ALGEBRE ABSOLUE

PAUL LESCOT

Résumé. Nous exposons la théorie de Zhu concernant un analogue formel du corps $\mathbf{F}_p$, "pour $p = 1$", et la comparons à celle de Deitmar.

We give an exposition of Zhu's theory concerning a formal analogue of the field $\mathbf{F}_p$, "for $p = 1$", and then compare it to Deitmar's.

Date: 04 Octobre 2009.

1. Introduction

Il a été, ces dernières années, proposé de nombreuses théories du "corps à un élément". Dans celle de Deitmar ([4],[5]), les objets de base sont les spectres de monoïdes (commutatifs, unitaires) et les schémas sont obtenus par recollement de tels objets. Le monoïde trivial $F_1 = \{1\}$ est donc l'objet final de la catégorie de Deitmar, et son spectre $Spec(F_1)$ l'objet initial de la catégorie des F_1–schémas.

Zhu ([7]) a proposé une autre approche : $B_1 = \{0, 1\}$ désigne pour lui un ensemble à *deux* éléments, muni de la multiplication habituelle, et d'une addition légèrement modifiée : $1 + 1 = 1$. Dans les paragraphes 2 et 3, nous développons, suivant Zhu mais avec des démonstrations, l'algèbre linéaire sur B_1 en restant aussi près que possible des définitions classiques. Il s'avère que la catégorie des B_1–modules de type fini est beaucoup plus complexe que celle des espaces vectoriels de dimension finie sur un corps : elle est en effet équivalente à la catégorie des treillis finis non vides.

L'analogie formelle entre le groupe symétrique Σ_n et le "groupe linéaire de rang n sur un corps de caractéristique 1"est bien connue des spécialistes de théorie des représentations ; il se trouve qu'en un sens naturel, on a bien $GL_n(B_1) \simeq \Sigma_n$ (Théorème 3.7). Le traitement naturel (§4) de l'algèbre commutative et de la géométrie algébrique sur B_1, par analogie avec l'étude des anneaux de polynômes sur un corps, nous amène à conclure que B_1 est "algébriquement clos", et que, pour chaque $n \geq 1$, $MaxSpec(B_1[x_1, ..., x_n])$ est de cardinal 2^n (Théorème 4.10), ce qui constitue, dans notre cadre, un analogue du *Nullstellensatz* de Hilbert.

Dans le cadre de la théorie de Deitmar, toute structure additive disparaît ; nous faisons voir que l'on peut, au sens de la théorie des catégories, plonger cette théorie dans celle de Zhu, et recréer ainsi une certaine structure additive (idempotente) sur les "anneaux de fonctions"des objets géométriques considérés. Ce point de vue mène à des descriptions qui nous semblent intuitivement très satisfaisantes (cf. les exemples (5.4) à (5.6)).

La prépublication récente de Connes et Consani([2]) est postérieure à la soumission de la première version de cet article. Son point de vue semble, à certains égards, analogue au nôtre.

Les paragraphes 2 à 4 du texte sont issus d'un exposé au Groupe de Travail Interuniversitaire en Algèbre, en date du 15 Janvier 2001 ; je remercie Jacques Alev, Dominique Castella, François Dumas et Laurent Rigal pour leurs commentaires à cette occasion. Une version préliminaire du texte complet est parue sous forme de deux prépublications de l'I.H.E.S. (M/06/61 et M/06/63) à l'automne 2006 ; celles-ci n'auraient pas vu le jour sans l'aide et la disponibilité constantes de Cécile Cheikhchoukh.

J'ai pu exposer les résultats de ce travail à l'I.H.E.S. lors de la conférence "Géométrie Algébrique sur le Corps à un Elément", le 29 Mars 2007 ; ce m'est un agréable devoir que de témoigner ma gratitude à Christophe Soulé pour son invitation, et à plusieurs des auditeurs pour leurs commentaires et leurs encouragements, notamment Christophe Breuil, Xavier Caruso et Ofer Gabber (cf. la preuve du Théorème 4.8), Anton Deitmar, et Nikolai Dourov (sur la suggestion duquel j'ai changé la notation de Zhu "F_1"en "B_1"afin de prévenir toute confusion).

Je remercie également le rapporteur pour de nombreuses remarques constructives, dont l'une est à l'origine du contre–exemple décrit dans la Remarque 3.5, et pour avoir attiré mon attention sur la prépublication [2].

Les notations sont entièrement standard ; si A est un monoïde (noté multiplicativement), nous noterons A^* l'ensemble de ses éléments inversibles. Si E est un ensemble, $\mathcal{P}_f(E)$ dénotera l'ensemble de ses parties finies, et

$$\begin{aligned} j_E \quad : \quad & E \to \mathcal{P}_f(E) \\ & x \mapsto \{x\} \end{aligned}$$

l'injection canonique.

Par $\mathcal{D}$ nous entendrons la catégorie des F_1–anneaux au sens de Deitmar, c'est–à–dire ([4], p.88) la catégorie des monoïdes commutatifs. Si $A \in \mathcal{D}$ est un monoïde commutatif et B un sous–monoïde de A, nous dirons que A est *entier* sur B si, pour chaque $a \in A$, il existe un entier $n \geq 1$ tel que $a^n \in B$.

2. Définition de B_1 et premières propriétés

Définition 2.1. On notera B_1 l'ensemble $\{0, 1\}$ muni des lois de composition internes + et . données par :

$$0 + 0 = 0 \ ,$$

$$0 + 1 = 1 + 0 = 1 + 1 = 1 \ ,$$

$$0.0 = 0.1 = 1.0 = 0 \ ,$$

et

$$1.1 = 1 \ .$$

Remarque 2.2. Il est visible que B_1 satisfait à tous les axiomes des corps commutatifs, excepté à celui qui affirme l'existence de symétriques pour l'addition.

Définition 2.3. On appelle B_1-module la donnée d'un monoïde commutatif M d'élément neutre 0 et d'une B_1-loi externe sur M (c'est-à-dire d'une application

$$(\lambda, x) \mapsto \lambda x$$

de $B_1 \times M$ dans M), ayant les propriétés usuelles, *i.e.* :

$$\forall (\lambda, \mu, x) \in B_1 \times B_1 \times M \quad (\lambda + \mu)x = \lambda x + \mu x \quad , \tag{1}$$

$$\forall (\lambda, x, y) \in B_1 \times M \times M \quad \lambda(x + y) = \lambda x + \lambda y \quad , \tag{2}$$

$$\forall x \in M \quad 1x = x \quad , \tag{3}$$

$$\forall x \in M \quad 0x = 0 \quad . \tag{4}$$

Définition 2.4. Un ensemble ordonné pointé $(E, \leq, 0)$ est dit décent s'il possède un (et nécessairement un seul) plus petit élément 0, et si en outre deux éléments quelconques de E possèdent une borne supérieure.

Théorème 2.5. *La catégorie $\mathcal{Z}$ des B_1–modules s'identifie canoniquement à la catégorie des ensembles ordonnés décents.*

Démonstration. Soit M un B_1–module ; pour $(a,b) \in M^2$, définissons :

$$a \leq b \equiv a+b=b \ .$$

Alors, pour tout $a \in M$:

(5)

$$\begin{aligned} a+a &= 1a+1a \\ &= (1+1)a \\ &= 1a \\ &= a \ , \end{aligned}$$

soit $a \leq a$. En outre, de $a \leq b$ et $b \leq a$, il suit :

$$a+b=b \ \text{ et } \ b+a=a \ ,$$

d'où $a=b+a=a+b=b$.

De plus, si $a \leq b$ et $b \leq c$, il vient :

$$\begin{aligned} a+c &= a+(b+c) \\ &= (a+b)+c \\ &= b+c \\ &= c \ , \end{aligned}$$

soit $a \leq c$. $\leq$ est donc une relation d'ordre sur M ; de plus, pour chaque $a \in M$:

$$0+a=a \quad , \tag{6}$$

soit $0 \leq a$; $(M, \leq)$ possède donc un plus petit élément : 0.

Soient $a \in M$ et $b \in M$; il est facile de voir que :

$$\begin{aligned} a+(a+b) &= (a+a)+b \\ &= a+b \ \text{ (d'après (5))} \ , \end{aligned}$$

soit $a \leq a+b$; de même $b \leq a+b$.

De plus, de $a \leq c$ et $b \leq c$ suivent $a+c=c$ et $b+c=c$, d'où :

$$\begin{aligned} (a+b)+c &= a+(b+c) \\ &= a+c \\ &= c \ , \end{aligned}$$

soit $a+b \leq c$; a et b possèdent donc une borne supérieure : $a \vee b = a+b$. On a bien montré que $(M, \leq, 0)$ était un ensemble ordonné décent.

Réciproquement, soit $(E, \leq, 0)$ un ensemble ordonné décent ; il est facile de voir que l'addition et la multiplication définies par

$$\forall (a,b) \in E^2 \ \ a+b=a \vee b \ \ ,$$

$$\forall a \in E \quad 0a=0 \ \ ,$$

et

$$\forall a \in E \quad 1a=a$$

font de E un B_1–module.

Il reste à déterminer les *morphismes* de B_1–modules. Soit $\varphi : M \to N$ un tel morphisme ; on a nécessairement :

$$\varphi(0_M) = \varphi(0.0_M) = 0.\varphi(0_M) = 0_N \ ,$$

et, pour $(m, m^{'}) \in M^2$:

$$\varphi(m \vee_M m^{'}) = \varphi(m + m^{'}) = \varphi(m) + \varphi(m^{'}) = \varphi(m) \vee_N \varphi(m^{'}) \ .$$

En tant qu'application entre ensembles ordonnés décents, φ doit donc préserver l'opération de borne supérieure (en particulier, être croissante) et le plus petit élément. Réciproquement, on vérifie aisément qu'une application entre ensembles ordonnés décents ayant ces deux propriétés constitue un morphisme pour les structures sous–jacentes de B_1–modules. □

Corollaire 2.6. *Modulo l'identification établie par le Théorème 2.5, la catégorie $\mathcal{Z}_f$ des B_1–modules finis s'identifie à celle des treillis finis non vides.*

Démonstration. Soit T un B_1–module fini ; par une récurrence immédiate sur le cardinal $|S|$ de S on voit que toute partie (même vide) S de T possède une borne supérieure ; en particulier, pour $(a, b) \in T^2$,

$$a \wedge b = \vee\{c \in T \mid c \leq a \ \text{ et } \ c \leq b\}$$

est bien défini : T est un treillis, et $T \neq \emptyset$ car $0 \in T$.

Réciproquement, soit T un treillis fini non vide ; il suffit de faire voir que T possède un plus petit élément ; mais, en tant qu'ensemble ordonné fini non vide, T possède un élément minimal m, et on a, pour tout $x \in T$:

$$m \wedge x \leq m \ ,$$

d'où

$$m \wedge x = m$$

et

$$m = m \wedge x \leq x \ ;$$

m est donc bien le plus petit élément de T. □

3. Algèbre linéaire sur B_1

Théorème 3.1. *Soit A un ensemble, et munissons l'ensemble $\mathcal{P}_f(A)$ de sa structure habituelle de treillis ($C \leq B$ si et seulement si $C \subset B$) ; alors l'injection*

$$\begin{aligned} j_A : \qquad & A \to \mathcal{P}_f(A) \\ & x \mapsto \{x\} \end{aligned}$$

fait de $\mathcal{P}_f(A)$ le B_1–module libre engendré par A. En particulier, la catégorie des B_1–modules libres de type fini (i.e. finis) s'identifie canoniquement à celle des algèbres de Boole finies.

Démonstration. Il s'agit de faire voir que, pour tout B_1–module M et toute application $\varphi : A \to M$, il existe un unique morphisme

$$\rho : \mathcal{P}_f(A) \to M$$

tel que $\varphi = \rho \circ j_A$. Pour tout $C \in \mathcal{P}_f(A)$, on doit avoir :

$$\begin{aligned}\rho(C) &= \rho(\bigcup_{x\in C}\{x\}) \\ &= \rho(\bigcup_{x\in C} j_A(x)) \\ &= \bigvee_{x\in C} \rho(j_A(x))\end{aligned}$$

soit :

$$\rho(C) = \bigvee_{x\in C} \varphi(x) \quad , \tag{7}$$

d'où l'unicité de ρ.

Réciproquement, il est visible que ρ défini par (7) est un morphisme de B_1–modules et répond à la question.

Lorsque A est fini, $\mathcal{P}_f(A) = \mathcal{P}(A)$ est une algèbre de Boole, d'où la dernière assertion. □

Plus généraux que les modules libres sont les modules *projectifs* , au sens général de la théorie des catégories : le B_1–module M est projectif si, quels que soient les B_1–modules N_1 et N_2 et les morphismes $\varphi : M \to N_2$ et $\psi : N_1 \twoheadrightarrow N_2$ avec ψ surjectif, il existe un morphisme $\rho : M \to N_1$ tel que $\psi \circ \rho = \varphi$. Tout B_1–module libre est évidemment projectif.

Définition 3.2. Soit $(E, \leq)$ un ensemble ordonné ; posons

$$\mathcal{O}(E) = \{A \subset E \,|\, \forall x \in A[y \leq x \Longrightarrow y \in A]\} \ ;$$

alors $(\mathcal{O}(E), \subset)$ est un treillis de plus petit élément $\emptyset$, donc un B_1–module (en fait, $\mathcal{O}(E)$ est un sous-treillis (distributif) de $\mathcal{P}(E)$).

Remarque 3.3. Le Théorème suivant ne sera pas utilisé dans la suite de l'article.

Théorème 3.4. *Les propriétés suivantes d'un treillis fini non vide M sont équivalentes :*

- *M, considéré comme B_1–module, est projectif.*
- *M est distributif.*
- *Il existe un ensemble ordonné fini E tel que M soit isomorphe à $\mathcal{O}(E)$.*
- *M, considéré comme B_1–module, est isomorphe à un sous–module d'un B_1–module libre.*

Remarque 3.5. L'équivalence (2) $\Longleftrightarrow$ (3) n'est autre que le cas particulier du Théorème de Représentation de Birkhoff relatif aux treillis finis : cf. par exemple [1], p.59, Theorem 3, ou [3], p.171, Theorem 8.17.

Démonstration. (1) $\Longrightarrow$ (2) :

Soient $N_1 = \mathcal{P}(M)$, $N_2 = M$ et

$$\begin{aligned}\psi : \quad \mathcal{P}(M) &\to M \\ A &\mapsto \bigvee_{x\in A} x \ .\end{aligned}$$

Il est visible que ψ est un morphisme surjectif de B_1–modules, donc il existe un morphisme $\rho : M \to \mathcal{P}(M)$ tel que $\psi\circ\rho = Id_M$. Mais alors, pour tout $(a, b, c) \in M^3$:

$$\begin{aligned}\rho(a \wedge (b \vee c)) &\leq \rho(a) \cap \rho(b \vee c) \\ &= \rho(a) \cap (\rho(b) \cup \rho(c)) \\ &= (\rho(a) \cap \rho(b)) \cup (\rho(a) \cap \rho(c))\end{aligned}$$

d'où :

$$\begin{aligned} a \wedge (b \vee c) &= \psi(\rho(a \wedge (b \vee c))) \\ &\le \psi((\rho(a) \cap \rho(b)) \cup (\rho(a) \cap \rho(c))) \\ &= \psi(\rho(a) \cap \rho(b)) \vee \psi(\rho(a) \cap \rho(c)) \\ &\le (\psi(\rho(a)) \wedge \psi(\rho(b))) \vee (\psi(\rho(a)) \wedge \psi(\rho(c))) \\ &= (a \wedge b) \vee (a \wedge c) \\ &\le a \wedge (b \vee c) \ , \end{aligned}$$

donc

$$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c) \ ,$$

c'est-à-dire que $\wedge$ est distributive par rapport à $\vee$. Mais, comme il est bien connu ([1], Theorem 9, p.11 ; [3], Lemma 6.3, p.130), la distributivité de $\vee$ par rapport à $\wedge$ s'ensuit. En effet, l'on peut écrire, pour $(a, b, c) \in M^3$:

$$\begin{aligned} (a \vee b) \wedge (a \vee c) &= ((a \vee b) \wedge a) \vee ((a \vee b) \wedge c) \ \text{(d'après le résultat ci–dessus)} \\ &= a \vee (c \wedge a) \vee (c \wedge b) \ \ (\textit{idem}\ ) \\ &= (a \vee (c \wedge a)) \vee (c \wedge b) \\ &= a \vee (b \wedge c) \ . \end{aligned}$$

(2) $\Longrightarrow$ (3) :

Soit E l'ensemble des éléments $m \neq 0$ de M *irréductibles pour* $\vee$, *i.e.* tels que :

$$\forall (x, y) \in M^2 \ \ x \vee y = m \Longrightarrow x = m \ \text{ou} \ y = m \ .$$

De la finitude de M résulte que chaque élément de M est la borne supérieure d'une famille (éventuellement vide) d'éléments de E ; dans le cas contraire, l'ensemble M_0 des éléments de M n'ayant pas cette propriété serait non vide, et aurait donc un élément minimal (pour $\le |_{M_0}$) a. Par hypothèse on aurait $a \neq 0$ et $a \notin E$, donc il existerait x et y tels que :

$$a = x \vee y \ , x \neq a \text{ et } y \neq a \ .$$

Mais alors $x < a$ et $y < a$, donc $x \notin M_0$ et $y \notin M_0$, d'où

$$x = \bigvee_{b \in E_x} b$$

et

$$y = \bigvee_{b \in E_y} b \ ,$$

avec $E_x \subset E$ et $E_y \subset E$. Il s'ensuivrait :

$$\begin{aligned} a &= x \vee y \\ &= \bigvee_{b \in E_x} b \vee \bigvee_{b \in E_y} b \\ &= \bigvee_{b \in E_x \cup E_y} b \notin M_0 \ , \end{aligned}$$

une contradiction.

On a donc :

$$\forall m \in M \ \ m = \bigvee_{x \in G_m} x \ ,$$

où

$$G_m = \{a \in E \mid a \leq m\} \ ;$$

il est visible que $G_m \in \mathcal{O}(E)$. Soit alors

$$\begin{aligned} \varphi : \quad & M \to \mathcal{O}(E) \\ & m \mapsto G_m \ ; \end{aligned}$$

j'affirme que φ est un morphisme bijectif de B_1–modules. L'injectivité de φ résulte de ce que

$$\forall m \in M \ \ m = \bigvee_{x \in \varphi(m)} x \ ,$$

la propriété $\varphi(0) = \emptyset$ est évidente, et $m \leq m^{'}$ entraîne $G_m \subset G_{m'}$, soit $\varphi(m) \subset \varphi(m^{'})$; il ne reste qu'à faire voir que :

$$\varphi(m) \cup \varphi(m^{'}) = \varphi(m \vee m^{'}) \ .$$

L'inclusion $\varphi(m) \cup \varphi(m^{'}) \ \subset \ \varphi(m \vee m^{'})$ étant évidente, il nous suffit d'établir que :

$$\forall x \in G_{m \vee m'} \ \ x \in \varphi(m) \cup \varphi(m^{'}) \ .$$

Mais on a

$$\begin{aligned} m \vee m^{'} &= \bigvee_{a \in G_m} a \vee \bigvee_{a \in G_{m'}} a \\ &= \bigvee_{a \in G_m \cup G_{m'}} a \ . \end{aligned}$$

Soit alors $x \in G_{m \vee m'}$; il vient :

$$\begin{aligned} x &= x \wedge (m \vee m^{'}) \\ &= x \wedge (\bigvee_{a \in G_m \cup G_{m'}} a) \\ &= \bigvee_{a \in G_m \cup G_{m'}} (x \wedge a) \ . \end{aligned}$$

Donc

$$\exists a \in G_m \cup G_{m'} \ \ x = x \wedge a \ .$$

Mais alors $x \leq a$, d'où $x \leq m$ si $a \in G_m$, et $x \leq m^{'}$ si $a \in G_{m'}$; en conclusion, $x \in \varphi(m)$ ou $x \in \varphi(m^{'})$, et en effet $x \in \varphi(m) \cup \varphi(m^{'})$.

Il reste maintenant à démontrer que $\varphi(M) = \mathcal{O}(E)$. Soit $T \in \mathcal{O}(E)$, et soit $m = \bigvee_{t \in T} t \in M$; alors, pour chaque $t \in T$, $t \leq m$, donc $t \in \varphi(m)$:

$$T \subset \varphi(m) \ .$$

Réciproquement, soit $v \in \varphi(m)$; on a $v \leq m$, d'où :

$$\begin{aligned} v &= v \wedge m \\ &= v \wedge (\bigvee_{t \in T} t) \\ &= \bigvee_{t \in T} (v \wedge t) \end{aligned}$$

donc

$$(\exists t_0 \in T) \quad v = v \wedge t_0 \ ,$$

soit

$$v \leq t_0 \ ,$$

d'où (car $T \in \mathcal{O}(E)$) :

$$v \in T \ .$$

Il s'ensuit que $\varphi(m) \subset T$, d'où

$$T = \varphi(m) \ ;$$

φ est donc bel et bien surjectif.

(3) $\Longrightarrow$ (4) :

C'est évident vu l'existence de l'injection canonique

$$\mathcal{O}(E) \hookrightarrow \mathcal{P}(E) = \mathcal{P}_f(E) \ .$$

(4) $\Longrightarrow$ (1) :

On peut supposer que M est un sous–B_1–module de $\mathcal{P}_f(E)$, pour un certain ensemble E ; en remplaçant éventuellement E par $E_1 = \bigcup_{m \in M} m$, on peut également supposer que E est fini, et que $E \in M$. Soit, pour $A \in \mathcal{P}(E)$:

$$\mathcal{S}(A) = \{B \in M | A \subset B\}.$$

Il est clair que $\mathcal{S}(A) \neq \emptyset$ (car $E \in \mathcal{S}(A)$) ; soit $\theta(A) = \bigcap_{B \in \mathcal{S}(A)} B$. $\theta(A)$ contient A ; du fait que M est un B_1–module *fini* , donc un treillis d'après le Corollaire 2.6, résulte que $\theta(A) \in M$; en particulier, $\theta(\theta(A)) = \theta(A)$, *i.e.* $\theta^2 = \theta$. Il est en outre clair que $\theta(\emptyset) = \emptyset$.

Soient A et B deux éléments de $\mathcal{P}(E)$; alors

$$A \subset \theta(A) \subset \theta(A) \cup \theta(B) \ ,$$

et de même

$$B \subset \theta(B) \subset \theta(A) \cup \theta(B) \ ,$$

soit :

$$A \cup B \subset \theta(A) \cup \theta(B) \ .$$

Mais $\theta(A) \cup \theta(B) \in M$, d'où :

$$\theta(A \cup B) \subset \theta(A) \cup \theta(B) \ .$$

Réciproquement, si $C \in M$ et $A \cup B \subset C$, on a $A \subset C$ et $B \subset C$, d'où $\theta(A) \subset C$ et $\theta(B) \subset C$, soit $\theta(A) \cup \theta(B) \subset C$, d'où

$$\theta(A) \cup \theta(B) \subset \theta(A \cup B) \ ,$$

et

$$\theta(A \cup B) = \theta(A) \cup \theta(B) \quad .$$

Nous avons donc construit un morphisme $\theta : \mathcal{P}(E) \to M$ tel que $\theta|_M = Id_M$, c'est-à-dire une *rétraction* de $\mathcal{P}(E)$ sur M. La projectivité de M s'ensuit alors par un raisonnement classique d'algèbre universelle : soient $\varphi : M \to N_2$ et $\psi : N_1 \twoheadrightarrow N_2$ surjectif deux morphismes de B_1–modules ; alors $\varphi \circ \theta : \mathcal{P}(E) \to N_2$ est un morphisme de B_1–modules. $\mathcal{P}(E) = \mathcal{P}_f(E)$ étant libre (Théorème 3.1), donc projectif, il existe un morphisme $\lambda : \mathcal{P}(E) \to N_1$ tel que $\psi \circ \lambda = \varphi \circ \theta$. Mais alors, en posant $\rho = \lambda|_M : M \to N_1$, on a :

$$\begin{aligned} \psi \circ \rho &= \psi \circ \lambda|_M \\ &= (\psi \circ \lambda)|_M \\ &= (\varphi \circ \theta)|_M \\ &= \varphi \circ \theta|_M \\ &= \varphi \circ Id_M \\ &= \varphi \ ; \end{aligned}$$

on a bien établi la projectivité de M. □

Remarque 3.6. On peut se demander s'il est possible de caractériser les treillis finis *modulaires* (lesquels forment une classe plus générale que celle des treillis distributifs) au moyen de leur structure de B_1–modules, obtenant ainsi un analogue du Théorème 3.3. Tel ne semble pas être le cas au vu de l'exemple suivant : soit $M = \{0, a, b, c, d, e\}$ un ensemble à 6 éléments, muni de la loi interne + commutative, associative, idempotente, ayant 0 pour élément neutre, et telle que

$$a + b = d \ ,$$

$$c + d = e \ ,$$

et

$$b + c = c \ .$$

Il est facile de vérifier que l'on définit ainsi sur M une structure de B_1–module, et que le treillis associé (*via* le Théorème 2.6) est modulaire. Soit alors $N = \{0, a, c, d, e\}$; on voit que N est un sous–B_1–module de M, et que, considéré comme treillis *via*, là encore, le Théorème 2.6, il n'est pas modulaire (il est en fait isomorphe au treillis non–modulaire minimal N_5 : cf. [3], (6.10), p. 134). Donc aucun énoncé portant sur un B_1–module M analogue à la dernière condition du Théorème 3.4 ne peut être équivalent à la modularité du treillis sous–jacent à M.

Dans l'exemple ci–dessus, N est un sous–B_1–module de M, mais bien sûr pas un sous–treillis de ce dernier : dans M

$$c \wedge_M d = b$$

et, dans N :

$$c \wedge_N d = 0 \ ;$$

aucune contradiction n'apparaît donc.

Théorème 3.7. $GL_n(B_1) \simeq \Sigma_n$.

Démonstration. $GL_n(B_1)$ désigne par définition le groupe des automorphismes d'un B_1–module libre (M) de rang n. D'après le Théorème 3.1, on peut supposer que $M = \mathcal{P}_f(A) = \mathcal{P}(A)$ avec $|A| = n$; un automorphisme α de M doit préserver $\emptyset$ et la relation d'inclusion, donc aussi les éléments minimaux de $M \setminus \{\emptyset\}$ pour l'inclusion, soit les parties à un élément :

$$\forall a \in A \ \exists f(a) \in A \ \ \alpha(\{a\}) = \{f(a)\} \ .$$

α étant injectif, l'application f est injective, donc bijective, et on a, pour tout $B \in M$:

$$\begin{aligned} \alpha(B) &= \alpha(\bigcup_{x\in B} \{x\}) \\ &= \bigcup_{x\in B} \alpha(\{x\}) \\ &= \bigcup_{x\in B} \{f(x)\} \\ &= \{f(x) | x \in B\} \\ &= f[B] \ , \end{aligned}$$

soit :

$$\alpha(B) = f[B] \quad . \tag{8}$$

Réciproquement, toute permutation f de A définit par la formule (8) un automorphisme α de M, d'où :

$$GL_n(B_1) \simeq \Sigma(A) \simeq \Sigma_n \ .$$

□

4. Géométrie algébrique sur B_1

Définition 4.1. On appelle B_1–algèbre (commutative, unitaire) la donnée d'un B_1–module $\mathcal{A}$, contenant B_1, et d'une multiplication sur $\mathcal{A}$, associative, commutative, d'élément neutre 1, et bilinéaire par rapport aux opérations de B_1–module. On note $\mathcal{Z}_a$ la catégorie de ces algèbres.

Définition 4.2. On appelle congruence sur la B_1–algèbre $\mathcal{A}$ une relation d'équivalence $\sim$ sur $\mathcal{A}$ telle que

$$0 \nsim 1$$

et

$$a \sim b \ \text{ et } \ a' \sim b' \Longrightarrow \ a + a' \sim b + b' \ \text{ et } \ aa' \sim bb' \ .$$

Les congruences jouent dans notre théorie le même rôle que les équivalences modulo un idéal en algèbre commutative ; en particulier, pour toute congruence $\sim$ sur $\mathcal{A}$, l'ensemble quotient $\mathcal{A}/\sim$ est muni d'une structure canonique de B_1–algèbre.

Définition 4.3. On définit sur l'ensemble des congruences sur la B_1–algèbre $\mathcal{A}$ une relation d'ordre $\geq$ par :

$$\sim_1 \geq \sim_2 \iff \forall (a,b) \in \mathcal{A}^2 \ a \sim_2 b \Longrightarrow a \sim_1 b \ .$$

Il est facile de voir que, si $\sim_1 \geq \sim_2$, alors il existe un morphisme surjectif canonique

$$\mathcal{A}/\sim_2 \twoheadrightarrow \mathcal{A}/\sim_1 .$$

En particulier,

Théorème 4.4. *Si l'algèbre quotient $\mathcal{A}/\sim$ est isomorphe à B_1, la congruence $\sim$ est maximale.*

Il est facile de voir que la B_1–algèbre libre $B_1[x]$ s'identifie à l'ensemble des sommes formelles (éventuellement vides) de puissances de x (en posant $x^0 = 1$). Plus généralement :

Théorème 4.5. *La B_1–algèbre libre sur $A = \{x_1, ..., x_n\}$ s'identifie à l'ensemble des sommes formelles de monômes $x_1^{\alpha_1}...x_n^{\alpha_n}$ ($\alpha_i \in \mathbf{N}$) muni des opérations évidentes. Plus précisément, soit*

$$B_1[A] = \mathcal{P}_f(\mathbf{N}^A)$$

l'ensemble des parties finies de $\mathbf{N}^A$, avec la structure naturelle de treillis, et la multiplication définie, pour $(R, S) \in \mathcal{P}_f(\mathbf{N}^A)^2$, par

$$RS = \{a + b \mid a \in R\ ,\ b \in S\}$$

(l'addition dans $\mathbf{N}^A$ étant définie composante par composante). Pour $a \in A$, posons $\delta_a = \mathbf{1}_{\{a\}}$; alors l'injection canonique

$$\begin{aligned} i : \quad A &\to \mathcal{P}_f(\mathbf{N}^A) \\ a &\mapsto \{\delta_a\} \end{aligned}$$

fait de $B_1[A]$ la B_1–algèbre libre sur A.

Démonstration. L'associativité et la commutativité de la multiplication sont évidentes, tout comme l'existence d'un élément neutre $U = \{0\}$; quant à la distributivité, elle suit de :

$$\begin{aligned} R(S+T) &= \{a + b \mid a \in R\ ,\ b \in S+T\} \\ &= \{a + b \mid a \in R\ ,\ b \in S \cup T\} \\ &= \{a + b \mid a \in R\ ,\ b \in S \text{ ou } b \in T\} \\ &= RS \cup RT \\ &= RS + RT\ . \end{aligned}$$

Soit maintenant $\varphi : A \to E$ une application de A dans la B_1–algèbre E. Il nous reste à montrer qu'existe un unique morphisme $\psi : \mathcal{P}_f(\mathbf{N}^A) \to E$ tel que $\psi \circ i = \varphi$. Si ψ est tel, on doit avoir , pour tout $F \in \mathcal{P}_f(\mathbf{N}^A)$:

$$\begin{aligned}
\psi(F) &= \psi(\bigcup_{x\in F}\{x\}) \\
&= \bigvee_{x\in F}\psi(\{x\}) \\
&= \bigvee_{x\in F}\psi(\{\sum_{a\in A}x(a)\delta_a\}) \\
&= \bigvee_{x\in F}\psi(\prod_{a\in A}\{\delta_a\}^{x(a)}) \\
&= \bigvee_{x\in F}\prod_{a\in A}\psi(\{\delta_a\})^{x(a)} \\
&= \bigvee_{x\in F}\prod_{a\in A}\psi(i(a))^{x(a)} \\
&= \bigvee_{x\in F}\prod_{a\in A}\varphi(a)^{x(a)} \\
&= \sum_{x\in F}\prod_{a\in A}\varphi(a)^{x(a)}
\end{aligned}$$

Réciproquement, il est très facile de voir que l'application ψ définie par (9) convient. □

Définition 4.6. Pour $I \subset A$ et $R \in B_1[A]$, soit

$$F_I(R) = \{r \in R \mid r(I) \subseteq \{0\}\}.$$

Théorème 4.7. *Pour chaque $I \subset A$, la relation $\sim_I$ sur $B_1[A]$ définie par :*

$R \sim_I S$ si et seulement si ($F_I(R) = F_I(S) = \emptyset$ ou $F_I(R) \neq \emptyset \neq F_I(S)$)

est une congruence sur $B_1[A]$, et

$$B_1[A]/{\sim_I} \simeq B_1 \ .$$

Démonstration. De

$$F_I(R+S) = F_I(R) \cup F_I(S) \ ,$$

$$F_I(RS) = F_I(R)F_I(S) \ ,$$

$$F_I(0) = \emptyset \ ,$$

et

$$F_I(1) = \{0\} = U$$

suivent aisément les propriétés qui définissent une congruence. De plus, il est clair que $R \sim_I 0$ si $F_I(R) = \emptyset$, et que $R \sim_I 1$ si $F_I(R) \neq \emptyset$; on a donc

$$B_1[A]/{\sim_I} = \{\bar{0}, \bar{1}\} \ ,$$

d'où :

$$B_1[A]/{\sim_I} \simeq B_1.$$

□

En particulier, pour chaque $I \subset A$, la congruence $\sim_I$ sur $B_1[A]$ est maximale (Théorème 4.4), et $B_1[A]/\sim_I \simeq B_1$. Réciproquement, toute congruence (maximale) $\sim$ sur $B_1[A]$ telle que $B_1[A]/\sim \simeq B_1$ est de la forme $\sim_I$ pour un $I \subset A$ (il suffit de prendre

$$I = \{x \in A | x \sim 0\} = \{x \in A | x \nsim 1\}).$$

On a d'ailleurs le

Théorème 4.8. *Tout quotient de $B_1[A]$ par une congruence maximale est isomorphe à B_1.*

Démonstration. Soit $\sim$ une congruence maximale sur $B_1[A]$. J'affirme que :

si $u \in B_1[A]$ et $v \in B_1[A]$ sont tels que $uv \sim 0$, alors $u \sim 0$ ou $v \sim 0$ (*) ,

(en d'autres termes, l'algèbre quotient $B_1[A]/\sim$ est "intègre") .

Raisonnons par l'absurde, et soit $\mathcal{R}_u$ la relation sur $B_1[A]$ définie par :

$$x \, \mathcal{R}_u \, y \equiv \exists (a, b) \in B_1[A]^2 \;\; x + ua \sim y + ub \; .$$

Il est très facile de voir que $\mathcal{R}_u$ est compatible avec l'addition et la multiplication, et que $x \sim y$ entraîne $x \, \mathcal{R}_u \, y$. En outre $0 \, \mathcal{R}_u \, u$, et $0 \nsim u$, donc $\sim \neq \mathcal{R}_u$. Il en résulte que $\mathcal{R}_u$ n'est pas une congruence, donc que $0 \, \mathcal{R}_u \, 1$, *i.e.*il existe $(a, b) \in B_1[A]^2$ tels que :

$$0 + ua = 1 + ub \; ,$$

soit

$$ua = 1 + ub \; .$$

Mais alors

$$(uv)a = v(ua) = v(1 + ub) = v + uvb$$

et de $uv \sim 0$ suit :

$$0 = 0a \sim (uv)a = v + uvb \sim v + 0b = v \; ,$$

soit $v \sim 0$, une contradiction ; $(*)$ est donc bien établi.

Posons $I = \{x \in A | x \sim 0\}$. Soit alors $z \in B_1[A]$; décomposons z en somme de monômes (en les éléments de A) distincts : $z = M_1 + ... + M_k$, et soit (pour $j \in \{1, ..., k\}$) $N_j =_{def} \sum_{l \neq j} M_l$. Si $z \sim 0$, alors, pour chaque $j \in \{1, ..., k\}$,

$$0 \sim z = M_j + N_j = (M_j + M_j) + N_j = M_j + (M_j + N_j) = M_j + z \sim M_j + 0 = M_j \; ,$$

donc $M_j \sim 0$. Mais alors, d'après $(*)$, l'un des éléments de A facteurs de M_j est $\sim$−équivalent à 0, donc appartient à I ; cela valant pour chaque $j \in \{1, ..., k\}$, on a $z \sim_I 0$.

Par ailleurs, si $z \nsim 0$, alors $M_j \nsim 0$ pour au moins un $j \in \{1, ..., k\}$; aucun des éléments de A facteurs de M_j n'appartient donc à I ; en particulier $M_j \sim_I 1$, donc $z \sim_I 1$.

Il en résulte que $z \sim z'$ entraîne $z \sim_I z'$, donc que $\sim \leq \sim_I$, d'où, au vu de la maximalité de $\sim$, $\sim = \sim_I$.

Cette démonstration est essentiellement due à Xavier Caruso ; j'y ai incorporé quelques suggestions d'Ofer Gabber. □

Remarque 4.9. D'après la discussion précédant le Théorème 4.8, toute congruence maximale sur $B_1[A]$ est de la forme $\sim_I$ pour un $I \subset A$. Afin d'appréhender la signification de cet énoncé, considérons-en l'analogue $(\mathcal{E}_K)$ sur un corps commutatif K :

$(\mathcal{E}_K)$ Chaque quotient maximal de $K[x_1, ..., x_n]$ est isomorphe à K, et ces quotients sont en bijection canonique avec les points de K^n.

Cet énoncé contient à la fois l'assertion que K est algébriquement clos, et le *Nullstellensatz* . Il semble donc naturel de reformuler le Théorème 4.8 en le

Théorème 4.10. *B_1 est algébriquement clos et, pour chaque $n \geq 1$, $MaxSpec(B_1[x_1, ..., x_n])$ est de cardinal 2^n.*

Remarque 4.11. Les B_1–algèbres *monogènes* forment déjà une famille très riche. Nous nous proposons de déterminer les types d'isomorphisme de B_1–algèbres de cardinal n, pour $n \leq 5$. Soit donc $\mathcal{A} = B_1[x]/\sim$ de cardinal n, et soit a l'image de $x \in B_1[x]$ dans $\mathcal{A}$ par la projection canonique.

Pour $n = 2$ on a $\mathcal{A} = B_1$, d'où

(4.11.2.1)
$$a = 0$$

ou

(4.11.2.2)
$$a = 1 \ ;$$

réciproquement, chacune de ces possibilités définit une congruence convenable, d'où

$$\mathbf{c_2 = 2} \ .$$

Pour $n = 3$, on a nécessairement $a \notin \{0, 1\}$, d'où $\mathcal{A} = \{0, a, 1\}$.Deux cas apparaissent alors :

1^0) $a + 1 = a$, soit $0 < 1 < a$. Il suit alors $a^2 + a = a^2$, d'où $a^2 \neq 1, 0$, soit $a^2 = a$, et :

(4.11.3.1)
$$\left\{ \begin{aligned} a + 1 &= a \\ a^2 &= a \end{aligned} \right\}$$

2^0) $a + 1 = 1$, soit $0 < a < 1$. Alors $a^2 + a = a$, d'où $a^2 = 0$ ou $a^2 = a$, soit

(4.11.3.2)
$$\left\{ \begin{aligned} a + 1 &= 1 \\ a^2 &= 0 \end{aligned} \right\}$$

ou :

(4.11.3.3)
$$\left\{ \begin{aligned} a + 1 &= 1 \\ a^2 &= a \end{aligned} \right\}.$$

On vérifie facilement que les algèbres respectivement définies par (4.11.3.1), (4.11.3.2) et (4.11.3.3) sont bien de cardinal 3. Il existe donc exactement trois congruences $\sim$ sur $B_1[x]$ telles que $B_1[x]/\sim$ soit de cardinal 3 :

$$\mathbf{c_3 = 3} \ .$$

Pour $n = 4$, distinguons deux cas :

1^0) $a^2 \in \{0,1,a\}$. Alors $a+1 \notin \{0,1,a\}$, sans quoi $\{0,1,a\}$ serait une sous–B_1–algèbre de $\mathcal{A}$ contenant a, et on aurait $\mathcal{A} = \{0,1,a\}$, une contradiction. On a donc $\mathcal{A} = \{0,1,a,1+a\}$, et $0 < 1 < 1+a$, $0 < a < 1+a$, et trois cas peuvent apparaître :

(4.11.4.1)
$$a^2 = 0 \ ,$$

(4.11.4.2)
$$a^2 = 1 \ ,$$

(4.11.4.3)
$$a^2 = a.$$

2^0) $a^2 \notin \{0,1,a\}$, d'où $\mathcal{A} = \{0,1,a,a^2\}$. Trois possibilités sont alors à distinguer :

$2^0)\alpha$) $a+1 = 1$; alors $a^2+a = a(a+1) = a$, d'où $a^3+a^2 = a(a^2+a) = a^2$, et $0 \leq a^3 \leq a^2 < a < 1$, et encore deux éventualités :

(4.11.4.4)
$$\left\{ \begin{array}{r} a+1=1 \\ a^3=a^2 \end{array} \right\} \ ,$$

et

(4.11.4.5)
$$\left\{ \begin{array}{r} a+1=1 \\ a^3=0 \end{array} \right\} \ .$$

$2^0)\beta$) $a+1 = a$. Alors $a^2+a = a(a+1) = aa = a^2$, d'où $a^3+a^2 = a^3$ et $0 < 1 < a < a^2 \leq a^3$, donc $a^2 = a^3$:

(4.11.4.6)
$$\left\{ \begin{array}{r} a+1=a \\ a^2=a^3 \end{array} \right\} \ .$$

$2^0)\gamma$)

(4.11.4.7)
$$a^2 = a+1 \ .$$

Réciproquement (4.11.4.1),..., (4.11.4.7) définissent chacun une algèbre de cardinal 4, d'où bien :

$$\mathbf{c_4 = 7} \ .$$

Pour $n = 5$, distinguons à nouveau deux cas :

1^0) $a+1 \in \{0,1,a\}$. Alors $a^2 \notin \{0,1,a\}$, sans quoi $\{0,1,a\}$ serait une sous–B_1–algèbre de $\mathcal{A}$ contenant a, et on aurait $\mathcal{A} = \{0,1,a\}$, une contradiction Deux cas peuvent alors se présenter :

$1^o)\alpha$)
$$a+1 = 1 \ .$$

Mais alors $a^2+a = a(a+1) = a.1 = a$, et $a^3+a^2 = a^2(a+1) = a^2.1 = a^2$, d'où $0 < a^3 < a^2 < a < 1$; en effet, on a nécessairement $a^3 \neq a^2$ et $a^3 \neq 0$, sans quoi $\{0,1,a,a^2\}$ serait une sous–algèbre stricte de $\mathcal{A}$ contenant a. Il en résulte que $\mathcal{A} = \{0,a^3,a^2,a,1\}$; du fait que $a^4+a^3 = a^3(a+1) = a^3.1 = a^3$ suit $a^4 \leq a^3$ d'où deux éventualités :

(4.11.5.1)
$$\begin{Bmatrix} a+1=1 \\ a^4=0 \end{Bmatrix} ,$$

et :

(4.11.5.2)
$$\begin{Bmatrix} a+1=1 \\ a^4=a^3 \end{Bmatrix} .$$

$1^o)\beta)$ $a+1=a$.

Alors $a^2+a=a^2$, $a^3+a^2=a^3$, et il suit d'arguments similaires à ceux utilisés en $1^0)\alpha)$ que $0<1<a<a^2<a^3$. Mais alors $a^4=a^3$ et :

(4.11.5.3)
$$\begin{Bmatrix} a+1=a \\ a^4=a^3 \end{Bmatrix} .$$

$2^0)$ $a+1\notin\{0,1,a\}$.

Il s'ensuit que $a^2\notin\{0,1,a,a+1\}$, sans quoi $\{0,1,a,a+1\}$ serait une sous–algèbre stricte de $\mathcal{A}$ contenant a. On a donc $\mathcal{A}=\{0,1,a,a+1,a^2\}$, et neuf possibilités sont alors à distinguer :

$2^0)\alpha)$ $a^2+1=1$ et $a^2+a=a$; alors $a^3+a^2=a(a^2+a)=a^2$, et $a^3+a=a(a^2+1)=a$, d'où $0\le a^3\le a^2<1$ et $0\le a^3\le a^2<a$ et encore deux éventualités :

(4.11.5.4)
$$\begin{Bmatrix} a^2+1=1 \\ a^2+a=a \\ a^3=0 \end{Bmatrix} ,$$

et :

(4.11.5.5)
$$\begin{Bmatrix} a^2+1=1 \\ a^2+a=a \\ a^3=a^2 \end{Bmatrix} .$$

$2^0)\beta)$ $a^2+1=1$ et $a^2+a=a^2$.

Mais alors $a+1=a+(a^2+1)=(a^2+a)+1=a^2+1=1$, une contradiction.

$2^0)\gamma)$ $a^2+1=1$ et $a^2+a=a+1$.

Mais alors $a^3+a=a$ et $a^3+a^2=a^2+a=a+1$ d'où $a^3\notin\{0,1,a+1,a^2\}$, et $a^3=a$:

(4.11.5.6)
$$\begin{Bmatrix} a^2+1=1 \\ a^2+a=a+1 \\ a^3=a \end{Bmatrix} .$$

$2^0)\delta)$ $a^2+1=a^2$ et $a^2+a=a$.

Alors $1<a^2<a$, d'où $a+1=a$, une contradiction.

$2^0)\epsilon)$ $a^2+1=a^2$ et $a^2+a=a^2$.

Alors il suit : $0<1<a^2$ et $0<a<a^2$, d'où $a^2>a+1$; de plus $a^3+a^2=a^3$ d'où $a^3\geq a^2$ et $a^3=a^2$:

(4.11.5.7)
$$\left\{\begin{aligned} a^2+1&=a^2\\ a^2+a&=a^2\\ a^3&=a^2\end{aligned}\right\} .$$

$2^0)\zeta)$ $a^2+1=a^2$ et $a^2+a=a+1$.

Alors $a^3+a=a^3$ et $a^3+a^2=a^2+a=a+1$, d'où $a^3\notin\{0,1,a^2\}$, et $a^3=a$ ou $a^3=a+1$, soit :

(4.11.5.8)
$$\left\{\begin{aligned} a^2+1&=a^2\\ a^2+a&=a+1\\ a^3&=a\end{aligned}\right\} \text{ , ou :}$$

(4.11.5.9)
$$\left\{\begin{aligned} a^2+1&=a^2\\ a^2+a&=a+1\\ a^3&=a+1\end{aligned}\right\} .$$

$2^0)\eta)$ $a^2+1=a+1$ et $a^2+a=a$. Alors $a^3+a=a^2+a=a$ et $a^3+a^2=a^2$, d'où $a^3\notin\{1,a,a+1\}$, et $a^3=0$ ou $a^3=a^2$:

(4.11.5.10)
$$\left\{\begin{aligned} a^2+1&=a+1\\ a^2+a&=a\\ a^3&=0\end{aligned}\right\} ,$$

ou :

(4.11.5.11)
$$\left\{\begin{aligned} a^2+1&=a+1\\ a^2+a&=a\\ a^3&=a^2\end{aligned}\right\} .$$

$2^0)\theta)$ $a^2+1=a+1$ et $a^2+a=a^2$.

Alors $a^3+a=a^2+a=a^2$ et $a^3+a^2=a^3$, d'où $a^3\notin\{0,1,a,a+1\}$, et $a^3=a^2$, soit :

(4.11.5.12)
$$\left\{\begin{aligned} a^2+1&=a+1\\ a^2+a&=a^2\\ a^3&=a^2\end{aligned}\right\} .$$

$2^0)\iota)$ $a^2+1=a+1$ et $a^2+a=a+1$.

Alors $a^3+a = a^2+a = a+1$ et $a^3+a^2 = a^2+a = a+1$ d'où $a^3 \notin \{0,a,a^2\}$, et $a^3=1$ ou $a^3=a+1$:

(4.11.5.13)
$$\begin{Bmatrix} a^2+1=a+1 \\ a^2+a=a+1 \\ a^3=1 \end{Bmatrix}$$

ou :

(4.11.5.14)
$$\begin{Bmatrix} a^2+1=a+1 \\ a^2+a=a+1 \\ a^3=a+1 \end{Bmatrix} .$$

Réciproquement (4.11.5.1),..., (4.11.5.14) définissent chacun une algèbre de cardinal 5, et on a bien :

$$\mathbf{c_5 = 14} .$$

On observe que, pour $2 \leq n \leq 5$,

$$c_n = \frac{3}{2}n^2 - \frac{13}{2}n + 9 .$$

Zhu ([7]) a conjecturé qu'il en était de même pour tout $n \geq 2$; il affirme l'avoir vérifié jusques $n = 8$ inclusivement.

5. Deux foncteurs

Comme ci–dessus, par $\mathcal{D}$ nous entendrons la catégorie des F_1–anneaux au sens de Deitmar, c'est–à–dire ([4], p.88) la catégorie des monoïdes commutatifs, et par $\mathcal{Z}_a$ la catégorie des B_1–algèbres au sens de la Définition 4.1.

Théorème 5.1. *Pour $A \in \mathcal{D}$, posons $\mathcal{F}(A) = \mathcal{P}_f(A)$, et définissons sur $\mathcal{F}(A)$ la multiplication suivante :*

$$B.C =_{def} \{xy | x \in B, y \in C\}.$$

Alors $\mathcal{F}(A)$, muni de la structure de B_1–module associée à sa structure naturelle d'ensemble ordonné décent (cf. Théorème 2.5) et de la multiplication sus-définie, constitue une B_1–algèbre. On a $\mathcal{F}(F_1) = B_1$. De plus, si A_1 et A_2 sont deux éléments de $\mathcal{D}$, et $\varphi : A_1 \to A_2$ un morphisme, alors $\mathcal{F}(\varphi) : \mathcal{F}(A_1) \to \mathcal{F}(A_2)$ défini par :

$$\forall B \in \mathcal{F}(A_1) \;\; \mathcal{F}(\varphi)(B) = \{\varphi(b) | b \in A_1\}$$

est un morphisme de $\mathcal{Z}_a$, et $\mathcal{F}$ définit un foncteur covariant de $\mathcal{D}$ dans $\mathcal{Z}_a$.

Démonstration. Que $\mathcal{F}(A) = \mathcal{P}_f(A)$, muni de sa structure naturelle de treillis, constitue un B_1–module, résulte du Théorème 2.5.

Il est clair que la multiplication définie ci–dessus est associative, commutative, et d'élément neutre $1_{\mathcal{F}(A)} = \{1_A\}$; sa distributivité par rapport à l'addition est également évidente, l'addition dans $\mathcal{F}(A)$ n'étant autre que la *réunion* ensembliste. De plus, pour chaque $B \in \mathcal{F}(A)$, on a :

$$\begin{aligned} 0_{\mathcal{F}(A)}.B &= \emptyset.B \\ &= \{ab|a \in \emptyset, b \in B\} \\ &= \emptyset \\ &= 0_{\mathcal{F}(A)} \ ; \end{aligned}$$

tous les axiomes de la Définition 4.1 sont bien satisfaits, et $\mathcal{F}(A)$ est une B_1–algèbre. Il est clair que $\mathcal{F}(F_1) = B_1$. La validité de la définition de $\mathcal{F}(\varphi)$ et la fonctorialité de $\mathcal{F}$ peuvent alors être vérifiées sans problème. □

Remarque 5.2. Si A est le monoïde libre sur un ensemble fini X (en d'autres termes, $A \simeq (\mathbb{N}^X, +)$), alors $\mathcal{F}(A)$ s'identifie à la B_1–algèbre libre $B_1[X]$ construite ci-dessus(cf. le Théorème 4.5, ainsi que la remarque le précédant).

Soit $\mathcal{G} : \mathcal{Z}_a \to \mathcal{D}$ le "foncteur d'oubli"associant à une B_1–algèbre le monoïde multiplicatif sous–jacent.

Proposition 5.3. *Les foncteurs $\mathcal{F}$ et $\mathcal{G}$ sont adjoints l'un de l'autre.*

Démonstration. Soient $A \in \mathcal{Z}_a$ et $B \in \mathcal{D}$; il s'agit de faire voir l'existence d'une bijection naturelle :

$$Hom_{\mathcal{Z}_a}(\mathcal{F}(B), A) \simeq Hom_{\mathcal{D}}(B, \mathcal{G}(A)) \ .$$

Soit donc $\varphi : \mathcal{F}(B) \to A$ un $\mathcal{Z}_a$–morphisme ; pour chaque $b \in B$, $\varphi(\{b\})$ est un élément $\psi(b) \in A$, et il est clair que ψ préserve la multiplication et l'élément neutre (car

$$\begin{aligned} \forall (b, b^{'}) \in B^2 \ \ \psi(bb^{'}) &= \varphi(\{bb^{'}\}) \\ &= \varphi(\{b\}\{b^{'}\}) \\ &= \varphi(\{b\})\varphi(\{b^{'}\}) \\ &= \psi(b)\psi(b^{'}) \end{aligned}$$

et

$$\psi(1_B) = \varphi(\{1_B\}) = \varphi(1_{\mathcal{F}(B)}) = 1_A) \ ,$$

donc $\psi : B \to A = \mathcal{G}(A)$ est un morphisme de $\mathcal{D}$. Définissant $\Lambda(\varphi) = \psi$, il est clair que

$$\Lambda : Hom_{\mathcal{Z}_a}(\mathcal{F}(B), A) \to Hom_{\mathcal{D}}(B, \mathcal{G}(A))$$

est une bijection, dont la bijection inverse est définie par :

$$\forall C \in \mathcal{F}(B) \ \ \Lambda^{-1}(\psi)(C) = \bigvee_{x \in C} \psi(x) \ .$$

□

Exemple 5.4. Si $A =< x >$ est le monoïde libre engendré par un élément x, alors $\mathcal{F}(A) = B_1[x]$ est l'anneau des fonctions sur la droite affine $Spec(C_\infty)$ de Deitmar ([4]).

Exemple 5.5. Si $A = \mu_n (n \geq 1)$ est le groupe cyclique d'ordre n ($A =< x >$ avec $x^n = 1$), alors $\mathcal{F}(A)$ est le quotient de $B_1[x]$ par la congruence (cf. Définition 4.2) engendrée par la relation $x^n \sim 1$: $\mathcal{F}(A)$ est de cardinal 2^n, et apparaît comme l'anneau des fonctions sur l'espace $Spec(\mu_n)$ au sens de Deitmar ([4]).

Exemple 5.6. Si $A =< \tau, \tau^{-1} >\simeq \mathbf{Z}$ est un groupe monogène infini (engendré par τ), $B_1[A] = B_1[\tau, \tau^{-1}]$ est le B_1–anneau des fonctions sur le groupe multiplicatif GL_1 de Deitmar ([4],p.93). On peut aussi le voir comme le quotient du B_1–anneau $B_1[x, y]$ par la congruence engendrée par la relation $xy \sim 1$.

Lemme 5.7. *Pour tout $A \in \mathcal{D}$,*

$$\mathcal{F}(A)^* = j_A(A^*) = \{\{u\}|u \in A^*\} \ .$$

Démonstration. Soit $B \in \mathcal{F}(A)$ inversible : alors il existe $C \in \mathcal{F}(A)$ tel que $BC = 1_{\mathcal{F}(A)} = \{1_A\}$. Alors on a nécessairement $B \neq \emptyset$ et $C \neq \emptyset$; soient alors fixés $b_0 \in B$ et $c_0 \in C$. On a $b_0c_0 \in BC$, donc $b_0c_0 = 1_A$: b_0 et c_0 sont inversibles. Pour chaque $b \in B$, on a donc $bc_0 \in BC = \{1_A\}$, donc $bc_0 = 1_A$ et $b = c_0^{-1} = b_0$: $B = \{b_0\} = j_A(b_0) \in j_A(A^*)$ d'où $\mathcal{F}(A)^* \subseteq j_A(A^*)$. L'inclusion réciproque est évidente. □

Corollaire 5.8. *Soit ψ un morphisme de $\mathcal{F}(A)$ dans $\mathcal{F}(B)$; alors*

$$\psi(j_A(A^*)) \subseteq j_B(B^*) \ .$$

Démonstration. Il suffit de remarquer que ψ transforme tout élement inversible de $\mathcal{F}(A)$ en un élément inversible de $\mathcal{F}(B)$, et d'appliquer le Lemme 5.7. □

Remarque 5.9. Le foncteur $\mathcal{F} : \mathcal{D} \to \mathcal{Z}_a$ n'est pas pleinement fidèle : si $A =< x >$ est un monoïde libre à un générateur x, le morphisme de $B_1[x] = B_1[A]$ dans lui-même défini par $x \to x + 1$ ne provient pas d'un morphisme de monoïdes de A dans lui-même .

Néanmoins la situation est meilleure si l'on se restreint à la catégorie des groupes (abéliens) :

Proposition 5.10. *La restriction de $\mathcal{F}$ à la catégorie $\mathcal{A}b$ des groupes abéliens (laquelle est une sous–catégorie pleine de $\mathcal{D}$) est pleinement fidèle.*

Démonstration. Si A et B sont des groupes abéliens et ψ un morphisme de $\mathcal{F}(A)$ dans $\mathcal{F}(B)$, il résulte de la Proposition que $\psi(j_A(A)) \subseteq j_B(B)$; donc, pour chaque $a \in A$, il existe $\varphi(a) \in B$ tel que $\psi(j_A(a)) = j_B(\varphi(a))$. Il est maintenant clair que $\varphi : A \to B$ est un morphisme, et que $\psi = \mathcal{F}(\varphi)$. L'application naturelle

$$Hom_{\mathcal{A}b}(A, B) \to Hom_{\mathcal{Z}_a}(\mathcal{F}(A), \mathcal{F}(B))$$

est donc surjective, d'où le résultat. □

6. Une remarque

Le Lemme suivant est l'analogue, pour des monoïdes, d'un résultat classique de Dedekind sur les anneaux.

Lemme 6.1. *Soient $A \in \mathcal{D}$ un monoïde commutatif, et $B \subset A$ un sous–monoïde de A tel que A soit entier sur B.*

Alors A est un groupe si et seulement si B en est un.

Démonstration. Supposons que A soit un groupe, et soit $b \in B$; alors il existe $b^{'} \in A$ tel que $bb^{'} = 1$. Mais, par hypothèse, on peut trouver un entier $n \geq 1$ tel que ${b^{'}}^{n} \in B$, d'où :

$$\begin{aligned} 1 &= 1^n \\ &= (bb^{'})^n \\ &= b^n {b^{'}}^{n} \\ &= b(b^{n-1}{b^{'}}^{n}). \end{aligned}$$

Soit $c = b^{n-1}{b^{'}}^{n}$; alors $c \in B$ et $bc = 1$: b est donc bien inversible *dans* B . Chaque élément de B y étant inversible, B est un groupe.

Réciproquement, supposons que B soit un groupe, et soit $a \in A$; par hypothèse, il existe un entier $n \geq 1$ tel que $a^n \in B$. B étant un groupe, il existe $b^{'} \in B$ tel que $a^n b^{'} = 1$; mais alors :

$$\begin{aligned} 1 &= a^n b^{'} \\ &= a(a^{n-1}b^{'}), \end{aligned}$$

et a est inversible : A est un groupe.

□

Il s'ensuit le :

Corollaire 6.2. *Si $B \subset A$ est une extension algébrique au sens de Deitmar (*[5], §2*), alors A est un groupe si et seulement si B en est un.*

Références

1. G.Birkhoff *Lattice Theory*, American Mathematical Society, Colloquium Publications, vol. 25, 1967.
2. A. Connes and C. Consani *Schemes over F_1 and zeta functions*, preprint ; arXiv :0903.2024 v3 9 Jul 2009
3. B.A.Davey and H.A.Priestley *Introduction to lattices and order*, Cambridge University Press, 1990.
4. A.Deitmar *Schemes over F_1*, in *Number Fields and Function Fields - two parallel worlds*, pages 87-100, Birkhaüser, Boston, 2005.
5. A. Deitmar *F_1–schemes and toric varieties*, preprint ; arXiv :math.NT/0608179 v9 29 Nov 2007
6. C. Soulé *Les variétés sur le corps à un élément*, Moscow Math. Journal, Vol. 4, no 1, 2004, pages 217-244.
7. Y. Zhu *Combinatorics and characteristic one algebra*, preprint, 2000.

Laboratoire de Mathématiques Raphaël Salem, UMR 6085 CNRS, Université de Rouen, Technopôle du Madrillet, Avenue de l'Université, B.P. 12, 76801 Saint-Etienne-du-Rouvray (FRANCE), Tél. 00 33 (0)2 32 95 52 24, Fax 00 33 (0)2 32 95 52 86, Paul.Lescot@univ-rouen.fr,