Sur un 'corps de caractéristique 1' (d'après Zhu)

Paul LESCOT

Institut des Hautes Études Scientifiques
35, route de Chartres
91440 – Bures-sur-Yvette (France)

Décembre 2006

IHES/M/06/61

SUR UN "CORPS DE CARACTÉRISTIQUE 1"(D'APRÈS ZHU)

PAUL LESCOT

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

1. Introduction et définitions

L'objet de cet exposé est de justifier certaines des affirmations contenues dans le *preprint* ([5]) de Zhu. 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. Zhu est parvenu à définir un objet algébrique F_1 possédant"la plupart"des propriétés des corps, et tel qu'en un sens précis, on ait $GL_n(F_1) \simeq \Sigma_n$. Nous allons développer l'algèbre linéaire et la géométrie algébrique sur F_1 en restant aussi près que possible des définitions classiques. Il s'avère que la catégorie des F_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.

Nous nous proposons de dégager dans une prochaine publication un terrain commun entre ces résultats et ceux de Deitmar ([3]) et Soulé ([4]).

Une première version de ce texte avait fait l'objet d'un exposé au Groupe de Travail Interuniversitaire d'Algèbre, le 15 Janvier 2001 ; je remercie Jacques Alev, Dominique Castella, François Dumas et Laurent Rigal pour leurs commentaires à cette occasion.

Définition 1.1. On notera F_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 1.2. Il est visible que F_1 satisfait à tous les axiomes des corps commutatifs, excepté à celui qui affirme l'existence de symétriques pour l'addition.

Définition 1.3. On appelle F_1-module la donnée d'un monoïde commutatif M d'élément neutre 0 et d'une F_1-loi externe sur M (c'est-à-dire d'une application

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

Date: 06 Décembre 2006.

de $F_1 \times M$ dans M), ayant les propriétés usuelles, *i.e.* :

$$\forall(\lambda,\mu,x) \in F_1 \times F_1 \times M \quad (\lambda+\mu)x = \lambda x + \mu x \quad , \tag{1}$$

$$\forall(\lambda,x,y) \in F_1 \times M \times M \quad \lambda(x+y) = \lambda x + \lambda y \quad , \tag{2}$$

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

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

Définition 1.4. 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 1.5. *La catégorie des F_1–modules s'identifie canoniquement à la catégorie des ensembles ordonnés décents.*

Démonstration. Soit M un F_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 $(E, \leq, 0)$ 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

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

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

et

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

font de E un F_1–module.

Il reste à déterminer les *morphismes* de F_1–modules. Soit $\varphi : M \to N$ un tel morphisme ; on a nécessairement :

$$\varphi(0_M) = \varphi(00_M) = 0\varphi(0_M) = 0_N ,$$

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 F_1–modules. □

Théorème 1.6. *Modulo l'identification établie par le Théorème 1.5, la catégorie des F_1–modules finis s'identifie à celle des treillis finis non vides.*

Démonstration. Soit T un F_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. □

2. Algèbre linéaire sur F_1

Théorème 2.1. *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*

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

fait de $\mathcal{P}_f(A)$ le F_1–module libre engendré par A. En particulier, la catégorie des F_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 F_1–module M et toute application $\varphi : A \to M$, il existe un unique morphisme

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

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

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

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 F_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 F_1–module M est projectif si, quels que soient les F_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 F_1–module libre est évidemment projectif.

Définition 2.2. 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 F_1–module (en fait, $\mathcal{O}(E)$ est un sous-treillis (distributif) de $\mathcal{P}(E)$).

Théorème 2.3. *Les propriétés suivantes d'un treillis fini non vide M sont équivalentes :*

- *M, considéré comme F_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 F_1–module, est isomorphe à un sous–module d'un F_1–module libre.*

Remarque 2.4. L'équivalence (2) $\iff$ (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 [2], p.171, Theorem 8.17.

Démonstration. (1) $\implies$ (2) :
Soient $N_1 = \mathcal{P}(M)$, $N_2 = M$ et

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

Il est visible que ψ est un morphisme surjectif de F_1–modules, donc il existe un morphisme $\rho : M \to \mathcal{P}(M)$ tel que $\psi\circ\rho = Id_M$. Mais alors, pour tout $(a, b, c) \in M^3$:

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

d'où :

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

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 ; [2], Lemma 6.3, p.130), la distributivité de $\vee$ par rapport à $\wedge$ s'ensuit. En effet, l'on peut écrire, pour $(a, b, c) \in M^3$:

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

(2) $\implies$ (3) :
Soit E l'ensemble des éléments $m \neq 0$ de M *irréductibles pour* $\vee$, *i.e.* tels que :

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

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 $\leq|_{M_0}$) 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

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

j'affirme que φ est un morphisme bijectif de F_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

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

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–F_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 F_1–module *fini* , donc un treillis d'après le Théorème 1.6, 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 F_1–modules ; alors $\varphi \circ \theta : \mathcal{P}(E) \to N_2$ est un morphisme de F_1–modules. $\mathcal{P}(E) = \mathcal{P}_f(E)$ étant libre (Théorème 2.1), 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. □

Théorème 2.5. $GL_n(F_1) \simeq \Sigma_n$.

Démonstration. $GL_n(F_1)$ désigne par définition le groupe des automorphismes d'un F_1–module libre (M) de rang n. D'après le Théorème 2.1, on peut supposer que $M = \mathcal{P}(A)$ 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 :

$$GL_n(F_1) \simeq \Sigma(A) \simeq \Sigma_n \ .$$

□

3. Géométrie algébrique sur F_1

Définition 3.1. On appelle F_1–algèbre (commutative, unitaire) la donnée d'un F_1–module $\mathcal{A}$, contenant F_1, et d'une multiplication sur $\mathcal{A}$, associative, commutative, d'élément neutre 1, et bilinéaire par rapport aux opérations de F_1–module.

Définition 3.2. On appelle congruence sur la F_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 F_1–algèbre.

Définition 3.3. On définit sur l'ensemble des congruences sur la F_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 3.4. *Si l'algèbre quotient $\mathcal{A}/\sim$ est isomorphe à F_1, la congruence $\sim$ est maximale.*

Il est facile de voir que la F_1–algèbre libre $F_1[x]$ s'identifie à l'ensemble des sommes formelles (éventuellement vides) de puissances de x (en posant $x^0 = 1$). Plus généralement :

Théorème 3.5. *La F_1–algèbre libre sur $A = \{x_1, ..., x_n\}$ s'identifie à l'ensemble des combinaisons libres de monômes $x_1^{\alpha_1}...x_n^{\alpha_n}$ ($\alpha_i \in \mathbf{N}$) muni des opérations évidentes. Plus précisément, soit*

$$F_1[A] = \mathcal{P}_f(\mathbf{N}^A)$$

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 $F_1[A]$ la F_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 F_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 $F \in \mathcal{P}_f(\mathbf{N}^A)$:

(9)

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

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

Définition 3.6. Pour $B \subset A$ et $R \in F_1[A]$, soit

$$F_B(R) = \{r \in R \mid r(B) \subseteq \{0\}\}.$$

Théorème 3.7. *Pour chaque $B \subset A$, la relation $\sim_B$ sur $F_1[A]$ définie par : $R \sim S$ si et seulement si $F_B(R) = F_B(S) = \emptyset$ ou $F_B(R) \neq \emptyset \neq F_B(S)$ est une congruence sur $F_1[A]$, et*

$$F_1[A]/\!\sim_B \simeq F_1 \ .$$

Démonstration. De

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

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

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

et

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

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

$$F_1[A]/\!\sim_B = \{\bar{0}, \bar{1}\} \ ,$$

d'où :

$$F_1[A]/\!\sim_B \simeq F_1.$$

□

En particulier, pour chaque $B \subset A$, la congruence $\sim_B$ sur $F_1[A]$ est maximale (Théorème 3.4), et $F_1[A]/\sim_B \simeq F_1$. Réciproquement, toute congruence (maximale) $\sim$ sur $F_1[A]$ telle que $F_1[A]/\sim \simeq F_1$ est de la forme $\sim_B$ pour un $B \subset A$ (il suffit de prendre

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

Il paraît plausible que soit correcte la

Conjecture 3.8. *Tout quotient de $F_1[A]$ par une congruence maximale est isomorphe à F_1.*

D'après la discussion précédente, il revient au même de dire que toute congruence maximale sur $F_1[A]$ est de la forme $\sim_B$ pour un $B \subset A$. 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 la Conjecture 3.8 en la

Conjecture 3.9. *F_1 est algébriquement clos et $Spec(F_1)$ se compose de 2^n points fermés.*

Les F_1–algèbres *monogènes* forment déjà une famille très riche. Soient en effet, pour $n \geq 2$, C_n l'ensemble des congruences $\sim$ sur $F_1[x]$ telles que $\mathcal{A} = F_1[x]/\sim$ soit de cardinal n, et soit $c_n = |C_n|$. Des expériences numériques incitent à croire en la

Conjecture 3.10. *Pour chaque $n \geq 2$, on a*

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

Nous allons vérifier cette hypothèse pour $2 \leq n \leq 5$, et déterminer ce faisant les types d'isomorphisme de F_1–algèbres de cardinal n. Soit donc $\mathcal{A} = F_1[x]/\sim$ de cardinal n, et soit a l'image de $x \in F_1[x]$ dans $\mathcal{A}$ par la projection canonique.

Pour $n = 2$ on a $\mathcal{A} = F_1$, d'où

(2.1)
$$a = 0$$

ou

(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 :

(3.1)
$$\left\{ \begin{array}{r} a + 1 = a \\ a^2 = a \end{array} \right\}$$

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

(3.2)
$$\left\{\begin{array}{c} a+1=1 \\ a^2=0 \end{array}\right\}$$

ou :

(3.3)
$$\left\{\begin{array}{c} a+1=1 \\ a^2=a \end{array}\right\}.$$

On vérifie facilement que les algèbres respectivement définies par (3.1), (3.2) et (3.3) sont bien de cardinal 3. Il existe donc exactement trois congruences $\sim$ sur $F_1[x]$ telles que $F_1[x]/\sim$ 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–F_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 :

(4.1)
$$a^2=0\ ,$$

(4.2)
$$a^2=1\ ,$$

(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 $0\le a^3\le a^2<a<1$, et encore deux éventualités :

(4.4)
$$\left\{\begin{array}{c} a+1=1 \\ a^3=a^2 \end{array}\right\}\ ,$$

et

(4.5)
$$\left\{\begin{array}{c} a+1=1 \\ a^3=0 \end{array}\right\}\ .$$

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

(4.6)
$$\left\{\begin{array}{c} a+1=a \\ a^2=a^3 \end{array}\right\}\ .$$

$2^0)\gamma$)

(4.7)
$$a^2 = a + 1 \ .$$

Réciproquement (4.1),..., (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–F_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 :

(5.1)
$$\left\{ \begin{array}{r} a + 1 = 1 \\ a^4 = 0 \end{array} \right\} \ ,$$

et :

(5.2)
$$\left\{ \begin{array}{r} a + 1 = 1 \\ a^4 = a^3 \end{array} \right\} \ .$$

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

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 :

(5.3)
$$\left\{ \begin{array}{r} a + 1 = a \\ a^4 = a^3 \end{array} \right\} \ .$$

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

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 $0 \leq a^3 \leq a^2 < 1$ et $0 \leq a^3 \leq a^2 < a$ et encore deux éventualités :

(5.4)
$$\left\{ \begin{array}{r} a^2 + 1 = 1 \\ a^2 + a = a \\ a^3 = 0 \end{array} \right\} \ ,$$

et :

(5.5)
$$\left\{\begin{array}{c} a^2+1=1 \\ a^2+a=a \\ a^3=a^2 \end{array}\right\} .$$

$2^0)\beta)$ $a^2+1=1$ 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 $a^3=a$:

(5.6)
$$\left\{\begin{array}{c} a^2+1=1 \\ a^2+a=a+1 \\ a^3=a \end{array}\right\} .$$

$2^0)\delta)$ $a^2+1=a^2$ 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 $a^3=a^2$:

(5.7)
$$\left\{\begin{array}{c} a^2+1=a^2 \\ a^2+a=a^2 \\ a^3=a^2 \end{array}\right\} .$$

$2^0)\zeta)$ $a^2+1=a^2$ 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 :

(5.8)
$$\left\{\begin{array}{c} a^2+1=a^2 \\ a^2+a=a+1 \\ a^3=a \end{array}\right\} \text{ , ou :}$$

(5.9)
$$\left\{\begin{array}{c} a^2+1=a^2 \\ a^2+a=a+1 \\ a^3=a+1 \end{array}\right\} .$$

$2^0)\eta)$ $a^2+1=a+1$ 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 $a^3=a^2$:

(5.10)
$$\left\{\begin{array}{c} a^2+1=a+1 \\ a^2+a=a \\ a^3=0 \end{array}\right\} ,$$

ou :

(5.11)
$$\left\{\begin{array}{c} a^2+1=a+1 \\ a^2+a=a \\ a^3=a^2 \end{array}\right\} .$$

$2^0)\theta)$ $a^2+1=a+1$ 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 :

(5.12)
$$\left\{\begin{array}{c} a^2+1=a+1 \\ a^2+a=a^2 \\ a^3=a^2 \end{array}\right\} .$$

$2^0)\iota)$ $a^2+1=a+1$ 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 $a^3=a+1$:

(5.13)
$$\left\{\begin{array}{c} a^2+1=a+1 \\ a^2+a=a+1 \\ a^3=1 \end{array}\right\}$$

ou :

(5.14)
$$\left\{\begin{array}{c} a^2+1=a+1 \\ a^2+a=a+1 \\ a^3=a+1 \end{array}\right\} .$$

Réciproquement (5.1),..., (5.14) définissent chacun une algèbre de cardinal 5, et on a bien :

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

Références

1. G.Birkhoff *Lattice Theory*, American Mathematical Society, Colloquium Publications, vol. 25, 1967.
2. B.A.Davey and H.A.Priestley *Introduction to lattices and order*, Cambridge University Press, 1990.
3. A.Deitmar *Schemes over F_1*, in *Number Fields and Function Fields - two parallel worlds*, pages 87-100, Birkhaüser, Boston, 2005.
4. C. Soulé *Les variétés sur le corps à un élément*, Moscow Math. Journal, Vol. 4, no 1, 2004, pages 217-244.
5. Y. Zhu *Combinatorics and characteristic one algebra*, preprint, 2000.

INSSET–Université de Picardie, 48 Rue Raspail, 02100 Saint–Quentin (FRANCE), paul.lescot@insset.u-picardie.fr, Fax 00 33 (0)3 23 62 89 35, LAMFA, Faculté de Mathématiques et d'Informatique, 33, Rue Saint-Leu, 80039 Amiens Cédex, Tél. 03 22 82 79 70, Fax 03 22 82 78 38, paul.lescot@u-picardie.fr,