DIAGRAMMES

LAURENT COPPEY

Décompositions multiplicatives directes des entiers

Diagrammes, tome 65-66 (2011), p. 1-68

<http://www.numdam.org/item?id=DIA_2011__65-66__1_0>

DIAGRAMMES VOLUMES 65+66, 2011

DECOMPOSITIONS MULTIPLICATIVES DIRECTES DES ENTIERS

Première Partie

Laurent Coppey

Sommaire.

Introduction.

Ce texte répond à une question que se posait paraît-il Jean Dieudonné, au moins si j'en crois mon ami J. Roubaud (de l'Université Pierre et Marie Curie à Paris) qui me fit cette confidence au rayon "Mathématiques" du grand libraire parisien Joseph Gibert, peu de temps après que nous eûmes pris notre retraite… : décrire tous les couples (A,B) d'entiers tels que tout nombre non nul n s'écrive *de manière unique* comme un produit d'un élément de A et d'un élément de B, autrement dit décrire toutes les *décompositions directes multiplicatives* de l'ensemble des entiers non nuls. Question dont l'énoncé est très simple, mais dont « la » solution l'est nettement moins. Sans doute Jean Dieudonné se la posait-il en vue d'obtenir toutes les décompositions en produits de séries des fonctions L de Dirichlet (dont la fonction ζ). Bien sûr, le problème pose d'emblée celui de déterminer toutes les décompositions *directes additives* des puissances de **N**, mais il ne se réduit pas tout à fait à cela.

Rédigé entre 2003 et 2005, ce texte reprend et développe une petite partie de ma thèse (il s'agissait d'un exemple), qui date de 1975. J'ai compris (un peu tardivement certes) que j'avais fait le pas essentiel avec la dimension 2, mais surtout avec ma méthode. Ivan Niven était parvenu 2 ou 3 ans avant moi au même résultat (toujours en dim. 2) avec une méthode radicalement différente (opération de groupes…).

J'ai jugé « pédagogique » de donner à ce texte une forme générale graduée, liée à la dimension, ce qui permet de s'habituer progressivement à la structure de prémonoïde bien ordonné, pratiquement seule en cause ici. On ne doit surtout pas confondre la propriété de « forte associativité » (dont il est question ici) avec celle de « totale associativité » qui est assez banale et conséquence de celle-là. J'ai consacré les deux premières sections (0 et 1) à ces questions générales de prémonoïdes (bien ordonnés) et leurs décompositions.

J'ai respecté la chronologie de mes trouvailles, ce qui permet de bien mettre en évidence leur véritable origine, à savoir cette partie de ma thèse qui remonte à 1975 et qui a fait l'objet d'une conférence au Séminaire de Brême avec publication, quelque temps après.

Bien sûr, la plupart des résultats obtenus s'étendent sans trop de difficulté aux entiers de certains corps de nombres algébriques (par exemple, ceux qui sont totalement positifs), mais nous ne traiterons pas ici de ces « généralisations ».

Voici donc la première partie de ce texte (qui en comptera deux). On y trouvera la solution, en forme additive, pour les dimensions ≤ 3, avec des petites incursions en dimensions supérieures. La seconde partie traitera du cas général.

0. Précatégories et prémonoïdes.

Définition 0-1.
Une *précatégorie* **C** est un graphe multiplicatif satisfaisant l'axiome dit d'*associativité forte* suivant :

$$\forall\, x, y, z \in \mathbf{C}\ \ [\ [\ \exists\, z.(y.x) \vee \exists\, (z.y).x\ ]\ \Rightarrow\ \exists\, [\ z.(y.x) = (z.y).x\ ]\ ]$$

Par convention, une formule telle que $\exists\ [\ A(x,y,\ldots) = B(x,y,\ldots)]$ est un raccourci pour la formule suivante : $[\ \exists\ A(x,y,\ldots)\ ] \wedge [\ \exists\ B(x,y,\ldots)] \ \wedge\ [\ A(x,y,\ldots) = B(x,y,\ldots)\ ]$.

Ainsi, dans une précatégorie, il suffit qu'un des composés (z.y).x ou z.(y.x) existe pour que tous les deux existent et soient égaux ; on peut noter ce composé sous la forme z.y.x sans ambiguïté possible.

Soit D_n l'ensemble des dispositions cohérentes de parenthèses à n « places », ensemble dont le cardinal est appelé parfois le $n^{ième}$ nombre de Catalan. Soient $x_1, x_2, \ldots, x_n$ des éléments d'un système multiplicatif et d_n un élément de D_n ; la formule $\exists\ d_n(x_1, x_2,\ldots, x_n)$ signifie que le calcul de l'expression $d_n(x_1, x_2,\ldots, x_n)$ est possible dans le système multiplicatif en question, et le résultat de ce calcul est naturellement désigné aussi par $d_n(x_1, x_2,\ldots, x_n)$.

Définition 0-2.
Un graphe multiplicatif **G** est dit *complètement associatif* s'il satisfait l'axiome d'*associativité complète* suivant :

$$\forall\, n \geq 3 \qquad \forall\, x_1,x_2,, x_n \in \mathbf{G} \qquad \forall\, d_n\,,\, \delta_n \in D_n$$
$$[\exists\, d_n(x_1,x_2,..,x_n) \wedge \exists\, \delta_n(x_1,x_2,..,x_n)\ ] \Rightarrow d_n(x_1,x_2,..,x_n) = \delta_n(x_1,x_2,..,x_n)$$

Proposition 0-1.
Une précatégorie est un graphe multiplicatif *complètement associatif.*

► On démontre cela par récurrence sur n , comme s'il s'agissait de lois de composition partout définies. Pour $n = 3$, on se reporte à la définition même, puisqu'il n'y a que 2 dispositions cohérentes de parenthèses. Supposons donc le résultat vrai jusqu'à l'ordre n-1 , et $n \geq 4$; soit $d_n(x_1, x_2,\ldots, x_n)$ une expression définie dans la précatégorie en question. Il existe un entier k, $1 \leq k < n$, tel qu'on puisse écrire :

$$d_n(x_1, x_2,\ldots, x_n) = d_k(x_1, x_2,\ldots, x_k).\ d_{n-k}(x_{k+1}, x_{k+2},\ldots, x_n)\ ;$$

l'hypothèse de récurrence entraîne qu'on peut écrire $d_k(x_1, x_2,\ldots, x_k)$ sous la forme d'un composé tel que $x_1.d_{k-1}(x_2, x_3,\ldots, x_k)$ (si $k = 1$, la partie « $d_{k-1}(x_2, x_3,\ldots, x_k)$ » de cette dernière expression est vide) ; on a alors :

$$d_n(x_1, x_2,\ldots, x_n) \ = \ (x_1.d_{k-1}(x_2, x_3,\ldots, x_k)).d_{n-k}(x_{k+1}, x_{k+2},\ldots, x_n)\ ;$$

si $k \geq 2$, on peut utiliser la propriété de définition de précatégorie et valider ainsi la formule:

$$\exists\ (x_1.d_{k-1}(x_2, x_3,\ldots, x_k)).d_{n-k}(x_{k+1}, x_{k+2},\ldots, x_n) \ = \ x_1.(d_{k-1}(x_2, x_3,\ldots, x_k).d_{n-k}(x_{k+1}, x_{k+2},\ldots, x_n))\ ;$$

en désignant par ∂_p la disposition cohérente canonique de parenthèses qui « rejette à droite » toutes les parenthèses fermantes, et en appliquant l'hypothèse de récurrence, on voit que :

$$\exists\ d_{k-1}(x_2, x_3,\ldots, x_k)).d_{n-k}(x_{k+1}, x_{k+2},\ldots, x_n) = \partial_{n-1}(x_2, x_3,\ldots, x_n)\ ;$$

et comme $x_1.\partial_{n-1}(x_2, x_3,\ldots, x_n) = \partial_n(x_1, x_2,\ldots, x_n)$, on en conclut que l'on a bien :

$$\exists\ d_n(x_1, x_2,\ldots, x_n) = \partial_n(x_1, x_2,\ldots, x_n)\ ;$$

formule qu'on obtient aussi, mais directement lorsque $k = 1$, et, si $k = 2$, on applique directement l'hypothèse de récurrence à $d_{n-1}(x_2, x_3,\ldots, x_n)$. Comme la disposition d_n est a priori quelconque, ceci achève la démonstration ◄

Cette proposition signifie donc que la *forte associativité* entraîne la *complète associativité,* mais l'inverse n'est pas vrai , comme le montre l'exemple prototype suivant : le graphe multiplicatif ayant trois flèches consécutives x,y,z (qui ne soient pas des identités) et trois autres composés non triviaux, à savoir z.y et y.x et z.(y.x), est évidemment complètement associatif, mais non fortement associatif, puisque le composé (z.y).x n'existe pas !

Remarques.
1) Dans une précatégorie, une expression du genre $\exists\ x_1.x_2\ldots x_n$ est valide dès lors qu'une au moins des expressions du genre $\exists\ d_n(x_1,x_2,..,x_n)$ est valide.

2) Une catégorie est une précatégorie particulière, dans laquelle y.x est défini dès lors que $\alpha(y) = \beta(x)$, α et β désignant respectivement les applications source et but.

3) Un graphe orienté s'identifie à une précatégorie particulière dans laquelle les seuls composés définis sont les composés triviaux (i.e. du genre $\beta(x).x$ ou $x.\alpha(x)$).

Définition 0-3.
Un *prémonoïde* est une précatégorie à un seul objet, lequel est identifié à l'élément neutre qu'il définit.
Un prémonoïde **M** est dit *commutatif* s'il satisfait l'axiome suivant :

$$\forall\ x, y \in \mathbf{M}\ [\ \exists\ y.x\ \Rightarrow\ [\exists\ x.y = y.x]\ ]$$

Définition 0-4.
Un *homomorphisme* $f : \mathbf{C} \rightarrow \mathbf{D}$ entre précatégories est déterminé par la donnée d'une précatégorie « source » **C**, d'une précatégorie « but » **D** et d'un *foncteur* f de **C** dans **D**, i.e. d'une application f de **C** dans **D** satisfaisant les axiomes suivants :

$$\forall\ e \in \mathbf{C}_0\ [\ f(e) \in \mathbf{D}_0\ ]$$
$$\forall\ x,y \in \mathbf{C}\ [\ \exists\ y.x\ \Rightarrow\ [\ \exists\ f(y).f(x) = f(y.x)\ ]\ ]$$

Ces homomorphismes se composent et constituent ainsi la catégorie **PréCat** des « petites » précatégories. Elle admet la catégorie **Cat** des « petites » catégories comme sous-catégorie pleine ; elle admet aussi comme sous-catégorie pleine la catégorie **Gro** des « petits » graphes

orientés, étant entendu qu'on identifie un graphe orienté au graphe multiplicatif trivial, dans lequel les seuls composés définis sont du genre : $x.\alpha(x) = \beta(x).x = x$. On dispose aussi de la catégorie **Gmca** des « petits » graphes multiplicatifs complètement associatifs, dont **PréCat** est une sous-catégorie pleine.

Proposition 0-2.
Tout graphe multiplicatif complètement associatif **C** engendre librement une catégorie **C**' dans laquelle il se plonge.

► Soit L(**C**) la catégorie libre des chemins propres du graphe orienté sous-jacent à **C** ; les éléments de L(**C**) sont les unités $e \in \mathbf{C}_0$ et tous les n-uples d'éléments non-unités de **C** $(x_n,x_{n-1},\ldots, x_1)$, $n \geq 1$, satisfaisant : $\forall\ 1 \leq k < n\ \ \beta(x_k) = \alpha(x_{k+1})$, encore appelés chemins propres de **C**; la source d'un tel chemin est la source de son premier élément x_1 et son but est le but de son dernier élément x_n : à part les composés triviaux (avec sources et buts) il y a les couples de chemins consécutifs qui se composent naturellement par simple juxtaposition. Dans L(**C**) on dispose de la relation d 'équivalence bicompatible engendrée par la relation qui identifie les chemins $(x_n,x_{n-1},\ldots, x_1)$ et (y) dès lors que, dans **C**, on a : $\exists\ d_n(x_n, x_{n-1},..,x_1) = y$; on vérifie facilement que le quotient **C**' = L(**C**) / ~ est une catégorie et que l'homomorphisme naturel de **C** dans **C**' ($x \mapsto (x)\mathrm{mod}\sim$) est injectif ◄

On peut dire qu'à isomorphisme près, un graphe complètement associatif est un sous-graphe multiplicatif d'une catégorie ; on obtient donc un objet de ce genre à partir d'une catégorie en « enlevant » de celle-ci des flèches et de la composition ; on peut procéder de la manière suivante: soit **C** une catégorie ; soit **G** un sous-graphe orienté du graphe orienté **C** sous-jacent à **C** ; soit **G**$*$**G** l'ensemble de tous les couples (y,x) d'éléments de **G** composables dans **C** et dont le composé y.x est encore dans **G** ; on constitue alors un graphe multiplicatif complètement associatif **G** en choisissant pour ensemble **G**$*$**G** un sous-ensemble quelconque de **G**$*$**G** contenant au moins les couples triviaux (i.e. ceux de la forme $(x,\alpha(x))$ ou $(\beta(x),x)$) , étant bien entendu que les valeurs des composés dans **G** sont celles qui prévalent dans **C**.

En particulier, toute précatégorie engendre librement une catégorie dans laquelle elle se plonge.

Engendrements.
Soit **C** une précatégorie et A une partie de **C** ; on dispose dans A d'une *loi de composition partielle induite* par celle de **C**, notée « $._A$ », définie de la manière suivante :

$$\forall\ x,y \in A\ \ [\ \exists\ y._A x\ \Leftrightarrow [\ \exists\ y.x \in \mathbf{C}\ \wedge y.x \in A\ ]\ ]\ ,$$

et on pose alors: $y._A x = y.x$.
L'objet **A** = $(A, ._A)$ est un graphe multiplicatif complètement associatif si et seulement si A contient $A_0 = \alpha(A) \cup \beta(A)$, mais en général ce n'est pas une précatégorie.

Soit U : **PréCat** $\rightarrow$ **Ens** le foncteur d'oubli naturel qui « oublie » la composition partielle. Soit **C** une précatégorie et A une partie de **C** contenant avec tout élément x ses source et but, $\alpha(x)$ et $\beta(x)$ (A définit donc un sous-graphe orienté de **C**). Notons **A** = $(A, ._A)$ le graphe multiplicatif induit par **C** sur A.

Proposition 0-3.
A est une sous-précatégorie de **C** (ou U-sous-structure de **C**) si et seulement si **A** est une précatégorie.

► Supposons d'abord que **A** soit une précatégorie ; l'inclusion $\mathbf{A} \to \mathbf{C}$ définit un foncteur, car on a :

$$\forall\, x,y \in A\ [\ \exists\, y._A x\ \Rightarrow [\ \exists\, y.x \in \mathbf{C}\ \wedge\ y.x = y._A x\ ]\ ]\ ,$$

par définition de la loi induite « $._A$ » ; de plus, si $F : \mathbf{D} \to \mathbf{C}$ est un foncteur entre précatégories tel que $F(D) \subset A$, alors la restriction de F (au but), soit $F' : \mathbf{D} \to \mathbf{A}$ est un foncteur : en effet, si $z = y.x$ est défini dans **D** , alors F(y).F(x) est défini dans **C** et on a l'égalité : F(y).F(x) = F(z) ; comme F(x), F(y), F(z) sont tous trois éléments de A, on voit que $F(y)._A F(x)$ est défini dans **A** et $F'(z) = F'(y)._A F'(x)$, ce qui prouve que **A** est bien une U-sous-structure de **C**.
Réciproquement, soit $\mathbf{A}^{\propto}$ une sous-précatégorie de **C** relative à U, ayant A pour ensemble d'éléments sous-jacent ; supposons $y.x$ défini dans $\mathbf{A}^{\propto}$; alors y.x est défini dans **C** et a même valeur (d'où, avec anticipation, la même notation pour les composés !), car l'inclusion définit un foncteur ; comme le composé est dans A par hypothèse, on en conclut que $y._A x$ est défini et égal à y.x ; supposons aussi $y._A x$ défini, pour la loi induite par **C** sur A ; soit **Z** la précatégorie constituée des trois éléments x,y et $z = y.x$, des unités voulues et des couples composables triviaux et (y,x) (avec valeur y.x du composé, bien sûr) ; l'inclusion I de Z dans C détermine un foncteur entre précatégories tel que $I(Z) \subset A$; comme $\mathbf{A}^{\propto}$ est une sous-précatégorie de **C** , on en conclut que y.x (dans $\mathbf{A}^{\propto}$) est défini et vaut $y._A x$, de sorte que la loi de $\mathbf{A}^{\propto}$ n'est autre que la loi induite par **C** sur A ; comme $\mathbf{A}^{\propto}$ est une précatégorie, ceci achève la démonstration.
La notation spéciale $\mathbf{A}^{\propto}$ devient donc inutile : il suffit de savoir que **A** est une précatégorie pour affirmer que c'est une sous-précatégorie de **C** ; toute sous-précatégorie de **C** est de cette forme ◄
.
Définition 0-5.
Soit **C** un graphe multiplicatif et **A** un sous-graphe multiplicatif de **C**. On dira que **A** est *multiplicativement plein* dans **C**, s'il satisfait la condition suivante :

$$\forall\, x,y \in A\ [\ \exists\, y.x \in \mathbf{C} \Rightarrow y.x \in A\ ]$$

Tout sous-graphe multiplicativement plein **A** d'une précatégorie en est une sous-précatégorie. Bien évidemment, l'inverse n'est pas vrai, en général.

Définition 0-6.
Soit **C** un graphe orienté et A une partie de C ; on dit que A est *pleine* dans **C** si elle satisfait la condition suivante :

$$\forall\, x \in C\ [\ x \in A\ \Leftrightarrow \alpha(x)\ ,\ \beta(x) \in A\ ]$$

Par définition, une partie pleine d'un graphe orienté définit déjà elle-même un graphe orienté.

Proposition 0-4.
Soit **C** un graphe orienté (resp. un graphe multiplicatif, un graphe multiplicatif complètement associatif, une précatégorie, une catégorie) et soit A une partie *pleine* de C. Alors le système multiplicatif **A** induit par **C** sur A est lui-même un graphe orienté (resp. un graphe

multiplicatif, un graphe multiplicatif complètement associatif, une précatégorie, une catégorie) et c'est dans chaque cas une sous-structure.

► Seul le cas de précatégorie nécessite un peu d'attention : le composé $y._A x$ est défini dans **A** si et seulement si y.x est défini dans **C** ; soient x,y,z ∈ A et supposons $z._A(y._A x)$ défini ; alors, d'après ce qui vient d'être rappelé, z.(y.x) est défini dans **C** ; comme **C** est une précatégorie, (z.y).x est aussi défini dans **C** (et égal à z.(y.x) !) ; comme **A** est multiplicativement plein dans **C**, z.y ∈ A ; alors, et pour la même raison (z.y).x ∈ A aussi ; le composé $(z._A y)._A x$ est donc bien défini dans **A**, et évidemment égal à $z._A(y._A x)$, puisque les deux sont égaux à z.y.x. Ainsi **A** est une précatégorie. D'après la proposition **0-3** c'est donc une sous-précatégorie de **C** ◄

Une sous-précatégorie pleine d'une précatégorie est multiplicativement pleine, mais la réciproque n'est pas vraie.

Proposition 0-5.
Soit **C** une précatégorie et **A** un sous-graphe multiplicatif de **C** ; il est complètement associatif ; il engendre dans **C** les sous-structures suivantes, relatives aux foncteurs d'oubli usuels : précatégorie, précatégorie multiplicativement pleine, précatégorie pleine.

• *Sous-précatégorie engendrée* : la sous-précatégorie $\mathbf{A}^{/p}$ engendrée par A est construite par récurrence comme suit : posons $\mathbf{A}_1 = \mathbf{A}$; supposons les $\mathbf{A}_k$ définis pour k = 1,2,…,n ; on définit $\mathbf{A}_{n+1}$ à partir de $\mathbf{A}_n$ par la formule ci-dessous, dans laquelle $*\mathbf{X}^3$ désigne l'ensemble des triplets de flèches consécutives de **X** (la première étant notée le plus à droite) :
$\mathbf{A}_{n+1} = \{ t \in C \mid \exists (z,y,x) \in *\mathbf{A}_n^{\,3} [[z.y,(z.y).x \in \mathbf{A}_n \wedge t = y.x] \vee [y.x,z.(y.x) \in \mathbf{A}_n \wedge t = z.y]] \}$
Alors $\mathbf{A}^{/p} = \mathbf{A}_1 \cup \mathbf{A}_2 \cup \ldots \cup \mathbf{A}_n \cup \ldots$est la plus petite sous-précatégorie de **C** contenant A.
Le plus petit entier n , s'il existe, tel que $\mathbf{A}^{/p} = \mathbf{A}_1 \cup \mathbf{A}_2 \cup \ldots \cup \mathbf{A}_n$ est noté n(A), sinon on pose n(A) = ∞.

On notera que dans un prémonoïde commutatif **M** la formule d'engendrement de $\mathbf{A}^{/p}$ à partir de **A** se simplifie en la suivante :

$$\mathbf{A}_{n+1} = \{ t \in M \mid \exists (z,y,x) \in *\mathbf{A}_n^{\,3} [z.y,(z.y).x \in \mathbf{A}_n \wedge t = y.x] \} ;$$

• *Sous-précatégorie multiplicativement pleine engendrée* : c'est la structure induite par **C** sur l'ensemble $\mathbf{A}^{*p}$ suivant :

$$\mathbf{A}^{*p} = \{ z \in \mathbf{C} \mid \exists x_1, x_2, \ldots, x_n \in A \wedge \exists [z = x_n.x_{n-1}\ldots x_1] \} ;$$

cette formule a bien un sens puisque, dans une précatégorie, l'associativité portant sur n éléments résulte de celle portant sur 3 éléments (proposition **0-1**) (ce qui n'est pas vrai dans un graphe multiplicatif, même complètement associatif) .

• *Sous-précatégorie pleine engendrée* : la sous-précatégorie pleine $\mathbf{A}^{pp}$ engendrée par **A** est constituée de tous les x ∈ C tels que α(x) et β(x) ∈ A_0 .

Remarque. On a : $A \subset A^{/p} \subset A^{*p} \subset A^{pp}$ et ces inclusions sont en général strictes . Voici un exemple. On prend pour précatégorie **C** le monoïde additif **N** et pour **A** le sous-graphe additif (ici l'addition fait office de « multiplication des flèches » !) induit par **N** sur l'ensemble de nombres suivant : A = 7.B , avec B = {0, 1, 2, 3, 6}, soit A = { 0, 7, 14, 21, 42 }.

Il est clair que $\mathbf{B}^{/p} = \mathbf{B}_1 = [0,6]$ et $\mathbf{A}^{/p} = \mathbf{A}_1 = 7.\mathbf{B}_1 = 7.[0,6] = \{ 0,7, 14, 21, 28, 35, 42\}$; par contre $\mathbf{B}^{*p} = 7.\mathbf{N}$ et $\mathbf{B}^{pp} = \mathbf{N}$. Bien sûr, on peut, dans ce type d'exemple, mettre à la place de 7 un nombre quelconque mais > 1.

Exemples dans le monoïde (**N**,+).
Dans le monoïde additif **N** il y a plusieurs problèmes intéressants. Certains sont résolus (depuis longtemps déjà), d'autres non. Citons seulement ceux-ci :

(i) On peut déterminer toutes les décompositions additives de **N** (voir plus loin), c'est-à-dire les familles de parties $(A_k)_{k \in K}$ de **N** telles que $\mathbf{N} = \bigoplus_{k \in K} A_k$, notation suggestive qui signifie, précisons-le, que tout entier n s'écrit de manière unique sous la forme $n = \sum_{k \in K} a_k$, où $a_k \in A_k$. L'ensemble d'indexation K peut être fini ou non, chaque facteur A_k aussi peut être fini ou non (tous les cas possibles a priori se présentent effectivement !). Quelle que soit la décomposition en cause, chaque facteur A_k détermine avec la structure additive induite un sous-prémonoïde $\mathbf{A}_k$ de **N.** Il semble difficile de démontrer qu'un facteur direct A de **N** définit un sous-prémonoïde additif **A** de **N** sans connaître «a priori » sa structure « fine » (liée à l'existence d'une certaine base généralisée de **N-**voir plus loin) ; cette question reste posée.

(ii) Une autre question est de caractériser simplement les sous-prémonoïdes de **N**, et pas seulement ceux qui sont facteurs directs de **N**. Parmi ces sous-prémonoïdes, il y a ceux qui sont indécomposables, et que j'ai proposé d'appeler les « nouveaux nombres premiers » , au moins ceux qui sont finis; en effet, les seules « parties-segments » **n** = [0,n-1] indécomposables sont celles correspondant aux entiers n premiers, et il est assez facile d'indiquer les décompositions additives d'un segment **n** en fonction de la décomposition de n en facteurs premiers (voir plus loin); par contre, il semble assez difficile de caractériser les « nouveaux nombres premiers » **A** ; notons quand même qu'une condition suffisante pour que **A** soit premier est que card(A) soit premier, mais c'est bien peu de chose !

(iii) Il serait intéressant aussi de savoir s'il y a pour les sous-prémonoïdes (finis) de **N** une propriété généralisant l'unique décomposition en facteurs premiers des entiers (déjà, pour les parties-segments **n**, la question n'est pas triviale, mais relativement aisée…en tout cas équivalente à la question des décompositions directes générales additives de **N**).

(iv) Pour une partie A de **N** donnée, il est facile de décrire le sous-monoïde « additivement » plein $\mathbf{A}^{*p}$ engendré par A : ses éléments sont toutes les sommes finies d'entiers de la forme n.a, où $n \in \mathbf{N}$ et $a \in A$ et sa structure additive est la structure induite .

(v) Bien plus difficile est le problème consistant à caractériser ou à décrire $\mathbf{A}^{/p}$, ou même à calculer n(A) !

Voici quelques résultats (propositions **0-6-1** à **0-6-11**) montrant bien ces difficultés, concernant l'ensemble **P** = {0,1,2,3,5,7,11,13,…,59,…} des nombres premiers, auquel on a ajouté 0 et 1 :

Proposition 0-6-1.
Si $\mathbf{U} = \{ u_0 = 0, u_1 = 1,\ldots, u_n ,\ldots\} \subset \mathbf{N}$, avec $u_n < u_{n+1} < 2u_n$, alors $\mathbf{U}^{/p} = \mathbf{N}$.

► Montrons ce fait par récurrence. Supposons établie l'inclusion $[0,u_n] \subset \mathbf{U}_n$; on sait que l'on a : $u_{n+1} < 2u_n$; soit t un nombre strictement compris entre u_n et u_{n+1} ; on a $u_{n+1} = t + u$

avec $u < u_n$; mais $t = u_n + v$ avec $v < u_n$ aussi ; par l'hypothèse de récurrence, on voit que u et $v \in \mathbf{U}_n$; d'autre part u_n et $u_{n+1} \in \mathbf{U} \subset \mathbf{U}_n$; on a aussi les égalités :

$$u_{n+1} = t + u = (u_n + v) + u = u_n + (v + u) ,$$

d'où $v + u < u_n$, c'est-à-dire que l'élément $v + u \in \mathbf{U}_n$; ainsi, $u_{n+1} = u_n + (v + u)$, u, v, u_n, $u+v \in \mathbf{U}_n$, donc $t = u_n + v \in \mathbf{U}_{n+1}$, par construction même de $\mathbf{U}_{n+1}$ à partir de $\mathbf{U}_n$ ◄

Corollaire.
$\mathbf{P}^{/p} = \mathbf{N}$ (utilise le fait que $p_{n+1} < 2p_n$, où p_n désigne le $n^{ème}$ nombre premier).

Soit $\mathbf{J} = \{n \in \mathbf{N} \mid n-1 , n+1 \in P\backslash\{0\}\}$; si $n \in \mathbf{J}$, alors n-1 et n+1 sont tous deux premiers ; on dit que ce sont des entiers premiers *jumeaux* ; pour cette raison nous dirons d'un élément de **J** que c'est un *jumeleur*. On ne sait pas si l'ensemble **J** est fini ou non. Par contre, on sait que la somme $\Sigma_{n \in J}\ 1/n$ est finie ; $\mathbf{J} = \{ 2, 4, 6, 12 , 18, 30, 42, 60, \ldots\}$; soit $n \in \mathbf{J}$: si $n > 4$, alors $n = 0$ modulo 6 , de même, si $n > 6$, alors n = 0, 12 ou 18 modulo 30, etc…

Proposition 0-6-2.
$\mathbf{P}_1 = \mathbf{P} \cup \mathbf{J}$.

► Montrons alors que $P_1 = P \cup J$. Rappelons que l'on a :

$$P_1 = \{ n \in \mathbf{N} \mid \exists\ a,b,c \in P \mid a+b ,\ a+b+c \in P \ \wedge\ n = b+c \} ;$$

Pour plus de concision et de clarté, nous écrirons parfois : $n \in P_1$ [[a,b,c]] pour signifier que a,b,c,a+b,a+b+c ∈ P et n = b+c (et en conséquence $n \in P_1$).

D'abord, $P \subset P_1$, car si $n \in P$, on voit que $n \in P_1$ [[0,n,0]].
Ensuite, $J \subset P_1$ car si n-1 et n+1 ∈ P\{0} (i.e. $n \in J$), on voit que $n \in P_1$ [[1,1,n-1]].

Reste à voir que $P_1 \subset P \cup J$; supposons donc que $n \in P_1$ [[a,b,c]] et $n \notin P$; on a déjà : $n \geq 4$ et si n = 4, alors $n \in J$.
Supposons donc n > 4 .
Si n était impair, n+a = a+b+c serait premier et > 4, donc impair, et a serait pair donc a = 0 ou a = 2 ; 0 est exclu puisque $n \notin P$; donc a = 2 et $2+b \in P$; comme $b \neq 0$ (sinon $n = c \in P$!) , b+2 est impair, donc b aussi et c serait pair (et non = 0 !), i.e. c = 2 aussi ; mais alors n = 2+b serait élément de P, contrairement à l'hypothèse.
Ainsi, n est nécessairement pair ; mais $n+a \in P$ donc a est impair, tout comme b et c (b = c = 2 est à écarter puisque n > 4 ; b = 2 ou (exclusif) c = 2 est aussi à écarter puisque n est pair) ; alors $a+b \in P$ est pair, i.e. a+b = 2, d'où a = b = 1 et $a+b+c = n+1 \in P$, puis n = c+1, c = n-1 ∈ P et finalement $n \in J$. ◄

Proposition 0-6-3.
$\mathbf{P}_2 \neq \mathbf{N}$, les inclusions $\mathbf{P}_1 \subset \mathbf{P}_2 \subset \mathbf{N}$ sont strictes donc $n(P) \geq 3$; $\inf\{\mathbf{N} \setminus \mathbf{P}_2\} = 93$.

► Rappelons que l'on a :

$$P_2 = \{ n \in \mathbf{N} \mid \exists\ a,b,c \in P_1 \mid a+b ,\ a+b+c \in P_1 \wedge\ n = b+c \} ;$$

d'abord, on a l'inclusion $P_1 \subset P_2$ car si $n \in P_1$, alors $n \in P_2$ [[0,n,0]] ; remarquons que cet argument est général : dès lors que $0 \in A_n$, alors $A_n \subset A_{n+1}$. L'inclusion $P_1 \subset P_2$ est stricte ; par exemple, $8 \notin P_1$ mais $8 \in P_2$ [[4,1,7]] ; il y a dans P_2 des nombres impairs non premiers, par exemple :$15 \in P_2$ [[2,11,4]] ; en fait , on peut vérifier que tous les nombres jusqu'à 92 inclus sont dans P_2 (voir ci-dessous) .

Par contre $93 \notin P_2$; supposons le contraire, à savoir que l'on a : $93 \in P_2$ [[a,b,c]] ; si a+b+c était pair, a serait premier impair et a+b+c = 0 (6), alors a = 3 (6) et donc a = 3 : c'est impossible car $96 \notin J$, puisque 95 n'est pas premier ; resterait la possibilité pour a+b+c d'être impair ; alors a serait pair ; a = 2 est impossible, toujours parce que 95 n'est pas premier ; a > 4 entraînerait : a = 0 (6) et donc a+b+c = 3 (6), soit a+b+c = 3, puisque ce nombre doit être premier, ce qui ne va pas avec a+b+c > 97 ! Il reste à examiner le cas où a serait égal à 4 ; 97 est bien premier ; b ne peut pas être pair ; en effet, a+b serait pair et élément de J , strictement supérieur à 4, donc on aurait : a+b = 0(6), d'où b = 2 (6), d'où b = 2, mais 91 = 93-2 n'est pas premier ; reste que b pourrait a priori être impair et c serait alors pair ; c = 2 ne convient pas, car 91 n'est pas premier ; c > 4 ne convient pas non plus, car alors b+c = 3 (6), donc b = 3 (6), soit b = 3, mais $90 \notin J$, car 91 n'est pas premier ; enfin, si c = 4, on a : a+b = 93, qui n'est pas premier ! ◄

Voici pourquoi on a : $[0,92] \subset P_2$; tenant compte de ce que $n \in P_2$ [[a,b,c]] entraîne aussi que $m \in P_2$ [[b,a,c]], on regroupe, quand le cas se présente, les deux nombres « produits » par un triplet [[a,b,c]] ; il suffit d'indiquer ces triplets pour les nombres suivants, qui ne sont ni premiers, ni jumeleurs, jusqu'à 92 inclus ; d'abord les nombres pairs :

8, 10, 14, 16, 20, 22, 24, 26, 28, 32, 34, 36, 38, 40, 44, 46, 48, 50, 52, 54, 56, 58, 62, 64, 66, 68, 70, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92 ;
pour simplifier encore la présentation, nous indiquons le triplet « a,b,c » puis le ou les deux nombres qu'il « engendre » dans P_2 :

1, 3, 7	↦	8, 10	1, 5, 31	↦	32, 36	5, 7, 59	↦	64
1, 3, 13	↦	14, 16	1, 5, 47	↦	48, 52	5, 7, 71	↦	76
1, 3, 19	↦	20, 22	1, 5, 53	↦	54, 58	5, 13, 43	↦	56
1, 3, 37	↦	38, 40	1, 5, 61	↦	62, 66	5, 13, 79	↦	92
1, 3, 43	↦	44, 46	1, 5, 73	↦	74, 78	7, 11, 43	↦	50
1, 3, 67	↦	68, 70	1, 5, 83	↦	84, 88	7, 11, 79	↦	86
1, 3, 79	↦	80, 82	5, 7, 19	↦	26	7, 11, 83	↦	90
1, 5, 23	↦	24, 28	5, 7, 29	↦	34			

Ensuite, les nombres impairs :

9, 15, 21, 25, 27, 33, 35, 39, 45, 49, 51, 55, 57, 63, 65, 69, 75, 77, 81, 85, 87, 91 ;

2, 2, 7	↦	9	2, 2, 67	↦	69	2, 4, 53	↦	55, 57
2, 2, 13	↦	15	2, 2, 79	↦	81	2, 4, 61	↦	63, 65
2, 2, 19	↦	21	2, 4, 23	↦	25, 27	2, 4, 73	↦	75, 77
2, 2, 37	↦	39	2, 4, 31	↦	33, 35	2, 4, 83	↦	85, 87
2, 2, 43	↦	45	2, 4, 47	↦	49, 51	6, 12, 79	↦	91

Posons $\mathbf{P}_{[2k]} = \{ p_n \in \mathbf{P} \mid p_{n+1} = p_n + 2k \}$ et $\mathbf{J}_{2k} = \bigcup_{p_n \in \mathbf{P}_{[2k]}}]p_n, p_{n+1}[$.

$\mathbf{J}_2$ = J = {2,4,6,12,18,30,42,60,72,…}
$\mathbf{J}_4$ = {8,9,10,14,15,16,20,21,22,38,39,40,68,69,70,80,81,82,…}
$\mathbf{J}_6$ = {24,25,26,27,28,32,33,34,35,36,48,49,50,51,52,54,55,56,57,58,62,63,64,65,66,…}
$\mathbf{J}_8$ = {90,91,92,93,94,95,96,360,361,362,363,364,365,366,390,391,392,393,394,395,396,…}
…
On voit que $\mathbf{N} = (\mathbf{P} \setminus \{2\}) \cup \mathbf{J}_2 \cup \mathbf{J}_4 \cup \ldots \cup \mathbf{J}_{2k} \cup \ldots$ et que cette réunion est disjointe; l'ensemble des k tels que $\mathbf{J}_{2k} \neq \emptyset$ est infini ; on ne sait pas s'il existe des entiers k tels que $\mathbf{J}_{2k}$ soit fini ou éventuellement vide ! On ne connaît pas d'entier k pour lequel on puisse affirmer que $\mathbf{J}_{2k}$ est infini. Ces questions généralisent en quelque sorte la conjecture dite des entiers premiers jumeaux, qui prétend que $\mathbf{J} = \mathbf{J}_2$ serait infini !

Proposition 0-6-4.
$\mathbf{J}_4 \subset \mathbf{P}_2$ et $\mathbf{J}_6 \subset \mathbf{P}_2$; pour tout $p \in \mathbf{P}_{[12]}$ les entiers p+1, p+5, p+6, p+7, p+11 sont éléments de $\mathbf{P}_2 \setminus \mathbf{P}_1$.

► Montrons que l'on a $J_4 \subset P_2$: soit p_n un nombre premier tel que $p_{n+1} - p_n = 4$; alors, on trouve : $p_n+1, p_n+3 \in P_2$ [[1,3,p_n]] et encore $p_n+2 \in P_2$ [[2,2,p_n]].
Montrons ensuite que l'on a $J_6 \subset P_2$: soit p_n un nombre premier tel que $p_{n+1} - p_n = 6$; alors, on dispose des éléments: $p_n+1, p_n+5 \in P_2$ [[1,5,p_n]] ; et $p_n+2, p_n+4 \in P_2$ [[2,4,p_n]] et $p_n+3 \in P_2$ [[3,3,p_n]]
Examinons le cas de J_{12} ; comme on peut écrire 12 = 1+11, 12 = 5+7 , 12 = 6+6, on voit que, pour tout entier premier p_n tel que $p_{n+1} - p_n = 12$, les entiers suivants sont dans P_2 (et aucun n'est dans P_1) : $p_n+1, p_n+5, p_n+6, p_n+7, p_n+11$. ◄

Comme on ne sait pas si J_4 , J_6 ou J_{12} est infini, on ne sait toujours pas si $P_2 \setminus P_1$ est infini ! Indiquons cependant cette petite proposition qui n'est pas très rassurante quant à la question de l'infinitude de $P_2 \setminus P_1$.

Proposition 0-6-5.
S'il existe une infinité d'entiers jumeleurs 2k tels que $\mathbf{J}_{2k}$ ne soit pas vide, ou s'il existe un entier jumeleur 2m > 2 tel que $\mathbf{J}_{2m}$ soit infini, alors $\mathbf{P}_2 \setminus \mathbf{P}_1$ est infini. Comme on ne sait pas si J_4 , J_6 ou J_{12} est infini, on ne sait toujours pas si $\mathbf{P}_2 \setminus \mathbf{P}_1$ est infini…

► En effet, soit p_n un entier premier tel que $p_{n+1} - p_n = 2k$ soit un jumeleur > 2 ; alors on dispose des éléments suivants de $P_2 \setminus P_1$: p_n+1 , $p_n+(2k-1) \in P_2$ [[1,2k-1,p_n]] ; on peut même indiquer que pour toute décomposition de 2k en somme de deux entiers q et q', tous deux premiers ou tous deux jumeleurs, alors p_n+q , $p_n+q' \in P_2 \setminus P_1$; quoiqu'il en soit, la première des hypothèses et le fait que les J_{2k} sont disjoints, ou la deuxième hypothèse entraînent bien que l'ensemble $P_2 \setminus P_1$ est infini ◄

Nous allons établir quelques propositions générales montrant que des nombres de forme particulière ne sont pas dans P_2 , ou au contraire sont dans P_2 ; on en conclura facilement que $\mathbf{N} \setminus P_2$ est infini, mais on ne pourra toujours pas se prononcer sur $P_2 \setminus P_1$. La question de savoir si $P_1 \setminus P$ est infini équivaut à la conjecture des jumeaux. Les arguments utilisés maintenant sont du même genre que ceux mis en œuvre pour établir que $93 \notin P_2$.

Proposition 0-6-6.
Pour que $6\ell+3 \notin P_2$ il faut et il suffit que l'un de ses *voisinages immédiats* au moins soit constitué de nombres non premiers. Les voisinages immédiats sont :

gauche $(6\ell-1, 6\ell+1)$ *milieu* $(6\ell+1, 6\ell+5)$ *droit* $(6\ell+5, 6\ell+7)$

Le résultat résultera en gros des 3 critères suivants : g (gauche), d(droit), m (milieu).

Critère (g)
Soit ℓ un entier > 0 ; si les entiers $6\ell-1$ et $6\ell+1$ ne sont pas premiers, alors $6\ell+3 \notin P_2$.

► D'abord $6\ell+3 \notin P$, car $\ell > 0$, et $6\ell+3 \notin J$ car impair, donc $6\ell+3 \notin P_1$. Supposons donc $6\ell+3 \in P_2$; il est au moins somme de deux nombres non nuls (car $6\ell+3 \notin P_1$) de P_1 ; l'un , a, est pair et appartient à J, et l'autre , p , est impair et premier ; $6\ell+3 = a+p$; $a = 2$ est exclu car $6\ell+1 \notin P$, $a = 4$ est exclu car $6\ell-1 \notin P$; resterait le cas où $a > 4$; mais alors, le calcul modulo 6 donne ceci : $a = 0\ (6)$, donc $p = 3\ (6)$, donc $p = 3$ et du coup $a = 6\ell \in J$, mais ceci n'est pas possible puisque $6\ell-1$ et $6\ell+1$ ne sont pas premiers ◄

Exemples. $123 \notin P_2$ car $119 = 7.17$ et $121 = 11.11$; c'est la première fois que le critère (g) s'applique ; le critère ne s'applique pas à 93, car 89 est premier ; voici les nombres (jusqu'à 1000) auxquels le critère (g) s'applique :

123, 147, 207, 219, 249, 291, 303, 327, 345, 417, 429, 477, 519, 531, 537, 555, 585, 627, 639, 669, 699, 717, 795, 807, 819, 837, 849, 873, 897, 903, 927, 963, (1005 …)

Critère (d)
Soit ℓ un entier > 0 ; si les entiers $6\ell+5$, $6\ell+7$ ne sont pas premiers, alors $6\ell+3 \notin P_2$.

► Raisonnons par l'absurde et supposons que $6\ell+3 \in P_2$; dans ce cas, il existe a, élément de J et p, premier impair, tels que $6\ell+3 = a+p$, et il existe $x \in P_1$ tel que $x+y$ et $x+a+p \in P_1$, où y = a ou p .
Supposons d'abord que $x+a+p$ soit pair, et donc élément de J congru à 0 modulo 6 (car il est plus grand que 6 !) ; alors $x = 3\ (6)$ et comme $x \in P_1$, $x = 3$, mais alors $x+a+p = 6\ell+6 \in J$, ce qui exige que $6\ell+5$ et $6\ell+7$ soient premiers, ce qui n'est pas.
Supposons alors que $x+a+p$ soit impair, et donc premier puisqu'il doit être élément de P_1 ; alors x serait pair, mais $x = 2$ est exclu car $6\ell+5$ n'est pas premier, $x = 4$ est exclu car $6\ell+7$ n'est pas premier, et $x > 4$ est impossible, car autrement on aurait : $x+a+p = 3\ (6)$ et donc $x+a+p = 3$ qui est un nombre premier. Contradiction ◄

Remarques.
1) Avec la seule hypothèse $6\ell+7$ non premier, mais $6\ell+5$ premier, le raisonnement précédent reste bon, sauf dans un cas : $x+a+p$ premier et $x = 2$ (alors $x+a+p = 2+6\ell+3 = 6\ell+5$ est premier).
Dans ce cas, si y = a, comme a est pair, $2+a \in J$ et donc a = 2 ou 4:
si a = 2, alors $6\ell+3 \in P_2$ [[2,2, $6\ell+1$]] , pour peu qu'on ait $6\ell+1 \in P$;
si a = 4, alors $6\ell+3 \in P_2$ [[2,4, $6\ell-1$]] , pour peu qu'on ait $6\ell-1 \in P$;

Et si y = p, il convient que p+2 et 2+a+p = 6ℓ+5 soient premiers ; p et p+2 doivent être des entiers premiers jumeaux ; on peut préciser que p = 5 (6) ; alors a+p = 3 (6) d'où a = 4 (6), soit a = 4, et p = 6ℓ-1 ; dans ce cas, on a : 6ℓ+3 ∈ P_2 [[2, 6ℓ-1, 4]].

2) Avec la seule hypothèse 6ℓ+5 non premier, mais 6ℓ+7 premier, le raisonnement précédent reste bon, sauf dans le cas x+a+p premier et x = 4 (alors x+a+p = 4+6ℓ+3 = 6ℓ+7 est premier).
Dans ce cas, si y = a, comme a est pair 4+a ∈ J, d'où a = 2 (6) d'où a = 2 ; ce cas est possible a priori à condition que p = 6ℓ+3-2 = 6ℓ+1 soit premier ; on peut conclure, dans ce cas : 6ℓ+3 ∈ P_2 [[4, 2, 6ℓ+1]] .
Et si y = p , il convient que 4+p et 4+a+p = 6ℓ+7 soient premiers :
si a = 2 , alors 6ℓ+3 ∈ P_2 [[4,2, p]] , pour peu qu'on ait 6ℓ+1 ∈ P ;
si a > 4, alors p = 3 et donc a = 6ℓ ; 6ℓ+3 ∈ P_2 [[4 ,3, 6ℓ]] , pour peu que 6ℓ-1 et 6ℓ+1 ∈ P ;
le cas a = 4 est exclu, car sinon p = 6ℓ-1 et 4+p = 3 (6), soit encore 4+p = 3 !

Exemples. La première fois que le critère (d) s'applique, mais ni (g) ni (m) (voir plus loin) c'est avec le nombre 213 ; en effet : 209 = 11.19 ∉ P , 211 ∈ P, 215 = 5.43 et 217 = 7.31 ∉ P; le critère (g) s'applique à 219 ; la 2ème fois que (d) s'applique, c'est pour 339 : 339 ∉ P_2 car 335 ∉ P , 337 ∈ P, 341 = 11.31 et 343 = 7.7.7 ∉ P; la 3ème fois que le critère (d) s'applique, c'est pour le nombre 549, etc…
Une question se pose ici : est-ce que (d) s'applique une infinité de fois sachant que la séquence (6ℓ-1, 6ℓ+1, 6ℓ+5, 6ℓ+7) est du type (∉ P, ∈ P, ∉ P, ∉ P) ? On peut supposer que la réponse est positive, et pas trop difficile à établir. Une autre question, certainement plus difficile, est de savoir si les séquences (6ℓ-1, 6ℓ+1 ; 6ℓ+5, 6ℓ+7) du type (∈P, ∈P ; ∉P, ∈P) ou (∉P, ∈P ; ∉P, ∈P) sont en nombre fini ou non. Cette question est en rapport avec la finitude ou non des ensembles J_2 , J_4 et J_6, mais le rapport n'est pas très clair.

On voit apparaître une « règle » selon la nature de la séquence (6ℓ-1, 6ℓ+1 ; 6ℓ+5, 6ℓ+7) ; on peut résumer les deux critères précédents par le petit tableau suivant, dans lequel **p** (resp. **n**) est un abrégé de « premier » (resp. « non premier ») et ∗ signifie « primarité indifférente », donc « premier ou non premier » :

critère	6ℓ-1	6ℓ+1	6ℓ+5	6ℓ+7	conséquence
g	**n**	**n**	∗	∗	⇒ 6ℓ+3 ∉ P_2
d	∗	∗	**n**	**n**	⇒ 6ℓ+3 ∉ P_2

Cela donne la réponse dans 7 cas sur 16 a priori : en effet chaque ligne correspond à 4 cas, mais la distribution (**n**, **n** ; **n**, **n**) est commune. Les remarques suivant le ***Critère*** (d) répondent à 5 nouveaux cas, à savoir : (∗, **p** ; **p** , **n**) , (**p**, ∗ ; **p** , **n**), ce qui en fait 3 et aussi (∗, **p** ; **n**, **p**), ce qui en fait encore 2. Venons-en alors au critère (m)

Critère (m)
Soit ℓ un entier > 0 ; si les entiers 6ℓ+1 et 6ℓ+5 ne sont pas premiers, alors 6ℓ+3 ∉ P_2.

► On peut le prendre comme complément du critère (g) : en effet, si 6ℓ-1 aussi est non premier, le résultat découle de (g) et l'hypothèse selon laquelle 6ℓ+5 n'est pas premier est inutile ; par contre cette dernière hypothèse s'avère utile dans le cas où 6ℓ-1 est premier, ce

que nous supposons donc. Reprenons les notations introduites dans la démonstration du critère (g). Soit donc $6\ell+3 = a+p$, avec $a \in J$ et p premier impair ; il n'est pas possible d'avoir $a = 2$ car $6\ell+1$ n'est pas premier ; si on avait $a > 4$, on aurait $a = 0\ (6)$ et $p = 3\ (6)$, d'où $p = 3$ et dans ce cas : $a = 6\ell$, mais $6\ell+1$ n'étant pas premier, a ne saurait être élément de J ; reste alors le cas $a = 4$, avec $6\ell-1 = p$. Intervient alors l'autre condition pour que $6\ell+3$ puisse être dans P_2 :

$$\exists\ x \in \mathbf{N}\ [\ x,\ x+y,\ x+6\ell+3 \in P_1\ ]\ ,\ \text{formule dans laquelle } y \text{ est } 6\ell-1 \text{ ou } 4\ ;$$

Cas $y = 6\ell-1$, x impair. L'entier x+y est pair et ≥ 6, donc $x+y = 0\ (6)$ d'où $x = 1\ (6)$, puis $x+6\ell+3 = 4\ (6)$, ce qui est incompatible avec le fait que $x+6\ell+3 \in J$, avec $\ell > 0$.
Cas $y = 6\ell-1$, x pair. L'égalité $x = 2$ est exclue car $6\ell+1$ n'est pas premier ; l'égalité $x = 4$ est exclue car $6\ell+3$ n'est pas premier ($\ell > 0$) ; resterait $x > 4$, donc $x = 0\ (6)$, qui entraîne la congruence $x+6\ell+3 = 3\ (6)$ incompatible avec $x+6\ell+3 \in P$ et $\ell > 0$.
Cas $y = 4$, x pair. Alors x+y est pair et > 4, donc $x+y = 0\ (6)$, d'où $x = 2\ (6)$, soit $x = 2$ puisque $x \in J$, et il est nécessaire que $6\ell+5$ soit premier pour que $6\ell+3$ soit dans P_2.
Cas $y = 4$, x impair. Dans ce cas, $x+6\ell+3$ est pair et > 6 donc $x+6\ell+3 = 0\ (6)$ et $x = 3$; alors $x+y = 7$ est bien premier, mais il faut que $6\ell+6$ soit élément de J ; donc ce cas n'est possible que si $6\ell+5$ et $6\ell+7$ sont tous deux premiers, ce qui n'est pas ◄

Le schéma correspondant à ce critère est le suivant :

critère	$6\ell-1$	$6\ell+1$	$6\ell+5$	$6\ell+7$	conséquence
m	*	**n**	**n**	*	$\Rightarrow\ 6\ell+3 \notin P_2$

Il correspond à 4 distributions de primarité de la séquence ($6\ell-1$, $6\ell+1$; $6\ell+5$, $6\ell+7$) , mais seule la distribution (**p**, **n** ; **n** , **p**) ressort de (m) et non de (g) ou (d) ; notons à ce sujet que lorsque (g) s'applique à $6\ell+3$, (d) s'applique à $6(\ell-1)+3 = 6\ell-3$ aussi, et lorsque (d) s'applique à $6\ell+3$, (g) s'applique à $6(\ell+1)+3 = 6\ell+9$ aussi.

On dispose maintenant de 13 « cas de figure » sur 16 .

► Reste à examiner les trois cas suivants : (**p**, **p** ; **p**, **p**) , (**n** , **p** ; **p**, **p**) et (**p**, **n** ; **p**, **p**) concernant la primarité de la séquence ($6\ell-1$, $6\ell+1$, $6\ell+5$, $6\ell+7$) . La réponse aux deux premiers consiste à reprendre ce qui a déjà été remarqué : $6\ell+3 \in P_2$ [[2,2, $6\ell+1$]], et la réponse au troisième consiste à noter encore : $6\ell+3 \in P_2$ [[2,4, $6\ell-1$]]. On aura remarqué que l'appartenance de $6\ell+3$ à P_2 correspond à l'une des distributions suivantes :

(*, **p** ; **p**, *), (**p**, * ; **p**, *), (*, **p** ; *, **p**)

qui sont au nombre de 8 ◄

En résumé, on a pu répondre dans tous les cas de figure à la question de savoir si $6\ell+3 \in P_2$ ou non, en analysant la primarité de la séquence ($6\ell-1$, $6\ell+1$; $6\ell+5$, $6\ell+7$) .
Peut-on en déduire un critère d'appartenance ou non appartenance à P_2 de tous les entiers impairs ? La réponse n'est pas simple, car il reste à étudier tous les nombres non premiers de la forme $6\ell+1$ ou $6\ell+5$. En tout état de cause, on dispose d'un test précis pour la suite des entiers $6\ell+3$, qu'on redonne sous forme du tableau récapitulatif suivant :

(**n**, **n** ; ∗, ∗) (**p**, **n** ; **n**, ∗) ⇔ ∉ (∗, **p** ; **n**, **n**)	(∗ , **p** ; **p**, ∗) (**p**, **n** ; **p**, ∗) ⇔ ∈ (∗, **p** ; **n**, **p**)

Ce tableau symbolise en un seul critère les trois critères (g), (d) et (m) .
En appelant *voisinages immédiats* de $6\ell+3$ dans la suite des nombres impairs les trois couples suivants:

$(6\ell-1, 6\ell+1)$, voisinage *gauche* de $6\ell+3$,
$(6\ell+1, 6\ell+5)$, voisinage du *milieu* de $6\ell+3$,
$(6\ell+5, 6\ell+7)$, voisinage *droite* de $6\ell+3$,

on obtient exactement l'énoncé de la proposition **0-6-6**.

Chaque combinaison de primarité de la séquence $(6\ell-1, 6\ell+1 ; 6\ell+5, 6\ell+7)$ se présente-t-elle effectivement ?
Voici le ***décompte jusqu'à*** 1000 : chaque séquence possible de primarité est suivie des nombres de la forme $6\ell+3$ tels que la séquence $(6\ell-1, 6\ell+1 ; 6\ell+5, 6\ell+7)$ présente cette disposition de primarité ; à la fin de la ligne, en gras, le nombre de tels nombres ; les 8 premières lignes correspondent à « $\in P_2$ » et les 8 suivantes à « $\notin P_2$ » .

Les huit dispositions correspondant à « $\in P_2$ »

(**p**, **p** ; **p**, **p**) 9, 15, 105, 195, 825,…**5**
(**p**, **p** ; **p**, **n**) 21, 45, 111, 231, 315, 351, 465, 645, 861, 885,…**10**
(**p**, **p** ; **n**, **p**) 33, 63, 75, 153, 273, 435, 573, 603,…**8**
(**p**, **n** ; **p**, **p**) 27, 57, 135, 177, 237, 267, 567, 597, 657,…**9**
(**p**, **n** ; **p**, **n**) 51,87,171,255,261,357,387,447,507, 561, 591,651, 681, 945, 951, 975, 981,...**17**
(**n**, **p** ; **p**, **p**) 39, 69, 99, 225, 279, 309, 459, 615, 855, 879,…**10**
(**n**, **p** ; **p**, **n**) 81, 129, 165, 381, 399, 441, 489, 501, 675, 741, 759, 771, 909, 939, 969,...**15**
(**n**, **p** ; **n**, **p**) 159, 333, 369, 375, 543, 609, 729, 735, 753, 993,…**10**

Les huit dispositions correspondant à « $\notin P_2$ »

(**n**, **p** ; **n**, **n**) 213, 339, 411, 549, 579, 633, 693, 711, 789, 921, 999,…**11**
(**n**, **n** ; **p**, **p**) 147, 189, 345, 417, 429, 519, 639, 807, 819,…**9**
(**n**, **n** ; **p**, **n**) 249, 291, 477, 555, 585, 699, 717, 795, 837, 927,…**10**
(**n**, **n** ; **n**, **p**) 123, 207, 219, 303, 327, 537, 627, 669, 783, 849, 873, 903, 963,…**13** (1005)
(**n**, **n** ; **n**, **n**) 531, 897,...**2**
(**p**, **p** ; **n**, **n**) 141, 183, 201, 243, 285, 423, 525, 621, 663, 813, 831,…**11**
(**p**, **n** ; **n**, **p**) 93, 363, 393, 405, 453, 483, 495, 687, 705, 723, 747, 765, 915, 933, 987,…**15**
(**p**, **n** ; **n**, **n**) 117, 297, 321, 471, 513, 777, 801, 843, 867, 891, 957,…**11**

Au total, il y a donc 166 (~ 1000/6) nombres, plus petits que 1000, concernés par la proposition **0-6-6** : 84 d'entre eux sont dans P_2 et 82 n'y sont pas ; voici une petite étude statistique de la répartition entre les « ∈ » et les « ∉ », par tranches de 100 ; les « ∈ » l'emportent nettement au début, on atteint quasiment l'égalité aux environs de 1000, et après les « ∉ » l'emportent :

< 100 : 15 ∈ / 1 ∉
< 200 : 25 ∈ / 7 ∉
< 300 : 33 ∈ / 16 ∉
< 400 : 43 ∈ / 23 ∉
< 500 : 49 ∈ / 33 ∉
< 600 : 57 ∈ / 42 ∉
< 700 : 65 ∈ / 51 ∉
< 800 : 71 ∈ / 61 ∉
< 900 : 76 ∈ / 73 ∉
<1000 : 84 ∈ / 82 ∉

On ne sait toujours pas si $P_2 \backslash P_1$ est infini !

La plus longue suite de nombres « consécutifs » de la forme $6\ell+3$ qui ne sont pas dans P_2, et qui apparaît avant 10000 a 12 éléments ; c'est la suivante :

7941, 7947, 7953, 7959, 7965, 7971, 7977, 7983, 7989, 7995, 8001, 8007,

elle fait intervenir 7 des 8 séquences de primarité liées à la non appartenance à P_2 ; seule la disposition (**p**, **n** ; **n**, **p**) n'y figure pas. Notons que cette disposition correspond à J_8 : précisément, il y a bijection naturelle entre les séquences de type (**p**, **n** ; **n**, **p**) et les entiers premiers p_n tels que $p_{n+1} = p_n+8$. On ne sait pas si J_8 est fini ou non. On peut constater par contre que ce cas semble de plus en plus rare quand n augmente…alors qu'il est deuxième ex aequo sur 16, jusqu'à 1000 (voir ci-dessus et ci-dessous)!

Il est intéressant de classer ces séquences en fonction de l'apparition de 0, 1, 2, 3, ou 4 fois le symbole **p** dedans. Voici le résultat brut :

Ensemble des séquences	de type ** **	$6\ell+3 \notin$ ou $\in P_2$	$< 10^4$	$< 10^5$	$< 10^6$	$< 3.10^6$	$< 10^7$
Z	**nn nn**	∉	223	3860	53271	178649	656431
U_1	**pn nn**	∉	155	1835	18684	55255	180907
U_2	**np nn**	∉	161	1864	18868	55496	181022
U_3	**nn pn**	∉	161	1865	18800	55441	180931
U_4	**nn np**	∉	163	1824	18790	55420	181021
D_{12}	**pp nn**	∉	105	740	5515	14717	42709
D_{14}	**pn np**	∉	101	773	5569	14687	42352
D_{34}	**nn pp**	∉	96	750	5477	14606	42685
D_{13}	**pn pn**	∈	106	751	5598	14661	42529
D_{23}	**np pn**	∈	102	746	5472	14565	42300
D_{24}	**np np**	∈	99	741	5445	14360	42115
T_1	**np pp**	∈	45	210	1278	2987	7778
T_2	**pn pp**	∈	50	224	1246	2940	7616
T_3	**pp np**	∈	44	224	1266	2941	7727
T_4	**pp pn**	∈	43	221	1227	2876	7644
Q	**pp pp**	∈	12	38	166	397	899

La notation des ensembles de séquences est claire : la première lettre de zéro, un, deux, trois, quatre selon le *nombre* de l'occurrence « **p** » dans le *type* de la séquence, et éventuellement, l'indice précise les places de **p** (pour U et D) ou de **n** (pour T). On désigne par D_i la réunion portant sur $j \neq i$ des $D_{i\,j}$ ou $D_{j\,i}$ (il y a 3 tels ensembles).
Le théorème de Dirichlet, appliqué aux classes modulo 6, montre entre autres choses qu'il y a une infinité de nombres premiers de la forme 6k + 1 et une infinité de nombres premiers de la forme 6k – 1 ; ceci permet de dire que les quatre ensembles suivants :

$$E_{-1} = U_1 \cup D_1 \cup (T \setminus T_1) \cup Q$$
$$E_{1} = U_2 \cup D_2 \cup (T \setminus T_2) \cup Q$$
$$E_{5} = U_3 \cup D_3 \cup (T \setminus T_3) \cup Q$$
$$E_{7} = U_4 \cup D_4 \cup (T \setminus T_4) \cup Q$$

sont infinis. Ce n'est pas très fameux!
Le raisonnement « plus simpliste » qui se base sur l'existence de tranches sans nombres premiers aussi larges et aussi loin que l'on veut permet de dire que les deux ensembles suivants :

$$F_g = U_1 \cup U_2 \cup D_{12}$$
$$F_d = U_3 \cup U_4 \cup D_{34}$$

sont aussi infinis.

Donnons encore la statistique globale jusqu'à 10000000 :

<10000 :	501 ∈	/	1165 ∉
<100000 :	3155 ∈	/	13511 ∉
<1000000 :	21692 ∈	/	144974 ∉
<10000000 :	158608 ∈	/	1508058 ∉

Proposition 0-6-7.
$\mathbf{N} \setminus \mathbf{P}_2$ est infini.

► Au stade où nous en sommes, il y a bien des manières d'établir ce résultat, toutes basées sur le fait qu'il existe des tranches d'entiers consécutifs non premiers aussi grandes que l'on veut, et donc en quantité infinie (cf. les ensembles Z, F_g ou F_d)◄

Proposition 0-6-8.
Soient p_n et p_{n+1} deux nombres premiers consécutifs et $2k = p_{n+1} - p_n$
Supposons $2k \geq 10$ et $2k = 1$ (resp.2) mod. 3 et soit 2h un entier pair tel que $4 < 2h < 2k$ et $2h = 2$ (resp.1) mod. 3 ; alors on a : $p_n+2h \notin \mathbf{P}_2$

► D'abord, $p_n+2h \notin P$ car on a : $p_n < p_n+2h < p_{n+1}$, et $p_n+2h \notin J$, car c'est un nombre impair ; donc $p_n+2h \notin P_1$.
Supposons alors que $p_n+2h \in P_2$; on peut écrire $p_n+2h = a+p$ avec $a \in J$ et p premier impair ; $a = 2$ (resp $a = 4$) n'est pas possible car p_n+2h-2 (resp. p_n+2h-4) n'est pas premier : $p_n < p_n+2h-4 < p_n+2h-2 < p_n+2h < p_n+2k = p_{n+1}$; donc $a = 0$ (6) ; alors on a : $p_n+2h = p$ (3) ; d'autre part, $p_{n+1} = p_n+2k = p-2h+2k$ (3).
Supposons $2k = 1$ (3) et $2h = 2$ (3) ; alors, $p_n = 2$ (3) est impossible car on aurait $p_{n+1} = 0$ (3) et donc $p_{n+1} = 3$, ce qui est absurde ; donc $p_n = 1$ (3), mais alors $p = p_n+2h = 1+2 = 0$ (3), $p = 3$. Supposons $2k = 2$ (3) et $2h = 1$ (3); alors, $p_n = 1$ (3) est impossible car on aurait $p_{n+1} = 0$ (3)

et donc $p_{n+1} = 3$, ce qui est absurde; donc $p_n = 2$ (3), mais alors $p = p_n+2h = 2+1 = 0$ (3), et donc encore $p = 3$.
Dans les deux cas, on trouve donc : $a = p_n+2h - p = p_n+2h - 3$, ce qui n'est pas possible car $p_n+2h - 2 \notin P$ (et $p_n+2h - 4$ non plus !) ◄

Exemple: pour tout n, si $p_{n+1} = p_n + 10$ alors $p_n + 8 \notin \mathbf{P}_2$. Mais on ne sait pas si J_{10} est infini, et donc si ce critère s'applique une infinité de fois ou non.

Remarques.

1) La première fois que cette proposition (avec 10) s'applique, c'est pour $p_n = 139$ car on a : $p_{n+1} = 149$; on peut conclure que $147 \notin P_2$. Ce critère doit être vu comme un cas particulier du critère (g). Voici pourquoi : l'égalité $p_n = 1$ (3) entraîne que $p_n+8 = 3$ (6) ; en effet, p_n est impair, et donc $p_n = 1$ (6) et $p_n+8 = 3$ (6) est de la forme $6\ell+3$; dans ce cas, $6\ell-1 = p_n+4$ et $6\ell+1 = p_n+6$ n'étant pas premiers,…le critère (g) s'applique.
2) Les proposition **0-6-8** et **0-6-6** sont presque ***équivalentes.***

Proposition 0-6-9.
Soit r un entier > 0 ; soit (s,t) l'un des trois couples d'entiers suivants :

(6r-1, 6r+1), (6r+1, 6r+5), (6r+5, 6r+7);

soit encore α (resp. β) un diviseur > 1 de s (resp. de t) ; alors la *progression arithmétique* $\{6\alpha\beta.\ell+6r+3, \ \ell > 0\}$ est entièrement contenue dans $\mathbf{N} \setminus \mathbf{P}_2$; de plus, si α et β sont des diviseurs propres de s et t respectivement, la *progression arithmétique* $\{6\alpha\beta.\ell+6r+3, \ \ell \geq 0\}$ est entièrement contenue dans $\mathbf{N} \setminus \mathbf{P}_2$.

► On examine des raisons suffisantes pour que $6(k+r)+3 \notin P_2$; on sait déjà, d'après ce qui précède, qu'une condition nécessaire et suffisante pour qu'il en soit ainsi est que l'un des trois couples suivants au moins soit formé de nombres décomposables :

(6(k+r)-1, 6(k+r)+1) , (6(k+r)+1, 6(k+r)+5) , (6(k+r)+5, 6(k+r)+7) ;

ces couples sont tout trois de la forme (6k+s, 6k+t), encore notée 6k + (s, t), les trois valeurs de (s, t) étant respectivement (6r-1, 6r+1), (6r+1, 6r+5), (6r+5, 6r+7); soit α un diviseur (autre que 1) de s et β un diviseur (autre que 1) de t ; une condition suffisante pour que 6k+s et 6k+t soient deux nombres décomposables est que k soit un multiple du produit $\alpha\beta$; en effet, si l'on a $k = \alpha\beta.\ell$, comme $s = \alpha.\alpha'$ et $t = \beta.\beta'$, on dispose des égalités suivantes: $6k+s = \alpha(6\beta.\ell+\alpha')$ et $6k+t = \beta(6\alpha.\ell+\beta')$ qui fournissent pour tout $\ell > 0$ des décompositions non triviales des deux nombres 6k+s et 6k+t, et ceci entraîne donc que $6(k+r)+3 \notin P_2$; la proposition en découle aussitôt ◄

Exemples.
En choisissant pour (α,β) l'un des couples (s,t) lui-même, on obtient ceci :
pour tout r > 0 , les progressions arithmétiques suivantes sont dans $\mathbf{N} \setminus \mathbf{P}_2$:

$\{ 6(36r^2-1).\ell + 6r+3 ; \quad 6(36r^2+36r+5).\ell + 6r+3 ; \quad 6(36r^2+72r+35).\ell + 6r+3 ; \quad \ell > 0\}$

Avec r = 1, on trouve : $\forall\ \ell > 0,\ 210.\ell + 9 ,\ 462.\ell + 9 ,\ 858.\ell + 9 \notin \mathbf{P}_2$.
Avec r = 0, on trouve : $\forall\ \ell > 0,\ 210.\ell + 3 \notin \mathbf{P}_2$.

Venons-en à $\mathbf{P_3}$, avec une proposition originale qui relie l'engendrement de **N** à partir de **P** et la conjecture des entiers premiers jumeaux. Soit **P**(**J**) l'ensemble de tous les nombres premiers p tels qu'il existe un jumeleur j (élément de **J**) pour lequel p' = p + j soit encore premier. Même si **J** est fini, rien n'indique que **P**(**J**) le soit aussi.

Proposition 0-6-10.
Si l'ensemble **P**(**J**) est fini alors $\mathbf{N}\backslash P_3$ est infini.

► Soit s = sup(**P**(**J**)) et t = sup(**J**) ; soit $j \in J$; j-1 et j+1 sont premiers et 2 = (j+1) - (j-1) est un jumeleur, donc $j - 1 \in \mathbf{P}(\mathbf{J})$; en particulier, $t - 1 \in \mathbf{P}(\mathbf{J})$; on a donc : $t - 1 \leq s$ et l'égalité a lieu si et seulement si $s+1 \in \mathbf{J}$.

Soit $n \in \mathbf{P}_2$ avec $n > 2s + 1$; si n est dans $\mathbf{P}_1$, comme $n > t = \sup(\mathbf{J})$, alors n est premier ; s'il n'est pas dans $\mathbf{P}_1$ il est d'une des formes suivantes a priori :

* soit somme de deux entiers premiers impairs $n = p+q$ et $\exists x [x, p, q, q+x, p+q+x \in \mathbf{P}_1]$; comme q+x et p+q+x sont de parités différentes, l'un des deux est pair et donc élément de **J** ; ce ne peut pas être p+q+x, puisque $p+q+x = n+x > s+1+x > t$; c'est donc q+x qui est pair et de ce fait $q+x \in \mathbf{J}$; alors x est lui-même impair, et q et x sont donc deux nombres premiers dont la somme est un jumeleur; alors la différence (p+q+x) - p est un jumeleur et $p \in \mathbf{P}(\mathbf{J})$; ainsi $n = p+q \leq s+t \leq 2s +1$; ceci est impossible car $n > 2s +1$;

* soit somme d'un entier premier impair p et d'un $j \in \mathbf{J}$ et $\exists x [x, p, j, j+x, p+j+x \in \mathbf{P}_1]$ ou bien $\exists x [x, p, j, p+x, p+j+x \in \mathbf{P}_1]$; comme $p+j+x = n + x > 2s+1 > t$ est élément de $\mathbf{P}_1$, c'est un premier impair ;
si l'on est dans le premier cas, j+x qui est pair est élément de **J**, tout comme j et j+x ; comme $(p+j+x) - p \in \mathbf{J}$, on a : $p \in \mathbf{P}(\mathbf{J})$ et $n = p+j \leq s + t \leq 2s+1$; ceci est impossible car $n > 2s+1$;
si l'on est dans le deuxième cas, p+x est impair aussi, donc x est pair, élément de J, et p+x tout comme p+j+x sont des nombres premiers ; ainsi $p+x \in \mathbf{P}(\mathbf{J})$; alors on a : $p \leq p + x \leq s$ et donc $n = p + j \leq s + t \leq 2s +1$; ceci est impossible car $n > 2s +1$.

Ainsi, si $n \in \mathbf{P}_2$ avec $n > 2s +1$, alors n est premier. Tout comme $\mathbf{P}_1$, l'ensemble $\mathbf{P}_2$ est réunion de l'ensemble des nombres premiers et d'un ensemble fini $F \subset [0, 2s+1]$

Soit alors C un entier arbitraire, D un autre entier > 2s+1, et T = [A, B] une tranche « très large » de nombres non premiers et située « très loin » : par « très large » nous voulons dire que sa largeur B - A est supérieure C + 4s +1 et par « très loin » nous voulons dire : A > D.
Soit alors n un nombre tel que $A +2s +1 < n \leq A + C + 2s + 1$: n est non premier, car élément de T; il n'est donc pas dans $\mathbf{P}_2$; supposons qu'il soit dans $\mathbf{P}_3$; alors il est somme de deux nombres de $\mathbf{P}_2$: $n = p+q$ avec $q \leq p$; on a $2p \geq n > A+2s +1 > D +2s +1 \geq 4s +2$, soit $p > 2s+1$; c'est donc un nombre premier, et de ce fait on a : $p < A$;
maintenant, $q = n - p > A + 2s +1 – A = 2s + 1$, donc q est un nombre premier (élément de $\mathbf{P}_2$ plus grand que 2s+1) ;
il existe enfin un élément x de $\mathbf{P}_2$ tel que n+x, et p+x ou q+x, soient éléments de $\mathbf{P}_2$; ceci est impossible : en effet, $n+x > n > 2s+1$ entraîne que n+x est un nombre premier ; dès lors x est un nombre impair (puisque n est pair); on a alors : $x \geq B - n > (A+C+4s+1) - (A+C+2s+1) = 2s$, soit encore $x \geq 2s+1$; qu'on ait $x > 2s+1$ ou $x = 2s+1$, c'est un nombre premier ; comme p+x ou q+x doit aussi être dans $\mathbf{P}_2$, il y a une contradiction de parité.
Ainsi le segment] A+2s +1, A+C+2s +1] , de longueur C, ne contient aucun élément de $\mathbf{P}_3$ ◄

Proposition 0-6-11.
Si n(P) = 3 , il existe au moins un entier 2k tel que J_{2k} soit infini.

► En effet, d'après la proposition précédente, **P**(**J**) est infini.
Si **J** est infini, on peut choisir 2k =2.
Sinon, **J** est fini, mais il existe alors $x \in \mathbf{J}$ tel que l'ensemble $\mathbf{E} = \{p \in \mathbf{P} \mid \exists\ p' \in \mathbf{P} \mid p'-p = x\}$ soit infini. Pour tout $p \in \mathbf{E}$ on a donc : $s(p) - p \leq x$, en désignant par s(p) le successeur de p ; par le principe des tiroirs, il existe donc une infinité de p dans E, tels que $s(p) - p = 2k$ soit constant, c'est bien dire que $\mathbf{J}_{2k}$ est infini. On ne peut pas dire a priori si un tel entier 2k est élément de **J** ou non ! ◄

Il est bien clair que l'énoncé « n(**P**) = 3 » flirte avec la conjecture des jumeaux, mais aussi avec la conjecture de Goldbach (je ne développe pas ce point de vue ici, qui est cependant très sérieux).
Il me faut reconnaître ici que, dans ma thèse, j'affirmais pouvoir démontrer que « n(**P**) = 3 ». J'avais sous le coude une démonstration d'environ 5 pages, mais à la relecture, quelques 30 ans plus tard, j'ai vu qu'il y avait une erreur justement liée à la conjecture de Goldbach (qui reste, au jour où j'écris cette remarque, une conjecture…) Que dire de mes juges sinon qu'ils n'ont pas du creuser beaucoup la question à l'époque ?! Mais n'est-ce pas au fond assez courant et même banal !?

Voici, pour finir cette section, quelques exemples de prémonoïdes commutatifs qui se présenteront naturellement dans la suite, la loi + étant chaque fois la loi *induite* par celle de **N,** ou $\mathbf{N}^k$.

- Si n est un entier, $\mathbf{n} = [0, n-1]$ est un sous-prémonoïde de **N**.
- Tout facteur direct de **N** est un sous-prémonoïde de **N** (ce sera démontré plus loin).
- Si $n_1, n_2, \ldots, n_k$ sont des entiers, $\mathbf{C} = \mathbf{n_1} \times \mathbf{n_2} \times \ldots \times \mathbf{n_k}$ et $\mathbf{L} = \{(m_1, m_2, \ldots, m_k) \mid \exists\ i\ \ m_i < n_i\}$ sont des sous-prémonoïdes de $\mathbf{N}^k$.
- Toute réunion d'ensembles tels que **C** ou **L**, dans $\mathbf{N}^k$, détermine un sous-prémonoïde de $\mathbf{N}^k$.
- Le foncteur d'oubli U : **PréCat** $\rightarrow$ **Ens** (qui « oublie » la composition partielle) reflète les limites inductives filtrantes, sa restriction à la sous-catégorie pleine **PréMon** aussi !

Beaucoup de facteurs directs de $\mathbf{N}^k$, avec $k \geq 2$ ***ne sont pas*** des sous-prémonoïdes de $\mathbf{N}^k$, et c'est ce qui fait en partie la difficulté du problème central de cet article, pour lequel les théorèmes de trivialité des décompositions produits ne s'appliquent pas toujours ! Cependant, ces théorèmes sont très utiles pour « dégrossir » la situation, et c'est à eux qu'est consacrée la section suivante.

1. Décompositions directes des prémonoïdes commutatifs bien ordonnés. et noyaux d'instabilité.

Définition 1-1.
Un prémonoïde commutatif *(bien) ordonné* $(E,+,\leq)$ est constitué d'un prémonoïde commutatif $(E, +)$ (d'élément neutre noté 0) et d'un *(bon) ordre* $\leq$ sur E satisfaisant les conditions suivantes :

si $z = x + y$, alors $x \leq z$ (et donc aussi $y \leq z$) et si $x = z$, alors $y = 0$.

Une conséquence immédiate de cette définition est la suivante : si $0 = x+y$, alors $x = y = 0$!

On conviendra d'employer systématiquement le symbole $<$ pour indiquer une inégalité *stricte.*
Si $z = x + y$, on a l'équivalence entre « $y \neq 0$ » et « $x < z$ ».
On emploie génériquement les symboles $+ , < , \leq , 0$ quand il n'y a pas de confusion possible.

Soit $(E_i ,+)_{i \in I}$ une famille de prémonoïdes commutatifs. Le produit cartésien $E = \prod_{i\in I} E_i$ est naturellement muni de la loi de composition + suivante :

$$\exists ((x_i) + (y_i)) \Leftrightarrow \forall i \in I \ \exists (x_i + y_i) \text{ et alors } (x_i)+(y_i) = (x_i + y_i),$$

de sorte que $(E,+)$ est un prémonoïde commutatif, produit des prémonoïdes $(E_i, +)$.

Soit maintenant $(E_i ,+, \leq)_{i \in I}$ une famille de prémonoïdes commutatifs bien ordonnés.
Etant donné un bon ordre sur I , on munit naturellement E de l'ordre lexicographique associé, qui est donc le suivant : $(x_i) < (y_i)$ si et seulement si $x_j < y_j$, en désignant par j le premier élément de I (pour le bon ordre donné sur I) pour lequel on a $x_i \neq y_i$ (on a donc, pour tout i tel que $i < j$, $x_i = y_i$). C'est un bon ordre sur E et $(E ,+, \leq)$ est un prémonoïde commutatif bien ordonné.

Notons qu'en général il n'y a pas de bon ordre sur E qui puisse faire de $(E,+, \leq)$ un produit des $(E_i ,+, \leq)$ dans la catégorie des prémonoïdes commutatifs bien ordonnés…

Définition 1-2
Soit E un prémonoïde commutatif . On dit que $\partial = (A,B)$ est une *décomposition directe* de E lorsque tout élément x de E se décompose de manière unique en somme d'un élément a de A et d'un élément b de B. On suppose en outre que $0 \in A \cap B$. On note aussi a et b de manière fonctionnelle, comme ceci: $a = \underline{a}(x)$ et $b = \underline{b}(x)$.

Remarques.
1) La composition + étant partielle a priori, l'ensemble $A * B$ des couples $(a,b) \in A \times B$ qui sont composables pour l'addition + n'est pas nécessairement le produit $A \times B$. Si E est un monoïde, alors $A * B = A \times B$. Mais on peut bien avoir cette égalité sans que pour autant E soit un monoïde.

Exemples : soit $E_7 = [0,7] = \{0,1,2,3,4,5,6,7\}$ et $\mathbf{E}_7 = (E_7,+)$ le prémonoïde naturel avec l'addition pour loi (limitée par 8 : 2+6, 3+5, etc…ne sont pas définis). Si $A = \{0,1,2,3 \}$ et $B = \{0,4\}$, le couple (A,B) est une décomposition de $\mathbf{E}_7$ pour laquelle $A * B = A \times B$. Par contre,

si A' = {0,1,2} et B' = {0,3,6} le couple (A',B') est aussi une décomposition directe de $(E_7,+)$ et pourtant A'*B' = A'×B' \{2,6} n'a que 8 éléments (comme E_7) !

2) L'élément neutre 0 se décompose , et comme $0 \in A \cap B$, on a : $\underline{a}(0) = \underline{b}(0) = 0$. De plus , il est clair que $A \cap B = \{0\}$. Le fait que $0 \in A \cap B$ ne découle pas de l'unicité de décomposition : par exemple, si $\mathbf{E} = (\mathbf{Z}, +)$, $A = \mathbf{Z}$ et $B = \{-1\}$, tout élément x s'écrit de manière unique comme somme d'un élément de A et d'un élément de B : $x = \underline{s}(x) + (-1)$, où $\underline{s}(x)$ désigne le successeur de x pour l'ordre usuel dans $\mathbf{Z}$; ici $A \cap B = \{-1\}$.

3) Dans le même ordre d'idées, et en se tenant à la définition ci-dessus, il est possible que tout élément de **E** ait un symétrique : par exemple, toujours avec $\mathbf{E} = (\mathbf{Z}, +)$ qui est un groupe, le couple (A,B) suivant est une décomposition directe : $A = \{3k\}$ et $B = \{0,-1,-2\}$.

Soit $\partial = (A,B)$ une décomposition directe du prémonoïde commutatif **E**, et X une partie de E. Les noyaux d'instabilité de ∂ sont des parties de A et B qui « mesurent » en quelque sorte leur défaut de stabilité par rapport à la loi de composition de prémonoïde de E.

Définition 1-3.
On définit les *noyaux d'instabilité* associés à cette décomposition ∂ comme étant les sous-ensembles suivants de A et de B respectivement, auxquels on adjoindra {0} par convention :

$$N_\partial(A) = \{ a \in A \mid \exists a' \in A \mid a+a' \in B \}$$
$$N_\partial(B) = \{ b \in B \mid \exists b' \in B \mid b+b' \in A \};$$

on les désignera aussi simplement par N(A) et N(B), s'il n'y a pas de confusion possible.

Définition1-4.
On définit les *noyaux d'instabilité relatifs à* X associés à cette décomposition ∂ comme étant les sous-ensembles suivants de $A \cap X$ et de $B \cap X$ respectivement, auxquels on adjoindra {0} par convention :

$$N_{\partial, X}(A) = \{ a \in A \cap X \mid \exists a' \in A \cap X \mid a+a' \in B \}$$
$$N_{\partial, X}(B) = \{ b \in B \cap X \mid \exists b' \in B \cap X \mid b+b' \in A \};$$

on les désignera aussi simplement par $N_X(A)$ et $N_X(B)$, s'il n'y a pas de confusion possible.

Examinons de plus près les décompositions d'un produit de deux prémonoïdes commutatifs bien ordonnés, bien qu'à l'évidence beaucoup des considérations suivantes restent valables pour un « produit » quelconque, et s'adaptent aussi facilement au cas d'un produit de *précatégories bien ordonnées*…

Soient $\mathbf{E}_1 = (E_1,+,\leq)$ et $\mathbf{E}_2 = (E_2,+,\leq)$ deux prémonoïdes commutatifs bien ordonnés. Munissons l'ensemble {1,2} du bon ordre usuel : 1 < 2. Ainsi , dans le produit $E = E_1 \times E_2$, on dispose du bon ordre : $(x_1,x_2) < (y_1,y_2)$ si et seulement si : soit $x_1 < y_1$, soit si $x_1 = y_1$, $x_2 < y_2$. On peut identifier $\mathbf{E}_1$ (resp.$\mathbf{E}_2$) avec le sous-prémonoïde *additivement plein* $\mathbf{E}_1 \times \{0\}$ (resp. $\mathbf{E}_2 \times \{0\}$) de $\mathbf{E} = \mathbf{E}_1 \times \mathbf{E}_2$, de sorte que **E** apparaît comme *somme directe* de $\mathbf{E}_1$ et $\mathbf{E}_2$, ou encore (E_1, E_2) est une décomposition directe de **E** en deux sous-prémonoïdes additivement pleins. Cette décomposition est complètement stable ($N(E_1) = N(E_2) = \{0\}$). Si $x = (x_1,x_2) \in E$, on écrira aussi : $x = x_1 + x_2$.

Soit (A, B) une décomposition directe de **E** ; rappelons que l'élément neutre 0 est élément de A et de B et que $A \cap B = \{0\}$; elle induit des décompositions directes (A_1, B_1) et (A_2, B_2) de

de $\mathbf{E}_1$ et de $\mathbf{E}_2$ respectivement. Alors tout élément x de **E** se décompose de manière unique en somme de quatre éléments : $x = a_1 + b_1 + a_2 + b_2$ où $(a_1 , b_1 , a_2 , b_2) \in A_1 \times B_1 \times A_2 \times B_2$, de sorte que le quadruplet (A_1, B_1 , A_2 , B_2) apparaît comme une décomposition directe de **E** en quatre facteurs. Plus généralement, quelles que soient les parties $X \subset E_1$ et $Y \subset E_2$, $X \oplus Y$ est défini et égal à $X \times Y$, car on a toujours : $(x,y) = (x,0)+(0,y)$.

Théorème 1-1 (version absolue).
Supposons que $[N(B_1) = B_1$ ***ou*** $N(B_2) = B_2]$ ***et*** que $[N(A_2) = A_2$ ***ou*** $N(A_1) = A_1]$, alors la décomposition (A,B) est *triviale*, dans le sens que l'on a: $A = A_1 \oplus A_2$ et $B = B_1 \oplus B_2$.

► Posons $A' = A_1 \oplus A_2$ et $B' = B_1 \oplus B_2$ (ce sont bien des sommes directes tout comme l'est $E_1 \oplus E_2$). Supposons prouvé que $A(x) = A'(x)$ et $B(x) = B'(x)$ pour tout $x < z$ (rappelons que $C(x) = \{ y \in C \mid y \leq x \}$) et montrons que $A(z) = A'(z)$ et $B(z) = B'(z)$, de sorte que le résultat sera acquis par récurrence (éventuellement transfinie). L'élément z s'écrit de manière unique :

$$z = a + b, \text{ où } (a, b) \in A \times B$$
$$\text{et } z = z_1 + z_2 \text{ où } (z_1, z_2) \in E_1 \times E_2 ,$$
$$z_1 = a_1 + b_1 , z_2 = a_2 + b_2 , \text{ où } (a_1 , b_1 , a_2 , b_2) \in A_1 \times B_1 \times A_2 \times B_2 ,$$

On doit bien faire attention au fait qu'a priori $a \neq a_1 + a_2$ et $b \neq b_1 + b_2$.
On distingue alors selon que $z \in A \cup B$ ou non.

1) $z \notin A \cup B$; ceci équivaut à dire : $a \neq 0$ et $b \neq 0$; d'abord, on a :

$$A(z) = \bigcup_{x<z} A(x) = \bigcup_{x<z} A'(x) = A'(z), \text{ car } z \notin A' = A_1 \oplus A_2 ;$$

supposons en effet que $z = a_1 + a_2$ où $a_1 \in A_1$ et $a_2 \in A_2$; on a aussi $z = a + b$ où a et $b \neq 0$; $b < z$ implique : $b \in B(b) = B'(b)$, et donc $b = b'_1 + b'_2$, où $b'_1 \in B_1$ et $b'_2 \in B_2$; $a < z$ implique: $a \in A(a) = A'(a)$, et donc $a = a'_1 + a'_2$, où $a'_1 \in A_1$ et $a'_2 \in A_2$; comme $E = E_1 \oplus E_2$, $E_1 = A_1 \oplus B_1$ et $E_2 = A_2 \oplus B_2$, on a : $a_1 = a'_1 + b'_1$ et $a_2 = a'_2 + b'_2$ de sorte que $b'_1 = b'_2 = 0$, soit $b = 0$, ce qui n'est pas.

2) $z \in A \cup B$ (et z non nul !); supposons $z = a \in A$; supposons $a_1 + a_2 = 0$, alors b_1 *et* $b_2 \neq 0$ (car $A \cap B = \{0\}$!) ; utilisons l'hypothèse « $N(B_1) = B_1$ » ; il existe $b'_1 \in B_1$ tel que $b_1 + b'_1 \in A_1$; nous disposons alors de « deux » décompositions possibles pour l'élément $b_1 + b'_1 + b_2$:

$$b_1 + b'_1 + b_2 = (b_1 + b'_1) + b_2 = (b_1 + b_2) + b'_1 ;$$

donc $a_1 + a_2 \neq 0$; on a $b_1 + b_2 < z = a$, et par l'hypothèse de récurrence, $b_1 + b_2 \in B$.

Si on avait aussi $b_1 + b_2 \neq 0$, alors $a_1 + a_2$ serait élément de A, de sorte que z = a aurait deux décompositions, ce qui est impossible, à moins que $a = a_1$ (et $a_2 = 0$) ou $a = a_2$ (et $a_1 = 0$), mais alors $b_1 + b_2 = 0$. La seule possibilité est donc effectivement que $b_1 + b_2 = 0$, et donc on a aussi $a = a_1 + a_2 \in A'$.

On a vu au passage que l'hypothèse « $N(B_1) = B_1$ » aurait pu être remplacée par « $N(B_2) = B_2$ » pour établir ce fait. On vient de voir donc que $A(z) = A'(z)$.

Remarquons aussi que le cas où $N(B_1) = B_1 = \{0\}$ n'est pas exclu ; en effet, si tel est le cas, on peut reprendre le point (2) précédent sous la forme suivante :

$2)^{bis}$ $z \in A \cup B$ (et z non nul !); supposons $z = a \in A$; supposons $a_1 + a_2 = 0$; comme $b_1 = 0$, $z = b_2 \in A \cap B = \{0\}$ et il y a une contradiction; donc $a_1 + a_2 \neq 0$; si on avait aussi $b_2 \neq 0$, alors $a_1 + a_2$ serait élément de A, de sorte que z = a aurait deux décompositions, ce qui est impossible, à moins que $a = a_1$ (et $a_2 = 0$) ou $a = a_2$ (et $a_1 = 0$), mais alors on aurait $b_2 = 0$. La seule possibilité est donc effectivement que $b_2 = 0$, et donc on a aussi $a = a_1 + a_2 \in A'$.

En utilisant l'hypothèse « $N(A_1) = A_1$ » ou « $N(A_2) = A_2$ » , on établit de façon analogue que B(z) = B'(z), ce qui achève la démonstration ◄

Application.
Nous caractériserons plus loin toutes les décompositions directes (A,B) de (**N**,+)**.** On verra qu'un facteur direct A d'une telle décomposition satisfait la condition suivante : $N(A) \neq A$ si et seulement si $|B| < \infty$.
Supposons que (A,B) soit une décomposition directe *non triviale* de $\mathbf{N}^2$; alors la condition :

$$[N(B_1) = B_1 \text{ ou } N(B_2) = B_2] \text{ et } [N(A_2) = A_2 \text{ ou } N(A_1) = A_1]$$

n'est pas remplie. Donc l'une au moins des deux conditions suivantes n'est pas remplie :

$$[N(B_1) = B_1 \text{ ou } N(B_2) = B_2] , [N(A_2) = A_2 \text{ ou } N(A_1) = A_1],$$

c'est à-dire que l'on a :

$$[N(B_1) \neq B_1 \text{ et } N(B_2) \neq B_2] \text{ ou } [N(A_2) \neq A_2 \text{ et } N(A_1) \neq A_1],$$

soit encore :

$$[|A_2| < \infty \text{ et } |A_1| < \infty] \text{ ou } [|B_1| < \infty \text{ et } |B_2| < \infty];$$

et ces deux conditions sont exclusives l'une de l'autre.

Raffinement de ce théorème à certaines parties de E, utilisant les noyaux relatifs.
On suppose toujours donné un prémonoïde commutatif bien ordonné **E** = (E,+, ≤) et une de ses décompositions directes $E = A \oplus B$.

Définition 1-5.
Une partie X de **E** est dite *propre* (relativement à la décomposition directe donnée) si elle est non vide et si, pour tout x élément de X, $\underline{a}(x)$ et $\underline{b}(x)$ sont aussi éléments de X.

Premières conséquences de cette définition:
soit X une partie propre :
- inf(X) = 0 ; en effet, soit x_0 le plus petit élément de X ; il se décompose en $x_0 = a_0 + b_0$ et a_0 , $b_0 \in X$ avec a_0 , $b_0 \leq x_0$, d'où $x_0 = a_0 = b_0 = 0$.
- Si $X^* = X \setminus \{0\}$ n'est pas vide, $x_1 = \inf(X^*) \in A \cup B$.
- Si $X^{**} = X^* \setminus \{x_1\}$n'est pas vide, $x_2 = \inf(X^{**}) \in A \cup B$: en effet, supposons que $x_1 \in A$ et soit $x_2 = a+b$ la décomposition de x_2 ; si $b \neq 0$, on a : $a < x_2$ et donc a = 0 ou $a = x_1$; si a = 0, alors $x_2 = b \in B$; le cas $a = x_1$ est impossible car incompatible avec « $b < x_2$ et $b \neq 0$ » ; et si b = 0, alors $x_2 \in A$.
- En poursuivant, il y a une section commençante dans X, qui est dans A (resp. B) : $x_0 = 0$, x_1, x_2,…, x_n ; s'il y a un premier élément, soit x_{n+1} (n peut être un ordinal transfini, limite ou non), qui n'est pas dans A (resp.B), il est obligatoirement dans B (resp.A) ; en effet, $x_{n+1} = a+b$ avec $b \neq 0$; si $b < x_{n+1}$ alors $b = x_m$ avec m < n+1, soit $b \in A$, donc b = 0 et $x_{n+1} \in A$, ce qui est une contradiction ; reste donc la seule possibilité : $b = x_{n+1} \in B$.
- A partir de là, on peut trouver des éléments qui ne sont pas dans $A \cup B$.

- Si X est un sous-prémonoïde de E, le couple $(A_X,B_X) = (A\cap X, B\cap Y)$ est une décomposition directe de X.

On reprend les conditions générales du **théorème 1-1**.
Soit X (resp. Y) une partie propre de **E** contenue dans E_1 (resp. dans E_2); c'est donc aussi une partie propre de $\mathbf{E}_1$ (resp. $\mathbf{E}_1$) pour la décomposition directe induite par (A,B) sur E_1 (resp. sur E_1), soit (A_1, B_1) (resp. (A_2, B_2)).

Théorème 1-2. (version relative).
Supposons $[N_X(B_1)=B_1\cap X$ ou $N_Y(B_2) = B_2 \cap Y]$ et $[N_Y(A_2) = A_2\cap Y$ ou $N_X(A_1) = A_1\cap X]$ et supposons aussi que $X \times Y$ est une partie propre de E .
Alors la décomposition $(A \cap X\times Y,\ B \cap X\times Y)$ est *triviale*, dans le sens que l'on a:

$$A_{X\times Y} = A \cap X\times Y = (A_1\cap X) \oplus (A_2 \cap Y) \text{ et } B_{X\times Y} \cap X\times Y = (B_1\cap X) \oplus (B_2 \cap Y) .$$

► Remarquons d'abord que X et Y peuvent être identifiées à des parties de $X\times Y$: X à $X\times\{0\}$ et Y à $\{0\}\times Y$ et que (X,Y) est une décomposition directe de $X\times Y$ (qui n'est peut-être pas un prémonoïde d'ailleurs !) : $X\times Y = X \oplus Y$.

Posons $A'_{X\times Y} = (A_1\cap X) \oplus (A_2 \cap Y)$ et $B'_{X\times Y} = (B_1\cap X) \oplus (B_2 \cap Y)$ (ce sont bien des sommes directes tout comme $E_1 \oplus E_2$).
Remarquons ensuite que l'on a :

$$A'_{X\times Y} = (A_1\cap X) \oplus (A_2 \cap Y) = (A_1\oplus A_2) \cap(X\times Y)$$
$$B'_{X\times Y} = (B_1\cap X) \oplus (B_2 \cap Y) = (B_1\oplus B_2) \cap(X\times Y)$$

Supposons prouvé que $A_{X\times Y}(x) = A'_{X\times Y}(x)$ et $B_{X\times Y}(x) = B'_{X\times Y}(x)$ pour tout $x < z$ (rappelons que $C(x) = \{ y \in C \mid y \leq x \}$) et montrons que $A_{X\times Y}(z) = A'_{X\times Y}(z)$ et $B_{X\times Y}(z) = B'_{X\times Y}(z)$, de sorte que le résultat sera acquis par récurrence (éventuellement transfinie).

L'élément z s'écrit de manière unique :

$$z = a + b, \text{ où } a \text{ et } b \in (A\cup B) \cap X\times Y \text{ car } X\times Y \text{ est propre}$$
$$\text{et } z = z_1 + z_2 \text{ où } (z_1, z_2) \in X\times Y ,$$
$$z_1 = a_1 + b_1 , z_2 = a_2 + b_2 , \text{ où } (a_1 , b_1 , a_2 , b_2) \in A_1 \times B_1 \times A_2 \times B_2 ,$$

On doit bien faire attention au fait qu'a priori $a \neq a_1+ a_2$ et $b \neq b_1+ b_2$.

On distingue alors selon que $z \in A \cup B$ ou non.

1) $z \notin A \cup B$; ceci équivaut à dire : $a \neq 0$ et $b \neq 0$; d'abord, on a :

$$A_{X\times Y}(z) = \bigcup_{x<z} A_{X\times Y}(x) = \bigcup_{x<z} A'_{X\times Y}(x) = A'_{X\times Y}(z), \text{ car } z \notin A_1\oplus A_2 \cap X\times Y;$$

supposons en effet que $z = a_1 + a_2$ où $a_1 \in A_1 \cap X$ et $a_2 \in A_2 \cap Y$; on a aussi $z = a + b$ où a et $b \neq 0$; $b < z$ implique : $b \in B_{X\times Y}(b) = B'_{X\times Y}(b)$ et donc $b = b'_1+b'_2$, où $b'_1 \in B_1$ et $b'_2 \in B_2$; et $a < z$ implique: $a \in A_{X\times Y}(a) = A'_{X\times Y}(a)$ et donc $a = a'_1+a'_2$, où $a'_1 \in A_1$ et $a'_2 \in A_2$; comme $E = E_1\oplus E_2$, $E_1 = A_1 \oplus B_1$ et $E_2 = A_2 \oplus B_2$, on a : $a_1 = a'_1+b'_1$ et $a_2 = a'_2+b'_2$ de sorte que $b'_1 = b'_2 = 0$, soit $b = 0$, ce qui n'est pas.

2) $z \in A \cup B$ (et z non nul !); supposons $z = a \in A$; supposons $a_1 + a_2 = 0$, alors b_1 *et* $b_2 \neq 0$ (car $A \cap B = \{0\}$!) ; utilisons l'hypothèse « $N_X(B_1) = B_1 \cap X$ » ; alors il existe $b'_1 \in B_1 \cap X$ tel que $b_1+b'_1 \in E_1$; nous disposons alors de « deux » décompositions possibles pour l'élément $b_1+ b'_1+ b_2$:

$$b_1+ b'_1+ b_2 = (b_1+ b'_1) + b_2 = (b_1+ b_2) + b'_1 ;$$

donc $a_1+a_2 \neq 0$; on a $b_1+b_2 < z = a$, et par l'hypothèse de récurrence, $b_1+b_2 \in B$; si on avait aussi $b_1+b_2 \neq 0$, alors a_1+a_2 serait aussi élément de A, de sorte que $z = a$ aurait deux décompositions, ce qui est impossible. Reste comme seule possibilité $b_1+b_2 = 0$ et donc aussi $a = a_1+a_2 \in A'$.

On a vu au passage que l'hypothèse « $N_X(B_1) = B_1 \cap X$ » aurait pu être remplacée par l'hypothèse « $N_Y(B_2) = B_2 \cap Y$ » pour établir ce fait. On vient donc d'établir que $A_{X\times Y}(z) = A'_{X\times Y}(z)$.
En utilisant l'hypothèse « $N_X(A_1) = A_1 \cap X$ » ou « $N_Y(A_2) = A_2 \cap Y$ » , on établit de façon analogue que $B_{X\times Y}(z) = B'_{X\times Y}(z)$, ce qui achève la démonstration. ◄

On aura besoin d'un autre résultat assez général, concernant la *simplifiabilité*.

Soit $(E,+,\leq)$ un prémonoïde commutatif *bien ordonné.* On désigne par $\boldsymbol{P_0}(E)$ l'ensemble des parties de E contenant 0.
Etant données deux parties A et B de E , on désigne par $A*B$ l'ensemble des éléments de $A\times B$ qui sont des couples composables pour la loi de prémonoïde donnée.

Définition1-6.
On dit que la *somme directe* de A et de B est définie si la composition $\underline{k}$ définit une bijection de $A*B$ sur son image $\underline{k}(A*B) = A + B$, et c'est cette somme qu'on désigne par $A\oplus B$.

Il n'est pas nécessaire que 0 soit élément de A ou de B pour que $A\oplus B$ soit défini. Mais si 0 est élément commun de A et B, alors le fait que $A\oplus B$ soit défini entraîne que $A\cap B = \{0\}$.

Exemples.
Toujours avec le prémonoïde $\mathbf{E}_7$ (voir remarque 1 suivant définition 1-2).
Soient $A' = \{1,2\}$ et $B'' = \{5,6\}$; la somme $A'+B''$ est égale à $\{6,7\}$ et $A'*B'' = \{(1,5), (1,6), (2,5)\}$; donc $A'+B''$ ne peut être une somme directe ; $A'\oplus B''$ n'est pas défini.
Soient $A' = \{1,2\}$ et $B' = \{3,6\}$; $A'+B' = \{4, 5, 7\}$ et $A'*B' = \{(1,3), (1,6), (2,3)\}$; $A'\oplus B'$ est bien défini et pourtant $A'*B'$ n'est pas égal à $A'\times B'$.
Ce n'est pas la condition « imposée » stipulant que 0 soit élément des parties concernées qui est à l'origine de ce phénomène ; en effet $A = A' \cup \{0\}$ et $B = B' \cup \{0\}$ constituent une décomposition directe de $\mathbf{E}_7$ pour laquelle $A*B = A\times B \setminus \{(1,6)\}$, comme déjà vu.

Théorème 1-3.
La loi $\oplus$ structure l'ensemble $\boldsymbol{P_0}(E)$ en un prémonoïde d'élément neutre $\mathbf{0} = \{0\}$, commutatif et *simplifiable*. De plus ($\boldsymbol{P_0}(E), \oplus, \subseteq$) est un prémonoïde commutatif *ordonné*.
Le sous-ensemble $\boldsymbol{P_0}^{\mathbf{f}}(E)$ des parties finies de E contenant 0 détermine aussi un prémonoïde *ordonné* ($\boldsymbol{P_0}^{\mathbf{f}}(E), \oplus, \subseteq$) commutatif et simplifiable.
($\boldsymbol{P_0}(E), \oplus, \subseteq$) possèdent des inf. et des sup.quelconques, ($\boldsymbol{P_0}^{\mathbf{f}}(E), \oplus, \subseteq$) des inf. quelconques et des sup. finis.

Enfin, la relation X $\angle$ Y définie par l'existence d'un X' tel que Y = X$\oplus$X' est une relation d'ordre et ($\boldsymbol{P_0}$(E), $\oplus$, $\angle$) et ($\boldsymbol{P_0^f}$(E), $\oplus$, $\angle$) sont des prémonoïdes ordonnés commutatifs et simplifiables. Bien sûr, X $\angle$ Y entraîne X $\subseteq$ Y mais pas l'inverse en général.

► Soient A , B et C $\in$ $\boldsymbol{P_0}$(E) tels que (A$\oplus$B)$\oplus$C soit défini ; soient b, b'$\in$ B et c, c'$\in$ C tels que b+c et b'+c' soient définis et égaux ; b = 0+b $\in$ A$\oplus$B, puisque (0,b) $\in$ A$*$B ; comme b+c est défini,, on voit que b+c $\in$ (A$\oplus$B)$\oplus$C ; on voit de même que b'+c' $\in$ (A$\oplus$B)$\oplus$C ; comme cette somme est directe et que b+c = b'+c', on peut en conclure que (b, c) = (b', c'), ainsi l'application + : B$*$C $\rightarrow$ E est injective, et donc + : B$*$C $\rightarrow$ B+C est bijective ; c'est dire que B$\oplus$C est bien défini ; soient a, a'$\in$ A et e, e'$\in$ B$\oplus$C tels que a+e et a'+e' soient définis et égaux; e et e' peuvent s'écrire (et de manière unique) : e = b+c, e' = b'+c', où b, b'$\in$ B et c, c'$\in$ C ; comme a+(b+c) = a+e est défini dans **E** et que **E** est fortement associatif, on voit que (a+b)+c est aussi défini et égal à a+e ; on voit de même que (a'+b')+c' est défini et égal à a'+e' ; alors (a+b)+c et (a'+b')+c' sont définis et égaux; comme (A$\oplus$B)$\oplus$C est défini , on en déduit que (a+b, c) et (a'+b',c') sont définis et égaux ; ainsi c = c' et a+b = a'+b' ; comme A$\oplus$B est défini, on a aussi : a = a' et b = b', puis e = e', et enfin (a ,e) = (a' , e'), cer qui achève de prouver que A$\oplus$(B$\oplus$C) est bien défini et égal à (A$\oplus$B)$\oplus$C (l'axiome de forte associativité doit s'appliquer encore une fois ici)

On prendra garde au fait suivant : si A$\oplus$B est défini et si a+b = a+b', alors b = b', mais cela ne signifie pas du tout que la loi + soit simplifiable dans **E** ; en effet, si a+b et a+b' sont définis et égaux, le mieux qu'on puisse dire c'est ceci : soient A = {0,a} et B = {0,b,b'} ; si A$\oplus$B est défini , alors b = b' ! Mais il se peut très bien que ce ne soit pas le cas : si a , b, b' sont différents et différents de 0, A$*$B possède 6 éléments tandis que justement A+B n'en a que 5, donc A$\oplus$B n'est pas défini.

Poursuivons : il est clair que pour tout A $\in$ $\boldsymbol{P_0}$(E) , A $\oplus$ **0** et **0** $\oplus$ A sont définis et égaux. Ainsi ($\boldsymbol{P_0}$(E), $\oplus$) est un prémonoïde.
Montrons qu'il est commutatif : supposons A$\oplus$B défini ; comme **E** est commutatif l'application A$*$B $\rightarrow$ B$*$A qui à (a,b) fait correspondre (b,a) est bijective (facile à établir) ; comme A+B = B+A aussi et que + : A$*$B $\rightarrow$ A+B est une bijection, on voit que + : B$*$A $\rightarrow$ B+A en est une aussi ; c'est dire que B$\oplus$A est défini, et bien évidemment égal à A$\oplus$B.
Ainsi ($\boldsymbol{P_0}$(E), $\oplus$) est un prémonoïde.
Supposons maintenant que l'on ait A$\oplus$B = A$\oplus$B'; soit b le plus petit élément, *s'il existe*, qui soit dans B$\cup$B' mais pas dans B$\cap$B'; étant donné les rôles symétriques joués par B et B'on peut supposer que b $\in$ B et $\notin$ B'; alors b = 0+b est élément de A$\oplus$B = A$\oplus$B' ; il existe donc un unique couple (a,b') , élément de A$\times$B', tel que b = a+b' ; comme (E,+,$\leq$) un prémonoïde commutatif *bien ordonné,* on a b' $\leq$ b ; b' = b est impossible puisque b $\notin$ B' ; nécessairement, on a : b' < b ; si b' n'appartenait pas à B, alors b ne serait pas le plus petit élément de B$\cup$B' non dans B$\cap$B' ; ainsi b' $\in$ B et l'unicité de décomposition selon (A,B) entraîne a = 0 et b = b', ce qui est encore une contradiction. Donc un tel élément b n'existe pas et B = B'. Ceci prouve que le prémonoïde ($\boldsymbol{P_0}$(E), $\oplus$) est simplifiable.
Supposons que C = A$\oplus$B alors B et A sont des parties de C, puisque 0 est élément de A et B ; donc A$\subseteq$C et B$\subseteq$C ; supposons encore que B = C ; soit a $\in$ A ; a est aussi élément de C, donc de B = C, et comme A$\cap$B = {0}, il s'en suit que a = 0 et donc A = **0**. Ceci prouve que le prémonoïde ($\boldsymbol{P_0}$(E), $\oplus$, $\subseteq$) est *ordonné*.
Clairement, $\subseteq$ définit un ordre dans $\boldsymbol{P_0^f}$(E) de sorte que ($\boldsymbol{P_0^f}$(E), $\oplus$, $\subseteq$) est un prémonoïde ordonné, commutatif et simplifiable.

Etant donnée une famille quelconque d'élément A_i de $\boldsymbol{P_0}(E)$ (resp. $\boldsymbol{P_0}^{\mathbf{f}}(E)$) , $\inf\{A_i\}$est bien défini comme étant l'intersection des A_i . Les sup. sont les réunions.
Supposons $X \angle Y$ et $Y \angle Z$; il existe donc X' et Y' tels que $X \oplus X'$ et $Y \oplus Y'$ soient définis et $Y = X \oplus X'$, $Z = Y \oplus Y'$; on a donc : $Z = Y \oplus Y' = (X \oplus X') \oplus Y' = X \oplus (X' \oplus Y')$, donc $X \angle Z$.
Si l'on a $X \angle Y$ et $Y \angle X$, on a aussi $X \subseteq Y$ et $Y \subseteq X$, et donc $X = Y$; la relation $\angle$ est un ordre. Clairement, $(\boldsymbol{P_0}(E), \oplus, \angle)$ et $(\boldsymbol{P_0}^{\mathbf{f}}(E), \oplus, \angle)$ sont des prémonoïdes ordonnés par définition de $\angle$; ils sont commutatifs et simplifiables. ◄

Définition 1-7.
Soit (A,B) une décomposition directe d'un prémonoïde commutatif (E,+) dont les noyaux d'instabilité (voir définition 1-3) sont :

$N(A) = \{a \in A \mid \exists\, a' \in A \mid a + a' \in B\}$ et $N(B) = \{b \in B \mid \exists\, b' \in B \mid b + b' \in A\}$.

Un élément tel que a' (resp. b') est appelé *complément* de a (resp.b).

On définit une *loi de composition partielle* $+_b$ dans A de la façon suivante: soient x et x' deux éléments de A ; $x +_b x'$ est défini si et seulement si $x + x'$ est défini, et sa valeur n'est autre que $x +_b x' = \underline{a}\,(x + x')$. On définit de même la loi de composition partielle $+_a$ dans B.
Si a' est un complément de a, on voit que $a +_b a'$ est défini et vaut 0 (d'où le nom de complément !)

Proposition 1-1. ***(Unicité des compléments)***
Si (A,B) est une décomposition directe d'un prémonoïde commutatif (E,+) et si l'ensemble A*B des couples composables pour l'addition + est le produit cartésien A×B, alors il y a unicité des compléments.

► Soit $a \in N(A)$; par définition, il existe un élément $a'' \in A$ tel que $b = a+a'' \in B$ soit défini ; supposons qu'il existe un élément $a''' \in A$ tel que $b' = a+a''' \in B$ soit aussi défini; alors les éléments $a''+(a+a') = a''+b$ et $a'+(a+a'') = a'+b'$ sont définis, puisque A*B = A×B; mais (E,+) est un prémonoïde commutatif, donc $a''+b = a'+b'$; l'unicité de décomposition (de l'élément $a+a'+a''$) selon (A,B) entraîne $a' = a''$ et $b = b'$.

Ainsi, pour la loi $+_b$, le noyau apparaît comme l'ensemble des inversibles, car $a+a' = b \in B$ se traduit encore par : $a +_b a' = 0$. ◄

Cas particulier.
Si (A,B) est une décomposition directe d'un monoïde commutatif (E,+), il y a unicité des compléments ; N(A) (resp. N(B)) est l'ensemble des inversibles de $(A, +_b)$ (resp. $(B, +_a)$). C'est le cas de toute décomposition additive directe de $\mathbf{N}^k$, $k \geq 1$.

Nous avons déjà vu qu'en général A*B n'est pas A×B tout entier, dans le cas « prémonoïde ».

Divers exemples.

1) Soit toujours $\mathbf{E}_7 = \{0,1,2,3,4,5,6,7\}$ avec l'addition pour loi (limitée par 8 : 2+6, 3+5, etc…ne sont pas définis) ; comme déjà vu, $A = \{0,1,2\}$ et $B = \{0,3,6\}$ constituent une décomposition directe de $\mathbf{E}_7$ pour laquelle $A*B = A \times B \setminus \{2,6\}$ n'a que 8 éléments (comme E_7).

Cependant ici il y a unicité des compléments , mais cela ne résulte pas de la démonstration ci-dessus.

2) Soit $\mathbf{E}_{13}$ = {0,1,2,3,4,5,6,7,8,9,10,11,12} avec l'addition pour loi (limitée à 13 : 6+7, 3+10, 2+11, 3+11, 4+11, 10+5, 10+11, etc...ne sont pas définis).
A = {0,1,2,3,4,10} et B = {0,5,11} constituent une décomposition directe de $\mathbf{E}_{13}$ et A*B = A×B\ R où R = {(2,11),(3,11),(4,11),(10,5),(10,11)} n'a que13 éléments.
L'élément 1 a deux compléments : $1 +_b 4 = 1 +_b 10 = 0$; le système $(A,+_b)$ n'est pas un prémonoïde ; plus précisément la loi $+_b$ est associative en dimension 3, mais non fortement associative, ni même complètement associative : par exemple, on a : $(3+_b4)+_b10$ est défini et vaut 1, tandis que $3+_b(4+_b10)$ n'est pas défini ($14 \geq 13$) ; de même $1+_b(2+_b10)$ est défini et vaut 2, tandis que $(1+_b2)+_b10 = 3+_b10$ n'est pas défini ($13 \geq 13$) ; la loi $+_b$ est associative en dimension 3 (i.e. si $(x+_by)+_bz$ et $x+_b(y+_bz)$ sont définis ils sont égaux) : en effet, d'abord si $x,y,z < 5$, $(x+_by)+_bz$ et $x+_b(y+_bz)$ (bien définis) sont égaux, car, à iso près, on est dans $\mathbf{Z}/5\mathbf{Z}$; supposons maintenant $x = 10$; comme $10+_by$ est supposé défini, y = 0,1 ou 2 et donc$10+_by$ = 10,0 ou 1 ; comme $x+_b(y+_bz)$ est supposé aussi défini, si $z < 5$, tout se passe encore comme si on était dans $\mathbf{Z}/5\mathbf{Z}$ l'élément 10 jouant le rôle de 4 = -1 ! Enfin, si z = 10 aussi, y ne peut pas être 0 sinon $10+_b10$ serait défini,ce qui n'est pas, et on a bien pour y = 1 ou 2 : $(10+_b y)+_b10 = 10+_b(y+_b10)$ (= 10 ou 0) ; pour montrer que la loi $+_b$ n'est pas associative, donnons cet exemple $+_b$:
$(((10 +_b 1) +_b (10 +_b 2)) +_b 3) +_b (1 +_b 10) = ((0 +_b 1) +_b 3) +_b 0 = 4$
$((10 +_b 1) +_b ((10 +_b 2) +_b (3 +_b 1))) +_b 10 = (0 +_b (1 +_b 4)) +_b 10 = 10$
Ceci fait voir au passage que la notion de *forte associativité* est bien plus intéressante que celle de *complète associativité*…

3) Soit $\mathbf{E}_{15}$ = {0,1,2,3,4,5,6,7,8,9,10,11,12,13,14} avec l'addition pour loi (limitée à 15: 4+11,10+5 etc…ne sont pas définis); les mêmes ensembles qu'au 2) A = {0,1,2,3,4,10} et B = {0,5,11} constituent une décomposition directe de $\mathbf{E}_{15}$ et A*B = A×B \ R où R = {(4,11),(10,5),(10,11)}, n'a que15 éléments (comme E_{15}) ! L'élément 1 a toujours deux compléments : $1 +_b 4 = 1 +_b 10 = 0$.
Par contre, ici la loi $+_b$ n'est pas associative, même en dimension 3 : en effet, $(10 +_b 2) +_b 3$ est défini et vaut $1 +_b 3 = 4$; de même $10 +_b (2 +_b 3)$ est défini et vaut $10 +_b 0 = 10$ (bien sûr, c'est l'élimination de 15 qui provoque ce phénomène…!)

Concernant l'associativité des lois $+_a$ et $+_b$, elle n'est donc pas acquise de manière générale comme le prouvent les exemples précédents.
Nous montrerons au paragraphe suivant que si (A,B) est une décomposition directe de $(\mathbf{N},+)$, alors $(A,+_b)$ et $(B,+_a)$ sont des monoïdes dont les groupes d'inversibles sont les noyaux N(A) et N(B). Ce résultat semble nécessiter la connaissance fine des décompositions de $(\mathbf{N},+)$.
En dimension 2, le résultat subsiste génériquement, mais se présentent déjà une infinité d'exceptions (décompositions non triviales et non génériques) dans lesquelles un des systèmes $(A,+_b)$ ou $(B,+_a)$ n'est pas associatif.

2. Structures des décompositions directes additives de N.

Soit (A,B) une décomposition (additive) directe de **N** en deux facteurs ; tout entier n s'écrit de manière unique comme somme d'un élément a de A et d'un élément b de B; on emploie aussi la notation *fonctionnelle* : a = $\underline{a}(n)$ et b = $\underline{b}(n)$. On remarque que $A \cap B = \{0\}$. Pour fixer les idées, on supposera $1 \in A$.

Proposition 2-1.
Il existe une unique suite dite des *multiplicateurs*, suite finie ou non d'entiers strictement supérieurs à 1, soit m_1 , m_2 ,…, m_k ,…, à laquelle est associée une autre suite dite *base généralisée de* **N** :

$$b_0 = 1 \ , \ b_1 = m_1.b_0 \ , \ b_2 = m_2.b_1 \ , \ b_k = m_k.b_{k-1} = m_k.\, m_{k-1}\ldots\, m_1 \ , \ \ldots$$

de sorte que tout nombre N s'écrit de manière unique sous la forme suivante :

$$N = \sum_{i=0}^{\ell} N_i b_i \ \text{ avec } \ N_i < m_{i+1} \text{ , pour tout i de } 0 \text{ à } \ell \text{ .}$$

S'il y a un dernier multiplicateur m_k , on peut convenir que $m_{k+1} = \infty$, de sorte qu'il n'y a simplement pas de condition de bornage sur N_k dans le terme $N_k b_k$ et on peut convenir aussi que l'on a : $\ell \leq k$.
Le lien avec la décomposition $\mathbf{N} = A \oplus B$ supposée est alors le suivant :

$$A = \{ N = \sum_{i=0}^{\ell} N_i b_i \mid N_{2i+1} = 0 \} \quad \text{et} \quad B = \{ N = \sum_{i=0}^{\ell} N_i b_i \mid N_{2i} = 0 \} ,$$

de sorte que tout nombre $N = \sum_{i=0}^{\ell} N_i b_i$ se décompose de façon unique en $N = \underline{a}(N)+\underline{b}(N)$ où

$$\underline{a}(N) = \sum_{i=0} N_{2i} b_{2i} \ \in \ A \quad \text{et} \quad \underline{b}(N) = \sum_{i=0} N_{2i+1} b_{2i+1} \ \in \ B$$

La suite dite des multiplicateurs peut être « vide », la « base généralisée » étant réduite alors à son seul terme $b_0 = 1$ (si $1 \in A$, alors $A = \mathbf{N}$ et $B = \{0\}$, si $1 \in B$, alors $B = \mathbf{N}$ et $A = \{0\}$).

►Indiquons seulement comment on récupère la base généralisée (ou la suite des multiplicateurs) à partir d'une décomposition directe donnée (A,B) de **N** pour laquelle $1 \in A$.
Le premier élément non nul qui n'est pas dans A (s'il existe) est évidemment $b_1 = m_1$; autrement, c'est que $B = \{0\}$ et $A = \mathbf{N}$. Si l'élément $2m_1$ n'est pas dans B, il est nécessairement dans A ; tous les éléments de la forme $2m_1 + a$, avec $a < m_1$ sont dans A et le multiplicateur $m_2 = 2$.
En fait, le premier multiple de b_1 qui ne soit pas dans B (s'il existe) est dans A; c'est $b_2 = m_2.b_1$; s'il n'existe pas c'est que $A = \{0,1,2,\ldots b_1 - 1\}$ et $B = b_1.\mathbf{N}$, c'est le cas de la simple division euclidienne par b_1.
On continue ainsi : le premier multiple de b_2 qui ne soit pas dans A (s'il existe) est dans B; c'est $b_3 = m_3.b_2 = m_3.\, m_2.b_1\ldots$Il convient de vérifier alors que tous les éléments de la forme $k.b_2 + a_1$ où $k < m_3$, $a_1 \in A$, $a_1 < b_2$ sont nécessairement dans A (c'est ici que la notion de complément peut être utile)…
Le schéma général est alors en place. ◄

Pour une démonstration plus poussée, je renvoie par exemple à ma thèse ou écrits antérieurs, où figurent bien d'autres résultats concernant ce problème.

Connaissant le résultat, il n'est pas bien difficile d'imaginer une démonstration, somme toute fort simple, consistant en :
- une cascade de divisions euclidiennes d'un entier N par les éléments de la base généralisée, commençant par le plus grand possible, laquelle base généralisée se définit aisément à partir de la donnée de (A,B) en termes de sup. ou de inf. « relatifs »,
- des mises en défaut adéquates de l'unicité de décomposition grâce à la notion de complément (relatif) liée à la description explicite des noyaux d'instabilité (voir plus loin).
Mais bien évidemment, si l'on n'est pas prévenu du résultat par la méthode « naturelle » (suggérée ci-dessus, et qui procède en sens inverse, qui se dispense a priori de la division euclidienne, qui n'utilise que l'addition et le bon ordre, qui est de portée nettement plus générale, et qui figure dans ma thèse à titre d'*exemple*), la démonstration que nous venons de décrire succinctement est complètement artificielle et de peu d'intérêt !

Il est clair que ce type de décompositions comprend le cas de la *division euclidienne* par b (en prenant $b_0 = 1$, $b_1 = b$, $b_2 = \infty$) et les divers *systèmes de numérations* en base b (suites constantes de multiplicateurs $m_k = b$).

On remarquera aussi que si A ou B est fini, la décomposition $A \oplus B$ apparaît comme une véritable division euclidienne (par le plus grand élément b de la base généralisée) accompagnée d'une décomposition directe du reste (i.e. une décomposition directe du *segment* $\mathbf{E}_b = [0,b-1]$).

Proposition 2-2.
Supposons $\mathbf{N} = A \oplus B$; alors A et B définissent des *sous-prémonoïdes* (commutatifs) de **N.**

► Supposons en effet que N, N', N'', N+N', N+N'+N'' $\in$ A et montrons que N'+N'' $\in$ A aussi .
Pour un indice i tel que N_i ou N'_i au moins soit différent de 0, il est clair que $N_i+N'_i < m_{i+1}$, car il ne peut pas y avoir de retenue, N+N'devant être encore dans A; ainsi on a, pour tout i, $(N+N')_i = N_i + N'_i$ (= 0 pour les i impairs); avec le même raisonnement, compte tenu de ce que (N+N')+N'' $\in$ A, on voit que pour tout i, $((N+N')+N'')_i = (N+N')_i + N''_i$ (= 0 pour les i impairs); d'où, pour tout i : $(N'+N'')_i = N'_i + N''_i$ (= 0 pour les i impairs) ; on en conclut bien que N'+N'' $\in$ A, et donc que A est un prémonoïde. On procède de même avec B. ◄

Remarques.

1) Les applications $\pi_i : A \rightarrow [0,m_i[$ qui à a $\in$ A font correspondre $N_i = \pi_i(a)$ déterminent des homomorphismes entre prémonoïdes commutatifs, et que A est naturellement isomorphe au prémonoïde somme (finie ou non) $\oplus_i [0,m_{2i}[$ via les *injections naturelles* s_{2i} définies par $s_{2i}(n) = n.b_{2i}$; cet objet somme est aussi un produit, via les *projections* $\pi_{2i} : A \rightarrow [0,m_{2i}[$ *naturelles*, dans le cas où A est fini, et seulement dans ce cas.

2) Entre les injections s_{2i} et les projections π_{2i} existent les relations bien connues dans les catégories additives.

3) On a aussi la bijection : $\mathbf{N} \sim (\oplus_i [0,m_{2i}[ ) \oplus (\oplus_i [0,m_{2i+1}[ )$, ces sommes pouvant être finies ou non, étant entendu qu'il faut introduire le multiplicateur ∞ une fois si nécessaire, c'est-à-

dire si l'ensemble des multiplicateurs est fini (voir plus loin). Ce n'est évidemment pas un isomorphisme de prémonoïdes (contrairement au cas de A ou B)

4) Pour tout entier $n > 0$, le segment $[0,n-1]$ définit le sous-prémonoïde **n** = de **N**, évidemment non plein puisque l'addition y est toujours partielle, sur lequel (A,B) induit une décomposition directe (A_n,B_n) où $A_n = A \cap [0,n]$ et $B_n = B \cap [0,n]$.

Décompositions en plusieurs facteurs.

Définition 2-1.

Une famille $(A_k)_{k\in K}$ de parties de **N** est appelé *décomposition directe additive de* **N** *en* K *facteurs* si tout entier n s'écrit de manière unique comme somme (à support fini dans K) d'éléments des A_k. On écrira : $\mathbf{N} = \oplus_{k\in K} A_k$. Il est clair que l'on a :

$$\forall\, k\in K, \forall\, k'\in K,\ k \neq k',\ A_k \cap A_{k'} = \{0\}.$$

Proposition 2-3.

Supposons que $\mathbf{N} = \oplus_{k\in K} A_k$.

Alors, il existe une unique suite dite des *multiplicateurs*, suite finie ou non d'entiers strictement supérieurs à 1, soit m_1 , m_2 ,…, m_i ,…, à laquelle est associée une autre suite dite *base généralisée de* **N** :

$$b_0 = 1\ ,\ b_1 = m_1.b_0\ ,\ b_2 = m_2.b_1\ ,\ b_i = m_i.b_{i-1} = m_i.\, m_{i-1}\ldots\, m_1\ ,\ \ldots$$

de sorte que tout nombre N s'écrit de manière unique sous la forme suivante :

$$N = \sum_{i=0}^{\ell} N_i b_i \ \text{ avec } \ N_i < m_{i+1}\ \text{, pour tout i de } 0 \text{ à } \ell\ .$$

S'il y a un dernier multiplicateur m_j , on peut convenir que $m_{j+1} = \infty$, de sorte qu'il n'y a simplement pas de condition de bornage sur N_j dans le terme $N_j b_j$ et on peut convenir aussi que l'on a : $\ell \leq j$.

Le lien avec la décomposition $\mathbf{N} = \oplus_{k\in K} A_k$ supposée est alors le suivant : il y a une partition de l'ensemble (fini ou non) $I = \{0,1,2,\ldots,i,\ldots\}$des indices de la base généralisée, soit $I = \oplus_{k\in K} I_k$ ayant les propriétés suivantes :

$$\forall\, i \in I\ \forall\, k \in K\ \ (\ i \in I_k\ \Rightarrow\ i+1 \notin I_k\ )$$

la convention de l'éventuel multiplicateur ∞ (lorsque I est fini !) permet de ne faire aucune restriction dans cette formulation.

$$\forall\, k \in K \quad A_k\ =\ \{\ N = \sum_{i=0}^{\ell} N_i b_i \mid \forall\, i \notin I_k\ ,\ N_i = 0\ \}$$

De sorte que tout nombre $N = \sum_{i=0}^{\ell} N_i b_i$ se décompose de façon unique en

$$N = \sum_{k\in K} \underline{a}_k(N) \quad \text{où} \quad \underline{a}_k(N) = \sum_{i\in I_k} N_i b_i$$

La suite dite des multiplicateurs peut être « vide », la « base généralisée » étant réduite alors à son seul terme $b_0 = 1$ (si $1 \in A_k$, alors $A_k = \mathbf{N}$ et $A_{k'} = \{0\}$, pour tout $k' \neq k$).

La démonstration est assez semblable au cas de deux facteurs et on peut faire les mêmes remarques générales que dans le cas de deux facteurs.

Remarque. Chaque facteur d'une décomposition (additive) de **N** en plusieurs facteurs est encore un sous-prémonoïde de **N** ; la démonstration est semblable au cas de deux facteurs.

Calcul des noyaux d'instabilité d'une décomposition (additive) de N.

Soit donc $\partial = (A,B)$ une décomposition directe de **N** avec $1 \in A$.

Proposition 2-4.
On distingue deux cas : (i) $|A| = |B| = \infty$ et (ii) $|A|$ ou $|B|$ est fini:
(i) Si $|A| = |B| = \infty$, alors $N(A) = A$ et $N(B) = B$.
(ii) Si $|B| < \infty$ (et $|A| = \infty$), alors $N(A) = A \cap [0, \beta^+]$ où $\beta^+ = \sup(B)$ et $N(B) = B$
Si $|A| < \infty$ (et $|B| = \infty$), alors $N(B) = B \cap [0, \alpha^+]$ où $\alpha^+ = \sup(A)$ et $N(A) = A$

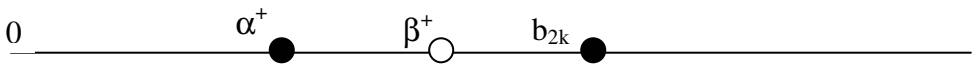
► (i) $|A| = |B| = \infty$. La suite des m_k est illimitée, de sorte que si $a = \sum^*_{i=0} N_{2i} b_{2i}$, on peut prendre $a' = \sum^*_{i=0} (m_{2i+1} - N_{2i}) b_{2i}$, qui est toujours défini, et on a bien $a+a' = \sum^*_{i=0} b_{2i+1} \in B$ (Le symbole $\sum^*_{i=0}$ signifie qu'on ne prend en compte, dans l'écriture même, que les indices i pour lesquels $N_{2i} > 0$, de sorte que l'on a bien aussi l'inégalité $m_{2i+1}-N_{2i} < m_{2i+1}$).

(ii) $1 < |B| < \infty$. La suite des multiplicateurs se termine avec un m_{2k} , et $m_{2k+1} = \infty$, de sorte que dans le terme $N_{2k}b_{2k}$, N_{2k} n'est pas borné. La base est finie : b_0 , b_1 ,…, b_{2k} .

Tout élément de A est de la forme $a = \sum_{i=0}^{k} N_{2i} b_{2i}$ sans borne a priori pour N_{2k} ;

Tout élément de B est de la forme $b = \sum_{i=0}^{k-1} N_{2i+1} b_{2i+1}$.

$|B| < \infty$



$\text{Sup}(B) = \beta^+ = \sum_{i=0}^{k-1} (m_{2i+2} - 1) b_{2i+1} = \sum_{i=0}^{k-1} b_{2i+2} - \sum_{i=0}^{k-1} b_{2i+1}$; donc pour tout $b \in B$, il existe $b' \in B$ tel que $b+b' \in A$, de sorte que $N(B) = B$ (pour $b \leq \beta^+$, c'est le même argument qu'en (i))

Par contre, $N(A) = A \cap [0,b_{2k}[= A \cap [0, \beta^+] = A \cap [0, \alpha^+]$, où $\alpha^+ = \sum_{i=0}^{k-1} (m_{2i+1} - 1) b_{2i}$ est le prédécesseur de b_{2k} dans A, ou le sup des a dominés par un élément de B.
On vérifie sans peine l'égalité suivante : $\alpha^+ + \beta^+ = b_{2k} - 1$

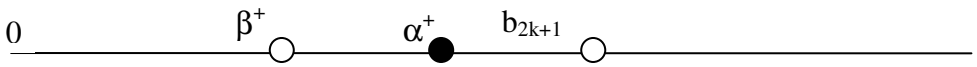
On notera que sont équivalentes les conditions suivantes :
- $a < B$, pour signifier qu'il existe un élément de B plus grand que a,
- $a < \beta^+$,
- $a < b_{2k}$,
- $a \leq \alpha^+$, ou bien est de la forme $\sum_{i=0}^{k-1} N_{2i} b_{2i}$.

(ii) $1 < |A| < \infty$. La suite des multiplicateurs se termine avec un m_{2k+1} , et $m_{2k+2} = \infty$, de sorte que dans le terme $N_{2k+1}b_{2k+1}$, N_{2k+1} n'est pas borné. La base est finie : $b_0, b_1 \ldots, b_{2k+1}$.

Tout élément de B est de la forme $b = \sum_{i=0}^{k} N_{2i+1}b_{2i+1}$ sans borne a priori pour N_{2k+1} ;

Tout élément de A est de la forme $a = \sum_{i=0}^{k} N_{2i}b_{2i}$

$|A| < \infty$



$\mathrm{Sup}(A) = \alpha^+ = \sum_{i=0}^{k}(m_{2i+1}-1)b_{2i} = \sum_{i=0}^{k} b_{2i+1} - \sum_{i=0}^{k} b_{2i}$; donc pour tout $a \in A$, il existe $a' \in A$ tel que $a+a' \in B$, de sorte que $N(A) = A$ (pour $a \leq \alpha^+$, c'est le même argument qu'en (i))

Par contre, $N(B) = B \cap [0,b_{2k+1}[= B \cap [0, \alpha^+] = B \cap [0, \beta^+]$, où $\beta^+ = \sum_{i=0}^{k-1}(m_{2i+2}-1)b_{2i+1}$ est le prédécesseur de b_{2k+1} dans B, ou le sup des b dominés par un élément de A.
On vérifie sans peine l'égalité suivante : $\alpha^+ + \beta^+ = b_{2k+1} - 1$

On notera que sont équivalentes les conditions suivantes :
- $b < A$, pour signifier qu'il existe un élément de A plus grand que b,
- $b < \alpha^+$,
- $b < b_{2k+1}$,
- $b \leq \beta^+$, ou bien est de la forme $\sum_{i=0}^{k-1} N_{2i+1}b_{2i+1}$.

On retiendra qu'on a toujours :
- $\alpha^+ + \beta^+ = b^{++} - 1$;
- $a + a' = \sum^{*}_{i=0} m_{i+1}.b_i = \sum^{*}_{i=0} b_{i+1}$
- Quand l'indice maximum i concerné par le symbole $\sum^{*}_{i=0}$ est maximum absolu, soit i^* , c'est que la somme $a + a'$ *dépasse* $b^{++} = b_{i^*+1}$.

Concernant les noyaux d'instabilité pour la décomposition $\partial = (A,B)$ donnée, on peut dire ceci : avec A fini, on a $N_\partial(A) = A$ et $N_\partial(B) = B \cap [0,b^{++}[= B \cap [0, \alpha^+] = B \cap [0, \beta^+]$ comme vu ci-dessus, et pour la décomposition induite $\partial^* = (A^*,B^*)$ sur $[0,b^{++}[$ on voit que : $N_{\partial^*}(A^*) = A^* \setminus A^+ = A \setminus A^+$ et $N_{\partial^*}(B^*) = B \cap [0,b^{++}[= B^*$; la situation est inversée pour les noyaux (maximum ou non !). Cependant il apparaîtra plus loin que les noyaux relatifs sont plus intéressants que les noyaux absolus ; ici, en posant $X = [0,b^{++}[$, on voit que les noyaux de A et B relatifs à X sont les suivants : $N_{\partial, X}(A) = A$ et $N_{\partial, X}(B) = B^*$, ce qui, par rapport à la situation précédente, « agrandit » $N_{\partial^*}(A^*) = A \setminus A^+$ en $N_{\partial, X}(A) = A$ … ◄

Remarques.

1) Pour $|B| < \infty$, l'élément b_{2k} de A joue le rôle de l'∞ du cas (i) ; l'élément α^+ est le prédécesseur de b_{2k} dans A.

2) Enfin, si $|B| = 1$, alors $B = \{0\}$ et $A = \mathbf{N}$; $N(B) = B$ et $N(A) = A \cap [0, \beta^+]$ car $\beta^+ = 0$; on peut convenir que $\alpha^+ = 0$, tandis que $b_{2k} = b_0 = 1$ (un seul multiplicateur $m_1 = \infty$)

3) Pour $|A| < \infty$, l'élément b_{2k+1} de B joue le rôle de l'∞ du cas (i) ; l'élément β^+ est le prédécesseur de b_{2k+1} dans B.

4) Si A est fini, mais que $1 \in B$, alors A se substitue à l'ensemble B tel que traité ci-dessus. Tant qu'on n'aura pas vraiment besoin de statuer sur ce fait on désignera par α^+ le sup(A), par β^+ le sup($B \cap [0, \alpha^+]$) et par b^{++} le premier élément de B qui n'est pas dans A.

5) Si $|A| = 1$, alors $A = \{0\}$ et $B = \mathbf{N}$; $N(A) = A$ et $N(B) = A \cap [0, \alpha^+]$ car $\alpha^+ = 0$; on peut convenir que $\beta^+ = 0$, tandis que $b_{2k} = b_0 = 1$.

6) Pour $a = \sum^*_{i=0} N_i b_i$ (que les i concernés soient tous pairs, ou tous impairs) on désignera *son complément* par a', c'est l'élément $a' = \sum^*_{i=0} (m_{i+1} - N_i) b_i$ (voir, dans la démonstration de la proposition 2-4, la signification de la notation astérisque). Celui-ci n'est défini que si $a \neq 0$.

Proposition 2-5.
Soit (A,B) une décomposition directe additive de (**N**,+), alors les lois $+_a$ et $+_b$ sont associatives. $\mathbf{A} = (A,+_b)$ et $\mathbf{B} = (B,+_a)$ sont donc des monoïdes commutatifs dont les groupes d'inversibles sont respectivement N(A) et N(B).
Particulièrement, si $|A| = |B| = \infty$, alors **A** et **B** sont des groupes abéliens.

► On suppose $1, n, n', n'' \in A$.
On sait que $A = \{ n \in \mathbf{N} \mid \forall i \quad n_{2i+1} = 0 \}$; les indices qui interviennent ici sont donc pairs .
Si $n_i + n'_i < m_i$, alors on sait que $(n + n')_i = n_i + n'_i = (n +_b n')_i$; par contre, si $n_i + n'_i \geq m_i$ on a : $(n + n')_i = n_i + n'_i - m_i = (n +_b n')_i$.
Donc,

$$n +_b n' = \sum^*_{n_i + n'_i < m_i} (n_i + n'_i) b_i \; + \sum^*_{n_i + n'_i \geq m_i} (n_i + n'_i - m_i) b_i \, ,$$

Nous avons alors :
$(n +_b n') +_b n'' =$

$$= \sum^*_{(n +_b n')_i + n''_i < m_i} ((n +_b n')_i + n''_i) b_i \; + \sum^*_{(n +_b n')_i + n''_i \geq m_i} ((n +_b n')_i + n''_i - m_i) b_i$$

$$= \sum^*_R (n + n'_i + n''_i) b_i \; + \sum^*_T (n + n'_i + n''_i - m_i) b_i \; + \sum^*_S (n + n'_i + n''_i - 2m_i) b_i$$

où $R = \{ i \mid 0 < n_i + n'_i + n''_i < m_i \}$, $S = \{ i \mid n_i + n'_i + n''_i \geq 2m_i \}$ et où
$T_1 = \{ i \mid n_i + n'_i + n''_i < 2m_i \wedge n_i + n'_i \geq m_i \}$ $T_2 = \{ i \mid n_i + n'_i + n''_i \geq m_i \wedge n_i + n'_i < m_i \}$ et $T = T_1 \cup T_2$
On trouve de même, simplement en échangeant les rôles de n et n'', car on est dans le cas commutatif :
$n +_b (n' +_b n'') =$

$$= \sum^*_R (n + n'_i + n''_i) b_i \; + \sum^*_{T'} (n + n'_i + n''_i - m_i) b_i \; + \sum^*_S (n + n'_i + n''_i - 2m_i) b_i \quad \text{où}$$

$T'_1 = \{ i \mid n_i + n'_i + n''_i < 2m_i \wedge n''_i + n'_i \geq m_i \}$ $T'_2 = \{ i \mid n_i + n'_i + n''_i \geq m_i \wedge n''_i + n'_i < m_i \}$ et
$T' = T'_1 \cup T'_2$.

Reste à vérifier que T = T'. Posons $U = \{ i \mid n_i + n'_i < m_i \}$ et $U^c = \{ i \mid n_i + n'_i \geq m_i \}$;
$T'_1 = (T'_1 \cap U) \cup (T'_1 \cap U^c)$; mais $(T'_1 \cap U) \subset T_2$ et $(T'_1 \cap U^c) \subset T_1$ d'où $T'_1 \subset T$;
de même $T'_2 = (T'_2 \cap U) \cup (T'_2 \cap U^c)$, $(T'_2 \cap U) \subset T_2$, $(T'_2 \cap U^c) \subset T_1$ d'où $T'_2 \subset T$;
on en déduit que l'on a : $T' \subset T$; on prouve de même que $T \subset T'$ et finalement $T = T'$.
Ceci achève de prouver que la loi $+_b$ est bien associative. Clairement 0 est élément neutre. ◄

Enfin on a déjà remarqué que le noyau N(A) n'est autre que le groupe des inversibles du monoïde $(A, +_b)$. La démonstration est analogue pour $(B, +_a)$.

On voit que dans le cas de (**N**, +), toujours en supposant $1 \in A$, on a :
$(A, +_b) = (N(A), +_b) \cong \coprod_i \mathbf{Z}/m_{2i+1}.\mathbf{Z}$ si $|B| = \infty$; c'est un groupe ;

$(A, +_b) \cong (\coprod_i \mathbf{Z}/m_{2i+1}.\mathbf{Z}) \oplus (\mathbf{N},+)$ si $|B| < \infty$; c'est un monoïde dont le groupe des inversibles n'est autre que $(N(A), +_b) \cong \coprod_i \mathbf{Z}/m_{2i+1}.\mathbf{Z}$, tandis que :

$(B, +_a) = (N(B), +_a) \cong \coprod_i \mathbf{Z}/m_{2i}.\mathbf{Z}$ si $|A| = \infty$; c'est un groupe ;

$(B, +_a) \cong (\coprod_i \mathbf{Z}/m_{2i}.\mathbf{Z}) \oplus (\mathbf{N},+)$ si $|A| < \infty$; c'est un monoïde dont le groupe des inversibles n'est autre que $(N(B), +_a) \cong \coprod_i \mathbf{Z}/m_{2i}.\mathbf{Z}$

Nous aurons besoin d'un autre résultat technique que voici. Nous conservons les notations précédentes pour une décomposition directe (A,B) de (**N**,+) donnée.

Etant donné un nombre n, on appelle *hauteur de* n (relative à (A,B), et on désigne par h(n), l'entier indice maximum i pour lequel $N_i \neq 0$ (il est donc pris en compte par le symbole de sommation avec astérisque $n = \sum^* N_i b_i$);

de plus, si $n \notin A$, on désigne par $i_B(n)$ le plus petit indice i tel que $N_i \neq 0$ et $b_i \in B$; si on a supposé que $1 \in A$, l'indice en question $i_B(n)$ est un entier impair $2j+1$.

On pose aussi $\alpha^+_r = (m_{r+1}-1).b_r + (m_{r-1}-1).b_{r-2} + \ldots + (m_{r-2s-1}-1).b_{r-2s-2} + \ldots$, éléments qu'on peut appeler *maximas relatifs* de A ; le maximum absolu, s'il existe, n'est autre que l'élément α^+_r avec r maximum ; si $1 \in A$, ce maximum absolu est de la forme α^+_{2r} ; c'est l'élément qu'on a déjà noté simplement α^+.

Avec ces conventions, nous pouvons énoncer la proposition suivante :

Proposition 2-5.
Soit (A,B) une décomposition directe de **N** ; soit n un entier non nul dominé par un élément a de A (i.e. : $n \leq a$) ; il existe un unique entier $\beta < a$ tel que :

$$\beta \in B \ , \ n + \beta \in A \ , \ n + \beta \leq a + \alpha^+_{h(a)-2} .$$

► On suppose que $1 \in A$, c'est-à-dire que $b_0 \in A$, les éléments de A étant de la forme $\sum^{*} N_{2i} b_{2i}$ et ceux de B de la forme $\sum^{*} N_{2i+1} b_{2i+1}$.

La démonstration est menée par récurrence sur l'entier h(a) (qui est pair) ; si h(a) = 0, l'entier n ($\leq$ a) est de la forme $N_0 b_0$ avec $N_0 < m_1$; c'est donc un élément de A, et il suffit de choisir $\beta = 0$ (par convention, ici, $\alpha^{+}_{0} = 0$).

Supposons le résultat établi pour tout entier (pair) plus petit que 2k et soit $a = \sum^{*} a_{2j} b_{2j}$ un élément de A tel que h(a) = 2k; soit alors $n = \sum^{*} N_i b_i \leq a$; posons h(n) = h .

- Si $N_h = a_{2k}$, alors h = 2k, $N_{h-1} = 0$ et $N_{h-2} \leq a_{2k-2}$ (car $n \leq a$ et $a \in A$); on soustrait l'élément $a^{*} = a_{2k}.b_{2k}$ de n et de a : $n' = n - a^{*}$ et $a' = a - a^{*}$; on a : $n' \leq a'$ et $h(a') < h(a)$; on peut donc appliquer l'hypothèse de récurrence : il existe un $\beta \in B$ tel que :

$$n' + \beta \in A \text{ et } n' + \beta \leq a' + \alpha^{+}_{h(a')-2};$$

alors, en rajoutant a^{*} à n' et à a', il vient bien :

$$n + \beta = n' + a^{*} + \beta \leq a' + \alpha^{+}_{h(a')-2} + a^{*} = a + \alpha^{+}_{h(a')-2} < a + \alpha^{+}_{h(a)-2} ,$$

car la suite $(\alpha^{+}_{2r})_{2r \geq 0}$ est strictement croissante .

- Autrement, on a : $N_{2k} < a_{2k}$ ou $h < 2k$. On peut supposer que $n \notin A$ (sinon il suffit de choisir $\beta = 0$) et donc l'entier $i_B(n) = 2j+1$ est bien défini et l'on a : $2j+1 < 2k$;

soit alors $\beta_1 = (m_{2j+2} - N_{2j+1}).b_{2j+1}$ et posons $n_1 = n + \beta_1 = \sum^{*} N_{1,i} b_i$.

Si $n_1 \in A$, on choisit $\beta = \beta_1$ et l'on a bien:

$$n_1 = n + \beta_1 \leq a_{2k}.b_{2k} + (m_1 - 1).b_0 + (m_3 - 1).b_2 + \ldots + (m_{2k-1} - 1).b_{2k-2} \leq a + \alpha^{+}_{h(a)-2}$$

car les coefficients $N_{1,2i+1}$ sont tous nuls.

Si $n_1 \notin A$, $i_B(n_1) = 2\ell+1$ est défini et l'on a : $i_B(n) < i_B(n_1)$; de plus, par le jeu des « retenues » possibles (chaque fois que $N_i + 1 = m_{i+1}$ et donc $N_{1,i} = 0$) , il n'est pas possible que $2\ell+1$ soit strictement supérieur à 2k (car $N_{2k}+1 \leq a_{2k}$ et $n_1 \notin A$); notons aussi qu'on a nécessairement: $n_1 \leq a$, puisque l'égalité $N_{1,2k} = a_{2k}$ est exclue (il y aurait sinon une retenue au niveau 2k-1 et n_1 serait élément de A) ; donc $N_{1,2k} < a_{2k}$ (et $n_1 < a$!)

- On peut alors recommencer et définir n_2 à partir de n_1 comme n_1 à partir de n ; on aura donc $n_2 = n_1 + \beta_2 = \sum^{*} N_{2,i} b_i$ où $\beta_2 = (m_{2\ell+2} - N_{2\ell+1}).b_{2\ell+1}$ est tel que $\beta_1 + \beta_2 \in B$; il y a donc un deuxième « train de retenues » qui s'amorce à l'indice $2\ell+1$. Le raisonnement dichotomique effectué pour n_1 peut être repris « mot à mot », puisque les conditions initiales sont bien les mêmes avec n_1 qu'avec n ; entre autres :
- Si $n_2 \in A$, on choisit $\beta = \beta_1 + \beta_2$ et l'on a bien :

$$n_2 = n + \beta_1 + \beta_2 = n_1 + \beta_2 \leq a_{2k}.b_{2k} + (m_1 - 1).b_0 + (m_3 - 1).b_2 + + (m_{2k-1} - 1).b_{2k-2} \leq a + \alpha^{+}_{h(a)-2}$$

car les coefficients $N_{2,2i+1}$ sont tous nuls.

- Si $n_2 \notin A$, $i_B(n_2) = 2\ell'+1$ est défini et l'on a : $i_B(n_1) < i_B(n_2)$; de plus, par le jeu des « retenues » possibles (chaque fois que $N_i+1 = m_{i+1}$ et donc $N_2,i = 0$) , il n'est pas possible que $2\ell'+1$ soit strictement supérieur à 2k (car $N_{2k}+1 \leq a_{2k}$ et $n_2 \notin A$); notons aussi qu'on a nécessairement: $n_2 \leq a$, puisque l'égalité $N_{2,2k} = a_{2k}$ est exclue (il y aurait sinon une retenue au niveau 2k-1 et n_2 serait élément de A) ; donc $N_{2,2k} < a_{2k}$ (et $n_2 < a$!)

Le processus lié à des « trains de retenues » successifs possibles se poursuit : n, n_1, n_2, …mais s'arrête nécessairement car la suite $i_B(n)$, $i_B(n_1)$, $i_B(n_2)$ … est strictement croissante et bornée par 2k. Il existe donc un entier q tel que $i_B(n)$, $i_B(n_1)$, $i_B(n_2)$, …, $i_B(n_{q-1})$ soient tous définis, mais pas $i_B(n_q)$, car $n_q = n_{q-1} + \beta_q = \ldots = n + \beta_1 + \beta_2 + \ldots + \beta_q$ est dans A ; clairement l'élément $\beta = \beta_1 + \beta_2 + \ldots + \beta_q$ est dans B et l'on a bien :

$n_q = n_{q-1} + \beta_q = n + \beta \leq a_{2k}.b_{2k} + (m_1-1).b_0 + (m_3-1).b_2 + \ldots + (m_{2k-1}-1).b_{2k-2} \leq a + \alpha^+_{h(a)-2}$,
car $i_B(n_{q-1}) \leq 2k-1$.

Si $1 \notin A$, le raisonnement est analogue, mais il convient d'échanger les rôles des indices pairs et impairs ◄

Remarques.

1) On a un énoncé analogue en échangeant les rôles de A et de B.

2) L'inégalité de la proposition 5 est la meilleure possible comme le montre l'exemple suivant : $n = (m_{2k} - 1).b_{2k-1} + (m_1-1).b_0 + (m_3-1).b_2 + \ldots + (m_{2k-1}-1).b_{2k-2}$ et $a = b_{2k}$; l'élément $\beta \in B$ tel que $n + \beta \in A$ est b_{2k-1} et $n + \beta = a + \alpha^+_{h(a)-2}$.

3) Lorsque le majorant a est égal à un *maximum relatif* α^+_{2k} , l'inégalité de la proposition 5 se simplifie *dans son écriture* : $n + \beta \leq a + \alpha^+_{h(a)-2}$ devient : $n + \beta \leq \alpha^+_{h(a)}$.

3. Les décompositions directes non triviales de $\mathbf{N}^2$ en deux facteurs.

Soit (A,B) une décomposition directe *non triviale* de $\mathbf{N}^2$. Elle induit les décompositions directes (A_1,B_1) sur $\mathbf{N} \times \{0\}$ et (A_2,B_2) sur $\{0\} \times \mathbf{N}$.
On a vu (application du **Théorème 1-1**) que [$|B_1| < \infty$ et $|B_2| < \infty$] ou [$|A_1| < \infty$ et $|A_2| < \infty$]
On supposera, pour fixer les idées, que l'on est dans la situation où $|A_1| < \infty$ et $|A_2| < \infty$.

On reprendra les notations génériques des décompositions directes de $\mathbf{N}$ (auquel $\mathbf{N} \times \{0\}$ et $\{0\} \times \mathbf{N}$ sont identifiés); entre autres :

$$\sup(A_i) = \alpha_i^+, \quad \sup(B_i \cap [0, \alpha_i^+]) = \beta_i^+ \text{ et } \inf(B_i \backslash A_i) = b_i^{++}, \ i = 1, 2$$

Considérons les sous-prémonoïdes de $\mathbf{N}^2$ suivants : $\mathbf{E}_1 = [0, b_1^{++}[\times \mathbf{N}$ et $\mathbf{E}_2 = \mathbf{N} \times [0, b_2^{++}[$. La décomposition donnée ∂ = (A,B) induit sur $\mathbf{E}_1$ et $\mathbf{E}_2$ des décompositions directes. Par application du **Théorème 1-1** ces décompositions sont triviales (les bons ordres induits sur $\mathbf{E}_1$ et $\mathbf{E}_2$ ne sont pas isomorphes (en général), et on peut, si on y tient, modifier le bon ordre sur $\mathbf{E}_1$, par exemple, en utilisant le bon ordre '2<1' plutôt que '1<2'. L'essentiel est de s'assurer qu'on dispose bien de bons ordres qui font de $\mathbf{E}_1$ et $\mathbf{E}_2$ des prémonoïdes bien ordonnés ; ce genre de remarques sera systématiquement utilisé par la suite, sans mention explicite…)

Soit $\mathbf{\Omega}$ le réseau engendré par $e_1 = (b_1^{++}, 0)$ et $e_2 = (0, b_2^{++})$.
Soit $\mathbf{C} = [0, b_1^{++}[\times [0, b_2^{++}[$.
On désigne toujours par $\underline{a}$ et $\underline{b}$ les applications qui fournissent les facteurs de décomposition : pour tout x, on a : $x = \underline{a}(x)+\underline{b}(x)$ avec $\underline{a}(x) \in A$ et $\underline{b}(x) \in B$.

Proposition 3-1.
($\mathbf{\Omega}$, $\mathbf{C}$) est une décomposition directe de $\mathbf{N}^2$; $\mathbf{\Omega}$ et $\mathbf{C}$ sont *propres* (***définition* 1-5**) pour la décomposition (A,B).
Plus précisément, tout $z \in \mathbf{N}^2$ s'écrit de façon unique $z = \omega+c$ où $\omega \in \mathbf{\Omega}$ et $c \in \mathbf{C}$, et on a :

$$\underline{a}(z) = \underline{a}(\omega) + \underline{a}(c) \text{ et } \underline{b}(z) = \underline{b}(\omega) + \underline{b}(c), \text{ avec } \underline{a}(\omega), \underline{b}(\omega) \in \mathbf{\Omega}.$$

► Remarquons d'abord qu'il serait erroné de dire que ($\mathbf{N}^2$, (A,B)) est isomorphe au produit cartésien de ($\mathbf{\Omega}$, (A_Ω, B_Ω)) et de ($\mathbf{C}$, (A_C, B_C)), car le monoïde $\mathbf{N}^2$ ne saurait être le produit du monoïde $\mathbf{\Omega}$ par le prémonoïde $\mathbf{C}$ (sauf dans le cas où celui-ci est égal à {0} !) Notons aussi que $\mathbf{C} \cap A \times B = A_C \times B_C = A_C * B_C$.

Soit $z = (x,y) \in \mathbf{N}^2$; par divisions euclidiennes, on voit qu'il existe un unique quadruplet d'entiers (p,q,r,s) tels que : $x = p.b_1^{++} + r$ avec $r < b_1^{++}$, $y = q.b_2^{++} + s$ avec $s < b_2^{++}$; ainsi $z = \omega+c$ où $\omega = (p.\, b_1^{++}, q.\, b_2^{++}) = pe_1 + qe_2 \in \mathbf{\Omega}$ et $c = (r,s) \in \mathbf{C}$.

Evidemment $\mathbf{C}$ est propre ; de plus , la décomposition induite par (A,B) sur $\mathbf{C}$ est triviale : on peut le voir de deux façons, soit en remarquant que $\mathbf{C}$ est inclus dans $\mathbf{E}_1$ ou $\mathbf{E}_2$ ($\mathbf{C} = \mathbf{E}_1 \cap \mathbf{E}_2$) qui sont déjà des sous-prémonoïdes de $\mathbf{N}^2$ sur lesquels (A,B) induit une décomposition triviale, soit en invoquant le théorème de décomposition dans sa version relative (ce qui, au fond, revient au même).

On procède maintenant par récurrence transfinie (avec l'ordre lexicographique dans $\mathbf{N}^2$). Supposons que, pour tout z' < z, on ait : $\underline{a}(z') = \underline{a}(\omega') + \underline{a}(c')$ et $\underline{b}(z') = \underline{b}(\omega') + \underline{b}(c')$, où (ω',c') est l'unique élément de $\mathbf{\Omega} \times \mathbf{C}$ tel que $z' = \omega'+c'$, avec $\underline{a}(\omega')$ et $\underline{b}(\omega') \in \mathbf{\Omega}$.
Venons-en alors à z et distinguons deux cas, selon que $z \in \mathbf{\Omega}$ ou que $z \notin \mathbf{\Omega}$:

- $z \in \mathbf{\Omega}$.

Si, en plus, $z \in A \cup B$, il n'y a rien à démontrer: soit $\underline{a}(z) = z$ et $\underline{b}(z) = 0$ si $z \in A$, soit $\underline{a}(z) = 0$ et $\underline{b}(z) = z$, si $z \in B$. 0

Supposons donc maintenant que $z \notin A \cup B$; $z = \underline{a}(z)+\underline{b}(z)$ avec $\underline{a}(z) < z$ et $\underline{b}(z) < z$; par hypothèse de récurrence, on peut écrire : $\underline{a}(z) = \omega_a + c_a$ et aussi $\underline{b}(z) = \omega_b + c_b$ où l'on a : $(\omega_a, c_a) \in (\mathbf{\Omega} \times \mathbf{C}) \cap A$ et $(\omega_b, c_b) \in (\mathbf{\Omega} \times \mathbf{C}) \cap B$; la somme c_a+c_b est nécessairement élément de **C**, puisque $(c_a, c_b) \in (A \times B) \cap \mathbf{C}$ et que la décomposition induite sur **C** est triviale ; mais $\omega_a+\omega_b \in \mathbf{\Omega}$, l'unicité de décomposition de z selon $(\mathbf{\Omega}, \mathbf{C})$ entraîne alors que $z = \omega_a + \omega_b$ ($c_a+ c_b =0$ et donc $c_a = c_b = 0$); ainsi $\underline{a}(z) = \omega_a$ et $\underline{b}(z) = \omega_b \in \mathbf{\Omega}$.

- $z \notin \mathbf{\Omega}$.

Si en plus, $z \notin A \cup B$, alors on est pratiquement dans la même situation que précédemment : $z = \underline{a}(z)+\underline{b}(z)$ avec $\underline{a}(z) < z$ et $\underline{b}(z) < z$; par hypothèse de récurrence, on a: $\underline{a}(z) = \omega_a+c_a$ et aussi $\underline{b}(z) = \omega_b+c_b$ où $(\omega_a, c_a) \in (\mathbf{\Omega} \times \mathbf{C}) \cap A$ et $(\omega_b, c_b) \in (\mathbf{\Omega} \times \mathbf{C}) \cap B$; soit $z = \omega + c$; l'unicité de décomposition de z selon $(\mathbf{\Omega}, \mathbf{C})$ entraîne : $\omega = \omega_a + \omega_b$ et $c = c_a+ c_b$; on a clairement: $\underline{a}(c) = c_a$, $\underline{b}(c) = c_b$, $\underline{a}(\omega) = \omega_a$ et $\underline{b}(\omega) = \omega_b$ de sorte que: $\underline{a}(z) = \underline{a}(\omega) + \underline{a}(c)$ et $\underline{b}(z) = \underline{b}(\omega) + \underline{b}(c)$.

Supposons donc maintenant que $z \in A \cup B$ (et toujours $z \notin \mathbf{\Omega}$) ; soit $z = \omega + c$, $c \neq 0$, la décomposition de z suivant $\mathbf{\Omega} \times \mathbf{C}$; alors $\omega < z$ s'écrit aussi $\omega_a + \omega_b$ et $c = c_a+ c_b$; on a donc encore : $z = \omega_a + c_a+ \omega_b + c_b$; supposons $\omega_b + c_b \neq 0$; alors $\omega_a + c_a < z$ et du coup, en utilisant l'hypothèse de récurrence, $\underline{a}(\omega_a + c_a) = \underline{a}(\omega_a) + \underline{a}(c_a) = \omega_a + c_a$, ce qui prouve que $\omega_a + c_a \in A$; supposons aussi $\omega_a + c_a \neq 0$; alors $\omega_b + c_b < z$ et du coup, en utilisant l'hypothèse de récurrence, $\underline{b}(\omega_b + c_b) = \underline{b}(\omega_b) + \underline{b}(c_b) = \omega_b+c_b$, ce qui prouve que $\omega_b+c_b \in B$; comme $z \in A \cup B$, il n'est pas possible d'avoir *en même temps* $\omega_b + c_b \neq 0$ et $\omega_a + c_a \neq 0$; on a donc soit $z = \omega_a + c_a$, soit $z = \omega_b + c_b$; reste à démontrer alors que dans le premier cas, on a bien $z \in A$, et que dans le second cas, on a bien $z \in B$.
On procède alors par l'absurde.
Supposons d'abord que $z \in B$ et $z = \omega_a + c_a$; on sait que $c_a = a_1 + a_2$ où $a_1 \in A_1$ et $a_2 \in A_2$; si $a_2 \neq 0$, son complément a'_2 est bien défini et tel que $a_2 + a'_2 = b_2 \in B_2 \subset B$; alors l'élément $z + a'_2$ aurait deux décompositions à savoir : $(a'_2 , z) \in A_2 \times B$, mais encore $(\omega_a+ a_1 , b_2) \in A \times B_2$ (en effet, $\omega_a + a_1 + b_2 = \omega_a + a_1 + a_2 + a'_2 = \omega_a + c_a + a'_2 = z + a'_2$, et le fait que a_2 soit différent de 0 fait que $\omega_a+ a_1 < z$ est bien un élément de A, par l'hypothèse de récurrence ; noter aussi que ces décompositions sont bien distinctes !) ; pour l'instant, on doit en conclure que, *nécessairement*, $a_2 = 0$ et $c_a = a_1$; comme $z = \omega_a + c_a \notin \mathbf{\Omega}$, on voit que $c_a = a_1 \neq 0$; son complément a'_1 est bien défini et tel que $a_1 + a'_1 = b_1 \in B_1 \subset B$; alors l'élément $z + a'_1$ aurait deux décompositions à savoir : $(a'_1 , z) \in A_1 \times B$, mais encore $(\omega_a , b_1) \in A \times B_1$ (en effet, $\omega_a + b_1 = \omega_a + a_1 + a'_1 = \omega_a + c_a + a'_1 = z + a'_1$, et le fait que a_1 tout comme a'_1 soient différents de 0 fait que $a'_1 \neq \omega_a$ est bien un élément de A, par l'hypothèse de récurrence ; noter aussi que ces décompositions sont bien distinctes !). On obtient encore une contradiction. La seule possibilité est bien $z \in A = \omega_a + c_a$, de sorte que l'on a bien $\underline{a}(z) = z = \underline{a}(\omega + c) = \omega_a + c_a = \underline{a}(\omega) + \underline{a}(c)$.

Supposons enfin que $z \in A$ et $z = \omega_b + c_b$; on peut reprendre le même schéma de démonstration que ci-dessus, en échangeant les rôles de A et B…Mais il y a ici une démonstration plus courte qui met bien en évidence la différence entre les deux cas de figure, ou si l'on veut entre noyaux absolus et noyaux relatifs. En effet, ici on peut traiter les deux dimensions simultanément et non séparément comme ci-dessus: l'élément c_b , qui est différent de 0, a *un complément* c'_b *dans* $\mathbf{C}$: si $c_b = b_1 + b_2$ où $b_1 \in B_1$ et $b_2 \in B_2$, les compléments b'_1 et b'_2 définis (au moins l'un des deux l'est) satisfont : $b'_1 < b_1^{++}$ et $b'_2 < b_2^{++}$, de sorte que $c'_b = b'_1 + b'_2$ (ou bien $c'_b = b'_1$, si $b_2 = 0$, ou bien $c'_b = b'_2$, si $b_1 = 0$) est tel que $a = c_b + c'_b \in A \cap \mathbf{C}$; le noyau relatif d'instabilité $N_{\mathbf{C}}(B \cap \mathbf{C})$ est aussi le noyau d'instabilité absolu de $B_{\mathbf{C}}$ dans $\mathbf{C}$! Le reste du raisonnement s'effectue avec l'élément $z+c'_b = \omega_b+c_b+c'_b = \omega_b+a$ …

En résumé, nous savons maintenant que :

$$\mathbf{N}^2 = \mathbf{\Omega} \oplus \mathbf{C} = A_{\mathbf{\Omega}} \oplus B_{\mathbf{\Omega}} \oplus A_{\mathbf{C}} \oplus B_{\mathbf{C}}, \text{ et que } A = A_{\mathbf{\Omega}} \oplus A_{\mathbf{C}} \text{ et } B = B_{\mathbf{\Omega}} \oplus B_{\mathbf{C}} .$$

On note bien qu'aucun parenthésage n'est nécessaire ici puisque $\boldsymbol{P_0}(\mathbf{N}^2)$ est un prémonoïde. ◄

Conservons toujours les mêmes notations que ci-dessus : le réseau $\mathbf{\Omega}$ engendré par e_1 et e_2 est une partie propre de $\mathbf{N}^2$ et ses *bords* $\mathbf{N}.e_1$ et $\mathbf{N}.e_2$ sont entièrement contenus dans $\mathbf{B}$. Comme la décomposition (A,B) n'est pas triviale, il existe un premier élément de A* (pour l'un ou l'autre des ordres lexicographiques de $\mathbf{\Omega} \approx \mathbf{N}^2$ c'est forcément le même élément !) soit $\omega^* = m.e_1 + n.e_2$ contenu dans $\mathbf{\Omega}$, ; on pose :

$$\mathbf{L} = \{\omega = m'.e_1 + n'.e_2 \in \mathbf{\Omega} \mid m' < m \text{ ou } n' < n\} ;$$

c'est, par définition de ω^*, un sous-ensemble de B. Enfin, on pose :

$$\mathbf{C}^* = [0, m.e_1[\times[0, n.e_2[\cap \mathbf{\Omega}$$

Proposition 3-2.
La « demi-droite » $\mathbf{D} = \mathbf{N}.\omega^*$ est un sous-ensemble propre de $\mathbf{\Omega}$ sur lequel la décomposition (A,B) induit une décomposition directe isomorphe à une décomposition de $\mathbf{N}$, soit $(A_{\mathbf{D}}, B_{\mathbf{D}})$ et la décomposition induite par (A,B) sur $\mathbf{\Omega}$ est donnée par :

$$\mathbf{\Omega} \cap A = A_{\mathbf{D}} \text{ et } \mathbf{\Omega} \cap B = \mathbf{L} \oplus B_{\mathbf{D}} ;$$

pour $\omega = m'.e_1 + n'.e_2 \in \mathbf{\Omega}$, on obtient $\underline{a}(\omega)$ et $\underline{b}(\omega)$ comme suit :
- si $m'/n' \leq m/n$, on effectue la division euclidienne de m' par m : $m' = p.m + r$, $r < m$; l'entier p s'écrit de manière unique $p_a + p_b$, de sorte que $p_a.\omega^* + p_b.\omega^*$ est la décomposition dans $\mathbf{D}$ de $p.\omega^*$ et $\underline{a}(\omega) = p_a.\omega^*$ et $\underline{b}(\omega) = r.e_1 + (n'-p.n).e_2 + p_b.\omega^*$;
- si $m'/n' \geq m/n$, on effectue la division euclidienne de n' par n : $n' = q.n + s$, $s < n$; l'entier q s'écrit de manière unique $q_a + q_b$, de sorte que $q_a.\omega^* + q_b.\omega^*$ est la décomposition dans $\mathbf{D}$ de $q.\omega^*$ et $\underline{a}(\omega) = q_a.\omega^*$ et $\underline{b}(\omega) = s.e_2 + (m'-q.m).e_1 + q_b.\omega^*$.

► On vérifie d'abord que l'on a bien :

$$p_a.\omega^* + r.e_1 + (n'-p.n).e_2 + p_b.\omega^* = p.\omega^* + r.e_1 + (n'-p.n).e_2 =$$
$$p.(m.e_1 + n.e_2) + r.e_1 + (n'-p.n).e_2 = (p.m+r).e_1 + n'.e_2 = m'.e_1 + n'.e_2 = \omega ,$$

pour $m'/n' \leq m/n$, et aussi :

$$q_a.\omega^* + s.e_2 + (m'-q.m).e_1 + q_b.\omega^* = q.\omega^* + s.e_2 + (m'-q.m).e_1 =$$
$$q.(m.e_1 + n.e_2) + s.e_2 + (m'-q.m).e_1 = (q.n+s).e_2 + m'.e_1 = m'.e_1 + n'.e_2 = \omega ,$$

pour $m'/n' \geq m/n$.

Les deux méthodes coïncident si $m'/n' = m/n$, puisque dans ce cas, $p = q$ et $r/s = m/n$, et $\underline{a}(\omega) = p_a.\omega^*$ et $\underline{b}(\omega) = r.e_1 + s.e_2 + p_b.\omega^* \in \mathbf{C}^* \oplus \mathbf{B_D} \subset \mathbf{L} \oplus \mathbf{B_D}$.

Ceci étant, on procède par récurrence portant sur les multiples entiers de ω^* ; par définition, de ω^*, on a : $\mathbf{L} \subset B$, et tout élément z de $\omega^* + \mathbf{L}$ se décompose de façon évidente en $\omega^* + \ell$ sachant que $\omega^* \in A$ et $\ell \in \mathbf{L} \subset B$, conformément à l'énoncé de la proposition.
Supposons établi le résultat pour tous les ensembles $p.\omega^* + \mathbf{L}$, avec $p < q$, à savoir que, pour tout $\ell \in \mathbf{L}$, on a : $\underline{a}(p\omega^* + \ell) = \underline{a}(p\omega^*)$ et $\underline{b}(p\omega^* + \ell) = \underline{b}(p\omega^*) + \ell$, avec $\underline{a}(p\omega^*)$ et $\underline{b}(p\omega^*) \in \mathbf{D}$.

Venons-en à l'ensemble $q.\omega^* + \mathbf{L}$; il y a trois cas à examiner :
- si $q.\omega^* \in A$, alors, on est dans la même situation que ci-dessus (cas $q = 1$) ; tout élément z de $q.\omega^* + \mathbf{L}$ se décompose de façon évidente en $q.\omega^* + \ell$ sachant que $q.\omega^* \in A$ et $\ell \in \mathbf{L} \subset B$;
- si $q.\omega^* \notin A \cup B$, alors $q.\omega^* = a + b$, où $(a,b) \in A^* \times B^*$; par hypothèse de récurrence, l'élément $a = \underline{a}(q.\omega^*)$ est a priori de la forme $p.\omega^*$, avec $0 < p < q$ et b est aussi un multiple de ω^*, puisqu'égal à $(q-p).\omega^*$; tout élément z de $q.\omega^* + \mathbf{L}$, $z = q.\omega^* + \ell$, se décompose alors de façon évidente : en effet, grâce à l'hypothèse de récurrence, l'élément $y = (q-p).\omega^* + \ell$ est dans B, puisque $\underline{b}(y) = \underline{b}((q-p).\omega^* + \ell) = \underline{b}((q-p).\omega^*) + \ell = (q-p).\omega^* + \ell = y$; l'unicité de décomposition achève d'établir que $\underline{a}(q.\omega^* + \ell) = \underline{a}(q.\omega^*)$ et $\underline{b}(q.\omega^* + \ell) = \underline{b}(q.\omega^*) + \ell$.
- si $q.\omega^* \in B$, alors $q.\omega^* + \ell \in B$ pour tout $\ell \in \mathbf{L} \subset B$; en effet, établissons d'abord ceci :
si , pour tout $\ell < \ell_1 \in L$, on a : $q.\omega^* + \ell \notin A$, alors, pour ces mêmes ℓ, on a $q.\omega^* + \ell \in B$; soit en effet $a = \underline{a}(q.\omega^* + \ell)$ et $b = \underline{b}(q.\omega^* + \ell)$; $b \neq 0$ car $q.\omega^* + \ell \notin A$; donc $a < q.\omega^* + \ell$; mais a priori a est de la forme $p.\omega^* + \ell'$ avec $p < q$ ($p > q$ est impossible, $p = q$ est exclu par hypothèse secondaire). L'hypothèse générale de récurrence s'applique alors : $\underline{a}(p.\omega^* + \ell') = \underline{a}(a) = a = p.\omega^* + \ell' = \underline{a}(p.\omega^*) \in \mathbf{N}.\omega^*$; donc $\ell' = 0$ et $a = p.\omega^* \in A$; alors $b = (q-p).\omega^* + \ell$; si $p > 0$, l'hypothèse générale de récurrence s'applique encore: $\underline{b}((q-p).\omega^* + \ell) = (q-p).\omega^* + \ell = \underline{b}((q-p).\omega^*) + \ell$ où $\underline{b}((q-p).\omega^*) \in B$; donc $\underline{b}((q-p).\omega^*) = (q-p).\omega^* \in B$; il y a alors une contradiction, puisque $q.\omega^*$ aurait deux décompositions : la triviale $q.\omega^* = 0 + q.\omega^*$ et l'autre $q.\omega^* = p.\omega^* + (q-p).\omega^*$ ($0 < p < q$). La seule possibilité qui reste est : $p = 0$, donc $a = 0$, donc $q.\omega^* + \ell \in B$.

Maintenant, supposons qu'il y ait dans $q.\omega^* + \mathbf{L}$ des éléments de A **;** soit $q.\omega^* + \ell$ le plus petit d'entre eux (pour un ordre lexicographique arbitraire !) ; on sait que $\ell = m'.e_1 + n'.e_2$, avec $m' < m$ ou $n' < n$ (ou non exclusif) ; effectuons les divisions de m' par m et de n' par n ; il existe donc des entiers s,s',r,r' tels que : $m' = s.m + r$, $n' = s'.n + r'$, avec $r < m$ et $r' < n$; l'un des entiers s ou s' au moins est nul ; distinguons alors deux cas : supposons d'abord que l'on ait : $r = r' = 0$; alors $\ell = m'.e_1 = sme_1$ avec $s > 0$ ou $\ell = n'.e_2 = s'ne_2$ avec $s' > 0$; mettons $\ell = m'.e_1 = sme_1$ avec $s > 0$, pour fixer les idées ; on pose $\ell_1 = (s-1)me_1$ de sorte que $\ell = \ell_1 + me_1$; il y a une contradiction concernant l'unique décomposition de l'élément $q.\omega^* + \ell + n.e_2$:

$$q.\omega^* + \ell + n.e_2 = (q.\omega^* + \ell)_A + (n.e_2)_B = q.\omega^* + \ell_1 + me_1 + n.e_2 = (q.\omega^* + \ell_1)_B + (\omega^*)_A$$

(comme $\ell_1 < \ell$, le résultat du début s'applique et on voit que $q.\omega^* + \ell_1 \in B$) ;
supposons maintenant que r ou r' soit $\neq 0$; alors $\tau = (m-r)e_1 + (n-r')e_2 \in \mathbf{L} \subset B$; de plus, on a : $\ell + \tau = \ell_1 + \omega^*$ où $\ell_1 = sme_1 + s'ne_2 < \ell$; il y a encore une contradiction concernant l'unique décomposition de l'élément $q.\omega^* + \ell + \tau$:

$$q.\omega^* + \ell + \tau \;=\; (q.\omega^* + \ell)_A + (\tau)_B \;=\; (q.\omega^* + \ell_1)_B + (\omega^*)_A$$

(comme $\ell_1 < \ell$, le résultat du début s'applique et on voit que $q.\omega^* + \ell_1 \in B$) .

Finalement, l'existence même d'un élément de A tel que $q.\omega^*+\ell$ conduit à une contradiction : tous les éléments de $q.\omega^* + \mathbf{L}$ sont dans B.

En résumé, nous savons maintenant que :

$$\mathbf{N}^2 \;=\; \mathbf{L} \oplus \mathbf{D} \oplus \mathbf{C} = \mathbf{L} \oplus A_{\mathbf{D}} \oplus B_{\mathbf{D}} \oplus A_{\mathbf{C}} \oplus B_{\mathbf{C}} \text{ où}$$
$$A = A_{\mathbf{\Omega}} \oplus A_{\mathbf{C}} = A_{\mathbf{D}} \oplus A_{\mathbf{C}} \text{ et } B = \mathbf{L} \oplus B_{\mathbf{D}} \oplus B_{\mathbf{C}}.$$

On note bien qu'aucun parenthésage n'est nécessaire ici puisque $\boldsymbol{P_0}(\mathbf{N}^2)$ est un prémonoïde ◄

L'ensemble $\mathbf{N}^2$ est naturellement en bijection avec l'ensemble $\mathbf{L} \times \mathbf{D} \times \mathbf{C}$, mais ce n'est évidemment pas un isomorphisme entre les prémonoïdes $\mathbf{N}^2$ et $\mathbf{L} \times \mathbf{D} \times \mathbf{C}$. On pourrait songer à appliquer les **Théorèmes 1-1** et **1-2** au produit de prémonoïdes $\mathbf{L} \times \mathbf{D} \times \mathbf{C}$, mais toute la « subtilité » des **Propositions 3-1** et **3-2** précédentes consiste à établir justement que ces parties sont propres, et il faudrait en plus calculer quelques noyaux…Notre propos est en fait inverse, et nous allons, seulement maintenant, calculer ces noyaux.

Nous conservons toutes les notations précédentes attachées à la donnée d'une décomposition directe $\partial = (A,B)$ de $\mathbf{N}^2$.

Proposition 3-3. (**Calcul des noyaux d'instabilité d'une décomposition directe de $\mathbf{N}^2$**)
- Si ∂ est triviale, i.e. produit de décompositions directes de **N**, alors on a :

$$N_\partial(A) = N_{\partial 1}(A_1) \times N_{\partial 2}(A_2) \text{ et } N_\partial(B) = N_{\partial 1}(B_1) \times N_{\partial 2}(B_2),$$

c'est-à-dire la trivialité des noyaux d'instabilité (ce résultat a une portée générale).
- Si ∂ est non triviale, mettons avec $|A_1|$ et $|A_2| < \infty$, alors on a :

$$N_\partial(A) = N_{\partial, \mathbf{C}}(A) \oplus N_{\partial, \mathbf{D}}(A),$$
$$N_\partial(B) = N_{\partial, \mathbf{C}}(B) \oplus \mathbf{L} \oplus N_{\partial, \mathbf{D}}(B) = B,$$

à la condition nécessaire et suffisante que $|A_{\mathbf{D}}|$ soit infini .
Par contre, si $|A_{\mathbf{D}}|$ est fini : $N_\partial(B) = N_{\partial, \mathbf{C}}(B) \oplus \mathbf{L}^< \oplus N_{\partial, \mathbf{D}}(B)$ où $\mathbf{L}^<$ est une certaine partie bornée de **L**.

► Supposons d'abord que ∂ est triviale : $A = A_1 \times A_2$ et $B = B_1 \times B_2$, et distinguons 3 cas :

1) $|A_1| = |A_2| = |B_1| = |B_2| = \infty$.
Soit $a = (a_1,a_2) \in A = A_1 \times A_2$ avec $a_1 \neq 0$ et $a_2 \neq 0$; comme $N(A_1) = A_1$ et $N(A_2) = A_2$, il existe $a' = (a'_1, a'_2) \in A = A_1 \times A_2$ tel que les sommes $a_1 + a'_1$ et $a_2 + a'_2$ soient respectivement dans B_1 et B_2 ; ainsi, l'élément a' est tel que $a + a' = (a_1 + a'_1, a_2 + a'_2) \in B = B_1 \times B_2$; si a'_1 et a'_2 sont les *compléments* respectifs de a_1 et de a_2 , alors on peut dire que $a' = (a'_1, a'_2)$ est le *complément* de a. Les autres cas ne présentent aucune difficulté: si $a = 0$, il n'y a pas de complément, mais $0 \in N(A)$ par définition ; si $a = (a_1,0)$ avec $a_1 \neq 0$, le complément de a est défini et vaut $a' = (a'_1,0)$; enfin si $a = (0,a_2)$ avec $a_2 \neq 0$, le complément de a est défini et vaut $a' = (0,a'_2)$. Tout ceci achève de montrer que $N(A) = A_1 \times A_2 = N(A_1) \times N(A_2) = A$.
On établit de même que $N(B) = B_1 \times B_2 = N(B_1) \times N(B_2) = B$.

2) $|A_1|$ et $|A_2| < \infty$ (et évidemment $|B_1| = |B_2| = \infty$).
Le même raisonnement prouve aussitôt que l'on a : $N(A) = A_1 \times A_2 = N(A_1) \times N(A_2) = A$ tandis que l'on trouve seulement $N(B) = (B_1 \cap [0,b_1^{++}[\ ) \times (B_2 \cap [0,b_2^{++}[\ ) = N(B_1) \times N(B_2)$ qui est différent de B.

3) $|A_1|$ et $|B_2| < \infty$ (et évidemment $|B_1| = |A_2| = \infty$).
Le même raisonnement prouve que l'on a : $N(A) = A_1 \times (A_2 \cap [0,b_2^{++}[) = N(A_1) \times N(A_2) \neq A$ tandis que l'on a $N(B) = (B_1 \cap [0,b_1^{++}[\ ) \times B_2 = N(B_1) \times N(B_2) \neq B$.

Dans tous les cas, on a bien:

$$N_\partial(A) = N_{\partial 1}(A_1) \times N_{\partial 2}(A_2) \text{ et } N_\partial(B) = N_{\partial 1}(B_1) \times N_{\partial 2}(B_2),$$

c'est-à-dire la trivialité des noyaux.
Ce résultat est de portée générale.

Supposons maintenant que ∂ est non triviale, et plus précisément encore que l'on a :

$$|A_1| \text{ et } |A_2| < \infty\ ,\ |B_1| = |B_2| = \infty$$

On a vu (**proposition 3-2**) que :

$$A = A_{\mathbf{C}} \oplus A_{\mathbf{D}} = (\mathbf{C} \cap A) \oplus (A \cap \mathbf{D}) \text{ et}$$

$$B = B_{\mathbf{C}} \oplus \mathbf{L} \oplus B_{\mathbf{D}} = (\mathbf{C} \cap B) \oplus \mathbf{L} \oplus (B \cap \mathbf{D}), \text{ avec } A_{\mathbf{D}} \neq \{0\}.$$

On doit distinguer selon que $|B_{\mathbf{D}}|$ est fini ou non.

1) Supposons d'abord $|B_{\mathbf{D}}| = \infty$, de sorte que $N_{\mathbf{D}}(A_{\mathbf{D}}) = A_{\mathbf{D}}$, que $A_{\mathbf{D}}$ soit fini ou non.

Soit $\alpha = \omega_a + c_a \in A$ ($\omega_a \in A_{\mathbf{D}}$ et $c_a \in A_{\mathbf{C}}$) ; supposons d'abord m ou n > 1 ; soit ω'_a le complément de ω_a dans **D** (il existe bien puisque $N_{\mathbf{D}}(A_{\mathbf{D}}) = A_{\mathbf{D}}$) ; ω'_a est donc tel que l'élément $\omega_a + \omega'_a \in B_{\mathbf{D}} = B \cap \mathbf{D}$; soit de même c'_a le *complément* de c_a dans **C** (dès lors que $c_a + c'_a < 2.(b_1^{++}, b_2^{++})$ on peut en parler et donc $c_a + c'_a \in \mathbf{L} \oplus B_{\mathbf{C}}$) ; on a bien :

$$\alpha' = \omega'_a + c'_a \in A \text{ et } \alpha + \alpha' = (\omega_a + \omega'_a) + (c_a + c'_a) \in B_{\mathbf{D}} \oplus \mathbf{L} \oplus B_{\mathbf{C}} \subset B;$$

supposons ensuite que l'on ait m = 1 et n = 1, c'est-à-dire que $\omega^* = (b_1^{++}, b_2^{++}) \in A$; posons $(b_1^{++}, 2.b_2^{++}) = \omega_{12}$, $(2.b_1^{++}, b_2^{++}) = \omega_{21}$; les trois rectangles **C**, $\omega_{21} + \mathbf{C}$ et $\omega_{12} + \mathbf{C}$ sont toujours «dans» **L**, mais le quatrième, $\omega^* + \mathbf{C}$, n'y est plus, puisque $\omega^* \in A$. Pour que la somme $c_a + c'_a$ soit dans ce dernier rectangle $\omega^* + \mathbf{C}$, il faut et il suffit que les indices maxima concernés par les composantes b_1^{++} et b_2^{++} de ω^* soient tous deux des indices maxima absolus ; on a alors :

$$c_a + c'_a = a_1 + a_2 + a'_1 + a'_2 = b_1^{++} + b_2^{++} + \beta_1 + \beta_2 = \omega^* + \beta_1 + \beta_2\ ,$$

où $\beta_1 + \beta_2$ est un certain élément de $B_{\mathbf{C}}$; dans ce cas, $\omega_a + \omega'_a + c_a + c'_a = \omega_a + \omega'_a + \omega^* + \beta_1 + \beta_2$; si $\omega_a = (\sum^*_{i=0} N_{2i} d_{2i})\omega^*$ (la base associée à la décomposition directe de **D** est désignée par (d_i) et les multiplicateurs par m_i) on distingue selon que le premier coefficient non nul est N_0 ou non ; pour $N_0 = 0$, on pose $\omega''_a = \omega'_a + (m_1 - 1)\ \omega^*$ et pour $N_0 \neq 0$, on pose $\omega''_a = \omega'_a - \omega^*$ de sorte que ω''_a est toujours bien défini et élément de A, ainsi que $\alpha'' = \omega''_a + c'_a$; de plus dans le premier cas, on a :

$$\begin{aligned}\alpha + \alpha'' &= \omega_a + c_a + \omega''_a + c'_a = \omega_a + \omega''_a + c_a + c'_a \\ &= \omega_a + \omega'_a + (m_1\text{-}1)\omega^* + \omega^* + \beta_1 + \beta_2 \\ &= \omega_a + \omega'_a + d_1.\omega^* + \beta_1 + \beta_2 \text{ qui est bien dans B,}\end{aligned}$$

et dans le deuxième cas, on a :

$$\begin{aligned}\alpha + \alpha'' &= \omega_a + c_a + \omega''_a + c'_a = \omega_a + \omega''_a + c_a + c'_a \\ &= \omega_a + \omega'_a - \omega^* + \omega^* + \beta_1 + \beta_2 \\ &= \omega_a + \omega'_a + \beta_1 + \beta_2 \text{ , qui est encore dans B.}\end{aligned}$$

On trouve donc que $N_\partial(A) = A = A_C \oplus A_D = N_{\partial, C}(A) \oplus N_{\partial, D}(A)$.

2) Supposons maintenant $|B_D| < \infty$, de sorte que $N_D(A_D) = A_D \cap [0,\omega^+[$, où ω^+ est le plus grand élément de B_D, que A_D soit fini ou non. Tout ce qui a été dit précédemment reste vrai à la condition de prendre $\omega_a \in A_D \cap [0,\omega^+[$ (i.e. $\omega_a < \omega^+$) . On trouve donc encore ceci :

$$N_\partial(A) = A = A_C \oplus (A_D \cap [0,\omega^+[) = N_{\partial, C}(A) \oplus N_{\partial, D}(A)$$

Dans tous les cas, on a bien : $N_\partial(A) = N_{\partial, C}(A) \oplus N_{\partial, D}(A)$.

Reste à établir que :

$$N_\partial(B) = N_{\partial, C}(B) \oplus \mathbf{L} \oplus N_{\partial, D}(B) = B,$$

à la condition nécessaire et suffisante que $|A_D|$ soit infini,
et que:

$$N_\partial(B) = N_{\partial, C}(B) \oplus \mathbf{L}^< \oplus N_{\partial, D}(B),$$

où $\mathbf{L}^<$ est une certaine partie bornée de $\mathbf{L}$,
si $|A_D|$ est fini.

Soit donc $\omega_b + c_b + \lambda_b$ un élément de B ; supposons qu'il existe un autre élément de B, soit $\omega'_b + c'_b + \lambda'_b$ tel que la somme $\omega_b + c_b + \lambda_b + \omega'_b + c'_b + \lambda'_b$ soit un élément de A, donc de la forme $\omega_a + c_a$; observons d'abord que la somme $c_b + c'_b$ ne peut pas admettre de « retenue au-delà de $b_1^{++} + b_2^{++}$ » ; elle ne peut dépasser $b_1^{++} + b_2^{++}$; elle est donc nécessairement élément de $\mathbf{C}$ et l'unicité de décomposition liée à $\mathbf{N}^2 = \mathbf{\Omega} \oplus \mathbf{C}$ permet de conclure que nécessairement : $c_a = c_b + c'_b$ et $\omega_a = \omega_b + \lambda_b + \omega'_b + \lambda'_b$; on voit donc déjà qu'on peut considérer que c'_b est le *complément* de c_b dans $\mathbf{C}$, si $c_b \neq 0$.

Ensuite, l'élément $\lambda_b + \lambda'_b$ doit être dans $\mathbf{D} = \omega^*\mathbf{N}$ puisque il est égal à $\omega_a - \omega_b - \omega'_b$; posons $\lambda_b = (m_0.b_1^{++}, n_0.b_2^{++})$ et $\lambda'_b = (m'.b_1^{++}, n'.b_2^{++})$; quitte à échanger les rôles de m et n (ou de A_1 et de A_2), on peut supposer que l'on a : $m_0/n_0 < m/n$ avec $m_0 < m$ (et donc $n' < n$) ; on effectue alors les deux divisions euclidiennes qui s'imposent : $m' = q'.m + r$, avec $r < m$, et $n_0 = q.n + s$, avec $s < n$; comme $m_0 + m'$ doit être un multiple de m, on doit avoir $r + m_0 = 0$ ou m ; de même $n_0 + n'$ doit être un multiple de n, on doit donc avoir $s + n' = 0$ ou n ; de plus, le multiplicateur est le même !

- Supposons d'abord $m_0 \neq 0$; alors $r + m_0 = m$, donc r est connu : $r = m - m_0$; on effectue alors la division de n_0 par n : et $n_0 = q.n + s$, avec $s < n$;

- supposons encore $s \neq 0$; alors $n' = n - s$; on a: $m_0 + m' = m_0 + q'.m + r = m_0 + q'.m + m - m_0 = (q'+1).m$ et $n_0 + n' = q.n + s + n - s = (q+1).n$; donc $q' = q = (n_0-s) / n$, d'où la seule solution possible pour que $\lambda_b + \lambda'_b$ soit dans **D** : $m' = (n_0-s).m / n + m - m_0 = (q+1).m - m_0$; et $n' = n - s =$ et l'on a : $\lambda_b + \lambda'_b = [(n_0-s)/n + 1].\omega^* = (q+1).\omega^*$.

- supposons maintenant $s = 0$; alors $n' = 0$; on a: $m_0 + m' = m_0 + q'.m + r = m_0 + q'.m + m - m_0 = (q'+1).m$ et $n_0 + n' = n_0 = q.n$; donc $q' = q-1 = n_0/n - 1$; alors $m_0 + m' = q.m$ et $n_0 + n' = q.n$, d'où la seule solution possible pour que $\lambda_b + \lambda'_b$ soit dans **D**: $m' = q.m - m_0$ et $n' = 0$; de sorte que l'on a : $\lambda_b + \lambda'_b = [(n_0-s)/n + 1].\omega^* = q.\omega^*$;

- Supposons ensuite $m_0 = 0$; alors $r = 0$; on a toujours : $n_0 = q.n + s$, avec $s < n$;

- supposons encore $s \neq 0$; alors $n' = n - s$; on a : $m_0 + m' = q'.m + r = q'.m$ et $n_0 + n' = q.n + s + n - s = (q+1).n$; donc $q' = q+1 = (n_0-s)/n + 1$, d'où la seule solution possible pour que $\lambda_b + \lambda'_b$ soit dans **D** : $m' = (n_0-s).m / n + m = (q+1).m$; et $n' = n - s$; de sorte que l'on a : $\lambda_b + \lambda'_b = [(n_0-s)/n + 1].\omega^* = (q+1).\omega^*$;

- supposons enfin $s = 0$; alors $n' = 0$; on a : $m_0 + m' = m' = q'.m$ et $n_0 + n' = n_0 = q.n$; donc $q' = q = n_0/n$, d'où la seule solution possible pour que $\lambda_b + \lambda'_b$ soit dans **D** : $m' = n_0.m / n = (q+1).m$; et $n' = n - s = n$; de sorte que l'on a : $\lambda_b + \lambda'_b = [(n_0-s)/n + 1].\omega^* = (q+1).\omega^*$.

En conclusion, on effectue la division de n_0 par n : $n_0 = q.n + s$, avec $s < n$ et on distingue selon que $m_0 \neq 0$ ou non :

- $m_0 = 0$: multiplicateur commun : $q+1$
- $m_0 \neq 0$: multiplicateur commun : $q+1$ si $s \neq 0$, q si $s = 0$.

Poursuivons et posons: $\omega_b = \beta.\omega^*$; $\omega'_b = \beta'.\omega^*$ et $\lambda_b + \lambda'_b = p.\omega^*$; $\omega_a = \alpha.\omega^*$; la décomposition $(A_{\mathbf{D}}, B_{\mathbf{D}})$ de $\mathbf{D} = \omega^*.\mathbf{N}$ est isomorphe à une décomposition de **N,** à laquelle on l'identifie à partir de maintenant ; rappelons que (d_i) désigne la base généralisée (finie ou non) associée, que $d_0 = 1 \in A_{\mathbf{D}}$; on doit avoir : $\alpha = \beta + \beta' + p$; le seul facteur sur lequel on puisse jouer est le choix de β' pour que α soit dans A ; à cet effet, il suffit d'appliquer la **proposition 2-5** à $n = \beta + p$; si ce nombre est majoré par un élément a de $A_{\mathbf{D}}$, il existe un élément β' de $B_{\mathbf{D}}$ tel que $n + \beta' = \beta + p + \beta'$ soit dans $A_{\mathbf{D}}$.

La seule condition qu'on ait rencontrée est cette majoration de $n = \beta + p$ par $A_{\mathbf{D}}$; si $A_{\mathbf{D}}$ est infini, la condition est automatiquement satisfaite, et on peut affirmer que $N_\partial(B) = B$. Si au contraire $A_{\mathbf{D}}$ est fini, il faut et il suffit que $n = \beta + p$ soit majoré par :

$$\sup(A_{\mathbf{D}}) = \alpha_{\mathbf{D}}^{+} = \sum_{i=0}^{k} (m_{2i+1} - 1) d_{2i} = \sum_{i=0}^{k} d_{2i+1} - \sum_{i=0}^{k} d_{2i} ;$$

et dans ce cas, on sait que l'élément $n = \beta + p$ est lui-même majoré par $\alpha_{\mathbf{D}}^{+}$ (remarque 3, suivant la **proposition 2-5**)

Reste à traduire techniquement l'inégalité $\beta + p \leq \alpha_{\mathbf{D}}^{+}$.

La procédure à suivre est résumée ici :
- m et n sont donnés par $\omega^* = (m.b_1^{++}, n.b_2^{++})$;
- m_0 et n_0 sont donnés par $\lambda_b = (m_0.b_1^{++}, n_0.b_2^{++})$ avec $m_0/n_0 < m/n$, pour l'exemple ;
- q et s sont calculés par division euclidienne : $n_0 = q.n + s$, $s < n$;

- si $m_0 \neq 0$ et $s = 0$, $p = q$; autrement $p = q+1$;
- β est donné par $\omega_b = \beta.\omega^* = (\beta.m.b_1^{++}, \beta.n.b_2^{++})$;
- $n = \beta + p$; le bornage requis est : $n \leq \alpha_D^+$;
- si cette condition est remplie, β' est calculé par la proposition 5.

Il est clair que la seule condition qui ressort de cette analyse est liée à l'existence même de $\alpha_{\mathbf{D}}^+$, c'est-à-dire au fait que $A_{\mathbf{D}}$ soit fini, et qu'il s'agit d'une condition de bornage : le noyau est *nécessairement* contenu dans $B \cap \mathbf{C}^{**}$ en désignant par $\mathbf{C}^{**}$ le « plus petit » rectangle canonique qui contient tous les éléments de A ◄

Proposition 3-4 (**Structure des facteurs directs de $\mathbf{N}^2$**)
- Si ∂ est triviale, A et B sont des prémonoïdes produits, $A \approx A_1 \times A_2$ et $B \approx B_1 \times B_2$.
- Si ∂ est non triviale, mettons avec $|A_1|$ et $|A_2| < \infty$; on trouve :
  - si $\omega^* \neq e_1 + e_2$, ou si $\omega^* = e_1 + e_2$ mais A_1 ou A_2 est réduit à 0, le facteur A est un sous-prémonoïde de $\mathbf{N}^2$ isomorphe à $A_{\mathbf{C}} \times A_{\mathbf{D}}$;
  - si $\omega^* = e_1 + e_2$ et A_1 et A_2 non réduits à 0, alors A n'est pas un sous-prémonoïde de $\mathbf{N}^2$ et le système additif $\mathbf{A} = (A, +_b)$ n'est pas associatif
  - pour que B soit un sous-prémonoïde de $\mathbf{N}^2$, il faut et il suffit que $B \cap \mathbf{N}.\omega^* = \{0\}$.

► Supposons d'abord $\omega^* \neq e_1 + e_2$; pour que la somme de deux éléments de A soit encore dans A, il est nécessaire que leurs composantes situées dans **C** ait encore une somme dans **C**; en effet, soit $x = m.\omega^* + c$ et $y = n.\omega^* + c'$, où c et $c' \in \mathbf{C}$, deux éléments de A tels que $x+y$ soit encore élément de A, mettons $x+y = p.\omega^* + d$ avec $d \in \mathbf{C}$; l'élément $c + c' - d$ est donc dans $2.\mathbf{C}$ (ou son opposé $-2.\mathbf{C}$) et dans $\mathbf{D} = \mathbf{N}.\omega^*$ (ou son opposé $-\mathbf{D}$) ; mais $\mathbf{D} \cap 2.\mathbf{C} = \{0\}$, car $\omega^* \neq e_1 + e_2$; on a donc : $c+c' = d$ et $m+n = p$; ceci prouve que A est isomorphe au produit des prémonoïdes $A_{\mathbf{C}}$ et $A_{\mathbf{D}}$; c'est donc un prémonoïde.

Supposons maintenant $\omega^* = e_1+e_2$ et, par exemple, $A_2 = \{0\}$; on reprend les notations précédentes pour x, y, x+y ; posons $d = d_1 + d_2$, où $d_1 \in E_1$ et $d_2 \in E_2$; comme $x+y \in A$, on voit que $d = d_1$ et $d_2 = 0$; en projetant sur E_2, il vient $0 = (m+n-p).e_2$, donc nécessairement $m+n-p = 0$; ici encore A est isomorphe au produit des prémonoïdes $A_{\mathbf{C}}$ et $A_{\mathbf{D}}$; c'est donc un prémonoïde ($A_{\mathbf{C}} = A_1 \times \{0\}$).

Supposons enfin $\omega^* = e_1+e_2$, $A_1 \neq \{0\}$ et $A_2 \neq \{0\}$; l'élément e_1 est de la forme $m.b_k$ où b_k est élément de A_1 et $m > 1$; de même $e_2 = n.b'_{k'}$ où $b'_{k'}$ est élément de A_2 et $n > 1$; décomposons m (resp. n) en somme de deux entiers non nuls, m' et m" (resp. n' et n") ; les éléments suivants sont dans A :

$a' = m'.b_k$; $a'' = n''.b'_{k'}$; $a = m''.b_k + n'.b'_{k'}$; $a' + a'' = a_1 = m'.b_k + n''.b'_{k'}$

et $a + (a' + a'') = m''.b_k + n'.b'_{k'} + m'.b_k + n''.b'_{k'} = m.b_k + n.b'_{k'} = e_1+e_2 = \omega^*$

tandis que ni $a + a' = e_1 + n'.b'_{k'}$, ni $a + a'' = e_2 + m''.b_k$ ne sont éléments de A ; ainsi A ne saurait être un prémonoïde. On voit aussi que : $a +_b (a' +_b a'') = \omega^*$, $(a +_b a') +_b a'' = 0$, et aussi : $a_1 +_b (a +_b a') = a'$, $(a_1 +_b a) +_b a' = 0$ et $a_1 +_b (a +_b a'') = a''$, $(a_1 +_b a) +_b a'' = 0$, ce qui montre que $\mathbf{A} = (A, +_b)$ est loin d'être associatif.

Venons-en au cas de B.
Supposons d'abord $B \cap \mathbf{D} = \{0\}$; soient $x = \ell + c$ et $y = \ell' + c'$, où $\ell, \ell' \in \mathbf{L}$ et $c, c' \in \mathbf{C} \cap B$, deux éléments de B, tels que la somme $x+y$ soit encore élément de B ; l'élément $c+c'$ est

encore dans **C** (cf. la structure des décompositions de **N**) ; alors $\ell+\ell' \in$ **L**, et B hérite donc de la structure de prémonoïde produit des prémonoïdes **C** $\cap$B et **L**.
Par contre, si B$\cap$**D** $\neq \{0\}$, il existe au moins un élément de B de la forme $n.\omega^*$ (avec $n \geq 2$) ; on sait que $\omega^* = \lambda.e_1 + \mu.e_2$, avec λ et $\mu > 0$; les éléments suivants sont dans B :

$b' = \lambda.e_1$, $b'' = (n-1)\lambda.e_1$, $b = n\mu.e_2$, $b' + b'' = n\lambda.e_1$ et $b + (b' + b'') = n.\omega^*$,

tandis que ni $b + b' = n\mu.e_2 + \lambda.e_1$ ni $b + b'' = n\mu.e_2 + (n-1)\lambda.e_1$ ne sont éléments de B ; en effet, aucun des éléments suivants n'est nul :

$\underline{a}(b + b') = \omega^*$, $\underline{b}(b + b') = (n-1)\mu.e_2$, $\underline{a}(b + b'') = \underline{a}((n-1)\omega^*)$, $\underline{b}(b + b'') = \underline{b}((n-1)\omega^*) + \mu.e_2$

Bien évidemment , **B** = $(B, +_a)$ est loin d'être associatif, dans ce cas ◄

4. Généralisation du résultat précédent à certaines décompositions de $\mathbf{N}^k$.

Tout ce qui a été établi jusqu'ici pour $\mathbf{N}^2$ est applicable pratiquement sans modification au cas de *certaines* décompositions additives directes des $\mathbf{N}^k$ avec $k \geq 2$. Nous allons cependant reprendre les *énoncés précis* concernant cette généralisation, avec les *conditions précises* dans lesquelles ils s'appliquent.

Soit donc (A,B) une décomposition directe de $\mathbf{N}^k$; on désigne par (A_p , B_p) la décomposition « induite » sur le $p^{ième}$ facteur de la puissance $\mathbf{N}^k$, qu'on identifie à une décomposition directe de $\mathbf{N}$; on reprend les notations génériques des décompositions directes de $\mathbf{N}$:

- si A_p est fini, $\sup(A_p) = \alpha_p^+$, $\sup(B_p \cap [0, \alpha_p^+]) = \beta_p^+$ et $\inf(B_p \backslash A_p) = b_p^{++}$; rappelons qu'on a : $\beta_p^+ \leq \alpha_p^+ < b_p^{++}$ ($\beta_p^+ = \alpha_p^+$ seulement si $A_p = \{0\}$ et alors $\alpha_p^+ = \beta_p^+ = 0 < b_p^{++} = 1$)

- si B_p est fini, $\sup(B_p) = \beta_p^+$, $\sup(A_p \cap [0, \beta_p^+]) = \alpha_p^+$ et $\inf(A_p \backslash B_p) = b_p^{++}$; rappelons qu'on a : $\alpha_p^+ \leq \beta_p^+ < b_p^{++}$ ($\alpha_p^+ = \beta_p^+$ seulement si $B_p = \{0\}$ et alors, $\beta_p^+ = \alpha_p^+ = 0 < b_p^{++} = 1$)

On suppose que, pour tout p de 1 à k, on a : $|A_p| < \infty$ ou $|B_p| < \infty$

Soit $\mathbf{\Omega}$ le réseau engendré par $e_1 = (b_1^{++}, 0,0,..)$, $e_2 = (0,0, b_2^{++},0,..)$, …, $e_k = (0,0,\ldots,b_k^{++})$.
Soit $\mathbf{C} = [0, b_1^{++}[\times [0, b_2^{++}[\ldots \times [0, b_k^{++}[$.
On désigne toujours par $\underline{a}$ et $\underline{b}$ les applications qui fournissent les facteurs de décomposition pour tout x, on a : $x = \underline{a}(x)+\underline{b}(x)$ avec $\underline{a}(x) \in A$ et $\underline{b}(x) \in B$.

Proposition 4-1 (**extension de la proposition 3-1**)
Si pour tout p de 1 à k, on a : $|A_p| < \infty$ ou $|B_p| < \infty$, alors ($\mathbf{\Omega}$, $\mathbf{C}$) est une décomposition directe de $\mathbf{N}^k$ en parties propres relatives à la décomposition (A,B) donnée; c'est dire que pour tout $z \in \mathbf{N}^k$, $z = \omega+c$ avec $(\omega,c) \in \mathbf{\Omega} \times \mathbf{C}$ on a :

$$\underline{a}(z) = \underline{a}(\omega) + \underline{a}(c) \text{ et } \underline{b}(z) = \underline{b}(\omega) + \underline{b}(c), \text{ avec } \underline{a}(\omega) \text{ et } \underline{b}(\omega) \in \mathbf{\Omega}.$$

► La décomposition unique de $z = \omega+c$ avec $(\omega,c) \in \mathbf{\Omega} \times \mathbf{C}$ est classique.
Si $z \in \mathbf{C}$, $\underline{a}(z)$ et $\underline{b}(z)$ sont aussi éléments de $\mathbf{C}$; de plus , la décomposition induite par (A,B) sur $\mathbf{C}$ est *complètement* triviale, dans le sens que $A \cap \mathbf{C} = \prod_{1 \leq p \leq k} ([0, b_p^{++}[\cap A_p)$, mais aussi

$B \cap \mathbf{C} = \prod_{1 \leq p \leq k} ([0, b_p^{++}[\cap B_p)$: une simple récurrence et l'application du théorème de décomposition triviale dans sa version relative permettent d'établir ce fait.

On procède maintenant par récurrence transfinie (avec l'ordre lexicographique dans $\mathbf{N}^k$). Supposons que, pour tout $z' < z$, on ait : $\underline{a}(z') = \underline{a}(\omega') + \underline{a}(c')$ et $\underline{b}(z') = \underline{b}(\omega') + \underline{b}(c')$, où (ω',c') est l'unique élément de $\mathbf{\Omega} \times \mathbf{C}$ tel que $z' = \omega'+c'$, avec $\underline{a}(\omega')$ et $\underline{b}(\omega') \in \mathbf{\Omega}$.
Remarquons que $\underline{a}(z') = \underline{a}(\omega') + \underline{a}(c')$ et $\underline{b}(z') = \underline{b}(\omega') + \underline{b}(c')$ sont les décompositions respectives de $\underline{a}(z')$ et $\underline{b}(z')$ selon la décomposition directe $\mathbf{N}^k = \mathbf{\Omega} \oplus \mathbf{C}$. Venons-en alors à z et distinguons deux cas, selon que $z \in \mathbf{\Omega}$ ou que $z \notin \mathbf{\Omega}$:
- $z \in \mathbf{\Omega}$.

Si, en plus, $z \in A \cup B$, il n'y a rien à démontrer: soit $\underline{a}(z) = z$ et $\underline{b}(z) = 0$, si $z \in A$, soit $\underline{a}(z) = 0$ et $\underline{b}(z) = z$, si $z \in B$.

Supposons donc maintenant que $z \notin A \cup B$; $z = \underline{a}(z)+\underline{b}(z)$ avec $\underline{a}(z) < z$ et $\underline{b}(z) < z$; par hypothèse de récurrence, on peut écrire : $\underline{a}(z) = \omega_a + c_a$ et aussi $\underline{b}(z) = \omega_b + c_b$ où l'on a : $(\omega_a, c_a) \in (\mathbf{\Omega} \times \mathbf{C}) \cap A$ et $(\omega_b, c_b) \in (\mathbf{\Omega} \times \mathbf{C}) \cap B$; la somme c_a+c_b est nécessairement élément de **C**, puisque $(c_a, c_b) \in (A \times B) \cap \mathbf{C}$ et que la décomposition induite sur **C** est justement triviale ; mais $\omega_a+\omega_b \in \mathbf{\Omega}$, l'unicité de décomposition de z selon ($\mathbf{\Omega}$, **C**) entraîne alors que $z = \omega_a + \omega_b$ ($c_a+ c_b =0$ et donc $c_a = c_b = 0$); ainsi $\underline{a}(z) = \omega_a$ et $\underline{b}(z) = \omega_b \in \mathbf{\Omega}$.

- $z \notin \mathbf{\Omega}$.

Si en plus, $z \notin A \cup B$, alors on est pratiquement dans la même situation que précédemment : $z = \underline{a}(z)+\underline{b}(z)$ avec $\underline{a}(z) < z$ et $\underline{b}(z) < z$; par hypothèse de récurrence, on a: $\underline{a}(z) = \omega_a+c_a$ et aussi $\underline{b}(z) = \omega_b+c_b$ où $(\omega_a, c_a) \in (\mathbf{\Omega} \times \mathbf{C}) \cap A$ et $(\omega_b, c_b) \in (\mathbf{\Omega} \times \mathbf{C}) \cap B$; la somme $c_a+ c_b$ est nécessairement élément de **C**, puisque $(c_a, c_b) \in (A \times B) \cap \mathbf{C}$ et que la décomposition induite sur **C** est triviale ; si $z = \omega + c$, l'unicité de décomposition de z selon ($\mathbf{\Omega}$, **C**) entraîne alors que $\omega = \omega_a + \omega_b$ et $c = c_a+ c_b$; clairement on a: $\underline{a}(c) = c_a$, $\underline{b}(c) = c_b$, $\underline{a}(\omega) = \omega_a$ et $\underline{b}(\omega) = \omega_b$ de sorte que: $\underline{a}(z) = \underline{a}(\omega) + \underline{a}(c)$ et $\underline{b}(z) = \underline{b}(\omega) + \underline{b}(c)$.

Supposons donc enfin que $z \in A \cup B$; soit $z = \omega + c$, $c \neq 0$ ($z \notin \mathbf{\Omega}$), la décomposition de z suivant $\mathbf{\Omega} \times \mathbf{C}$; alors $\omega < z$ s'écrit aussi $\omega_a + \omega_b$ et $c = c_a+ c_b$ d'où $z = \omega_a+c_a+\omega_b+c_b$; supposons $\omega_b + c_b \neq 0$; alors $\omega_a + c_a < z$ et du coup, en utilisant l'hypothèse de récurrence, $\underline{a}(\omega_a + c_a) = \underline{a}(\omega_a) + \underline{a}(c_a) = \omega_a + c_a$, ce qui prouve que $\omega_a + c_a \in A$; supposons aussi $\omega_a + c_a \neq 0$; alors $\omega_b + c_b < z$ et du coup, en utilisant l'hypothèse de récurrence, $\underline{b}(\omega_b + c_b) = \underline{b}(\omega_b) + \underline{b}(c_b) = \omega_b+c_b$, ce qui prouve que $\omega_b+c_b \in B$; comme $z \in A \cup B$, il n'est pas possible d'avoir *en même temps* $\omega_b + c_b \neq 0$ et $\omega_a + c_a \neq 0$; on a donc soit $z = \omega_a + c_a$, soit $z = \omega_b + c_b$; Reste à voir que, dans le premier cas on a bien $z \in A$, et dans le second cas, on a bien $z \in B$.

On procède alors par l'absurde :

- supposons d'abord que $z = \omega_a + c_a$ et $z \in B$; on sait que $c_a = (a_p)_{1 \leq p \leq k}$, $a_p \in A_p$, est différent de 0 ; il existe donc un indice p tel que $a_p \neq 0$; son complément a'_p est bien défini et tel que $a_p + a'_p = b_p \in B_p \subset B$; définissons l'élément $a_p^{\S}$ (resp. $a'^{\S}_p$) comme ayant pour seule composante non nulle la composante $p^{\text{ième}}$, justement égale à a_p (resp. a'_p) ; alors l'élément $z + a'^{\S}_p$ aurait deux décompositions à savoir : $(a'^{\S}_p , z) \in A_p \times B$, mais encore $(\omega_a+ c_{a,p} , b_p) \in A \times B_p$ où $c_{a,p} = c_a - a_p^{\S}$; en effet, on a :

$$\omega_a + c_{a,p} + b_p = \omega_a + c_{a,p} + a_p^{\S} + a'^{\S}_p = \omega_a + c_a + a'^{\S}_p = z + a'^{\S}_p ,$$

et le fait que a_p soit différent de 0 entraîne que $\omega_a+ c_{a,p} < z$ est bien un élément de A, par l'hypothèse de récurrence ; notons aussi que ces décompositions sont bien distinctes ! ; il y a donc une contradiction et $z = \omega_a + c_a \in A$ et $\underline{a}(z) = z = \underline{a}(\omega + c) = \omega_a + c_a = \underline{a}(\omega) + \underline{a}(c)$;

- supposons enfin $z = \omega_b + c_b$; on montre comme ci-dessus que nécessairement $z \in B$ et $\underline{b}(z) = z = \underline{b}(\omega + c) = \omega_b + c_b = \underline{b}(\omega) + \underline{b}(c)$.

En résumé, nous avons établi que :
$\mathbf{N}^k = \mathbf{\Omega} \oplus \mathbf{C} = A_{\mathbf{\Omega}} \oplus B_{\mathbf{\Omega}} \oplus A_{\mathbf{C}} \oplus B_{\mathbf{C}}$, et que $A = A_{\mathbf{\Omega}} \oplus A_{\mathbf{C}}$ et $B = B_{\mathbf{\Omega}} \oplus B_{\mathbf{C}}$ ◄

Remarque.
Certains des entiers b_p^{++} peuvent fort bien être égaux à 1 ; dans ce cas le « segment » correspondant $[0, b_p^{++}[$ est réduit à $\{0\}$. On dira aussi que **C** est l'*intérieur* de l'hypercube $\overline{\mathbf{C}} = \prod_{1 \leq p \leq k} ([0, b_p^{++}]$; on parlera aussi de la *dimension* de **C** : c'est le nombre d'entiers $p \leq k$ tels que l'on ait : $b_p^{++} > 1$; elle peut être a priori tout nombre compris entre 0 et k ; quelle qu'elle

soit, le théorème précédent est valable (si elle est nulle, des cas évoqués dans la démonstration ne se présentent pas, tout simplement…)
La **proposition 3-2**, qui complète la **proposition 3-1** et conduit à la description complète des décompositions non triviales de $\mathbf{N}^2$, ne se laisse pas généraliser d'aussi facile façon que la **proposition 3-1** en la **proposition 4-1**.

Nous terminerons cette partie en fournissant quelques éléments sur les décompositions additives en petites dimensions (3, 4 et 5).

4) bis. Exploration en petites dimensions (3, 4 et 5).

Classification des décompositions non triviales de $\mathbf{N}^3$.
En principe, cette section se veut seulement pédagogique, puisqu'une lecture du cas général est théoriquement possible. Cependant, étant passé par là, je reste persuadé que je n'aurais pas mis au point le cas général sans le passage par la dimension 3.
Pour mieux marquer le coup, nous identifions $\mathbf{N}^3$ à un sous-ensemble de $\mathbf{R}^3$, espace auquel on empruntera les notations les plus usuelles, Ox, Oy, Oz, …par exemple et le vocabulaire (point, droite, plan, etc….)

On suppose que les facteurs de A sur les axes, soient A_x, A_y, A_z , sont finis. On suppose aussi que la décomposition induite dans le plan Oyz n'est pas triviale. Il y a donc dans ce plan des éléments de A dont les deux composantes sont non nulles et éléments de B. Il y en a un « minimum » (au sens d'un ordre lexicographique) , mettons $\alpha = \beta_y + \beta_z$, avec β_y , $\beta_z \neq 0$, $\beta_y \in B_y$ et $\beta_z \in B_z$.

La **proposition 4-1** s'applique : on est ramené à la décomposition de $\mathbf{\Omega}$, réseau qui est naturellement isomorphe à $\mathbf{N}^3$ et on peut donc supposer en plus que A_x, A_y, A_z sont réduits à $\{0\}$, c'est-à-dire aussi que $\mathbf{N}.e_x = B_x$, $\mathbf{N}.e_y = B_y$ et $\mathbf{N}.e_z = B_z$, où e_x, e_y et e_z forment la base canonique de $\mathbf{N}^3$

Proposition 4-1-1.
Sous les hypothèses précédentes, tous les éléments de Oxy et Oyz sont dans B.

► Les axes Oy et Oz jouent des rôles symétriques par rapport à Ox ; il suffit donc d'établir que Oxy est contenu dans B.

On raisonne par l'absurde. Soit $\alpha_0 = \beta'_x + \beta'_y$ le plus petit élément de A dans le plan Oxy (supposé exister) ; il est tel que β'_x , $\beta'_y \neq 0$, $\beta'_x \in B_x$ et $\beta'_y \in B_y$. On pose alors:

$$\beta'_y = \lambda'.b_y^{++} \quad \text{et} \quad \beta_y = \lambda.b_y^{++}.$$

Si $\lambda' \geq \lambda$, on examine l'élément $\alpha_0 + \beta_z$ qui aurait deux décompositions :

$$\alpha_0 + \beta_z = \beta'_x + \beta'_y + \beta_z = \beta'_x + \beta'_y - \beta_y + \beta_y + \beta_z = \alpha + \beta'_x + (\lambda'-\lambda).b_y^{++} ;$$

ce dernier élément $\beta'_x + (\lambda'-\lambda).b_y^{++}$ est strictement plus petit que $\alpha_0 = \beta'_x + \beta'_y$ car $\lambda \neq 0$ et est donc dans $B_{xy} \subset B$; c'est un élément de B.

Si $\lambda' < \lambda$, on examine l'élément $\alpha + \beta'_x$ qui aurait deux décompositions :

$$\alpha + \beta'_x = \beta_y + \beta_z + \beta'_x = \beta'_y + \beta_z + \beta'_x + \beta_y - \beta'_y = \alpha_0 + (\lambda-\lambda').b_y^{++} + \beta_z ;$$

mais l'élément $(\lambda-\lambda').b_y^{++} + \beta_z$ est strictement plus petit que $\alpha = \beta_y + \beta_z$ car $\lambda' \neq 0$ et à ce titre, c'est un élément de B.

Dans les deux cas, on disposerait d'un élément ayant deux décompositions. C'est une contradiction ◄

Supposons toujours A_x, A_y et A_z finis, et en fait réduits à {0}, après une éventuelle réduction (application de la **proposition 4-1** et identification à $\mathbf{N}^3$ du réseau $\mathbf{\Omega}$).
Supposons encore la décomposition induite sur Oyz non triviale, avec « droite exceptionnelle » $\mathbf{D}_{yz} = \mathbf{D} = \mathbf{N}.\alpha^*$, où $\alpha^* = m.e_y + n.e_z \in A$. On sait que cette dernière est propre. Si on suppose que $A_{\mathbf{D}}$ est infini, le théorème de décomposition directe triviale s'applique : la décomposition (A,B) de $\mathbf{N}^3$ donnée est produit des décompositions induites sur Ox et Oyz respectivement, cette dernière étant non triviale. On la dira *semi-triviale*.
On se place donc justement dans le cas où les conditions suffisantes d'application du **théorème 1-1** ne s'appliquent pas, c'est-à-dire dans le cas où $A_{\mathbf{D}}$ est fini.

Proposition 4-1-2.
Avec ces hypothèses (A_x, A_y , A_z et $A_{\mathbf{D}}$ finis) , si la décomposition directe de $\mathbf{N}^3$ considérée n'est pas *semi-triviale*, alors le plan $\mathbf{P} = Ox \oplus \mathbf{D}_{yz}$ est une partie propre de $\mathbf{N}^3$ sur laquelle (A,B) induit une décomposition (A_0, B_0) isomorphe à une décomposition non triviale de $\mathbf{N}^2$.

► Réduction.
La décomposition du « cube » $\mathbf{C} = [0,1[\times [0,m[\times [0,n[$ est triviale dans ce sens que l'on a : $A_{\mathbf{C}} = \{0\}\times\{0\}\times\{0\}$ et $B_{\mathbf{C}} = \{0\}\times [0,m[\times [0,n[$. Le réseau $\mathbf{\Omega}$ engendré par $e_x = (1, 0, 0)$, $e_y = (0, m, 0)$ et $e_z = (0, 0, n)$ est une partie propre pour la décomposition (A,B) : en effet, la **proposition 4-1** s'applique, dans un cas trivial puisque **C** est entièrement contenu dans B (notons aussi que $\dim(\mathbf{C}) \leq 2$, plus précisément : $\dim(\mathbf{C}) = 2$ si m et $n > 1$; $\dim(\mathbf{C}) = 1$ si m ou $n = 1$, mais pas m et n ; enfin, $\dim(\mathbf{C}) = 0$ si $m = n = 1$).

Pour alléger les notations, on identifie $\mathbf{\Omega}$ à $\mathbf{N}^3$, on note encore (A,B) la décomposition de $\mathbf{N}^3$ correspondant à $(A_{\mathbf{\Omega}},B_{\mathbf{\Omega}})$; on suppose donc: $\mathbf{N}_x$, $\mathbf{N}_y$ et $\mathbf{N}_z \subset$ B. Avec cette identification, l'hypothèse $\inf(A_{yz}^*) = m.e_y+n.e_z = \alpha^*$ devient : $\inf(A_{yz}^*) = (0,1,1)$ et la droite exceptionnelle $\mathbf{D}_{yz} = \mathbf{D} = \mathbf{N}.(0,1,1)$ est la diagonale de Oyz ; elle admet une décomposition induite isomorphe à une décomposition de **N**, dont la base généralisée notée $(d_i)_{\ 1 \leq i \leq 2k+1}$ est finie d'ordre impair puisque $1 \in$ A et B est infini.

L'hypothèse de récurrence : pour tout u' < u, on a $\underline{a}(u') \in \mathbf{P} = \{(x,y,y)\}$ et $\underline{b}(u')$ est de la forme $\underline{b}_{\mathbf{P}}(u') + \underline{r}(u')$ où $\underline{b}_{\mathbf{P}}(u') \in \mathbf{P} \cap B$, et $\underline{r}(u') \in Oy \cup Oz$; plus précisément, si $\underline{b}(u') = (x,y,z)$, ou bien $y \geq z$ et alors $\underline{b}_{\mathbf{P}}(u') = (x,z,z)$, $\underline{r}(u') = (0,y-z,0) \in Oy$, ou bien $z \geq y$, et alors $\underline{b}_{\mathbf{P}}(u') = (x,y,y)$, $\underline{r}(u') = (0,0,z-y) \in Oz$.

On notera bien que le couple (**P**, Oy ∪ Oz) est une décomposition directe de $\mathbf{N}^3$. L'important dans l'hypothèse de récurrence ci-dessus consiste donc en « $\underline{a}(u') \in \mathbf{P}$ » et « $\underline{b}_{\mathbf{P}}(u') \in$ B» ; dans cette hypothèse de récurrence figure la décomposition explicite de u' selon (**P**,Oy ∪ Oz) donné par :

$$u' = (\underline{a}(u') + \underline{b}_{\mathbf{P}}(u'))_{\mathbf{P}} + \underline{r}(u')_{Oy\cup Oz} \ ,$$

de sorte qu'on peut calculer $\underline{r}(u')$ avant de calculer $\underline{b}(u')$. Si u' = (x, y, z), ou bien $y \geq z$, et $\underline{r}(u) = (0,y-z,0)$, ou bien $z \geq y$, et $\underline{r}(u) = (0,0,z-y)$.

Venons-en à u.

Supposons d'abord $u \notin A \cup B$. Alors $u = \underline{a}(u) + \underline{b}(u)$, avec $\underline{a}(u) < u$ et $\underline{b}(u) < u$;

comme $\underline{a}(u) < u$, l'hypothèse de récurrence s'applique, et on a donc : $\underline{a}(\underline{a}(u)) = \underline{a}(u) \in \mathbf{P} = \{(x,y,y)\}$; comme $\underline{b}(u) < u$, l'hypothèse de récurrence s'applique encore, et on a donc : $\underline{b}(\underline{b}(u)) = \underline{b}(u) = \underline{b}_{\mathbf{P}}(\underline{b}(u)) + \underline{r}(\underline{b}(u))$; si $\underline{b}(u) = u' = (x,y,z)$, avec $z \geq y$; alors $\underline{b}(u') = u' = (x,y,z)$ aussi, de sorte que $\underline{b}_{\mathbf{P}}(u') = (x,y,y) \in \mathbf{P} \cap B$ et $\underline{r}(u') = (0,0,z-y) \in Oz$; donc $\underline{b}_{\mathbf{P}}(u) = \underline{b}_{\mathbf{P}}(u') = (x,y,y)$ et $\underline{r}(u) = \underline{r}(u') = (0,0,z-y)$; on traite de la même manière l'autre cas (i.e. $y \geq z$).

Supposons maintenant $u \in A \cup B$.

Si $u \in \mathbf{P}$ aussi, alors, ou bien $u \in A$ et dans ce cas on a : $u = \underline{a}(u) \in \mathbf{P}$ et $\underline{b}(u) = 0$ ($\underline{b}_{\mathbf{P}}(u) = \underline{r}(u) = 0$), ou bien $u \in B$ et alors on a: $u = \underline{b}(u) \in \mathbf{P}$ ($\underline{b}_{\mathbf{P}}(u) = \underline{b}(u)$ et $\underline{r}(u) = 0$) et $\underline{a}(u) = 0$.

Si $u \notin \mathbf{P}$, supposons, par exemple, que l'on ait $z > y$; soit alors $u' = u - (0,0,z-y)$ (i.e. : u' est l'unique élément de $\mathbf{P}$ tel que $u' + (0,0,z-y) = u$) ; comme $u' < u$, l'hypothèse de récurrence s'applique : $\underline{a}(u') \in \mathbf{P}$ et $\underline{b}(u')$ est de la forme $\underline{b}_{\mathbf{P}}(u') + \underline{r}(u')$ où $\underline{b}_{\mathbf{P}}(u') \in \mathbf{P} \cap B$ et $\underline{r}(u') = 0$ (vu la définition de u') ; supposons $\underline{a}(u') \neq 0$, alors $u'' = \underline{b}(u') + (0,0,z-y) < u$ et l'hypothèse de récurrence s'applique : $\underline{a}(u'') \in \mathbf{P}$ et $\underline{b}(u'')$ est de la forme $\underline{b}_{\mathbf{P}}(u'') + \underline{r}(u'')$ où $\underline{b}_{\mathbf{P}}(u'') \in \mathbf{P} \cap B$ et $\underline{r}(u'') = (0,0,z-y)$ (vu la définition de u''et le fait que $\underline{b}(u') = \underline{b}_{\mathbf{P}}(u') \in \mathbf{P} \cap B$); on a alors :

$$\begin{aligned} u'' &= \underline{b}(u') + (0,0,z-y) = \underline{a}(u'') + \underline{b}(u'') \\ &= \underline{a}(u'') + \underline{b}_{\mathbf{P}}(u'') + \underline{r}(u'') \\ &= \underline{a}(u'') + \underline{b}_{\mathbf{P}}(u'') + (0,0,z-y) \end{aligned}$$

d'où , après simplification par (0,0,z-y) :

$$\underline{b}(u') = \underline{a}(u'') + \underline{b}_{\mathbf{P}}(u'') ;$$

l'unicité de décomposition entraîne alors que $\underline{a}(u'') = 0$, donc $u'' \in B$; mais $u = \underline{a}(u') + u''$ aurait alors deux décompositions : contradiction ! Donc $\underline{a}(u') = 0$, de sorte que $u' \in B$ et $\underline{b}_{\mathbf{P}}(u') = \underline{b}(u') = u'$.

Reste à écarter l'éventualité : « $u' + (0,0,z-y) \in A$» ; on traite ce point grâce à une **récurrence secondaire** : supposons établi que $u' + (0,0,v)$ est élément de B pour tout v, $0 \leq v < z-y$; comme $z-y \geq 1$, on peut considérer l'élément $u'_{-1} = u' + (0,0,z-y-1)$; par l'hypothèse de récurrence secondaire, c'est un élément de B; si $u' + (0,0,z-y)$ était élément de A, alors l'élément $u^* = u'+(0,1,z-y)$ aurait deux décompositions selon (A,B) :

$$\begin{aligned} u^* &= u' + (0,1,z-y) = (u' + (0,0,z-y))_A + (0,1,0)_B \text{ , d'une part} \\ u^* &= u' + (0,1,z-y) = (0,1,1)_A + (u' + (0,0,z-y-1))_B \text{ , d'autre part ;} \end{aligned}$$

ainsi, l'élément $u' + (0,0,z-y)$ est dans B.

La démonstration est pratiquement achevée : le « plan » $\mathbf{P}$ est propre pour la décomposition donnée. Il est isomorphe à $\mathbf{N}^2$; on identifie $(A_{\mathbf{P}}, B_{\mathbf{P}})$ à une décomposition (A_0, B_0) de $\mathbf{N}^2$. Si celle-ci était triviale, alors la décomposition de $\mathbf{N}^3$ donnée serait, elle, *semi-triviale* , ce qui n'est pas ◄

Supposons maintenant B_x, A_y et A_z finis. Supposons encore la décomposition induite sur Oyz non triviale, avec « droite exceptionnelle » $\mathbf{D}_{yz} = \mathbf{D} = \mathbf{N}.\alpha^*$, où $\alpha^* = m.e_y + n.e_z$. On sait que cette dernière est stable. Si on suppose que $B_{\mathbf{D}}$ est infini, la valeur des noyaux d'instabilité fait que le théorème de décomposition directe triviale s'applique : $N_{\partial yz}(A_{yz})$ (= A_{yz} d'après la

proposition 3-3) et $N_{\partial x}(B_x)$ (= B_x d'après les premiers calculs). Dans ce cas, on dira que la décomposition (A,B) de $\mathbf{N}^3$ est *semi-triviale* (i.e. produit des décompositions induites sur Ox et Oyz respectivement, cette dernière étant non triviale). On se place donc justement dans le cas où les conditions suffisantes d'application du **théorème 1-1** ne s'appliquent pas, c'est-à-dire dans le cas où $B_{\mathbf{D}}$ est fini.

Proposition 4-1-3.

Avec ces hypothèses (B_x, A_y , A_z et $B_{\mathbf{D}}$ finis) , si la décomposition directe de $\mathbf{N}^3$ considérée n'est pas semi-triviale, alors le plan $\mathbf{P} = Ox \oplus \mathbf{D}_{yz}$ est une partie propre de $\mathbf{N}^3$ sur laquelle (A,B) induit une décomposition (A_0, B_0) isomorphe à une décomposition non triviale de $\mathbf{N}^2$.

► On pourrait pratiquement se contenter d'un…« par un raisonnement tout à fait analogue à celui de la proposition précédente », mais nous allons au contraire « rallonger la sauce », dans l'unique but de fixer des notations pour la version « programmatique » de ces propositions, et les exemples numériques afférents.

Quelques réductions (sans simplification afférente des notations).
D'après la **proposition 4-1**, ($\mathbf{\Omega}$, **C**) est une décomposition directe de $\mathbf{N}^3$; $\mathbf{\Omega}$ et **C** sont propres pour la décomposition (A,B) donnée ; plus précisément, tout $t \in \mathbf{N}^3$ s'écrit de façon unique : $t = \omega+c$, où $\omega \in \mathbf{\Omega}$ et $c \in \mathbf{C}$, et l'on a : $\underline{a}(t) = \underline{a}(\omega) + \underline{a}(c)$ et $\underline{b}(t) = \underline{b}(\omega) + \underline{b}(c)$, sachant que $\underline{a}(\omega)$, $\underline{b}(\omega) \in \mathbf{\Omega}$.

On est donc ramené à trouver la décomposition induite par (A,B) sur $\mathbf{\Omega} = \mathbf{N}.e_x \oplus \mathbf{N}.e_y \oplus \mathbf{N}.e_z$ sachant que $\mathbf{N}.e_x$ est trivial : $\mathbf{N}.e_x \subset$ A, et que $\mathbf{N}.e_y \oplus \mathbf{N}.e_z$, muni de la décomposition induite par (A,B) est isomorphe à une décomposition non triviale de $\mathbf{N}^2$, dont les « bords » $\mathbf{N}.e_y$ et $\mathbf{N}.e_z$ sont dans B, et dont les noyaux d'instabilité ne sont ni l'un ni l'autre maximaux, de sorte que le théorème de décomposition triviale (même sous sa forme relative) n'est pas applicable.

Pour alléger les notations, on identifie $\mathbf{\Omega}$ à $\mathbf{N}^3$, on note (A',B') la décomposition de $\mathbf{N}^3$ correspondant à la décomposition ($A_{\mathbf{\Omega}}$,$B_{\mathbf{\Omega}}$) de $\mathbf{\Omega}$, et on suppose donc: $\mathbf{N}_x \subset$ A', $\mathbf{N}_y$ et $\mathbf{N}_z \subset$ B'.
D'après la **proposition 3-2**, on sait qu'il existe un unique couple d'entiers ($m \geq 1$, $n \geq 1$) tel que $\inf(A'^{*}_{yz}) = m.e_y+n.e_z = \alpha^*$; la droite exceptionnelle $\mathbf{D}'_{yz} = \mathbf{D}' = \mathbf{N}.\alpha^*$ admet une décomposition induite isomorphe à une décomposition de **N**, dont la base généralisée est notée $(d_i)_{\ 1 \leq i \leq 2k}$ (elle est finie et s'arrête sur un indice pair, puisque $B_{\mathbf{D}}$ est fini et «$1 \in A'_{\mathbf{D}}$»).
Maintenant, l'élément à décomposer t' n'est autre que l'élément correspondant à ω dans l'identification faite entre $\mathbf{\Omega}$ et $\mathbf{N}^3$. Si $\omega = x.e_x + y.e_y + z.e_z$, alors t' = (x, y, z)

La décomposition du « cube » $\mathbf{C}' = [0,1[\times [0,m[\times [0,n[$ est triviale dans ce sens que l'on a : $A'_{\mathbf{C}'} = \{0\}\times\{0\}\times\{0\}$ et $B'_{\mathbf{C}'} = \{0\}\times [0,m[\times [0,n[$. Le réseau $\mathbf{\Omega}'$ engendré par $e'_x = (1, 0, 0)$, $e'_y = (0, m, 0)$ et $e'_z = (0, 0, n)$, éléments qui correspondent respectivement à e_x , $m.e_y$ et $n.e_z$ dans l'identification faite entre $\mathbf{\Omega}$ et $\mathbf{N}^3$, est une partie propre pour la décomposition (A',B') : en effet, la **proposition 4-1** s'applique à nouveau, et dans un cas relativement trivial puisque $\mathbf{C}'$ est entièrement contenu dans B' (notons aussi que $\dim(\mathbf{C}') \leq 2$, plus précisément : $\dim(\mathbf{C}') = 2$ si m et n > 1 ; $\dim(\mathbf{C}') = 1$ si m > 1 et n = 1, ou si m = 1 et n > 1 ; enfin, $\dim(\mathbf{C}') = 0$ si m = n = 1).
Donc t' s'écrit de manière unique $t' = \omega'+c'$, où $\omega' \in \mathbf{\Omega}'$ et $c' \in \mathbf{C}'$, et l'on a : $\underline{a}(t') = \underline{a}(\omega') + \underline{a}(c')$ et $\underline{b}(t') = \underline{b}(\omega') + \underline{b}(c')$, sachant que $\underline{a}(\omega')$, $\underline{b}(\omega') \in \mathbf{\Omega}'$.

Précisément, on effectue les divisions euclidiennes de y par m et de z par n :
$y = m.y' + m'$ et $z = n.z' + n'$, avec $m' < m$ et $n' < n$.
On a : $c' = (0, m', n') \in B'$ et $\omega' = (x, m.y', n.z')$ reste à décomposer.

Pour alléger les notations, on identifie $\mathbf{\Omega}'$ à $\mathbf{N}^3$, on note (A'',B'') la décomposition de $\mathbf{N}^3$ correspondant à $(A'_{\mathbf{\Omega}'}, B'_{\mathbf{\Omega}'})$; on suppose donc: $\mathbf{N}_x \subset A''$, $\mathbf{N}_y$ et $\mathbf{N}_z \subset B''$. Avec cette identification, l'hypothèse $\inf(A_{yz}^*) = m.e_y+n.e_z = \alpha^*$, devenue déjà $\inf(A'_{yz}{}^*) = (0,m,n)$, devient : $\inf(A''_{yz}{}^*) = (0,1,1)$; la droite exceptionnelle $\mathbf{D}''_{yz} = \mathbf{D}'' = \mathbf{N}.(0,1,1)$ est la diagonale de Oyz ; elle admet une décomposition induite isomorphe à une décomposition de **N**, dont la base généralisée est toujours notée par $(d_i)_{\ 1 \le i \le 2k}$; l'élément u qui reste à décomposer et correspondant à ω' est $u = (x , y', z')$.

L'hypothèse de récurrence : pour tout $u' < u$, on a $\underline{a}(u') \in \mathbf{P} = \{(x,y,y)\}$ et $\underline{b}(u')$ est de la forme $\underline{b}_{\mathbf{P}}(u') + \underline{r}(u')$ où $\underline{b}_{\mathbf{P}}(u') \in \mathbf{P} \cap B''$, $\mathbf{P} = \{(x,y,y)\}$, et $\underline{r}(u') \in Oy \cup Oz$; plus précisément, si $\underline{b}(u') = (x,y,z)$, ou bien $y \ge z$ et alors $\underline{b}_{\mathbf{P}}(u') = (x,z,z)$, $\underline{r}(u') = (0,y-z,0) \in Oy$, ou bien $z \ge y$, et alors $\underline{b}_{\mathbf{P}}(u') = (x,y,y)$, $\underline{r}(u') = (0,0,z-y) \in Oz$.
On notera bien que le couple $(\mathbf{P}, Oy \cup Oz)$ est une décomposition directe de $\mathbf{N}^3$. L'important dans l'hypothèse de récurrence ci-dessus consiste donc en « $\underline{a}(u') \in \mathbf{P}$ » et « $\underline{b}_{\mathbf{P}}(u') \in B''$» ; dans cette hypothèse de récurrence figure donc la décomposition explicite de u, donc de ω', donc de ω, donc de t. La décomposition de u' selon $(\mathbf{P}, Oy \cup Oz)$ est donné par :

$$u' = (\underline{a}(u') + \underline{b}_{\mathbf{P}}(u'))_{\mathbf{P}} + \underline{r}(u')_{Oy \cup Oz} \ ,$$

de sorte qu'on peut calculer $\underline{r}(u')$ avant de calculer $\underline{b}(u')$. Si $u' = (x', y', z')$, ou bien $y' \ge z'$, et $\underline{r}(u') = (0,y'-z',0)$, ou bien $z' \ge y'$, et $\underline{r}(u') = (0,0,z'-y')$; si $\underline{b}(u') = (x, y, z)$, ou bien $y \ge z$ et dans ce cas $y'-z' = y-z \ge 0$, ou bien $z \ge y$ et dans ce cas $z'-y' = z-y \ge 0$;

Venons-en à u.

Supposons d'abord $u \notin A'' \cup B''$. Alors $u = \underline{a}(u) + \underline{b}(u)$, avec $\underline{a}(u) < u$ et $\underline{b}(u) < u$; comme $\underline{a}(u) < u$, l'hypothèse de récurrence s'applique, et on a donc : $\underline{a}(\underline{a}(u)) = \underline{a}(u) \in \mathbf{P} = \{(x,y,y)\}$; comme $\underline{b}(u) < u$, l'hypothèse de récurrence s'applique encore, et on a donc : $\underline{b}(\underline{b}(u)) = \underline{b}(u) = \underline{b}_{\mathbf{P}}(\underline{b}(u)) + \underline{r}(\underline{b}(u))$; si $\underline{b}(u) = u' = (x,y,z)$, avec $z \ge y$; alors $\underline{b}(u') = u' = (x,y,z)$ aussi de sorte que $\underline{b}_{\mathbf{P}}(u') = (x,y,y) \in \mathbf{P} \cap B''$et $\underline{r}(u') = (0,0,z-y) \in Oz$; donc $\underline{b}_{\mathbf{P}}(u) = \underline{b}_{\mathbf{P}}(u') = (x,y,y)$ et $\underline{r}(u) = \underline{r}(u') = (0,0,z-y)$; on traite de la même manière l'autre cas (i.e. $y \ge z$).

Supposons maintenant $u \in A'' \cup B''$.

Si $u \in \mathbf{P}$ aussi, alors, ou bien $u \in A''$ et dans ce cas on a : $u = \underline{a}(u) \in \mathbf{P}$ et $\underline{b}(u) = 0$ ($\underline{b}_{\mathbf{P}}(u) = \underline{r}(u) = 0$), ou bien $u \in B''$et alors on a: $u = \underline{b}(u) \in \mathbf{P}$ ($\underline{b}_{\mathbf{P}}(u) = \underline{b}(u)$ et $\underline{r}(u) = 0$) et $\underline{a}(u) = 0$.

Si $u \notin \mathbf{P}$, supposons, par exemple, que l'on ait $z > y$; soit alors $u' = u - (0,0,z-y)$ (i.e. : u' est l'unique élément de **P** tel que $u' + (0,0,z-y) = u$) ; comme $u' < u$, l'hypothèse de récurrence s'applique : $\underline{a}(u') \in \mathbf{P}$ et $\underline{b}(u')$ est de la forme $\underline{b}_{\mathbf{P}}(u') + \underline{r}(u')$ où $\underline{b}_{\mathbf{P}}(u') \in \mathbf{P} \cap B''$et $\underline{r}(u') = 0$ (vu la définition de u') ; supposons $\underline{a}(u') \ne 0$, alors l'élément $u'' = \underline{b}(u') + (0,0,z-y)$ est strictement plus petit que u et l'hypothèse de récurrence s'applique : $\underline{a}(u'') \in \mathbf{P}$ et $\underline{b}(u'')$ est de la forme $\underline{b}_{\mathbf{P}}(u'') + \underline{r}(u'')$ où $\underline{b}_{\mathbf{P}}(u'') \in \mathbf{P} \cap B''$et $\underline{r}(u'') = (0,0,z-y)$ (vu la définition de u''et le fait que $\underline{b}(u') = \underline{b}_{\mathbf{P}}(u') \in \mathbf{P} \cap B''$); on a alors :

$$u'' = \underline{b}(u') + (0,0,z-y) = \underline{a}(u'') + \underline{b}(u'')$$
$$= \underline{a}(u'') + \underline{b}_{\mathbf{P}}(u'') + \underline{r}(u'')$$
$$= \underline{a}(u'') + \underline{b}_{\mathbf{P}}(u'') + (0,0,z-y)$$

d'où , après simplification par (0,0,z-y) :

$$\underline{b}(u') = \underline{a}(u'') + \underline{b}_{\mathbf{P}}(u'') ;$$

l'unicité de décomposition entraîne alors que $\underline{a}(u'') = 0$, donc $u'' \in B''$; mais $u = \underline{a}(u') + u''$ aurait alors deux décompositions ! Il y a une contradiction : $\underline{a}(u') = 0$ de sorte que $u' \in B''$et $\underline{b}_{\mathbf{P}}(u') = \underline{b}(u') = u'$.

Reste à écarter l'éventualité : « $u' + (0,0,z-y) \in A''$ » ; on traite ce point grâce à une **récurrence secondaire** : supposons établi que $u' + (0,0,v)$ est élément de B'' pour tout v, $0 \leq v < z-y$; comme $z-y \geq 1$, on peut considérer l'élément $u'_{-1} = u' + (0,0,z-y-1)$; par l'hypothèse de récurrence secondaire, c'est un élément de B'' ; si $u' + (0,0,z-y)$ était élément de A'', alors l'élément $u^* = u'+(0,1,z-y)$ aurait deux décompositions selon (A'', B'') :

$$u^* = u' + (0,1,z-y) = (u' + (0,0,z-y)) + (0,1,0), \text{ d'une part}$$
$$u^* = u' + (0,1,z-y) = (0,1,1) + (u' + (0,0,z-y-1)), \text{ d'autre part ;}$$

ainsi, l'élément $u' + (0,0,z-y)$ est dans B''.

La démonstration est pratiquement achevée : le « plan » **P** est propre pour la décomposition donnée. Il est isomorphe à $\mathbf{N}^2$; on identifie $(A''_{\mathbf{P}}, B''_{\mathbf{P}})$ à une décomposition (A_0, B_0) de $\mathbf{N}^2$. Si celle-ci était triviale, alors la décomposition de $\mathbf{N}^3$ donnée serait, elle, semi-triviale , ce qui n'est pas ◄

Vers un programme. Un exemple numérique en dimension 3.

Il faudra entrer les paramètres d'une telle décomposition, à savoir :

- les listes des multiplicateurs sur les trois axes ; si une liste n'est pas exhaustive (bien que finie), elle doit être fournie par un sous-programme approprié, qui fournit à la fois une borne supérieure effective de l'ensemble des indices des multiplicateurs, et la valeur des multiplicateurs en fonction de leur rang ;

- les choix : $1 \in A$ ou $1 \in B$, sur les trois axes ; comme B_x est censé être fini, la parité du nombre de multiplicateurs détermine le choix « $1 \in A_x$ ou $1 \in B_x$ »: impair si $1 \in B_x$, pair si $1 \in A_x$; de même, comme A_y est censé être fini, le nombre des multiplicateurs détermine le choix : $1 \in A_y$ ou $1 \in B_y$: impair si $1 \in A_y$, pair si $1 \in B_y$; même remarque pour Oz ;

- le couple d'entiers (m,n) qui définit α^* dans le plan Oyz ; $\alpha^* = m.e_y + n.e_z$;

- la liste finie des multiplicateurs (α^* est censé être élément de A), sur la droite $\mathbf{N}.\alpha^*$ (ou la diagonale de Oyz après identification de $\mathbf{\Omega}$ avec $\mathbf{N}^3$) ; même remarque que ci-dessus à propos

de l'exhaustivité de la liste ; il doit y avoir un nombre pair de tels multiplicateurs, puisque B_D est censé être fini ; $d_1, d_2, \ldots, d_{2k}$; on obtient alors $\beta^* = d_{2k} \ldots d_2.d_1.\alpha^*$;

- le couple d'entiers (m_0,n_0) qui définit γ^* dans le plan **P** engendré par (1,0,0) (en lieu de e_1) et (0,1,1) (en lieu de α^*) ; $\gamma^* = m_0.e_x + n_0.\beta^*$

- la liste (finie ou non) des multiplicateurs (γ^* est censé être élément de B), sur la droite $\mathbf{N}.\gamma^*$; même remarque que ci-dessus à propos de l'exhaustivité et de la calculabilité de la liste (sous-programme éventuel).

Le corps de la démonstration précédente fournit le corps du programme des calculs à effectuer :

- $t = (t_x , t_y , t_z)$ est fourni ;
- calcul des trois nombres produits des multiplicateurs, sur chaque axe, soit m_x, m_y, m_z ;
noter que $e_x = (m_x, 0, 0)$, $e_y = (0, m_y, 0)$ et $e_z = (0, 0, m_z)$; $t = \omega + c$;
- divisions : $t_x = x.m_x + c_x$, $c_x < m_x$; $t_y = y.m_y + c_y$, $c_y < m_y$; $t_z = z.m_z + c_z$, $c_z < m_z$;
noter que $\omega = x.e_x + y.e_y + z.e_z$; $c = (c_x, c_y, c_z)$ est à décomposer (sous-programme) ;
- ω devient $t' = (x, y, z)$; divisions : $y = m.y' + m'$, $m' < m$; $z = n.z' + n'$, $n' < n$;
noter que $t' = \omega' + c'$; $\omega' = (x, m.y', n.z')$ est à décomposer ; $c' = (0, m', n') \in B'$;
- $\beta^* = d_{2k} \ldots d_2.d_1.\alpha^* = m_D.\ \alpha^*$
- ω' devient $u = (x, y', z')$ tandis que :
α^* devient (0,1,1) , β^* devient $(0, m_D, m_D)$ et $\gamma^* = m_0.e_x + n_0.\beta^*$ devient $(m_0, n_0.m_D, n_0.m_D)$
- si $y' \geq z'$, $r(u) = (0,y'-z',0)$ et (x, z', z') est à décomposer dans **P** ;
si $z' \geq y'$, $r(u) = (0, 0, z'-y')$ et (x, y', y') est à décomposer dans **P** ; soit $y° = \inf(y',z')$
- la décomposition de $(x, y°, y°)$ dans **P** revient à celle de $(x, y°)$ dans $\mathbf{N}^2$: on calcule d'abord les restes relatifs aux divisions de x et y° par 1 et m_D respectivement: $x = x.1 + 0$ (trivial !) et $y° = y.m_D + r$, avec $r < m_D$; on décompose r en $\underline{a}(r) + \underline{b}(r)$ selon la liste des multiplicateurs $d_1, d_2, \ldots, d_{2k}$, ce qui fournit les éléments $(0, \underline{a}(r))_A$ et $(0, \underline{b}(r))_B$ qui contribuent au calcul de $\underline{a}(x, y°)$ et $\underline{b}(x, y°)$, et donc au calcul de $\underline{a}(u)$ et $\underline{b}(u)$, $\underline{a}(\omega')$ et $\underline{b}(\omega')$, $\underline{a}(t')$ et $\underline{b}(t')$, $\underline{a}(t)$ et $\underline{b}(t)$!
- reste à décomposer (x,y) dans le réseau engendré par $(1,m_D)$ selon la procédure indiquée dans l'énoncé de la **proposition 3-2**, dont nous adaptons ici simplement les notations :
- si $x /y \leq m_0 /n_0$, on effectue la division euclidienne de x par m_0 : $x = p.m_0 + s$, $s < m_0$; l'entier p s'écrit de manière unique $p_a + p_b$, de sorte que $p.(m_0,n_0) = p_a.(m_0,n_0) + p_b.(m_0,n_0)$ et puis $\underline{a}(x,y) = p_a.(m_0,n_0)$ et $\underline{b}(x,y) = s.(1,0) + (y-p.n_0).(0,1) + p_b.(m_0,n_0)$;
- si $x /y \geq m_0 /n_0$, on effectue la division euclidienne de y par n_0 : $y = q.n_0 + s'$, $s' < n_0$; l'entier q s'écrit de manière unique $q_a + q_b$, de sorte que $q.(m_0,n_0) = q_a.(m_0,n_0) + q_b.(m_0,n_0)$ et puis $\underline{a}(x,y) = q_a.(m_0,n_0)$ et $\underline{b}(x,y) = s'.(0,1) + (x-q.m_0).(1,0) + q_b.(m_0,n_0)$
- fin des calculs et remontée vérificatrice:
$\underline{a}(x,y) = q_a.(m_0,n_0) = (q_a.m_0, q_a.n_0)$;
$\underline{a}(x,y°) = (q_a.m_0, m_D.q_a.n_0) + (0,\underline{a}(r))_A = (q_a.m_0, m_D.q_a.n_0+\underline{a}(r))_A$;
$\underline{a}(x, y°, y°) = (q_a.m_0, m_D.q_a.n_0+\underline{a}(r), m_D.q_a.n_0+\underline{a}(r))_A$;
$\underline{b}(x,y) = s'.(0,1) + (x-q.m_0).(1,0) + q_b.(m_0,n_0) = (x-q_a.m_0, s'+q_b.n_0)$;
$\underline{b}(x,y°) = (x-q_a.m_0, m_D.(s'+q_b.n_0)) + (0,\underline{b}(r))_B = (x-q_a.m_0, m_D.(s'+q_b.n_0)+\underline{b}(r))_B$;
$\underline{b}(x, y°, y°) = (x-q_a.m_0, m_D.(s'+q_b.n_0)+\underline{b}(r), m_D.(s'+q_b.n_0)+\underline{b}(r))_B$;
$(x, y°, y°) =$
$(q_a.m_0, m_D.q_a.n_0+\underline{a}(r), m_D.q_a.n_0+\underline{a}(r))_A + (x-q_a.m_0, m_D.(s'+q_b.n_0)+\underline{b}(r), m_D.(s'+q_b.n_0)+\underline{b}(r))_B$;
Si $y° = y'$, $r(u) = (0, 0, z'-y')$ et $(x, y', y') = (x, y°, y°)$
$\underline{a}(x, y', z') = (q_a.m_0, m_D.q_a.n_0+\underline{a}(r), m_D.q_a.n_0+\underline{a}(r))_A$

$\underline{b}(x, y', z') = (x-q_a.m_0, m_D.(s'+q_b.n_0)+\underline{b}(r), m_D.(s'+q_b.n_0)+\underline{b}(r) + z'-y')_B$;

Si $y° = z'$, $\underline{r}(u) = (0, y'-z', 0)$ et $(x, z', z') = (x, y°, y°)$

$\underline{a}(x, y', z') = (q_a.m_0, m_D.q_a.n_0+\underline{a}(r), m_D.q_a.n_0+\underline{a}(r))_A$

$\underline{b}(x, y', z') = (x-q_a.m_0, m_D.(s'+q_b.n_0)+\underline{b}(r) + y'-z', m_D.(s'+q_b.n_0)+\underline{b}(r))_B$;

$\underline{a}(\omega') = (q_a.m_0, m.(m_D.q_a.n_0+\underline{a}(r)) , n.(m_D.q_a.n_0+\underline{a}(r)))_A$;

$\underline{b}(\omega') = (x-q_a.m_0, m.(m_D.(s'+q_b.n_0)+\underline{b}(r)) , n.(m_D.(s'+q_b.n_0)+\underline{b}(r) + z'-y'))_B$ si $y° = y'$,

$\underline{b}(\omega') = (x-q_a.m_0, m.(m_D.(s'+q_b.n_0)+\underline{b}(r) + y'-z') , n.(m_D.(s'+q_b.n_0)+\underline{b}(r)))_B$ si $y° = z'$,

$\underline{a}(t') = \underline{a}(\omega') = (q_a.m_0, m.(m_D.q_a.n_0+\underline{a}(r)) , n.(m_D.q_a.n_0+\underline{a}(r)))_A$;

$\underline{b}(t') = (x-q_a.m_0, m.(m_D.(s'+q_b.n_0)+\underline{b}(r))+m' , n.(m_D.(s'+q_b.n_0)+\underline{b}(r)+z'-y')+n')_B$ si $y° = y'$,

$\underline{b}(t') = (x-q_a.m_0, m.(m_D.(s'+q_b.n_0)+\underline{b}(r)+y'-z')+m' , n.(m_D.(s'+q_b.n_0)+\underline{b}(r))+n')_B$ si $y° = z'$,

$\omega = x.e_x + y.e_y + z.e_z$; $e_x = (m_x, 0, 0)$, $e_y = (0, m_y, 0)$ et $e_z = (0, 0, m_z)$

$\underline{a}(\omega) = (m_x.q_a.m_0, m_y.(m.(m_D.q_a.n_0+\underline{a}(r))) , m_z.(n.(m_D.q_a.n_0+\underline{a}(r))))_A$;

si $y° = y'$, $\underline{b}(\omega) =$

$(m_x.(x-q_a.m_0), m_y.(m.(m_D.(s'+q_b.n_0)+\underline{b}(r))+m'), m_z.(n.(m_D.(s'+q_b.n_0)+\underline{b}(r)+z'-y')+n'))_B$

si $y° = z'$, $\underline{b}(\omega) =$

$(m_x.(x-q_a.m_0), m_y.(m.(m_D.(s'+q_b.n_0)+\underline{b}(r)+y'-z')+m'), m_z.(n.(m_D.(s'+q_b.n_0)+\underline{b}(r))+n'))_B$

$\underline{a}(t) = (m_x.q_a.m_0+\underline{a}(c_x) , m_y.(m.(m_D.q_a.n_0+\underline{a}(r))) + \underline{a}(c_y), m_z.(n.(m_D.q_a.n_0+\underline{a}(r))) + \underline{a}(c_z))_A$;

si $y° = y'$: $\underline{b}(t) = (m_x.(x-q_a.m_0) + b(c_x),$

$m_y.(m.(m_D.(s'+q_b.n_0)+\underline{b}(r))+m') + \underline{b}(c_y),$

$m_z.(n.(m_D.(s'+q_b.n_0)+\underline{b}(r)+z'-y')+n') + \underline{b}(c_z))_B$,

si $y° = z'$: $\underline{b}(t) = (m_x.(x-q_a.m_0) + \underline{b}(c_x),$

$m_y.(m.(m_D.(s'+q_b.n_0)+\underline{b}(r)+y'-z')+m') + \underline{b}(c_y),$

$m_z.(n.(m_D.(s'+q_b.n_0)+\underline{b}(r))+n') + \underline{b}(c_z))_B.$

Vérifications:

$m_x.q_a.m_0 + \underline{a}(c_x) + (m_x.(x-q_a.m_0) + \underline{b}(c_x) = m_x.x + c_x = t_x$;

et si $y° = y'$:

$m_y.(m.(m_D.q_a.n_0+\underline{a}(r))) + \underline{a}(c_y) + m_y.(m.(m_D.(s'+q_b.n_0)+\underline{b}(r))+m') + \underline{b}(c_y) = t_y$;

$m_z.(n.(m_D.q_a.n_0+\underline{a}(r))) + \underline{a}(c_z) + m_z.(n.(m_D.(s'+q_b.n_0)+\underline{b}(r)+z'-y')+n') + \underline{b}(c_z)) = t_z$;

et si $y° = z'$:

$m_y.(m.(m_D.q_a.n_0+\underline{a}(r))) + \underline{a}(c_y) + m_y.(m.(m_D.(s'+q_b.n_0)+\underline{b}(r)+y'-z')+m') + \underline{b}(c_y) = t_y$;

$m_z.(n.(m_D.q_a.n_0+\underline{a}(r))) + \underline{a}(c_z) + m_z.(n.(m_D.(s'+q_b.n_0)+\underline{b}(r))+n') + \underline{b}(c_z)) = t_z$.

Un exemple numérique.

Choix des paramètres :

Multiplicateurs sur les 3 axes :

Sur Ox : $1 \in A$; $m_1 = 2, m_2 = 2, m_3 = 3, m_4 = 7$; $b_x^{++} = 84$ $(2.2.3.7) \in A$ $(\sup(B_x) = 14)$

Sur Oy : $1 \in A$; $m_1 = 5, m_2 = 3, m_3 = 3$; $b_y^{++} = 45$ $(3.3.5) \in B$ $(\sup(A_y) = 34)$

Sur Oz : $1 \in B$; $m_1 = 3, m_2 = 2, m_3 = 3$; $m_4 = 2$; $b_z^{++} = 36$ $(3.2.3.2) \in B$ $(\sup(A_z) = 21)$

Couple $(m,n)_{yz}$: (3,5) d'où $\alpha^* = (135, 180) \in A$

Multiplicateurs sur **D** :

$1.\alpha^* \in A$; $m_1 = 3, m_2 = 2, m_3 = 3, m_4 = 5$; $b_D^{++} = 90.\alpha^*$ $(3.2.3.5) \in A_D$ $(\sup(B_D) = 21.\alpha^*)$

Couple $(m_0 ,n_0)_{xyy}$:

(7,3) d'où $\beta^* = (7.b_x^{++} , 3.b_D^{++}) = (7.84, 3.90.\ \alpha^*\ ) = (588, 36450, 48600) \in B$

Multiplicateurs sur $\mathbf{D}_0$:
$1.\beta^* \in B$; $m_1 = 3$, $m_2 = 7$, $m_3 = 2$; $b_{D0}^{++} = 42.\beta^*$ (3.7.2) $\in A_{D0}$ $(\sup(B_{D0}) = 22.\beta^*)$
$b_{D0}^{++} = 42.\beta^* = 42.(588, 36450, 48600) = (24696, 1530900, 2041200)$
Les calculs.
- $t = (t_x , t_y , t_z) = (796523, 22434083, 35684219)$
- $(m_x, m_y, m_z) = (84, 45, 36)$; $e_x = (84, 0, 0)$, $e_y = (0, 45, 0)$ et $e_z = (0, 0, 36)$

Les 3 premières divisions: 796523 : 84 = 9482 + 35:84
22434083: 45 = 498535 + 8:45
35684219: 36 = 991228 + 11:36
Les trois restes: 35, 8, 11 et leurs décompositions :
$35 = 2.12 + 2.4 + 1.2 + 1 = 9_A + 26_B$
$8 = 1.5 + 3.1 = 3_A + 5_B$
$11 = 1.6 + 1.3 + 2.1 = 3_A + 8_B$
Contribution des 3 restes à la décomposition : $t = \omega + c$;
$\omega = x.e_x + y.e_y + z.e_z = 9482(84, 0, 0) + 498535(0, 45, 0) + 991228(0, 0, 36)$
$t' = (9482, 498535, 991228)$ et $c = (9, 3, 3)_A + (26, 5, 8)_B$
$y = 498535 = m.y' + m' = 3.166178+1$, $y' = 166178$, $m'=1$
$z = 991228 = n.z' + n' = 5.198245 + 3$, $z' = 198245$, $n' = 3$
$c' = (0,1,3) \in B'$; $\omega' = (x, m.y', n.z') = (9482, 498534 , 991225)$;
$u = (9482, 166178, 198245)$; on est dans le cas : $z' \geq y'$; $\underline{r}(u) = (0, 0, z'-y') = (0,0,32067)$
$y^\circ = \inf(y',z') = y' = 166178$; $m_D = 3.2.3.5 = 90$
$y^\circ = 166178 = y.m_D + r = 1846.90 + 38$; $y = 1846$; $r = 38$
$\underline{a}(r) = 2$; $\underline{b}(r) = 36$; $(x,y) = (9482, 1846)$; $(m_0 ,n_0) = (7,3)$; $x /y \geq m_0 /n_0$;
$y = 615.3 + 1$; $q = 615$; $s' = 1$; $615 = 14.42+1.21+2.3$; $q_a = 594$; $q_b = 21$;
$\underline{a}(x,y) = q_a.(m_0,n_0) = 594.(7,3) = (4158, 1782)$;
$\underline{b}(x,y) = s'.(0,1)+(x-q.m_0).(1,0)+q_b.(m_0,n_0) = 1.(0,1)+5177.(1,0)+21.(7,3) = (5324, 64)$
$\underline{a}(x,y^\circ) = (q_a.m_0, m_D.q_a.n_0+\underline{a}(r))_A = (4158, 90.1782+2) = (4158, 160382)$;
$\underline{a}(x, y^\circ, y^\circ) = (4158, 160382, 160382)$;
$\underline{b}(x,y^\circ) = (x-q_a.m_0, m_D.(s'+q_b.n_0)+\underline{b}(r))_B = (5324, 5796)$;
$\underline{b}(x, y^\circ, y^\circ) = (5324, 5796, 5796)$;
$(x, y^\circ, y^\circ) = (4158, 160382, 160382)+(5324, 5796, 5796) = (9482, 166178, 166178)$;
$[y^\circ = y']$, $\underline{r}(u) = (0, 0, z'-y') = (0,0,32067)$ et $(x, y', y') = (9482, 166178, 166178)$;
$\underline{a}(x, y', z') = (4158, 160382, 160382)$
$\underline{b}(x, y', z') = (5324, 5796, 5796) + (0,0,32067) = (5324, 5796, 37863)$
$\underline{a}(\omega') = (4158, 3.160382 , 5.160382) = (4158, 481146, 801910)$;
$\underline{b}(\omega') = (5324, 3.5796, 5.37863) = (5324, 17388, 189315)$ $[y^\circ = y']$,
$\underline{a}(t') = \underline{a}(\omega') = (4158, 481146, 801910)$;
$\underline{b}(t') = (5324, 17388, 189315) + (0,1,3) = (5324, 17389, 189318)$ $[y^\circ = y']$,
$\underline{a}(\omega) = (m_x.q_a.m_0, m_y.(m.(m_D.q_a.n_0+\underline{a}(r))) , m_z.(n.(m_D.q_a.n_0+\underline{a}(r))))$
$= (84, 45, 36).(4158, 481146, 801910) = (349272, 21651570, 28868760)$;
$[y^\circ = y']$,
$\underline{b}(\omega) = (m_x.(x-q_a.m_0), m_y.(m.(m_D.(s'+q_b.n_0)+\underline{b}(r))+m'), m_z.(n.(m_D.(s'+q_b.n_0)+\underline{b}(r)+z'-y')+n'))$
$= (84, 45, 36)_*(5324, 17389, 189318) = (447216 , 782505, 6815448)$;
$\underline{a}(t) = (349272, 21651570, 28868760) + (9, 3, 3) = (349281, 21651573, 28868763)$
$\underline{b}(t) = (447216 , 782505, 6815448) + (26, 5, 8) = (447242, 782510, 6815456)$

$\underline{a}(796523, 22434083, 35684219) = (349281, 21651573, 28868763)$
$\underline{b}(796523, 22434083, 35684219) = (447242, 782510, 6815456)$

Un autre exemple, d'ordre plus théorique.

Choix des paramètres :
Sur Ox : $1 \in A$; multiplicateurs : $\varnothing$; $A_x = \mathbf{N}$
Sur Oy : $1 \in B$; multiplicateurs : $\varnothing$; $B_y = \mathbf{N}$
Sur Oz : $1 \in B$; multiplicateurs : $\varnothing$; $B_z = \mathbf{N}$
Elément $\alpha^* = (1,1) \in A$
Sur **D**: $\alpha^* \in A$; multiplicateurs : $\varnothing$; $A_{\mathbf{D}} = \mathbf{N}$
Elément $\beta^* = (1,0,0) + \alpha^* (1,1,1) \in B$
Sur $\mathbf{D}_0$: $\beta^* \in B$; multiplicateurs : $\varnothing\beta^*$; $B_{\mathbf{D}0} = \mathbf{N}$
Soit 4 paramètres, tous égaux à 1 !

$A = \mathbf{N}.(1,0,0) \cup \mathbf{N}.(0,1,1)$ $\quad B = (\mathbf{N}.(0,1,0) \cup \mathbf{N}.(0,0,1)) \oplus \mathbf{N}.(1,1,1)$
Décomposition d'un élément $(\mathbf{x,y,z})$: en posant $\mathbf{u} = \inf(\mathbf{x,y,z})$ et $\mathbf{v} = \inf(\mathbf{y-u,z-u})$ on voit que :

Si $\mathbf{u \neq x}$: $\underline{\mathbf{a}}\ (\mathbf{x,y,z}) = (\mathbf{x-u,0,0})$, $\underline{\mathbf{b}}\ (\mathbf{x,y,z}) = (\mathbf{u,y,z})$
Si $\mathbf{u = x}$: $\underline{\mathbf{a}}\ (\mathbf{x,y,z}) = (\mathbf{0,v,v})$, $\underline{\mathbf{b}}\ (\mathbf{x,y,z}) = (\mathbf{x,y-v,z-v})$

Cet exemple est *générique* en un certain sens: suites vides de multiplicateurs et composantes des éléments exceptionnels α^* et β^* réduites au minimum : 1. C'est un des ***squelettes sains*** qui seront décrits plus loin en toute généralité.

Caractérisation de toutes les décompositions directes de $\mathbf{N}^3$.
Si les traces de A *et* B sont infinies sur l'un au moins des axes **N**.(1,0,0), **N**.(0,1,0), **N**.(0,0,1) la décomposition de $\mathbf{N}^3$ considérée se présente comme produit de décompositions induites, isomorphes à des décompositions de **N** ou $\mathbf{N}^2$: ce sont les cas de *trivialité* ou de *semi-trivialité*. Cette condition suffisante n'est évidemment pas nécessaire.
Pour achever la classification, il suffit de décrire les décompositions qui ne se présentent pas comme des produits canoniques de décompositions : on les qualifie d'*irréductibles* dans la classification générale. Aux permutations des axes près, et à l'échange des rôles entre A et B près, il y a trois types « nouveaux » de décompositions qui se présentent effectivement, eu égard aux 3 propositions précédentes :

(i) $A_x, A_y, A_z = \{0\}$ après réduction (**proposition 4-1**); il existe un triplet d'entiers non nuls (m,n,p) tel que :

- $\mathbf{L} = \{(x,y,z) \mid x<m \vee y<n \vee z<p\} \subset B$
- $\alpha = (m, n, p) \in A$;
- $\mathbf{D} = \mathbf{N}\alpha$ est une partie propre sur laquelle (A,B) induit une décomposition directe ;
- Tout élément $u = p\alpha + \ell$ où $p\alpha \in \mathbf{D}$, $\ell \in \mathbf{L}$ et $\underline{a}(u) = \underline{a}(p\alpha)$, $\underline{b}(u) = \underline{b}(p\alpha) + \ell$.

(ii) $A_x, A_y, A_z = \{0\}$ après réduction (**proposition 4-1**); il existe deux couples d'entiers non nuls (m,n) et (p,q) tels que :

- $\alpha = (0, m, n) \in A$;
- $\mathbf{D} = \mathbf{N}\alpha$ est une partie propre sur laquelle (A,B) induit une décomposition directe pour laquelle $A_{\mathbf{D}}$ est finie ; on pose $\beta = \inf\{b \in B_{\mathbf{D}} \mid b > A_{\mathbf{D}}\}$; $\beta = k(0,m,n)$
- $\alpha' = (p, qkm, qkn) \in A$
- $\mathbf{D}' = \mathbf{N}\alpha'$ est une partie propre sur laquelle (A,B) induit une décomposition directe;

(iii) $B_x, A_y, A_z = \{0\}$ après réduction (***proposition* 4-1**) ; il existe deux couples d'entiers non nuls (m,n) et (p,q) tels que :

- $\alpha = (0, m, n) \in A$;

- $\mathbf{D} = \mathbf{N}\alpha$ est une partie propre sur laquelle (A,B) induit une décomposition directe pour laquelle $B_{\mathbf{D}}$ est finie ; on pose $\alpha^1 = \inf\{a \in A_{\mathbf{D}} \mid a > B_{\mathbf{D}}\}$; $\alpha^1 = r(0,m,n)$
- $\beta = (p, qrm, qrn) \in B$
- $\mathbf{D}' = \mathbf{N}\beta$ est une partie propre sur laquelle (A,B) induit une décomposition directe;

Dans les cas (ii) et (iii) la décomposition d'un élément de $\mathbf{N}^3$ est fournie par un programme, comme suggéré dans l'exemple numérique ci-dessus.

Ces trois cas d'irréductibilité ne sont pas du même niveau : on peut dire que le premier est simple, ou d'ordre1 (cf. la droite $\mathbf{D} = \mathbf{N}\alpha$), tandis que les deux autres sont d'ordre 2 (cf. les couples de droites (**D,D'**), **D**' s'appuyant en quelque sorte sur **D**. Nous préciserons plus loin cette notion *d'ordre d'irréductibilité.*

Petite incursion en dimensions 4 et 5
La classification générale fera l'objet d'un chapitre à part. En y regardant un peu vite, les deux derniers cas d'irréductibilité précités pourraient apparaître comme des exceptions, or il s'agit au contraire des deux exemples qu'il faut avoir en tête pour bien saisir le cas général.

Réductions et squelettes sains.
Le premier type de réduction consiste à remplacer les décompositions induites sur les droites « canoniques » (axes et autres droites auxiliaires, désignées jusqu'ici par la lettre D) par des décompositions *triviales* (donc avec A ou B réduit à {0} là où A ou B devrait être seulement fini ! Les suites de multiplicateurs sont systématiquement vides); nous renvoyons aux ***propositions* 3-1 *et* 4-1** concernées par ce type de réduction.

Se trouvent écartées de fait les décompositions comme celle de $\mathbf{N}^3$, dite de type (ii) dans le paragraphe précédent : en effet, par essence $A_{\mathbf{D}}$ est fini ***et*** non réduit à {0}; il ne saurait donc être choisi égal à {0}! Par contre les deux autres types du paragraphe précédent, (i) et (iii), sont représentés par des squelettes sains que l'on mentionne ci-dessous.

Se trouvent écartées aussi les décompositions qui induiraient sur une droite « canonique » une décomposition avec A et B infinis!

Le second type de réduction consiste à choisir systématiquement égales à 1 les coordonnées non nulles des *éléments spéciaux* du type α, α^1, β …(générateurs des « droites » **D**, **D'**…)

Définition 4-1.
Après application des deux types de réduction, on obtient *des* décompositions appelées *squelettes sains*.

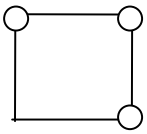
Les squelettes sains sont entièrement déterminés par leurs traces sur le cube (ou hypercube) de côté 1 construit sur les axes et dont un sommet est à l'origine. Ils forment une *typologie* de *certaines* décompositions possibles (*mais pas toutes* !).

Nous reviendrons plus loin sur la notion générale de squelette, mais auparavant, nous présentons la classification des **squelettes sains** en dimensions 2, 3 et 4, en évitant les redites dues à l'échange des rôles de A et de B, ou à certaines permutations des axes.

Ici, les *ronds blancs* représentent des éléments de B, les *ronds noirs* des éléments de A, et les *ronds gris* des éléments qui se décomposent non trivialement.

Squelettes sains de dimension 2.

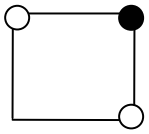
Trivial



$A = \{0\}$ $B = \{xy\}$

$(x,y) = (0,0)_A + (x,y)_B$

Irréductible



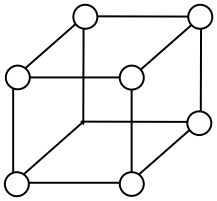
$A = \{xx\}$ $B = \{x\} \cup \{y\}$

$(x,y) = (u,u)_A + (x-u,y-u)_B$

$[u = \inf(x,y)]$

Squelettes sains de dimension 3.

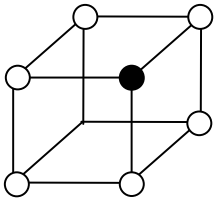
Trivial



$A = \{0\}$ $B = \mathbf{N}^3$

$(x,y,z) = (0,0,0)_A + (x,y,z)_B$

Irréductible (d'ordre 1*)* ***Type (i)***

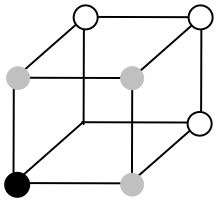


$A=\{xxx\}$ $B=\{xy\}\cup\{yz\}\cup\{xz\}$

$(x,y,z) = (u,u,u)_A + (x-u,y-u,z-u)_B$

$[u=\inf(x,y,z)]$

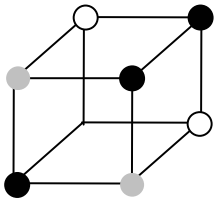
Trivial



$A=\{x\}$ $B=\{yz\}$

$(x,y,z) = (x,0,0)_A + (0,y,z)_B$

Semi-trivial

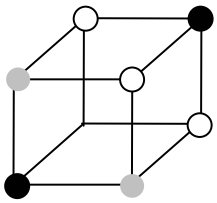


$A=\{x\}\oplus\{yy\}$ $B=\{y\}\cup\{z\}$

$(x,y,z) = (x,u,u)_A + (0,y-u,z-u)_B$

$[u=\inf(y,z)]$

Irréductible (d'ordre 2*)* ***Type (iii)***



$A=\{x\}\cup\{yy\}$ $B = (\{y\}\cup\{z\})\oplus\{xxx\}$

$(x,y,z) = (0,v,v)_A + (x,y-v,z-v)_B$ $[u = x]$

$(x,y,z) = (x-u,0,0)_A + (u,y,z)_B$ $[u \neq x]$

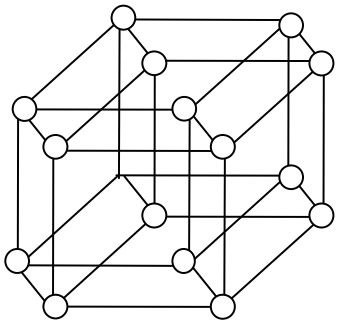
$[u=\inf(x,y,z)]$ $[v=\inf(y-u,z-u)]$

Le type (ii) correspond à un squelette suturé (voir plus tard)

Squelettes sains de dimension 4.

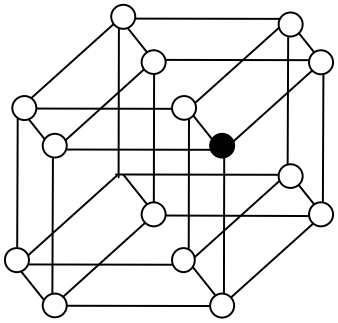
4B

Trivial



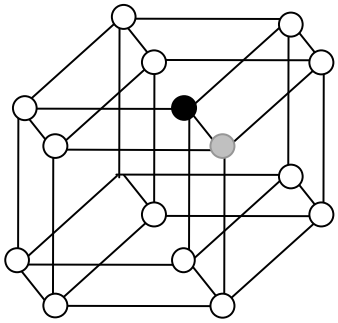
4B

Irréductible (ordre 1)

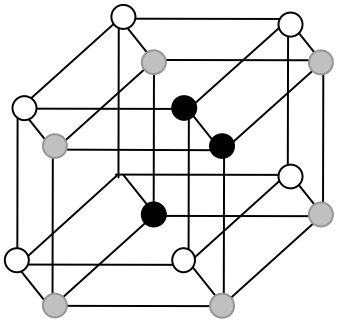


4B

Semi-triviaux

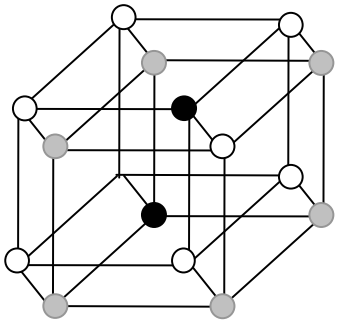


3B



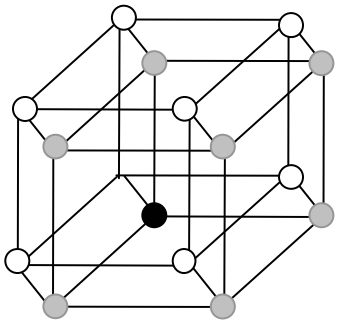
3B

Irréductible (ordre 2)



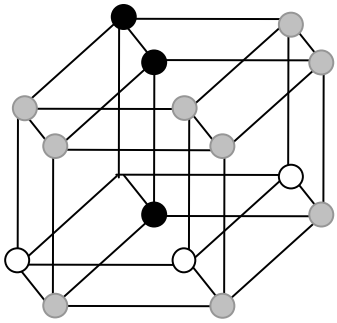
3B

Trivial



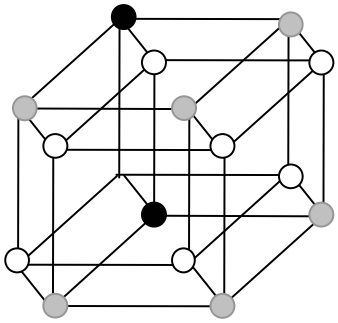
2B

Trivial

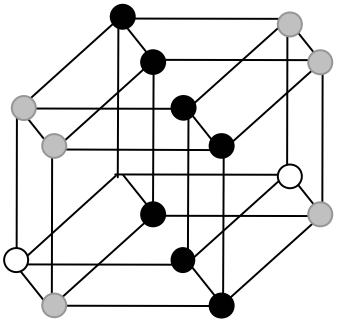


2B

Semi-trivial

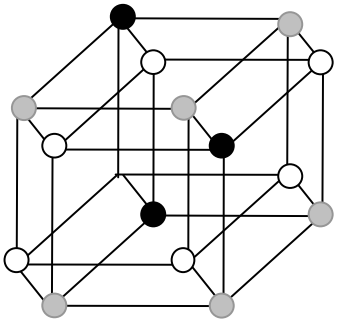


Réplique
(A ~ B)

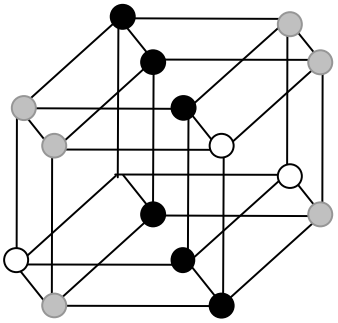


2B

Irréductible
(ordre 2)

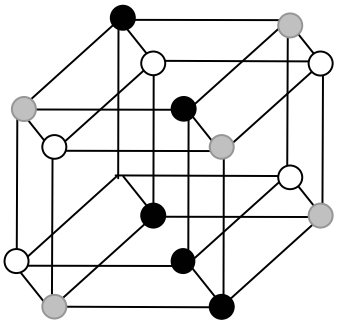


Réplique
(A ~ B)



2B

Semi-trivial



Un squelette sain de dimension 5 pour finir.

Montage du squelette ou données génératrices

$10000 \in B$ $11000 \in A$ $11001 \in B$ $11111 \in A$
$01000 \in B$ $00110 \in B$
$00100 \in A$
$00010 \in A$
$00001 \in A$

La justification du fait que ces seules données suffisent à déterminer complètement le squelette sain sera donnée plus tard en toute généralité.

Pour l'instant, nous nous contentons d'indiquer comment sont effectivement déterminées les natures (B ou blanc, A ou noir, A+B ou gris) de tous les sommets de l'hypercube (il y en a 32 en comptant 00000, qui est commun à A et B).

Déductions. ("$\in$ A+B" signifie " $\exists \in$ B et $\exists \in$ A " , i.e. « a une décomposition non triviale ») :

« ***** $\in$ A » et « ***** $\in$ B » sont soit des données génératrices (recopie pure et simple) soit des déductions indiquées entre parenthèses, et dans ce cas :

« ***** $\in$ A+B » signifie « $\exists$***** $\in$ B et $\exists$***** $\in$ A» (***** a une décomposition non triviale) l'argument numérique est alors spécifié : il s'agit soit d'une indication de la décomposition soit d'une indication de non unicité de décomposition explicite.

$10000 \in B$
$01000 \in B$
$00100 \in A$
$00010 \in A$
$00001 \in A$

$11000 \in A$
$10100 \in A+B$
$10010 \in A+B$
$10001 \in A+B$
$01100 \in A+B$
$01010 \in A+B$
$01001 \in A+B$
$00110 \in B$
$00101 \in A$ ($\exists \in B : 00101_B + 00010_A = 00110_B + 00001_A$)
$00011 \in A$ ($\exists \in B : 00011_B + 00100_A = 00110_B + 00001_A$)

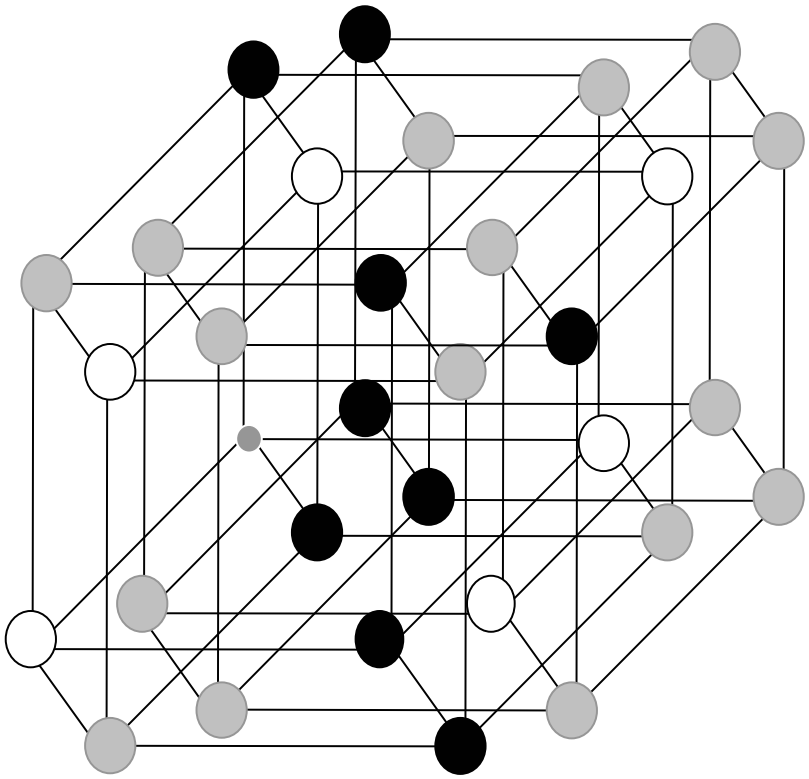
$11100 \in A$ ($\exists \in B : 11100_B + 00011_A = 11111_A$ et $\exists \in A+B$)
$11010 \in A$ ($\exists \in B : 11010_B + 00100_A = 11110 = 11000_A + 00110_B$ et $\exists \in A+B$)
$11001 \in B$

$10110 \in B$ ($\exists \in A : 10110_A + 01000_B = 11110 = 11000_A + 00110_B$ et $\exists \in A+B$)
$10101 \in A+B$ ($10000_B + 00101_A$)
$10011 \in A+B$ ($10000_B + 00011_A$)
$01110 \in B$ ($\exists \in A : 01110_A + 10000_B = 11110 = 11000_A + 00110_B$ et $\exists \in A+B$)
$01101 \in A+B$ ($01000_B + 00101_A$)
$01011 \in A+B$ ($01000_B + 00011_A$)
$00111 \in A+B$ ($00110_B + 00001_A$)

$11110 \in A+B$ ($11000_A + 00110_B$)
$11101 \in A+B$ ($11001_B + 00100_A$)
$11011 \in A+B$ ($11001_B + 00010_A$)
$10111 \in A+B$ ($10110_B + 00001_A$)
$01111 \in A+B$ ($01110_B + 00001_A$)

$11111 \in A$

Ce squelette sain de dimension 5 est irréductible d'ordre 3



Retenons essentiellement que les squelettes sains offrent une bonne typologie de *certaines* décompositions directes additives des puissances de **N**, mais ***pas toutes***.
Pour une typologie plus complète, on doit introduire les notions de *suture* et de *terminaison* qui permettent de définir des *squelettes* plus généraux que les squelettes sains envisagés jusqu'ici. Il paraît sage de s'habituer un peu aux squelettes « sains » avant d'aborder le cas général.