)$: c'est l'extensionnalité, car $\mathcal{P}(A) = \{X \mid X \subseteq A\}$. Réciproquement, si $A \neq B$, il existe $x \in B$, $x \notin A$ (ou $x \in A, x \notin B$, cas qui se traite de la même manière). Dans le premier cas, $\{x\} \subseteq B$ mais $\{x\} \not\subseteq A$, car sinon $x \in A$. Ainsi $\{x\} \in \mathcal{P}(B)$ mais $\{x\} \notin \mathcal{P}(A)$, donc par extensionnalité $\mathcal{P}(A) \neq \mathcal{P}(B)$. Par contraposée, $\mathcal{P}(A) = \mathcal{P}(B) \Rightarrow A = B$, d'où l'équivalence. ■

Remarque. Une chose remarquable du théorème, et que l'égalité des ensembles des parties n'est qu'une égalité d'ensembles, et pas une correspondance deux à deux des parties.

Théorème. *(Singletons associés)*
$\forall A, B\ A = B \Leftrightarrow \{A\} = \{B\}$.

▷ D'une part, on suppose $A = B$. Soit $x \in \{A\}$. Alors puisque c'est un singleton, $x = A$. Or $A = B$, donc $x = B$, et $B \in \{B\}$ donc $x \in \{B\}$. Ainsi $\{A\} \subseteq \{B\}$. Semblablement, $\{B\} \subseteq \{A\}$, donc par double inclusion $\{A\} = \{B\}$.

Réciproquement, supposons $\{A\} = \{B\}$. $A \in \{A\}$ et $\{A\} = \{B\} \Leftrightarrow (\forall x \in \{A\}\ x \in \{B\} \wedge \forall x \in \{B\}\ x \in \{A\})$. Le premier point de la conjonction, avec la première remarque faite donne $A \in \{B\}$, soit $A = B$, car $\{B\}$ est un singleton. ■

Remarques.

1. De même que pour le théorème précédement, l'existence du singleton contenant A est axiomatique. (Elle vient de l'axiome... de la paire. Il n'y pas d'axiome du singleton : pour l'en déduire, il suffit de prendre, dans la paire, les deux éléments identiques, et l'on se rend compte qu'un axiome de singleton serait superflu, car il est déjà constructible à partir de l'axiome de la paire.)
2. La contraposée du théorème donne : $A \neq B \Leftrightarrow \{A\} \neq \{B\}$.

Propriété. *(Partition triviale par événements atomiques, partition discrète)*
Soit Ω un ensemble. Alors $(\{x\})_{x \in \Omega}$ partitionne Ω.

▷ Il suffit de reprendre point par point la définition de partition.

- ▶ **Habitations.** Soit $x \in \Omega$, c'est-à-dire $\{x\}$ dans la partition. $\text{card}(\{x\}) = 1 \neq 0$, donc les parties de la partition ne sont pas vides.
- ▶ **Disjonction deux à deux.** C'est la contraposée du théorème des singletons associés.

▶ **Réunion.** $\bigcup_{x\in\Omega} = \Omega$. En effet : $X \in \bigcup_{x\in\Omega} \Leftrightarrow \exists x \in \Omega\ x = X$, soit $\bigcup_{x\in\Omega} \Leftrightarrow x \in \Omega$. Ainsi, on a l'égalité par extensionnalité,

ce qui termine la preuve. ■

Remarque. On aurait pu le démontrer beaucoup plus rapidement : l'égalité sur E est une relation d'équivalence, dont les classes sont les $(\{x\})_{x\in\Omega}$ et d'après le théorème fondamental des relations d'équivalence, c'est une partition de Ω.

3.3.1.3 Clarification de l'ambivalence entre ensemble et élément

On a vu que tout élément est en fait un ensemble complétement, et que la distinction entre les deux n'est réellement qu'un agrément de langage. Dans l'assertion :

$$E \in F,$$

E, F sont des ensembles, mais on dit plutôt que E est un élément, à savoir un élément de F. D'autre part, tout ensemble peut être vu comme un élément, on l'a déjà remarqué, car $\forall x, \in x \in \{x\}$, ce qui justifie de confondre le concept d'élément avec celui d'ensembles. Nous voulons, dans ce qui suit, corriger les imprécisions mentales issues de l'ambivalence entre les deux termes.

Propriété. *(Inclusions générales)*
(1) Tout ensemble inclut un ensemble ;
(2) Tout ensemble est inclus dans un ensemble ;
(3) Dans le cas où $\text{card}(E) \geqslant 1$, un ensemble inclut un autre ensemble ;
(4) Dans le cas général, tout ensemble est inclus dans un autre ensemble.

▷ Dans chacun des cas :

(1) $E \subseteq E$;
(2) $E \subseteq E$;
(3) $\emptyset \subseteq E$, et $E \neq \emptyset$, car, par hypothèse, il est de cardinal non nul, et l'ensemble vide existe d'après un axiome ;
(4) Soit F un ensemble, $F \notin E$. Il existe d'après le paradoxe de Cantor. Alors $E \subseteq E \cup \{F\} = G$, mais $G \neq E$, car $F \in G$ mais $F \notin E$,

et tout a été démontré. ■

En général, un élément d'un ensemble n'en est pas une partie. Par exemple $\{1\} \in \{\{1\}\}$, mais $1 \notin \{\{1\}\}$ donc $\{1\} \not\subseteq \{\{1\}\}$. Ceci n'est pas universel, c'est même faux dès que $E \ni \emptyset$ (pourquoi ?). Réciproquement, une partie d'un ensemble, en général, ne lui appartient pas : $\{1, 2\} \notin \mathbb{N}$ alors que $\{1, 2\} \subseteq \mathbb{N}$.

Propriété. *(Remarques supplémentaires)*
(1) Un ensemble n'est pas nécessairement disjoint de l'ensemble de ses parties ;
(2) On peut avoir $E \subseteq F$ et $E \in F$ même si $E \neq \emptyset$;
(3) Pour tout E, il existe F tel que $E \subseteq F$ et $E \in F$.

▷ (1) et (2) ont déjà été traités ci-dessus. Pour (3), il suffit de choisir $F = E \cup \{E\}$. ■

Remarquons que $E \cup \{E\} \neq E$: cette propriété universelle découle de l'axiome de fondation ; avant de l'introduire, on rend compte des implications d'une trop grande liberté dans les constructions relatives relation d'appartenance.

3.3.2 Bizarreries de la relation d'appartenance

Formalisons les conséquences des propriétés juste précédentes, pour en montrer les limites. Le premier objet bizarre engendré par de telles constructions est celui d'*ensemble transitif*.

3.3.2.1 Ensembles transitifs

On a vu que $\in$ n'était pas *a priori* transitive, mais également, qu'elle n'était pas pour autant intransitive. Les ensembles transitifs sont tels que la transitivité est toujours vraie, lorsqu'on ne regarde qu'eux, un par un.

Définition. *(Ensemble transitif)*
Un ensemble est dit *transitif* si les éléments de ses éléments en sont tous des éléments, autrement dit, A est transitif si et seulement si $\forall x \in A \forall a \in X \quad x \in A$.

Exemples.
1. $\emptyset$ est transitif. En effet, $\forall x \in \emptyset \ \forall a \in x \ x \in \emptyset$, car toute propriété commençant par $\forall x \in \emptyset$ est vraie par principe d'explosion ;
2. $\emptyset \cup \{\emptyset\}$ est transitif (le vérifier) ; ainsi l'ensemble vide n'est pas le seul transitif.

La notion d'ensemble transitif n'est pas du tout intuitive : elle montre les pathologies de la relation d'appartenance. AF n'interdit pas les ensembles transitifs, mais il les limite[10], en pratique, à ceux que nous voyons maintenant, c'est-à-dire, l'ensemble vide et ses composés selon le théorème suivant.

L'ensemble des parties d'un ensemble A est noté indifféremment $\mathcal{P}(A)$ ou $\beta(A)$.

Propriété. *(Caractérisation de la transitivité par l'ensemble des parties)*
Un ensemble A est transitif si et seulement si $A \subseteq \beta(A)$.

[10] En effet, si $E \in E$, alors E est automatiquement transitif.

▷ C'est une simple reformulation de la définition. Le lecteur un peu perdu aura intérêt à rédiger l'équivalence. ■

Théorème. *(Construction des ensembles transitif)*
Soit A un ensemble transitif.
(i) Alors $A \cup \{A\}$ est transitif ;
(ii) $\mathcal{P}(A)$ est également transitif.

▷ On montre l'une et l'autre des deux assertions :

(i) On fait une disjonction des cas : si $x \in A \cup \{A\}$, soit $x \in A$, dans ce cas, on applique la transitivité de A, donc pour tout $a \in x$, $x \in A$ donc $x \in A \cup \{A\}$. Si d'autre part $x \in \{A\}$, alors $x = A$, donc si $a \in x = A$, $a \in A$ donc $a \in A \cup \{A\}$ de même.

(ii) Si $x \in a \in \mathcal{P}(A)$, $x \in a \subseteq A$, soit $x \in A$ par définition de l'inclusion, donc par définition $x \subseteq A$, soit $x \in \mathcal{P}(A)$ et $\mathcal{P}(A)$ est transitif.

Ainsi l'on a montré les deux règles de construction. ■

On espère avoir assez brouillé les esprits croyant l'apparente commodité de la relation d'appartenance. Avant de passer à l'énoncé de AF, on rappelle le paradoxe suivant, beaucoup utile.

3.3.2.2 Paradoxe de Russell

Soit la collection des objets : $\{X \mid X \notin X\} = \mathcal{C}$.

Paradoxe. *(Paradoxe de Russell)*
La construction de $\mathcal{C}$ est paradoxale.

▷ Par principe logique de tiers-exclu, on a, soit $\mathcal{C} \in \mathcal{C}$, soit $\mathcal{C} \notin \mathcal{C}$. Supposons pour commencer $\mathcal{C} \in \mathcal{C}$. Alors par définition de $\mathcal{C}$, $\mathcal{C} \notin \mathcal{C}$, car $\mathcal{C}$ est un X tel que $X \in \mathcal{C}$. Inversement, supposons que $\mathcal{C} \notin \mathcal{C}$. Par définition, $\mathcal{C}$ contient tous les X tels que $X \notin X$, et $\mathcal{C}$ vérifie ce prédicat logique, donc $\mathcal{C} \in \mathcal{C}$. Ainsi, dans les deux cas logiques possibles, on a ($\mathcal{C} \in \mathcal{C}$ ET $\mathcal{C} \notin \mathcal{C}$), donc cette proposition est universellement vraie. Or elle est universellement fausse selon le principe de non-contradiction, donc la propriété « la propriété $\mathcal{C} \in \mathcal{C}$ ET $\mathcal{C} \notin \mathcal{C}$ est vraie » est la fois vraie et fausse, ce qui est contradictoire par non-contradiction. ■

Le constat du paradoxe de Russell a conduit à la création d'un des premiers axiomes de la théorie des ensembles, les schémas de séparation : on ne peut pas construire des ensembles à partir de rien, mais il y a une règle : si E existe, et $\mathcal{P}$ est un prédicat logiquement bien formé sur E, alors on peut considérer l'ensemble $\{x \in E \mid \mathcal{P}(x)\}$, d'où le nom de définition par séparation et compréhension. C'est la raison pour laquelle il faut écrire toujours : $\forall x \in \mathbb{R}...$, $\forall f \in \mathbb{C}^{\mathbb{Z}}...$

(Notons qu'il faut également postuler l'existence d'au moins un ensemble, ce que l'on fait avec l'axiome de l'ensemble vide.)

La faute commise dans le paradoxe de Russell est d'avoir postulé l'existence de l'ensemble $\mathcal{C}$: il n'est pas défini par séparation, donc *a priori*, il n'existe pas. En effet, l'on sait que $\mathcal{C}$, d'après l'axiome de fondation, est Ens la classe de tous les ensembles, et d'après le théorème de Cantor, ce n'est pas un ensemble, autrement dit une classe impropre.

3.3.3 L'axiome de fondation proprement dit

⟶ **Notation.** On notera $ZF_\bullet$ l'ensemble des axiomes de Zermelo-Fraenkel sans l'axiome de fondation, et $ZF = ZF_\bullet + AF$.

On rappelle les quelques interrogations initiales de cette section :

⋆ $\in$ est-elle réflexive ?

⋆ $\in$ est-elle symétrique, antisymétrique, ou sous quelles conditions ?

c'est-à-dire, existe-t-il, et lesquels, des ensembles E, F tels que :

⋆ $E \in E$?

⋆ $E \in F$ et $F \in E$?

3.3.3.1 Énoncé et premières propriétés

Axiome. *(Axiome de fondation)*
Pour tout ensemble A, $A \neq \emptyset \Rightarrow \exists B \in A \; B \cap A = \emptyset$.

Remarques.

1. C'est chelou.
2. On verra que ceci exprime que la relation $\in$ est *bien fondée* sur la classe des ensembles, c'est-à-dire, qu'il existe toujours sur tout ensemble et l'ensemble des éléments qu'il contient, et l'ensemble des éléments qu'ils contiennent, etc., un élément minimal pour l'appartenance, et donc qu'il n'existe pas de suite infinie du type $E \ni F \ni G \ni ...$ Nous verrons même que, modulo un axiome du choix spécial, cette assertion est équivalente à AF.

Théorème. *(Irréflexivité de $\in$)*
Pour tout ensemble E, $E \notin E$.

▷ Si $E \in E$ pour un certain ensemble E, notons $A = \{E\}$. Dans ce cas, $A \neq \emptyset$, car A est un singleton donc de cardinal $1 \neq 0$. De plus, si $x \in A$, $x \in \{E\}$ soit $x = E$ et $x \cap A \neq \emptyset$, car $x \cap A = E \cap \{E\}$, et puisque $E \in \{E\}$ et $E \in E$ par hytpohèse, on aurait $E \in E \cap \{E\}$, ce qui contredirait AF. Par contraposition, $AF \Rightarrow \forall E, \; E \notin E$, c'est-à-dire $\nexists E, \; E \in E$. ■

Remarques.

1. Ce théorème d'irréflexivité se réécrit en : il n'existe pas d'ensemble E tel que $E = \{E\}$.
2. On en déduit immédiatement ce que l'on a évoqué tout à l'heure : pour tout ensemble E, $E \cup \{E\} \neq E$. En effet, cela voudrait dire que, comme $E \in E \cup \{E\}$, $E \in E$.
3. On constate que l'irréflexivité est encore vérifiée pour l'ensemble vide. En effet, $\emptyset$ ne peut contenir aucun élément, y compris $\emptyset$.

On arrive désormais aux équivalences centrales de cette partie, qui donnent tout son sens à la formulation initiale un peu obscure de l'axiome de fondation. Avant cela, on rappelle l'énoncé de l'axiome du choix dépendant qui servira ensuite pour établir une formulation équivalente de AF.

Axiome. *(Axiome du choix dépendant)*

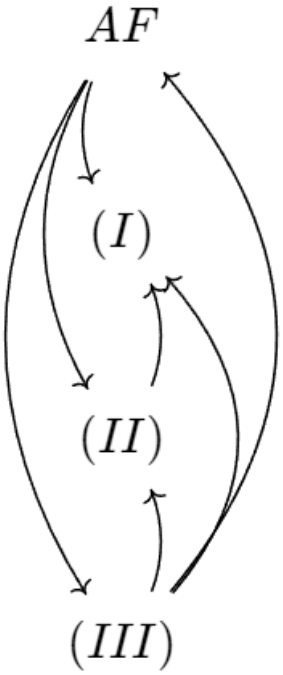
Pour tout $X \neq \emptyset$, pour toute relation binaire $\mathcal{R}$ sur X, si le domaine de définition de $\mathcal{R}$ est bien X (autrement dit si tout élément $x \in X$ est bien tel qu'il existe un $y \in X$ tel que $(x, y) \in \mathcal{R}$), alors il existe une suite $(x_n) \in X^{\mathbb{N}}$ telle que pour tout entier naturel n, $x_n \mathcal{R} x_{n+1}$. On note cet axiome DC.

Propriété. *(Formulations diverses de l'axiome de fondation)*

On considère les propriétés suivantes :
AF l'axiome de fondation ;
(I) l'irréflexivité de la relation d'appartenance ;
(II) « Il n'existe pas $x_1, ..., x_n$ n ensembles, $n \in \mathbb{N}^*$ tels que $x_1 = x_n$ et $x_1 \in ... \in x_n$ » ;
(III) « $\in$ est bien fondée, c'est-à-dire qu'il n'existe pas de suite $(x_n)_{n\in\mathbb{N}}$ d'ensembles décroissante pour $\in$ » .
Alors on a les implications relatives comme représentées sur la figure. En particulier, elles sont toutes vraies dans un système ayant pour axiome AF. Les autres sont de simples conséquences logiques les unes des autres, mais $(III) \Leftrightarrow AF$ en présence de l'axiome du choix dépendant.

▷ Montrons chacune des flèches précédentes, qui représentent des implications.

- ► $AF \Rightarrow (I)$. On l'a déjà montré, c'est l'objet de la propriété précédente.
- ► $AF \Rightarrow (II)$. De même, par contraposée. Supposons $x_1 \in ... \in x_n = x_1$. On pose $E = \{x_1, ..., x_n\}$, qui n'est pas vide puisque $n \neq 0$. On construit ainsi un contre-exemple de l'axiome de fondation. En effet, soit $x \in E$. $x = x_i$ où $i \in [\![1, n[\![$, car $x_1 = x_n$. $x \cap E = x_i \cap \{x_1, ..., x_{n-1}\}$. Dans le premier cas, $i \neq 1$. On a $x_{i-1} \in x_i$ par hypothèse et $x_{i_1} \in \{x_1, ..., x_{n-1}\}$, donc $x_{i-1} \in x \cap E$ qui est donc non vide. Dans le deuxième cas, $i = 1$. Alors $x_{n-1} \in x_i = x_n$ et $x_{n-1} \in \{x_1, ..., x_{n-1}\}$ donc $x_{n-1} \in x \cap E$ qui n'est pas vide encore une fois. Ainsi $\neg AF$.
- ► $AF \Rightarrow (III)$. Remarquons en passant que c'est faux pour une suite qui serait croissante, il suffit de prendre $x_0 = \emptyset$ et $x_{i+1} = \{x_i\}$ pour tout $i \in \mathbb{N}$. Soit donc une suite infinie décroissante $x_0 \ni$



$... \ni x_n \ni ...$; l'axiome de la réunion permet de former $E = \cup_{n\in\mathbb{N}}\{x_n\} = \mathrm{Im}(x)$: l'existence de la suite (x_n) est hypothétique donc certaine. $E \neq \emptyset$, car $E \ni x_{47}$. Soit $x \in E$. $x \cap E = x_i \cap \cup_{n\in\mathbb{N}}\{x_n\}$, $i \in \mathbb{N}$ fixé choisi. On a à la fois $x_{i+1} \in x_i$ par hypothèse de chaîne et $x_{i+1} \in \{x_0, ..., x_n, ...\} = \cup_{n\in\mathbb{N}}\{x_n\}$ donc $x_{i+1} \in x \cap E$ qui est non vide. Ainsi, on nie l'axiome de fondation et l'on conclut par contraposition.

- $(III) \Rightarrow (I)$. On raisonne encore par contraposée : si $A \in A$, alors la suite constante $(A)_{n\in\mathbb{N}}$ convient pour nier (III).
- $(III) \Rightarrow (II)$. On raisonne par contraposée, en concaténant : $x_n \ni ... \ni x_1 \ni x_{n-1} \ni ... \ni x_1 \ni x_{n-1} \ni ....$ Plus précisément, on définit comme contre-exemple de (III) la suite infinie décroissante : $(u_i)_{i\in\mathbb{N}}$ telle que $u_0 = x_n$, et pour tout $i \in \mathbb{N}$, $u_i = x_{n-k-1}$ où k est le reste dans la division euclidienne de i par n.
- $(II) \Rightarrow (I)$. Il suffit de prendre $n = 1 \in \mathbb{N}^*$.
- $(III), DC \Rightarrow AF$. Toujours par contraposition. Le principe de démonstration est le suivant : nions AF. On suppose qu'il existe $A_0 \neq \emptyset$ tel que $\forall B \in A_0, B \cap A_0 \neq \emptyset$ (c'est exactement $negAF$). A_0 étant non vide, prenons $B_0 \in A_0$. $B_0 \cap A_0$ d'après ce qui précède, donc on peut prendre $A_1 \in B_0 \cap A_0$. Mais en particulier $A_1 \in A_0$, donc $A_1 \cap A_0 \neq \emptyset$ par hypothèse. Alors on peut prendre $A_2 \in A_1 \cap A_0$. Mais $A_2 \in A_0$, donc $A_2 \cap A_0 \neq \emptyset$ toujours par hypothèse, et l'on prend $A_3 \in A_2 \cap A_0$, etc. Cette intuition que l'on va pouvoir creuser à l'infini dans les éléments de B, d'où le terme de fondation, se formalise exactement avec DC. On prend, dans la définition de DC, $X = A_0 \neq \emptyset$ et pour relation $\ni$ la relation symétrique de $\in$. $\ni$ est bien définie partout sur X, en effet c'est l'hypothèse : $\forall B \in A_0\ B \cap A_0 \neq \emptyset$, c'est-à-dire, $\forall B \in A_0\ \exists x \in A_0\ x \in B$ soit $B \ni x$. Ainsi, DC s'applique et il existe une suite $(x_i)_{i\in\mathbb{N}}$ telle que $\forall i \in \mathbb{N}, x_i \ni x_{i+1}$, soit $\neg(III)$,

et tout a été démontré. ■

Enfin, on règle le compte de la symétrie de la relation d'appartenance. On voit qu'elle n'est pas symétrique, et même asymétrique. De plus, elle n'est asymétrique que si l'un des deux ensembles est vide afin d'appliquer le principe d'explosion.

Corollaire. *(Asymétrie de la relation d'appartenance)*
Il n'existe pas d'ensembles E, F tels que $E \in F$ et $F \in E$.

▷ C'est une conséquence de (II) pour $n = 2$. ■

Remarque. Une autre façon de le dire, est qu'aucun ensemble n'est élément d'un de ses éléments.

Questions ouvertes. Il est naturel de se demander si l'on peut clore le diagramme ci-dessous, de sorte que les quatre propositions soient en fait équivalentes : (II), et *a fortiori* (I), impliquent-ils AF ? La question n'a peut-être pas de réponse, car trouver un exemple de théorie (on dit : un *modèle*) dans laquelle les axiomes de ZF sont vérifiés est en fait impossible, c'est le théorème d'incomplétude de Gödel, et il serait problématique de montrer alors que AF et (I) ne sont pas équivalentes, d'où la difficulté de traiter $\neg AF \Rightarrow \neg(I)$.

3.3.3.2 Conséquences pour la construction d'objets mathématiques

Exercice 86
Montrer que $\{\{\emptyset\}\} \neq \{\emptyset\}$.

Exercice 87
Montrer que, pour tout ensemble x, $\{\{x\}\} \neq x$.

Exercice 88
Montrer que, pour tout ensemble x, pour tout $p \in \mathbb{N}^*$, $\underbrace{\{\{...\{}_{p \text{ fois}} x \underbrace{\}...\}\}}_{p \text{ fois}} \neq x$.

Exercice 89
Montrer que, pour tout ensemble x, pour tous $n, p \in \mathbb{N}^*$, $\underbrace{\{\{...\{}_{n \text{ fois}} x \underbrace{\}...\}\}}_{n \text{ fois}} \neq \underbrace{\{\{...\{}_{p \text{ fois}} x \underbrace{\}...\}\}}_{p \text{ fois}}$ si et seulement si $n \neq p$.

On va, sommairement, construire de façon ensembliste quelques-uns des objets mathématiques les plus utilisés, notamment les entiers naturels de l'ensemble $\mathbb{N}$. L'axiome de fondation permet, non de créer les entiers naturels (c'est l'axiome de l'infini qui le permet), mais de montrer que les constructions obtenues sont deux à deux distinctes, autrement, de justifier que $1 \neq 2$. Il est important de comprendre que la « représentation » ci-dessous est bel et bien une

construction, c'est-à-dire une façon tout au moins de justifier l'existence de tels objets, même si, l'on en convient, ce qu'ils sont n'a pratiquement aucun intérêt à côté de leurs propriétés ; elles sont l'objet de l'arithmétique.

Définition. *(Représentation des entiers naturels de Von Neumann)*
Nous posons : $0 = \emptyset$, puis : $1 = \{\emptyset\} = \{0\}$, puis $2 = \{0, 1\} = 1 \cup \{1\} = \{\emptyset, \{\emptyset\}\}$, etc., c'est-à-dire, à l'infini (ce qui est justifié par l'axiome de l'infini) $n + 1 = n \cup \{n\}$. L'existence de $\emptyset$ est garantie par l'axiome de l'ensemble vide.

John Von Neumann

D'origine hongroise, fils d'un banquier réputé, János Lajos Neumann, dit Von Neumann commence à étudier à Budapest. Enfant surdoué, il lit et mémorise tout ce qui lui tombe sous la main, parle grec et latin à l'âge de six ans. Calculateur prodige, il stupéfie ses instituteurs et les amis de la famille, dont Lipót Fejér qui dirigera sa thèse, par sa mémoire prodigieuse et ses capacités en calcul mental.

Malgré une situation politique instable en Hongrie, Neumann entreprend des études supérieures de mathématiques à Budapest en 1919 qu'il complète par trois années d'études de chimie à Berlin et Zurich. Il rencontrera ainsi Erhard Schmidt, Herman Weyl et Polya. Il s'intéresse en fait plus aux ensembles et aux nombres transfinis de Cantor qu'à la chimie... C'est à Budapest qu'il soutiendra finalement sa thèse dirigée par Fejér portant sur les ensembles transfinis, fin 1926.

Professeur à Göttingen puis à l'université de Berlin, la réputation de Neumann s'instaure outre-Atlantique : il se rend aux États-Unis à Princeton à l'invitation de Veblen en 1930 à l'occasion de la mise en place du tout nouveau Institute for Advanced Study.

Juif, afin d'échapper à la répression du pouvoir hitlérien soutenu par le régime hongrois, von Neumann s'installe définitivement aux Etats-Unis en 1933 et fit toute sa carrière au célèbre institut. Il meurt prématurément, en 1954, à 54 ans, d'un cancer des os sans doute causé par ses nombreuses expositions aux radiations lors des expérimentations pour la mise au point de la première bombe atomique.

L'ensemble formé par cette infinité d'ensembles est noté $\mathbb{N}$; on peut lui définir une addition, une multiplication, et vérifier qu'elles vérifient toutes les propriétés habituelles qui lui sont associés ; également un ordre qui permet d'énoncer la propriété fondamentale de $\mathbb{N}$: toute partie non vide a un minimum. C'est peu intéressant et sans révolution conceptuelle non plus ; le lecteur intéressé trouvera une construction plutôt complète dans *Épistémologie mathématique* de Henri Lombardi. De plus, on vérifie qu'il vérifie les cinq propriétés axiomatiques de l'arithmétique de Peano, que nous énonçons à titre informatif ci-dessous :

Définition. *(Arithmétique de Peano)*
On appelle *entiers naturels de Peano*, un ensemble $\mathbb{N}$ vérifiant les propriétés suivantes, dits *axiomes de Peano* :
1. il contient au moins un élément, notons le 0 ;
2. il existe une fonction σ de $\mathbb{N}$ dans $\mathbb{N}$, appelée *successeur* ;
3. aucun entier naturel n'est suivi par 0 ($0 \notin \mathrm{Im}(\sigma)$) ;
4. deux entiers naturels ayant le même successeur sont égaux (σ est injective) ;
5. un principe de récurrence : si un ensemble contient 0 et le successeur de chacun de ses éléments, cet ensemble est $\mathbb{N}$.

Habituellement, la fonction successeur est donnée par $\sigma(n) = n + 1$.

Concluons par l'intérêt principal de cette partie.

Théorème. *(Distinction deux à deux des entiers naturels)*
En présence de l'axiome de fondation, les entiers naturels de Von Neumann sont deux à deux distincts.

▷ On l'a déjà vu : n ne peut appartenir à n, pour tout n, donc $n + 1 \neq n = n \cup \{n\}$. Ceci montre que deux entiers successifs sont distincts. Pour montrer que les entiers naturels sont deux à deux distincts, il s'agit simplement le principe du quatrième exercice présenté ci-dessus, qui en découle. ■

Nous espérons que, par ces considérations, le lecteur sera convaincu que la totalité des objets mathématiques qu'il manipule est une construction ensembliste : un ordre, par exemple, est une relation sur, disons, $\mathbb{N}$, c'est-à-dire une partie du produit $\mathbb{N} \times \mathbb{N}$: la notation $n \leqslant p$ traduit simplement $(n, p) \in \leqslant$. Une fonction f est un triplet $f = (E, F, \Gamma)$, où E est l'ensemble de départ, F l'ensemble d'arrivée et Γ une partie de $E \times F$ vérifiant la propriété fondamentale des fonctions : tout élément a au plus une image. Les nombres réels sont identifiés, par exemple, aux coupures de Dedekind : ce sont alors des couples (A, B) tels que $A, B \subseteq \mathbb{Q}$, $AcupB = \mathbb{Q}$, $A \cap B = \emptyset$ et $\forall a \in A \forall b \in B \quad a < b$. Et ainsi de suite.

3.3.3.3 Considérations logiques

On peut montrer que si $ZF_\bullet$ est consistant, *i. e.* s'il n'y a pas d'incohérence dans ses axiomes et qu'un modèle est envisageable, alors il ne prouve ni AF, ni sa négation : on dit que AF est indépendant des axiomes de $ZF_\bullet$. Cela s'exprime :

$$ZF_\bullet \text{ consistant} \Rightarrow ZF \text{ consistant.}$$

Table des matières