

C. P. Bruter

Sur la construction des nombres

0. INTRODUCTION

On supposera connues, dans cet article d'exposition rédigé en 1971, les notions élémentaires de théorie des ensembles. Elles suffisent pour présenter et dérouler un mécanisme formel qui permet de construire les "nombres". Ce mécanisme repose sur la vieille notion d'extension. Nous avons formulé dans [1] le problème d'extension sous une forme très générale. Nous traitons dans ce texte un exemple élémentaire de tel problème. Nous remercions P. Samuel d'avoir bien voulu relire le manuscrit, et de ses pertinentes critiques.

1. JUSTIFICATION DE LA MÉTHODE

La notion d'extension est définie, dans les livres d'Algèbre, au moment où l'on aborde les extensions quadratiques. Auparavant, on a étudié, tant bien que mal, par des méthodes différentes et souvent laborieuses, la construction des entiers et des fractionnaires; cette dernière pose souvent des problèmes d'assimilation à l'étudiant. Par ailleurs, les réels et les complexes lui sont en général imposés, soit par définition, soit en admettant des théorèmes qui nécessitent déjà, pour leur compréhension, la connaissance de bonnes notions d'algèbre ou d'analyse.

Il est sans doute préférable, pour construire cette diversité de "nombres", de mettre en oeuvre une seule méthode générale, de conception très simple. L'esprit y voit clair, assimile vite, enrichit ses capacités créatrices, puisqu'il

se permet de postuler l'existence d'un objet qu'il n'a pu encore saisir dans sa totalité. L'avantage pédagogique est certain.

Notons de plus que la présentation choisie permet d'introduire les opérations de "multiplication", "puissance", comme résultats de l'action d'un demi-groupe sur un groupoïde: on se familiarise déjà avec la notion importante de système dynamique.

L'exposition qui suit, à l'envers de la véritable démarche pédagogique, est didactique, et parfois condensée. Le lecteur voudra bien nous pardonner d'avoir sacrifié à la raisonnable tradition stylistique mathématique: elle vise à l'économie des moyens.

2. OPÉRATIONS ENGENDRÉES PAR UNE OPÉRATION FONDAMENTALE

Définition 1: Un p -groupoïde $p(E, \circ)$, ou groupoïde partiel, est la donnée d'un ensemble E et d'une loi de composition binaire \circ définie entre certains couples $(x, y) \in E \times E$. Si cette loi est définie entre tous les couples (x, y) de $E \times E$, on dit qu'on a un groupoïde (E, \circ) . Si plusieurs lois de composition binaires sont définies sur E , on dit qu'on a un $poly-p$ -groupoïde.

Définition 2: Un p -groupoïde $p(E, \circ)$ est une chaîne si la loi \circ vérifie les règles suivantes:

- (i) $p(E, \circ)$ est un p -groupoïde neutre à gauche: $x \circ y$ défini $\Rightarrow x \circ y = y$
- (ii) antisymétrie : $x \circ y$ non défini $\Rightarrow y \circ x$ défini
- (iii) réflexivité : $x \circ x = x$
- (iv) linéarité — associativité — transitivité : $(x \circ y) \circ z = x \circ (y \circ z)$ quand ces opérations sont définies.
On convient alors d'écrire $(x \circ y) \circ z = x \circ y \circ z$

Une chaîne possède un *minorant universel*, noté O , s'il n'existe pas $x \neq O, x \in E$ tel que $x \circ O = O$.

Définition 3: Un p -groupoïde $p(E, \circ)$ possède un ensemble B de *générateurs* si tout élément de E s'obtient en composant, répétitions permises, des éléments de B . Si $|B| = 1$, le p -groupoïde est dit *monogène*; on note 1 le générateur correspondant.

Définition 4: On appelle *entiers naturels modulo $n+1$* les éléments de l'ensemble sous-jacent à un $poly-p$ -groupoïde $p(N/n+1, \circ, +)$ qui possède les propriétés suivantes:

- (i) $p(N/n+1, \circ)$ est une chaîne finie avec minorant universel O .
- (ii) $\forall k \in N/n+1, k+O = O+k = k : O$ est neutre à droite et à gauche.

(iii) $(N/n+1 - (N/n+1 - \{O\}), +)$ est un p -groupeïde monogène de sorte que

$$x+1 = y \Rightarrow x \circ y = y = 1+x$$

On note $N/n+1 = \{O, 1, 2, \dots, n\}$

Comme on le remarque, l'opération $n+1$ n'est pas définie. Le problème est alors le suivant: agrandir, étendre l'ensemble $N/n+1$ en un ensemble N/m de manière à pouvoir plonger $p(N/n+1, \circ, +)$ dans $p(N/m, \circ, +)$ où l'opération $n+1$ ait un sens. On notera $N/n+2$ le plus petit ensemble dans lequel le plongement précédent est possible. (On a laissé au lecteur le soin de définir les termes plonger et plongement). En poursuivant ad libitum un tel processus d'extension, on construit ainsi $N/\infty = N$, ensemble des entiers naturels.

On voit ainsi qu'en partant de l'ensemble des entiers modulo 2, soit $\{0, 1\}$, on construit sans difficulté: $N = \{O, 1, 2, \dots, n, \dots\}$.

Définition 5: On appellera (p) -demi-groupe $D_p(E, \circ)$ tout (p) -groupeïde pour la loi associative \circ (voir définition 2, (iv)). Si $x \circ y = y \circ x$ la loi est commutative.

Proposition 1: $D(N, +)$ est un demi-groupe commutatif monogène à élément neutre.

Démonstration abrégée: $D(N, +)$ possède O comme élément neutre d'après (ii). La loi $+$ est associative; c'est trivial si x, y ou $z = O$ d'après (ii), et si $x = y = 1$ d'après (iii). La démonstration peut se poursuivre par récurrence en tenant compte du fait que $D(N, +)$ est un groupeïde monogène. La commutativité de la loi résulte de l'associativité et de (iii). C. Q. F. D.

On représente souvent la ligne d'évolution d'un objet dans l'espace-temps par la trajectoire d'un point dans cet espace. Le point, qui symbolise l'objet, est soumis localement à l'action d'une force qui le fait mouvoir sur sa trajectoire; dans un voisinage du point considéré, les déplacements qu'il effectue forment un groupe qui, en somme, „opère” sur les images successives du point. On peut naturellement affaiblir ces données, et supposer que la trajectoire est un p -groupeïde $p(E, \circ)$ sur lequel opère localement un p -demi-groupe $D_p(F, \square)$.

Définition 6: On dit que le p -demi-groupe monogène $D_p(F, \square)$ opère sur le p -groupeïde $p(E, \circ)$ s'il existe une application $h: F \times E \rightarrow E$, on note $h(f, e) = f * e$, qui vérifie les propriétés suivantes:

(j) $h(1, e) = e$

(jj) $h(x \square y, e) = h(x, e) \circ h(y, e)$ chaque fois que ces opérations sont définies. L'action d'un p -demi-groupe sur un p -groupeïde $p(E, \circ)$ définit donc une nouvelle loi de composition entre les éléments de E : on l'appelle fonction puissance pour les opérations (\square, \circ) .

Le modèle devient plus signifiant lorsqu'on choisit comme p -demi-groupe $D(N, +)$. Dans ce cas, on adjoint $O \in N$ à E et on pose:

$$h(O, e) = O * e = e * O = O$$

$$h(n, e) = \underbrace{e \circ e \circ \dots \circ e}_{n \text{ fois}} = n * e = e^{n(\circ)}.$$

Si $p(E, \circ)$ est un demi-groupe monogène, on peut alors définir entre tous les couples d'éléments de $E \cup O$, la loi $*$ par la relation $f * g = m * (m * 1)$ où $f = m * 1$, $g = n * 1$.

Il est alors clair que:

Proposition 2: $D_p(E \cup O, *)$ est un p -demi-groupe.

Exemple: On considère l'action du demi-groupe des entiers naturels sur lui-même. Alors

$$h(3+4, 5) = h(3, 5) + h(4, 5) = 5, \quad 7(+)= (5+5+5) + (5+5+5+5) = 35$$

$D(N, *)$ est noté plus communément $D(N, \times)$: $3 \times 2 = 3 \times (1+1) = (1+1) + (1+1) + (1+1) = 6$.

On peut renouveler l'action de $D(N, +)$: sur $D_p(E \cup O, *)$ pour obtenir $D_p(E \cup O, **)$; sur $D_p(E \cup O, **)$ pour obtenir $D_p(E \cup O, ***)$, etc.

Exemple: L'action de $D(N, +)$ sur $D(N, \times)$ amène à définir la fonction puissance traditionnelle: $h(4, 3) = 3 \times 3 \times 3 \times 3 = (3)_\times^4 = 3^4$ qu'on peut appeler fonction puissance multiplicative première. On peut ensuite définir la fonction multiplicative seconde, $h(3, 4^2) = (4^2)^3$, troisième, etc.

On peut également, par exemple, faire agir $D_p(E \cup O, **)$ sur $D_p(E \cup O, ****)$. On construit ainsi, formellement, un ensemble non fini de p -demi-groupes à partir d'un seul p -groupeïde de base $p(E, \circ)$. On obtient un poly- p -groupeïde qui est un p -demi-groupe pour toute opération différente de l'opération fondamentale \circ . Puisque les opérations $** \dots *$ traduisent la prise en compte en bloc d'un grand nombre d'opérations \circ , il est clair que $p(E, \circ)$ et $p(E, ** \dots *)$ ont mêmes propriétés.

3. EXTENSIONS DE P-GROUPOÏDES

Au lieu d'étudier $p(E \cup O, \circ, *, **, \dots)$ on peut de façon plus générale l'intéresser à un poly- p -groupeïde muni de lois de composition binaires que nous désignerons par $\tilde{1}, \tilde{2}, \dots, \tilde{n}, \dots$, et chercher à résoudre des „équations” définies sur ce poly- p -groupeïde.

Définition 7: On appelle *monôme* par rapport à l'opération \tilde{i} , et à une indéterminée X , de degré n , toute expression de la forme

$$M_{\tilde{i}}(X) = e \underbrace{\tilde{i} X \tilde{i} X \tilde{i} \dots \tilde{i} X}_{n \text{ fois}} \quad (e \in E)$$

On peut convenir également de noter $M_{\tilde{i}}(X) = e \tilde{i} X_{\tilde{i}}^n$.

L'indéterminée X représente une case vide: ce qu'elle peut contenir n'est pas déterminé à priori.

On appelle *polynôme* par rapport aux opérations $\tilde{i}, \tilde{j}, \dots, \tilde{k}$, et à une indéterminée X , toute expression de la forme

$$P(\tilde{i}, \tilde{j} \dots \tilde{k})(X) = e_1 \tilde{i} X_i^{n_1} \tilde{j} (f_1 \tilde{j} X_j^{m_1}) \dots \tilde{i} (e_2 \tilde{i} X_i^{n_2}) \dots \tilde{k} (g_p \tilde{k} X_k^{n_k, p})$$

où le nombre d'opérations $\tilde{i}, \tilde{j}, \dots, \tilde{k}$ est fini.

On note par $S(\tilde{i}, \tilde{j}, \dots, \tilde{k})(X)$ une expression de même type que celle de $P(\tilde{i}, \tilde{j}, \dots, \tilde{k})(X)$ où une au moins des opérations $\tilde{i}, \tilde{j}, \dots, \tilde{k}$ apparaît un nombre non fini de fois. On dit que $S(\tilde{i}, \tilde{j}, \dots, \tilde{k})(X)$ est une *série entière*.

Les éléments e_i, f_i, \dots sont les *coefficients* du polynôme ou de la série entière.

Exemple: Considérons $p(E \cup O, \circ, *) = D(N, +, X)$, un monôme à une indéterminée: de la forme $m + nX$ pour l'opération $+$; de la forme mX^n pour l'opération \times . Un polynôme s'écrit $m + nX + p_1 X^{q_1} + \dots + p_k X^{q_k}$ ($k < \infty$).

Définition 8: On dit que le poly-groupeïde $\Pi = (E, \dots, \tilde{j}, \dots)$ est une *P-extension régulière* (res. *S. extension régulière*) ou *extension (régulière) algébrique* (resp. *transcendante*) du poly-groupeïde $I = (E, \dots, \tilde{j}, \dots)$ par rapport aux opérations $\tilde{i}, \tilde{j}, \dots, \tilde{k}$ sur $E' \subseteq E$ si:

(i): Les groupeïdes I et II ont mêmes lois de composition $\tilde{i}, \tilde{j}, \dots, \tilde{k}$ qui satisfont aux mêmes propriétés.

(ii): Quel que soit $g \in E'$, l'équation $P(\tilde{i}, \tilde{j}, \dots, \tilde{k})(x) = g$ (resp. $S(\tilde{i}, \tilde{j}, \dots, \tilde{k})(x) = g$) a un sens et une solution (notée $g^{-1}(P, g)$ (resp. $g^{-1}(S, g)$) dans II mais non dans I.

L'élément du type $g^{-1}(P, g)$ est dit *algébrique* sur E (resp. $g^{-1}(S, g)$ est transcendant sur E , s'il n'est pas algébrique sur E).

On n'établit pas ici l'existence de telles extensions dans le cas le plus général. On se limite au cas *signifiant* des „nombres”.

4. EXTENSIONS ALGÈBRIQUES D'ORDRE 1 (OU FRACTIONNAIRE) DE $D(N, \circ, +)$

(Un exposé moins formel pourra débiter par la présentation de N ; on peut ensuite montrer l'action de $D(N, +)$ sur lui-même, sur $D(N, \times)$, etc..., et introduire sur $D(N, +)$ la définition d'une extension).

On peut donner à la proposition suivante un énoncé plus affaibli et plus général:

Proposition 3: *Le monôme $x + n = O$ définit une extension de $D(N, \circ, +)$, soit $D(Z, \circ, +)$, indépendante du choix de $n \in N - O$.*

Démonstration: Supposons $n = 1$. Il n'existe pas d'élément de N tel que $1 + 1 = O$ de par la définition (iv) de N . Nous allons postuler l'existence d'une extension de $D(N, +)$ définie par le monôme $x + 1 = O$; soit $D(Z, +)$ cette extension: nous allons la construire, ce sera d'ailleurs la seule qu'on puisse construire de manière à respecter la définition 8.

Soit alors $e \in N$ un élément tel que $e+1 = O$. On convient d'écrire $e = -1$. Cet élément doit être unique: en effet lorsque l'équation $mx+n = O$ a une solution dans N , cette solution est unique; d'après la définition 8 (i) cette propriété est vraie dans toute extension de $D(N, +)$.

Puisqu'on peut composer tout élément $n \in N$ avec lui-même par l'opération $+$, il en est de même avec tout élément de Z (définition 8 (ii)). Par suite $e' = (-1) + (-1)$ est un élément de Z . La loi $+$ est associative et commutative sur N ; il doit en être de même sur Z . Par suite

$$((-1) + (-1)) + (1+1) = e' + 2 = O.$$

Comme il n'existe pas d'élément $e' \in N$ tel que $O = e' + 2$, $e' \in Z - N$. On convient de poser $e' = -2$; cet élément est encore unique.

On poursuit ce mode de raisonnement pour construire $-3, -4$, etc... Finalement $Z = N \cup -N$ où $-O = O$.

Si $n \neq O, 1$, on procède de la même façon pour construire Z . Il est facile de vérifier que la loi $+$ a mêmes propriétés dans $D(Z, +)$ et $D(N, +)$.

Enfin cette extension doit être compatible avec la loi d'ordre \circ sur N qu'il faut étendre sur Z : la relation $(-1) + 1 = O$ implique d'après la définition (iv) des entiers naturels que $(-1) \circ O = O$, et de façon générale on a $(-p) + 1 = -(p-1)$ donc $(-p) \circ (-p-1) = -(p-1)$.

Définition 9: $D(Z, \circ, +)$ est le demi-groupe des entiers. Les éléments de $N - O$ en sont les positifs; ceux de $(-N) - O$ en sont les négatifs.

La proposition suivante se démontre exactement comme la précédente (et la contient, $m = n = 1$). Etant donnée l'unicité de la construction, on peut parler de l'extension.

Proposition 4: $N^+[m, n] = \left\{ p \frac{n}{m}; p \in Z \right\} \cup N$ est l'ensemble des éléments sous-jacents à l'extension de $D(N, \circ, +)$ définie par le monôme $mx+n = O$, $m, n \in N - O$.

Remarque 1: Si x est solution de l'équation $mx+n = O$, on aura posé par convention $x = \frac{-n}{m}$ (n est le numérateur, m le dénominateur de la fraction $\frac{-n}{m}$).

Mais x sera également solution de l'équation $q(mx+n) = O$ soit $qmx+qn = O$. Par suite $N^+[m, n] = N^+[qm, qn]$ et puisque x est solution de $qmx+qn = O$, $x = \frac{-qn}{qm} = \frac{-n}{m}$ quel que soit $x \in N - O$.

On peut réitérer le processus d'extension:

Proposition 5: $N^+[m, n][p, q] = \left\{ \frac{rn}{m} + \frac{sq}{p}; r, s \in Z \right\} \cup N$ est l'ensemble des éléments sous-jacents à l'extension de $D(N^+[m, n], \circ, +)$ définie par le monôme $px+q = O$.

D'après la remarque précédente:

$$\frac{rn}{m} + \frac{sq}{p} = \frac{rpn}{mp} + \frac{sqm}{pm} = \frac{rpn + sqm}{pm}.$$

Définition 10: On peut convenir de dire que $D(N^+[m, n], \circ, +)$ est une *extension algébrique d'ordre 1* (ou *extension fractionnaire*), *simple* pour l'addition, que $D(N^+[m, n][p, q], \circ, +)$ est une extension fractionnaire double pour l'addition, etc...; enfin $N^+[m, n][\dots][p, q][\dots] = \mathcal{Q}$ est l'ensemble des *fractions*, ensemble *clos* pour les extensions fractionnaires puisque $\mathcal{Q}^+[r, s] = \mathcal{Q}$.

Nous avons épuisé les extensions fractionnaires — elles sont relatives au groupoïde $(E \cup O, \circ)$, nous allons aborder les extensions multiplicatives relatives au polygroupoïde $(E \cup O, \circ, *)$. De même qu'on vient d'étudier $N^+[X]$, $N^+[X_1][X_2], \dots, \mathcal{Q} = \mathcal{Q}^+[X]$, on peut maintenant étudier les $N^+[X^2]$ définis comme des extensions de N par des polynômes du type $mx^2 + n = O$, les $N^+[X_1^2][X_2^2], \dots, \mathcal{Q}^+[X^2]$, les $N^+[X][X^2], \dots$, les $N^+[X^p], \dots, \mathcal{Q}^+[X_1^2][X_2^2] \dots$, avec cette particularité: nous travaillons sur $(N, +, \times)$ comme polygroupoïde de base.

La première question qui se pose est celle de savoir si dans l'extension de (E, \circ) qui définit (F, \circ) , la loi $*$ reste valable entre tous les couples d'éléments de F et de quelle manière elle opère. Dans les cas signifiants $Z, N^+[m, n][p, q], \mathcal{Q}$ qui nous intéressent, il est facile de voir ce qu'il en est:

(i) pour Z , obtenu comme extension de $(N, +, \times)$ par le monôme $x+1 = O$: puisque $x+1 = O$, $2 \times (x+1) = 2 \times O = O = 2 \times (x) + 2 \times 1 = O$: d'où l'on déduit que $2 \times (-1) = -2$, et plus généralement $n \times (-p) = -(n \times p)$. En particulier si $n = x+1 = O$, $(-1) \times (x+1) = O = (-1) \times (x) + (-1) \times 1 = O$ d'où la règle $(-1) \times (-1) = +1$ et plus généralement:

$$(-n) \times (-p) = n \times p$$

(ii) pour l'extension fractionnaire $N^+[m, n][p, q]$: l'opération $\frac{n}{m} \times \frac{q}{p}$ est-elle définie dans $N^+[m, n][p, q]$? Ce n'est pas vrai en général. Il nous faut alors introduire les extensions fractionnaires compatibles avec la multiplication:

$$N^+[m, n][p, q] = N^+[m, n][p, q] \cup \left\{ k \times \frac{n \times q}{m \times p}; k \in Z \right\}.$$

(iii) Pour \mathcal{Q} : puisque \mathcal{Q} est clos pour l'extension fractionnaire, toute expression $\frac{n \times q}{n \times p} = \frac{n}{m} \times \frac{q}{p}$ est parfaitement définie.

Remarque 2: Notons que toute extension $(E, \underbrace{** \dots}_{k \text{ fois}})$ de $(E, \underbrace{** \dots}_{k' < k})$

(j) est aussi une extension de $(E, \underbrace{** \dots}_{k' < k})$;

(jj) est compatible avec l'opération (** ...) (k' ou k'' fois): en effet $(E, \underbrace{** \dots}_{k' < k})$.
 est un „cas particulier” de $(E, \underbrace{** \dots}_k)$.

5. EXTENSIONS ALGÈBRIQUES D'ORDRE n SUPÉRIEUR À 1

Nous nous trouvons en ce moment précis au point de rencontre avec les expositions classiques sur les nombres que donnent les livres d'algèbre, puisqu'il conviendrait maintenant d'aborder les extensions d'ordre 2 ou quadratiques, d'ordre 3 etc..., pour en venir finalement aux complexes et aux réels. Il a semblé prudent de renvoyer pour l'instant aux ouvrages classiques.

BIBLIOGRAPHIE

- [1] *Sur la Nature des Mathématiques*, Gauthier-Villars, Paris 1973.