Gerbes primitives

Friedrich Wehrung

ALGÈBRE. Gerbes primitives. Friedrich WEHRUNG.

Résumé. - On étudie ici certaines structures distributives à gauche (gerbes) que nous qualifierons de linéaires, pour lesquelles on peut définir un certain invariant que nous appellerons hauteur. Nous montrons que les gerbes finies obtenues par R. Laver par passage au quotient de la gerbe (hypothétique) associée à une injection élémentaire sont exactement les gerbes linéaires de hauteur 1.

Primitive left-distributive structures.

Abstract. - *We study here certain left-distributive structures (clumps) which we will qualify linear, for which one can define an invariant which we will call height. We show that the finite clumps obtained by R. Laver by quotienting the (hypothetic) clump associated with an elementary embedding are exactly the linear clumps of height 1.*

Abridged English Version - As in [1], we will call a *clump* (or *LD-magma*) a structure $(\mathfrak{g}, *)$ such that $*$ is a binary operation on $\mathfrak{g}$ which is *left-distributive*, *i.e.* it satisfies the identity

$$x * (y * z) = (x * y) * (x * z).$$

The theory of clumps has recently got benefit from a significant breakthrough by R. Laver (*see* [4]), who proved that the monogenic clump of set theory $\mathfrak{a}^j$ generated by a non-trivial elementary embedding j from a limit rank into itself is free, and P. Dehornoy (*see* [3]) who proposed an alternative proof, showing the algebraic hard core of the result. Moreover [5], for every positive integer n, Laver defines a quotient clump $\mathfrak{p}_n$ of $\mathfrak{a}^j$ which has exactly 2^n elements, and notices that its operation satisfies simple recurrence relations, given here by (G1), (G2), (G3), which are enough to compute the whole operation. This makes the status of the $\mathfrak{p}_n$ appear as rather strange, since without any (very) large cardinal assumption, there is no known natural example of free clump - the best attempt in that direction perhaps being the one in [2]. On the other side, we will provide here several completely *algebraic* characterizations of the clumps $\mathfrak{p}_n$, independent from any large cardinal assumption *a priori*. Nevertheless, we emphasize that we are indebted to Laver for having accepted to communicate us the basic ideas of the construction of the $\mathfrak{p}_n$'s, which are all his.

If $(\mathfrak{g}, *)$ is a clump and if x is an element of $\mathfrak{g}$, we will define the sequence $(x^{[n]})_{n\in\mathbb{N}\setminus\{0\}}$ by the following recurrence relations:

$$x^{[1]} = x \text{ and } (\forall n \in \mathbb{N}\setminus\{0\})(x^{[n+1]} = x^{[n]} * x).$$

We will say that an element x of $\mathfrak{g}$ is a *linear generator* of $\mathfrak{g}$ when we have

$$\mathfrak{g} = \{x^{[n]} : n \in \mathbb{N}\setminus\{0\}\},$$

and that $\mathfrak{g}$ is *linear* when it has a linear generator. If $\mathfrak{g}$ is linear finite of size n, then every generator of $\mathfrak{g}$ is linear and if x is one of them, then the unique h in $[1,\ n]$ such that $x^{[n+1]} = x^{[h]}$ does not depend on x; we will call it the *height* of $\mathfrak{g}$. We will say that $\mathfrak{g}$ is *primitive* when it has height 1. Finally, we will define the height of any infinite linear clump to be infinite; the latter definition is not vacuous, since there are some simple examples, due to A. Sesboüé, of infinite linear clumps.

PROPOSITION 3. - *Let $\mathfrak{g}$ be a monogenic clump. Then:*

(i) *Every monogenic subclump of $\mathfrak{g}$ is a quotient of $\mathfrak{g}$.*

(ii) *If $\mathfrak{g}$ is linear, then every quotient clump of $\mathfrak{g}$ is linear of height at most the height of $\mathfrak{g}$.* ∎

Now, for all x and n in $\mathbb{N}\backslash\{0\}$, let x mod n be the unique y in the interval $[1,\ n]$ (of $\mathbb{N}$) such that x and y are congruent modulo n. For every n in $\mathbb{N}\backslash\{0\}$ and every binary operation $*$ on $[1,\ n]$, consider the following three conditions on $*$:

(G1) $(\forall x \in [1,\ n])\big(x * 1 = (x+1) \bmod n\big)$;

(G2) $(\forall x, y \in [1,\ n[)\big(x * (y+1) = (x * y) * (x+1)\big)$;

(G3) $(\forall y \in [1,\ n])(n * y = y)$.

LEMMA 4. - *For every n in $\mathbb{N}\backslash\{0\}$, there is one and only one binary operation (which we will denote by $*_n$) on $[1,\ n]$ satisfying (G1), (G2), (G3). Moreover, for all x, y in $[1,\ n]$, we have*

$$x < n \ \Rightarrow\ x *_n y > x.$$ ∎

It is easy to see that in fact, the only primitive clumps are exactly those $\mathfrak{g}_n$ such that $\mathfrak{g}_n$ is a clump. These are given by the following theorem:

THEOREM 11. - *Let n in $\mathbb{N}\backslash\{0\}$. Then $\mathfrak{g}_n$ is a clump if and only if n is a power of 2; therefore, the primitive clumps are exactly the $\mathfrak{g}_{2^m}$ where m is a positive integer.* ∎

It follows that if there is a non-trivial elementary embedding from a limit rank into itself, then for every positive integer n, the Laver clump $\mathfrak{p}_n$ is isomorphic to $\mathfrak{g}_{2^n}$. This leads to the natural definition $\mathfrak{p}_n = \mathfrak{g}_{2^n}$, even without making *a priori* any large cardinal assumption.

Thus, it follows from proposition 3 that for every positive integer n, every *monogenic* subclump or every quotient clump of $\mathfrak{p}_n$ is isomorphic to some $\mathfrak{p}_m$, where $m \leq n$.

We finally conclude with a new and simple presentation of the clumps $\mathfrak{p}_n$.

COROLLARY 12. - *Let n in $\mathbb{N}\backslash\{0\}$, let m be the largest integer such that 2^m divides n. Then the clump $\mathfrak{h}_n$ defined by one generator 1 and the relation $1^{[n+1]} = 1$ is isomorphic to $\mathfrak{p}_m$.* ∎

Conformément à [1], nous appellerons *gerbe* tout magma $(\mathfrak{g}, *)$ distributif à gauche, *i.e.* satisfaisant l'identité

$$x * (y * z) = (x * y) * (x * z).$$

L'étude des gerbes reçut récemment une importante contribution par R. Laver, qui prouva (*voir* [4]) que la gerbe de théorie des ensembles $\mathfrak{a}^j$ construite à partir de l'itération d'une injection élémentaire non triviale j est exactement la gerbe monogène libre, et par P. Dehornoy, qui proposa (*voir* [3]) une preuve différente montrant le "noyau dur" algébrique

du résultat. De plus [5], Laver définit pour tout entier naturel n un certain quotient $\mathfrak{p}_n$ de $\mathfrak{a}^j$ qui a exactement 2^n éléments, et dont il constata que la loi peut être engendrée par des relations de récurrence simples - données ici par (G1), (G2), (G3). Les gerbes $\mathfrak{p}_n$ sont alors en situation un tant soit peu ambiguë, car ce sont des quotients finis (donc parfaitement appréhendables au sens intuitif) d'un objet hypothétique (la gerbe $\mathfrak{a}^j$) dont aucune construction "naturelle" sans (très) grands cardinaux n'est connue (*voir* [2]). Nous présentons ici plusieurs caractérisations parfaitement *algébriques* (et indépendantes de toute hypothèse de grand cardinal) des $\mathfrak{p}_n$, qui permet d'en obtenir facilement quelques propriétés dont la démonstration serait beaucoup plus malaisée à partir de la définition originelle. Ainsi, notre démarche est une sorte de "réciproque" de celle de Laver, dans le sens où notre point de départ est purement algébrique et nous amène à l'unicité des quotients de Laver, alors que ce dernier part de $\mathfrak{a}^j$ et en définit des quotients de façon "concrète". Ceci étant, nous insistons sur le fait que l'idée originale de considérer les gerbes $\mathfrak{p}_n$ et leur définition (dans le cas où elles existent) par les règles (G1), (G2), (G3) revient entièrement à Laver.

Si $(\mathfrak{g}, *)$ est une gerbe et x est un élément de $\mathfrak{g}$, on définit la suite $(x^{[n]})_{n\in\mathbb{N}\setminus\{0\}}$ des *arêtes gauches* basées sur x par la relation de récurrence suivante:

$$x^{[1]} = x \text{ et } (\forall n \in \mathbb{N}\setminus\{0\})(x^{[n+1]} = x^{[n]} * x).$$

Nous dirons qu'un élément x de $\mathfrak{g}$ est un *générateur linéaire* de $\mathfrak{g}$ quand on a

$$\mathfrak{g} = \{x^{[n]} : n \in \mathbb{N} \setminus \{0\}\},$$

et nous dirons que $\mathfrak{g}$ est *linéaire* quand elle admet au moins un générateur linéaire, de sorte que toute gerbe linéaire est monogène; la réciproque est fausse.

LEMME 1. - *Soient P et Q deux éléments du magma libre monogène, soit $\mathfrak{g}$ une gerbe monogène, soit x un générateur de $\mathfrak{g}$ tel que $P(x) = Q(x)$. Alors pour tout y dans $\mathfrak{g}$, on a $P(y) = Q(y)$.*

Démonstration. - D'après la condition de distributivité à gauche, il est clair que l'ensemble X des éléments y de $\mathfrak{g}$ tels que $P(y) = Q(y)$ est stable par translation à gauche, c'est donc une sous-gerbe de $\mathfrak{g}$. De plus, x est un élément de X, d'où $X = \mathfrak{g}$. ∎

On en déduit en particulier que deux générateurs d'une gerbe monogène satisfont les mêmes identités. On en déduit facilement le résultat suivant:

LEMME 2. - *Soit $\mathfrak{g}$ une gerbe linéaire finie de cardinal n, soit x un générateur de $\mathfrak{g}$. Alors*

(i) *L'application de $[1,\ n]$ vers $\mathfrak{g}$ qui à k associe $x^{[k]}$ est une bijection.*

(ii) *Tout générateur de $\mathfrak{g}$ est linéaire, et l'unique élément h de $[1,\ n]$ tel que $x^{[n+1]} = x^{[h]}$ ne dépend pas de x.* ∎

Nous appellerons l'entier h défini dans le lemme 2 la *hauteur* de $\mathfrak{g}$; nous dirons que toute gerbe linéaire infinie a une hauteur infinie; il existe des exemples simples de gerbes linéaires infinies, dus à A. Sesboüé. Nous dirons qu'une gerbe $\mathfrak{g}$ est *primitive* quand elle est linéaire [finie] de hauteur 1. Le lemme 1 permet alors d'établir le résultat suivant:

PROPOSITION 3. - *Soit $\mathfrak{g}$ une gerbe monogène. Alors:*

(i) *Toute sous-gerbe monogène de $\mathfrak{g}$ est un quotient de $\mathfrak{g}$.*

(ii) *Supposons que $\mathfrak{g}$ soit linéaire. Alors toute gerbe quotient de $\mathfrak{g}$ est une gerbe linéaire de hauteur au plus égale à la hauteur de $\mathfrak{g}$.*

En particulier, il résulte de (ii) que toute gerbe quotient d'une gerbe primitive est primitive.

Démonstration. - Soit $\mathfrak{g}$ une gerbe monogène, soit x un générateur de $\mathfrak{g}$. Soit y un élément de $\mathfrak{g}$. D'après le lemme 1, toute identité satisfaite par x est aussi satisfaite par y, ce qui montre qu'il existe un homomorphisme surjectif ϕ de $\mathfrak{g}$ sur la gerbe monogène $\mathfrak{h}$ engendrée par y tel que $\phi(x) = y$; (i) s'ensuit.

Supposons maintenant $\mathfrak{g}$ linéaire finie de hauteur h, de cardinal n et soit ϕ un homomorphisme surjectif de $\mathfrak{g}$ sur une gerbe $\mathfrak{h}$; si l'on pose $y = \phi(x)$, alors toute identité satisfaite par x l'est aussi (via ϕ) par y, d'où $y^{[n+1]} = y^{[h]}$, donc $y^{[h]}$ appartient à l'ensemble des $y^{[k]}$ pour $k > h$; ceci impose que la hauteur de $\mathfrak{h}$ est au plus égale à h. ∎

Pour tous éléments $x,\ n$ de $\mathbb{N}\backslash\{0\}$, notons x mod n l'unique élément y de l'intervalle $[1,\ n]$ (de $\mathbb{N}$) tel que x et y soient congrus modulo n. Si $\mathfrak{g}$ est une gerbe primitive de cardinal n, désignons par $*$ la loi de composition interne sur $[1,\ n]$ obtenue par transport de structure de $\mathfrak{g}$ par la bijection donnée au lemme 2, (i). Il est alors immédiat que $*$ satisfait les trois propriétés suivantes:

(G1) $(\forall x \in [1,\ n])\big(x * 1 = (x+1) \bmod n\big)$;

(G2) $(\forall x, y \in [1,\ n[)\big(x * (y+1) = (x * y) * (x+1)\big)$;

(G3) $(\forall y \in [1,\ n])(n * y = y)$.

LEMME 4. - *Soit n dans $\mathbb{N}\backslash\{0\}$. Alors il existe une et une seule loi de composition interne $*_n$ sur $[1,\ n]$ satisfaisant* (G1), (G2), (G3). *De plus, on a*

$$(\forall x \in [1,\ n[)(\forall y \in [1,\ n])(x *_n y > x). \qquad (\#)$$

Démonstration. - On montre d'abord (#) par récurrence descendante sur x et ordinaire sur y pour toute loi de composition interne sur $[1,\ n]$ satisfaisant (G1), (G2), (G3). On en déduit alors aisément l'assertion d'unicité par le même type de récurrence. La définition de $x *_n y$ se fait alors aisément par encore le même type de récurrence. ∎

Par la suite, nous noterons $\mathfrak{g}_n$ la structure $([1,\ n], *_n)$. Il s'ensuit alors que déterminer les gerbes primitives revient à déterminer l'ensemble des n tels que $\mathfrak{g}_n$ soit une gerbe.

LEMME 5. - *Soient $n,\ u,\ v$ dans $\mathbb{N}\backslash\{0\}$ tels que $1 \leq u \leq v \leq n$, soit x dans $[1,\ n]$ tel que $(\forall y \in [u,\ v[\ )(x *_n y \neq n)$. Alors l'application qui à tout y dans $[u,\ v]$ associe $x *_n y$ est strictement croissante.*

Démonstration. - Immédiat par récurrence sur y et en utilisant la propriété (#) de $\mathfrak{g}_n$. ∎

Notons que la table de toute gerbe monogène finie possède au moins une colonne constante (c'est une conséquence immédiate du corollaire 2 de [1]). Ici, nous obtenons un énoncé un peu plus précis, obtenu simultanément par A. Sesboüé.

LEMME 6. - *Soit n dans $\mathbb{N}\backslash\{0\}$. Alors les conditions suivantes sont équivalentes:*

(i) $\mathfrak{g}_n$ *est une gerbe;*

(ii) $\mathfrak{g}_n$ *satisfait la condition* (G4): $(\forall x \in [1,\ n])(x *_n n = n)$.

Démonstration. - Si (G4) est satisfait, alors on peut montrer sans difficulté, en utilisant (G1), (G2), (G3), par récurrence descendante sur x puis ordinaire sur y puis ordinaire sur z que pour tous $x,\ y,\ z$ dans $[1,\ n]$, on a $x *_n (y *_n z) = (x *_n y) *_n (x *_n z)$. Réciproquement, $n *_n n = n$ (par (G3)), donc si $\mathfrak{g}_n$ est une gerbe, alors pour tout x dans $[1,\ n]$, on a $x *_n n = (x *_n n) *_n (x *_n n)$, d'où $x *_n n = n$ en raison de (#). ∎

On peut également facilement démontrer par récurrence (en utilisant (#)) les deux lemmes suivants:

LEMME 7. - *Soit n dans $\mathbb{N}\backslash\{0\}$ et soit d un diviseur de n. Alors l'application π_d^n de $\mathfrak{g}_n$ vers $\mathfrak{g}_d$ définie par $(\pi_d^n(x) = x \bmod d)$ est un homomorphisme de magmas.* ∎

LEMME 8. - *Soient n dans $\mathbb{N}\backslash\{0\}$, soient $x,\ y$ dans $[1,\ n]$ tels que $x *_n y = n$. Alors pour tout z dans $[1,\ n]$, on a $x *_n z = x *_n (z \bmod y)$.* ∎

En utilisant le lemme 5, on en déduit alors facilement le

LEMME 9. - *Soient n dans $\mathbb{N}\backslash\{0\}$, soit x dans $[1,\ n]$. Alors il existe un plus petit élément y de $[1,\ n]$ au sens de la divisibilité tel que $x *_n y = n$. De plus, si $x < n$, alors $y < n$.* ∎

COROLLAIRE 10. - *Soit n dans $\mathbb{N}\backslash\{0\}$ tel que $\mathfrak{g}_n$ soit une gerbe. Alors n est une puissance de 2.*

Démonstration. - Soit p un diviseur premier de n; notons $\pi = \pi_p^n$. Par les lemmes 6 et 7 et le fait que $\pi(n) = p$, on a $1 *_p p = p$. Il résulte alors du lemme 9 que si k est le plus petit élément de $[1,\ p]$ tel que $1 *_p k = p$, alors $k < p$ et k divise p; mais p est premier, d'où $k = 1$, d'où $p = 1 *_p k = 1 *_p 1 = 2$, ce qui permet de conclure. ∎

Nous pouvons alors démontrer le

THÉORÈME 11. - *Pour tout n dans $\mathbb{N}\backslash\{0\}$, $\mathfrak{g}_n$ est une gerbe si et seulement si n est une puissance de 2; par suite, les gerbes primitives sont les $\mathfrak{g}_{2^m}$ où m est dans $\mathbb{N}$.*

Démonstration. - L'implication directe est exactement le résultat du corollaire 10. Réciproquement, nous allons montrer par récurrence sur n que pour tout entier naturel n, $\mathfrak{g}_{2^n}$ est une gerbe. C'est évident pour $n = 0$. Supposons donc que $\mathfrak{g}_{2^n}$ soit une gerbe; posons $(\mathfrak{g}, *) = (\mathfrak{g}_{2^n}, *_{2^n})$, $(\mathfrak{g}', *') = (\mathfrak{g}_{2^{n+1}}, *_{2^{n+1}})$ et $\pi = \pi_{2^n}^{2^{n+1}}$. D'après le lemme 6, il suffit de montrer que pour tout x dans $[1,\ 2^{n+1}]$, on a $x *' 2^{n+1} = 2^{n+1}$. Soit k le plus petit élément de $[1,\ 2^n]$ tel que $\pi(x) * k = 2^n$. Puisque $\mathfrak{g}$ est une gerbe, il résulte de (G4) et du lemme 9 qu'il existe h dans $[0,\ n]$ tel que $k = 2^h$. Il résulte alors du lemme 7 que pour tout i dans $\{h, h+1\}$, $x *' 2^i$ est égal soit à 2^n, soit à 2^{n+1}. Raisonnons par l'absurde, en supposant que $x *' 2^{h+1} = 2^n$; $x *' 2^h$ ne peut alors être égal à 2^{n+1} (par le lemme 8), donc on a $x *' 2^h = 2^n$. Mais alors pour tout y dans $[1,\ 2^{h+1}[$, on ne peut avoir $x *' y = 2^{n+1}$, sinon nous aurions $\pi(x) * \pi(y) = 2^n$ par le lemme 7, donc 2^h diviserait $\pi(y)$ par le lemme 9, on aurait donc $y = 2^h$, d'où $x *' y = 2^n$ par hypothèse, contradiction. Il

résulte alors du lemme 5 que l'application de $[1,\ 2^{h+1}]$ vers $[1,\ 2^{n+1}]$ qui à tout y associe $x *' y$ est strictement croissante; mais elle envoie 2^h et 2^{h+1} sur 2^n, contradiction. Ainsi, $x *' 2^{h+1} = 2^{n+1}$, d'où $x *' 2^{n+1} = 2^{n+1}$ par le lemme 8, ce qui permet de conclure. ∎

Puisqu'en présence d'une injection élémentaire non triviale d'un rang dans lui-même la gerbe de Laver $\mathfrak{p}_n$ est primitive d'ordre 2^n, il résulte du théorème 11 que $\mathfrak{g}_{2^n}$ et $\mathfrak{p}_n$ sont *isomorphes*; ceci conduit donc naturellement à poser $\mathfrak{p}_n = \mathfrak{g}_{2^n}$ même en l'absence *a priori* de toute hypothèse de grand cardinal.

Il résulte alors immédiatement de la proposition 3 que toute sous-gerbe *monogène* ou toute gerbe quotient d'un $\mathfrak{p}_n$ est isomorphe à $\mathfrak{p}_m$ pour un certain m au plus égal à n. Notons également que pour n au moins égal à 2, $[2,\ 2^n]$ est une sous-gerbe non monogène de $\mathfrak{p}_n$.

Enfin, les résultats précédents nous permettent de trouver une nouvelle présentation plus simple des gerbes $\mathfrak{p}_n$, n dans $\mathbb{N}$:

COROLLAIRE 12. - *Soit n dans $\mathbb{N}\backslash\{0\}$, soit m le plus grand entier naturel tel que 2^m divise n. Alors la gerbe $\mathfrak{h}_n$ engendrée par un générateur 1 et la relation $1^{[n+1]} = 1$ est isomorphe à $\mathfrak{p}_m$.*

Démonstration. - Soit ϕ l'application de $\mathfrak{g}_n$ vers $\mathfrak{h}_n$ qui à tout k associe $1^{[k]}$. Il est alors facile de démontrer par récurrence (en utilisant (#)) que ϕ est un homomorphisme de magmas. Par suite, l'image de ϕ est stable par la loi de $\mathfrak{h}_n$, c'est donc une sous-gerbe de $\mathfrak{h}_n$; mais elle a 1 pour élément, il en résulte que ϕ est surjectif; donc $\mathfrak{h}_n$ est primitive par la proposition 3, donc isomorphe à un certain $\mathfrak{p}_k$ où k est dans $\mathbb{N}$ par le théorème 11. Mais puisque $\mathfrak{h}_n$ satisfait $1^{[n+1]} = 1$, il vient que 2^k divise n, k est donc au plus égal à m. Réciproquement, $\mathfrak{p}_m$ satisfait la relation $1^{[n+1]} = 1$, et est donc une gerbe quotient de $\mathfrak{h}_n$, d'où $m \leq k$, ce qui permet de conclure. ∎

RÉFÉRENCES BIBLIOGRAPHIQUES

[1] P. DEHORNOY, Sur la structure des gerbes libres, *C. R. Acad. Sci. Paris, t.* 309, *Série I, pp.* 143-148, 1989.

[2] P. DEHORNOY, Algebraic properties of the shift mapping, *Proceedings AMS,* 106-3 (1989), 617-623.

[3] P. DEHORNOY, An alternative proof of Laver's results on the algebra generated by elementary embeddings, *preprint* 1989.

[4] R. LAVER, The left distributive law and the freeness of an algebra of elementary embeddings, *preprint* 1989.

[5] R. LAVER, *communication personnelle.*

Université de Caen, département de Mathématiques, 14032 Caen Cedex.