Défaut(s) de signature *

Colas Bardavid* et Éric Pité

11 juillet 2020

Introduction

Il est bien connu que pour tout $n \geqslant 2$, il existe un unique morphisme $\varepsilon : \mathfrak{S}_n \longrightarrow \{-1, 1\}$ non trivial, à savoir la signature. Dans cet article, on est parti de cette question : qu'en est-il dans le cas infini ; quels sont les morphismes $\mathfrak{S}_{\mathbb{N}} \longrightarrow \{-1, 1\}$ non triviaux ?
On s'est très vite douté qu'il n'y avait aucun tel morphisme, et on s'est même dit que cela pourrait faire un exercice de colle sympathique. Mais, en essayant d'établir ce résultat formellement, on constatait que cette question était plus technique qu'il n'y paraissait. À mesure que la preuve avançait, il y avait toujours un cas plus compliqué qui se présentait, et la « chirurgie de $\mathfrak{S}_{\mathbb{N}}$ » semblait bel et bien incontournable.
On présente ici plusieurs résultats autour de cette question, du plus élémentaire au plus difficile. Finalement, oui, le seul morphisme $\mathfrak{S}_{\mathbb{N}} \longrightarrow \{-1, 1\}$ est bien le morphisme trivial.

Notations

- Si E est un ensemble, on note $\mathfrak{S}_E$ le groupe des bijections de E dans E. On note $\mathfrak{S}_n$ le groupe des permutations de $[\![1, n]\!]$.
- Si E est un ensemble et si $\sigma \in \mathfrak{S}_E$, on appelle *support de* σ l'ensemble

$$\operatorname{Supp}(\sigma) := \{x \in E \mid \sigma(x) \neq x\}.$$

- Si x et g sont des éléments d'un groupe, on note $x^g := gxg^{-1}$ le conjugué de x par g.

Plan de l'article

- La partie 1 montre que la signature $\varepsilon : \mathfrak{S}_n \longrightarrow \{-1, 1\}$ n'admet pas d'extension à $\mathfrak{S}_{\mathbb{N}^*}$.

*2020 Mathematics Subject Classifications : 20-03, 20B10, 20B30

- Dans la partie 2, on explique comment les permutations de $\mathbb{Z}$ peuvent s'écrire comme « produits » de cycles à supports disjoints. On introduit le type d'une permutation.
- Les parties 3 et 4 traitent des permutations sans points fixes et de quelques cas particuliers dont on a besoin pour le cas général.
- Dans la partie 5, à l'aide des résultats précédents, on démontre le théorème principal.
- Dans la dernière partie, on rassemble quelques repères historiques et on présente d'autres preuves du théorème principal ainsi que quelques extensions.

1 La signature usuelle n'admet pas d'extension

Soit $n \in \mathbb{N}_{\geqslant 2}$.
On note $i : \mathfrak{S}_n \longrightarrow \mathfrak{S}_{\mathbb{N}^*}$ l'injection qui a $\sigma \in \mathfrak{S}_n$ associe son « extension à $\mathbb{N}^*$ » qui agit sur les entiers $k > n$ en les fixant. On va montrer que la signature usuelle $\varepsilon : \mathfrak{S}_n \longrightarrow \{-1, 1\}$ n'admet pas d'extension à $\mathfrak{S}_{\mathbb{N}^*}$.

$$\boxed{\text{On se fixe donc } \varepsilon_{\mathbb{N}^*} : \mathfrak{S}_{\mathbb{N}^*} \longrightarrow \{-1,1\} \text{ un morphisme de groupes.}}$$

Notre but est de montrer qu'on ne peut pas avoir $\varepsilon_{\mathbb{N}^*} \circ i = \varepsilon$.
Voici le plan de la preuve :

- on va introduire une permutation bien choisie σ ;
- on va considérer une conjuguée σ^{φ} bien choisie ;
- on remarque que $\varepsilon_{\mathbb{N}^*}(\sigma) = \varepsilon_{\mathbb{N}^*}(\sigma^{\varphi})$;
- comme on a $(1\ 2) = \sigma \circ \sigma^{\varphi}$, cela conclut.

On commence par quelques remarques générales.

1.1 Invariance par conjugaison

Proposition 1. *Le morphisme $\varepsilon_{\mathbb{N}^*}$ est invariant par conjuguaison.*

Démonstration. En effet, si $\sigma, g \in \mathfrak{S}_{\mathbb{N}^*}$, on a

$$\varepsilon_{\mathbb{N}^*}\left(\sigma^g\right) = \varepsilon_{\mathbb{N}^*}(g)\varepsilon_{\mathbb{N}^*}(\sigma)\varepsilon_{\mathbb{N}^*}\left(g^{-1}\right) = \varepsilon_{\mathbb{N}^*}(\sigma),$$

puisque $\{-1, 1\}$ est commutatif. ***cqfd***

1.2 Cycles et conjuguaison

Si $p \in \mathbb{N}_{\geqslant 2}$ et si $(a_i)_{1 \leqslant i \leqslant p} \in (\mathbb{N}^*)^p$ est une famille d'entiers deux à deux distincts, on notera, classiquement, $(a_1\ a_2\ a_3\ a_4\ \cdots\ a_p)$ la permutation de $\mathbb{N}^*$ qui envoie a_i sur a_{i+1} pour $i \in [\![1, p-1]\!]$, qui envoie a_p sur a_1, et qui laisse fixe tous les autres entiers.
On utilisera abondamment le fait suivant (qui résulte d'un simple calcul).

Proposition 2. *Soit* $\varphi : \mathbb{N}^* \longrightarrow \mathbb{N}^*$ *une bijection. Alors,*

$$\big(a_1\ a_2\ a_3\ a_4\ \cdots\ a_n\big)^{\varphi} = \big(\varphi(a_1)\ \varphi(a_2)\ \varphi(a_3)\ \varphi(a_4)\ \cdots\ \varphi(a_n)\big).$$

1.3 Un « produit infini » de transposition

On considère la permutation de $\mathbb{N}^*$

$$\sigma : \left\{ \begin{array}{ccl} \mathbb{N}^* & \longrightarrow & \mathbb{N}^* \\ n & \longmapsto & \begin{cases} n & \text{si } n \equiv 0\ \ (3) \\ n+1 & \text{si } n \equiv 1\ \ (3) \\ n-1 & \text{si } n \equiv 2\ \ (3)\ . \end{cases} \end{array} \right.$$

Pour vérifier que σ est bien une bijection, on peut par exemple remarquer que $\sigma \circ \sigma = \mathrm{Id}_{\mathbb{N}^*}$. Cependant, la meilleure façon est de voir que « σ est un produit infini de transpositions ». Voici schématiquement l'action de σ sur $\mathbb{N}^*$:

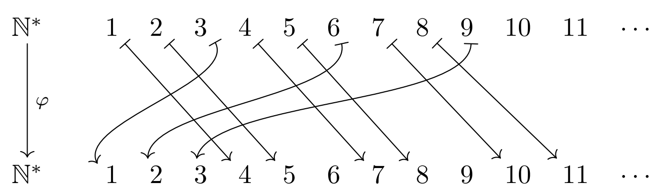
$$\begin{tikzcd} 1 \arrow[r, bend right] & 2 \arrow[l, bend right] & 3 & 4 \arrow[r, bend right] & 5 \arrow[l, bend right] & 6 & 7 \arrow[r, bend right] & 8 \arrow[l, bend right] & 9 & \cdots \end{tikzcd}$$

On s'autorisera à noter $\sigma =$ « $(1\ 2)(4\ 5)(7\ 8)\cdots$ ».

Exercice 1. Le groupe $\mathfrak{S}_{\mathbb{N}^*}$ est-il engendré par les transpositions ?

1.4 Une conjuguée bien choisie

Considérons une bijection φ de $\mathbb{N}^*$ dans $\mathbb{N}^*$ qui envoie le couple $(1,2)$ sur $(4,5)$, le couple $(4,5)$ sur le couple $(7,8)$, ce qu'on pourrait représenter par :



Plus formellement, on définit

$$\varphi : \left\{ \begin{array}{ccl} \mathbb{N}^* & \longrightarrow & \mathbb{N}^* \\ n & \longmapsto & \begin{cases} n+3 & \text{si } n \equiv -1, 1\ \ (3) \\ 1 & \text{si } n = 3 \\ 2 & \text{si } n = 6 \\ n-6 & \text{si } n \geqslant 9 \text{ et } n \equiv 0\ \ (3). \end{cases} \end{array} \right.$$

On laisse le lecteur se convaincre qu'il s'agit bien d'une bijection de $\mathbb{N}^*$ dans $\mathbb{N}^*$.

1.5 Conclusion

La proposition **??** permet de voir que la conjuguée de σ par φ vaut

$$\sigma^{\varphi} = \text{« } (4\ 5)(7\ 8)(10\ 11) \cdots \text{ »}$$

et donc que $\sigma \circ \sigma^{\varphi} = (1\ 2)$.
On a donc

$$\begin{aligned} \varepsilon_{\mathbb{N}^*}\big((1\ 2)\big) &= \varepsilon_{\mathbb{N}^*}\left(\sigma \circ \sigma^{\varphi}\right) \\ &= \varepsilon_{\mathbb{N}^*}\left(\sigma\right) \times \varepsilon_{\mathbb{N}^*}\left(\sigma^{\varphi}\right) \\ &= \varepsilon_{\mathbb{N}^*}\left(\sigma\right)^2 \\ &= 1. \end{aligned}$$

Or $\varepsilon\big((1\ 2)\big) = -1$. On a donc montré :

Théorème 1. *Il n'existe aucun morphisme $\varepsilon_{\mathbb{N}^*} : \mathfrak{S}_{\mathbb{N}^*} \longrightarrow \{-1, 1\}$ qui fasse commuter le diagramme*

$$\begin{tikzcd} \mathfrak{S}_{\mathbb{N}^*} \arrow[r, "\varepsilon_{\mathbb{N}^*}"] & \{-1,1\}. \\ \mathfrak{S}_n \arrow[u, hook, "i"] \arrow[ur, "\varepsilon"'] & \end{tikzcd}$$

2 Décomposition et type d'une permutation

On va dans la suite démontrer des résultats de plus en plus forts en suivant les mêmes idées : introduire des permutations bien choisies et travailler avec des conjuguées. Pour commencer, on va opérer une dissection du groupe $\mathfrak{S}_{\mathbb{Z}}$ qui nous permettra de mieux l'étudier.

2.1 Réduction à $\mathfrak{S}_{\mathbb{Z}}$

Si E et F sont des ensembles équipotents, alors les groupes $\mathfrak{S}_E$ et $\mathfrak{S}_F$ sont isomorphes. De plus, dans ce cas, le groupe $\mathfrak{S}_E$ n'admet pas de morphisme non trivial vers $\{-1, 1\}$ si et seulement si c'est le cas pour $\mathfrak{S}_F$.
Ainsi, comme $\mathbb{N}$ et $\mathbb{Z}$ sont équipotents, il nous suffit d'étudier les « signatures » de $\mathfrak{S}_{\mathbb{Z}}$, ce qu'on fera dans la suite. L'avantage de $\mathfrak{S}_{\mathbb{Z}}$ sur $\mathfrak{S}_{\mathbb{N}}$, c'est qu'il y est plus simple de donner un exemple de cycle infini.

Exercice 2. Existe-t-il deux ensembles X et Y non équipotents tels que les groupes $\mathfrak{S}_X$ et $\mathfrak{S}_Y$ soient isomorphes ?

2.2 Décomposition d'une permutation

En faisant agir à gauche $\mathfrak{S}_{\mathbb{Z}}$ sur $\mathbb{Z}$ par

$$\begin{aligned} \mathfrak{S}_{\mathbb{Z}} \times \mathbb{Z} &\longrightarrow \mathbb{Z} \\ (\sigma, n) &\longmapsto \sigma(n) \end{aligned}$$

et en considérant les orbites de cette action, on peut montrer que toute permutation s'écrit comme « produit » de cycles à supports disjoints ; ce produit de cycles étant unique, à l'ordre près. Ici, on a mis « produit » entre guillemets car le nombre de cycles pouvant intervenir dans la décomposition peut être infini. Par exemple, si σ_1 est la permutation de $\mathbb{Z}$ qui échange un entier pair avec son successeur, on écrira

$$\sigma_1 = \text{« } \cdots (-2\ \ -1)(0\ 1)(2\ 3)(4\ 5) \cdots \text{ »}.$$

Une autre différence avec le cas des groupes $\mathfrak{S}_n$ est que la décomposition d'une permutation peut faire intervenir des « cycles infinis ». Un exemple de « cycle infini » est la bijection

$$\sigma_2 : \begin{cases} \mathbb{Z} \longrightarrow \mathbb{Z} \\ n \longmapsto n+1 \end{cases} .$$

Proposition 3. *Soit $\sigma \in \mathfrak{S}_{\mathbb{Z}}$. Alors, il existe une unique partition $\mathcal{A} \subset \mathcal{P}(\mathbb{Z})$ de $\mathbb{Z}$ telle que, pour tout $A \in \mathcal{A}$, σ agit transitivement sur A.*

Exercice 3. Montrer la proposition **??**.

Exercice 4. Déterminer le centre du groupe $\mathfrak{S}_{\mathbb{Z}}$.

2.3 Type d'une permutation

2.3.1 Définition

Définition. Soit $\sigma \in \mathfrak{S}_{\mathbb{Z}}$.

- On note $\mathrm{Fixe}(\sigma)$ l'ensemble des points fixes de σ.
- Si $i \in \mathbb{N}_{\geqslant 2} \cup \{\infty\}$, on note $\mathrm{N}_i(\sigma) \in \mathbb{N} \cup \{\infty\}$ le nombre de cycles de longueur i dans la décomposition de σ en produit de cycles à supports disjoints.
- On appelle *type de* σ et on note $\mathrm{Type}\,(\sigma)$ la famille définie par

$$\mathrm{Type}\,(\sigma) := \Big(\big|\mathrm{Fixe}(\sigma)\big|, \big(\mathrm{N}_i(\sigma)\big)_{i \in \mathbb{N}_{\geqslant 2}}, \mathrm{N}_\infty(\sigma) \Big).$$

2.3.2 Quelques faits

On laisse au lecteur le soin de vérifier que

- $\mathrm{Supp}(\sigma) = \mathbb{Z} \setminus \mathrm{Fixe}(\sigma)$ et réciproquement ;
- on a

$$\big|\mathrm{Fixe}(\sigma)\big| \quad + \sum_{i \in \mathbb{N}_{\geqslant 2} \cup \{\infty\}} \mathrm{N}_i(\sigma) \quad + \quad \mathrm{N}_\infty(\sigma) \times \infty = \infty,$$

  avec la convention $0 \times \infty = 0$.

2.3.3 Exemples

Pour les permutations σ_1 et σ_2 introduites ci-dessus, on a

$$\begin{aligned} & \mathrm{Type}\,(\sigma_1) = \big(0, (\infty, 0, 0, \ldots), 0\big) \\ \text{et} \quad & \mathrm{Type}\,(\sigma_2) = \big(0, (0, 0, 0, \ldots), 1\big). \end{aligned}$$

Exercice 5. Existe-t-il des permutations de $\mathfrak{S}_{\mathbb{Z}}$ de tout type ? C'est-à-dire, quels que soient $k, \ell \in \mathbb{N} \cup \{\infty\}$ et u une suite d'éléments dans $\mathbb{N} \cup \{\infty\}$, existe-t-il $\sigma \in \mathfrak{S}_{\mathbb{Z}}$ tel que $\mathrm{Type}\,(\sigma) = (k, u, \ell)$?

2.4 Classification des classes de conjugaison

Proposition 4. *Deux permutations sont conjuguées si et seulement si elles ont même type.*

Démonstration. On donne une idée de la preuve. Soient $\sigma, \tau \in \mathfrak{S}_{\mathbb{Z}}$ deux permutations ayant même type. On considère une bijection $\varphi : \mathbb{Z} \longrightarrow \mathbb{Z}$ qui envoie les supports des cycles de la décomposition de σ sur les supports de même longueur des cycles de la décomposition de τ, et qui sur chacun de ces supports « suit le même ordre ». On a alors $\sigma^{\varphi} = \tau$. ***cqfd***

3 Réduction au cas des permutations sans point fixe

On rappelle que notre but est de montrer que si $\varepsilon : \mathfrak{S}_{\mathbb{Z}} \longrightarrow \{-1, 1\}$ est un morphisme alors ε est trivial. Dans cette partie, on va montrer que le cas le plus difficile à traiter est celui où σ n'a pas de point fixe.

3.1 Permutations universellement paires

Définition. Soit $\sigma \in \mathfrak{S}_{\mathbb{Z}}$. On dit que σ *est universellement paire* si pour tout morphisme $\varepsilon : \mathfrak{S}_{\mathbb{Z}} \longrightarrow \{-1, 1\}$ on a $\varepsilon(\sigma) = 1$.

Voici quelques faits dont la preuve est laissée au lecteur :

- Deux permutations conjuguées sont universellement paires en même temps.
- Le caractère universellement pair d'une permutation ne dépend que de son type.
- Les permutations universellement paires forment un sous-groupe distingué de $\mathfrak{S}_{\mathbb{Z}}$.

3.2 Cas des permutations à support fini

Proposition 5. *Toute permutation $\sigma \in \mathfrak{S}_{\mathbb{Z}}$ à support fini est universellement paire.*

Démonstration. C'est exactement ce qu'on a vu avec le théorème **??**. Voici plus de détails.
Soit un morphisme $\varepsilon_{\mathbb{Z}} : \mathfrak{S}_{\mathbb{Z}} \longrightarrow \{-1,1\}$. On note $j : \mathfrak{S}_{\mathbb{N}^*} \longrightarrow \mathfrak{S}_{\mathbb{Z}}$ le morphisme injectif qui à une permutation de $\mathbb{N}^*$ associe son extension à $\mathbb{Z}$ qui laisse $\mathbb{Z}_{\leqslant 0}$ fixe. On dispose du diagramme

$$\begin{tikzcd}
\mathfrak{S}_{\mathbb{N}^*} \arrow[r, "j"] & \mathfrak{S}_{\mathbb{Z}} \arrow[r, "\varepsilon_{\mathbb{Z}}"] & \{-1,1\}. \\
\mathfrak{S}_2 \arrow[u, hook, "i"'] \arrow[urr, "\varepsilon"'] & &
\end{tikzcd}$$

On a vu qu'il ne pouvait pas être commutatif. Donc, on a

$$\forall \sigma \in \mathfrak{S}_2,\ \varepsilon_{\mathbb{Z}}\big(j \circ i(\sigma)\big) = 1.$$

En particulier, on a $\varepsilon_{\mathbb{Z}}\big((1\ 2)\big) = 1$.
Ainsi, $(1\ 2)$ est universellement paire.
Or, les transpositions sont toutes conjuguées les unes aux autres dans $\mathfrak{S}_{\mathbb{Z}}$; elle sont donc toutes universellement paires. Comme les transpositions engendrent le sous-groupe des permutations à support fini, le résultat annoncé est démontré.
cqfd

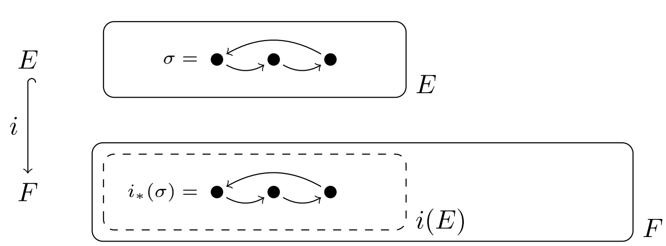
Exercice 6. Donner un exemple de permutation de $\mathfrak{S}_{\mathbb{Z}}$ à support infini et universellement paire.

3.3 Réduction au cas sans point fixe

On va maintenant montrer que dans le problème qui nous occupe, le cas sans point fixe est le plus compliqué. Si on sait qu'une permutation σ est universellement paire, alors on va prouver que toutes les permutations qui ont le même type que σ, sauf éventuellement plus de points fixes, sont aussi universellement paires.

3.3.1 Induction entre permutations via une injection

Soient E et F deux ensembles et $i : E \longrightarrow F$ une injection.
Si $\sigma \in \mathfrak{S}_E$, on note $i_*(\sigma)$ la permutation de F qui agit sur $i(E)$ comme σ agit sur E et qui laisse les autres éléments de F fixes :



Plus formellement, pour $\sigma \in \mathfrak{S}_E$, on pose

$$i_*(\sigma) : \begin{cases} F \longrightarrow F \\ y \longmapsto \begin{cases} i\Big(\sigma\big(i^{-1}(y)\big)\Big) & \text{si } y \in i(E) \\ y & \text{sinon.} \end{cases} \end{cases}$$

On obtient un morphisme de groupes

$$i_* : \mathfrak{S}_E \longrightarrow \mathfrak{S}_F$$

qui est injectif et dont l'image est exactement le groupe des permutations de F dont l'ensemble des points fixes contient $F \setminus i(E)$.

3.3.2 Le résultat

Proposition 6. *Soit $\sigma \in \mathfrak{S}_\mathbb{Z}$ universellement paire et soit $\tau \in \mathfrak{S}_\mathbb{Z}$. Alors,*

$$\left.\begin{array}{l} \big|\mathrm{Fixe}(\tau)\big| \geqslant \big|\mathrm{Fixe}(\sigma)\big| \\ \forall i \in \mathbb{N}_{\geqslant 2} \cup \{\infty\},\ \mathrm{N}_i(\tau) = \mathrm{N}_i(\sigma) \end{array}\right\} \Longrightarrow \tau \textit{ universellement paire.}$$

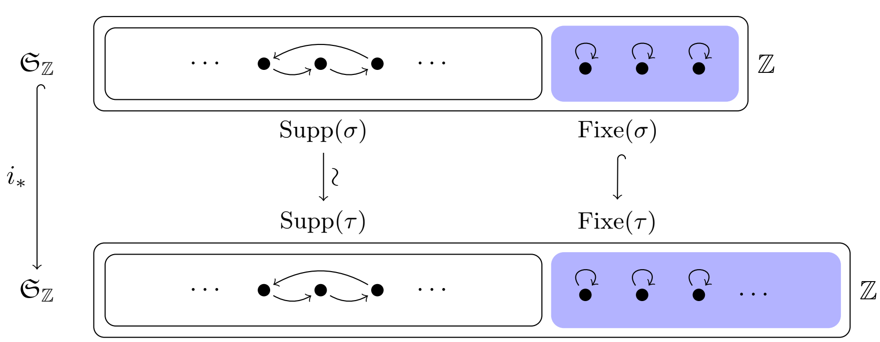
Démonstration. On suppose que

$$\big|\mathrm{Fixe}(\tau)\big| \geqslant \big|\mathrm{Fixe}(\sigma)\big| \quad \text{et} \quad \forall i \in \mathbb{N}_{\geqslant 2} \cup \{\infty\},\ \mathrm{N}_i(\tau) = \mathrm{N}_i(\sigma).$$

Si τ est à support fini, alors on sait que τ est universellement paire. On suppose donc que $\mathrm{Supp}(\tau)$ est infini ; comme $\mathrm{Supp}(\sigma) = \mathbb{Z} \setminus \mathrm{Fixe}(\sigma)$, on a également $\mathrm{Supp}(\sigma)$ infini. On peut donc trouver une bijection

$$\mathbb{Z} \setminus \mathrm{Fixe}(\sigma) \longrightarrow \mathbb{Z} \setminus \mathrm{Fixe}(\tau).$$

On complète cette bijection avec une injection $\mathrm{Fixe}(\sigma) \longrightarrow \mathrm{Fixe}(\tau)$. On note $i : \mathbb{Z} \longrightarrow \mathbb{Z}$ l'injection obtenue. On considère le morphisme de groupes $i_* : \mathfrak{S}_\mathbb{Z} \longrightarrow \mathfrak{S}_\mathbb{Z}$, qu'on peut représenter ainsi :



Considérons $i_*(\sigma)$. Comme illustré ci-dessus, l'ensemble des points fixes de $i_*(\sigma)$ est exactement $\mathrm{Fixe}(\tau)$. De plus, sur les entiers restants, $i_*(\sigma)$ agit comme σ. Ainsi, on a :

$$\Big|\mathrm{Fixe}\big(i_*(\sigma)\big)\Big| = \big|\mathrm{Fixe}(\tau)\big| \quad \text{et} \quad \forall i \in \mathbb{N}_{\geqslant 2} \cup \{\infty\},\ \mathrm{N}_i\big(i_*(\sigma)\big) = \mathrm{N}_i(\tau) = \mathrm{N}_i(\sigma).$$

Donc, τ et $i_*(\sigma)$ ont même type.
Soit maintenant $\varepsilon : \mathfrak{S}_{\mathbb{Z}} \longrightarrow \{-1, 1\}$ un morphisme. Déjà, on a $\varepsilon(\tau) = \varepsilon\big(i_*(\sigma)\big)$. On veut montrer que $\varepsilon(\tau) = 1$. On considère $\varepsilon \circ i_*$; c'est aussi un morphisme de $\mathfrak{S}_{\mathbb{Z}}$ dans $\{-1, 1\}$. Comme σ est universellement paire, on a $\varepsilon \circ i_*(\sigma) = 1$.
Ainsi, on a bien $\varepsilon(\tau) = 1$; et, donc, τ est universellement paire. ***cqfd***

3.3.3 Conclusion

Ainsi, si on veut montrer que tout permutation est universellement paire, il suffit de le faire pour les permutations sans point fixe.

4 Étude de cas particuliers

4.1 La signature ε

Dans la suite, on fixe $\varepsilon : \mathfrak{S}_{\mathbb{Z}} \longrightarrow \{-1, 1\}$ un morphisme de groupes. On appelle *signature* d'une permutation $\sigma \in \mathfrak{S}_{\mathbb{Z}}$ l'entier $\varepsilon(\sigma)$.

Notre but est de montrer que $\forall \sigma \in \mathfrak{S}_{\mathbb{Z}}$, $\varepsilon(\sigma) = 1$, ce qu'on fera en considérant des cas particuliers bien choisis.

4.2 La permutation $\sigma_{\infty,\infty}$ et sa signature

On considère la permutation

$$\sigma_{\infty,\infty} : \left\{ \begin{array}{l} \mathbb{Z} \longrightarrow \mathbb{Z} \\ n \longmapsto \begin{cases} n & \text{si } n < 0 \\ n+1 & \text{si } n \geqslant 0 \text{ et } n \text{ est pair} \\ n-1 & \text{si } n \geqslant 0 \text{ et } n \text{ est impair.} \end{cases} \end{array} \right.$$

La permutation $\sigma_{\infty,\infty}$ laisse $\mathbb{Z}_{<0}$ invariant, puis échange 0 et 1, 2 et 3, *etc.* De façon imagée, on a

$$\sigma_{\infty,\infty} = \text{« } (0\ 1)(2\ 3)(4\ 5)\cdots \text{ ».}$$

On a choisi la notation $\sigma_{\infty,\infty}$ car $\mathrm{Type}\,(\sigma_{\infty,\infty}) = \big(\infty, (\infty, 0, 0, \ldots), 0\big)$.

Proposition 7. *On a* $\varepsilon(\sigma_{\infty,\infty}) = 1$.

Démonstration. On considère une bijection φ de $\mathbb{Z}$ telle qu'on ait

$$\forall n \in \mathbb{N}, \quad \begin{cases} \varphi(n) = 2n & \text{si } n \text{ est pair} \\ \varphi(n) = 2n+1 & \text{sinon} \end{cases}$$

ce qu'on peut visualiser de la façon suivante :

$$\begin{tikzcd}
\mathbb{Z} \arrow[d, "\varphi"'] & 0 \arrow[d, mapsto] & 1 \arrow[d, mapsto] & 2 \arrow[drr, mapsto] & 3 \arrow[drr, mapsto] & 4 \arrow[drrrr, mapsto] & 5 \arrow[drrrr, mapsto] & & \cdots & & & & & \\
\mathbb{Z} & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & \cdots
\end{tikzcd}$$

Une telle bijection existe pour des raisons de cardinalité.
On a alors

$$\sigma^{\varphi}_{\infty,\infty} = « \,(0\ 1)(4\ 5)(8\ 9)(12\ 13)\cdots\, »$$

et donc

$$\sigma_{\infty,\infty} \circ \sigma^{\varphi}_{\infty,\infty} = « \,(2\ 3)(6\ 7)(10\ 11)(14\ 15)\cdots\, ».$$

Ainsi, le type de $\sigma_{\infty,\infty} \circ \sigma^{\varphi}_{\infty,\infty}$ est $\big(\infty, (\infty, 0, \ldots), 0\big)$. D'après la proposition **??**, on a donc

$$\varepsilon\left(\sigma_{\infty,\infty} \circ \sigma^{\varphi}_{\infty,\infty}\right) = \varepsilon\left(\sigma_{\infty,\infty}\right).$$

Donc, $\varepsilon\left(\sigma^{\varphi}_{\infty,\infty}\right) = \varepsilon\left(\sigma_{\infty,\infty}\right) = 1.$ ***cqfd***

4.3 La permutation $\sigma_{0,\infty}$ et sa signature

On considère la permutation

$$\sigma_{0,\infty} : \left\{ \begin{array}{l} \mathbb{Z} \longrightarrow \mathbb{Z} \\ n \longmapsto \begin{cases} n+1 & \text{si } n \text{ est pair} \\ n-1 & \text{si } n \text{ est impair.} \end{cases} \end{array} \right.$$

De façon imagée, on a

$$\sigma_{0,\infty} = « \cdots(-4\ \ -3)(-2\ \ -1)(0\ 1)(2\ 3)(4\ 5)\cdots ».$$

On a choisi la notation $\sigma_{0,\infty}$ car $\operatorname{Type}(\sigma_{0,\infty}) = \big(0, (\infty, 0, 0, \ldots), 0\big)$.

Proposition 8. *On a* $\varepsilon(\sigma_{0,\infty}) = 1$.

Démonstration. Tout simplement, on a

$$\sigma_{0,\infty} \circ \sigma_{\infty,\infty} = « \cdots(-6\ \ -5)(-4\ \ -3)(-2\ \ -1) »,$$

qui est de type $\big(\infty, (\infty, 0, \ldots), 0\big)$. D'après la proposition **??**, on a

$$\varepsilon\left(\sigma_{0,\infty} \circ \sigma_{\infty,\infty}\right) = \varepsilon\left(\sigma_{\infty,\infty}\right).$$

Donc, $\varepsilon(\sigma_{0,\infty}) = 1$. ***cqfd***

4.4 Le shift $[+1]$ et sa signature

On considère la permutation

$$[+1] : \begin{cases} \mathbb{Z} \longrightarrow \mathbb{Z} \\ n \longmapsto n+1 \end{cases}$$

De façon plus générale, si $p \in \mathbb{N}^*$, on note

$$[+p] : \begin{cases} \mathbb{Z} \longrightarrow \mathbb{Z} \\ n \longmapsto n+p \end{cases} .$$

On a évidemment $[+1]^p = [+p]$ pour $p \in \mathbb{N}^*$.

Proposition 9. *On a* $\varepsilon\big([+1]\big) = 1$.

Démonstration. Considérons la permutation

$$\sigma := « \cdots (-3\ \ -1)(1\ 3)(5\ 7) \cdots »,$$

plus formellement définie par

$$\sigma(n) = \begin{cases} n+2 & \text{si } n \equiv 1 \ \ (4) \\ n-2 & \text{si } n \equiv 3 \ \ (4) \\ n & \text{sinon.} \end{cases}$$

On a $\mathrm{Type}\,(\sigma) = \big(\infty, (\infty, 0, \ldots), 0\big)$. D'après les propositions **??** et **??**, on a $\varepsilon(\sigma) = 1$.
Calculons $\sigma_{0,\infty} \circ \sigma$. Soit $n \in \mathbb{Z}$.

- Si n est pair, alors $\sigma_{0,\infty} \circ \sigma(n) = \sigma_{0,\infty}(n) = n+1$ par définition de $\sigma_{0,\infty}$.
- Si n est impair, alors, de même, on a $\sigma_{0,\infty} \circ \sigma(n) = \sigma_{0,\infty}(n+2) = n+1$.

Donc, on a $\sigma_{0,\infty} \circ \sigma = [+1]$. Comme $\varepsilon\,(\sigma_{0,\infty}) = 1$, on a $\varepsilon\big([+1]\big) = 1$. ***cqfd***

5 Démonstration du théorème principal

5.1 Cas des permutations faites de cycles infinis

Proposition 10. *Soit* $\sigma \in \mathfrak{S}_{\mathbb{Z}}$. *Alors,*

$$\left.\begin{array}{l} \mathrm{N}_\infty(\sigma) \geqslant 1 \\ \forall i \in \mathbb{N}_{\geqslant 2},\ \ \mathrm{N}_i(\sigma) = 0 \end{array}\right\} \implies \varepsilon\,(\sigma) = 1.$$

Démonstration. On suppose que

$$\mathrm{N}_\infty(\sigma) \geqslant 1 \quad \text{ et } \quad \forall i \in \mathbb{N}_{\geqslant 2},\ \ \mathrm{N}_i(\sigma) = 0.$$

On distingue plusieurs cas.

a) Si $\mathrm{N}_\infty(\sigma) = p \in \mathbb{N}^*$ et $\mathrm{Fixe}(\sigma) = \varnothing$.
Il suffit de considérer la permutation $[+p]$. En effet, comme un calcul le montre, on a $\mathrm{Type}\left([+p]\right) = \big(0, (0, \dots), p\big)$. Puis,

$$\varepsilon\big([+p]\big) = \varepsilon\big([+1]^p\big) = \varepsilon\big([+1]\big)^p = 1.$$

b) Si $\mathrm{N}_\infty(\sigma) = \infty$.
Alors, comme un calcul le montre, on a $\mathrm{Type}\left(\sigma\right) = \mathrm{Type}\left(\sigma^2\right)$.
Donc, $\varepsilon\left(\sigma\right) = \varepsilon\left(\sigma^2\right) = \varepsilon\left(\sigma\right)^2 = 1$.

c) Si $\mathrm{N}_\infty(\sigma) = p \in \mathbb{N}^*$ et $\big|\mathrm{Fixe}(\sigma)\big| > 0$.
On conlut grâce à la proposition **??** et au cas a).

cqfd

5.2 Conclusion

Théorème 2. *On a :* $\forall \sigma \in \mathfrak{S}_{\mathbb{Z}},\ \varepsilon\left(\sigma\right) = 1.$

Démonstration. Soit $\sigma \in \mathfrak{S}_{\mathbb{Z}}$.

- Grâce à la proposition **??**, on peut multiplier σ par la permutation constituée uniquement des inverses de cycles infinis de σ. On peut donc supposer que $\mathrm{N}_\infty(\sigma) = 0$.
- Si de plus on a $\forall i \in \mathbb{N}_{\geqslant 2}$, $\mathrm{N}_i(\sigma) < \infty$, cela veut dire que σ est à support fini et la proposition **??** permet de conclure.
- Il nous reste donc un cas à traiter : celui où σ est un « produit infini » de cycles à supports finis et disjoints. On suppose que

$$\sigma = \text{«} \prod_{i \in \mathbb{Z}} \sigma_i \text{»}$$

  où les σ_i sont des cycles à supports finis et disjoints. Pour chaque $i \in \mathbb{Z}$, on note $\ell_i := |\mathrm{Supp}(\sigma_i)|$ et on se donne des entiers $a_1^{[i]}, a_2^{[i]}, \dots, a_{\ell_i}^{[i]}$ tels que

$$\sigma_i = \begin{pmatrix} a_1^{[i]} & a_2^{[i]} & \cdots & a_{\ell_i}^{[i]} \end{pmatrix}.$$

  On condidère le cycle infini τ défini par

$$\tau := \text{«} \begin{pmatrix} \cdots & a_{\ell_{-2}}^{[-2]} & a_{\ell_{-1}}^{[-1]} & a_{\ell_0}^{[0]} & a_{\ell_1}^{[1]} & a_{\ell_2}^{[2]} & \cdots \end{pmatrix} \text{»}.$$

  On vérifie que $\tau \circ \sigma$ est un cycle infini qui « enchaîne les cycles σ_i » : si $i \in \mathbb{Z}$, alors

$$\tau \circ \sigma\Big(a_j^{[i]}\Big) = \begin{cases} a_{j+1}^{[i]} & \text{si } j < \ell_i \\ a_1^{[i+1]} & \text{sinon.} \end{cases}$$

  Ainsi, $\tau \circ \sigma$ remplit les conditions de la proposition **??** et on a $\varepsilon\left(\tau \circ \sigma\right) = 1$; comme on a également $\varepsilon\left(\tau\right) = 1$, on conclut que $\varepsilon\left(\sigma\right) = 1$.

cqfd

5.3 Groupe dérivé de $\mathfrak{S}_\mathbb{Z}$

Pour le lecteur courageux, remarquons que la preuve du théorème **??** présentée dans cet article, modulo quelques adaptations, permettrait aussi de montrer que le groupe dérivé de $\mathfrak{S}_\mathbb{Z}$ vérifie $D(\mathfrak{S}_\mathbb{Z}) = \mathfrak{S}_\mathbb{Z}$.

6 Approches historiques et extensions

Il semblerait que la première étude du groupe $\mathfrak{S}_\mathbb{Z}$ ait été menée par l'italien Giuseppe Vitali en 1915, sans utiliser le langage de la théorie des groupes. Dans [**?**], il prouve le théorème **??**. Sa preuve consiste à montrer que toute permutation est un produit d'au plus 3 carrés.

Théorème 3. *Soit $\sigma \in \mathfrak{S}_\mathbb{Z}$. Il existe $\tau_1, \tau_2, \tau_3 \in \mathfrak{S}_\mathbb{Z}$ tels que $\sigma = {\tau_1}^2{\tau_2}^2{\tau_3}^2$.*

Notons également qu'en 1951, Oystein Ore montra que tout élément de $\mathfrak{S}_\mathbb{Z}$ est un commutateur, c'est-à-dire que

Théorème 4. *Soit $\sigma \in \mathfrak{S}_\mathbb{Z}$. Il existe $\alpha, \beta \in \mathfrak{S}_\mathbb{Z}$ tel que $\sigma = \alpha\beta\alpha^{-1}\beta^{-1}$.*

Une démonstration se trouve dans [**?**]. Le théorème **??** peut être vu comme un corollaire immédiat des théorèmes **??** ou **??**.
La preuve du théorème **??** est comparable en complexité à celle du théorème **??**. À première vue, la preuve du théorème **??** semble plus courte ; mais, quand on détaille les nombreux points sur lesquels Vitali passe en vitesse, on constate que l'« étude chirurgicale de $\mathfrak{S}_\mathbb{N}$ » reste tout de même incontournable.
Cependant, le théorème **??** permet d'obtenir en plus que $\mathfrak{S}_\mathbb{Z}$ est un groupe parfait (c'est-à-dire égal à son groupe dérivé). Dit autrement, l'abélianisé de $\mathfrak{S}_\mathbb{Z}$ est trivial. Une conséquence immédiate du théorème **??** est la généralisation suivante du théorème **??**.

Théorème 5. *Soit $\varphi : \mathfrak{S}_\mathbb{Z} \longrightarrow G$ un morphisme de groupes, avec G abélien. Alors, pour tout $\sigma \in \mathfrak{S}_\mathbb{Z}$, on a $\varphi(\sigma) = 1$.*

En particulier, il est impossible de généraliser la notion de groupe alterné $\mathfrak{A}_n$ au cas infini dénombrable. Lorsque $n \geqslant 5$, on sait que $\mathfrak{A}_n$ est l'unique sous-groupe distingué non trivial de $\mathfrak{S}_n$. Qu'en est-il pour $\mathfrak{S}_\mathbb{Z}$?
En 1929, Onofri établit dans [**?**] que $\mathfrak{S}_\mathbb{Z}$ a exactement 4 sous-groupes distingués. Le théorème d'Onofri a été redécouvert en 1933 par Schreier et Ulam dans [**?**] et s'énonce ainsi :

Théorème 6. *Les sous-groupes distingués non triviaux de $\mathfrak{S}_\mathbb{Z}$ sont le groupe des permutations à support fini et le groupe des permutations à support fini qui sont paires.*

On trouvera une démonstration de ce théorème dans le chapitre 8 de [**?**].
Ce théorème a été généralisé par Baer un an plus tard, avec la classification des sous-groupes distingués de $\mathfrak{S}_E$ pour un ensemble infini arbitraire E, [**?**].

Références

[1] Baer R., *Die Kompositionsreihe der Gruppe aller eineindeutigen Abbildungen einer unendlichen Menge auf sich.* Studia Math. (1934) vol. 5(1) pp. 15–17

[2] Dixon J. D., Mortimer B., *Permutation groups*, Graduate Texts in Mathematics, 163, Springer-Verlag, (1996)

[3] Onofri L., *Teoria delle sostituzioni che operano su una infinità numerabile di elementi*, Memoria III. Annali di Matematica Pura ed Applicata (1929) vol. 7(1), pp. 103–130

[4] Ore O., *Some remarks on commutators*, Proceedings of the American Mathematical Society, vol. 2 (2), (Apr., 1951), pp. 307–314

[5] Schreier J., Ulam S.,*Über die Permutationsgruppe der natürlichen Zahlenfolge*, Studia Mathematica (1933) vol. 4(1), pp. 134–141

[6] Vitali G., *Sostituzioni sopra una infinità numerabile di elementi*, Bollettino Mathesis (1915) 7 : pp. 29–31