# Périodes dans les tables de Laver

S. Pépin Lehalleur - P. Simon

## Table des matières

" Réciproquement, supposons $n = p2^q$ avec p impair, $p \geq 3$. On a envie de montrer que la ligne $n-2^{q+1}$ est de période $2^{q+1}$. $S_{2^q}$ est LD, donc clairement les "périodes" de $1, \ldots, 2^n - 1$ divisent $2^n$, et en fait bien sûr $2^{n-1}$. C'est-à-dire que, d'après un lemme précédent , dans $S_n$, on pourrait dire que les périodes de $N - 2^{n+1} + 1, \ldots, N - 1$ divisent $2^n$. Un autre lemme précedent permet alors de conclure trivialement."

*Merci à Patrick Dehornoy de nous avoir évité ça...*

# Introduction

L'un des développements les plus spectaculaires de la théorie des ensembles est l'étude des *axiomes de grands cardinaux*, à savoir d'axiomes postulant l'existence d'ensembles tellement grands que leur existence est indémontrable dans le cadre de ZFC. Il s'agit de poursuivre la démarche d'exploration de l'infini initiée par Cantor, en poussant au delà des possibilités du système axiomatique actuel, pour un jour, pourquoi pas, accéder à un consensus sur la nécessité d'accepter de nouveaux axiomes dans le champ des mathématiques usuelles.

D'autre part, ce sont des outils fondamentaux pour aborder les problèmes d'équiconsistance : quel est la force relative de divers axiomes ? Le fait encore mal compris que ces axiomes semblent s'ordonner suivant une hiérarchie croissante de consistance permet parfois de localiser précisément un axiome dans cette hiérarchie.

Dans ce texte, on présente les travaux de Richard Laver, qui, en étudiant un cadre naturel pour énoncer de tels axiomes : l'algèbre des itérés des plongements élémentaires d'un rang, a mis en lumière un problème sous-jacent de combinatoire finie. Il a défini les tables qui portent aujourd'hui son nom et a montré que certaines propriétés de ces objets finis étaient mieux appréhendées dans le contexte ensembliste. Au point que certains résultats démontrés dans ce contexte, c'est-à-dire sous le coup d'une hypothèse indémontrable dans ZFC, n'ont pas reçu de démonstration élémentaire. Le statut de tels résultats est paradoxal : ils ont acquis une forte plausibilité, mais la preuve repose sur une prémisse non démontrable dans ZFC, et aucune preuve élémentaire n'est en vue.

Dans une première partie, on présente les grandes lignes de cette théorie, en malmenant un peu l'ordre historique de la découverte. On commence par construire ex nihilo les tables de Laver afin d'énoncer une conjecture sur leur comportement à l'infini. Ensuite on voit comment ces tables apparaissent dans un cadre ensembliste sous une hypothèse de grands cardinaux et comment cette approche permet de démontrer le résultat annoncé. En conclusion de cette partie, on éclaircit le statut métamathématique de ces constructions.

Dans une seconde partie, on reprend plus en détail certains points techniques : discussion de la pertinence de la relation d'équivalence introduite dans le cours de la preuve, erratum d'une preuve de [Deh00], une preuve de la borne de Kunen.

# Première partie
# Survol des résultats de Laver

## 1 Théorie élémentaire des tables de Laver

Nous allons construire une suite de systèmes algébriques finis vérifiant la loi d'auto-distributivité à gauche :

**Définition 1.1.** Une opération $*$ est dite auto-distributive à gauche (abrégé en LD) si

$$\forall x, y, z,\ x * (y * z) = (x * y) * (x * z). \tag{1}$$

Nous énoncerons ensuite une conjecture naturelle sur leur comportement à l'infini.

## 1.1 Systèmes $S_n$

Les opérations considérées sont définies sur les ensembles finis $[|n|] = \{1, ..., n\}$. On note alors, pour $a \in \mathbb{Z}$, $(a)_n$ l'unique élement de $[|n|]$ congru à $a$ modulo $n$. Commençons par partir d'une table incomplète, que nous remplirons grâce à l'identité (LD) :

$$\forall a,\ a * 1 = (a + 1)_n. \tag{2}$$

| $*$ | 1 | 2 | ... | $n$ |
|---|---|---|---|---|
| 1 | 2 | | | |
| 2 | 3 | | | |
| $\vdots$ | $\vdots$ | | | |
| $n-1$ | $n$ | | | |
| $n$ | 1 | | | |

En utilisant (LD) sous la forme partielle : $\forall a, b,\ a * (b * 1) = (a * b) * (a * 1)$, on calcule la ligne $n$ :

$$n * 2 = n * (1 * 1) = (n * 1) * (n * 1) = 1 * 1 = 2,$$

puis plus généralement $n * a = a$ par la récurrence

$$n * (a + 1) = n * (a * 1) = (n * a) * 1$$

valable pour $a < n$.
De même, une fois que l'on dispose de la ligne $n$, on calcule la ligne $(n-1)$ par : $(n-1) * (a+1) = ((n-1) * a)) * n = (n-1)$ qui donne $(n-1) * a = cste = n$. On calcule ainsi, de proche en proche, toutes les lignes de la table (sans obtenir de formule explicite simple au delà des premières lignes).
À chaque fois, on fait apparaître une périodicité dans la ligne $a$ : les valeurs croissent jusqu'à $n$ puis retombent à $a + 1$ et recommencent cycliquement. En formalisant ce calcul, on obtient :

**Lemme 1.2.** *(i) Il existe une unique opération $*$ sur $[|n|]$ vérifiant (1) et :*

$$\forall a, b,\ a * (b * 1) = (a * b) * (a * 1). \tag{3}$$

*(ii) On a alors les relations :*

$$a * b \begin{cases} = & b & \text{pour } a = n, \\ = & a+1 & \text{pour } b = 1 \text{ et } a*(b-1) = n, \\ > & a*(b-1) & \text{sinon.} \end{cases}$$

*De plus la ligne $a$ est périodique de période au plus $n - a$ : le motif périodique est croissant, commence par $a + 1$ et finit par $n$.*
*En particulier, le seul idempotent est $n$.*

On notera $(S_n, *_n)$ ou $(S_n, *)$ le système algébrique ainsi formé.

| $*$ | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| 1 | 2 | 4 | 2 | 4 |
| 2 | 3 | 4 | 3 | 4 |
| 3 | 4 | 4 | 4 | 4 |
| 4 | 1 | 2 | 3 | 4 |

| $*$ | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| 1 | 2 | 4 | 5 | 2 | 4 |
| 2 | 3 | 4 | 5 | 3 | 4 |
| 3 | 4 | 5 | 4 | 5 | 4 |
| 4 | 5 | 5 | 5 | 5 | 5 |
| 5 | 1 | 2 | 3 | 4 | 5 |

TAB. 1 – $S_4$, $S_5$

Une question non évidente est de déterminer quels systèmes $S_n$ satisfont l'identité (LD). L'observation des premières tables montre que, dans certains cas, la colonne $n$ n'est pas constante à $n$ (*i.e.* la période de certaines lignes ne divise pas $n$), et qu'alors on arrive à obtenir des contre-exemples en jouant sur ce défaut de périodicité : dans $S_5$, $4 = 3*1 = 3*(5*1) \neq (3*5)*(3*1) = 4*4 = 5$. Le point surprenant est que la réciproque est vraie :

**Lemme 1.3.** *Pour chaque $n$, il y a équivalence entre :*

*(i) le système $S_n$ vérifie (LD) ;*

*(ii) on a $a * n = n$ pour tout $a$ de $[|n|]$ ;*

*(iii) la période de chaque ligne de $S_n$ divise $n$.*

**Preuve**. Supposons d'abord que $S_n$ est un LD-système. Alors pour tout $a$,

$$a * n = a * (n * n) = (a * n) * (a * n),$$

donc $a * n$ est idempotent, de sorte que $a * n = n$ d'après le lemme précédent. Pour la réciproque, on montre (LD) par triple induction : décroissante en $x$, décroissante en $y$, croissante en $z$. Il suffit d'appliquer (3) à chaque étape pour se ramener aux cas précédents ; $a * n = n$ amorce les recurrences. □

Ensuite, on remarque que les tables $S_n$ sont imbriquées les unes dans les autres au sens suivant.

**Lemme 1.4.** *Supposons que $S_n$ est un LD-système et que $n|m$. Alors $a \mapsto (a)_n$ définit un morphisme de $S_m$ sur $S_n$.*

**Preuve**. Posons $\pi(a) = (a)_n$, et vérifions $\pi(a*b) = \pi(a)*\pi(b)$ (avec $*$ désignant selon le contexte la loi de $S_m$ ou $S_n$) par récurrence double, décroissante en $a$ et croissante en $b$.
Pour $a = m$, on a :

$$\pi(m * b) = \pi(b) = n * \pi(b) = \pi(m) * \pi(b) \text{ (car } n|m).$$

Pour $a < m$, $b = 1$, on a :

$$\pi(a * 1) = \pi(a + 1) = (a + 1)_n = (a)_n * 1 = \pi(a) * \pi(1).$$

Pour $a < m$, $b = c + 1$, $c < m$, on a $\pi(a * b) = \pi((a * c) * (a * 1))$, d'où, comme $a * c > a$,

$$\begin{aligned}\pi(a * b) = \pi(a * c) * \pi(a * 1) &= (\pi(a) * \pi(c)) * (\pi(a) * \pi(1)) \\ &= \pi(a) * (\pi(c) * \pi(1)) = \pi(a) * \pi(b) \quad (4)\end{aligned}$$

où dans la dernère égalité on a utilisé le cas $a$ quelconque, $b = 1$. □

Plus précisément, on a la relation suivante :

**Lemme 1.5.** *Supposons que $S_n$ est un LD-système, et $n|m$ avec $n \neq m$. Alors on a les égalités suivantes, pour tout $b$ dans $S_m$ :*

*(i) Pour $m - n < a \leq m$,*

$$a *_m b = (a)_n *_n (b)_n + m - n.$$

*En particulier, la période de $a$ dans $S_m$ est celle de $(a)_n$ dans $S_n$.*

*(ii) Pour $a = m - n$,*

$$(m - n) *_m b = (b)_n + m - n.$$

*En particulier, la période de $(m - n)$ dans $S_m$ est $n$.*

*(iii) Pour $m - 2n \leq a < m - n$*

$$a *_m b = (a)_n *_n (b)_n + m - 2n + \delta(a, b)n$$

*avec $\delta(a, b) \in \{0, 1\}$.*
*En particulier, la période de $a$ dans $S_m$ est ou bien celle de $(a)_n$ dans $S_n$ ou bien son double.*

**Preuve**. *(i),(ii)* : Le lemme précédent détermine $a *_m b$ modulo $n$ ; or si l'on pose $d = m - n$, pour tout $k \in \{0, ..., n\}$, $(d + k) *_m b \geq d$. $a *_m b$ est donc déterminé uniquement, avec la bonne formule.
*(iii)* : Même raisonnement ; il y a deux valeurs possibles pour le produit. Notons $p$ la periode de $(a)_n$ dans $S_n$. Si la période de $a$ n'est pas $p$, elle est au moins égale à $2p$ car les $p < p' < 2p$ sont exclus par congruence, mais comme $p|n, p \neq n$, $2p \leq n$ implique $(a *_m 2p)_n = (a)_n *_n (2p)_n = (a)_n *_n (2p) = n$ on a $a *_m (2p) > a *_m (p) = m - n$ et on conclut que $a *_m (2p) = m$. □

Encore un petit lemme technique :

**Lemme 1.6.** *Supposons que les périodes de $a+1, \ldots, a+(d-1)$ dans $S_n$ divisent $a$. Alors, pour $1 \leq b \leq d$, on a $a * b = a + b$.*

**Preuve**. Par récurrence sur $b$. □

Voici le théorème central :

**Théorème 1.7.** *Le système $S_n$ verifie (LD) si et seulement si $n$ est une puissance de 2.*

**Preuve**. Montrons par récurrence sur $n \geq 0$ que les $S_{2^n}$ sont LD. Cela est vrai pour $n = 0$ ; si $S_{2^{n-1}}$ est LD, alors d'après le lemme (1.3) la période de chaque ligne divise $2^{n-1}$, donc d'après le lemme (1.5), la période de chaque ligne dans $S_{2^n}$ divise $2^n$, donc toujours d'après le lemme (1.3), $S_{2^n}$ est LD.
Réciproquement, supposons $n = p2^q$ avec $p$ impair, $p \geq 3$. Nous allons montrer que la ligne $n - 2^{q+1}$ est de période $2^{q+1}$. Le système $S_{2^q}$ est LD, donc les périodes de $1, \ldots, 2^n - 1$ divisent $2^n$, et en fait $2^{n-1}$. Donc d'après le lemme (1.5), dans $S_n$, les périodes de $N - 2^{n+1} + 1, \ldots, N - 1$ divisent $2^n$. Le lemme précédent permet alors de conclure. □

**Par conséquent, il existe un LD-système d'ordre $n$ satisfaisant (2) si et seulement si $n$ est une puissance de 2, et il est alors unique à isomorphisme près.**

## 1.2 Tables de Laver

Ce travail préliminaire étant accompli, nous avons enfin mis la main sur les objets désirés : on renomme $(S_{2^n}, *_{2^n})$ en $(A_n, *_n)$ et on l'appelle $n$-ième table de Laver.

**Proposition 1.8.** *(i) $A_n$ est un LD-système, dont l'unique générateur est 1 et l'unique idempotent est $2^n$.*

*(ii) Pour $m \geq n$, $a \mapsto (a)_{2^n}$ est un morphisme surjectif de $A_m$ sur $A_n$.*

Les questions auxquelles nous allons essayer de répondre par la suite concernent le comportement asymptotique des périodes des lignes. Par exemple, la proposition précédente implique que la suite des périodes de la ligne 1 est croissante au sens large. Ses premières valeurs sont : $1, 1, 2, 4, 4, 8, 8, 8, 8, 16, 16, \ldots$

**Question 1.9.** *Cette suite tend-elle vers l'infini avec $n$ ?*

# 2 Un peu de théorie des ensembles

## 2.1 Ordinaux

On a souvent besoin en mathématiques de faire des constructions pas à pas, ou *par récurrence*. Pour cela, on a besoin d'indiquer l'étape initiale et la

méthode de passage d'une étape à la suivante. Chaque étape est alors indexée par un entier.

En théorie des ensembles, on effectue aussi ce genre de démarche, mais on a besoin en général de plus d'étapes que ne l'autorisent les entiers. On utilise alors d'autres objets pour les indexer : les ordinaux.

La suite des entiers est caractérisée par le fait qu'elle a un premier element, 0, et que tout élément a un successeur. Pour construire les ordinaux, on ajoute un outil : le passage à la limite. Toute suite croissante d'ordinaux admet une borne supérieure. On distingue deux classes d'ordinaux : les *successeurs*, qui s'écrivent $\alpha + 1$, et les *limites*, qui n'ont pas de prédécesseur et sont la borne supérieure des ordinaux strictement inférieurs.

Les entiers sont ainsi les premiers ordinaux. Ensuite vient leur borne supérieure, le premier ordinal limite, noté $\omega$, puis son successeur $\omega + 1$, puis $\omega + 2$, $\omega + 3$, $\dots$ , $\omega + \omega = \omega * 2$ et ainsi de suite :

$$\omega * 2 + 1, \dots, \omega * 3, \omega * 4, \dots, \omega * \omega = \omega^2, \omega^3, \dots, \omega^\omega \dots$$

La construction exacte qu'on prend importe peu. La propriété essentielle des ordinaux est qu'ils sont bien ordonnées, *i.e.* tout ensemble d'ordinaux admet un plus petit élément. Ce qui permet de faire des récurrences : par rapport à la récurrence usuelle, il faut ajouter une étape pour les ordinaux limites.

En plus, il existe des ordinaux aussi grands qu'on veut : l'ensemble de tous les ordinaux n'existe pas, sinon on pourrait prendre le successeur du sup de tous les ordinaux, qui serait un ordinal strictement plus grand que tous les ordinaux.

On appelle *cardinal* un ordinal qui ne peut être mis en bijection avec aucun ordinal strictement plus petit que lui. On peut démontrer en utilisant l'axiome du choix que tout ensemble est en bijection avec un unique cardinal.

Le premiers cardinaux sont les entiers. Ensuite vient $\omega$ qu'on note $\aleph_0$ quand on le regarde comme un cardinal. Les ordinaux étant bien ordonnés, il existe un plus petit cardinal strictement plus grand qu'$\aleph_0$. On le note $\aleph_1$. On peut continuer comme cela en définissant la suite $(\aleph_\alpha)$ des cardinaux infinis où $\alpha$ parcourt les ordinaux.

Une des activités favorites du théoricien des ensembles est l'étude des *grands cardinaux*, à savoir des cardinaux qui ont de tels propriétés qu'ils doivent être plus grands que tous ceux qu'on manipule habituellement. Le cardinal $\aleph_0$ est le premier grand cardinal dans le sens que le passage du fini à l'infini demande un saut conceptuel important et qu'il jouit de propriétés impossibles pour un ensemble fini. Par exemple, il admet une injection non-surjective de lui-même dans lui-même. C'est une propriété de cet ordre là, mais beaucoup plus restrictive, qui permettra de définir des grands cardinaux qui seront alors en quelque sorte aux infinis usuels ce que l'infini est au fini.

Un des axiomes de ZFC dit qu'il existe un ensemble infini. Cet axiome est indispensable au sens où avec uniquement des ensembles finis à notre disposition,

on ne peut pas démontrer l'existence d'un ensemble infini. Il en va de même pour les grands cardinaux. On ne peut démontrer leur existence à partir des axiomes de ZFC. Pour les manipuler, on est forcé d'ajouter de nouveaux axiomes.

En fait, la situation est pire : on ne peut même pas démontrer leur consistance relative, c'est-à-dire qu'on ne peut pas démontrer qu'en introduisant de tels ensembles, on n'introduit pas des contradictions dans la théorie.

Il y a donc deux possibilités : soit ces axiomes sont consistants avec les précédents, mais alors on ne le saura jamais. Soit ils ne le sont pas, et on en trouvera peut-être un jour la démonstration. Sauf à contourner la contradiction en reformulant les preuves, tous les résultats qui auront été montré à partir d'eux n'auront alors plus aucune valeur.

Néanmoins, une telle contradiction n'ayant toujours pas été trouvée, on peut raisonnablement supposer qu'il n'en existe pas et les manier comme si leur existence était cohérente avec le reste de la théorie des ensembles.

## 2.2 Rangs

Un apport conceptuel important de la théorie des ensembles est que toutes les mathématiques peuvent être formalisées en ne considérant qu'un seul type d'objets : les ensembles, qui sont ensembles d'ensembles d'ensembles etc. ; le etc. prenant fin lorsqu'on arrive sur l'ensemble vide.

On peut inversement remonter la construction et construire tous les ensembles en partant de $\emptyset$. On va ainsi faire apparaître une hiérarchie entre les ensembles, hiérarchie qu'on indexe par les ordinaux.

**Définition 2.1** (Rangs)**.** On définit par induction ordinale les ensembles $R_\alpha$ par :

$$\begin{array}{lcll} R_0 & = & \emptyset & \\ R_{\alpha+1} & = & \mathfrak{P}(R_\alpha) & \\ R_\lambda & = & \cup_{\alpha<\lambda} R_\alpha & \text{pour } \lambda \text{ limite.} \end{array}$$

(où $\mathfrak{P}$ désigne l'ensemble des parties d'un ensemble).

Les ensembles $R_\alpha$ sont appelés *rangs*.

La suite des rangs est croissante et *l'axiome de fondation* de ZFC exprime que chaque ensemble est inclus dans un des $R_\alpha$. La construction des ordinaux assure que l'ordinal $\alpha$ est dans le rang $R_{\alpha+1}$ mais pas dans le rang $R_\alpha$.

Exemple 2.2. *Les premiers rangs sont comme suit :*

$$R_0 = \emptyset, \qquad R_1 = \{\emptyset\}, \qquad R_2 = \{\emptyset, \{\emptyset\}\}, \qquad R_3 = \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}\}, \quad \ldots$$

## 2.3 Plongements élémentaires

Venons-en à présent à la présentation de l'objet à la base de tout ce qui va suivre : le *plongement élémentaire*. Avant d'en donner la définition formelle, expliquons ce dont il s'agit.

Un plongement élémentaire $j : R_\alpha \to R_\alpha$ est une application définie sur le rang $R_\alpha$ dans lui-même qui conserve toutes les propriétés formalisables en théorie des ensembles.

Expliquons ce que cela veut dire.

On considère les énoncés qu'on peut écrire sous la forme d'une formule mathématique avec des quantificateurs $\forall$, $\exists$, des liens logiques $\wedge$,$\vee$,$\neg$, et des symboles ensemblistes $\in$,$\subseteq$,$\{..\}$ ...

En fait ces conditions sont très peu restrictives et on sait bien que l'on peut traduire tous les énoncés mathématiques usuels en une formule de ce type.

Par exemple pour dire qu'une fonction $f$ est injective, on a envie d'écrire

$$(\forall x, y)(f(x) = f(y) \Rightarrow x = y).$$

La notion $f(x)$ n'est a priori pas ensembliste, mais peut le devenir facilement. En effet, si on assimile une fonction à un ensemble de couples on a :

$$f(x) = y \Leftrightarrow (x, y) \in f.$$

On considèrera ainsi la première formule comme permise sachant qu'on pourrait la récrire de manière à ne faire apparaître que des symboles ensemblistes.

Il en va de même pour tous les concepts introduits en maths.

**Définition 2.3.** Soit $R_\alpha$ un rang. Un *plongement élémentaire* de $R_\alpha$ dans $R_\alpha$ est une application $j : R_\alpha \to R_\alpha$ telle que pour toute formule $\phi(x_1, \ldots, x_n)$ et pour tout $(a_1, \ldots, a_n) \in R_\alpha^n$ on ait :

$$\phi(a_1, \ldots, a_n) \Leftrightarrow \phi(j(a_1), \ldots, j(a_n)).$$

Par exemple, si $f : A \to B$ est une fonction injective telle que $f, A, B \in R_\alpha$, alors $j(f)$ est aussi une fonction injective, avec $j(f) : j(A) \to j(B)$.

L'identité est bien sûr toujours un plongement élémentaire, dit trivial. Très souvent, c'est le seul et il faut considérer des rangs extrêmement gros pour qu'il en existe d'autres.

**Définition 2.4.** Un rang $R_\alpha$ est dit *auto-similaire* lorsqu'il existe un plongement élémentaire $j : R_\alpha \to R_\alpha$ non trivial. On définit alors $\hat{E}_\alpha$ comme étant l'ensemble de ces plongements élémentaires, et $E_\alpha = \hat{E}_\alpha \setminus \{id\}$ l'ensemble des plongements élémentaires non triviaux.

On justifiera par la suite que l'existence d'un tel $\alpha$ est une hypothèse de grand cardinal, qui entre dans le cadre mentionné plus haut : on ne peut démontrer qu'il en existe et jusqu'à présent personne n'en a tiré une contradiction.

## 2.4 Ordinal critique

**Définition 2.5.** *L'ordinal critique* de $j \in \hat{E}_\alpha$ est le plus petit ordinal non-invariant par $j$, s'il existe. On le note $\mathrm{crit}(j)$.

La proposition suivante montre que le comportement de $j$ sur les ordinaux détermine en partie $j$, et que l'ordinal critique joue un rôle pivot.

**Proposition 2.6.** *Soit $j \in E_\alpha$.*

*(i) L'application $j$ stabilise l'ensemble des ordinaux strictement inférieurs à $\alpha$ et y est strictement croissant.*

*(ii) De plus, $j$ a un ordinal critique $\kappa$. On a $j(\kappa) > \kappa$, et $j \restriction R_\kappa = id_{R_\kappa}$. En particulier, $j$ n'est pas surjective.*

**Preuve**. *(i)* La propriété "être un ordinal" est définissable par une formule, donc $j$ envoie ordinaux plus petits que $\alpha$ sur ordinaux plus petits que $\alpha$. Par ailleurs, la construction des ordinaux montre que la relation d'ordre strict sur les ordinaux se confond avec $\in$, donc elle est bien préservée par $j$.

*(ii)* On commence par établir :

**Lemme 2.7.** *Soit $\theta$ un ordinal de $R_\alpha$. Supposons que $j$ est l'identité sur les ordinaux plus petits que $\theta$. Alors pour tout $\gamma \leq \theta$, $j \restriction R_\gamma = id_{R_\gamma}$.*

*Preuve.* Par récurrence ordinale sur $\gamma$.

Pour $\gamma = \delta + 1$, soit $x \in R_\gamma$, c'est-à-dire $x \subseteq R_\delta$. Si $y \in x$, alors $y \in R_\delta$, donc $j(y) = y$ par hypothèse de récurrence. Comme $x \in y$ implique $j(x) \in j(y)$, $x \subseteq j(x)$. Réciproquement, $j(x) \in R_{j(\delta+1)=R_{j(\delta)+1}} = R_{\delta+1}$, donc si $y \in j(x)$, $y \in R_{\delta+1}$ (car $R_{\delta+1}$ est transitif), et $y = j(y)$. Donc $y \in j(x)$ entraîne $j(y) \in j(x)$ et $y \in x$ d'où $j(x) \subseteq x$. Donc $j(x) = x$.

Pour $\gamma$ limite, la récurrence est évidente. ■

Le lemme implique qu'il existe un ordinal critique : si cela n'était pas le cas, $j$ serait l'identité sur $R_\alpha$. En réappliquant le lemme à $\kappa$, et en utilisant l'injectivité de $j$, on obtient le résultat. □

On peut montrer que l'ordinal critique est en fait un cardinal, dont l'existence n'est pas démontrable dans ZFC (on peut par exemple montrer qu'il s'agit d'un cardinal *mesurable*). C'est en ce sens que l'existence d'un rang autosimilaire est un axiome de grand cardinal, et que les résultats démontrés à partir de cette hypothèse (donc tout ce qui suit) a un statut problématique. L'idée est que si l'ordinal critique $\kappa$ était définissable par des opérations ensemblistes à partir des ordinaux plus petits (donc points fixes de $j$), en appliquant $j$ à cette définition, on obtiendrait que $j(\kappa)$ vérifie la même définition, donc serait égal à $\kappa$ ! Donc $\kappa$ est inaccessible à partir des ordinaux plus petits, ce qui est une caractéristique des grands cardinaux.

En étudiant la consistance des axiomes de grands cardinaux définis à partir de plongements élementaires, Kunen a démontré le résultat suivant (cf. 6) :

**Théorème 2.8** (borne de Kunen)**.** *Soit $R_\alpha$ un rang auto-similaire, $j \in E_\alpha$, $\kappa = \mathrm{crit}(j)$. Alors :*

$$\alpha = \sup_{n\in\mathbb{N}} j^n(\kappa) \text{ ou } \alpha = \sup_{n\in\mathbb{N}} j^n(\kappa) + 1.$$

Donc en particulier $\alpha$ est soit un ordinal limite soit le sucesseur d'un ordinal limite, et $j$ est trivial jusqu'à tout près du sommet du rang. Dans la suite on se place dans le cas $\alpha = \lambda$ limite.

## 2.5 Application sur $E_\lambda$

Fixons un rang limite autosimilaire $R_\lambda$. On dispose sur $E_\lambda$ d'une opération évidente, à savoir la composition. Mais la structure de rang limite permet de définir une autre opération de nature différente :

**Définition 2.9.** Soient $j_1, j_2$ dans $E_\lambda$. On veut définir *l'application de $j_1$ à $j_2$, $j_1[j_2]$*. $j_2$ n'est pas un élément de $E_\lambda$, donc $j_1(j_2)$ n'a pas de sens. Mais parce que $\lambda$ est limite, on peut poser :

$$j_1[j_2] = \bigcup_{\theta<\lambda} j_1(j_2 \restriction R_\theta).$$

Cela a bien un sens car :

$$j_2 \restriction R_\theta \subseteq R_{j_2(\theta)+2} \in R_\lambda.$$

Il s'agit d'une application de $R_\lambda$ dans lui-même par cohérence.

Il n'est pas difficile de vérifier que $j_1[j_2]$ est encore un plongement élémentaire, par la méthode suivante, qui illustre bien le fait que la nécessité de restreindre à un rang plus petit n'est qu'une difficulté technique : Si $F(\vec{x})$ ( où $\vec{x}$ désigne les paramètres ) est une formule de théorie des ensembles, on a puisque $j_2$ est élémentaire :

$$F(\vec{a}) \Leftrightarrow F(j_2(\vec{a})).$$

En particulier c'est vrai lorsqu'on se restreint à un rang $R_\gamma$ plus petit, en remplaçant $j_2$ par $j_2 \restriction R_\gamma$. Si l'on note G la formule

$$(\forall \vec{x} \in \mathrm{Dom}(f))(F(\vec{x}) \Leftrightarrow F(f(\vec{x})))$$

on a donc $G(j_2 \restriction R_\gamma)$. Comme $j_1$ est élémentaire, on a également $G(j_1(j_2 \restriction R_\gamma))$, et ce pour tout $\gamma < \lambda$, d'où le résultat.

Tout se passe comme si on appliquait effectivement $j_1$ à $j_2$. Par exemple, si l'on représente $j_2$ comme un ensemble de couples et si $x$ est dans l'image de $j_1$, $x = j_1(y)$, on a dans $j_2$ le couple $(y, j_2(y))$ et donc on a dans $j_1[j_2]$ le couple $(x, j_1 \circ j_2(y)) = (x, j_1 \circ j_2 \circ j_1^{-1}(x))$.

D'où la formule explicite :

$$j_1[j_2] \restriction \mathrm{Im}(j_1) = j_1 \circ j_2 \circ j_1^{-1}.$$

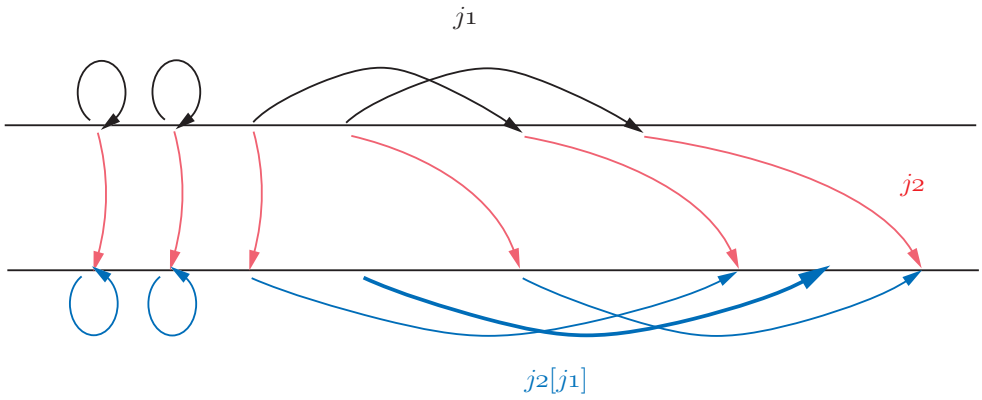


FIG. 1 – Application $j_1[j_2]$ (représentée sur les ordinaux)

Le comportement hors de l'image de $j_1$ (on a vu qu'elle n'était pas surjective) est plus délicat, et on n'a pas de formule explicite.

La propriété la plus importante de l'application, et celle qui nous rapproche des tables de Laver, est qu'elle satisfait l'identité (LD). Là encore, aux problèmes de restriction près, il suffit "d'appliquer" $j_1$ à $j_2[j_3]$ pour obtenir

$$j_1[j_2[j_3]] = j_1[j_2][j_1[j_3]].$$

Enfin, un coup d'oeil à la figure 1 rend clair le fait que l'ordinal critique d'une application vérifie :

$$\mathrm{crit}(j_1[j_2]) = j_1(\mathrm{crit}(j_2)).$$

**Définition 2.10.** On note $\mathrm{Iter}(j)$ le sous-LD système de $(E_\lambda, [\,])$ engendré par $j$. On définit la suite $\mathrm{crit}_n$ par : $\mathrm{crit}_n$ est le $n$-ième plus petit ordinal qui est un ordinal critique d'un élément de $\mathrm{Iter}(j)$, qui existe parce que les ordinaux forment un bon ordre.

# 3 Quotients finis et tables de Laver

## 3.1 Congruence

Nous avons à présent un système autodistributif $\mathrm{Iter}(j)$ engendré par un unique élément $j$. Afin de faire le lien avec les tables de Laver, il nous reste à quotienter cet ensemble par une congruence adaptée.

**Définition 3.1.** Soit $\gamma$ un ordinal limite inférieur à $\lambda$. On dit que deux plongements élémentaires $j$ et $j'$ de $R_\lambda$ sont $\gamma$-équivalents si, pour tout $x \in R_\gamma$, on

a $j(x) \cap R_\gamma = j'(x) \cap R_\gamma$. On notera alors

$$j \overset{\gamma}{=} j'.$$

De manière équivalente, on a, en gardant les même notations

$$(\forall x, y \in R_\gamma)(y \in j(x) \Leftrightarrow y \in j'(x)).$$

Intuitivement, deux plongements sont $\gamma$-équivalents s'ils se comportent de la même maniére vis-a-vis de $R_\gamma$, mais la condition qu'on met est strictement plus faible que celle peut-être plus naturelle a priori : $j \restriction R_\gamma = j' \restriction R_\gamma$ (voir la deuxième partie pour plus de précisions).

Remarquons par contre que si $j$ et $j'$ sont $\gamma$-équivalents, que $x \in R_\gamma$, et que $j(x) \in R_\gamma$, alors $j'(x) = j(x)$ (Pour le voir, prendre $\{x\}$ dans la définition).

Le résultat facile suivant sera utile par la suite :

**Fait 3.2.** *$j$ est $\gamma$-équivalent à l'identité si et seulement si $\gamma \leq \mathrm{crit}(j)$.*

D'autre part, si $\mathrm{crit}(j) < \gamma$, alors tout ordinal $\gamma$-équivalent à $j$ a le même ordinal critique que $j$.

On peut montrer que ces relations de $\gamma$-équivalence sont des congruences pour l'application (cf. 4 pour une discussion de cette question).

**Proposition 3.3.** *Soit $\gamma$ un ordinal limite, $j_1, j_2, j_1', j_2'$ des plongements élémentaires. On suppose qu'on a $j_1 \overset{\gamma}{=} j_2$, $j_1' \overset{\gamma}{=} j_2'$, alors*

$$j_1[j_1'] \overset{\gamma}{=} j_2[j_2'].$$

## 3.2 Quotients

On a vu précédemment comment construire une suite croissante d'ordinaux $(\mathrm{crit}_n(j))_{n\in\mathbb{N}}$ liée aux plongements élémentaires de $\mathrm{Iter}(j)$. On peut utiliser ces ordinaux comme paramètres dans la congruence précédente pour quotienter cet ensemble. On obtient ainsi des systèmes auto-distributifs finis isomorphes aux des tables de Laver.

Pour cela, on définit les puissances à gauche de $j$ par récurrence : $j_{[1]} = j$, $j_{[n+1]} = j_{[n]}[j]$. On peut démontrer que, pour tout $n$, tout élément de $\mathrm{Iter}(j)$ est $\mathrm{crit}_n(j)$-équivalent à une certaine puissance à gauche de $j$.

Or on peut décrire en détails la $\mathrm{crit}_n$-équivalence sur les puissances à gauche :

**Proposition 3.4.** *Les puissances à gauche $j_{[p]}$ et $j_{[p']}$ sont $\mathrm{crit}_n$-équivalents ssi on a $p \equiv p' \ mod\ 2^n$.*

Ainsi, les éléments $j_{[1]}$, ..., $j_{[2^n]}$ forment un système de représentants des classes de $\mathrm{crit}_n$-équivalences sur $\mathrm{Iter}(j)$. On a même mieux.

**Théorème 3.5.** *Soit $n \in \mathbb{N}$, alors le quotient de $\mathrm{Iter}(j)$ par la congruence $\overset{crit_n(j)}{=}$ est isomorphe à la table de Laver $A_n$, un isomorphisme étant donné par $\phi : i \to \overline{j_{[i]}}$.*

En effet, on a bien $j_{[i]}[j_{[1]}] = j_{[i+1]}$ pour $1 \leq i \leq 2^n - 1$, et $j_{[2^n]}[j_{[1]}] = j_{[2^n+1]} \overset{\text{crit}_n}{=} j_{[1]}$.

Cet isomorphisme permet de ramener des calculs sur les plongements élémentaires à des identités dans les tables de Laver. Il implique notamment que les ordinaux de la suite $(\text{crit}_n)$ sont des ordinaux critiques de puissances à gauche de $j$.

EXEMPLE 3.6. *Soit $n \in \mathbb{N}$, on sait que tout élément de $f$ de Iter(j) est $\text{crit}_n$-équivalent à un $j_{[k]}$ pour un certain $k$. On peut utiliser les tables de Laver pour calculer la valeur de $k$ dans des cas précis.*

*Prenons par exemple $n = 4$ et $f = j[j[j_{[3]}]]$. Alors, en reprenant la notation du théorème précédent, l'isomorphisme $\phi^{-1}$ envoie $f$ sur $1 *_4 (1 *_4 3)$.*

*On lit directement dans la table $A_4$ : $1 *_4 (1 *_4 3) = 12$. On en conclut donc la congruence $j[j[j_{[3]}]] \overset{crit_4}{=} j_{[12]}$.*

Inversement, on peut utiliser les résultats connus sur les plongements élémentaires pour en déduire des propriétés des tables de Laver.

## 3.3 Période des tables de Laver

Revenons au problème de départ, à savoir celui de la période de la première ligne des tables de Laver. On va montrer comment apporter une réponse à cette question grâce aux plongements élémentaires.

La premiére idée est que l'augmentation de la période de la première ligne d'une table de Laver à la suivante peut se caractériser algébriquement de manière simple :

**Proposition 3.7.** *La période de la première ligne passe de $2^m$ à $2^{m+1}$ entre les tables $A_n$ et $A_{n+1}$ si et seulement si :*

$$1 *_{n+1} 2^m = 2^n.$$

**Preuve**. En effet, l'égalité $1 *_{n+1} 2^m = 2^n$ implique que la période de 1 dans $A_{n+1}$ est supérieure à $2^{m+1}$. D'autre part, en appliquant le morphisme canonique de $A_{n+1}$ sur $A_n$, on obtient $1 *_n 2^m = 2^n$. Donc la période de 1 dans $A_n$ est au plus $2^m$.

Or, entre une table et la suivante, la période d'une ligne reste identique ou double. On en conclut donc que la période de la première ligne passe de $2^m$ à $2^{m+1}$ entre les tables $A_n$ et $A_{n+1}$.

Réciproquement, si la période de 1 passe de $2^m$ à $2^{m+1}$ entre $A_n$ et $A_{n+1}$, alors on a $1 *_n 2^m = 2^n$, donc $1 *_{n+1} 2^m$ vaut $2^n$ ou $2^{n+1}$. Cette dernière valeur est exclue car la période de 1 dans $A_{n+1}$ est strictement supérieure à $2^m$. □

Tout se ramène donc à trouver à $m$ fixé, une solution en $n$ de l'équation $1 *_{n+1} 2^m = 2^n$. Si c'est possible, on sera certain que la période de la première ligne des tables de Laver tend vers l'infini.

Or cette équation est équivalente à $j[j_{[2^m]}] \overset{\text{crit}_{n+1}(j)}{=} j_{[2^n]}$.

**Proposition 3.8.** *Pour tout terme t, s'il existe n tel que* $\mathrm{crit}(t(j)) = \mathrm{crit}_n(j)$, *alors*

$$t(j) \overset{crit_{n+1}(j)}{=} j_{[2^n]}.$$

**Preuve**. Puisque $n = \mathrm{crit}(t(j))$, $t(j)$ est $\mathrm{crit}_n$-équivalent à l'identité. Ce qui se traduit par $t(1) = 2^n$ dans $A_n$. Il y a donc deux valeurs possibles pour $t(1)$ calculé dans $A_{n+1}$ qui sont $2^n$ et $2^{n+1}$.

Supposons que $t(1)$ dans $A_{n+1}$ vaille $2^{n+1}$. Cela veut dire que $t(j)$ est $\mathrm{crit}_{n+1}$-équivalent à l'identité. Donc que son ordinal critique est supérieur à $\mathrm{crit}_{n+1}$. Ce qui contredit les hypothèses.

Ainsi, on a bien $t(1) = 2^n$ dans $A_{n+1}$, c'est-à-dire $t(j) \overset{\mathrm{crit}_{n+1}(j)}{=} j_{[2^n]}$ □

Il suffirait donc de démontrer qu'un tel $n$ existe toujours. Ce ne serait pas le cas si et seulement si $\mathrm{crit}(t(j))$ était plus grand que tous les $\mathrm{crit}_n$. Ici intervient un théorème important.

**Théorème 3.9** (Laver-Steel)**.** *Soit* $(j_n)$ *une suite de plongements élémentaires tels que pour tout* $i \geq 0$, $j_i$ *est un diviseur à gauche de* $j_{i+1}$ *dans* $\mathrm{Iter}(j)$. *Alors :*

$$\sup_n \mathrm{crit}(j_n) = \lambda$$

En particulier, le résultat s'applique à la suite des puissances à gauche de $j$ : les ordinaux critiques des $j_{[p]}$ s'ordonnent en une suite strictement croissante qui tend vers $\lambda$. Et on a vu dans la remarque suivant le théorème 3.5 que les ordinaux critiques des $j_{[p]}$ étaient exactement les $\mathrm{crit}_n$, ce qui permet de conclure.

**Ainsi la période de la première ligne de $A_n$ tend vers l'infini avec $n$. On a même un résultat plus précis : le $n$ minimal tel que cette période vaille $2^{m+1}$ est tel que** $\mathrm{crit}(j[j_{[2^m]}]) = \mathrm{crit}_n(j)$.

## 3.4 Conclusion

La résultat qu'on obtenu a un statut particulier. En effet, toute la démonstration qui précède repose sur l'existence d'un rang auto-similaire. Or on sait qu'on ne peut démontrer même la consistance de cette hypothèse. On ne peut ainsi certainement considérer avoir démontré que la période de la première ligne des tables de Laver tendait vers l'infini. Cette démonstration en appelle une autre qui serait plus élémentaire (si on peut dire...).

Elle n'est pas pour autant inutile puisqu'elle nous indique que ce résultat a de grandes chances d'être vrai. En effet, on considère que l'existence d'un rang auto-similaire est une hypothèse très probablement consistante.

Appelons (Inf) le résultat : "La période de la première ligne des tables de Laver $A_n$ tend vers l'infini avec $n$".

On peut résumer la situation par la disjonction de cas suivante :
**Cas 1** :

On peut démontrer dans ZFC qu'il n'existe pas de rang auto-similaire.

Dans ce cas, on peut espérer trouver un jour une telle démonstration. La preuve faite ci-dessus n'a telle quelle aucune valeur, et on ne sait rien de plus sur la périodicité des tables de Laver.

**Cas 2** :
L'hypothèse de l'existence d'un rang auto-similaire est consistante avec ZFC.

Si on est dans ce cas, on ne pourra jamais le savoir.
Par contre la démonstration ci-dessus a alors un sens et donne essentiellement comme résultat :
* ZFC ne démontre pas que (Inf) est faux.
En fait, on peut faire une nouvelle distinction de cas :

*sous-cas 1.* ZFC prouve (Inf)
C'est la situation qu'on espère. Ce résultat serait alors vrai au même titre que tout autre résultat mathématique.
Mais il faut envisager un deuxième cas :

*sous-cas 2.* ZFC ne prouve ni (Inf), ni sa négation.
Ce serait là une situation intéressante : on aurait un résultat simple de combinatoire finie indécidable dans ZFC.
De plus, ce cas montre que même en supposant la consistance de l'existence d'un rang auto-similaire, on ne peut en conclure (Inf) pour autant. Il faudrait en fait faire l'hypothèse autrement plus forte de l'existence d'un modèle de ZFC+"Il existe un rang autosimilaire" ne contenant que des entiers standards.

## Deuxième partie

# Approfondissements

## 4 Pourquoi l'équivalence ?

Revenons sur la congruence des plongements élémentaires définie dans la première partie.

Rappelons la définition de la $\gamma$-équivalence :

$$j \stackrel{\gamma}{=} j' \Leftrightarrow (\forall x \in R_\gamma)(j(x) \cap R_\gamma = j'(x) \cap R_\gamma). \tag{5}$$

Il s'avère que cette relation d'équivalence est une congruence pour l'application.

Le lecteur peut se demander à juste titre pourquoi on a pris cette relation d'équivalence et pas une autre.

En fait, on aurait pu en envisager deux autres qui seraient définies par

$$j \restriction R_\gamma = j' \restriction R_\gamma$$

et

$$j \restriction R_\gamma^2 = j' \restriction R_\gamma^2.$$

(Remarquer qu'on considère $j$ comme une fonction dans la première définition et comme un ensemble de couples dans la seconde).

Ces deux équivalences — appelons-les respectivement (Eq 1) et (Eq 2) — en fait ne sont pas compatibles avec l'application. Essayons de voir pourquoi.

Supposons que $j_1$, $j_1'$ soient $\gamma$-équivalents au sens de (Eq 1) et soit $j_2$ un autre plongement élémentaire. Prenons un $x \in R_\gamma$. On aimerait montrer que $j_1[j_2](x) = j_1'[j_2](x)$. Supposons que $x$ est dans l'image de $j_1$, *i.e.* $j_1(y) = x$. On a alors $y \in R_\gamma$ et $j_1'(y) = x$. La valeur de $j_1[j_2](x)$ est alors donnée par $j_1(j_2(y))$. Seulement $j_2(y)$ n'est pas a priori dans $R_\gamma$ et il n'y a donc aucune raison pour que $j_1'(j_2(y))$ soit égal à $j_1(j_2(y))$.

Ceci explique que l'équivalence (Eq 1) ne soit pas en général compatible avec l'application.

Exemple 4.1. *Soit $j$ un plongement élémentaire non trivial du rang $R_\gamma$. Soit $\alpha_0 =$*crit$(j)$*. On sait qu'il existe $j_1 \in Iter(j)$ tel que $\alpha_1 :=$* crit$(j_1) = j(\alpha_0)$.

*On a alors, $j_1 \restriction R_{\alpha_1} = id \restriction R_{\alpha_1}$, mais d'autre part : $(j_1 \circ j)(\alpha_0) = j_1(\alpha_1) > \alpha_1$, alors que $(id \circ j)(\alpha_0) = \alpha_1$, donc $(j_1 \circ j) \restriction R_{\alpha_1} \neq (id \circ j) \restriction R_{\alpha_1}$.*

Intéressons-nous maintenant à la deuxième équivalence envisagée.

Introduisons la notation $x =\restriction_\gamma y$ pour signifier "si $x$ ou $y$ est dans $R_\gamma$, alors $x = y$".

Cette équivalence peut alors se reformuler de la manière suivante : $j$ et $j'$ sont $\gamma$-équivalents au sens de (Eq 2) si, pour tout $x \in R_\gamma$, $j(x) =\restriction_\gamma j'(x)$.

Cette relation n'est pas mise en défaut par le cas particulier où nous nous sommes placés ci-dessus. Mais elle n'est quand même pas assez forte pour être compatible avec [ ] dans le cas général.

Plus précisément, en reprenant les notations précédentes, si $x \in R_\gamma$ avec $x = j_1(y) = j'_1(y)$, alors soit $j_2(y) \in R_\gamma$ auquel cas $j'_2(y) = j_2(y)$ et $j_1[j_2](x) = j_1(j_2(y)) =\restriction_\gamma j'_1[j'_2](x)$, soit $j_2(y) \notin R_\gamma$ auquel cas on a $j'_2(y) \notin R_\gamma$ et a fortiori $j_1[j_2](x) \notin R_\gamma$. De même $j'_1[j'_2](x) \notin R_\gamma$, ce qui assure à nouveau $j_1[j_2](x) =\restriction_\gamma j'_1[j'_2](x)$.

(Eq 2) se comporte donc bien dans l'image de $j_1$. Maintenant soit $x$ quelconque dans $R_\gamma$. On peut dire que $j_1[j_2](x) =\restriction_\gamma j_1[j'_2](x)$. En effet, la phrase suivante est vérifiée :

$$(\forall x \in R_\gamma)((j_2 \restriction R_\gamma)(x) =\restriction_\gamma (j'_2 \restriction R_\gamma)(x).$$

Donc en appliquant $j_1$, compte tenu du fait que $j_1(\gamma) \geq \gamma$, on obtient

$$(\forall x \in R_\gamma)((j_1(j_2 \restriction R_\gamma))(x) =\restriction_\gamma (j_1(j'_2 \restriction R_\gamma))(x).$$

Ceci permet de conclure que $j_1[j_2]$ et $j_1[j'_2]$ sont $\gamma$-équivalents au sens de (Eq 2).

On ne peut pour autant pas affiner ce résultat en $j_1[j_2]$ et $j'_1[j'_2]$ $\gamma$-équivalents. Le problème étant que $j_1(j_2 \restriction R_\gamma)$ et $j'_1(j'_2 \restriction R_\gamma)$ ne sont pas en général des éléments de $R_\gamma$. L'hypothèse d'équivalence sur $j_1$ et $j'_1$ ne permet donc pas d'affirmer quoi que ce soit sur ces deux éléments. C'est là qu'il est utile d'avoir l'hypothèse plus forte $j_1 \stackrel{\gamma}{=} j'_1$.

Bien entendu, nous n'avons ici pas démontré que la deuxième équivalence n'était pas une congruence. Nous avons juste tenté de montrer pourquoi la démonstration faite pour la $\gamma$-équivalence (5) ne pouvait s'appliquer ici. En fait, nous n'avons pas réussi à construire de contre-exemple, et il n'est pas exclu a priori que cette équivalence soit une congruence. Tout ce qu'on peut dire, c'est que ce n'est pas évident et qu'il semble peu probable qu'elle en soit une.

## 4.1 Naturalité de la gamma-équivalence

La vraie $\gamma$-équivalence peut se reformuler :

$$j \stackrel{\gamma}{=} j' \Leftrightarrow (\forall x, y \in R_\gamma)(y \in j(x) \Leftrightarrow y \in j'(x)).$$

Nous allons montrer, un résultat plus fort qui finira de montrer la naturalité de cette équivalence.

On considère des formules $\phi$ écrite dans la signature $\Sigma = \{\in, f\}$, où $f$ est un symbole de fonction. Pour simplifier l'écriture, on notera une telle formule $\phi(f, x_1, \ldots, x_n)$ où on considère $f$ comme ayant le statut d'une variable. De plus, on notera $\phi^{R_\gamma}$ la formule obtenue en restreignant tous les quantificateurs de $\phi$ à $R_\gamma$ selon la procédure habituelle.

**Proposition 4.2.** *Supposons $j \stackrel{\gamma}{=} j'$. Alors, quelle que soit la $\Sigma$-formule $\phi(f, x_1, \ldots, x_n)$, et quels que soient $a_1, \ldots, a_n$ dans $R_\gamma$, on a*

$$\phi^{R_\gamma}(j, a_1, \ldots, a_n) \Leftrightarrow \phi^{R_\gamma}(j', a_1, \ldots, a_n).$$

**Preuve**. Montrons cela par récurrence sur la complexité de la formule $\phi$.

Si $\phi$ est atomique de la forme $x_i = x_j$ ou $x_i \in x_j$, le résultat est évident.

Soient $t(f, x_1, \ldots, x_n)$ et $t'(f, x_1, \ldots, x_n)$ deux termes, montrons

$$(\forall \bar{a} \in R_\gamma)(t(j, \bar{a}) \in t'(j, \bar{a}) \Leftrightarrow t(j', \bar{a}) \in t'(j', \bar{a}))$$

par récurrence sur la complexité de $t$ et $t'$.

Il existe $p$, $q$, $k$ et $l$ tels qu'on ait $t = f^{(p)}(x_k)$ et $t' = f^{(q)}(x_l)$.

Le cas ($p = 0$, $q = 1$) est la définition de la $\gamma$-équivalence. Pour le cas ($p = 1$, $q = 0$), ie $\phi = j(x_k) \in x_l$, remarquons que si on a $j(a_k) \in a_l$, avec $a_k, a_l \in R_\gamma$, alors $j(a_k) \in R_\gamma$, donc $j'(a_k) = j(a_k)$ et le résultat en découle.

Le cas ($p = 0$, $q > 1$) (*resp.* ($p > 1$, $q = 0$)) se ramène au cas précédent appliqué à la formule $\phi' = (x_k = f(x_l))$ (*resp.* $\phi' = (f(x_k) = x_l)$) et aux plongements élémentaires $\gamma$-équivalents $j^{(q)}$ et $j'^{(q)}$ (*resp.* $j^{(p)}$ et $j'^{(p)}$).

Enfin, si $p > 0$ et $q > 0$, on est aussi ramené au cas ci-dessus grâce à l'équivalence vraie pour tout $a_k, a_l \in R_\lambda$ :

$$j(a_k) \in j(a_l) \Leftrightarrow a_k \in a_l.$$

Pour montrer l'équivalence

$$(\forall \bar{a} \in R_\gamma)(t(j, \bar{a}) = t'(j, \bar{a}) \Leftrightarrow t(j', \bar{a}) = t'(j', \bar{a}))$$

on procède de la même manière.

Notons qu'on a

$$(\forall x, y \in R_\gamma)(j(x) = y \Leftrightarrow j'(x) = y),$$

car $j(\{x\}) = \{j(x)\}$ et que la $\gamma$-équivalence ($\gamma$ limite) implique
$y \in j(\{x\}) \Leftrightarrow y \in j'(\{x\})$.

Le résultat est donc démontré pour $\phi$ atomique. Si $\phi = \phi_1 \wedge \phi_2$, ou $\phi = \neg\phi_1$ on applique l'hypothèse de récurrence sur $\phi_1$ et $\phi_2$.

Enifn, si $\phi = (\forall x)\psi(f, x, x_1, \ldots, x_n)$, on a $\phi^{R_\gamma} = (\forall x \in R_\gamma)(\psi(f, x, x_1, \ldots, x_n))$.

L'hypothèse de récurrence permet d'écrire

$$(\forall a, a_1, \ldots, a_n \in R_\gamma)(\psi^{R_\gamma}(j, a, a_1, \ldots, a_n) \Leftrightarrow \psi^{R_\gamma}(j', a, a_1, \ldots, a_n)),$$

ce qui implique

$$(\forall a_1, \ldots, a_n \in R_\gamma)((\forall a \in R_\gamma)\psi^{R_\gamma}(j, a, a_1, \ldots, a_n) \Leftrightarrow (\forall a \in R_\gamma)\psi^{R_\gamma}(j', a, a_1, \ldots, a_n)).$$

□

Ainsi, si on considère un plongement élémentaire comme il se doit, c'est-à-dire comme un objet appartenant à la logique, la seule équivalence raisonnable est celle de la conclusion du thèorème ci-dessus, qui est justement la $\gamma$-équivalence '$\overset{\gamma}{=}$'.

# 5 Un erratum

Dans la mesure où le travail préparatoire pour ce mémoire consistait pour une part importante à lire une partie de [Deh00], nous avons eu l'occasion de repérer une erreur dans la preuve du lemme 4.17 du chapitre XII ; en voici une version corrigée où l'on modifie légèrement l'hypothèse de récurrence.

**Lemme 5.1** (Avec les notations habituelles)**.** *Pour tout p, si m est le plus grand entier tel que $2^m|p$ (que l'on notera m(p) dans la preuve), on a :*

$$\mathrm{crit}(j_{[p]}) = \mathrm{crit}_m(j).$$

**Preuve**. On procède par récurrence sur $n \geq 0$ pour montrer :

$$P(n) : \begin{cases} \mathrm{crit}(j_{[2^n]}) \geq \mathrm{crit}_n(j), \\ \forall p < 2^n,\ \mathrm{crit}(j_{[p]}) = \mathrm{crit}(j_{[2^{m(p)}]}), \\ \text{la fonction } [|n|] \to Ord, k \mapsto \mathrm{crit}(j_{[2^k]}) \text{ est strictement croissante.} \end{cases}$$

D'abord, $P(0)$ est équivalent à $\mathrm{crit}(j) = \mathrm{crit}_0(j)$.

Ensuite, supposons $P(n)$. Fixons $1 \leq p \leq n$. Les deux dernières énoncés de celle-ci assurent que :

$$\forall l < 2^n, \mathrm{crit}(j_{[l]}) < \mathrm{crit}(j_{[2^n]}).$$

Avec le premier, on est dans les conditions d'application du lemme 4.8(ii) avec $j_0 = j_{[2^n]}$, $j_1 = \ldots = j_p = j$, on obtient :

$$\mathrm{crit}(j_{[2^n+p]}) = j_{[2^n]}(\mathrm{crit}(j_{[p]}).$$

Pour $p < 2^n$, les inégalités précédentes montrent que l'ordinal critique de $j_{[2^n]})$ est supérieur à $\mathrm{crit}(j_{[p]})$, d'où la seconde partie de $P(n+1)$ :

$$\mathrm{crit}(j_{[2^n+p]}) = \mathrm{crit}(j_{[p]}) = \mathrm{crit}_{m(p)} = \mathrm{crit}_{m(2^n+p)}\,.$$

Pour $p = 2^n$, on obtient les deux énoncés restants de P(n+1) :

$$\mathrm{crit}(j_{[2^{n+1}]}) = j_{[2^n]}(\mathrm{crit}(j_{[2^n]})) > \mathrm{crit}(j_{[2^n]}) \leq \mathrm{crit}_n(j).$$

Donc on a établi $P(n+1)$.

À partir de $P(n)$, on en déduit que les valeurs prises par la suite des ordinaux critiques des puissances à gauche de $j$ sont les ordinaux critiques des puissances à gauche d'indice une puissance de 2, qui sont eux-mêmes les valeurs prises par

une suite extraite de $(\mathrm{crit}_m)$. Or le lemme 4.15 montre que toutes les valeurs de cette dernière suite sont atteintes par la première, donc la seule possibilité est :

$$\mathrm{crit}(j_{[2^n]}) = \mathrm{crit}_n(j)$$

ce qui conclut la preuve. □

# 6 Preuve de la borne de Kunen

Dans cette section, on présente une preuve due à Woodin de la borne de Kunen différente de la preuve de [Deh00], qui est exposée dans [Kan94]. Elle repose sur la théorie des ensembles stationnaires. On rappelle le résultat suivant

**Lemme 6.1.** *Soit $\lambda > \omega$ un cardinal régulier, $S \subseteq \lambda$ stationnaire. Si $\nu < \lambda$ est régulier et $S \subseteq \{\xi < \lambda | \mathrm{cf}(\xi) = \nu\}$, alors $S$ rencontre tout ensemble $\nu$-clos cofinal.*

La preuve de Woodin repose sur le lemme combinatoire suivant, dû à Solovay :

**Lemme 6.2.** *Soit $\kappa$ un cardinal régulier non dénombrable, $X \subseteq \kappa$ stationnaire. Alors $X$ peut être partitionné en $\kappa$ ensembles stationnaires.*

On admet ce résultat (la preuve n'ayant rien à voir avec la théorie des grands cardinaux, donc hors de propos ici, cf [Jec78] théorème 85).

**Preuve**. On procède par l'absurde en supposant que l'on ait un plongement élémentaire $j : V_{\delta+2} \to V_{\delta+2}$. Notons $\kappa$ son ordinal critique, et $\lambda = \sup j^n(\kappa) \leq \delta$. Par restriction, comme $j(\lambda) = \lambda$, on peut supposer $\delta = \lambda$ pour simplifier.

D'après le lemme de Solovay, on peut trouver une fonction injective $S : \kappa \to \mathcal{P}(\lambda^+)$ telle que l'image de $S$ est une partition de $\{\xi < \lambda^+ | \mathrm{cf}(\xi) = \omega\}$ (qui est de cardinalité $\lambda^+ > \kappa$) en ensembles stationnaires.

Le point clé est que $S$ est codable dans $V_{\lambda+2}$, donc peut se voir appliquer $j$. Pour le voir il suffit comme $\kappa < \lambda$ de vérifier que toute partie $X$ de $\lambda^+$ peut être codée dans $V_{\lambda+2}$. Or on a le mécanisme suivant. Si $R$ est un bon ordre de $\lambda$, notons $\alpha_R$ son type d'ordre (qui est un ordinal plus petit que $\lambda^+$) et $e_R$ l'isomorphisme entre $(\alpha_R, <)$ et $(\lambda, R)$ (en particulier, on utilise l'axiome du choix). Fixons une bijection $p : (\lambda \times \lambda) \times \lambda \to \lambda$, qui est dans $V_\lambda$. Alors :

**Lemme 6.3.**

$$X \subseteq \lambda^+ \mapsto f(X) = \{p(R \times e_R(X \cap \alpha_R)) | R \text{ bon ordre de } \lambda\} \in V_{\lambda+2}$$

*est injective (et peut ainsi servir pour coder $X$).*

*Preuve.* Il est facile de voir que $f(X)$ est défini et appartient à $V_{\lambda+2}$. Supposons $X \neq Y$. Alors il existe $\alpha$ ordinal inférieur à $\lambda^+$, $X \cap \alpha \neq Y \cap \alpha$. On prend alors un bon ordre sur $\lambda$ dont c'est le type d'ordre ; c'est possible car le cardinal de $\alpha$ est un cardinal inférieur à $\lambda^+$, donc inférieur ou égal à $\lambda$. ■

Dans la suite de la preuve, on identifie les ensembles et leurs codes ; l'important est qu'il existe une formule du premier ordre reliant les deux approches. Par élémentarité, comme $j(\lambda) = \lambda$, on a $j(\lambda^+) = \lambda^+$, et $j(S) : j(\kappa) \mapsto \mathcal{P}(\lambda^+)$ vérifie :

$$j(S)(\kappa) \subseteq \{\xi < \lambda^+ \operatorname{cf}(\xi) = \omega\} \text{ est stationnaire dans } \lambda^+$$

Comme l'union de $< \lambda^+$ ensembles non-stationnaires n'est pas stationnaire, il existe $\alpha_0 < \kappa$ avec $j(S)(\kappa) \cap S(\alpha_0)$ stationnaire dans $\lambda^+$. Or

$$C = \{\xi < \lambda^+ | j(\xi) = \xi \text{ et } \operatorname{cf}(\xi) = \omega\}$$

est $\omega$-clos et cofinal dans $\lambda^+$, donc (d'après le résultat rappelé précédemment) rencontre non-trivialement ce dernier. Soit $\xi_0$ dans l'intersection ; $\xi_0 = j(\xi_0) \in j(S(\alpha_0)) = j(S)(\alpha_0)$, donc $\xi_0 \in j(S)(\alpha_0) \cap j(S)(\kappa)$, ce qui contredit le fait que $j(S)$, comme $S$, envoie des éléments distincts sur des parties disjointes. □

Cette preuve montre également que si $V$ est un modèle de ZFC, il ne peut exister de plongement élémentaire non-trivial de $V$ dans $V$ (résultat original de Kunen). Dans cette perspective, la borne de Kunen montre que l'existence d'une tel plongement n'est pas un axiome de grand cardinal consistant, et a amené au sujet qui nous intéresse à savoir l'étude de tels plongements sur des rangs. Un autre point important est que le codage de $S$ dans $V_{\lambda+2}$ utilise l'axiome du choix, et on ne connaît pas de preuve qui s'en dispense.

## Annexe : premières tables de Laver

| $A_0$ | 1 |
|---|---|
| 1 | 1 |

| $A_1$ | 1 | 2 |
|---|---|---|
| 1 | 2 | 2 |
| 2 | 1 | 2 |

| $A_2$ | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| 1 | 2 | 4 | 2 | 4 |
| 2 | 3 | 4 | 3 | 4 |
| 3 | 4 | 4 | 4 | 4 |
| 4 | 1 | 2 | 3 | 4 |

| $A_3$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 4 | 6 | 8 | 2 | 4 | 6 | 8 |
| 2 | 3 | 4 | 7 | 8 | 3 | 4 | 7 | 8 |
| 3 | 4 | 8 | 4 | 8 | 4 | 8 | 4 | 8 |
| 4 | 5 | 6 | 7 | 8 | 5 | 6 | 7 | 8 |
| 5 | 6 | 8 | 6 | 8 | 6 | 8 | 6 | 8 |
| 6 | 7 | 8 | 7 | 8 | 7 | 8 | 7 | 8 |
| 7 | 8 | 8 | 8 | 8 | 8 | 8 | 8 | 8 |
| 8 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |

| $A_4$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 12 | 14 | 16 | 2 | 12 | 14 | 16 | 2 | 12 | 14 | 16 | 2 | 12 | 14 | 16 |
| 2 | 3 | 12 | 15 | 16 | 3 | 12 | 15 | 16 | 3 | 12 | 15 | 16 | 3 | 12 | 15 | 16 |
| 3 | 4 | 8 | 12 | 16 | 4 | 8 | 12 | 16 | 4 | 8 | 12 | 16 | 4 | 8 | 12 | 16 |
| 4 | 5 | 6 | 7 | 8 | 13 | 14 | 15 | 16 | 5 | 6 | 7 | 8 | 13 | 14 | 15 | 16 |
| 5 | 6 | 8 | 14 | 16 | 6 | 8 | 14 | 16 | 6 | 8 | 14 | 16 | 6 | 8 | 14 | 16 |
| 6 | 7 | 8 | 15 | 16 | 7 | 8 | 15 | 16 | 7 | 8 | 15 | 16 | 7 | 8 | 15 | 16 |
| 7 | 8 | 16 | 8 | 16 | 8 | 16 | 8 | 16 | 8 | 16 | 8 | 16 | 8 | 16 | 8 | 16 |
| 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| 9 | 10 | 12 | 14 | 16 | 10 | 12 | 14 | 16 | 10 | 12 | 14 | 16 | 10 | 12 | 14 | 16 |
| 10 | 11 | 12 | 15 | 16 | 11 | 12 | 15 | 16 | 11 | 12 | 15 | 16 | 11 | 12 | 15 | 16 |
| 11 | 12 | 16 | 12 | 16 | 12 | 16 | 12 | 16 | 12 | 16 | 12 | 16 | 12 | 16 | 12 | 16 |
| 12 | 13 | 14 | 15 | 16 | 13 | 14 | 15 | 16 | 13 | 14 | 15 | 16 | 13 | 14 | 15 | 16 |
| 13 | 14 | 16 | 14 | 16 | 14 | 16 | 14 | 16 | 14 | 16 | 14 | 16 | 14 | 16 | 14 | 16 |
| 14 | 15 | 16 | 15 | 16 | 15 | 16 | 15 | 16 | 15 | 16 | 15 | 16 | 15 | 16 | 15 | 16 |
| 15 | 16 | 16 | 16 | 16 | 16 | 16 | 16 | 16 | 16 | 16 | 16 | 16 | 16 | 16 | 16 | 16 |
| 16 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |

## Références


[Deh00] Patrick Dehornoy. *Braids and Self-Distributivity*. Progress in mathematics. Birkhaüser, 2000.

[Jec78] Thomas Jech. *Set Theory*. Academic Press, 1978.

[Kan94] Akihiro Kanamori. *The Higher Infinite*. Perspectives in Mathematical Logic. Springer-Verlag, 1994.