Chapitre XIV

Les grands cardinaux (II)

Ce chapitre est une suite directe du précédent. On y explore la partie supérieure de la hiérarchie des grands cardinaux, où la notion de plongement élémentaire d'un modèle de ZFC dans un (autre) modèle joue un rôle prépondérant. On introduit quelques-unes des très nombreuses notions de grand cardinaux considérées à ce jour, avec, à nouveau, le but principal de comparer ces notions entre elles et d'établir le résultat, *a priori* étonnant, qu'elles s'ordonnent en une hiérarchie totalement ordonnée. Un développement particulier est consacré aux cardinaux et aux tables de Laver, qui mènent à des applications de la théorie des ensembles d'un type nouveau.

> ▷ *Les tables de Laver sont des structures algébriques finies à 2^n éléments, construites par une définition inductive simple, et formant lorsque n varie un système projectif. Le point étonnant, et même paradoxal, est que certaines propriétés combinatoires de ces tables n'ont été établies pour le moment qu'en utilisant comme hypothèse l'existence de ce qui va être appelé un cardinal de Laver, une des notions extrêmes de la hiérarchie des grands cardinaux. Jusqu'à preuve du contraire, et même si des applications potentielles en théorie des nœuds peuvent être espérées, les tables de Laver sont des objets mathématiques assez marginaux, et les résultats mentionnés ici sont plutôt mineurs. En revanche, ce qui rend ces objets fascinants est l'existence du lien avec les plongements élémentaires, et le fait que des axiomes de grands cardinaux extrêmement éloignés des mathématiques usuelles puissent permettre d'établir des propriétés simples d'objets finis.* ◁

Le chapitre comporte trois sections. Dans la section 1, on décrit plusieurs types de cardinaux définis par l'existence de plongements élémentaires de $\boldsymbol{V}$, ou d'un sous-ensemble V_α, vers un modèle intérieur soumis à des conditions de clôture de plus en plus fortes : apparaissent successivement les cardinaux forts, les cardinaux de Woodin, et les cardinaux supercompacts. Dans la section 2, on montre que l'existence d'un plongement élémentaire de l'univers dans lui-même est une borne inatteignable, dite borne de Kunen, et on introduit les cardinaux de Laver comme une des dernières notions compatibles avec la borne de Kunen. On montre alors qu'un cardinal de Laver donne naissance à une structure algébrique obéissant à la loi d'autodistributivité. Dans la section 3, on présente les tables de Laver et on montre comment les propriétés des itérations de plongements élémentaires liés à un cardinal de Laver mènent à des résultats sur les périodes des lignes de ces tables.

Sources et compléments. *Comme pour le chapitre* XIII*, une source classique sur le sujet est le livre* [59] *d'A. Kanamori, où se trouve une multitude de résultats au-delà de ceux présentés ici dans les sections* 1 *et* 2*. Pour les tables de Laver, les articles originaux* [75, 76] *ne sont pas aisés, et la présentation de* [16] *est imparfaite, c'est pourquoi on a inclus ici des arguments complets.*

1. Les « grands » grands cardinaux

La hiérarchie des grands cardinaux continue au-delà des cardinaux mesurables, avec une suite de notions de plus en plus fortes. Le point commun de tous les « grands » grands cardinaux est d'être définis par l'existence de plongements élémentaires de plus en plus contraints.

▷ *Un ensemble A est infini s'il existe une injection non surjective ϕ de A dans A, ce qui est un principe d'auto-similarité : $\phi[A]$ est une copie de A, qui est pourtant une partie propre de A. Par exemple, l'ensemble $\mathbb{N}$ (alias ω) est infini car le décalage $\phi : n \mapsto n+1$ est une injection non surjective de $\mathbb{N}$ dans lui-même. La notion de plongement élémentaire non trivial renforce la même idée : à nouveau, on requiert que la partie soit semblable au tout, mais on exige de plus que la similitude préserve une structure additionnelle. Par exemple, alors qu'il existe une injection non surjective de $\mathbb{N}$ dans lui-même, il ne peut exister de plongement élémentaire ϕ non trivial (c'est-à-dire non surjectif) de $(\mathbb{N}, <)$ dans lui-même : 0 étant défini comme le plus petit élément de $(\mathbb{N}, <)$, on doit avoir $\phi(0) = 0$, puis $\phi(1) = 1$ car 1 est le plus petit élément de $(\mathbb{N}, <)$ qui n'est pas 0, etc. C'est essentiellement l'argument qui, élaboré comme en* XIII.2.3.10*, établit que l'ordinal critique d'un plongement élémentaire de $\boldsymbol{V}$ dans un modèle intérieur est Π^2_1-indescriptible.* ◁

On mentionne ici plusieurs nouvelles notions de grands cardinaux : cardinaux forts, cardinaux de Woodin, cardinaux extensibles, cardinaux supercompacts, et on compare ces notions les unes aux autres. Comme on le verra dans les chapitres XV et XVI, les cardinaux de Woodin et les cardinaux supercompacts jouent un rôle critique dans les résultats à ce jour, et c'est pour cela que l'accent est mis sur ces notions ici.

Cette section est structurée en trois sous-sections. Dans la sous-section 1.1, on établit quelques propriétés générales des plongements élémentaires de modèles de ZFC. Dans la sous-section 1.2, on introduit les cardinaux forts et les cardinaux de Woodin, définis par des conditions de clôture du modèle-but des plongements élémentaires, et approximables par des extendeurs. Dans la sous-section 1.3, on introduit de même les cardinaux supercompacts et on les compare aux cardinaux de Woodin.

1.1. Plongements élémentaires

▶ Résumé.— Sous des hypothèses faibles, l'ordinal critique d'un plongement élémentaire est un cardinal mesurable. ◀

1.1.1.— On commence ici par quelques généralités sur les plongements élémentaires, avant d'établir la réciproque de XIII.2.3.4.

On rappelle que, si M est un ensemble ou une classe transitif et que l'on parle de la structure ou du modèle M, on suppose toujours que la relation d'appartenance considérée est la restriction de $\in$ à M. Par ailleurs, toutes les classes considérées sont supposées être des classes pour le modèle de référence $\boldsymbol{V}$; c'est en particulier le cas pour les plongements élémentaires $\boldsymbol{j}$ de $\boldsymbol{V}$ dans un modèle intérieur, ce qui signifie qu'il est supposé légitime d'utiliser $\boldsymbol{j}$ dans des définitions par séparation ou remplacement.

1.1.2. Lemme.— *Si $\boldsymbol{j}$ est un plongement élémentaire de $\boldsymbol{V}$ dans un modèle intérieur $\boldsymbol{M}$, alors, pour tout α, la restriction $\boldsymbol{j}\restriction V_\alpha$ est un plongement élémentaire de V_α dans $V^{\boldsymbol{M}}_{\boldsymbol{j}(\alpha)}$.*

Démonstration. L'hypothèse que $\boldsymbol{j}$ est une classe pour $\boldsymbol{V}$ implique que, pour tout α, la restriction de $\boldsymbol{j}$ à V_α est un ensemble, élément de $\boldsymbol{V}$. Par élémentarité, $\boldsymbol{V} \models x \in V_\alpha$ entraîne $\boldsymbol{M} \models \boldsymbol{j}(x) \in V_{\boldsymbol{j}(\alpha)}$, soit $\boldsymbol{j}(x) \in V^{\boldsymbol{M}}_{\boldsymbol{j}(\alpha)}$. Si $\Phi(\vec{x})$ est une formule ensembliste et que $\vec{a}$ est une famille d'éléments de V_α, alors $(V_\alpha, \in) \models \Phi(\vec{a})$ est vraie si, et seulement si, $(\boldsymbol{V}, \in) \models \Phi^{V_\alpha}(\vec{a})$ l'est, où Φ^{V_α} est la relativisation de Φ dans laquelle chaque quantification Qx est remplacée par $Qx{\in}V_\alpha$. Par élémentarité, cette formule équivaut à $\Phi^{V_{\boldsymbol{j}(\alpha)}}(\boldsymbol{j}(\vec{a}))$, donc, étant donné que $\boldsymbol{M}$ est modèle intérieur de $\boldsymbol{V}$, à $(V^{\boldsymbol{M}}_{\boldsymbol{j}(\alpha)}, \in) \models \Phi(\boldsymbol{j}(\vec{a}))$. Par conséquent, $\boldsymbol{j}$ est un plongement élémentaire de $(V_\alpha, \in)$ dans $(V^{\boldsymbol{M}}_{\boldsymbol{j}(\alpha)}, \in)$. □

1.1.3. Lemme.— *Supposons que $\boldsymbol{M}, \boldsymbol{N}$ sont des modèles intérieurs de $\boldsymbol{V}$ et que j est un plongement élémentaire de $V^{\boldsymbol{M}}_\alpha$ dans $V^{\boldsymbol{N}}_\beta$.*

(i) *Si ξ est un ordinal $<\alpha$, alors $j(\xi)$ est un ordinal vérifiant $\xi \leqslant j(\xi) < \beta$. De plus, $\xi < \eta$ entraîne $j(\xi) < j(\eta)$.*

(ii) *Si x appartient à $V^{\boldsymbol{M}}_\xi$ avec $\xi < \alpha$, alors $j(x)$ appartient à $V^{\boldsymbol{N}}_{j(\xi)}$ et on a $\mathrm{rg}(j(x)) = j(\mathrm{rg}(x))$.*

(iii) *Si $j\restriction\theta$ est l'identité, alors $j\restriction V_\theta$ est l'identité.*

(iv) *Si j n'est pas l'identité, il existe un ordinal $<\alpha$ non invariant par j.*

Démonstration. (i) Supposons $\xi < \alpha$. Comme $V^{\boldsymbol{M}}_\alpha$ est transitif, $(V^{\boldsymbol{M}}_\alpha, \in)$ satisfait $\mathbf{Ord}(\xi)$. Par élémentarité de j, on déduit $(V^{\boldsymbol{N}}_\beta, \in) \models \mathbf{Ord}(j(\xi))$. Comme $V^{\boldsymbol{N}}_\beta$ est transitif dans $\boldsymbol{N}$, on déduit que $j(\xi)$ est un ordinal dans $\boldsymbol{N}$, donc dans $\boldsymbol{V}$ dont $\boldsymbol{N}$ est modèle intérieur, et aussi qu'il satisfait $j(\xi) < \beta$. Par élémentarité, $\xi < \eta < \alpha$, c'est-à-dire $\xi \in \eta \in \alpha$, entraîne $j(\xi) \in j(\eta)$, soit $j(\xi) < j(\eta)$. Donc, $j\restriction\alpha$ est une injection strictement croissante de α dans β. Par II.1.2.3, on déduit $\xi \leqslant j(\xi)$ pour tout ξ dans $\mathrm{Dom}(j)$.

(ii) Comme ci-dessus, $x \in V^{\boldsymbol{M}}_\xi$ entraîne $(V^{\boldsymbol{M}}_\alpha, \in) \models x \in V_\xi$ puisque $V_\xi^{V^{\boldsymbol{M}}_\alpha}$ est $V^{\boldsymbol{M}}_\xi$, qui, par élémentarité de j, équivaut à $(V^{\boldsymbol{N}}_\beta, \in) \models j(x) \in V_{j(\xi)}$, donc à $j(x) \in V^{\boldsymbol{N}}_{j(\xi)}$, qui implique $j(x) \in V_{j(\xi)}$ puisque $\boldsymbol{N}$ est modèle intérieur de $\boldsymbol{V}$. Soit ξ le rang de x. Alors, $\forall\eta{<}\xi\,(x \notin V_\eta)$ entraîne $\forall\eta{<}j(\xi)\,(j(x) \notin V_\eta)$, d'où $j(\xi) = \mathrm{rg}(j(x))$.

(iii) Soit x un élément non invariant par j de rang minimal. Comme on a $j(\emptyset) = \emptyset$, on a $x \neq \emptyset$, et donc le rang de x est de la forme $\xi + 1$. Alors, $y \in V_\xi$ entraîne $\mathrm{rg}(y) \leqslant \xi$ donc, par construction, $j(y) = y$ et, de là, $y \in x \Leftrightarrow y \in j(x)$. On a donc $j(x) \cap V_\xi = x \cap V_\xi = x$. D'un autre côté, $x \subseteq V_\xi$ entraîne $j(x) \subseteq V_{j(\xi)}$, et, de là $j(x) = j(x) \cap V_{j(\xi)}$. Par conséquent, $x \neq j(x)$ requiert $j(x) \cap V_\xi \neq j(x) \cap V_{j(\xi)}$, donc $V_\xi \neq V_{j(\xi)}$, et de là $\xi \neq j(\xi)$. Par contraposition, $j{\restriction}\theta = \mathrm{id}$ entraîne $j{\restriction}V_\theta = \mathrm{id}$.

Enfin, pour (iv), on applique (iii) avec $\theta := \alpha$. □

Par 1.1.2, les résultats de 1.1.3 restent valables pour $\alpha = \beta = \infty$, c'est-à-dire dans le cas d'un plongement élémentaire de l'intégralité de $\boldsymbol{M}$ dans $\boldsymbol{N}$.

1.1.4. Définition (ordinal critique).— Si $\boldsymbol{M}, \boldsymbol{N}$ sont modèles intérieurs et si j est un plongement élémentaire non trivial de $V_\alpha^{\boldsymbol{M}}$ dans $V_\beta^{\boldsymbol{N}}$, l'*ordinal critique* $\mathrm{cr}(j)$ de j est le plus petit ordinal non invariant par j.

Exemple. Si κ est un cardinal mesurable et si $\boldsymbol{j}$ est le plongement élémentaire associé à une ultrapuissance par un ultrafiltre κ-complet sur κ, alors, par XIII.2.3.7, *l'ordinal critique de $\boldsymbol{j}$ est κ.*

1.1.5.— Des hypothèses très faibles impliquent que l'ordinal critique d'un plongement élémentaire non trivial est nécessairement un cardinal mesurable dans le modèle source.

Lemme.— *Supposons que $\boldsymbol{M}, \boldsymbol{N}$ sont des modèles intérieurs, que j est un plongement élémentaire non trivial de $V_\alpha^{\boldsymbol{M}}$ dans $V_\beta^{\boldsymbol{N}}$ d'ordinal critique κ, et que $j{\restriction}\mathfrak{P}^{\boldsymbol{M}}(\kappa)$ appartient à $\boldsymbol{M}$. Soit*

$$U := \{X \in \mathfrak{P}^{\boldsymbol{M}}(\kappa) \mid \kappa \in j(X)\}. \qquad (\#1)$$

Alors, U est, dans $\boldsymbol{M}$, un ultrafiltre normal sur κ, et κ est un cardinal mesurable dans $\boldsymbol{M}$. De plus, j se factorise par le plongement élémentaire canonique de $V_\alpha^{\boldsymbol{M}}$ dans son ultrapuissance par U.

Démonstration. D'abord (#1) fait sens puisque, si X est inclus dans κ et appartient à $\boldsymbol{M}$, alors X appartient à $V_{\kappa+1}^{\boldsymbol{M}}$, donc à $V_\alpha^{\boldsymbol{M}}$ et, par hypothèse, $j(X)$ est défini et c'est un élément de $\mathfrak{P}^{\boldsymbol{N}}(j(\kappa))$. L'hypothèse $j{\restriction}\mathfrak{P}^{\boldsymbol{M}}(\kappa) \in \boldsymbol{M}$ entraîne $U \in \boldsymbol{M}$, puisqu'alors (#1) est une définition par compréhension légitime dans $\boldsymbol{M}$.

Comme $\emptyset$ est définissable dans $(V_\alpha^{\boldsymbol{M}}, \in)$, on a $j(\emptyset) = \emptyset$, d'où $\kappa \notin \emptyset$, et $\emptyset \notin U$. Ensuite, $X \subseteq X'$ entraîne $j(X) \subseteq j(X')$, et alors $\kappa \in j(X)$ entraîne $\kappa \in j(X')$. De là, $X \in U$ entraîne $X' \in U$.

Supposons maintenant $\lambda < \kappa$ et que $(X_\xi)_{\xi<\lambda}$ est une suite d'éléments de U appartenant à $\boldsymbol{M}$. On a donc $\kappa \in j(X_\xi)$ pour chaque ξ. L'image par j de la suite $(X_\xi)_{\xi<\lambda}$ est une suite de longueur $j(\lambda)$, qui est λ puisque κ est le plus petit ordinal bougé par j. Pour chaque ξ, le $j(\xi)^{\text{ième}}$ élément de cette suite est l'image par j du $\xi^{\text{ième}}$ élément de la suite $(X_\xi)_{\xi<\lambda}$, qui est $j(X_\xi)$. Comme on a $j(\xi) = \xi$, on déduit que l'image par j de la suite $(X_\xi)_{\xi<\lambda}$ est la suite $(j(X_\xi))_{\xi<\lambda}$. On déduit que l'intersection des ensembles $j(X_\xi)$ est l'image par j de l'intersection des ensembles X_ξ.

On a alors
$$\kappa \in \bigcap_{\xi<\lambda} j(X_\xi) = j(\bigcap_{\xi<\lambda} X_\xi),$$
d'où $\bigcap_{\xi<\lambda} X_\xi \in U$. Par conséquent U est, dans $\boldsymbol{M}$, un ultrafiltre κ-complet sur κ.

Finalement, supposons $\xi < \kappa$. On a $j(\{\xi\}) = \{j(\xi)\} = \{\xi\}$, donc $\kappa \notin j(\{\xi\})$, soit $\{\xi\} \notin U$. Donc, U est non principal, et κ est un cardinal mesurable dans $\boldsymbol{M}$.

Pour la normalité, supposons $[f]_U < [\mathrm{id}_\kappa]_U$, soit $\{\xi < \kappa \mid f(\xi) < \xi\} \in U$. Par (#1), on a donc $\kappa \in j(\{\xi \mid f(\xi) < \xi\})$, soit $j(f)(\kappa) < \kappa$. Il existe donc $\theta < \kappa$ vérifiant $j(f)(\kappa) = \theta = j(\theta)$. On déduit $\kappa \in j(\{\xi < \kappa \mid f(\xi) = \theta\})$, d'où
$$\{\xi < \kappa \mid f(\xi) = \theta\} \in U,$$
et $[f]_U = \theta < \kappa$. Par XIII.2.3.7, on conclut que U est normal.

La normalité de U entraîne que, pour toute fonction f de κ dans $V_\alpha^{\boldsymbol{M}}$, on a l'égalité $[f]_U = j_U(f)(\kappa)$, où j_U est le plongement canonique dans l'ultrapuissance Ult_U. Ensuite, une égalité $[f]_U = [g]_U$ implique $\{\xi < \kappa \mid f(\xi) = g(\xi)\} \in U$, d'où la relation $\kappa \in j(\{\xi < \kappa \mid f(\xi) = g(\xi)\})$, soit $j_U(f)(\kappa) = j_U(g)(\kappa)$. Par conséquent, l'application $k : [f]_U \mapsto j_U(f)(\kappa)$ est bien définie. Par le théorème de Łoś et l'hypothèse que j est élémentaire, k est un plongement élémentaire de Ult_U dans $V_\beta^{\boldsymbol{N}}$, et, par construction, on a $j = k \circ j_U$: en effet, pour tout x dans $V_\alpha^{\boldsymbol{M}}$, l'élément $j_U(x)$ est égal à $[c_x]_U$, où c_x est la fonction constante de valeur x, et on déduit $k(j_U(x)) = j(c_x)(\kappa) = j(x)$, puisque $j(c_x)$ est constante de valeur $j(x)$. □

▷ *Toutes les hypothèses de* 1.1.5 *sont utilisées dans la démonstration : si la restriction de $\boldsymbol{j}$ à $\mathfrak{P}(\kappa)^{\boldsymbol{M}}$ n'est pas supposée appartenir à $\boldsymbol{M}$, alors U n'a aucune raison d'appartenir à $\boldsymbol{M}$ et l'argument avorte. La définition de U est toujours légitime dans $\boldsymbol{V}$ mais, dans $\boldsymbol{V}$, il n'y a aucune raison pour que U soit κ-complet puisqu'il peut exister des suites de sous-ensembles de κ qui sont dans $\boldsymbol{V}$ mais pas dans $\boldsymbol{M}$, et donc auxquelles j ne s'applique pas. Par exemple, on peut montrer que l'existence de $0^\sharp$, c'est-à-dire d'un plongement élémentaire de $\boldsymbol{L}$ dans $\boldsymbol{L}$ (sous-section* XIII.3.2) *n'entraîne pas celle d'un cardinal mesurable.* ◁

1.1.6.— Par XIII.2.3.7, l'hypothèse que κ est un cardinal mesurable implique l'existence d'un plongement élémentaire $\boldsymbol{j}$ de l'univers $\boldsymbol{V}$ dans un modèle intérieur $\boldsymbol{M}$ dont l'ordinal critique est κ. On déduit facilement des lemmes précédents que cette implication est une équivalence.

Proposition (mesurable *vs.* plongement).— *Pour tout cardinal κ, il y a équivalence entre*
(i) *Le cardinal κ est mesurable ;*
(ii) *Il existe un plongement élémentaire $\boldsymbol{j}$ de $\boldsymbol{V}$ dans un modèle intérieur $\boldsymbol{M}$ vérifiant* $\mathrm{cr}(\boldsymbol{j}) = \kappa$.

Démonstration. L'implication (i)⇒(ii) a été établie dans XIII.2.3.7.

Réciproquement, supposons que $\boldsymbol{j}$ est un plongement élémentaire de $\boldsymbol{V}$ dans un modèle intérieur $\boldsymbol{M}$. Soit $\kappa := \mathrm{cr}(\boldsymbol{j})$, et $j := \boldsymbol{j}{\restriction}V_{\kappa+2}$. Par 1.1.2, j est un plongement élémentaire de $V_{\kappa+2}$ dans $V_{\boldsymbol{j}(\kappa)+2} \cap \boldsymbol{M}$, et, puisque $\boldsymbol{j}$ est une classe pour $\boldsymbol{V}$, par remplacement, sa restriction j est dans $\boldsymbol{V}$, de même que $j{\restriction}\mathfrak{P}^{\boldsymbol{M}}(\kappa)$ Alors, 1.1.5 implique que κ est mesurable dans $\boldsymbol{V}$. □

1.1.7.— Si, dans 1.1.6, partant d'un ultrafiltre κ-complet U sur κ, on déduit un plongement élémentaire $\boldsymbol{j}_U$, dont on dérive un ultrafiltre U' par (#1), il n'y a pas de raison pour que U' coïncide avec U en général : l'ultrafiltre donné par (#1) est toujours normal, et les correspondances sont réciproques l'une de l'autre si, et seulement si, U est normal. Noter que l'on obtient ainsi une nouvelle démonstration de XIII.2.1.7.

1.2. Les cardinaux forts et les cardinaux de Woodin

▶ Résumé.— Définis par l'existence d'extendeurs convenables, les cardinaux forts et de Woodin surpassent les cardinaux mesurables. ◀

1.2.1.— L'existence d'un plongement élémentaire de $\boldsymbol{V}$ dans un modèle intérieur $\boldsymbol{M}$ équivaut à celle d'un cardinal mesurable, et c'est donc un axiome de grand cardinal, non prouvable dans ZFC. Le principe supplémentaire se dégageant de la suite est qu'exiger que le modèle d'arrivée $\boldsymbol{M}$ soit de plus en plus proche du modèle de départ $\boldsymbol{V}$ correspond à des grands cardinaux de plus en plus grands, donc à des axiomes de plus en plus forts.

▷ *L'existence d'un plongement élémentaire $\boldsymbol{j}$ de $\boldsymbol{V}$ dans un modèle intérieur $\boldsymbol{M}$ implique une similitude parfaite entre $\boldsymbol{M}$ et $\boldsymbol{V}$, puisqu'elle implique la préservation de* toutes *les notions définissables à partir de $\in$, donc virtuellement de toutes les notions mathématiques, alors que le plongement n'est pas l'identité : c'est donc, dans la lignée de l'axiome d'infini qui affirme l'existence d'un ensemble si grand qu'une de ses parties est aussi grande que le tout, une hypothèse sur la taille de l'ensemble, si grand qu'il reste toujours un espace pour loger de nouveaux éléments à côté d'une copie du tout. Dans cette situation, on pourrait s'attendre à ce qu'il soit plus facile que $\boldsymbol{M}$ soit proche de $\boldsymbol{V}$, et donc qu'exiger plus de distance entre $\boldsymbol{V}$ et $\boldsymbol{M}$ corresponde à un axiome plus fort : cette intuition est trompeuse, et on va voir qu'au contraire c'est exiger que $\boldsymbol{M}$ soit proche de $\boldsymbol{V}$ qui correspond aux axiomes les plus forts. Ce fait n'est pas étonnant car, l'hypothèse que $\boldsymbol{j}$ n'est pas l'identité implique que l'image de $\boldsymbol{j}$ ne peut être l'intégralité de $\boldsymbol{M}$ et, de là, plus $\boldsymbol{M}$ est proche de $\boldsymbol{V}$, moins il reste de place pour $\boldsymbol{M} \setminus \mathrm{Im}(\boldsymbol{j})$.* ◁

1.2.2.— Dans toute la suite, on écrit « $\boldsymbol{j} : \boldsymbol{V} \xrightarrow{\preceq} \boldsymbol{M}$ » pour « $\boldsymbol{j}$ est un plongement élémentaire non trivial de $\boldsymbol{V}$ dans un modèle intérieur $\boldsymbol{M}$ ». La première notion introduite ici est celle de cardinal *fort*.

Définition (cardinal fort).— Un cardinal κ est dit *γ-fort* s'il existe un plongement $\boldsymbol{j} : \boldsymbol{V} \xrightarrow{\preceq} \boldsymbol{M}$ vérifiant $\mathrm{cr}(\boldsymbol{j}) = \kappa$ et $V_{\kappa+\gamma} \subseteq \boldsymbol{M}$. Un cardinal est *fort* s'il est γ-fort pour tout γ.

▷ *La condition $\boldsymbol{j}(\kappa) > \kappa + \gamma$ est parfois ajoutée dans la définition d'un cardinal γ-fort, mais l'omettre ne change pas la notion car une itération de $\boldsymbol{j}$ permet de monter la valeur de $\boldsymbol{j}(\kappa)$ arbitrairement. Eu égard à* 1.1.6, *quel que soit γ, un cardinal γ-fort est mesurable, puisque la mesurabilité de κ équivaut à l'existence d'un plongement élémentaire d'ordinal critique κ sans contrainte supplémentaire.*

En revanche, l'hypothèse que κ est mesurable ne garantit que l'existence du plongement élémentaire $\boldsymbol{j}_U$ associé à une ultrapuissance, et, dans ce cas, XIII.2.3.7(iv) *implique $U \notin \boldsymbol{M}$, donc $V_{\kappa+2} \not\subseteq \boldsymbol{M}$: tout cardinal mesurable est 1-fort, mais il n'est pas évident qu'il existe un cardinal γ-fort avec $\gamma \geqslant 2$.* ◁

1.2.3.— Même si celle-ci n'est pas utilisée dans la suite, mentionnons ici une définition alternative particulièrement naturelle des cardinaux forts.

Proposition (cardinal fort).— *Un cardinal κ est fort si, et seulement si, pour tout ensemble A, il existe $\boldsymbol{j} : \boldsymbol{V} \xrightarrow{\preccurlyeq} \boldsymbol{M}$ vérifiant $\mathrm{cr}(\boldsymbol{j}) = \kappa$ et $A \in \boldsymbol{M}$.*

Démonstration. La condition est nécessaire puisque, étant donné A, il existe γ tel que A appartienne à $V_{\kappa+\gamma}$, et $V_{\kappa+\gamma} \subseteq \boldsymbol{M}$ implique $A \in M$. Elle est suffisante, puisque faire $A = V_{\kappa+\gamma}$ garantit $V_{\kappa+\gamma} \in \boldsymbol{M}$, donc $V_{\kappa+\gamma} \subseteq \boldsymbol{M}$. □

1.2.4.— Nous nous concentrons ici sur la comparaison des grands cardinaux entre eux. De ce point de vue, les cardinaux 2-forts, et donc *a fortiori* les cardinaux forts, surpassent (de beaucoup) les cardinaux mesurables.

Proposition (fort *vs.* mesurable).— *Si κ est un cardinal 2-fort, alors il existe sur κ un ultrafiltre normal U tel que U-presque tout cardinal $<\kappa$ est mesurable ; en particulier, κ est le $\kappa^{\text{ième}}$ cardinal mesurable.*

Démonstration. Soit $\boldsymbol{j} : \boldsymbol{V} \xrightarrow{\preccurlyeq} \boldsymbol{M}$ vérifiant $\mathrm{cr}(\boldsymbol{j}) = \kappa$ et $V_{\kappa+2} \subseteq \boldsymbol{M}$. Comme dans 1.1.5, posons $U := \{X \subseteq \kappa \mid \kappa \in \boldsymbol{j}(X)\}$. Alors, U est un ultrafiltre normal sur κ, appartenant à $V_{\kappa+2}$, donc à $\boldsymbol{M}$. On déduit $\boldsymbol{M} \models$ « κ est mesurable », soit

$$\boldsymbol{M} \models \text{« } [\mathrm{id}_\kappa] \text{ est mesurable »}, \tag{\#2}$$

puisque U est normal. Par le théorème de Łoś, (#2) équivaut à

$$\{\xi < \kappa \mid \boldsymbol{V} \models \text{« } \xi \text{ est mesurable »}\} \in U.$$

Enfin, puisque U est normal, tous les éléments de U ont pour cardinalité κ. □

▷ *Si l'on appelle « mesurable d'ordre 2 » un cardinal mesurable admettant une mesure normale s'accumulant sur les cardinaux mesurables, on peut introduire de même les cardinaux mesurables d'ordre 3, puis, inductivement, d'ordre θ pour tout ordinal θ. L'argument de la démonstration de 1.2.4 montre alors que, si κ est 2-fort, il est mesurable d'ordre $(2^\kappa)^+$, qui est beaucoup plus que mesurable.* ◁

1.2.5.— Suivant le schéma désormais habituel, on déduit l'impossibilité d'établir l'existence d'un cardinal fort.

Corollaire (existence d'un cardinal 2-fort).— *S'il est consistant, le système* ZFC+ *« il existe un cardinal mesurable » ne prouve pas « il existe un cardinal 2-fort ». La consistance de* ZFC+ *« il existe un cardinal mesurable » n'entraîne pas celle de* ZFC+ *« il existe un cardinal 2-fort ».*

Des résultats analogues valent lorsque « 2-fort » est remplacé par « fort ».

1.2.6.— La définition 1.2.2 comporte une quantification existentielle sur des classes $\boldsymbol{j}$ et $\boldsymbol{M}$, et n'est donc *pas* une formule ensembliste. Il n'est donc pas clair que « être un cardinal γ-fort » soit une propriété ensembliste, c'est-à-dire qu'il existe une formule ensembliste $\Phi(x, \gamma)$ telle que κ est γ-fort si, et seulement si, $\Phi(\kappa, \gamma)$ est vérifiée.

▷ *Par* 1.1.6*, un cardinal κ est mesurable si, et seulement si, il existe un plongement élémentaire $\boldsymbol{j}$ d'ordinal critique κ allant de $\boldsymbol{V}$ dans une classe $\boldsymbol{M}$ qui inclut V_κ, et alors l'ultrafiltre U défini par $U := \{X \subseteq \kappa \mid \kappa \in \boldsymbol{j}(X)\}$ contient suffisamment d'informations pour construire, par le biais de l'ultrapuissance* Ult_U*, un plongement élémentaire possédant les mêmes propriétés que $\boldsymbol{j}$. De ce fait, être l'ordinal critique d'un plongement élémentaire de l'univers dans une des ses sous-classes est une propriété ensembliste. Pour des plongements élémentaires avec des propriétés de clôture plus fortes, typiquement ceux qui interviennent dans la définition des cardinaux forts, aucun ultrafiltre ne contient assez d'informations pour construire un plongement du type voulu, et l'argument est en défaut.* ◁

1.2.7.— Le problème est de définir une approximation locale d'un plongement élémentaire permettant d'obtenir davantage de clôture du modèle d'arrivée qu'une ultrapuissance. La réponse est donnée par la notion d'*extendeur*, qui remplace un unique ultrafiltre par une famille cohérente d'ultrafiltres permettant de construire collectivement un plongement élémentaire dont le modèle-but peut satisfaire des propriétés de clôture plus fortes que celui provenant d'une ultrapuissance simple.

Proposition (approximation).— *Supposons* $\boldsymbol{j} : \boldsymbol{V} \xrightarrow{\preceq} \boldsymbol{M}$ *avec* $\mathrm{cr}(\boldsymbol{j}) = \kappa$ *et* $V_{\kappa+\gamma} \subseteq \boldsymbol{M}$*, et de plus* $\boldsymbol{j}(\kappa) > \kappa + \gamma$*. Soit* $\lambda := \|V_{\kappa+\gamma}\|^+$ *et, pour* a *dans* $\mathfrak{P}_{\mathrm{fini}}(\lambda)$*, soit*

$$E_a := \{X \subseteq \mathfrak{P}_{\mathrm{fini}}(\kappa) \mid a \in \boldsymbol{j}(X)\}. \qquad (\#3)$$

(i) *Pour chaque* a*, l'ensemble* E_a *est un ultrafiltre* κ*-complet sur* $\mathfrak{P}_{\mathrm{fini}}(\kappa)$*, et il existe une factorisation* $\boldsymbol{j} = \boldsymbol{k}_a \circ \boldsymbol{j}_a$ *où* $\boldsymbol{j}_a$ *est le plongement élémentaire de* $\boldsymbol{V}$ *dans* Ult_{E_a} *et* $\boldsymbol{k}_a$ *un plongement élémentaire de* Ult_{E_a} *dans* $\boldsymbol{M}$*.*

(ii) *Pour* $a \subseteq b$ *dans* $\mathfrak{P}_{\mathrm{fini}}(\lambda)$*, et* $\mathrm{pr}_{b,a}$ *défini par* $\mathrm{pr}_{b,a}(Y) := Y \cap a$*, l'application* $\boldsymbol{j}_{a,b} : [f]_{E_a} \mapsto [f \circ \mathrm{pr}_{b,a}]_{E_b}$ *est bien définie et est un plongement élémentaire de* Ult_{E_a} *dans* Ult_{E_b}*, et on a* $\boldsymbol{k}_a = \boldsymbol{k}_b \circ \boldsymbol{j}_{a,b}$*.*

(iii) *La limite inductive* $(\mathrm{Ult}_E, \boldsymbol{j}_E)$ *du système* $(\mathrm{Ult}_{E_a}, \boldsymbol{j}_{a,b})_{a \subseteq b \in \mathfrak{P}_{\mathrm{fini}}(\lambda)}$ *est bien fondée ;* $\boldsymbol{j}_E$ *est un plongement élémentaire de* $\boldsymbol{V}$ *dans* Ult_E *d'ordinal critique* κ*, et on a* $V_{\kappa+\gamma} \subseteq \mathrm{Ult}_E$*.*

Démonstration (esquisse). Le point (i) se montre comme 1.1.5. Le point (ii) résulte de ce que $a \in j(\{X \in \mathfrak{P}_{\mathrm{fini}}(\kappa) \mid f(X) = g(X)\})$ implique

$$b \in j(\{Y \in \mathfrak{P}_{\mathrm{fini}}(\kappa) \mid f(\mathrm{pr}_{b,a}(Y)) = g(\mathrm{pr}_{b,a}(Y))\})$$

et du théorème de Łoś (XIII.2.3.2). Pour (iii), la factorisation $\boldsymbol{j} = \boldsymbol{k}_a \circ \boldsymbol{j}_a$ obtenue en (i) et la cohérence des plongements $\boldsymbol{j}_a$ entraîne, par passage à la limite inductive, l'existence d'une factorisation de $\boldsymbol{j}$ par $\boldsymbol{j}_E$, donc d'un plongement élémentaire $\boldsymbol{k}$ de Ult_E dans $\boldsymbol{M}$ vérifiant $\boldsymbol{j} = \boldsymbol{k} \circ \boldsymbol{j}_E$. Il résulte alors de la définition de $\boldsymbol{k}_a$, et, de là, de $\boldsymbol{k}$, qu'un élément de $\boldsymbol{M}$ est dans l'image de $\boldsymbol{k}$ si, et seulement si, il peut s'écrire sous la forme $\boldsymbol{j}(f)(a)$ avec $a \in \mathfrak{P}_{\mathrm{fini}}(\lambda)$ et $f : \mathfrak{P}_{\mathrm{fini}}(\kappa) \to a$. Le point crucial est alors que, pour tout a dans $\mathfrak{P}_{\rm fini}(\lambda)$, on a $\boldsymbol{k}_a([\mathrm{id}_{\mathfrak{P}_{\rm fini}(\kappa)}]_{E_a}) = a$, par un argument de normalité comme dans 1.1.5. Cela implique que l'ordinal critique de $\boldsymbol{k}$ est $\geqslant\lambda$, et, de là, on déduit que tout élément de $V_{\kappa+\gamma}$ est dans Ult_E. □

Ainsi, le plongement élémentaire $\boldsymbol{j}_E$ associé à Ult_E fournit une approximation de $\boldsymbol{j}$ fidèle jusqu'au niveau de $V_{\kappa+\gamma}$.

1.2.8.— La famille $(E_a \mid a \in \mathfrak{P}_{\rm fini}(\lambda))$ définie par (#3) est appelée le (κ, λ)-*extendeur* associé à $\boldsymbol{j}$. Sans partir d'un plongement élémentaire préexistant, on peut définir abstraitement un (κ, λ)-extendeur comme une famille cohérente d'ultrafiltres E vérifiant des conditions *ad hoc* de normalité et de bonne fondation de la limite, et lui associer un plongement élémentaire $\boldsymbol{j}_E$ de sorte que l'extendeur associé à $\boldsymbol{j}_E$ soit E.

Corollaire (ensembliste).— *« Être un cardinal γ-fort » et « être un cardinal fort » sont des propriétés ensemblistes.*

Démonstration. Par 1.2.7, κ est un cardinal γ-fort si, et seulement, il existe un $(\kappa, \|V^+_{\kappa+\gamma}\|)$-extendeur E témoignant de ce que κ est γ-fort dans Ult_E : la quantification existentielle sur la classe propre $\boldsymbol{j}$ peut être remplacée par la quantification existentielle sur un extendeur E, qui est un ensemble, et donc peut être exprimée par une formule ensembliste. Il en est de même pour la propriété d'être fort, en ajoutant une quantification $\forall\gamma$. □

▷ *La notion d'extendeur joue un rôle technique crucial dans l'analyse des plongements élémentaires associés aux « grands grands cardinaux ». Plusieurs variantes de la notion d'extendeur associé à un plongement élémentaire $\boldsymbol{j}$ ont été introduites, voir par exemple* [34, chapitre 22, pp. 1881 sq.]*, le principe étant toujours qu'un extendeur capture une portion suffisante du plongement élémentaire qu'il s'agit d'approximer. Dans* [122]*, le (κ, λ)-extendeur associé à un plongement élémentaire $\boldsymbol{j} : \boldsymbol{V} \xrightarrow{\prec} \boldsymbol{M}$ est simplement défini comme la fonction $E : \mathfrak{P}(\lambda) \to \mathfrak{P}(\lambda)$ définie par $E(a) := \boldsymbol{j}(a) \cap \lambda$.* ◁

1.2.9.— Continuant à monter dans la hiérarchie des grands cardinaux, on passe maintenant aux cardinaux de Woodin.

Définition (cardinal de Woodin).— Un cardinal δ est un cardinal *de Woodin* si, pour toute fonction $f : \delta \to \delta$, il existe $\kappa < \delta$ et $\boldsymbol{j} : \boldsymbol{V} \xrightarrow{\prec} \boldsymbol{M}$ vérifiant $\mathrm{cr}(\boldsymbol{j}) = \kappa$ avec $V_{\boldsymbol{j}(f)(\kappa)} \subseteq \boldsymbol{M}$ et $\mathrm{Im}(f{\restriction}\kappa) \subseteq \kappa$.

▷ *La définition* 1.2.9 *peut paraître peu naturelle, mais on verra au chapitre* XV *qu'elle correspond exactement à la quantité de réflexion* (*au sens de* XI.1.2.3 *et telle que précisée ci-dessous*) *nécessaire pour l'analyse de la détermination des ensembles projectifs.* ◁

1.2.10.— Les cardinaux de Woodin surpassent les cardinaux γ-forts.

Proposition (Woodin *vs.* fort).— *Si δ est un cardinal de Woodin, alors, pour tout $\gamma < \delta$, l'ensemble des cardinaux γ-forts plus petits que δ a pour cardinalité δ.*

Démonstration. Supposons que δ est un cardinal de Woodin. Si δ n'est pas un cardinal régulier, il existe $\theta < \delta$ et $g : \theta \to \delta$ cofinale. Soit alors $f : \delta \to \delta$ définie par $f(\xi) := \theta + 1 + g(\xi)$ pour $\xi < \theta$ et $f(\xi) := \theta + 1$ pour $\theta \leqslant \xi < \delta$. Aucun ordinal κ ne peut alors vérifier $\xi < \kappa \Rightarrow f(\xi) < \kappa$, ce qui contredit que δ soit de Woodin.

Soient θ, γ quelconques $<\delta$. Soit $f : \delta \to \delta$ définie par $f(\xi) := \max(\theta + 1, \xi + \gamma)$. Par définition, il existe un plongement élémentaire $\boldsymbol{j} : \boldsymbol{V} \xrightarrow{\prec} \boldsymbol{M}$ tel que, en posant $\kappa := \mathrm{cr}(\boldsymbol{j})$, on a $\kappa < \delta$, $V_{\boldsymbol{j}(f)(\kappa)} \subseteq \boldsymbol{M}$, et $\xi < \kappa \Rightarrow f(\xi) < \kappa$. La dernière condition implique $\kappa > \theta$, donc $\boldsymbol{j}(\theta) = \theta$, et $\boldsymbol{j}(f)(\kappa) = \max(\theta+1, \kappa+\boldsymbol{j}(\gamma)) \geqslant \kappa+\gamma$, d'où $V_{\kappa+\gamma} \subseteq \boldsymbol{M}$. Par définition, κ est alors γ-fort. Les cardinaux γ-forts sont donc cofinaux sous δ. Puisque δ est régulier, cela implique que l'ensemble des cardinaux γ-forts sous δ a pour cardinalité δ. $\square$

$\triangleright$ *L'implication de* 1.2.10 *est proche d'une équivalence : si κ est dit γ-fort* pour A *s'il existe $\boldsymbol{j} : \boldsymbol{V} \xrightarrow{\prec} \boldsymbol{M}$ vérifiant $\mathrm{cr}(\boldsymbol{j}) = \kappa$, $\boldsymbol{j}(\kappa) > \gamma$, $V_{\kappa+\gamma} \subseteq \boldsymbol{M}$ et, de plus, $A \cap V_{\kappa+\gamma} = \boldsymbol{j}(A) \cap V_{\kappa+\gamma}$, alors δ est de Woodin si, et seulement si, pour tout $\gamma < \delta$ et tout $A \subseteq V_\delta$, les cardinaux γ-forts pour A sont cofinaux dans δ.* $\triangleleft$

1.2.11.— Suivant le schéma habituel, on déduit l'impossibilité d'établir l'existence d'un cardinal de Woodin.

Corollaire (existence d'un cardinal de Woodin).— *S'il est consistant, le système* ZFC+ *« il existe un cardinal 2-fort » ne prouve pas « il existe un cardinal de Woodin ». La consistance de* ZFC+ *« il existe un cardinal 2-fort » n'entraîne pas celle de* ZFC+ *« il existe un cardinal de Woodin ».*

1.2.12.— Comme dans le cas des cardinaux γ-forts et forts, les plongements élémentaires apparaissant dans la définition des cardinaux de Woodin peuvent être approximés par des extendeurs convenables. De là, le même argument qu'en 1.2.8 montre que « être un cardinal de Woodin » est une propriété ensembliste.

1.2.13.— Par définition, un cardinal de Woodin est inaccessible et limite de cardinaux 2-forts, et donc l'existence d'un tel cardinal est axiome de (très) grand cardinal. Pour autant, la définition ne requiert pas qu'un cardinal de Woodin soit lui-même l'ordinal critique d'un plongement élémentaire, et, de fait, il est faux qu'un cardinal de Woodin soit nécessairement mesurable, ou même faiblement compact.

Proposition (premier cardinal de Woodin).— *S'il existe, le plus petit cardinal de Woodin n'est pas faiblement compact.*

Démonstration. La définition 1.2.9 ne comporte qu'une quantification universelle sur les parties de V_κ (« $\forall f : \kappa \to \kappa \ldots$ »), puis des propriétés pouvant s'exprimer par des formules bornées dans V_κ à partir du moment où la quantification sur les plongements élémentaires est remplacée par une quantifications sur des extendeurs convenables. Être un cardinal de Woodin est donc une propriété Π^1_1-descriptible et, par conséquent, le premier cardinal de Woodin (s'il existe) n'est pas Π^1_1-indescriptible, et donc, par XIII.1.3.5, il n'est pas faiblement compact. □

En quelque sorte, un cardinal de Woodin est donc un témoin de l'existence de très grands cardinaux sans être lui-même un de ces très grands cardinaux (mais il est néanmoins nécessairement de très grande taille) — une situation que l'on retrouvera plus loin avec les cardinaux de Laver.

1.3. Les cardinaux supercompacts

▶ Résumé.— Les cardinaux supercompacts sont issus d'ultrafiltres normaux sur les ensembles $\mathfrak{P}_{<\kappa}(\lambda)$ et dépassent les cardinaux de Woodin. ◀

1.3.1.— Les grands cardinaux de la sous-section 1.2 sont définis par l'existence de plongements élémentaires $\boldsymbol{j} : \boldsymbol{V} \xrightarrow{\preceq} \boldsymbol{M}$ tels que le modèle d'arrivée $\boldsymbol{M}$ coïncide avec $\boldsymbol{V}$ jusqu'à un certain rang. Réclamer que $\boldsymbol{M}$ soit clos par suites d'une longueur fixée, c'est-à-dire que l'on ait ${}^\lambda\boldsymbol{M} \subseteq \boldsymbol{M}$, mène à des notions encore plus fortes. De la sorte, on arrive à la notion de cardinal supercompact.

Définition (supercompact).— Un cardinal κ est dit λ-*supercompact* s'il existe $\boldsymbol{j} : \boldsymbol{V} \xrightarrow{\preceq} \boldsymbol{M}$ vérifiant $\mathrm{cr}(\boldsymbol{j}) = \kappa$, $\boldsymbol{j}(\mathrm{cr}(\boldsymbol{j})) > \lambda$, et ${}^\lambda\boldsymbol{M} \subseteq \boldsymbol{M}$; κ est dit *supercompact* s'il est λ-supercompact pour tout λ.

Exemple. Par 1.1.6 *et* XIII.2.3.7*, un cardinal κ est κ-supercompact si, et seulement si, il est mesurable : la notion de cardinal λ-supercompact ne devient spécifique que pour $\lambda > \kappa$. Une induction immédiate sur $\alpha \leqslant \lambda$ montre que, au moins pour λ inaccessible, ${}^\lambda\boldsymbol{M} \subseteq \boldsymbol{M}$ implique $V_\alpha \subseteq \boldsymbol{M}$: tout élément de $V_{\alpha+1}$ est une partie de V_α, donc est codé par une application de V_α dans $\{0,1\}$, donc un élément de ${}^{\|V_\alpha\|}\boldsymbol{M}$. Pour λ inaccessible, un plongement élémentaire témoignant que κ est λ-supercompact témoigne donc aussi de ce que κ est λ-fort.*

1.3.2.— En fait, être supercompact est une propriété (beaucoup) plus forte qu'être fort, et même qu'être de Woodin — et, comme la démonstration ci-dessous le montre, que plusieurs autres propriétés intermédiaires.

Proposition (supercompact *vs.* Woodin).— *Si κ est 2^κ-supercompact, alors κ est le $\kappa^{\text{ième}}$ cardinal de Woodin.*

Démonstration. Supposons que κ est 2^κ-supercompact. Soit $\boldsymbol{j} : \boldsymbol{V} \xrightarrow{\preceq} \boldsymbol{M}$ vérifiant $\mathrm{cr}(\boldsymbol{j}) = \kappa$, $\boldsymbol{j}(\kappa) > 2^\kappa$, et ${}^{2^\kappa}\boldsymbol{M} \subseteq \boldsymbol{M}$. Posons $j' := j{\restriction}V_{\kappa+1}$. Par 1.1.2, j' est un plongement élémentaire de $V_{\kappa+1}$ dans $V^{\boldsymbol{M}}_{\boldsymbol{j}(\kappa)+1}$. Par hypothèse, on a $V^{\boldsymbol{M}}_\alpha = V_\alpha$

pour tout $\alpha \leqslant \kappa + 1$: on a donc $j' \subseteq \boldsymbol{M}$, donc $j' \in \boldsymbol{M}$ puisque $\|j'\|$ est 2^κ. Déclarons que θ est 1-*extensible* s'il est l'ordinal critique d'un plongement i de $V_{\theta+1}$ dans $V_{i(\theta)+1}$. On vient donc de montrer que κ est 1-extensible dans $\boldsymbol{M}$. Soit alors U défini par (#1), soit $U := \{X \subseteq \kappa \mid \kappa \in \boldsymbol{j}(X)\}$. Par 1.1.5, U est un ultrafiltre normal sur κ. Soit $X := \{\theta < \kappa \mid$ « θ est 1-extensible »$\}$. Par élémentarité, on a

$$\boldsymbol{j}(X) := \{\theta < \boldsymbol{j}(\kappa) \mid \boldsymbol{M} \models \text{« } \theta \text{ est 1-extensible »}\},$$

et on a donc $\kappa \in \boldsymbol{j}(X)$, soit $X \in U$. Donc, κ est le $\kappa^{\text{ième}}$ cardinal 1-extensible.

Ensuite, supposons que θ est 1-extensible : il existe $i : V_{\theta+1} \xrightarrow{\prec} V_{i(\theta)+1}$. Soit E le $(\theta, i(\theta))$-extendeur associé à i. Alors, j_E donne un plongement élémentaire de $\boldsymbol{V}$ dans l'ultrapuissance Ult_E de cardinal critique θ et vérifiant $j_E(\theta) = i(\theta)$ et $V_{j_E(\theta)} \subseteq \mathrm{Ult}_E$, ce qui est traduit en déclarant que θ est *superfort*. En fait, comme E est alors dans $\boldsymbol{M}$, on a non seulement qu'un cardinal 1-extensible est superfort, mais que, comme il reste superfort dans le modèle d'arrivée, il existe un ultrafiltre normal sur θ s'accumulant sur les cardinaux superforts $<\theta$, et donc θ est limite de cardinaux superforts.

Enfin, supposons $\kappa = \mathrm{cr}(\boldsymbol{j})$ avec $\boldsymbol{j} : \boldsymbol{V} \xrightarrow{\prec} \boldsymbol{M}$ et $V_{\boldsymbol{j}(\kappa)} \subseteq \boldsymbol{M}$. Soit $f : \kappa \to \kappa$. Alors, $\boldsymbol{j}(f)$ est une application de $\boldsymbol{j}(\kappa)$ dans $\boldsymbol{j}(\kappa)$, et on a $\mathrm{Im}(\boldsymbol{j}(f){\restriction}\kappa) = \mathrm{Im}(f) \subseteq \kappa$. Soit $\lambda := \|V^{\boldsymbol{M}}_{\boldsymbol{j}(f)(\kappa)}\|$ et soit E le (κ, λ)-extendeur associé à $\boldsymbol{j}$. Par construction, on a $\boldsymbol{j}(f)(\kappa) < \boldsymbol{j}(\kappa)$, d'où $\lambda < \boldsymbol{j}(\kappa)$ puisque $\boldsymbol{j}(\kappa)$ est inaccessible dans $\boldsymbol{M}$. L'extendeur E est donc inclus dans $\boldsymbol{M}$. On a alors $\boldsymbol{j}_E(f) = \boldsymbol{j}(f)$, et $V_{\boldsymbol{j}_E(f)(\kappa)} \subseteq \mathrm{Ult}_E$, d'où on tire

$$\begin{aligned}\boldsymbol{M} \models \exists E\,(&\text{« } E \text{ est un extendeur et } \mathrm{cr}(\boldsymbol{j}_E) = \kappa \\ &\text{et } \mathrm{Im}(\boldsymbol{j}(f){\restriction}\kappa) \subseteq \kappa \text{ et } V_{\boldsymbol{j}_E(f)(\kappa)} \subseteq \mathrm{Ult}_E \text{ »}),\end{aligned}$$

qui implique

$$\begin{aligned}\boldsymbol{M} \models \exists E\,(&\text{« } E \text{ est un extendeur et } \mathrm{cr}(\boldsymbol{j}_E) < \boldsymbol{j}(\kappa) \\ &\text{et } \mathrm{Im}(\boldsymbol{j}(f){\restriction}\mathrm{cr}(\boldsymbol{j}_E)) \subseteq \mathrm{cr}(\boldsymbol{j}_E) \text{ et } V_{\boldsymbol{j}(f)(\mathrm{cr}(\boldsymbol{j}_E))} \subseteq \mathrm{Ult}_E \text{ »}),\end{aligned}$$

d'où, par élémentarité de $\boldsymbol{j}$,

$$\begin{aligned}\boldsymbol{V} \models \exists E\,(&\text{« } E \text{ est un extendeur et } \mathrm{cr}(\boldsymbol{j}_E) < \kappa \\ &\text{et } \mathrm{Im}(f{\restriction}\mathrm{cr}(\boldsymbol{j}_E)) \subseteq \mathrm{cr}(\boldsymbol{j}_E) \text{ et } V_{f(\mathrm{cr}(\boldsymbol{j}_E))} \subseteq \mathrm{Ult}_E \text{ »}) :\end{aligned}$$

l'existence d'un tel plongement élémentaire $\boldsymbol{j}_E$ pour chaque fonction f montre que κ est un cardinal de Woodin. À nouveau, on peut observer que κ reste un cardinal de Woodin dans $\boldsymbol{M}$, et, de là, il existe un ultrafiltre normal sur κ s'accumulant sur les cardinaux de Woodin $<\kappa$.

Au total, si κ est 2^κ-supercompact, il est le $\kappa^{\text{ième}}$ cardinal 1-extensible ; si κ est 1-extensible, il est le $\kappa^{\text{ième}}$ cardinal superfort ; et si κ est superfort, il est le $\kappa^{\text{ième}}$ cardinal de Woodin. □

1.3.3. Corollaire (existence d'un cardinal supercompact).— *S'il est consistant, le système* ZFC+ *« il existe un cardinal de Woodin » ne prouve pas « il existe un cardinal supercompact ». La consistance de* ZFC+ *« il existe un cardinal de Woodin » n'entraîne pas celle de* ZFC+ *« il existe un cardinal supercompact ».*

1.3.4.— Comme pour les cardinaux forts et de Woodin, il n'est pas évident que la supercompacité soit une propriété ensembliste puisque définie par l'existence d'un plongement élémentaire mettant en jeu toute la classe $\boldsymbol{V}$.

▷ *L'approximation par des extendeurs n'est pas suffisante ici, car, par construction, un extendeur (tout au moins du type considéré dans* 1.2.7) *ne garantit pour le modèle d'arrivée des plongements qu'une condition du type* $V_\lambda \subseteq \boldsymbol{M}$*, mais pas* ${}^\lambda\boldsymbol{M} \subseteq \boldsymbol{M}$. ◁

1.3.5.— Un nouveau type d'ultrafiltre intervient ici, non plus sur un ordinal mais sur un ensemble de parties. On rappelle que $\mathfrak{P}_{<\kappa}(\lambda)$ est l'ensemble des parties de λ de cardinal $<\kappa$.

Définition (normal).— Un ultrafiltre U sur $\mathfrak{P}_{<\kappa}(\lambda)$ est dit *normal* s'il est κ-complet, contient chaque ensemble $\{x \in \mathfrak{P}_{<\kappa}(\lambda) \mid a \subseteq x\}$ pour a dans $\mathfrak{P}_{<\kappa}(\lambda)$, et, si $(X_\alpha \mid \alpha \in \lambda)$ est une famille d'éléments de U, alors l'intersection diagonale $\triangle_{\alpha<\lambda} X_a := \{x \in \mathfrak{P}_{<\kappa}(\lambda) \mid \forall\alpha{\in}x\,(x \in X_\alpha)\}$ est aussi dans U.

▷ *Dans* 1.3.5*, ce sont les éléments de* $\mathfrak{P}_{<\kappa}(\lambda)$ *— donc les petites parties de* λ *— qui jouent le rôle des ordinaux dans les ultrafiltres de* XIII.2.3.7 *: ce sont donc les ensembles de petites parties de* λ *qui sont ou non dans l'ultrafiltre, et pas les petites parties de* λ. ◁

1.3.6.— Cette notion d'ultrafiltre donne la caractérisation espérée.

Proposition (supercompact).— *Un cardinal* κ *est* λ*-supercompact si, et seulement si, il existe un ultrafiltre normal sur* $\mathfrak{P}_{<\kappa}(\lambda)$.

Démonstration. Supposons que $\boldsymbol{j} : \boldsymbol{V} \xrightarrow{\prec} \boldsymbol{M}$ témoigne de la λ-supercompacité de κ. Posons

$$U := \{X \subseteq \mathfrak{P}_{<\kappa}(\lambda) \mid \mathrm{Im}(\boldsymbol{j}{\restriction}\lambda) \in \boldsymbol{j}(X)\}.$$

Puisque $\boldsymbol{M}$ est clos par suite de longueur λ, l'ensemble $\mathrm{Im}(\boldsymbol{j}{\restriction}\lambda)$ appartient à $\boldsymbol{M}$ et, dans $\boldsymbol{M}$, c'est un élément de $\mathfrak{P}_{<\boldsymbol{j}(\kappa)}(\boldsymbol{j}(\lambda))$, qui est $\boldsymbol{j}(\mathfrak{P}_{<\kappa}(\lambda))$, donc, par définition, $\mathfrak{P}_{<\kappa}(\lambda)$ est dans U. Le même argument que pour 1.1.5 montre que U est un ultrafiltre κ-complet. Ensuite, soit a quelconque dans $\mathfrak{P}_{<\kappa}(\lambda)$. Posons

$$X_a := \{x \in \mathfrak{P}_{<\kappa}(\lambda) \mid a \subseteq x\}.$$

On a $\boldsymbol{j}(X_a) = \{x \in \mathfrak{P}_{<\boldsymbol{j}(\kappa)}(\boldsymbol{j}(\lambda)) \mid \boldsymbol{j}(a) \subseteq x\}$. Par hypothèse, on a $\|a\| < \kappa$, d'où $\boldsymbol{j}(a) = \{\boldsymbol{j}(\xi) \mid \xi \in a\}$ et, de là, $\boldsymbol{j}(a) \subseteq \mathrm{Im}(\boldsymbol{j}{\restriction}\lambda)$, donc $X_a \in U$. Enfin, supposons $X_\alpha \in U$ pour $\alpha < \lambda$, soit $\mathrm{Im}(\boldsymbol{j}{\restriction}\lambda) \in \boldsymbol{j}(X_\alpha)$. Soit $X := \triangle_{\alpha<\lambda} X_\alpha$. On trouve

$$\boldsymbol{j}(X) = \{x \in \mathfrak{P}_{<\boldsymbol{j}(\kappa)}(\boldsymbol{j}(\lambda)) \mid \forall\alpha{\in}x\,(x \in \boldsymbol{j}((X_\xi \mid \xi < \lambda))_\alpha\}.$$

La question est de savoir si $\mathrm{Im}(\boldsymbol{j}{\restriction}\lambda)$ est dans $\boldsymbol{j}(X)$, donc de savoir si, pour tout α dans $\mathrm{Im}(\boldsymbol{j}{\restriction}\lambda)$, donc pour tout α pouvant s'écrire $\boldsymbol{j}(\beta)$ avec $\beta < \lambda$, l'ensemble $\mathrm{Im}(\boldsymbol{j}{\restriction}\lambda)$ appartient au $\alpha^{\text{ième}}$ terme de la suite $\boldsymbol{j}((X_\xi \mid \xi < \lambda))$: or le $\boldsymbol{j}(\beta)^{\text{ième}}$ terme de cette suite est $\boldsymbol{j}(X_\beta)$, qui contient $\mathrm{Im}(\boldsymbol{j}{\restriction}\lambda)$ puisque, par hypothèse, X_β est dans U. Donc, U est un ultrafiltre normal sur $\mathfrak{P}_{<\kappa}(\lambda)$.

Inversement, supposons que U est un ultrafiltre normal sur $\mathfrak{P}_{<\kappa}(\lambda)$. On forme l'ultrapuissance Ult_U comme en XIII.2.3.7, et on obtient un modèle intérieur et un plongement élémentaire $\boldsymbol{j}_U$ de $\boldsymbol{V}$ dans Ult_U. Comme dans XIII.2.3.7, l'ordinal critique de $\boldsymbol{j}_U$ est κ. La κ-complétude de U entraîne $\boldsymbol{j}_U{\restriction}\kappa = \mathrm{id}_\kappa$. Par ailleurs, la classe $[\mathrm{id}]_U$ de la fonction identité de $\mathfrak{P}_{<\kappa}(\lambda)$ est un sous-ensemble de $\boldsymbol{j}(\lambda)$. Pour tout $\alpha < \lambda$, l'ensemble des x dans $\mathfrak{P}_{<\kappa}(\lambda)$ qui contiennent α est dans U par hypothèse, donc $\boldsymbol{j}(\alpha)$ est dans $[\mathrm{id}]_U$ et, de là, $\mathrm{Im}(\boldsymbol{j}{\restriction}\lambda) \subseteq [\mathrm{id}]_U$. Inversement, supposons que $f : \mathfrak{P}_{<\kappa}(\lambda) \to \mathfrak{P}(\lambda)$ satisfait $\boldsymbol{j}(\alpha) \in [f]_U$ pour tout $\alpha < \lambda$: alors l'ensemble X_α défini par $X_\alpha := \{x \in \mathfrak{P}_{<\kappa}(\lambda) \mid \alpha \in f(x)\}$ est dans U. Il en est donc de même de $\triangle_{\alpha<\lambda} X_\alpha$. Or, on a

$$\begin{aligned}\triangle_{\alpha<\lambda} X_\alpha &:= \{x \in \mathfrak{P}_{<\kappa}(\lambda) \mid \forall\alpha{\in}x\,(x \in X_\alpha)\}\\ &= \{x \in \mathfrak{P}_{<\kappa}(\lambda) \mid \forall\alpha{\in}x\,(\alpha \in f(x))\} = \{x \in \mathfrak{P}_{<\kappa}(\lambda) \mid x \subseteq f(x)\} :\end{aligned}$$

on a donc $[\mathrm{id}]_U \subseteq [f]_U$, d'où $[\mathrm{id}]_U = \mathrm{Im}(\boldsymbol{j}{\restriction}\lambda)$.

Enfin, supposons que $([f_\alpha]_U \mid \alpha < \lambda)$ est une λ-suite d'éléments de Ult_U. Considérons $g : \mathfrak{P}_{<\kappa}(\lambda) \to \boldsymbol{V}$ où $g(x)$ est la fonction de domaine x vérifiant $g(\alpha) = f_\alpha(x)$ pour α dans x. Alors, $[g]_U$ est une fonction de domaine $[\mathrm{id}]_U$, c'est-à-dire $\mathrm{Im}(\boldsymbol{j}{\restriction}\lambda)$, vérifiant $[g]_U(\boldsymbol{j}(\alpha)) = [f_\alpha]_U$. Donc, $([f_\alpha]_U \mid \alpha < \lambda)$ est dans Ult_U. □

▷ *Pour $\lambda = \kappa$, on retrouve la situation d'un cardinal mesurable et d'un ultrafiltre sur κ : en effet,* $\mathrm{Im}(\boldsymbol{j}{\restriction}\kappa)$ *coïncide avec κ et, si κ est strictement inclus dans $\mathfrak{P}_{<\kappa}(\kappa)$, on a $\kappa \in \boldsymbol{j}(\kappa)$, et κ est un segment initial de $\boldsymbol{j}(\kappa)$, donc les parties initiales de κ, c'est-à-dire les éléments de κ, forment une partie de $\mathfrak{P}_{<\kappa}(\kappa)$ qui est dans U. Si U est un ultrafiltre normal sur $\mathfrak{P}_{<\kappa}(\kappa)$, la trace de U sur κ est un ultrafiltre normal sur κ, et vice versa.* ◁

1.3.7.— Comme en 1.2.8, l'existence d'une caractérisation locale par l'existence d'un ultrafiltre convenable entraîne le caractère ensembliste.

Corollaire (ensembliste).— *« Être un cardinal λ-supercompact » et « être un cardinal supercompact » sont des propriétés ensemblistes.*

2. Rangs autosimilaires

On continue à renforcer les hypothèses de clôture du modèle d'arrivée des plongements élémentaires. L'hypothèse ultime dans cette direction est l'existence d'un plongement élémentaire $\boldsymbol{j} : \boldsymbol{V} \xrightarrow{\preceq} \boldsymbol{V}$. Mais cette condition se révèle contradictoire, au moins en présence de l'axiome du choix : c'est la borne de Kunen, qui place une limite au sommet de la hiérarchie des grands cardinaux. La contradiction disparaît quand on se restreint à un plongement élémentaire d'un fragment V_α dans lui-même : ainsi apparaissent les cardinaux de Laver, qui seront ici étudiés de façon approfondie en raison des propriétés algébriques étonnantes auxquelles ils mènent.

La section est divisée en trois sous-sections. Dans la sous-section 2.1, on montre l'impossibilité de l'existence d'un plongement élémentaire non trivial de $\boldsymbol{V}$ dans lui-même, et on introduit les axiomes I_0–I_3 à partir de plongements du type $V_\lambda \xrightarrow{\preceq} V_\lambda$, versions miniatures d'un impossible plongement $\boldsymbol{V} \xrightarrow{\preceq} \boldsymbol{V}$. Dans la sous-section 2.2, on introduit les cardinaux de Laver associés à l'axiome I_3, et on montre qu'ils surpassent les cardinaux supercompacts en passant par l'intermédiaire des cardinaux géants. Enfin, dans la sous-section 2.3, on montre que les plongements élémentaires associés à un cardinal de Laver sont munis d'une opération binaire naturelle, l'application, obéissant à la loi d'autodistributivité à gauche.

2.1. La borne de Kunen

▶ Résumé.— Il n'existe pas de plongement élémentaire de l'univers dans lui-même. ◀

2.1.1.— On a vu dans la section 1 que, lorsque l'on considère un plongement élémentaire $\boldsymbol{j} : \boldsymbol{V} \xrightarrow{\preceq} \boldsymbol{M}$, imposer au modèle d'arrivée $\boldsymbol{M}$ une proximité de plus en plus grande avec le modèle de départ $\boldsymbol{V}$ correspond à des hypothèses d'existence de plus en plus fortes. Le cas ultime est celui de l'égalité $\boldsymbol{M} = \boldsymbol{V}$. On va montrer ci-dessous que cette limite est inatteignable, au moins en présence de l'axiome du choix.

2.1.2.— Le noyau technique pour la suite est un résultat de non-clôture.

Lemme.— (AC) *Pour tout plongement élémentaire $\boldsymbol{j} : \boldsymbol{V} \xrightarrow{\preceq} \boldsymbol{M}$, si l'on pose $\lambda = \sup_{n<\omega} \boldsymbol{j}^n(\mathrm{cr}(\boldsymbol{j}))$, alors $V_{\lambda+1}$ n'est pas inclus dans $\boldsymbol{M}$.*

Démonstration. Soit $\kappa_0 := \mathrm{cr}(\boldsymbol{j})$ et $\kappa_n := \boldsymbol{j}(\kappa_{n-1})$ pour $n \geqslant 1$. Par définition, on a donc $\lambda = \sup_n \kappa_n$. De plus, on a $\kappa_1 = \boldsymbol{j}(\kappa_0) > \kappa_0$, d'où $\kappa_{n+1} > \kappa_n$ pour tout n par élémentarité de $\boldsymbol{j}$. L'égalité $\lambda = \sup_n \kappa_n$ entraîne

$$\boldsymbol{j}(\lambda) = \sup_n \boldsymbol{j}(\kappa_n) = \sup_n \kappa_{n+1} = \lambda.$$

Si V_λ n'est pas inclus dans $\boldsymbol{M}$, il en est *a fortiori* de même de $V_{\lambda+1}$. On suppose donc $V_\lambda \subseteq \boldsymbol{M}$, et on va montrer que $\mathrm{Im}(\boldsymbol{j}{\restriction}\lambda)$, qui est inclus dans λ donc appartient à $V_{\lambda+1}$, n'appartient pas à $\boldsymbol{M}$.

Par 1.1.6, κ_0 est un cardinal mesurable dans $\boldsymbol{V}$. Par élémentarité, κ_1 est mesurable dans $\boldsymbol{M}$, donc aussi dans $\boldsymbol{V}$ puisque, par hypothèse, $V^{\boldsymbol{M}}_{\kappa_1+2}$ coïncide avec V_{κ_1+2}. Inductivement, chaque ordinal κ_n est mesurable dans $\boldsymbol{V}$ et dans $\boldsymbol{M}$, et λ est donc un cardinal limite de cofinalité ω dans $\boldsymbol{V}$.

Pour tout n, on a $\|\mathfrak{P}(\kappa_n)\| = 2^{\kappa_n} < \kappa_{n+1} < \lambda$ puisque κ_{n+1} est inaccessible. On peut donc pour chaque n fixer une injection I_n de $\mathfrak{P}(\kappa_n)$ dans λ, et, de là, définir une injection I de $\mathfrak{P}(\lambda)$ dans λ^ω en posant $I(a) = (I_n(a \cap \kappa_n))_{n<\omega}$: l'injectivité de I vient de ce que, si a et b sont des sous-ensembles distincts de λ, il doit exister n vérifiant $a \cap V_{\kappa_n} \neq b \cap V_{\kappa_n}$.

On rappelle que, si μ est un cardinal, $\mathfrak{P}_\mu(A)$ désigne l'ensemble des parties de A de cardinal μ. Le point crucial est l'existence d'une fonction $F : \lambda^\omega \to \lambda$ vérifiant

$$\text{pour tout } X \text{ dans } \mathfrak{P}_\lambda(\lambda)\text{, l'image de } F{\restriction}X^\omega \text{ est l'intégralité de } \lambda. \qquad (\#4)$$

Or, puisque λ est fortement limite de cofinalité ω, par l'injection I ci-dessus, on a

$$\|\lambda \times \mathfrak{P}_\lambda(\lambda)\| \leqslant \|\lambda \times \mathfrak{P}(\lambda)\| = \|\mathfrak{P}(\lambda)\| \leqslant \|\lambda^\omega\|.$$

Par ailleurs, il est trivial de construire une injection de λ^ω dans $\mathfrak{P}_{\aleph_0}(\lambda)$ et *a fortiori* dans $\lambda \times \mathfrak{P}_\lambda(\lambda)$, donc on a $\|\lambda \times \mathfrak{P}_\lambda(\lambda)\| = \|\lambda^\omega\| = \lambda^{\aleph_0}$. Par conséquent, avec l'axiome du choix, on peut fixer une énumération de $\lambda \times \mathfrak{P}_\lambda(\lambda)$, soit $(\gamma_\xi, X_\xi)_{\xi<\lambda^{\aleph_0}}$, puis construire inductivement une suite injective $(s_\xi)_{\xi<\lambda^{\aleph_0}}$ dans λ^ω telle que s_ξ appartient à X_ξ^ω : cela est possible puisque les cardinalités de $\lambda \times \mathfrak{P}_\lambda(\lambda)$ et λ^ω sont égales. Définissons alors $F : \lambda^\omega \to \lambda$ par $F(s) := \gamma_\xi$ pour $s = s_\xi$ et $F(s) := 0$ pour $\forall \xi\, (s \neq s_\xi)$. Alors, F satisfait (#4). En effet, soient $X \in \mathfrak{P}_\lambda(\lambda)$ et $\gamma < \lambda$ quelconques. Par construction, il existe $\xi < \lambda^{\aleph_0}$ vérifiant $(\gamma, X) = (\gamma_\xi, X_\xi)$, et alors, par hypothèse, on a $s_\xi \in X_\xi^\omega$, d'où $F(s_\xi) = \gamma$.

Considérons alors la fonction $\boldsymbol{j}(F)$. Comme $\boldsymbol{j}$ est un plongement élémentaire et qu'il laisse λ fixe, $\boldsymbol{j}(F)$ est une fonction de λ^ω dans λ qui satisfait (#4) dans $\boldsymbol{M}$. Or, considérons $X := \{\boldsymbol{j}(\xi) \mid \xi < \lambda\}$, et supposons, en vue d'une contradiction, que X est dans $\boldsymbol{M}$. Par (#4), il doit exister s dans X^ω vérifiant $\boldsymbol{j}(F)(s) = \kappa_0$. En notant s_n le $n^{\text{ième}}$ terme de s, pour chaque n, il existe ξ_n vérifiant $s_n = \boldsymbol{j}(\xi_n)$, et on a donc $s = \boldsymbol{j}(s')$ où s' est la suite dont le $n^{\text{ième}}$ terme est ξ_n, puis

$$\kappa_0 = \boldsymbol{j}(F)(s) = \boldsymbol{j}(F)(\boldsymbol{j}(s')) = \boldsymbol{j}(F(s')).$$

Cela est impossible puisque κ_0 n'est pas dans $\mathrm{Im}(\boldsymbol{j})$. L'hypothèse que X appartient à $\boldsymbol{M}$ est donc contradictoire. $\square$

2.1.3.— À partir de là, on déduit directement la borne annoncée.

Proposition (borne de Kunen).— *Il n'existe pas de plongement élémentaire de $\boldsymbol{V}$ dans $\boldsymbol{V}$.*

Démonstration. Si on avait $\boldsymbol{j} : \boldsymbol{V} \xrightarrow{\prec} \boldsymbol{V}$, alors 2.1.2 impliquerait $V_{\lambda+1} \not\subseteq \boldsymbol{V}$, ce qui est absurde. $\square$

▷ *On rappelle que, lorsqu'il est question d'un plongement élémentaire $\boldsymbol{j}$, on ne suppose pas nécessairement $\boldsymbol{j}$ définissable, mais on suppose que $\boldsymbol{j}$ est une classe* pour $\boldsymbol{V}$*, c'est-à-dire qu'il est légitime d'utiliser $\boldsymbol{j}$ dans une définition ensembliste par compréhension ou remplacement, comme par exemple dans la démonstration de* 2.1.2*. Le résultat de* 2.1.3 *ne contredit donc pas l'existence de* $0^\sharp$*, qui, par* XIII.3.2.6*, équivaut à l'existence d'un plongement élémentaire de $\boldsymbol{L}$ dans $\boldsymbol{L}$: la compatibilité avec* 2.1.3 *exige seulement qu'un tel plongement ne soit pas une classe pour $\boldsymbol{L}$, c'est-à-dire soit invisible depuis $\boldsymbol{L}$.* ◁

2.1.4.— Eu égard à 2.1.2, le résultat de clôture maximal non *a priori* exclu à ce point est donc la condition, sur laquelle on reviendra plus loin,

I_2 : « Il existe $\boldsymbol{j} : \boldsymbol{V} \xrightarrow{\prec} \boldsymbol{M}$ satisfaisant $V_\lambda \subseteq \boldsymbol{M}$ avec $\lambda = \sup_{n<\omega} \boldsymbol{j}^n(\mathrm{cr}(\boldsymbol{j}))$ ».

2.1.5.— D'un autre côté, on peut également considérer des plongements élémentaires dont la source est un ensemble V_α et non l'univers $\boldsymbol{V}$ entier. L'argument de 2.1.2 n'exclut alors pas la possibilité d'un plongement élémentaire non trivial de V_α dans lui-même, mais il introduit une borne supérieure sur les valeurs possibles de l'ordinal α.

Lemme.— *Supposons que j est un plongement élémentaire non trivial de V_α dans V_α. Posons $\lambda := \sup_{n<\omega} j^n(\mathrm{cr}(j))$. On a alors soit $\alpha = \lambda$, soit $\alpha = \lambda + 1$, et λ est le plus petit point fixe de j au-dessus de* $\mathrm{cr}(j)$.

Démonstration. L'hypothèse que j est non trivial implique l'existence de $\mathrm{cr}(j)$. Comme plus haut, posons $\kappa := \mathrm{cr}(j)$ et $\kappa_0 := \kappa$ puis, inductivement, $\kappa_n = j(\kappa_{n-1})$ pour $n \geqslant 1$, et $\lambda := \sup_n \kappa_n$. Par hypothèse, κ_0 appartient au domaine de j. Par construction, chaque ordinal κ_n est dans V_α, et on a donc $\alpha \geqslant \sup_n \kappa_n$, soit $\alpha \geqslant \lambda$.

Supposons $\alpha \geqslant \lambda + 2$. Comme dans la démonstration de 2.1.2, soit $F : \lambda^\omega \to \lambda$ satisfaisant (#4). Par construction, la fonction F appartient à $V_{\lambda+2}$, donc $j(F)$ est définie et, par élémentarité de j, la fonction $j(F)$ satisfait elle aussi (#4) puisque cette formule, qui s'écrit

$$\forall X{\in}\mathfrak{P}_\lambda(\lambda)\ \forall\gamma{\in}\lambda\ \exists s{\in}X^\omega\ (F(s) = \gamma),$$

ne met en jeu que des paramètres, à savoir $\mathfrak{P}_\lambda(\lambda)$, λ, et ω, appartenant à $V_{\lambda+2}$ et invariants par $\boldsymbol{j}$. Or, comme précédemment, on obtient une contradiction en considérant l'ensemble $X = \{\boldsymbol{j}(\xi) \mid \xi \in \lambda\}$, qui appartient à $\mathfrak{P}_\lambda(\lambda)$ mais est tel que, quel que soit s dans X^ω, on ne peut avoir $j(F)(s) = \kappa$. Donc, $\alpha \geqslant \lambda + 2$ est contradictoire, et les seules possibilités restantes sont $\alpha = \lambda$ et $\alpha = \lambda + 1$.

Pour le dernier point, tout ordinal ξ dans $[\kappa_0, \lambda[$ appartient à un unique intervalle $[\kappa_n, \kappa_{n+1}[$. Alors, $j(\xi)$ appartient à $[\kappa_{n+1}, \kappa_{n+2}[$, et ne peut être égal à ξ. □

2.1.6.— Nous obtenons ainsi deux nouvelles conditions :
I1 : « Il existe $j : V_{\lambda+1} \xrightarrow{\preceq} V_{\lambda+1}$ avec $\lambda = \sup_{n<\omega} j^n(\mathrm{cr}(j))$ »,
I3 : « Il existe $j : V_\lambda \xrightarrow{\preceq} V_\lambda$ avec $\lambda = \sup_{n<\omega} j^n(\mathrm{cr}(j))$ ».

2.1.7.— Par 1.1.2, tant I_1 que I_2 impliquent I_3. En fait, comme le suggère la terminologie, I_1, I_2, et I_3 forment une suite monotone.

Proposition (axiomes I_1–I_3).— *L'axiome I_1 entraîne I_2, qui entraîne I_3.*

Démonstration (esquisse). Le point est que I_2 (dont il n'est pas *a priori* clair qu'il soit ensembliste), équivaut à la condition ensembliste
« Il existe $j : V_\lambda \xrightarrow{\preceq} V_\lambda$ avec $\lambda = \sup_{n<\omega} j^n(\mathrm{cr}(j))$,
et, pour toute $R \subseteq V_\lambda$ bien fondée, $\bigcup_{\alpha<\lambda} j(R \cap V_\alpha)$ est bien fondée » :
le caractère suffisant de cette condition vient de ce qu'elle garantit l'itérabilité (bonne fondation des itérés) d'une approximation de j par une ultrapuissance et, de là, l'extension à toute la classe $\boldsymbol{V}$. Il est alors facile de voir que I_1 entraîne cette forme de I_2, et clair que I_3 en est une version faible. □

▷ *Les implications précédentes sont fortes, au sens où la satisfaction de la prémisse en un cardinal λ entraîne l'existence non seulement d'un plongement élémentaire témoignant de la conclusion, mais même l'existence d'une famille de plongements élémentaires en témoignant dont les cardinaux critiques sont non bornés sous λ.* ◁

2.1.8.— Pour terminer, on peut encore mentionner
I0 : « Il existe $j : \boldsymbol{L}[V_{\lambda+1}] \xrightarrow{\preceq} \boldsymbol{L}[V_{\lambda+1}]$ avec $\lambda = \sup_{n<\omega} j^n(\mathrm{cr}(j))$ »,
qui, au-dessus de I_1, est à peu près le plus fort des axiomes de grands cardinaux introduits à ce jour.

▷ *En présence de I_0, on peut établir un parallèle entre ω et λ, de sorte que le modèle $\boldsymbol{L}[V_{\lambda+1}]$ présente des analogies avec le modèle $\boldsymbol{L}[V_{\omega+1}]$, c'est-à-dire $\boldsymbol{L}[\mathbb{R}]$, menant à une sorte de théorie descriptive des ensembles au niveau λ.* ◁

2.2. Les cardinaux de Laver

▶ Résumé.— Les cardinaux de Laver sont des points fixes pour l'autosimilarité. Ils dépassent tous les cardinaux précédemment introduits. ◀

2.2.1.— Dans toute la suite, on se concentre sur la situation de l'axiome I_3. Il est alors commode d'introduire une terminologie spécifique.

Définition (cardinal de Laver).— Un cardinal λ est *de Laver* s'il est limite et s'il existe un plongement élémentaire non trivial de V_λ dans V_λ ; un couple (j, κ) vérifiant $j : V_\lambda \xrightarrow{\preceq} V_\lambda$ et $\kappa = \mathrm{cr}(j)$ est appelé *témoin* pour λ.

2.2.2.— On a vu en 2.1.6 que tout cardinal de Laver est fortement limite, borne supérieure d'une ω-suite de cardinaux mesurables. On va montrer qu'il est bien plus que cela, et surpasse (de beaucoup) tous les grands cardinaux considérés jusqu'à présent. Pour cela, on introduit deux notions intermédiaires.

Définition (cardinal m-géant).— Un cardinal κ est appelé *m-géant* s'il existe un plongement élémentaire $\boldsymbol{j} : \boldsymbol{V} \xrightarrow{\preceq} \boldsymbol{M}$ d'ordinal critique κ vérifiant ${}^{\boldsymbol{j}^m(\kappa)}\boldsymbol{M} \subseteq \boldsymbol{M}$.

Par 1.1.6, un cardinal est 0-géant si, et seulement si, il est mesurable.

> ▷ *La définition du caractère m-géant ressemble à celle d'un cardinal supercompact, la différence étant qu'elle inclut une auto-référence supplémentaire : pour un cardinal λ-supercompact, on demande un plongement élémentaire dont le modèle-but est clos par λ-suite, alors que, pour un cardinal 1-géant, on demande que le modèle-but soit clos par $\boldsymbol{j}(\kappa)$-suite, qui dépend lui-même de $\boldsymbol{j}$. La condition ${}^{\boldsymbol{j}(\kappa)}\boldsymbol{M} \subseteq \boldsymbol{M}$ est à la fois plus forte que la condition ${}^{\lambda}\boldsymbol{M} \subseteq \boldsymbol{M}$ du cas λ-supercompact, qui s'accompagne de $\boldsymbol{j}(\kappa) > \lambda$, mais, en même temps, elle n'a aucune raison d'impliquer la λ-supercompacité pour $\lambda > \boldsymbol{j}(\kappa)$. De fait, on peut montrer que, s'il existe, le premier cardinal 1-géant est plus petit que le premier cardinal supercompact. En revanche, en termes de consistance, on verra ci-dessous que l'existence de cardinaux géants est une hypothèse (beaucoup) plus forte que celle de cardinaux supercompacts*[1].
>
> *La définition de cardinal m-géant peut être prolongée au-delà des entiers : il devrait être clair que la condition I_2 signifie que κ est ω-géant, et que la borne de Kunen implique qu'il ne peut exister de cardinal $(\omega+1)$-géant.* ◁

2.2.3.— Comme pour la supercompacité en 1.3.6, on montre que le caractère géant s'exprime par l'existence d'un ultrafiltre convenable. La notion d'ultrafiltre complet et normal considérée ci-dessous est celle de 1.3.5, au remplacement de $\mathfrak{P}_{<\kappa}(\lambda)$ par $\mathfrak{P}(\kappa_m)$ près.

Proposition (géant *vs.* ultrafiltre).— *Un cardinal κ est m-géant si, et seulement si, il existe des cardinaux $\kappa_0 = \kappa < \kappa_1 < \cdots < \kappa_m$ et un ultrafiltre κ-complet normal U sur $\mathfrak{P}(\kappa_m)$ tels que, pour tout $0 \leqslant p < m$, l'ensemble $\{x \in \mathfrak{P}(\kappa_m) \mid \mathrm{ord}(x \cap \kappa_{p+1}) = \kappa_p\}$ est dans U.*

---

1. Ce phénomène d'inversion n'est pas isolé : une hypothèse locale (ne portant que sur des ensembles V_α avec α borné, comme par exemple l'axiome I_1) peut être plus forte en termes de consistance qu'une hypothèse globale (portant sur toute la classe $\boldsymbol{V}$, par exemple la supercompacité ou l'axiome I_2) tout en ne l'impliquant pas nécessairement.

Démonstration. Supposons que $\boldsymbol{j} : \boldsymbol{V} \xrightarrow{\prec} \boldsymbol{M}$ témoigne de ce que κ est m-géant. Pour $0 \leqslant p \leqslant m$, on pose $\kappa_p := \boldsymbol{j}^p(\kappa)$, et on définit

$$U := \{X \subseteq \mathfrak{P}(\kappa_m) \mid \mathrm{Im}(\boldsymbol{j}{\restriction}\kappa_m) \in \boldsymbol{j}(X)\}. \qquad (\#5)$$

Exactement comme en 1.3.6, U est un ultrafiltre κ-complet et normal sur $\mathfrak{P}(\kappa_m)$. De plus, pour $0 \leqslant p < m$, comme on a $\mathrm{Im}(\boldsymbol{j}{\restriction}\kappa_m) \cap \kappa_{p+1} = \mathrm{Im}(\boldsymbol{j}{\restriction}\kappa_{p+1})$, le type d'ordre de $\mathrm{Im}(\boldsymbol{j}{\restriction}\kappa_m) \cap \boldsymbol{j}(\kappa_{p+1})$ est $\boldsymbol{j}(\kappa_p)$, ce qui, par le théorème de Łoś et puisque, par normalité, $\mathrm{Im}(\boldsymbol{j}{\restriction}\kappa_m)$ est la classe de la fonction $\mathrm{id}_{\mathfrak{P}(\kappa_m)}$, signifie que l'ensemble $\{x \in \mathfrak{P}(\kappa_m) \mid \mathrm{ord}(x \cap \kappa_{p+1}) = \kappa_p\}$ est dans U.

Inversement, supposons que $\kappa_0, \ldots, \kappa_m$ et U sont comme dans l'énoncé de la proposition. On considère l'ultrapuissance de $\boldsymbol{V}$ par U, et on note $\boldsymbol{j}_U$ le plongement élémentaire associé de $\boldsymbol{V}$ dans Ult_U. Puisque U est normal, la U-classe de id_{κ_m} est $\mathrm{Im}(\boldsymbol{j}_U{\restriction}\kappa_m)$, et, comme dans le dernier paragraphe de la démonstration de 1.3.6, il en résulte que Ult_U est clos par κ_m-suite. De plus, pour $0 \leqslant p < m$, le type d'ordre de $\mathrm{Im}(\boldsymbol{j}_U{\restriction}\kappa_m) \cap \boldsymbol{j}_U(\kappa_{p+1})$ est κ_{p+1}, ce qui signifie que κ_{p+1} est la U-classe de la fonction $x \mapsto \mathrm{ord}(x \cap \kappa_{p+1})$, laquelle, par hypothèse, est égale U-presque partout à $x \mapsto \kappa_p$, et donc on obtient $\kappa_{p+1} = \boldsymbol{j}_U(\kappa_p)$ pour $0 \leqslant p < m$. Enfin, comme U est supposé κ-complet, on a $j_U(\xi) = \xi$ pour $\xi < \kappa$, tandis que l'on vient de voir $\boldsymbol{j}_U(\kappa) = \kappa_1$. Donc, κ est l'ordinal critique de $\boldsymbol{j}_U$. Alors, $\boldsymbol{j}_U$ témoigne du caractère m-géant de κ. □

2.2.4.— On conclut comme en 1.2.8 et 1.3.7.

Corollaire (ensembliste).— *Pour tout entier m, « être un cardinal m-géant » est une propriété ensembliste.*

2.2.5.— On va maintenant comparer les cardinaux de Laver avec les cardinaux supercompacts de la sous-section 1.3. On procède en plusieurs étapes. La première relie les cardinaux de Laver aux cardinaux géants.

Lemme.— *Si κ est l'ordinal critique d'un plongement élémentaire témoignant que λ est un cardinal de Laver, alors κ est m-géant pour tout m.*

Démonstration. Fixons m. Supposons que (j, κ) témoigne de ce que λ est un cardinal de Laver. Par hypothèse, on a $j : V_\lambda \xrightarrow{\prec} V_\lambda$ avec $\kappa_n := j^n(\kappa)$ et $\lambda = \sup_n \kappa_n$, une hypothèse *a priori* différente de celle $\boldsymbol{j} : \boldsymbol{V} \xrightarrow{\prec} \boldsymbol{M}$ avec ${}^{\kappa_m}\boldsymbol{M} \subseteq \boldsymbol{M}$ de 2.2.2. Mais on peut calquer ce qui a été fait plus haut et poser

$$U := \{X \subseteq \mathfrak{P}(\kappa_m) \mid \mathrm{Im}(j{\restriction}\kappa_m) \in \boldsymbol{j}(X)\},$$

exactement comme en (#5). Alors, U est un ultrafiltre κ-complet normal sur $\mathfrak{P}(\kappa_m)$ et, pour $0 \leqslant p < m$, l'ensemble $\{x \in \mathfrak{P}(\lambda) \mid \mathrm{ord}(x \cap \kappa_{p+1}) = \kappa_p\}$ est dans U : l'argument est le même qu'en 2.2.3, le point étant que l'ensemble $\mathrm{Im}(j{\restriction}\kappa_m)$ appartient à la structure d'arrivée de j, ici V_λ. La seconde moitié de 2.2.3 implique alors que κ est m-géant. □

2.2.6.— Exploitant mieux les propriétés d'autosimilarité des cardinaux de Laver, on voit que ceux-ci surpassent (de beaucoup) les cardinaux géants.

Proposition (Laver *vs.* géant).— *Si λ est un cardinal de Laver, il existe λ cardinaux plus petits que λ qui sont m-géants pour tout m.*

Démonstration. Supposons que (j, κ) témoigne de ce que λ est un cardinal de Laver. Par 2.2.5, κ est m-géant pour tout m. Par la caractérisation de 2.2.3, la propriété pour κ d'être m-géant est une propriété de V_{κ_m+2}, donc *a fortiori* de V_λ, et on a donc $V_\lambda \models \forall m$ (« κ est m-géant »). Soit U l'ultrafiltre normal sur κ associé à j suivant (#1), et soit $A := \{\xi < \kappa \mid V_\lambda \models \forall m\,(« \xi \text{ est } m\text{-géant} »)\}$. Par élémentarité de j, on obtient $j(A) := \{\xi < j(\kappa) \mid V_\lambda \models \forall m\,(« \xi \text{ est } m\text{-géant} »)\}$, et le lemme 2.2.5 implique $\kappa \in j(A)$, d'où $A \in U$. On déduit en particulier

$$V_\lambda \models \|\{\xi < \kappa \mid \forall m\,((« \xi \text{ est } m\text{-géant} »))\}\| = \kappa,$$

puis, en appliquant j de façon répétée,

$$V_\lambda \models \|\{\xi < \kappa_n \mid \forall m\,(« \xi \text{ est } m\text{-géant} »)\}\| = \kappa_n \text{ pour tout } n,$$

et finalement le résultat annoncé en passant à la borne supérieure sur n. □

2.2.7.— Pour achever la comparaison des cardinaux de Laver avec les cardinaux supercompacts, il suffit donc désormais de comparer les cardinaux géants et les cardinaux supercompacts.

▷ *Le résultat que l'on montre ci-dessous n'est pas optimal ; en particulier, on saute par-dessus plusieurs notions intermédiaires possibles, dont les cardinaux* extensibles*, définis par la condition que κ est extensible si, pour tout $\alpha > \kappa$, il existe β et un plongement élémentaire $j : V_\alpha \xrightarrow{\prec} V_\beta$ d'ordinal critique κ. Comme on l'a déjà signalé, dans tous les cas, on ne peut espérer établir qu'un résultat de consistance relative, et pas une implication, entre les cardinaux géants, définis par des hypothèses locales, et les cardinaux extensibles ou supercompacts, définis par des hypothèses globales.* ◁

2.2.8. Proposition (géant *vs.* supercompact).— *Si κ est un cardinal 2-géant, alors, dans le modèle $(V_\kappa, \in)$ de* ZFC*, il existe une classe non bornée de cardinaux supercompacts.*

Démonstration. Supposons que κ est 2-géant et que $\boldsymbol{j} : \boldsymbol{V} \xrightarrow{\prec} \boldsymbol{M}$ en témoigne. Alors, κ est *a fortiori* 0-géant, donc mesurable, donc inaccessible, et donc $(V_\kappa, \in)$ est un modèle de ZFC. Considérons la propriété

$$\exists \boldsymbol{k} : \boldsymbol{V} \xrightarrow{\prec} \boldsymbol{M}\,(\mathrm{cr}(\boldsymbol{k}) = \xi \wedge \eta = \boldsymbol{k}(\xi) \wedge {}^\eta\boldsymbol{M} \subseteq \boldsymbol{M}),$$

qui exprime que ξ est 1-géant et qu'il existe un plongement élémentaire $\boldsymbol{k}$ en témoignant qui envoie ξ sur η : par 2.2.3, c'est une propriété ensembliste, équivalant à l'existence d'un ultrafiltre d'un certain type sur $\mathfrak{P}(\eta)$, donc à une propriété de $V_{\eta+2}$, et qui peut être exprimée par une formule ensembliste $\Phi(\xi, \eta)$.

Puisque κ est 2-géant, il est en particulier 1-géant, et la formule $\Phi(\kappa, \boldsymbol{j}(\kappa))$ est satisfaite dans $\boldsymbol{V}$, donc aussi dans $\boldsymbol{M}$, puisque l'on a $V^{\boldsymbol{M}}_{\boldsymbol{j}(\kappa)+2} = V_{\boldsymbol{j}(\kappa)+2}$. Soit

$$A := \{\xi < \kappa \mid \boldsymbol{V} \models \Phi(\xi, \kappa)\}.$$

On a alors $\boldsymbol{j}(A) := \{\xi < \boldsymbol{j}(\kappa) \mid \boldsymbol{M} \models \Phi(\xi, \boldsymbol{j}(\kappa))\}$, d'où $\kappa \in \boldsymbol{j}(A)$ puis $A \in U$, où U est l'ultrafiltre κ-complet associé à $\boldsymbol{j}$ par (#1). Or, soit ξ un élément de A. Par définition, on a $\boldsymbol{V} \models \Phi(\xi, \kappa)$, d'où $\boldsymbol{M} \models \Phi(\xi, \kappa)$ puisque $V^{\boldsymbol{M}}_{\kappa+2}$ et $V_{\kappa+2}$ coïncident. L'ultrafiltre U est normal, donc κ est la U-classe de id_κ. Par le théorème de Łoś, $\boldsymbol{M} \models \Phi(\xi, \kappa)$ entraîne $\{\eta < \kappa \mid \Phi(\xi, \eta)\} \in U$, et, de là, $\{\eta < \kappa \mid \Phi(\xi, \eta)\}$ est non borné dans κ. Revenant à la définition, on déduit, pour tout ξ dans A,

$$(V_\kappa, \in) \models \forall \zeta\ \exists \eta{>}\zeta\ \exists \boldsymbol{k} : \boldsymbol{V} \xrightarrow{\prec} \boldsymbol{M}\,(\mathrm{cr}(\boldsymbol{k}) = \xi \wedge \boldsymbol{k}(\xi) = \eta \wedge {}^\eta\boldsymbol{M} \subseteq \boldsymbol{M}),$$

qui implique *a fortiori*

$$(V_\kappa, \in) \models \forall \zeta\ \exists \boldsymbol{k} : \boldsymbol{V} \xrightarrow{\prec} \boldsymbol{M}\,(\mathrm{cr}(\boldsymbol{k}) = \xi \wedge {}^\zeta\boldsymbol{M} \subseteq \boldsymbol{M}),$$

montrant que ξ est supercompact dans $(V_\kappa, \in)$. □

Corollaire (existence d'un cardinal de Laver).— *La consistance du système* ZFC+ *« il existe un cardinal de Laver » entraîne celle du système* ZFC+ *« il existe une classe propre de cardinaux supercompacts ». En revanche, la consistance de* ZFC+ *« il existe un cardinal supercompact » n'entraîne pas celle de* ZFC+ *« il existe un cardinal de Laver ».*

2.2.9.— Récapitulant les résultats de comparaison, on a montré

« il existe un cardinal de Laver »
$\Rrightarrow$ « il existe un cardinal géant »
($\Rrightarrow$) « il existe cardinal supercompact »
$\Rrightarrow$ « il existe un cardinal de Woodin »
$\Rrightarrow$ « il existe un cardinal fort »
$\Rrightarrow$ « il existe un cardinal mesurable »
$\Rrightarrow$ « $0^\sharp$ existe »
$\Rrightarrow$ « il existe un cardinal faiblement compact »
$\Rrightarrow$ « il existe un cardinal inaccessible »
$\Rrightarrow$ « il existe un cardinal non dénombrable »
$\Rightarrow$ « il existe un cardinal infini »,

où $\Rrightarrow$ indique non seulement une implication, mais même que, si κ a la propriété indiquée, il est le $\kappa^{\text{ième}}$ à avoir la propriété suivante. La parenthèse indique un résultat en terme de consistance.

2.3. Itérations d'un plongement élémentaire

► Résumé.— La famille des plongements élémentaires associés à un cardinal de Laver est munie d'une opération autodistributive. ◄

2.3.1.— La coïncidence de la source et du but des plongements élémentaires liés aux cardinaux de Laver entraîne l'existence d'une structure algébrique spécifique, lié à la possibilité d'*appliquer* un plongement élémentaire à un autre. La propriété de préservation universelle des plongements élémentaires implique alors que l'opération algébrique ainsi obtenue obéit à la loi d'autodistributivité, et on va établir en particulier que la famille des itérés d'un plongement est une SD-structure libre à un générateur.

Notation.— Si λ est un ordinal limite, on note $\mathcal{E}_\lambda^+$ (*resp.,* $\mathcal{E}_\lambda$) la famille de tous les plongements élémentaires (*resp.,* plongements élémentaires non triviaux) de $(V_\lambda, \in)$ dans lui-même.

On a donc $\mathcal{E}_\lambda^+ = \mathcal{E}_\lambda \cup \{\mathrm{id}_{V_\lambda}\}$, et $\mathcal{E}_\lambda$ est non vide si, et seulement si, λ est un cardinal de Laver.

2.3.2.— On introduit alors une opération binaire sur les plongements élémentaires en partant de l'*application* d'une fonction à son argument.

Définition (application).— Pour λ limite et i, j dans $\mathcal{E}_\lambda^+$, on pose

$$i[j] := \bigcup_{\gamma<\lambda} i(j\restriction V_\gamma), \tag{\#6}$$

et on dit que $i[j]$ est obtenue en *appliquant* i à j.

La formule (#6) fait sens puisque $x \in V_\gamma$ entraîne $j(x) \in V_{j(\gamma)}$, et, de là, $j\restriction V_\gamma \subseteq V_\gamma \times V_{j(\gamma)}$, d'où $j\restriction V_\gamma \in V_{j(\gamma)+3}$, puis $j\restriction V_\gamma \in V_\lambda$, et par conséquent l'image par i de $j\restriction V_\gamma$ est bien définie. Noter que la définition implique, pour tous i et j dans $\mathcal{E}_\lambda^+$ et pour tout $\gamma < \lambda$,

$$i[j]\restriction V_{i(\gamma)} = i(j\restriction V_\gamma), \tag{\#7}$$

ainsi que

$$i[\mathrm{id}_{V_\lambda}] = \mathrm{id}_{V_\lambda} \quad \text{et} \quad \mathrm{id}_{V_\lambda}[j] = j. \tag{\#8}$$

$\triangleright$ *Insistons fortement sur le fait qu'appliquer un plongement élémentaire à un autre n'est* pas *les composer : (#8) le montre. Pour une autre illustration, supposant j dans $\mathcal{E}_\lambda$, et soit κ l'ordinal critique de j. Alors, $j \circ j$ envoie κ sur $j(j(\kappa))$ et, puisque l'on a $\kappa < j(\kappa)$ par hypothèse, on déduit $\kappa < j(\kappa) < j(j(\kappa))$ puisque j est élémentaire. Or, on a $j\restriction V_\kappa = \mathrm{id}_{V_\kappa}$, d'où $j(j\restriction V_\kappa) = j[j]\restriction V_{j(\kappa)} = \mathrm{id}_{V_{j(\kappa)}}$. Donc, puisque κ appartient à $j(\kappa)$, on en déduit $j[j](\kappa) = \kappa$, et donc $j[j](\kappa) < (j \circ j)(\kappa)$, soit certainement $j[j] \neq j \circ j$.* $\triangleleft$

2.3.3.— Le point fondamental pour la suite est que l'application définit une opération interne dans $\mathcal{E}_\lambda^+$.

Lemme.— *Pour tous i, j dans $\mathcal{E}_\lambda^+$, l'ensemble $i[j]$ appartient à $\mathcal{E}_\lambda^+$. De plus, $j \neq \mathrm{id}_{V_\lambda}$ entraîne $i[j] \neq \mathrm{id}_{V_\lambda}$, et on a alors*

$$\mathrm{cr}(i[j]) = i(\mathrm{cr}(j)). \tag{\#9}$$

Démonstration. Quand γ parcourt les ordinaux moindres que λ, les différentes applications $j\restriction V_\gamma$ sont deux à deux compatibles puisque toutes incluses dans j. Par élémentarité de i, il en est de même des différentes applications $i(j\restriction V_\gamma)$, et donc $i[j]$ est une application de V_λ dans lui-même.

Soit $\Phi(\vec{x})$ est une formule ensembliste. Pour tout $\vec{a}$ dans V_λ, puisque j est un plongement élémentaire, $(V_\lambda, \in) \models \Phi(\vec{a})$ équivaut à $(V_\lambda, \in) \models \Phi(j(\vec{a}))$. Si $\vec{a}$ appartient à V_γ, alors $j(\vec{a})$ est aussi $j\restriction V_\gamma(\vec{a})$ et, par conséquent, en notant $\Psi(f)$ la formule $\forall \vec{x} {\in} \mathrm{Dom}(f)\, (\Phi(\vec{x}) \Leftrightarrow \Phi(f(\vec{x})))$, alors $\Psi(j\restriction V_\gamma)$ est satisfaite pour tout $\gamma < \lambda$. Puisque i est un plongement élémentaire, il en est de même de la formule $\Psi(i(j\restriction V_\gamma))$, ce qui signifie que, pour tout $\vec{a}$ dans le domaine de $i(j\restriction V_\gamma)$, on a

$$\Phi(\vec{a}) \Leftrightarrow \Phi(i(j\restriction V_\gamma))(\vec{a}).$$

Par cohérence des applications $i(j\restriction V_\gamma)$, cela signifie que, pour tout $\vec{a}$ dans V_λ, la formule $\Phi(\vec{a})$ est satisfaite si, et seulement si, $\Phi(i[j](\vec{a}))$ l'est, et donc $i[j]$ est un plongement élémentaire de V_λ dans lui-même.

Supposons $j \neq \mathrm{id}_{V_\lambda}$, et soit κ l'ordinal critique de j. Par définition, la formule $\forall \alpha{<}\kappa\, (j(\alpha) = \alpha)$ est satisfaite, et il en est de même de la formule équivalente $\forall \alpha{<}\kappa\, ((j\restriction V_\kappa)(\alpha) = \alpha)$, une formule ensembliste avec une variable liée α et deux paramètres, κ et $j\restriction V_\kappa$. Puisque i est un plongement élémentaire, est également satisfaite la formule obtenue en appliquant i à tous les paramètres, c'est-à-dire en remplaçant κ par $i(\kappa)$ et $j\restriction V_\kappa$ par $i(j\restriction V_\kappa)$. On a donc

$$\forall \alpha{<}i(\kappa)\, (i(j\restriction V_\kappa)(\alpha) = \alpha).$$

Par définition, $i(j\restriction V_\kappa)$ est une restriction de $i[j]$, et on a aussi

$$\forall \alpha{<}i(\kappa)\, (i[j](\alpha) = \alpha). \tag{\#10}$$

De la même façon, on a $j(\kappa) > \kappa$, donc $(j{\restriction}V_{\kappa+1})(\kappa) > \kappa$, d'où, en appliquant i, l'inégalité $i(j{\restriction}V_{\kappa+1})(i(\kappa)) > i(\kappa)$, et finalement $i[j](i(\kappa)) > i(\kappa)$. De là, $i[j]$ n'est pas l'identité et, par (#10), son ordinal critique est $i(\kappa)$, d'où (#9). □

2.3.4.— Ensuite, l'élémentarité des plongements implique que l'opération d'application sur $\mathcal{E}_\lambda^+$ obéit à une loi algébrique simple.

Lemme.— *Pour tous i, j, k dans $\mathcal{E}_\lambda^+$, on a*

$$i[j[k]] = i[j][i[k]]. \tag{\#11}$$

Démonstration. Soient i, j, $k \in \mathcal{E}_\lambda$ et $\gamma < \lambda$. Il existe $\beta < \lambda$ tel que $k{\restriction}V_\gamma$ appartient à V_β. Par définition, on a $j[k]{\restriction}V_{j(\gamma)} = (j{\restriction}V_\beta)(k{\restriction}V_\gamma)$. En appliquant i à cette égalité, on déduit

$$i(j[k]{\restriction}V_{j(\gamma)}) = i(j{\restriction}V_\beta)[i(k{\restriction}V_\gamma)].$$

Le terme de gauche est la restriction de $i[j[k]]$ à $V_{i(j(\gamma))}$, tandis que celui de droite est la restriction de $i[j][i[k]]$ à $V_{i(j(\gamma))}$, puisque $i(j(\gamma))$ et $i[j](i(\gamma))$ sont égaux. Comme γ est quelconque, (#11) s'ensuit. □

2.3.5.— La relation (#11) exprime que la structure algébrique $(\mathcal{E}_\lambda, \text{-[-]})$ obéit à la loi d'*autodistributivité* (à gauche) : l'opération -[-] est distributive par rapport à elle-même. On fixe ici une terminologie spécifique.

Définition (SD-structure).— Une SD-*structure* [2] (à gauche) est une structure algébrique $(S, *)$ telle que $*$ est une opération binaire sur S obéissant à la loi [3] d'autodistributivité à gauche [4]

$$(\mathrm{SD}) : x * (y * z) = (x * y) * (x * z).$$

Exemples. Si X est un ensemble et f une application de X dans X, et que, pour x, y dans X, on pose $x{*}y := f(y)$, alors $(X, *)$ est une SD-structure (triviale).

Si G est un groupe et que, pour x, y dans G, on pose $x * y := xyx^{-1}$, alors $(G, *)$ est une SD-structure.

Si E un R-module et que, pour x, y dans E, on pose $x * y := (1 - \lambda)x + \lambda y$ avec $\lambda \in R$, alors $(E, *)$ est une SD-structure.

Si $\mathfrak{I}_\mathbb{N}$ est l'ensemble des injections de $\mathbb{N}$ dans $\mathbb{N}$ et que, pour f, g dans $\mathfrak{I}_\mathbb{N}$, on définit $f * g$ par $(f * g)(n) := f(g(f^{-1}(n)))$ pour $n \in \mathrm{Im}(f)$, et $(f * g)(n) := n$ sinon, alors $(\mathfrak{I}_\mathbb{N}, *)$ est une SD-structure.

Enfin, si B_∞ est le groupe des tresses d'Artin à une infinité de brins, c'est-à-dire le groupe engendré par une suite infinie d'éléments $\sigma_1, \sigma_2, \ldots$ soumis aux relations $\sigma_i\sigma_j = \sigma_j\sigma_i$ pour $|i - j| \geqslant 2$ et $\sigma_i\sigma_j\sigma_i = \sigma_j\sigma_i\sigma_j$ pour $|i - j| = 1$ et que, pour x, y dans B_∞, on pose $x * y := x\,\mathrm{sh}(y)\,\sigma_1\,\mathrm{sh}(x)^{-1}$, où sh est l'endomorphisme de B_∞ défini par $\mathrm{sh}(\sigma_i) := \sigma_{i+1}$ pour tout i, alors $(B_\infty, *)$ est une SD-structure (remarquable), voir [16].

2. Divers noms ont été employés pour de telles structures : « LD-système », « LD-groupoïde », *etc.* Une terminologie désormais usuelle en topologie de basse dimension (en anglais) est « shelf ».

3. C'est-à-dire satisfaisant la formule $\forall x, \mathsf{y}, \mathsf{z}\,(\ldots)$.

4. Là aussi, plusieurs notations apparaissent dans la littérature, dont « LD »(pour « left (self)-distributivity »), et « SD » pour « (left) self-distributivity », qui a l'avantage de mettre l'accent sur « self », le point important.

Avec cette terminologie, 2.3.4 exprime que, pour tout ordinal limite λ, les structures $(\mathcal{E}_\lambda, \text{-[-]})$ et $(\mathcal{E}_\lambda^+, \text{-[-]})$ sont des SD-structures, résultat dont le contenu n'est réel que si λ est un cardinal de Laver : autrement, $(\mathcal{E}_\lambda^+, \text{-[-]})$ est la SD-structure triviale à un élément, et $(\mathcal{E}_\lambda, \text{-[-]})$ est vide et donc, conformément aux définitions du chapitre VII, n'est pas une structure.

2.3.6.— La définition entraîne directement que le composé de deux plongements élémentaires est un plongement élémentaire. Par conséquent, la composition est une seconde opération binaire définie sur $\mathcal{E}_\lambda$ et $\mathcal{E}_\lambda^+$. Il est standard que la composition est associative, et que id_{V_λ} est élément neutre, donc $(\mathcal{E}_\lambda, \circ)$ est un semi-groupe, et $(\mathcal{E}_\lambda^+, \circ, \mathrm{id}_{V_\lambda})$ un monoïde. Il est facile de vérifier que l'application et la composition sont reliées par les relations suivantes, valables pour tous i, j, k dans $\mathcal{E}_\lambda^+$:

$$i \circ j = i[j] \circ i, \tag{\#12}$$

$$(i \circ j)[k] = i[j[k]], \tag{\#13}$$

$$i[j \circ k] = i[j] \circ i[k], \tag{\#14}$$

ce que l'on exprimera en déclarant que $(\mathcal{E}_\lambda^+, \text{-[-]}, \circ)$ est une SD$^+$-*structure.*

2.3.7.— Pour tout plongement élémentaire j dans $\mathcal{E}_\lambda$, il est alors naturel de considérer les sous-structures de $\mathcal{E}_\lambda$ et $\mathcal{E}_\lambda^+$ engendrées par j.

Définition (itéré).— Pour j dans $\mathcal{E}_\lambda$, on note $\mathrm{Iter}(j)$ et $\mathrm{Iter}^+(j)$ les sous-structures de $(\mathcal{E}_\lambda, \text{-[-]})$ et $(\mathcal{E}_\lambda^+, \text{-[-]}, \circ)$, respectivement, engendrées par j ; leurs éléments sont appelés les *itérés purs* (*resp.*, les *itérés*) de j.

> *Exemple. Des itérés purs typiques de j sont $j[j]$, $j[j][j]$, etc., donc l'évaluation en j de termes en l'opération* -[-]. *Pour des itérés quelconques, on peut utiliser de surcroît la composition, comme dans $j \circ j$ ou $(j \circ j[j])[j]$.*

2.3.8.— L'énoncé suivant résume les acquis à ce point.

Proposition (SD-structure I).— *Si λ est un cardinal de Laver, alors, pour tout j dans $\mathcal{E}_\lambda$, la structure* $\mathrm{Iter}(j)$ *est une SD-structure infinie monogène, et* $\mathrm{Iter}^+(j)$ *est une* SD$^+$*-structure infinie monogène.*

> *Démonstration.* Les SD et SD$^+$-structures sont définies par des lois algébriques, donc toute sous-structure d'une telle structure en est une. Par ailleurs, $\mathrm{Iter}(j)$ et $\mathrm{Iter}^+(j)$ sont engendrées par j donc sont monogènes. Le seul point à justifier est que $\mathrm{Iter}(j)$ est infini. Définissons j_n par $j_0 := j$ et $j_n := j[j_{n-1}]$ pour $n \geqslant 1$. Par définition, tous les plongements j_n sont dans $\mathrm{Iter}(j)$. Soit $\kappa := \mathrm{cr}(j)$. De (#9) on déduit $\mathrm{cr}(j_n) = j^n(\kappa)$. Or, par définition, on a $\kappa < j(\kappa)$, donc, de proche en proche, la suite $(j^n(\kappa))_{n \geqslant 0}$ est strictement croissante. On déduit donc
>
> $$\mathrm{cr}(j_0) < \mathrm{cr}(j_1) < \mathrm{cr}(j_2) < \cdots,$$
>
> ce qui montre que les plongements j_n sont deux à deux distincts. Enfin, par définition, on a $\mathrm{Iter}(j) \subseteq \mathrm{Iter}^+(j)$, donc $\mathrm{Iter}^+(j)$ est infinie. □

2.3.9.— Mentionnons ici sans démonstration le résultat plus précis suivant, où le point supplémentaire est le caractère *libre* des structures.

▷ *Pour toute variété algébrique $\mathcal{V}$, c'est-à-dire toute classe de structures définie par l'obéissance à des lois algébriques, et pour tout ensemble S, il existe dans $\mathcal{V}$ une structure* libre *de base S, à savoir une structure $\mathcal{F}_S$ de $\mathcal{V}$ telle que toute application de S dans une structure $\mathcal{X}$ de $\mathcal{V}$ se prolonge en un morphisme de $\mathcal{F}_S$ dans $\mathcal{X}$. En d'autres termes, $\mathcal{F}_S$ est un objet initial de la catégorie associée à $\mathcal{V}$: elle est engendrée par S et est la plus générale de toutes les structures de $\mathcal{V}$ engendrées par S, au sens où toute telle structure est un quotient de $\mathcal{F}_S$.* ◁

Proposition (SD-structure II).— *Si λ est un cardinal de Laver, alors, pour tout j dans $\mathcal{E}_\lambda$, la structure* $\mathrm{Iter}(j)$ *est une SD-structure monogène libre, et* $\mathrm{Iter}^+(j)$ *est une* SD^+*-structure monogène libre.*

Démonstration (principe). Le résultat est délicat, et repose sur deux ingrédients (voir [16]) : un critère caractérisant les SD-structures monogènes libres, à savoir (dans le formalisme de -[-]), l'impossibilité de toute égalité de la forme

$$j = j[j_1]\cdots[j_n] \text{ avec } n \geqslant 1, \qquad (\#15)$$

puis la vérification de (#15) dans le cas de $\mathrm{Iter}(j)$, qui est facile à partir des calculs de la sous-section 3.2. □

Ce résultat implique en particulier que, à isomorphisme près, les structures algébriques $\mathrm{Iter}(j)$ et $\mathrm{Iter}^+(j)$ ne dépendent ni du cardinal de Laver λ sous-jacent, ni du choix du plongement élémentaire j dans $\mathcal{E}_\lambda$.

3. Périodes dans les tables de Laver

On va maintenant décrire des applications remarquables des développements précédents mettant en jeu les tables de Laver, qui sont des structures combinatoires finies introduites par une construction inductive simple. De façon plus précise, les tables de Laver sont des tableaux carrés dont les lignes sont périodiques, et on va établir, à l'aide des plongements élémentaires associés à un cardinal de Laver, deux résultats sur ces périodes, à savoir la comparaison des périodes des lignes 1 et 2, et le comportement asymptotique de la période de 1.

▷ *Comme on l'a déjà dit dans l'introduction du chapitre, et même si elle ne contredit aucun résultat général, l'existence d'un lien entre les cardinaux de Laver, des objets gigantesques dont l'existence ne peut pas être établie dans* ZFC *(ni même dans* ZFC+ *« il existe une infinité de cardinaux supercompacts » ...) et des structures combinatoires finies est (très) surprenante.* ◁

Le texte est organisé comme suit. La sous-section 3.1 contient une introduction aux tables de Laver et à leurs périodes, la plupart des démonstrations étant omises. Dans la sous-section 3.2, on montre que les tables de Laver sont des quotients de la structure $\mathrm{Iter}(j)$ associées à un plongement élémentaire. Cela permet, dans la sous-section 3.3, d'utiliser les propriétés des plongements élémentaires et de leurs ordinaux critiques pour établir les propriétés annoncées des périodes des tables de Laver. Dans la sous-section 3.4, on discute brièvement du statut des applications ainsi obtenues. Enfin, un appendice contient les démonstrations des résultats de la sous-section 3.1, élémentaires mais sans rapport avec la théorie des ensembles.

3.1. Les tables de Laver

▶ Résumé.— Pour tout n, la table de Laver A_n est une SD-structure monogène à 2^n éléments, contrepartie autodistributive de $\mathbb{Z}/n\mathbb{Z}$. ◀

3.1.1.— Comme dans 2.3.5, on considère des SD-structures, c'est-à-dire des structures formées d'un ensemble muni d'une opération binaire obéissant à la loi d'autodistributivité à gauche. Le point de départ est l'existence de telles SD-structures finies, à 2^n éléments.

Proposition (table de Laver).— *Pour tout entier $n \geqslant 0$, il existe une unique* SD-*structure A_n de domaine $\{1, \dots, 2^n\}$ vérifiant*

$$p * 1 = p + 1 \text{ pour } p < 2^n, \quad \text{et} \quad 2^n * 1 = 1. \qquad (\#16)$$

La structure A_n est appelée la $n^{\text{ième}}$ table de Laver.

3.1.2.— Élémentaire et purement combinatoire, la démonstration est donnée dans l'appendice. Notons ici que, si l'existence est délicate à établir, l'unicité, elle, est facile : en effet, (#16) prescrit la première colonne de la table de A_n, à partir de quoi on vérifie facilement qu'il existe au plus une façon de compléter la table en déduisant chaque nouvelle valeur des valeurs précédemment calculées suivant une induction rétrograde sur les lignes de 2^n à 1 et, pour chaque ligne, une induction sur les colonnes de 2 à 2^n, c'est-à-dire de gauche à droite et de bas en haut, voir 3.A.2.

Exemple. Suivant les indications ci-dessus, il est facile de calculer, à la main ou avec l'aide d'un programme, les premières tables. Inspecter les valeurs dans A_3 et A_4 est intéressant : dans un premier temps, celles-ci apparaissent mystérieuses, puis on découvre des motifs réguliers qui laissent espérer un schéma explicatif global… avant de s'apercevoir que toute tentative en ce sens est vaine : il est sans espoir de trouver par exemple une formule explicite simple donnant la valeur de $p*q$ dans A_n en fonction de p et q. En dépit de la possibilité de remplir la table par une induction double simple, les tables de Laver sont des objets combinatoires extrêmement compliqués.

3.1.3.— Les tables de Laver occupent, parmi les SD-structures, une place comparable aux groupes cycliques $\mathbb{Z}/n\mathbb{Z}$ parmi les structures associatives : de même que ces derniers, elles peuvent être caractérisées par une présentation en termes d'une unique relation de torsion.

▷ *On a rappelé ci-dessus que, si $\mathcal{V}$ est une variété algébrique et S est un ensemble, toute structure $\mathcal{X}$ de $\mathcal{V}$ engendrée par S est un quotient de la structure*

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	11	12	15	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

FIGURE 1.— Les premières tables de Laver.

libre $\mathcal{F}_S$, c'est-à-dire qu'il existe une congruence[5] $\equiv$ *sur $\mathcal{F}_S$ telle que $\mathcal{X}$ est isomorphe à $\mathcal{F}_S/\equiv$. Si $\equiv$ est engendrée par une famille R de paires d'éléments de $\mathcal{F}_S$ (« relations »), on dit que $\mathcal{X}$ admet la présentation $\langle S \mid R\rangle_{\mathcal{V}}$. Par exemple, on sait qu'un groupe cyclique à n éléments de générateur g admet, en tant que groupe, la présentation $\langle g \mid (g^n, 1)\rangle$, qu'il est usuel de noter $\langle g \mid g^n = 1\rangle$ puisque quotienter par une congruence qui contient la paire $(g^n, 1)$ revient à imposer que les classes de g^n et 1 soient égales dans la structure-quotient.* ◁

3.1.4.— Lorsque la loi d'associativité est obéie, il n'y a pas d'ambiguïté sur la notion de puissance d'un élément puisque les parenthèses n'influent pas. Hors de ce contexte, plusieurs notions de puissances apparaissent.

Définition (puissances).— Si $(S, *)$ est une structure et a un élément de S, on définit inductivement $a_{[k]}$ ($k^{\text{ième}}$ *puissance gauche*) et $a^{[k]}$ ($k^{\text{ième}}$ *puissance droite*) par $a_{[1]} = a^{[1]} := a$ et $a_{[k]} := a_{[k-1]} * a$ et $a^{[k]} := a * a^{[k-1]}$ pour $k > 1$.

3.1.5.— Une induction directe donne $1_{[p]} = p$ pour $p \leqslant 2^n$ dans A_n, puis, par (#16), $1_{[2^n+1]} = 1$. Cette dernière égalité fournit une présentation.

5. C'est-à-dire une relation d'équivalence compatible avec les opérations.

Proposition (présentation).— *Pour tout n, la table de Laver A_n admet la présentation $\langle 1 \mid 1_{[2^n+1]} = 1\rangle_{\mathrm{SD}}$.*

▷ *Que la table A_n soit engendrée par l'élément 1 résulte immédiatement de (#16) : si une sous-structure de A_n contient 1, elle contient aussi $1{*}1$, qui est 2, puis $2{*}1$, qui est 3, etc. jusqu'à 2^n. Le point non trivial est donc de montrer que l'unique relation $1_{[2^n+1]} = 1$ présente A_n, ce qui est fait dans l'appendice.* ◁

3.1.6.— Une conséquence importante de 3.1.5 est que, de même que tout semi-groupe fini à un générateur s'obtient à partir des groupes cycliques $\mathbb{Z}/N\mathbb{Z}$ par produit et ajout d'une chaîne, toute SD-structure monogène finie s'obtient à partir de tables de Laver par des opérations de type produit, duplication d'élément, et ajout de chaîne, voir [28].

3.1.7.— Pour ce qui nous concerne ici, l'intérêt de 3.1.5 est de fournir une caractérisation de A_n parmi les SD-structures monogènes finies.

Corollaire (caractérisation).— *Supposons que S est une* SD-*structure engendrée par un élément g et que $\simeq$ est une congruence sur S. Alors, $S/{\simeq}$ est isomorphe à A_n si, et seulement si, la relation $\simeq$ a 2^n classes d'équivalence, qui sont celles de g, $g_{[2]}, \ldots, g_{[2^n]}$, et on a $g_{[2^n+1]} \simeq g$.*

Démonstration. Par hypothèse, $S/{\simeq}$ est une SD-structure à 2^n éléments. Soit $\mathcal{F}$ la SD-structure libre engendré par un élément 1, et soit $\equiv$ la congruence sur $\mathcal{F}$ telle que A_n est isomorphe à $\mathcal{F}/{\equiv}$. Puisque $\mathcal{F}$ est libre et que S est engendré par g, il existe un morphisme $\phi : \mathcal{F} \to S$ envoyant 1 sur g, donc, par composition, un morphisme $\overline{\phi}$ de $\mathcal{F}$ sur $S/{\simeq}$ envoyant 1 sur la $\simeq$-classe $\overline{g}$ de g. Puisque $\overline{\phi}$ est un morphisme, il envoie $1_{[p]}$ sur la $\simeq$-classe $\overline{g_{[p]}}$ de $g_{[p]}$ pour tout p et donc, par hypothèse, l'image de $\overline{\phi}$ a 2^n éléments. De plus, puisque, toujours par hypothèse, les $\simeq$-classes de $g_{[2^n+1]}$ et de g coïncident, on a $\overline{\phi}(1_{[2^n+1]}) = \overline{\phi}(1)$. De là, $\overline{\phi}$ factorise par $\equiv$, et il induit donc un morphisme surjectif de A_n dans $S/{\simeq}$ dont l'image a 2^n éléments. Puisque A_n a lui-même 2^n éléments, ce morphisme est un isomorphisme. □

3.1.8.— Comme on l'a dit plus haut, les tables de Laver, en dépit de leur définition simple, sont des objets combinatoires compliqués. Un paramètre important dans leur description est le nombre de valeurs distinctes apparaissant dans chaque ligne. Le point de départ pour l'étude de ce paramètre est l'observation suivante.

Proposition (période).— *Pour tout n et tout $p \leqslant 2^n$, il existe un entier $\pi_n(p)$, qui est une puissance de 2, tel que la ligne de p dans la table de A_n consiste en la répétition périodique de $\pi_n(p)$ valeurs croissant de $p+1$ à 2^n (cas $p < 2^n$) ou de 1 à 2^n (cas $p = 2^n$).*

Exemple. On a toujours $\pi_n(2^n) = 2^n$, et $\pi_n(2^n-1) = 1$. Pour les autres valeurs, il n'existe pas de formule simple. Sur la table de A_3, on lit

$$\pi_3(1) = 4,\quad \pi_3(2) = 4,\quad \pi_3(3) = 2,\quad \pi_3(4) = 4,\quad \pi_3(5) = 2,\quad \pi_3(6) = 2.$$

L'entier $\pi_n(p)$ sera naturellement appelé la *période* de p dans A_n. Suivant 3.1.8, $\pi_n(p)$ est le nombre de valeurs distinctes apparaissant dans la $p^{\text{ième}}$ ligne de la table de A_n. Une fois encore, la démonstration de la proposition est repoussée à l'appendice.

3.1.9.— L'étude des périodes $\pi_n(p)$ est la question qui va nous occuper dans la suite de cette sous-section. Le point de départ est l'existence d'une projection de A_n sur A_{n-1}, un cas particulier de 3.A.4 dans l'appendice.

Lemme.— *Pour tout n, l'application pr_n qui envoie chaque élément p de $\{1, \ldots, 2^n\}$ sur l'élément de $\{1, \ldots, 2^{n-1}\}$ qui lui est congru modulo 2^{n-1} est un homomorphisme de A_n sur A_{n-1}.*

Noter que ce résultat implique que, pour tout $n \geqslant 1$, la table de A_n se compose de quatre « presque-copies » de celle de A_{n-1}, au sens où les valeurs sont soit celles de A_{n-1}, soit celles-là augmentées de 2^{n-1} (voir la proposition 3.A.9 dans l'appendice pour davantage de précision). Il implique aussi que les tables de Laver forment un système projectif, dont la limite est une SD-structure dont le domaine est l'ensemble $\mathbb{Z}_2$ des entiers 2-adiques.

3.1.10.— Pour ce qui concerne les périodes, 3.1.9 implique une inégalité simple reliant $\pi_n(p)$ à $\pi_{n-1}(p)$.

Proposition (comparaison).— *Pour tout n et tout $p \leqslant 2^n$, on a, en notant p' l'élément de $\{1, \ldots, 2^{n-1}\}$ qui est congru à p modulo 2^{n-1}, ou bien $\pi_n(p) = \pi_{n-1}(p')$, ou bien $\pi_n(p) = 2\pi_{n-1}(p')$, ce dernier cas ne pouvant se produire que pour $p \leqslant 2^{n-1}$ ou pour $p = 2^n$.*

Démonstration. Soit ℓ la période de p dans A_n, et ℓ' celle de p' dans A_{n-1}. Il y a donc ℓ valeurs distinctes dans la ligne de p dans (la table de) A_n, et ℓ' valeurs dans la ligne de p' dans celle de A_{n-1}. Comme chaque entier dans $\{1, \ldots, 2^{n-1}\}$ est la projection d'exactement deux entiers dans $\{1, \ldots, 2^n\}$, 3.1.9 implique d'une part $\ell' \geqslant \ell/2$, et d'autre part $\ell' \leqslant \ell$. Comme ℓ et ℓ' sont des puissances de 2, les seules possibilités sont $\ell = \ell'$ et $\ell = 2\ell'$.

Pour $2^{n-1} < p < 2^n$ (qui implique $p = p' + 2^{n-1}$), toutes les valeurs apparaissant dans la ligne de p dans A_n sont strictement supérieures à 2^{n-1}, la projection pr est injective sur ces valeurs, et on a alors nécessairement $\ell = \ell'$. $\square$

3.1.11.— Le résultat de 3.1.10 implique que, pour tout p fixé, la suite des valeurs $(\pi_n(p))_{n \geqslant \lceil \log_2(p) \rceil}$ est non décroissante. Il est facile de calculer les premières valeurs, et on trouve les valeurs ci-dessous.

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$\pi_n(1)$	1	2	4	4	8	8	8	8	16	16	16	16	16	16
$\pi_n(2)$	2	2	4	4	8	8	16	16	16	16	16	16	16	16
$\pi_n(4)$	-	4	4	8	16	16	16	16	16	16	16	16	16	16
$\pi_n(8)$	-	-	8	8	16	16	16	16	16	16	16	16	16	16
$\pi_n(16)$	-	-	-	16	16	32	64	64	128	128	128	128	128	128

3.1.12.— L'inspection des valeurs suggère les questions suivantes.

Question (périodes).— (i) *La période de 2 dans A_n est-elle toujours supérieure ou égale à celle de 1 ? Même question pour les périodes de $p * p$ et p pour tout p.*
(ii) *La période de 1 dans A_n tend-elle vers ∞ avec n ?*

Une réponse sera apportée dans la sous-section 3.3.

3.2. Quotients finis de $\mathrm{Iter}(j)$

► Résumé.— Les tables de Laver sont des quotients des structures $\mathrm{Iter}(j)$ obtenues en itérant un plongement élémentaire. ◄

3.2.1.— D'après 2.3.8, chaque plongement élémentaire non trivial j issu d'un cardinal de Laver λ donne naissance à une SD-structure $\mathrm{Iter}(j)$ infinie. Il est naturel d'étudier cette structure d'un point de vue algébrique et, en particulier, d'en chercher d'éventuels quotients finis, soit encore d'étudier les congruences sur $\mathrm{Iter}(j)$, c'est-à-dire les relations d'équivalence compatibles avec l'opération.

▷ *Étant donné que l'ordinal λ considéré est limite, le rang V_λ est la réunion des rangs V_γ pour $\gamma < \lambda$, et il serait naturel de considérer sur $\mathcal{E}_\lambda$ les relations d'équivalence du type « $j{\restriction}V_\gamma = j'{\restriction}V_\gamma$ ». Ce choix naïf ne convient pas, car les relations ainsi obtenues ne sont en général pas compatibles avec l'opération binaire -[-]. On considère donc une notion voisine mieux adaptée.* ◁

Définition (équivalence).— Supposons que λ est un cardinal de Laver. Pour $\gamma < \lambda$ avec γ limite, deux plongements j et j' de $\mathcal{E}_\lambda^+$ sont déclarés γ-*équivalents*, noté $j \equiv_\gamma j'$, si l'on a

$$\forall x{\in}V_\lambda\, (j(x) \cap V_\gamma = j'(x) \cap V_\gamma). \qquad (\#17)$$

3.2.2.— On se propose de montrer que la relation $\equiv_\gamma$ est une congruence sur $\mathcal{E}_\lambda^+$. Qu'elle soit une relation d'équivalence compatible avec la composition résulte directement de la définition, et le point est d'établir la compatibilité avec l'opération d'application, c'est-à-dire de montrer que la conjonction de $i' \equiv_\gamma i$ et $j' \equiv_\gamma j$ entraîne $i'[j'] \equiv_\gamma i[j]$. Ce n'est pas difficile, mais il est utile de commencer par des résultats préparatoires.

Lemme.— *Supposons $\gamma < \lambda$ avec γ limite, et $j, j' \in \mathcal{E}_\lambda^+$.*
(i) *Si on a $j' \equiv_\gamma j$, alors, pour tout $\alpha < \lambda$, on a soit $j'(\alpha) = j(\alpha) < \gamma$, soit $j(\alpha) \geqslant \gamma$ et $j'(\alpha) \geqslant \gamma$.*
(ii) *Si on a $j' \equiv_\gamma j$ avec $j, j' \neq \mathrm{id}_{V_\lambda}$, on a soit $\mathrm{cr}(j) = \mathrm{cr}(j') < \gamma$, soit $\mathrm{cr}(j) \geqslant \gamma$ et $\mathrm{cr}(j') \geqslant \gamma$.*
(iii) *Si, pour $f : V_\lambda \to V_\lambda$, on pose $f \cap^* V_\gamma = \{(x, y) \in V_\gamma^2 \mid y \in f(x)\}$, la relation $j' \equiv_\gamma j$ équivaut à $j' \cap^* V_\gamma = j \cap^* V_\gamma$.*
(iv) *Pour $j \neq \mathrm{id}_{V_\lambda}$, la relation $j \equiv_\gamma \mathrm{id}$ équivaut à $\mathrm{cr}(j) \geqslant \gamma$.*

Démonstration. (i) Si α est un ordinal, on a $j(\alpha)\cap V_\gamma = \min(j(\alpha), \gamma)$, donc l'égalité $j(\alpha)\cap V_\gamma = j(\alpha')\cap V_\gamma$ équivaut à $\min(j(\alpha'), \gamma) = \min(j(\alpha), \gamma)$, qui implique (i).

(ii) Supposons $\mathrm{cr}(j) = \kappa < \gamma$. Pour $\alpha < \kappa$, on a $j(\alpha) = \alpha$, donc $j'(\alpha) = \alpha$ par (i). Par (i) à nouveau, $j(\kappa) < \gamma$ entraîne $j'(\kappa) = j(\kappa)$, tandis que $j(\kappa) \geqslant \gamma$ entraîne $j'(\kappa) \geqslant \gamma$. Dans tous les cas, on a $j'(\kappa) > \kappa$, d'où $\mathrm{cr}(j') = \kappa = \mathrm{cr}(j)$. Cela donne (ii) puisque $\mathrm{cr}(j) \geqslant \gamma$ interdit $\mathrm{cr}(j') < \gamma$ qui, par symétrie, impliquerait $\mathrm{cr}(j) < \gamma$, donc $\mathrm{cr}(j) \geqslant \gamma$ implique $\mathrm{cr}(j') \geqslant \gamma$.

(iii) Supposons $j' \equiv_\gamma j$ et $(x, y) \in j \cap^* V_\gamma$. Par définition, on a $y \in j(x) \cap V_\gamma$, donc $y \in j'(x) \cap V_\gamma$ par (#17), d'où $j \cap^* V_\gamma \subseteq j' \cap^* V_\gamma$, puis, de là et par symétrie, $j \cap^* V_\gamma = j' \cap^* V_\gamma$.

Inversement, supposons $j \cap^* V_\gamma = j' \cap^* V_\gamma$. Soit x quelconque dans V_λ et y satisfaisant $y \in j(x) \cap V_\gamma$. Puisque γ est limite, il existe $\alpha < \gamma$ tel que y est dans V_α, et, puisque $j(\alpha) \geqslant \alpha$ est assuré, on trouve

$$y \in j(x) \cap V_\alpha \subseteq j(x) \cap V_{j(\alpha)} = j(x \cap V_\alpha).$$

L'ensemble $x \cap V_\alpha$ appartient à $V_{\alpha+1}$, donc à V_γ, et $(x \cap V_\alpha, y)$ est dans $j \cap^* V_\gamma$. Appliquant l'hypothèse, on déduit que $(x\cap V_\alpha, y)$ est dans $j' \cap^* V_\gamma$, donc que y est dans $j'(x\cap V_\alpha)$. Comme $x\cap V_\alpha \subseteq x$ entraîne $j'(x\cap V_\alpha) \subseteq j'(x)$, on déduit $y \in j'(x)$, d'où $j(x) \cap V_\gamma \subseteq j'(x) \cap V_\gamma$, et (#17) par symétrie.

(iv) Supposons $j \equiv_\gamma \mathrm{id}_{V_\lambda}$. Pour tout $\alpha < \gamma$, on a alors $j(\alpha) = \mathrm{id}(\alpha) = \alpha$ par (i), d'où $\mathrm{cr}(j) \geqslant \gamma$. Inversement, supposons $\mathrm{cr}(j) \geqslant \gamma$. Pour tout $\alpha < \gamma$, on a alors $j(\alpha) = \alpha$. Par 1.1.3(iii), on déduit $j(x) = x$ pour tout x dans V_γ, d'où $j \cap^* V_\gamma = \mathrm{id} \cap^* V_\gamma$, et $j \equiv_\gamma \mathrm{id}$ par (iii). □

3.2.3. Lemme.— *Supposons $i, j, i', j' \in \mathcal{E}_\lambda^+$ avec $i \neq \mathrm{id}_{V_\lambda}$.*

(i) *Les plongements j, $i[j]$, et $i \circ j$ sont* $\mathrm{cr}(i)$*-équivalents.*

(ii) *Pour γ, δ limites $<\lambda$, la conjonction de $i' \equiv_\gamma i$ et $j' \equiv_\delta j$ avec $i(\delta) \geqslant \gamma$ entraîne $i'[j'] \equiv_\gamma i[j]$.*

Démonstration. (i) Soit $\gamma = \mathrm{cr}(i)$. Alors, γ est un ordinal limite et $z \in V_\gamma$ entraîne $i(z) = z$ par 1.1.3. Pour $x, y \in V_\gamma$, la relation $y \in j(x)$ équivaut à $i(y) \in i(j(x))$, donc à $y \in i[j](x)$, car on a $i(y) = y$, et $i(j(x)) = i[j](i(x)) = i[j](x)$. On a donc $j(x) \cap V_\gamma = i[j](x) \cap V_\gamma$, soit $j \equiv_\gamma i[j]$. D'autre part, pour y dans V_γ, on a $y = i(y)$ et la relation $y \in j(x)$, qui équivaut à $i(y) \in i(j(x))$ par élémentarité de i, équivaut aussi à $y \in i(j(x))$. On a donc $j(x) \cap V_\lambda = i(j(x)) \cap V_\lambda$ pour tout x, soit $j \equiv_\gamma i \circ j$.

(ii) Supposons d'abord $\mathrm{cr}(i) \geqslant \gamma$. Pour $i' \neq \mathrm{id}_{V_\lambda}$, on a $\mathrm{cr}(i') \geqslant \gamma$ par 3.2.2(ii). De plus, on doit avoir $\delta \geqslant \gamma$ puisque $\delta < \gamma$ entraînerait $i(\delta) = \delta < \gamma$. Donc, $j \equiv_\delta j'$ entraîne $j \equiv_\gamma j'$. Dans tous les cas, (i) entraîne alors $i'[j'] \equiv_\gamma j' \equiv_\gamma j \equiv_\gamma i[j]$.

Supposons maintenant $\mathrm{cr}(i) < \gamma$, d'où $\mathrm{cr}(i') = \mathrm{cr}(i)$ par 3.2.2(ii). Comme $j' \equiv_\delta j$ implique directement $j' \equiv_{\delta'} j$ pour $\delta' \leqslant \delta$, on peut supposer que δ est le plus petit ordinal vérifiant $i(\delta) \geqslant \gamma$. Puisque γ est limite et que l'on a $\mathrm{cr}(i) < \gamma$, il existe γ' vérifiant $\mathrm{cr}(i) < \gamma' < \gamma$ et $i(\gamma') > \gamma$: pour $\kappa_n := \mathrm{cr}(i^{[n]})$, il existe m tel que γ appartient à $[\kappa_m, \kappa_{m+1}[$ par 2.1.5, et on peut prendre $\gamma' := \kappa_m$ pour $\gamma \neq \kappa_m$, et $\gamma' := \kappa_{m-1} + 1$ sinon. On a donc $\gamma' \geqslant \delta$ et, par suite, $\gamma > \delta$. On trouve alors

$$i[j] \cap^* V_\gamma = (i[j] \cap^* V_{i(\delta)}) \cap V_\gamma^2 = i(j \cap^* V_\delta) \cap V_\gamma^2.$$

Comme γ est limite, on a $V_\gamma^2 = V_\gamma$. De même, comme $j \cap^* V_\delta$ est inclus dans V_δ^2 avec $\delta < \gamma$, on a $j \cap^* V_\delta \in V_\gamma$. Par 3.2.2(iii), on a

$$j' \cap^* V_\delta = j \cap^* V_\delta \text{ et } i'(x) \cap V_\gamma = i(x) \cap V_\gamma \text{ pour } x \in V_\gamma.$$

En particulier, on a $i'(\delta) \cap \gamma = i(\delta) \cap \gamma$, donc $i'(\delta) \geqslant \gamma$. On en déduit

$$\begin{aligned} i'[j'] \cap^* V_\gamma &= i'(j' \cap^* V_\delta) \cap V_\gamma \quad (\text{eu égard à } i'(\delta) \geqslant \gamma)\\ &= i'(j \cap^* V_\delta) \cap V_\gamma = i(j \cap^* V_\delta) \cap V_\gamma = i[j] \cap^* V_\gamma \end{aligned}$$

(eu égard à $i(\delta) \geqslant \gamma$), d'où $i'[j'] \equiv_\gamma i[j]$ dans tous les cas. □

3.2.4.— Appliquant 3.2.3(ii) avec $\delta := \gamma$, ce qui est loisible puisque l'on a toujours $i(\gamma) \geqslant \gamma$, on obtient la compatibilité de $\equiv_\gamma$ avec l'application.

Proposition (congruence).— *Pour tout $\gamma < \lambda$ avec γ limite, la relation $\equiv_\gamma$ est une congruence sur $\mathcal{E}_\lambda^+$.*

3.2.5.— Pour chaque ordinal limite $\gamma < \lambda$, la structure-quotient $\mathrm{Iter}(j)/{\equiv_\gamma}$ est donc bien définie. Par construction, celle-ci est une SD-structure, et on va montrer maintenant que, pour γ convenablement choisi, elle est (isomorphe à) la table de Laver A_n. On rappelle que $j_{[p]}$ désigne la $p^{\text{ième}}$ puissance gauche de j (3.1.4).

Proposition (table de Laver).— *Supposons que λ est un cardinal de Laver et que j appartient à $\mathcal{E}_\lambda$. Pour tout $n \geqslant 0$, posons $\gamma_n := \mathrm{cr}(j_{[2^n]})$. Alors, la structure-quotient $\mathrm{Iter}(j)/{\equiv_{\gamma_n}}$ a 2^n éléments, et l'application ϕ_n qui associe à tout p dans $\{1, \dots, 2^n\}$ la $\equiv_{\gamma_n}$-classe de $j_{[p]}$ est un isomorphisme de A_n sur $\mathrm{Iter}(j)/{\equiv_{\gamma_n}}$.*

▷ *La démonstration de ce résultat est délicate et repose sur une suite de lemmes préparatoires. Le cœur de l'argument consistera à montrer que tout itéré d'un plongement j est $\equiv_\gamma$-équivalent à une puissance gauche $j_{[p]}$.* ◁

3.2.6. Définition (critique itéré).— Pour j dans $\mathcal{E}_\lambda$ et n entier, on note $\mathrm{cr}_n(j)$ le $(n+1)^{\text{ième}}$ élément de l'ensemble $\{\mathrm{cr}(i) \mid i \in \mathrm{Iter}^+(j)\}$ rangé par ordre croissant.

Exemple. Par élémentarité de i, on a toujours

$$\mathrm{cr}(i[j]) = i(\mathrm{cr}(j)) \text{ et } \mathrm{cr}(i \circ j) = \inf(\mathrm{cr}(i), \mathrm{cr}(j)),$$

et une induction immédiate entraîne $\mathrm{cr}(i) \geqslant \mathrm{cr}(j)$ pour tout i dans $\mathrm{Iter}(j)$. Par conséquent, on a $\mathrm{cr}_0(j) = \mathrm{cr}(j)$. L'égalité $\mathrm{cr}_1(j) = \mathrm{cr}(j_{[2]})$ et, plus généralement, $\mathrm{cr}_n(j) = \mathrm{cr}(j_{[2^n]})$, sera établie plus loin.

Noter qu'il n'y a *a priori* aucune raison pour que tout cardinal critique d'un itéré de j soit de la forme $\mathrm{cr}_n(j)$: il se pourrait que le type d'ordre de $\{\mathrm{cr}(i) \mid i \in \mathrm{Iter}^+(j)\}$ soit un ordinal plus grand que ω. En fait, on montrera en 3.3.7 que ce n'est pas le cas, mais ce n'est pas évident.

3.2.7. Lemme.— *Supposons $i[j_1[j_2]\cdots[j_\ell]](\mathrm{cr}(i)) \geqslant \delta$ pour $1 \leqslant \ell < r$, avec $i, j_1, \dots, j_r$ dans $\mathcal{E}_\lambda$. On a alors*

$$i[j_1][j_2]\cdots[j_r] \equiv_\delta i[j_1[j_2]\cdots[j_r]]. \qquad (\#18)$$

Démonstration. On utilise une induction sur $r \geqslant 1$. Pour $r = 1$, l'équivalence est une égalité. Supposons $r \geqslant 2$. Par hypothèse d'induction, on a

$$i[j_1][j_2]\cdots[j_{r-1}] \equiv_\delta i[j_1[j_2]\cdots[j_{r-1}]],$$

et donc, par 3.2.3,

$$i[j_1][j_2]\cdots[j_{r-1}]\,[j_r] \equiv_\delta i[j_1[j_2]\cdots[j_{r-1}]]\,[j_r]. \qquad (\#19)$$

Posons $\gamma = \mathrm{cr}(i)$. Par le lemme 3.2.3(i), on a $j_r \equiv_\gamma i[j_r]$, d'où

$$i[j_1[j_2]\cdots[j_{r-1}]]\,[j_r] \equiv_\delta i[j_1[j_2]\cdots[j_{r-1}]]\,[i[j_r]], \qquad (\#20)$$

puisque, par hypothèse, on a $i[j_1[j_2]\cdots[j_{r-1}]](\gamma) \geqslant \delta$. Par (SD), le second membre de (#20) est aussi $i[j_1[j_2]\cdots[j_r]]$, d'où (#18) en combinant (#19) et (#20). □

3.2.8. Lemme.— *Supposons* $\mathrm{cr}(i[j_1]\cdots[j_\ell]) < \mathrm{cr}(i)$ *pour* $1 \leqslant \ell < r$ *et* $\mathrm{cr}(i[j_1]\cdots[j_r]) \leqslant \mathrm{cr}(i)$*, avec* $i, j_1, \ldots, j_r$ *dans* $\mathcal{E}_\lambda$*. On a alors*

$$\mathrm{cr}(i[j_1][j_2]\cdots[j_r]) = i(\mathrm{cr}(j_1[j_2]\cdots[j_r])). \qquad (\#21)$$

Démonstration. Le résultat est évident pour $r = 1$. Supposons $r \geqslant 2$, et posons $\gamma := \mathrm{cr}(i)$, et soit δ le plus petit des ordinaux

$$i[j_1](\gamma),\ i[j_1[j_2]](\gamma),\ \ldots\ ,\ i[j_1[j_2]\cdots[j_{r-1}]](\gamma).$$

Alors, 3.2.7 donne

$$i[j_1][j_2]\cdots[j_r] \equiv_\delta i[j_1[j_2]\cdots[j_r]]. \qquad (\#22)$$

Soit q le plus petit entier vérifiant $\delta = i[j_1[j_2]\cdots[j_q]](\gamma)$, et $j := i[j_1][j_2]\cdots[j_q]$. On a alors $\delta = i[j](\gamma)$. Maintenant, par hypothèse, on a $\mathrm{cr}(j) < \gamma$ et, donc, il existe α satisfaisant $\alpha < \gamma \leqslant j(\alpha)$ et on déduit

$$i(\gamma) \leqslant i(j(\alpha)) = i[j](i(\alpha)) = i[j](\alpha) < i[j](\gamma) = \delta.$$

Alors, $\mathrm{cr}(i[j_1][j_2]\cdots[j_r]) \leqslant \gamma$ implique $\mathrm{cr}(i[j_1[j_2]\cdots[j_r]]) \leqslant i(\gamma) < \delta$. Le cardinal critique du terme de droite dans (#22) est donc plus petit que δ. Par 3.2.2(ii), il en est de même du terme de gauche, et les deux cardinaux critiques sont égaux, ce qui est le résultat annoncé. □

3.2.9. Lemme.— *Pour tous* j *dans* $\mathcal{E}_\lambda$ *et* $i_1, \ldots, i_{2^n}$ *dans* $\mathrm{Iter}(j)$*, il existe* $p \leqslant 2^n$ *vérifiant* $\mathrm{cr}(i_1[i_2]\cdots[i_p]) \geqslant \mathrm{cr}_n(j)$*.*

Démonstration. On utilise une induction sur $n \geqslant 0$. Pour $n = 0$, il s'agit d'établir l'inégalité $\mathrm{cr}(i_1) \geqslant \mathrm{cr}(j)$, ce qui a été vu plus haut. Supposons désormais $n \geqslant 1$. Par hypothèse d'induction, il existe $q \leqslant 2^{n-1}$ vérifiant

$$\mathrm{cr}(i_1[i_2]\cdots[i_q]) \geqslant \mathrm{cr}_{n-1}(j). \qquad (\#23)$$

Si l'inégalité est stricte, alors on a $\mathrm{cr}(i_1[i_2]\cdots[i_q]) \geqslant \mathrm{cr}_n(j)$ par définition de $\mathrm{cr}_n(j)$, ce qui est la conclusion cherchée. Sinon, (#23) est une égalité. Par hypothèse d'induction à nouveau, il existe $r \leqslant 2^{n-1}$ vérifiant

$$\mathrm{cr}(i_{q+1}[i_{q+2}]\cdots[i_{q+r}]) \geqslant \mathrm{cr}_{n-1}(j). \qquad (\#24)$$

Supposons r minimal. Alors, 3.2.7 s'applique avec $i = i_1[i_2]\cdots[i_q]$, $j_\ell = i_{q+\ell}$, et $\delta = \mathrm{cr}_n(i)$ puisque, posant $\gamma := \mathrm{cr}_{n-1}(j)$, on a alors $\mathrm{cr}(i) = \gamma$ et, par hypothèse, $\mathrm{cr}(i[i_1]\cdots[i_\ell]) < \gamma$ pour $1 \leqslant \ell < r$, donc $\mathrm{cr}(i[i_1[i_2]\cdots[i_\ell]]) < \gamma$, et donc

$$i[i_1[i_2]\cdots[i_\ell]](\gamma) > \gamma,$$

d'où $i[i_1[i_2]\cdots[i_\ell]](\gamma) \geqslant \delta$. Alors, 3.2.7 donne $i[j_1][j_2]\cdots[j_r] \equiv_\delta i[j_1[j_2]\cdots[j_r]]$, soit

$$i_1[i_2]\cdots[i_q][i_{q+1}][i_{q+2}]\cdots[i_{q+r}] \equiv_\delta i[i_{q+1}[i_{q+2}]\cdots[i_{q+r}]]. \qquad (\#25)$$

Par (#24), on a $\mathrm{cr}(i_{q+1}[i_{q+2}]\cdots[i_{q+r}]) \geqslant \gamma$, donc

$$\mathrm{cr}(i[i_{q+1}[i_{q+2}]\cdots[i_{q+r}]]) \geqslant i(\gamma) \geqslant \delta,$$

et donc, par 3.2.2(ii), l'équivalence de (#25) entraîne

$$\mathrm{cr}(i_1[i_2]\cdots[i_q][i_{q+1}][i_{q+2}]\cdots[i_{q+r}]) \geqslant \delta,$$

ce qui est le résultat escompté puisque δ est $\mathrm{cr}_n(j)$. □

3.2.10.— En appliquant 3.2.9 avec $i_1 = \cdots = i_{2^n} = j$, on voit en particulier que, pour tout n, il existe $p \leqslant 2^n$ vérifiant $\mathrm{cr}(j_{[p]}) \geqslant \mathrm{cr}_n(j)$.

Lemme.— *Pour tout* j *dans* $\mathcal{E}_\lambda$*, tout* i *dans* $\mathrm{Iter}^+(j)$*, et tout* n*, il existe* i' *dans* $\mathrm{Iter}(j)$ *tel que* i *est* $\mathrm{cr}_n(j)$*-équivalent à* i'*.*

Démonstration. Soit S l'ensemble des éléments de $\mathrm{Iter}^+(j)$ qui sont $\mathrm{cr}_n(j)$-équivalents à un élément de $\mathrm{Iter}(j)$. L'ensemble S contient j, et il est clos par l'opération -[-] puisque, d'après 3.2.3, si i'_1 est $\mathrm{cr}_n(j)$-équivalent à i_1 et i'_2 est $\mathrm{cr}_n(j)$-équivalent à i_2, alors $i'_1[i'_2]$ est $\mathrm{cr}_n(j)$-équivalent à $i_1[i_2]$. Pour montrer le résultat, c'est-à-dire pour montrer que S est l'intégralité de $\mathrm{Iter}^+(j)$, il suffit donc de montrer que S est clos par composition. De plus, comme chaque relation $\equiv_\gamma$ est compatible avec la composition, il suffit de montrer que, pour tous i_1, i_2 dans $\mathrm{Iter}(j)$, il existe i dans $\mathrm{Iter}(j)$ qui est $\mathrm{cr}_n(j)$-équivalent à $i_2 \circ i_1$.

Soient donc i_1, i_2 dans $\mathrm{Iter}(j)$. On définit inductivement une suite i_3, i_4, ... d'itérés de j par $i_{p+2} = i_{p+1}[i_p]$. Comme observé en 2.3.6, l'égalité $i \circ j = i[j] \circ i$ est valide pour tous i, j dans $\mathcal{E}_\lambda^+$, et on en déduit $i_3 \circ i_2 = i_2[i_1] \circ i_2 = i_2 \circ i_1$ et, de proche en proche, $i_{p+1} \circ i_p = i_2 \circ i_1$ pour tout p. On considère deux cas.

Supposons d'abord $\mathrm{cr}(i_2) > \mathrm{cr}(i_1)$. On trouve alors

$$\mathrm{cr}(i_3) = \mathrm{cr}(i_2[i_1]) = i_2(\mathrm{cr}(i_1)) = \mathrm{cr}(i_1), \text{ et}$$
$$\mathrm{cr}(i_4) = i_3(\mathrm{cr}(i_2)) = i_2[i_1](\mathrm{cr}(i_2)) \geqslant i_2(\mathrm{cr}(i_2)) > \mathrm{cr}(i_2),$$

et une induction facile donne

$$\mathrm{cr}(i_1) = \mathrm{cr}(i_3) = \mathrm{cr}(i_5) = ... \text{ et } \mathrm{cr}(i_2) < \mathrm{cr}(i_4) < \mathrm{cr}(i_6) < \dots .$$

Par définition, on a $\mathrm{cr}(i_1) \geqslant \mathrm{cr}_0(j)$, d'où $\mathrm{cr}(i_2) \geqslant \mathrm{cr}_1(j)$, et, de proche en proche, $\mathrm{cr}(i_{2n}) \geqslant \mathrm{cr}_n(j)$.

Supposons maintenant $\mathrm{cr}(i_2) \leqslant \mathrm{cr}(i_1)$. Un calcul semblable donne

$$\mathrm{cr}(i_1) < \mathrm{cr}(i_3) < \mathrm{cr}(i_5) < \dots, \text{ et } \mathrm{cr}(i_2) = \mathrm{cr}(i_4) = \mathrm{cr}(i_6) = \dots,$$

d'où $\mathrm{cr}(i_{2n+1}) \geqslant \mathrm{cr}_n(j)$.

Dans les deux cas, il existe donc p vérifiant $\mathrm{cr}(i_p) \geqslant \mathrm{cr}_n(j)$. Par 3.2.3(i), $i_p \circ i_{p-1}$, qui est égal à $i_2 \circ i_1$, est alors $\mathrm{cr}_n(j)$-équivalent à i_{p-1}, qui par construction appartient à $\mathrm{Iter}(j)$. □

3.2.11.— Nous pouvons maintenant montrer que toute classe d'un élément de $\mathrm{Iter}(j)$, et même de $\mathrm{Iter}^+(j)$, vis-à-vis de la $\mathrm{cr}_n(j)$-équivalence contient une puissance gauche $j_{[p]}$ avec $p \leqslant 2^n$.

Lemme.— *Pour tout j dans $\mathcal{E}_\lambda$, tout i dans $\mathrm{Iter}^+(j)$, et tout n, il existe $p \leqslant 2^n$ tel que i est $\mathrm{cr}_n(j)$-équivalent à $j_{[p]}$.*

Démonstration. D'après 3.2.10, il suffit de considérer le cas $i \in \mathrm{Iter}(j)$. Le principe est de diviser à droite par j autant que faire se peut. À cette fin, on construit des éléments i_0, i_1, ... dans $\mathrm{Iter}(j)$ tels que i_0 est i, et i_p est $\mathrm{cr}_n(j)$-équivalent à $i_{p+1}[j]$ pour tout p. Alors, i est $\mathrm{cr}_n(j)$-équivalent à $i_p[j]\cdots[j]$, avec p fois j, cela pour tout p. Le processus s'arrête soit si on trouve $i_p = j$, auquel cas i est $\mathrm{cr}_n(j)$-équivalent à $j_{[p+1]}$, soit si on trouve $p = 2^n$, auquel cas on a obtenu une suite de 2^n itérés de j, et 3.2.9 donne la conclusion escomptée.

Pour montrer que la construction est possible, supposons que i_p a été obtenu. Si on a $i_p = j$, la construction s'arrête. Sinon, i_p a la forme $i'_1[i'_2[\cdots[i'_r[j]]\cdots]]$, où $i'_1, \dots, i'_r$ sont des éléments de $\mathrm{Iter}(j)$. Appliquant (#13) r fois, on obtient l'égalité $i_p = (i'_1 \circ \cdots \circ i'_r)[j]$, et, appliquant 3.2.10, on définit i_{p+1} comme un élément de $\mathrm{Iter}(j)$ qui est $\mathrm{cr}_n(j)$-équivalent à $i'_1 \circ \cdots \circ i'_r$.

Supposons que la construction continue pendant au moins 2^n étapes, et considérons les 2^n plongements $i_{2^n}[j]$, $i_{2^n}[j][j], \dots, i_{2^n}[j][j]\cdots[j]$, 2^n fois j. Par 3.2.9, il existe $p \leqslant 2^n$ tel que $\mathrm{cr}(i_{2^n}[j][j]\cdots[j])$, p fois j, est $\geqslant \mathrm{cr}_n(j)$. Soit i' ce plongement. Alors, i est $\mathrm{cr}_n(j)$-équivalent à $i_{2^n}[j][j]\cdots[j]$, avec 2^n fois j, lequel est aussi $i'[j][j]\cdots[j]$, avec $2^n - p$ fois j, et, par conséquent, i est $\mathrm{cr}_n(j)$-équivalent à $j[j]\cdots[j]$ avec $2^n - p$ fois j, c'est-à-dire à $j_{[2^n - p]}$, comme escompté. □

3.2.12.— On peut alors exprimer les ordinaux $\mathrm{cr}_n(j)$ en fonction des cardinaux critiques des puissances gauches de j.

Lemme.— *Pour tout j dans $\mathcal{E}_\lambda$ et tout p, on a $\mathrm{cr}(j_{[p]}) = \mathrm{cr}_m(j)$, où m est le plus grand entier tel que 2^m divise p.*

Démonstration. Pour tout entier p, soit $f(p)$ le plus grand entier m tel que 2^m divise p. On va montrer par induction sur $n \geqslant 0$ l'énoncé

$$\mathrm{cr}(j_{[2^n]}) \geqslant \mathrm{cr}_n(j) \quad \text{et} \quad \forall p{<}2^n\ (\mathrm{cr}(j_{[p]}) = \mathrm{cr}_{f(p)}(j)). \tag{\#26}$$

autrement dit procéder par blocs de longueurs 2^n doublant à chaque étape.

Pour $n = 0$, on a $\mathrm{cr}(j) = \mathrm{cr}_0(j)$, ce qui suffit pour vérifier (#26). Supposons $n \geqslant 1$. Considérons les plongements $j_{[2^n+p]}$ pour $1 \leqslant p \leqslant 2^n$. Par définition, on a

$$j_{[2^n+p]} = j_{[2^n]}[j]\cdots[j], \text{ avec } p \text{ fois } j,$$

et, par hypothèse d'induction, $\mathrm{cr}(j_{[2^n]}) \geqslant \mathrm{cr}_n(j)$ et $\mathrm{cr}(j_{[\ell]}) < \mathrm{cr}(j_{[2^n]})$ pour $\ell < 2^n$. Alors, 3.2.8 avec $i = j_{[2^n]}$, $r = p$, et $j_1 = \cdots = j_p = j$ donne

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

Pour $p < 2^n$, on déduit $\mathrm{cr}(j_{[2^n+p]}) = \mathrm{cr}(j_{[p]}) = \mathrm{cr}_m(j)$ avec m maximal tel que 2^m divise p, donc aussi maximal tel que 2^m divise $2^n + p$. Pour $p = 2^n$, on obtient

$$\mathrm{cr}(j_{[2^{n+1}]}) = j_{[2^n]}(\mathrm{cr}(j_{[2^n]}) > \mathrm{cr}(j_{[2^n]}) = \mathrm{cr}_n(j),$$

et on déduit $\mathrm{cr}(j_{[2^{n+1}]}) \geqslant \mathrm{cr}_{n+1}(j)$, ce qui achève la vérification de (#26).

Alors, 3.2.11 implique que le cardinal critique de tout élément de $\mathrm{Iter}^+(j)$ est soit égal à celui d'une puissance gauche de j, soit est plus grand que tous les ordinaux $\mathrm{cr}_m(j)$. Comme la suite des ordinaux $\mathrm{cr}(j_{[2^n]})$ est strictement croissante, la seule possibilité est $\mathrm{cr}(j_{[2^n]}) = \mathrm{cr}_n(j)$. □

3.2.13. Lemme.— *Supposons $j \in \mathcal{E}_\lambda$ Alors, $j_{[p]}$ et $j_{[p']}$ sont $\mathrm{cr}_n(j)$-équivalents si, et seulement si, p et p' sont congrus modulo 2^n.*

Démonstration. On a $\mathrm{cr}(j_{[2^n]}) = \mathrm{cr}_n(j)$, donc $j_{[2^n]}$ est $\mathrm{cr}_n(j)$-équivalent à l'application identité de V_λ, ce qui, par 3.2.3(ii), implique que $j_{[p]}$ et $j_{[2^n+p]}$ sont $\mathrm{cr}_n(j)$-équivalents pour tout p. La condition du lemme est donc suffisante.

Réciproquement, on montre par induction sur $n \geqslant 0$ que $1 \leqslant p < p' \leqslant 2^n$ implique que $j_{[p]}$ et $j_{[p']}$ ne sont pas $\mathrm{cr}_n(j)$-équivalents. Le résultat est vide pour $n = 0$. Supposons $n \geqslant 1$. Pour $p' \neq 2^{n-1} + p$, l'hypothèse d'induction entraîne que $j_{[p]}$ et $j_{[p']}$ ne sont pas $\mathrm{cr}_{n-1}(j)$-équivalents, donc *a fortiori* ils ne sont pas $\mathrm{cr}_n(j)$-équivalents. Supposons maintenant $p' = 2^{n-1} + p$, et que $j_{[p]}$ et $j_{[p']}$ sont $\mathrm{cr}_n(j)$-équivalents. En appliquant $2^{n-1} - p$ fois 3.2.3, on déduit que $j_{[2^{n-1}]}$ et $j_{[2^n]}$ sont $\mathrm{cr}_n(j)$-équivalents, ce qui est impossible puisque le lemme 3.2.12 assure $\mathrm{cr}(j_{[2^{n-1}]}) = \mathrm{cr}_{n-1}(j)$ et $\mathrm{cr}(j_{[2^n]}) = \mathrm{cr}_n(j)$ et que, par définition, on a $\mathrm{cr}_{n-1}(j) < \mathrm{cr}_n(j)$. □

3.2.14.— On peut (enfin !) compléter l'argument pour 3.2.5.

Démonstration de la proposition 3.2.5. Suivant 3.1.7, il s'agit de montrer qu'il existe 2^n classes pour la $\mathrm{cr}(j_{[n]})$-équivalence, c'est-à-dire, par 3.2.12, pour la $\mathrm{cr}_n(j)$-équivalence. Or, d'après 3.2.11, toute classe pour la $\mathrm{cr}_n(j)$-équivalence contient une puissance gauche $j_{[p]}$ avec $p \leqslant 2^n$ et, d'après 3.2.13, deux telles puissances gauches ne sont jamais $\mathrm{cr}_n(j)$-équivalentes. Il existe donc 2^n classes d'équivalence, qui sont les classes de $j, j_{[2]}, \ldots, j_{[2^n]}$. Enfin, on a $\mathrm{cr}(j_{[2^n]}) = \mathrm{cr}_n(j)$ donc, par 3.2.2(iv), le plongement $j_{[2^n]}$ est $\mathrm{cr}_n(j)$-équivalent à id_{V_λ} et, de là, par 3.2.3, $j_{[2^n+1]}$, qui est $j_{[2^n]}[j]$ est $\mathrm{cr}_n(j)$-équivalent à j. On est donc exactement dans les conditions d'application de 3.1.7, la $\mathrm{cr}_n(j)$-équivalence jouant le rôle de $\simeq$ et j celui de g. □

3.3. Deux résultats sur les périodes

► Résumé.— On répond aux questions de la sous-section 3.1 sur les périodes dans A_n en utilisant les propriétés des plongements de $\mathcal{E}_\lambda$. ◄

3.3.1.— On a obtenu dans la sous-section 3.2 une réalisation de la table de Laver A_n comme quotient de l'algèbre $\mathrm{Iter}(j)$ des itérés purs d'un plongement élémentaire j associé à un cardinal de Laver. En utilisant les propriétés spécifiques des plongements élémentaires, notamment de leurs ordinaux critiques, on va établir des réponses, en l'occurrence positives, aux questions de 3.1.12 sur les périodes. On rappelle que, pour $p \leqslant 2^n$, la période $\pi_n(p)$ est le nombre de valeurs apparaissant au début de la $p^{\text{ième}}$ ligne de la table A_n et se reproduisant ensuite périodiquement.

3.3.2.— Conformément au formalisme du chapitre VII, si $t(x)$ est un terme à une variable libre en la signature Σ comportant une opération binaire, si $\mathcal{S}$ est une structure de type Σ, et si a est un élément du domaine de $\mathcal{S}$, on notera $t(a)^{\mathcal{S}}$, ou simplement $t(a)$, la valeur de $t(x)$ en a dans $\mathcal{S}$. L'existence de l'isomorphisme ϕ_n de 3.2.5 entre $\mathrm{Iter}(j)/{\equiv_{\mathrm{cr}_n(j)}}$ et A_n implique alors, pour tout terme $t(x)$, une relation simple entre les évaluations de $t(j)$ dans $\mathrm{Iter}(j)$ et de $t(1)$ dans A_n : si, pour i dans $\mathcal{E}_\lambda$, on note $\psi_n(i)$ l'image de la $\mathrm{cr}_n(j)$-classe de i par ϕ_n, alors, pour tout terme $t(x)$, on a

$$\psi_n(t(j)^{\mathrm{Iter}(j)}) = t(1)^{A_n}. \tag{\#27}$$

En effet, par définition, on a $\psi_n(j) = 1$, donc (#27) est vraie pour $t(x) = x$, et de là inductivement pour tout $t(x)$ puisque ψ_n est un homomorphisme.

Exemple. Par 3.2.11, *tout itéré de j est $\mathrm{cr}_n(j)$-équivalent à une puissance gauche de j (dépendant de n). La formule* (#27) *permet de déterminer certains exposants. Par exemple,* (#27) *affirme que l'image par ϕ_4 de la $\mathrm{cr}_4(j)$-classe de la puissance droite $j^{[3]}$ est $1^{[3]}$ calculé dans A_4 : on lit dans la table que la valeur est* 12, *et on conclut que $j^{[3]}$ est $\mathrm{cr}_4(j)$-équivalent à la puissance gauche $j_{[12]}$.*

3.3.3.— Le point-clé est alors l'existence d'un lien simple entre les périodes des tables de Laver et les ordinaux critiques des plongements de $\mathrm{Iter}(j)$.

Lemme.— *Pour tout j dans $\mathcal{E}_\lambda$, tout terme $t(x)$, et tout n, on a*

$$t(1)^{A_n} = 2^n \quad\Leftrightarrow\quad \mathrm{cr}(t(j)^{\mathrm{Iter}(j)}) \geqslant \mathrm{cr}_n(j). \tag{\#28}$$

$$t(1)^{A_{n+1}} = 2^n \quad\Leftrightarrow\quad \mathrm{cr}(t(j)^{\mathrm{Iter}(j)}) = \mathrm{cr}_n(j). \tag{\#29}$$

Démonstration. On écrit $t(j)$ pour $t(j)^{\mathrm{Iter}(j)}$. Pour (#28), d'après 3.2.2(iv), on a $\mathrm{cr}(t(j)) \geqslant \mathrm{cr}_n(j)$ si, et seulement si, $t(j)$ est $\mathrm{cr}_n(j)$-équivalent à id_{V_λ}, donc aussi, par 3.2.13, à $j_{[2^n]}$, donc si, et seulement si, on a $\psi_n(t(j)) = \psi_n(j_{[2^n]})$. Par (#27), cela équivaut à $t(1)^{A_n} = (1_{[2^n]})^{A_n}$, donc à $t(1)^{A_n} = 2^n$ puisque $1_{[2^n]}$ dans A_n est 2^n.

Pour (#29), on remarque que $\mathrm{cr}(t(j)) = \mathrm{cr}_n(j)$ équivaut à la conjonction de

$$\mathrm{cr}(t(j)) \geqslant \mathrm{cr}_n(j) \quad \text{et} \quad \mathrm{cr}(t(j)) \not\geqslant \mathrm{cr}_{n+1}(j),$$

donc, par (#28), à celle de

$$t(1)^{A_n} = 2^n \quad \text{et} \quad t(1)^{A_{n+1}} \neq 2^{n+1}. \tag{\#30}$$

Or, par 3.1.10, $t(1)^{A_n} = 2^n$ entraîne $t(1)^{A_{n+1}} \in \{2^n, 2^{n+1}\}$, donc (#30) entraîne $t(1)^{A_{n+1}} = 2^n$. Inversement, $t(1)^{A_{n+1}} = 2^n$ entraîne $t(1)^{A_n} = 2^n$ par projection, et $t(1)^{A_{n+1}} \neq 2^{n+1}$ trivialement, d'où l'équivalence avec (#30). $\square$

Exemple. On lit dans la table que $1^{[3]}$ *calculé dans* A_3 *est* 4, *donc, par* (#29), *on déduit* $\mathrm{cr}(j^{[3]}) = \mathrm{cr}_2(j)$, *soit, par* 3.2.12, $\mathrm{cr}(j^{[3]}) = \mathrm{cr}(j_{[4]})$. *De même, on pourra vérifier que* $1^{[4]}$ *calculé dans* A_5 *est* 16, *d'où, toujours par* (#29) *et* 3.2.12, *les égalités* $\mathrm{cr}(j^{[4]}) = \mathrm{cr}_4(j) = \mathrm{cr}(j_{[16]})$.

3.3.4.— On en déduit un dictionnaire simple reliant les changements de période dans les tables de Laver au comportement des ordinaux critiques des itérés d'un plongement élémentaire. On rappelle (3.1.10) que, pour tout n et tout terme $t(x)$, la période de $t(1)$ dans A_{n+1} est soit la même, soit le double de celle dans A_n.

Proposition (dictionnaire).— *Si λ est un cardinal de Laver et si j appartient à $\mathcal{E}_\lambda$, alors, pour tout terme $t(x)$ et tous $m < n$, les conditions suivantes sont équivalentes :*

(i) *La période de $t(1)^{A_n}$ passe de 2^m à 2^{m+1} entre A_n et A_{n+1} ;*

(ii) *Le plongement $t(j)^{\mathrm{Iter}(j)}$ envoie $\mathrm{cr}_m(j)$ sur $\mathrm{cr}_n(j)$.*

En particulier, pour $p \leqslant 2^n$ et $m < n$, la période de p passe de 2^m à 2^{m+1} entre A_n et A_{n+1} si, et seulement si, $j_{[p]}$ envoie $\mathrm{cr}_m(j)$ sur $\mathrm{cr}_n(j)$.

Démonstration. Écrivons $t(j)$ pour $t(j)^{\mathrm{Iter}(j)}$. Pour tout i, on a $\mathrm{cr}(i[j]) = i(\mathrm{cr}(j))$ et, par 3.2.12, $\mathrm{cr}_m(j) = \mathrm{cr}(j_{[2^m]})$, d'où $t(j)(\mathrm{cr}_m(j)) = \mathrm{cr}(t(j)[j_{[2^m]}])$. Par conséquent, (ii) équivaut à $\mathrm{cr}(t(j)[j_{[2^m]}]) = \mathrm{cr}_n(j)$, qui, par (#29), équivaut à

$$(t(1) * 1_{[2^m]})^{A_{n+1}} = 2^n,$$

soit, comme on a $m \leqslant n$ et que donc l'évaluation de $1_{[2^m]}$ dans A_{n+1} est 2^m, à

$$(t(1) * 2^m)^{A_{n+1}} = 2^n. \tag{#31}$$

Donc, (ii) équivaut à (#31).

Supposons alors (ii), donc (#31). Puisque, dans A_{n+1}, on n'a pas $t(1)*2^m = 2^{n+1}$, on déduit que la période ℓ de $t(1)^{A_{n+1}}$ dans A_{n+1} est multiple de 2^{m+1}. D'un autre côté, en utilisant 3.1.9 et en projetant (#31) sur A_n, on obtient

$$(t(1) * 2^m)^{A_n+1} = 2^n, \tag{#32}$$

qui montre que la période ℓ' de $t(1)^{A_n}$ dans A_n divise 2^m. Or, par 3.1.10, on a soit $\ell = \ell'$, soit $\ell = 2\ell'$. Par les résultats ci-dessus, la seule possibilité ici est que l'on soit dans le second cas, avec $\ell = 2^{m+1}$ et $\ell' = 2^m$. Donc, (ii) entraîne (i).

Inversement, supposons (i). D'après 3.1.9, on a ou bien $t(1)^{A_{n+1}} = t(1)^{A_n}$, ou bien $t(1)^{A_{n+1}} = t(1)^{A_n} + 2^n$. Par 3.1.10, le second cas implique l'égalité des périodes, contredisant (i). On a donc $t(1)^{A_{n+1}} = t(1)^{A_n}$ et, de là, (#31), dont on a vu ci-dessus qu'il équivaut à (ii). Donc, (i) implique (ii).

L'assertion finale de la proposition correspond au cas où $t(x)$ est le terme $x_{[p]}$, qui s'évalue en $j_{[p]}$ dans $\mathrm{Iter}(j)$, et en p dans A_n vue l'hypothèse $p \leqslant 2^n$. $\square$

Exemple. On lit sur les tables que la période de 1 *passe de* 4 *à* 8 *entre* A_4 *et* A_5 *: on en déduit que tout plongement j de $\mathcal{E}_\lambda$ envoie* $\mathrm{cr}_2(j)$ *sur* $\mathrm{cr}_4(j)$. *De même, la période de* 3 *passe de* 8 *à* 16 *entre* A_5 *et* A_6 *: on en déduit que* $j_{[3]}$ *envoie* $\mathrm{cr}_3(j)$ *sur* $\mathrm{cr}_5(j)$, *etc.*

3.3.5.— Dans les exemples ci-dessus, on a utilisé la correspondance entre plongements et tables de Laver pour déduire des valeurs observées dans les tables des résultats sur les ordinaux critiques des plongements. Mais on peut aussi utiliser le dictionnaire dans l'autre sens, et déduire de résultats généraux sur les plongements des résultats sur les tables de Laver.

Lemme.— *Pour tout j dans $\mathcal{E}_\lambda$ et tout $\alpha < \lambda$, on a $j[j](\alpha) \leqslant j(\alpha)$.*

Démonstration. Supposons $\alpha < \lambda$. On a $j(\alpha+1) = j(\alpha) + 1 > j(\alpha) \geqslant \alpha$, donc il existe un ordinal β satisfaisant $j(\beta) > \alpha$, et il existe donc un plus petit tel ordinal. Par construction, on a alors $j(\beta) > \alpha$ et $\forall\gamma{<}\beta\ (j(\gamma) \leqslant \alpha)$, cette dernière étant aussi équivalente à

$$\forall\gamma{<}\beta\ ((j{\upharpoonright}V_\beta)(\gamma) \leqslant \alpha)$$

puisque j et $j{\upharpoonright}V_\beta$ prennent les mêmes valeurs sur β. Comme j est un plongement élémentaire, la satisfaction de cette formule entraîne celle de la formule obtenue en appliquant j aux trois paramètres β, $j{\upharpoonright}V_\beta$, et α, à savoir

$$\forall\gamma{<}j(\beta)\ (j(j{\upharpoonright}V_\beta)(\gamma) \leqslant j(\alpha)).$$

Par définition, $j(j{\upharpoonright}V_\beta)$ est une restriction de $j[j]$, et on a donc aussi

$$\forall\gamma{<}j(\beta)\ (j[j](\gamma) \leqslant j(\alpha)). \qquad (\#33)$$

Or, par hypothèse, on a $\alpha < j(\beta)$, donc (#33) s'applique avec $\gamma := \alpha$, impliquant $j[j](\alpha) \leqslant j(\alpha)$, comme annoncé. □

3.3.6.— Une application directe de 3.3.5 est une réponse positive à la question 3.1.12(i).

Proposition (inégalité).— *S'il existe un cardinal de Laver, alors, pour tout $n \geqslant 1$ et tout $p < 2^n$, la période de $p * p$ est supérieure ou égale à celle de p dans A_n. En particulier, pour tout n, la période de 2 est supérieure ou égale à celle de 1 dans A_n.*

Démonstration. Supposons d'abord $\pi_n(p) = 1$. Ce cas est trivial, puisqu'il ne se produit que pour $p = 2^n - 1$, auquel cas on a $p * p = 2^n$, de période $2^n > 1$.

Supposons maintenant $\pi_n(p) \geqslant 2$. Écrivons $\pi_n(p) = 2^{m+1}$, et soit $\overline{n}$ le plus grand entier tel que la période de $1_{[p]}$ dans $A_{\overline{n}}$ est 2^m : puisque la période ne peut progresser que par doublement (3.1.8), et que la période de $1_{[p]}$ dans A_m est $\leqslant 2^m$, un tel entier $\overline{n}$ existe et on a $m \leqslant \overline{n} < n$.

Soit λ un cardinal de Laver, et soit j un plongement élémentaire dans $\mathcal{E}_\lambda$. Par hypothèse, la période de $1_{[p]}$ passe de 2^m à 2^{m+1} entre $A_{\overline{n}}$ et $A_{\overline{n}+1}$. Par 3.3.4, on déduit que $j_{[p]}$ envoie $\mathrm{cr}_m(j)$ sur $\mathrm{cr}_{\overline{n}}(j)$. D'un autre côté, par 3.3.5, on a

$$j_{[p]}[j_{[p]}](\mathrm{cr}_m(j)) \leqslant j_{[p]}(\mathrm{cr}_m(j)) = \mathrm{cr}_{\overline{n}}(j),$$

et donc il existe $n' \leqslant \overline{n}$ tel que $j_{[p]}[j_{[p]}]$ envoie $\mathrm{cr}_m(j)$ sur $\mathrm{cr}_{n'}(j)$. Le plongement $j_{[p]}[j_{[p]}]$ est l'évaluation dans $\mathrm{Iter}(j)$ du terme $x_{[p]} * x_{[p]}$, donc, par 3.3.4, cette fois dans l'autre sens, la période de $1_{[p]} * 1_{[p]}$ passe de 2^m à 2^{m+1} entre $A_{n'}$ et $A_{n'+1}$. Puisque l'on a $n' \leqslant \overline{n} \leqslant n$, on déduit que la période de $1_{[p]} * 1_{[p]}$ dans A_n est au moins 2^{m+1} : l'évaluation de $1_{[p]} * 1_{[p]}$ dans A_n est le produit $p * p$, d'où le résultat annoncé. Les cas particuliers de 1 et 2 s'ensuivent, puisque, pour $n \geqslant 1$, on a $2 = 1 * 1$ dans A_n. □

Exemple. On a $2*2 = 4$ *dans* A_2 *et* A_3*, et* $2*2 = 12$ *dans* $A_4, \dots, A_{14}$*, donc* 3.3.6 *implique* $\pi_n(4) \geqslant \pi_n(2)$ *pour* $n = 2, 3$ *et* $\pi_n(12) \geqslant \pi_n(2)$ *pour* $n = 4, \dots, 14$*. En revanche,* 3.3.6 *ne dit a priori rien de* $\pi_n(4)$ *pour ces dernières valeurs (pour* $n = 4$*, on a forcément* $\pi_4(4) \geqslant \pi_4(12)$ *puisque* 4 *et* 12 *sont congrus modulo* 8*, mais ensuite le lien disparaît).*

3.3.7.— Pour une seconde application, on partira d'un résultat plus délicat sur les plongements élémentaires.

$\triangleright$ *La borne de Kunen montre que, quel que soit* j *dans* $\mathcal{E}_\lambda$*, la* ω*-suite formé par les ordinaux critiques des puissances droites* $j^{[m]}$ *de* j *est cofinale dans* λ*. Mais cela ne dit rien sur le type d'ordre de l'ensemble des ordinaux critiques de tous les itérés (purs) de* j *: on sait que les* ω *premiers éléments de cet ensemble sont les ordinaux critiques des puissances gauches* $j_{[n]}$ *de* j*, mais, a priori, il se pourrait qu'il existe des ordinaux critiques au-delà de ceux-ci, c'est-à-dire que le type d'ordre de l'ensemble des ordinaux critiques soit un ordinal strictement plus grand que* ω *: c'est cette éventualité qui est écartée ci-dessous.* $\triangleleft$

Lemme.— *Pour tout* j *dans* $\mathcal{E}_\lambda$*, les ordinaux* $\mathrm{cr}_n(j)$ *sont cofinaux dans* λ *et ils énumèrent l'intégralité de l'ensemble* $\{\mathrm{cr}(i) \mid i \in \mathrm{Iter}^+(j)\}$*.*

Démonstration. On commence par un résultat général auxiliaire. Pour j dans $\mathcal{E}_\lambda$ et $\gamma < \lambda$, définissons $o_\gamma(j)$ comme le type d'ordre de l'ensemble

$$O_\gamma(j) := \{\alpha{\in}\mathbf{Ord} \mid \exists f{\in}V_\gamma\ \exists x{\in}V_\gamma\ (\text{« } f \text{ fonctionnel » et } \alpha{=}j(f)(x))\}.$$

On va montrer que, pour tous i, j dans $\mathcal{E}_\lambda$,

$$\text{Si } \gamma \text{ est inaccessible et vérifie } \mathrm{cr}(i) < \gamma < \lambda, \text{ on a } o_\gamma(i) > o_\gamma(i[j]). \qquad (\#34)$$

Supposons que γ, i, et j satisfont les hypothèses de (#34). Par 2.1.5, on doit avoir $\lambda = \sup_n i^n(\mathrm{cr}(i))$, donc le plongement i ne peut avoir de point fixe au-dessus de $\mathrm{cr}(i)$, et l'hypothèse $\mathrm{cr}(i) < \gamma$ implique l'existence d'un entier n vérifiant $i^n(\mathrm{cr}(i)) < \gamma \leqslant i^{n+1}(\mathrm{cr}(i))$, soit $\delta < \gamma \leqslant i(\delta)$ pour $\delta := i^n(\mathrm{cr}(i))$. Soit ϕ l'application de $V_\delta \times V_\delta$ dans $\mathbf{Ord}$ qui à (f, x) avec f fonctionnel associe $j(f)(x)$. Par définition, $O_\delta(j)$ est l'image de ϕ. Comme γ est inaccessible, on a

$$o_\delta(j) < \|O_\delta(j)\|^+ \leqslant \|\phi\| \leqslant \|V_\delta \times V_\delta\| < \gamma.$$

Posons $\theta := o_\delta(j)$, et soit π l'isomorphisme de $(O_\delta(j), <)$ sur $(\theta, <)$. Par élémentarité, $i(\pi)$ est un isomorphisme de $(i(O_\delta(j)), <)$, qui est $(O_{i(\delta)}(i[j]), <)$, sur $(i(\theta), <)$. Comme on a $\gamma \leqslant i(\delta)$, l'ensemble $O_\gamma(i[j])$ est inclus dans $O_{i(\delta)}(i[j])$ et, par conséquent, $i(\pi)$ est une injection croissante envoyant $O_\gamma(i[j])$ dans $i(\theta)$.

Par ailleurs, considérons α dans $O_\gamma(i[j])$. Par définition, il existe une fonction f et un élément x de V_γ vérifiant $\alpha = i[j](f)(x)$. On trouve alors

$$i(\pi)(\alpha) = i(\pi)(i[j](f)(x)) = i(\pi)(i(\phi)((f, x))) = i(\pi \circ \phi)((f, x)). \qquad (\#35)$$

Par construction, π et ϕ appartiennent à V_γ, et il en est de même de $\pi \circ \phi$ et de (f, x). Alors, (#35) montre que l'ordinal $i(\pi)(\alpha)$ appartient à $O_\gamma(i)$. Par conséquent, $i(\pi)$ envoie $O_\gamma(i[j])$ dans $O_\gamma(i)$. En fusionnant avec ce qui précède, on déduit que $i(\pi)$ est une injection croissante de $O_\gamma(i[j])$ dans $O_\gamma(i) \cap i(\theta)$.

Pour conclure que le type d'ordre de $O_\gamma(i[j])$ est strictement inférieur à celui de $O_\gamma(i)$, il suffit donc de montrer que $O_\gamma(i) \cap i(\theta)$ est un sous-ensemble strict de $O_\gamma(i)$ et, pour cela, que $i(\theta)$ appartient à $O_\gamma(i)$. Or, ce point est évident puisque l'on a $i(\theta) = i(f)(0)$ avec $f = \{(0, \theta)\}$ et que f et 0 sont dans V_γ. Donc, (#34) est établi.

Revenant alors à la situation du lemme, supposons, en vue d'une contradiction,

$$\sup_n\{\mathrm{cr}_n(j) \mid n \geqslant 0\} < \lambda. \qquad (\#36)$$

Par 2.1.5 à nouveau, on a $\lambda = \sup_{m\geqslant 0} j^m(\mathrm{cr}(j))$, donc $\lambda = \sup_{m\geqslant 0} \mathrm{cr}(j^{[m]})$. Par conséquent, (#36) implique l'existence de m satisfaisant $\mathrm{cr}_n(j) < \mathrm{cr}(j^{[m]})$ pour tout n. Posons $\gamma := \mathrm{cr}(j^{[m]})$. Par 1.1.5, γ est un cardinal mesurable, donc inaccessible. Avec les mêmes notations que ci-dessus, soit $o_\gamma(j_{[n]})$ le type d'ordre de $O_\gamma(j_{[n]})$. Pour tout n, on a $j_{[n+1]} = j_{[n]}[j]$ par définition, et donc (#34) implique $o_\gamma(j_{[n]}) > o_\gamma(j_{[n+1]})$, d'où une suite d'ordinaux strictement décroissante. C'est donc que (#36) est une hypothèse contradictoire. □

3.3.8.— Une application directe de 3.3.7 est une réponse positive à la question 3.1.12(ii).

Proposition (limite de période).— *S'il existe un cardinal de Laver, alors, pour tout p, la période de p dans A_n tend vers l'infini avec n.*

Démonstration. Il suffit de montrer que, pour tout entier m, il existe un entier n tel que la période de p passe de 2^m à 2^{m+1} entre A_n et A_{n+1}. Fixons un entier m, soit λ un cardinal de Laver, et soit j un plongement élémentaire dans $\mathcal{E}_\lambda$. Par 3.2.12, $\mathrm{cr}_m(j)$ est l'ordinal critique de $j_{[2^m]}$ et donc, par (#9), $j_{[p]}(\mathrm{cr}_m(j))$ est l'ordinal critique de $j_{[p]}[j_{[2^m]}]$, un élément de $\mathrm{Iter}(j)$. Par 3.3.7, tout ordinal critique d'un itéré de j est de la forme $\mathrm{cr}_n(j)$, et il existe donc n vérifiant

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

Par 3.3.4, on déduit que la période de p atteint 2^{m+1} dans A_{n+1}. □

▷ *Le résultat de* 3.3.8 *prouve que, pour chaque p, la suite des périodes de p dans A_n tend vers l'infini avec n, mais l'argument, fondé sur le raisonnement par l'absurde de* 3.3.7, *ne donne aucune indication sur la rapidité de la croissance. On a vu en* 3.1.11 *que, pour $n \geqslant 9$, la période de* 1 *dans A_n est au moins* 16, *et* 3.3.8 *implique que, s'il existe un cardinal de Laver, alors il existe un plus petit entier n tel que la période de* 1 *dans A_n soit* 32. *Le seul résultat connu à ce jour sur l'entier n est la borne inférieure $n \geqslant f_9^{\mathrm{Ack}}(f_8^{\mathrm{Ack}}(f_8^{\mathrm{Ack}}(254)))$, où f_m^{Ack} est le $m^{\text{ième}}$ étage de la fonction d'Ackermann* [22] *: c'est un entier gigantesque.* ◁

3.4. Un type nouveau d'application de la théorie des ensembles

► Résumé.— Quel que soit le statut logique final des résultats sur les périodes dans les tables de Laver, la théorie des ensembles aura joué un rôle essentiel dans leur découverte. ◄

3.4.1.— Le statut logique des résultats de la sous-section 3.3 reste incertain à ce jour : les résultats sur les périodes dans les tables de Laver énoncés en 3.3.6 et 3.3.8 ont été déduits ici de l'existence d'un cardinal de Laver, donc d'un axiome de grand cardinal indémontrable dans ZFC (et *a fortiori* dans PA_1) et, pour le moment, aucun argument alternatif formalisable dans ZFC n'est connu : même l'existence d'un entier n tel que la période de 1 dans A_n atteigne 32 n'est pas établie dans ZFC.

3.4.2.— À ce point, deux situations pourraient se produire. La première serait qu'il existe une démonstration alternative des résultats de la sous-section 3.3 dans ZFC, donc sans faire appel à des grands cardinaux. Des résultats partiels dans cette direction ont été obtenus : la construction d'homomorphismes de type $A_n \to A_{n+2^d}$ [25], $A_n \to A_{n2^d}$ [26], et $A_n \to A_{\exp^n(d)}$ (exponentielle itérée) [27] réalise les trois premières étapes d'un programme qui, s'il était complété, devrait mener à une démonstration de 3.3.8 dans l'arithmétique de Peano PA_1.

3.4.3.— En général considérée comme moins probable, la seconde situation serait celle où l'hypothèse de grand cardinal ne pourrait être omise dans une démonstration de 3.3.6 ou de 3.3.8. Il s'agirait d'une situation paradoxale : les tables de Laver sont des objets finis, aisément codables par exemple dans $(V_\omega, \in)$ ou $(\mathbb{N}, 0, S, +, \cdot)$ et, *a priori*, on imagine mal comment les propriétés combinatoires de ces tables pourraient être reliées à l'existence de grands cardinaux, mais, pour autant, aucun argument général n'interdit, en théorie, l'existence d'une telle connection, à l'instar du résultat mentionné plus loin en XVI.2.3.6.

$\triangleright$ *Une façon d'établir un tel résultat serait, en inversant le dictionnaire de* 3.3.4, *de construire, à partir des périodes dans les tables de Laver, des objets se rapprochant suffisamment des ordinaux et des plongements élémentaires sur ceux-ci pour obtenir la consistance d'un système équivalent à* ZFC+ *« il existe un cardinal de Laver », ou, tout au moins, plus fort que* ZFC*. Des résultats* (*très*) *partiels en ce sens apparaissent dans* [24]*. Mais, à ce jour, la seule borne inférieure prouvée à ce jour est la non-prouvabilité de* 3.3.8 *dans l'arithmétique primitive récursive, qui est le sous-système de* PA_1 *dans lequel le principe d'induction est limité aux prédicats primitifs récursifs* [22] *: la raison est que la fonction qui, à tout entier m associe le plus petit entier n vérifiant $\pi_n(1) \geqslant 2^m$ croît plus vite que toute fonction primitive récursive. Mais ce résultat reste très éloigné d'une non-prouvabilité dans* PA_1*, et a fortiori dans* ZFC*.* $\triangleleft$

3.4.4.— Si la situation finale est celle de 3.4.3, les résultats sur les périodes des tables de Laver constitueront une application spectaculaire des grands cardinaux, particulièrement simple conceptuellement. Mais, même si la balance devait pencher pour la situation de 3.4.2, c'est-à-dire si toute hypothèse de grand cardinal pouvait finalement être omise dans les démonstrations, le rôle essentiel de la théorie des ensembles n'en serait pas pour autant diminué : c'est l'étude des plongements élémentaires d'un rang dans lui-même qui a mené R. Laver à la découverte des tables A_n et des propriétés de leurs périodes, et il semble peu probable que celles-ci aient été rencontrées hors de ce cadre. Dans cette mesure, et quoi qu'il advienne ultérieurement, il semble légitime de considérer que les propriétés ainsi découvertes sont — et resteront — des *applications* de la théorie des ensembles et des grands cardinaux.

$\triangleright$ *Il est tentant ici de faire un parallèle avec la physique : nombreux sont les concepts et les énoncés mathématiques proposés par des physiciens sur la base d'une « intuition physique » et ultérieurement justifiés rigoureusement par des* *définitions et démonstrations mathématiques formelles ; le schéma est ici le même si l'on voit les concepts et les énoncés de théorie des ensembles comme issus d'une « intuition ensembliste » qu'il reste ensuite éventuellement à justifier rigoureusement, c'est-à-dire dans le cadre, disons, de* ZFC*. Dans tous les cas, le rôle de l'intuition initiale venue d'un autre monde est primordial.* ◁

3.4.5.— Notons qu'à ce point, conformément à la discussion de la sous-section XIII.3.4, il n'y a pas d'élément justifiant l'adoption dans le système de référence des axiomes de grands cardinaux, et spécialement celle de l'existence des cardinaux de Laver qui se trouve très haut dans la hiérarchie. Mais, du point de vue des applications comme celles de la sous-section 3.3, ce qui compte n'est pas la vérité ou plausibilité des axiomes mis en jeu, mais plutôt leur créativité et la richesse des intuitions auxquelles ils mènent : point n'est besoin ici de *croire* à l'existence des cardinaux de Laver, ni même à l'existence de l'infini actuel, pour en étudier les conséquences. Il serait donc regrettable de se priver des énoncés ainsi découverts au prétexte que le statut logique des bases qui y ont mené est incertain.

3.4.6.— On peut considérer l'existence d'applications du type de celles décrites plus haut comme un argument puissant en faveur de la théorie des ensembles et de l'exploration de l'infini, même dans ses formes les plus hypothétiques. Force est de reconnaître que, pour l'instant, de telles applications restent rares.

▷ *Un autre exemple, également lié aux cardinaux de Laver et aux propriétés d'autosimilarité auxquelles ils donnent lieu, est apparue à la fin des années 1980, lorsque l'ordonnabilité des* SD*-structures libres et la décidabilité du problème de mot de la loi* (SD) *ont été dérivées de l'existence d'un cardinal de Laver via la réalisation de la* SD*-structure libre de rang* 1 *fournie par* 2.3.9 [75]*. Dans ce cas, la situation s'est avérée ultérieurement être celle de* 3.4.2*, et pas celle de* 3.4.3 *: grâce à une réalisation alternative de la* SD*-structure libre de rang* 1 *dans le groupe des tresses* B_∞*, les résultats ci-dessus ont pu être établis dans l'arithmétique de Peano* [16]*. Pour autant, tant les propriétés ainsi obtenues que les applications qui ont découlé de la construction, en particulier l'ordonnabilité des groupes de tresses et ses multiples ramifications* [18]*, peuvent être considérées comme des* applications *et, partant, des* justifications *de la théorie des ensembles et des grands cardinaux.* ◁

3.A. Appendice : propriétés élémentaires des tables de Laver

3.A.1.— On trouvera ici les démonstrations manquant dans la sous-section 3.1 et quelques points supplémentaires. On commence par la construction des tables.

3.A.2.— Le point de départ est le résultat suivant, qui concerne toutes les tailles, et pas seulement les puissances de 2.

Lemme.— *Pour tout entier* $N \geqslant 1$*, il existe une unique structure* S_N *de domaine* $\{1, 2, ..., N\}$ *vérifiant pour tous* $p, q \leqslant N$ *les conditions*

- $p * 1 = p + 1$ *pour* $p < N$*, et* $N * 1 = 1$*,* (#37)
- $p * (q * 1) = (p * q) * (p * 1)$*.* (#38)

Les implications suivantes sont alors satisfaites pour tous $p, q \leqslant N$

- $p < N \Rightarrow p * q > p,$ (#39)
- $p = N \Rightarrow p * q = q,$ (#40)
- $(q \geqslant 2 \text{ et } p * (q-1) < N) \Rightarrow p * q > p * (q-1),$ (#41)
- $(q \geqslant 2 \text{ et } p * (q-1) = N) \Rightarrow p * q = p * 1.$ (#42)

De plus, pour chaque $p < N$, il existe un entier ℓ, noté $\pi_{S_N}(p)$ et appelé période de p dans S_N*, tel que la ligne de p dans la table de S_N consiste en la répétition périodique de ℓ valeurs croissant de $p+1$ à N.*

Démonstration. On va établir par induction sur p descendant de N à 1 et, pour p fixé, par induction sur q augmentant de 2 à N que (#37) et (#38) déterminent la valeur de $p * q$ et imposent(#39)–(#42). Il en résulte en particulier que la table de S_N est uniquement déterminée.

Supposons d'abord $p = N$. Pour $q = 1$, (#37) impose $p*q = 1$, conforme à (#40), tandis que (#39), (#41), et (#42) sont vraies par défaut. Pour $q \geqslant 2$, (#37) impose $q = (q-1)*1$, puis (#38) ainsi que (#40) appliquée à p et $q-1$ donnent

$$p * q = N * ((q-1) * 1) = (N * (q-1)) * (N * 1) = (q-1) * 1 = q,$$

conforme à (#40) et (#41), tandis que (#39) et (#42) sont vraies par défaut.

Supposons maintenant $p < N$. Pour $q = 1$, (#37) impose $p * q = p + 1$, qui est conforme à (#39), tandis que (#40)–(#42) sont vraies par défaut. Pour $q \geqslant 2$, on a à nouveau $q = (q-1) * 1$ par (#37), et (#38) donne

$$p * q = p * ((q-1) * 1) = (p * (q-1)) * (p * 1) = (p * (q-1)) * (p+1).$$

Par hypothèse d'induction, on a $p*(q-1) > p$ par (#40) pour $(p, q-1)$, donc, par hypothèse d'induction à nouveau, la valeur de $(p*(q-1))*(p+1)$ est déterminée. Supposons d'abord $p*(q-1) < N$. Par (#40) appliquée à $p*(q-1)$ et $p+1$, on a alors $p*q > p*(q-1)$, donc (#41) est vérifiée ; de plus, par (#39) appliquée à p et $q-1$, on a $p*(q-1) > p$, d'où *a fortiori* $p*q > p$, et (#39) est vérifiée, tandis que (#40) et (#42) sont vraies par défaut. Supposons enfin $p*(q-1) = N$. Par (#40) appliquée à N et $p+1$, on a alors $p*q = (p*(q-1))*(p+1) = N*(p+1) = p+1$. Alors, (#39) et (#42) sont vérifiées, et (#40) et (#41) sont vraies par défaut.

Pour le dernier point, supposons $p < N$. D'après (#37) et (#41), les valeurs apparaissant dans la ligne de p démarrent à $p+1$ et croissent strictement tant que N n'est pas atteinte. Il existe donc un entier ℓ, au plus égal à $N-p-1$, vérifiant $p * \ell = N$. D'après (#42), on a alors $p * (\ell + 1) = p * 1$. Or, on a vu ci-dessus l'égalité $p * q = (p * (q-1)) * (p+1)$ pour $q \geqslant 2$, d'où l'implication $p * (q'-1) = p * (q-1) \Rightarrow p * q' = p * q$ pour $q, q' \geqslant 2$. De là, partant de $p * (1 + \ell) = p * 1$, on déduit inductivement $p * (q + \ell) = p * q$ pour tout q, ce qui est dire que ℓ valeurs se répètent périodiquement sur la ligne de p. □

3.A.3.— Pour $N = 2^n$, (#37) coïncide avec (#16), le système S_N de 2 est la table A_n de 3.1.1, et l'unicité de cette dernière est donc établie. En revanche, il n'est pas clair que S_N soit une SD-structure : la table de S_N est construite en utilisant les instances particulières (#38) de la loi (SD), mais cela ne suffit pas à impliquer que toutes les instances de celles-ci soient satisfaites. De fait, on va montrer qu'elles ne le sont que si N est puissance de 2. La démonstration se fait en plusieurs étapes, toutes fondés sur des arguments de récurrence sur les lignes ou les colonnes des tables.

Lemme.— *La structure S_N est une* SD*-structure si, et seulement si, pour tout p, la période de p dans S_N divise N.*

Démonstration. Par définition, la période de p dans S_N est le plus petit entier ℓ satisfaisant $p*\ell = N$, et on a alors $p*q = N$ si, et seulement si, q est multiple de ℓ. Par conséquent, les conditions $\ell \mid N$ et $p*N = N$ sont équivalentes, et il s'agit donc de montrer que S_N est une SD-structure si, et seulement si, l'égalité $p * N = N$ est vraie pour tout p.

Or, supposons que S_N est une SD-structure. Alors, par (#40), on a $N * N = N$, d'où $(p*N)*(p*N) = p*(N*N) = p*N$ pour tout p en appliquant (SD). D'un autre côté, d'après (#39), si on a $p*N < N$, alors on doit avoir $(p*N)*(p*N) > p*N$. La seule possibilité est donc d'avoir $p * N = N$.

Inversement, supposons que, pour tout p, on a $p*N = N$ dans S_N. On va montrer l'égalité $p*(q*r) = (p*q)*(p*r)$ pour tous p, q, r en utilisant une induction sur p décroissant de N à 1 puis, pour p fixé, sur q décroissant de N à 1 puis, pour p et q fixés, sur r croissant de 1 à N.

Supposons d'abord $p = N$. Par (#40), on a $p * x = x$ pour tout x, et on trouve $p * (q * r) = q * r = (p * q) * (p * r)$.

Supposons maintenant $p < N$, et d'abord $q = N$. Par (#40), on a $q * r = r$, d'où $p * (q * r) = p * r$. D'un autre côté, par hypothèse, on a $p * q = N$, d'où, par (#40), $(p * q) * (p * r) = p * r$.

Supposons finalement $p < N$ et $q < N$. Pour $r = 1$, (#38) donne l'égalité escomptée. Pour $r = r' + 1 \geqslant 2$, on a $q * r = (q * r') * (q * 1)$ par (#38), d'où

$$\begin{aligned}
p * (q * r) &= p * ((q * r') * (q * 1))\\
&= (p * (q * r')) * (p * (q * 1))\\
&\qquad \text{par hypothèse d'induction puisque, par (\#40), on a } q * r' > q\\
&= ((p * q) * (p * r')) * (p * (q * 1))\\
&\qquad \text{par hypothèse d'induction puisque l'on a } r' < r\\
&= ((p * q) * (p * r')) * ((p * q) * (p * 1)) && \text{par (\#38)}\\
&= (p * q) * ((p * r') * (p * 1))\\
&\qquad \text{par hypothèse d'induction puisque, par (\#40), on a } p * q > p\\
&= (p * q) * (p * (r' * 1)) && \text{par (\#38)}\\
&= (p * q) * (p * r).
\end{aligned}$$

L'induction est donc complète et, par conséquent, S_N est une SD-structure. □

3.A.4.— L'étape suivante consiste à comparer les opérations dans S_N et $S_{N'}$, et en particulier les périodes, lorsque N' est multiple de N.

Lemme.— *Si N' est multiple de N, l'application* pr *qui envoie chaque entier de $\{1, ..., N'\}$ sur l'unique entier de $\{1, ..., N\}$ qui lui est congru modulo N est un homomorphisme de $S_{N'}$ sur S_N.*

Démonstration. Notant $*'$ l'opération de $S_{N'}$ et $*$ celle de S_N, on va montrer l'égalité $\mathrm{pr}(p *' q) = \mathrm{pr}(p) * \mathrm{pr}(q)$ pour tous p, q par induction sur p décroissant de N' à 1 et, pour p fixé, sur q croissant de 1 à N'. Pour $p = N'$, on trouve

$$\begin{aligned}
\mathrm{pr}(p *' q) &= \mathrm{pr}(N' *' q) = \mathrm{pr}(q) && \text{par (\#40) dans } S_{N'},\\
&= N * \mathrm{pr}(q) = \mathrm{pr}(p) * \mathrm{pr}(q) && \text{par (\#40) dans } S_N.
\end{aligned}$$

Pour $p < N'$ et $q = 1$, on trouve

$$\mathrm{pr}(p *' q) = \mathrm{pr}(p + 1) = \mathrm{pr}(p) + 1 = \mathrm{pr}(p) * 1 = \mathrm{pr}(p) * \mathrm{pr}(q)$$
dans le cas $\mathrm{pr}(p) < N$, par (#37) dans $S_{N'}$ et dans S_N.

$$\mathrm{pr}(p *' q) = \mathrm{pr}(p + 1) = 1 = \mathrm{pr}(q) = \mathrm{pr}(p) * \mathrm{pr}(q)$$
dans le cas $\mathrm{pr}(p) = N$, par (#37) dans $S_{N'}$ et (#40) dans S_N.

Enfin, pour $p < N'$ et $q = r + 1 \geqslant 2$, on trouve

$$\begin{aligned}
\mathrm{pr}(p *' q) &= \mathrm{pr}(p *' (r' *' 1)) \\
&= \mathrm{pr}((p *' r) *' (p' *' 1)) && \text{par (\#38) dans } S_{N'} \\
&= \mathrm{pr}(p *' r) * \mathrm{pr}(p' *' 1) \\
& \quad \text{par hypothèse d'induction eu égard à } p *' r > p \text{ par (\#39) dans } S_{N'} \\
&= (\mathrm{pr}(p) * \mathrm{pr}(r)) * (\mathrm{pr}(p) * 1) \\
& \quad \text{par hypothèse d'induction eu égard à } r < q \text{ et } 1 < q \\
&= \mathrm{pr}(p) * (\mathrm{pr}(r) * 1) && \text{par (\#38) dans } S_N \\
&= \mathrm{pr}(p) * \mathrm{pr}(r + 1) = \mathrm{pr}(p) * \mathrm{pr}(q) && \text{par } r < N \text{ et (\#37) dans } S_N. \ \square
\end{aligned}$$

3.A.5.— Conjugué avec le lemme chinois, 3.A.4 implique que, dans le cas $N = N_1 N_2$ avec N_1 et N_2 premiers entre eux, S_N est isomorphe au produit direct $S_{N_1} \times S_{N_2}$. L'étape suivante relie les périodes.

Lemme.— *Si N' est multiple de N, alors, pour tout $p < N'$, la période de p dans $S_{N'}$ est multiple de la période de* $\mathrm{pr}(p)$ *dans S_N ; de plus, on a $\pi_{S_{N'}}(p)/\pi_{S_N}(\mathrm{pr}(p)) \leqslant N'/N - \lfloor p/N \rfloor$.*

Démonstration. Soit ℓ la période de $\mathrm{pr}(p)$ dans S_N. Par (#41), on a

$$\mathrm{pr}(p) * 1 < \mathrm{pr}(p) * 2 < \cdots < \mathrm{pr}(p) * \ell = N.$$

Aucune des valeurs $\mathrm{pr}(p) * 1, \ldots, \mathrm{pr}(p) * (\ell - 1)$ n'est égale à N, donc, en vertu de 3.A.4, aucune des valeurs $p *' 1, \ldots, p *' (\ell - 1)$ dans $S_{N'}$ ne peut être égale à N', tandis que $p *' \ell$ doit être multiple de N, et on a donc

$$p *' 1 < p *' 2 < \cdots < p *' (\ell - 1) < p *' \ell = m_1 N$$

avec $m_1 \geqslant \lfloor p/N \rfloor + 1$ puisque l'on a $m_1 N \geqslant p *' 1 = p + 1 > p \geqslant \lfloor p/N \rfloor N$. Si on a $m_1 N = N'$, alors on obtient $\pi_{S_{N'}}(p) = \ell = \pi_{S_N}(\mathrm{pr}(p))$. Sinon, par 3.A.4 à nouveau, aucune des valeurs $p *' (\ell + 1), \ldots, p *' (2\ell - 1)$ ne peut être égale à N', tandis que $p *' 2\ell$ doit être multiple de N, et on obtient

$$\begin{aligned}
p *' 1 < p *' 2 < \cdots < p *' (\ell - 1) < p *' \ell = m_1 N \\
< p *' (\ell + 1) < \cdots < p *' (2\ell - 1) < p *' 2\ell = m_2 N
\end{aligned}$$

avec $m_2 \geqslant \lfloor p/N \rfloor + 2$ puisque l'on a $m_2 N > m_1 N$. Si on a $m_2 N = N'$, alors on obtient $\pi_{S_{N'}}(p) = 2\ell = 2\pi_{S_N}(\mathrm{pr}(p))$. Sinon, on recommence et on obtient

$$\begin{aligned}
p *' 1 < p *' 2 < \cdots < p *' (\ell - 1) < p *' \ell = m_1 N \\
< p *' (\ell + 1) < \cdots < p *' (2\ell - 1) < p *' 2\ell = m_2 N \\
< p *' (2\ell + 1) < \cdots < p *' (3\ell - 1) < p *' 3\ell = m_3 N
\end{aligned}$$

avec $m_3 \geqslant \lfloor p/N \rfloor + 3$ puisque l'on a $m_3 N > m_2 N$, et ainsi de suite tant que N' n'est pas atteint. Or, à la $k^{\text{ième}}$ étape, on a $m_k \geqslant \lfloor p/N \rfloor + k$, d'où $m_k N > N'$ pour $k > N'/N - \lfloor p/N \rfloor$. Par conséquent, on atteint N' après au plus $N'/N - \lfloor p/N \rfloor$ étapes, ce qui est affirmer $\pi_{S_{N'}}(p) = k\ell = k\pi_{S_N}(\mathrm{pr}(p))$ pour un entier k au plus égal à $N'/N - \lfloor p/N \rfloor$. $\square$

$\triangleright$ *Par exemple,* 3.A.5 *implique que, pour $N' = 3N$, les périodes des $N - 1$ dernières lignes de $S_{N'}$ sont les mêmes que celles des lignes correspondantes de S_N, puis que les périodes des N lignes médianes sont les précédentes multipliées par* 1 *ou* 2, *et enfin que les périodes des N premières lignes sont les précédentes multipliées par* 1, 2, *ou* 3. $\triangleleft$

3.A.6.— On est enfin en mesure de déterminer si S_N est une SD-structure.

Lemme.— *La structure S_N est une* SD*-structure si, et seulement si, N est une puissance de* 2.

Démonstration. On montre d'abord par induction sur n que, pour tout n, la structure S_{2^n} est une SD-structure. Par 3.A.3, il suffit de montrer que, pour tout $p < 2^n$, la période de p dans S_{2^n} divise 2^n. Pour $n = 1$, on a $\pi_{S_1}(1) = 1$, et le résultat est vrai. Supposons $n \geqslant 2$, et considérons $p < 2^n$. Trois cas sont possibles. Pour $p = 2^n$, on a $\pi_{S_{2^n}}(p) = 2^n$ par (#40). Pour p compris entre $2^{n-1}+1$ et 2^n-1, le lemme 3.A.5 implique que la période de p dans S_{2^n} est la même que celle de $\mathrm{pr}(p)$ (c'est-à-dire de $p - 2^{n-1}$) dans $S_{2^{n-1}}$, laquelle divise 2^{n-1} par hypothèse de récurrence, donc *a fortiori* 2^n. Enfin, pour p compris entre 1 et 2^{n-1}, 3.A.5 implique que la période de p dans S_{2^n} est soit la même, soit le double de celle de $\mathrm{pr}(p)$ (c'est-à-dire de p) dans $S_{2^{n-1}}$: par hypothèse de récurrence, cette dernière divise 2^{n-1} et donc, dans tous les cas, $\pi_{S_{2^n}}(p)$ divise 2^n. Donc, S_{2^n} est une SD-structure.

Supposons maintenant $N = 2^n N'$ avec N' impair et $N' \geqslant 3$. Soit $p := N - 2^{n+1}$, donc $p = 2^n(N' - 2)$. On va montrer que la période de p dans S_N est 2^{n+1}, qui ne divise pas N, et, de là, par 3.A.3, S_N n'est pas une SD-structure. Pour cela, on montre par induction sur q croissant de 1 à 2^{n+1} que, dans S_N, on a $p * q = p + q$. Pour $q = 1$, on a $p * q = p + 1$ par (#37), et le résultat est vrai. Supposons $q = r + 1$ avec $1 \leqslant r < 2^{n+1}$. Par (#38), on a $p * q = p * (r * 1) = (p * r) * (p * 1)$, d'où $p * q = (p + r) * (p + 1)$ par hypothèse d'induction et par (#37). Pour $r < 2^n$, 3.A.5 implique que la période de $p + r$ dans S_N est soit la même, soit le double de celle de $\mathrm{pr}(p + r)$, c'est-à-dire de r, dans S_{2^n}. Puisque S_{2^n} est une SD-structure, cette dernière période divise 2^n, et l'hypothèse $r < 2^n$ entraîne $\pi_{S_{2^n}}(\mathrm{pr}(r)) < 2^n$, donc $\pi_{S_{2^n}}(\mathrm{pr}(r))$ divise 2^{n-1}, et donc $\pi_{S_N}(p+r)$ divise 2^n. Pour $2^n \leqslant r < 2^{n+1}$, 3.A.5 implique que la période de $p + r$ dans S_N est celle de $\mathrm{pr}(p + r)$, c'est-à-dire de $r - 2^n$, dans S_{2^n}, et donc à nouveau $\pi_{S_N}(p+r)$ divise 2^n. Pour tout r considéré, $\pi_{S_N}(p+r)$ divise donc p d'où, par définition de la période, $(p+r)*(1+p) = (p+r)*1$, et, de là, $p * q = (p + r) + 1 = p + q$. Donc, S_N n'est pas une SD-structure. □

▷ *On pourra par exemple vérifier que S_6 n'est pas une* SD*-structure car la période de* 2 *dans S_6 est* 4. *Dans le cas de S_6, il s'agit de la seule période qui ne divise pas* 6, *mais cela suffit à ce que, sur les* 216 *triplets pouvant être formés à partir des éléments de la table,* 31 *violent la loi* (SD). ◁

3.A.7.— La démonstration de 3.1.1 est maintenant complète. À partir de là, on peut également compléter la démonstration des autres propriétés affirmées dans la sous-section 3.1.

Démonstration de 3.1.5. On a déjà noté que A_n est engendré par 1, et que la relation $1_{[2^n+1]} = 1$ est vérifiée dans A_n. Montrer que cette relation présente A_n signifie montrer que, si $\mathcal{F}$ est la SD-structure libre de base $\{1\}$, alors la congruence $\equiv$ sur $\mathcal{F}$ telle que A_n est (isomorphe à) $\mathcal{F}/{\equiv}$ est le plus petite congruence sur $\mathcal{F}$ contenant la paire $(1_{[2^n+1]}, 1)$. Or, supposons que $\simeq$ est une congruence sur $\mathcal{F}$ contenant $(1_{[2^n+1]}, 1)$. On veut montrer que $\simeq$ inclut $\equiv$.

Soit S la structure-quotient $\mathcal{F}/\simeq$ et soit s la classe de 1 dans S. Par hypothèse, S est une SD-structure engendrée par s et, dans S, on a $s_{[2^n+1]} = s$. Soit ϕ l'application de A_n dans S définie par $\phi(p) = s_{[p]}$. On va montrer que ϕ est un homomorphisme en établissant l'égalité $\phi(p * q) = \phi(p) * \phi(q)$ par induction sur p décroissant de 2^n à 1 et, pour p fixé, sur q croissant de 1 à 2^n. Comme préliminaire, on montre par induction sur q croissant de 1 à 2^n l'égalité $s_{[2^n]} * s_{[q]} = s_{[q]}$ dans S : pour $q = 1$, c'est l'hypothèse, pour $q = r + 1 \geqslant 2$, on trouve

$$\begin{aligned} s_{[2^n]} * s_{[q]} &= s_{[2^n]} * (s_{[r]} * s) \\ &= (s_{[2^n]} * s_{[r]}) * (s_{[2^n]} * s) && \text{par (SD) dans } S \\ &= s_{[r]} * s = s_{[q]} && \text{par hypothèse d'induction et hypothèse sur } s. \end{aligned}$$

Appliquant ce qui précède, on trouve pour $p = 2^n$

$$\phi(p * q) = \phi(2^n * q) = \phi(q) = s_{[q]} = s_{[2^n]} * s_{[q]} = \phi(p) * \phi(q).$$

Puis, pour $p < 2^n$ et $q = 1$, la définition de $s_{[p+1]}$ donne

$$\phi(p * q) = \phi(p + 1) = s_{[p+1]} = s_{[p]} * s = \phi(p) * \phi(q).$$

Enfin, pour $p < 2^n$ et $q = r + 1 \geqslant 2$, il vient

$$\begin{aligned} \phi(p * q) &= \phi(p * (r * 1)) = \phi((p * r) * (p * 1)) \\ &= \phi(p * r) * \phi(p * 1) \quad \text{par hypothèse d'induction eu égard à } p * r > p \\ &= (\phi(p) * \phi(r)) * (\phi(p) * \phi(1)) = (s_{[p]} * s_{[r]}) * (s_{[p]} * s) \\ &\qquad \text{par hypothèse d'induction eu égard à } r < q \text{ et } 1 < q \\ &= s_{[p]} * (s_{[r]} * s) = s_{[p]} * s_{[q]} = \phi(p) * \phi(q) \qquad \text{par (SD) dans } S. \end{aligned}$$

Notons Π et Π' les projections canoniques de $\mathcal{F}$ sur A_n et S, c'est-à-dire les homéomorphismes surjectifs qui envoient un élément de $\mathcal{F}$ sur sa classe *modulo* $\equiv$ et sur sa classe *modulo* $\simeq$, respectivement. Alors, $\phi \circ \Pi$ et Π' sont deux homomorphismes de $\mathcal{F}$ dans S envoyant 1 sur s, et, comme $\mathcal{F}$ est une SD-structure libre, on a $\phi \circ \Pi = \Pi'$. Par conséquent, pour f, g dans $\mathcal{F}$, l'égalité $\Pi(f) = \Pi(g)$, c'est-à-dire $f \equiv g$, implique $\Pi'(f) = \Pi'(g)$, donc $f \simeq g$. Cela montre que S est quotient de A_n, et donc que A_n admet la présentation annoncée. □

▷ *Un corollaire du résultat précédent est que, pour tout* $p \leqslant 2^n$*, il existe un entier* m *tel que la sous-structure de* A_n *engendrée par* p *est isomorphe à* A_m *: en effet, si* N *est le plus petit entier vérifiant* $p_{[N]} = 2^n$*,* 3.A.6 *implique que* N *est puissance de* 2*, et, de là,* 3.1.5 *donne le résultat.* ◁

Démonstration de 3.1.8. Par (#40), le cas $p = 2^n$ est trivial. Supposons $p < 2^n$. Que les valeurs de $p*q$ forment une suite strictement croissante à partir de $p+1$ tant que 2^n n'est pas atteint puis se répètent périodiquement est affirmé dans 3.A.2, et on a donc $\pi_n(p) = \pi_{S_{2^n}}(p)$. D'autre part, puisque A_n est une SD-structure, 3.A.3 affirme que $\pi_n(p)$ doit diviser 2^n, donc être une puissance de 2. □

3.A.8.— On termine avec quelques précisions supplémentaires sur le passage de A_{n-1} à A_n. Par 3.1.8, il suffit, pour spécifier la table A_n à partir de celle de A_{n-1}, de donner, pour chaque élément p, les $\pi_n(p)$ premières valeurs de la ligne de p. Soient donc p, q dans $\{1, ..., 2^n\}$, et posons $p' := \mathrm{pr}_n(p)$ et $q' := \mathrm{pr}_n(q)$. Par 3.1.9, on a, avec des notations qui devraient être claires,

$$\mathrm{pr}(p *_n q) = p' *_{n-1} q', \tag{\#43}$$

donc le point est de déterminer la valeur de $p *_n q$ parmi les deux antécédents possibles de $p' *_{n-1} q'$, à savoir $p' *_{n-1} q'$ et $p' *_{n-1} q' + 2^{n-1}$.

3.A.9.— On va établir que la connaissance d'un unique entier $\theta_n(p)$ détermine complètement la ligne de p dans la table de A_n.

Proposition (seuil).— *Soit $n \geqslant 1$. Pour tout $p \leqslant 2^n$, il existe un entier $\theta_n(p)$ (le* seuil *pour p) tel que, si $r_1 < \cdots < r_\ell$ apparaissent dans la ligne de* $\mathrm{pr}_n(p)$ *dans A_{n-1}, alors, dans la ligne de p dans A_n, apparaissent*

- $r_1 < \cdots < r_\ell < r_1{+}2^{n-1} < \cdots < r_\ell{+}2^{n-1}$ *dans le cas $\theta_n(p) = \ell$,*
- $r_1 < \cdots < r_{\theta_n(p)} < r_{\theta_n(p)+1}{+}2^{n-1} < \cdots < r_\ell{+}2^{n-1}$ *sinon.*

Démonstration. Pour $2^{n-1} \leqslant p < 2^n$, 3.1.8 implique $p *_n q > 2^{n-1}$, et, de là, les seules valeurs possibles pour la ligne de p au vu de (#43) sont

$$r_1 + 2^{n-1} < \cdots < r_\ell + 2^{n-1},$$

ce qui est le résultat avec $\theta_n(p) := 0$. Ensuite, par 3.A.3, on a $2^n *_n q = q$ pour tout q, ce qui donne le résultat avec $\theta_n(2^n) := 2^{n-1}$.

Supposons maintenant $p < 2^{n-1}$ avec $\pi_n(p) = 2\ell$. Dans A_n, on a alors nécessairement $p * \ell < 2^n$, donc $p * \ell = 2^{n-1}$. Dans ce cas, les ℓ premières valeurs de la ligne de p sont $\leqslant 2^{n-1}$, donc ce sont $r_1 < \cdots < r_\ell$, tandis que les ℓ suivantes sont nécessairement $r_1{+}2^{n-1} < \cdots < r_\ell{+}2^{n-1}$. On a donc le résultat avec $\theta_n(p) := \ell$.

Supposons enfin $p < 2^{n-1}$ avec $\pi_n(p) = \ell$. Dans A_n, on a nécessairement $p{*}\ell = 2^n$. D'un autre côté, on a $p * 1 = p + 1 \leqslant 2^{n-1}$. Les ℓ valeurs de la ligne de p vont en croissant, il existe donc un plus grand indice $i < \ell$ tel que la $i^{\text{ième}}$ valeur est $\leqslant 2^{n-1}$, et les valeurs doivent être $r_1 < \cdots < r_i < r_{i+1}{+}2^{n-1} < \cdots < r_\ell{+}2^{n-1} = 2^n$. On a donc le résultat annoncé avec $\theta_n(p) := i$. □

Le seuil $\theta_n(p)$ est le nombre de valeurs de la ligne de p dans A_{n-1} préservées dans la ligne de p dans A_n. La démonstration ci-dessus montre que l'on a toujours $\theta_n(p) = 0$ pour $2^{n-1} < p < 2^n$ et $\theta_n(2^n) = 2^{n-1}$, et donc que la moitié basse de la table de A_n est donc complètement déterminée à partir de la table de A_{n-1}. Pour la moitié haute, la situation est plus compliquée et on peut seulement affirmer que, pour $p \leqslant 2^{n-1}$, on a $1 \leqslant \theta_n(p) \leqslant \pi_{n-1}(p)$.

Exemple. Dans A_3, la période de 1 est 4 et le motif de base est $2 < 4 < 6 < 8$; dans A_4, la période de 1 reste 4, avec comme motif de base $2 < 12 < 14 < 16$. On a donc $\theta_4(1) = 1$: seule la première valeur est préservée, tandis que les trois autres sont translatées. De même, dans A_3, la période de 3 est 2, avec comme motif de base $4 < 8$, tandis que, dans A_4, la période de 3 passe à 4, avec le motif $4 < 8 < 12 < 16$. On a donc $\theta_4(3) = 2$.

3.A.10.— L'itération de 3.A.9 montre que la ligne de p dans A_n est déterminée, à partir de celle de 1 dans A_0 par la suite des seuils $\theta_k(p_k)$ pour $k = 1, \ldots, n$, où l'on introduit $p_n := p$, p_{n-1}, ... comme les projections successives de p.

Exemple. Soit à déterminer la ligne de 12 dans la table A_9. Les projections successives de 12 modulo 2^{n-1} et les valeurs correspondantes des seuils sont

k	1	2	3	4	5	6	7	8	9
p_k	2	4	4	12	12	12	12	12	12
$\theta_k(p_k)$	1	2	0	0	4	8	3	3	2

Partant de la ligne de 1 *dans* A_0*, qui correspond à* $\pi_0(1) = 1$ *avec le motif*
1,
on lit $\theta_1(2) = 1$*, donc le motif de la ligne de* 2 *dans* A_1 *s'obtient en dupliquant le précédent, d'où* $\pi_1(2) = 2$ *avec les valeurs*
1, 2.
Ensuite, on lit $\theta_2(4) = 2$*, donc le motif de la ligne de* 4 *dans* A_2 *s'obtient en dupliquant le précédent, d'où* $\pi_2(4) = 4$ *avec les valeurs*
1, 2, 3, 4.
Puis on lit $\theta_3(4) = 0$*, donc le motif de la ligne de* 4 *dans* A_3 *s'obtient en translatant le précédent, d'où* $\pi_3(4) = 4$ *avec les valeurs*
5, 6, 7, 8.
De $\theta_4(12) = 0$ *on déduit que le motif de la ligne de* 12 *dans* A_4 *s'obtient en translatant le précédent, d'où* $\pi_4(12) = 4$ *avec les valeurs*
13, 14, 15, 16.
De $\theta_5(12) = 4$ *on déduit que le motif de la ligne de* 12 *dans* A_5 *s'obtient en dupliquant le précédent, d'où* $\pi_5(12) = 8$ *avec les valeurs*
13, 14, 15, 16, 29, 30, 31, 32.
De $\theta_6(12) = 8$ *on déduit que le motif de la ligne de* 12 *dans* A_6 *s'obtient en dupliquant le précédent, d'où* $\pi_6(12) = 16$ *avec les valeurs*
13, 14, 15, 16, 29, 30, 31, 32, 45, 46, 47, 48, 61, 62, 63, 64.
De $\theta_7(12) = 3$ *on déduit que le motif de la ligne de* 12 *dans* A_7 *s'obtient en gardant* 3 *éléments et translatant les suivants, d'où* $\pi_7(12){=}16$ *et les valeurs*
13, 14, 15, 80, 93, 94, 95, 96, 109, 110, 111, 112, 125, 126, 127, 128.
De $\theta_8(12) = 3$ *on déduit que le motif de la ligne de* 12 *dans* A_8 *s'obtient en gardant* 3 *éléments et translatant les suivants, d'où* $\pi_8(12){=}16$ *et les valeurs*
13, 14, 15, 208, 221, 222, 223, 224, 237, 238, 239, 240, 253, 254, 255, 256.
Enfin, de $\theta_9(12) = 2$ *on déduit que le motif de la ligne de* 12 *dans* A_9 *s'obtient en gardant* 2 *éléments et translatant les suivants, d'où* $\pi_9(12){=}16$ *et les valeurs*
13, 14, 271, 464, 477, 478, 479, 480, 493, 494, 495, 496, 509, 510, 511, 512.

Les seuils itérés codent donc de façon compacte les valeurs apparemment chaotiques et imprédictibles apparaissant dans les lignes des tables A_n.

—==000==—

Repères chronologiques

▸ Les plongements élémentaires entre (fragments de) modèles de ZFC ont été étudiés à partir des années 1960, notamment par H. Gaifman (thèse en 1962) et W. Reinhardt (thèse en 1967).

▸ Les cardinaux forts ont été introduits par H. Gaifman en 1974 ; la notion aujourd'hui appelée cardinal de Woodin a été isolée par W.H. Woodin (né en 1955) en 1984.

▸ Les cardinaux supercompacts ont été introduits par R. Solovay (né en 1938) et W. Reinhardt en 1968.

▸ La borne de Kunen a été établie par K. Kunen (né en 1943) en 1971. Les axiomes I_1–I_3 ont été introduits par H. Gaifman en 1974 et R. Solovay–W. Reinhardt–A. Kanamori en 1978.

▸ Les tables de Laver ont été introduites et les applications mentionnées ici ont été établies par R. Laver (1942–2012) en 1994.

Résumé du chapitre XIV

▶ Sous des hypothèses faibles, l'ordinal critique d'un plongement élémentaire est un cardinal mesurable.

▶ Définis par l'existence d'extendeurs convenables, les cardinaux forts et de Woodin surpassent les cardinaux mesurables.

▶ Les cardinaux supercompacts dépassent les cardinaux de Woodin et correspondent à des ultrafiltres normaux sur les ensembles $\mathfrak{P}_{<\kappa}(\lambda)$.

▶ Il n'existe pas de plongement élémentaire de l'univers dans lui-même.

▶ Les cardinaux de Laver sont des points fixes pour l'autosimilarité. Ils dépassent tous les cardinaux précédemment introduits.

▶ La famille des plongements élémentaires associés à un cardinal de Laver est munie d'une opération autodistributive.

▶ Pour chaque n, la table de Laver A_n est une SD-structure monogène à 2^n éléments, sorte de contrepartie de $\mathbb{Z}/n\mathbb{Z}$ dans le monde autodistributif.

▶ Les tables de Laver sont des quotients des structures $\mathrm{Iter}(j)$ obtenues en itérant un plongement élémentaire.

▶ On répond aux questions de la sous-section 3.1 sur les périodes dans A_n en utilisant les propriétés des plongements de $\mathcal{E}_\lambda$.

▶ Quel que soit le statut logique final des résultats sur les périodes dans les tables de Laver, la théorie des ensembles aura joué un rôle essentiel dans leur découverte.

—==000==—