Traduction de la partie 5 de l'article de Connes-Consani paru sur arxiv en août 2022 (Denise Vella-Chemla, août 2022)

5. $\mathbb{S}[\pm 1][3]$ et l'anneau des entiers

Dans notre travail récent [1] sur le théorème de Riemann-Roch arithmétique pour $\overline{Spec\,\mathbb{Z}}$, le nombre 3 joue le rôle d'un générateur naturel, permettant d'étiqueter les entiers $m \in \mathbb{Z}$ comme des polynômes de puissances de 3 avec coefficients dans $\mathbb{S}[\pm 1]$

$$P(X) = \sum_{j=0}^{k} a_j X^j, \quad a_j \in \{-1, 0, 1\}, \ \forall j. \tag{5.1}$$

La subtilité de la description de la structure d'anneau des entiers $\mathbb{Z}$ dans cette paramétrisation découle de l'addition des polynômes à coefficients dans le monoïde multiplicatif $\{-1, 0, 1\}$. Ici $\{-1, 0, 1\}$ est muni de la règle évidente de la multiplication, donc on sait comment multiplier les monômes *i.e.* $a\,X^n \times b\,X^m = (ab)\,X^{n+m}$, alors que le produit de polynômes est obtenu de manière unique, en utilisant la loi de distributivité, en supposant qu'on sait comment les additionner. La somme de deux monômes $a\,X^n, b\,X^m$ de degrés différents est simplement le polynôme $a\,X^n + b\,X^m$ et quand les degrés sont identiques la loi de distributivité $a\,X^n + b\,X^n = (a+b)X^n$ se réduit à reconstruire la somme des polynômes de degré 0.

Nous allons nous assurer que l'addition est définie sur les polynômes de degré 0 de telle façon que la règle suivante soit vérifiée :

La somme de 3 polynômes de degré 0 est un polynôme de degré $\leqslant 1$.

En utilisant cette hypothèse, on obtient, par induction sur le degré n, que la somme de deux polynômes de degré $\leqslant n$ est un polynôme de degré $\leqslant n+1$. Le besoin de nécessiter que la somme de trois polynômes de degré 0 soit de degré $\leqslant 1$ (plutôt que seulement la somme de deux polynômes), est dû au rôle de la retenue lorsqu'on ajoute des polynômes arbitraires.

Considérons maintenant l'addition de deux éléments de $\{-1, 0, 1\}$. Si l'un d'eux est 0 ou s'ils sont de signes opposés, alors la somme est la somme évidente. Ainsi, en utilisant la symétrie $x \mapsto -x$, on peut supposer qu'il sont tous les deux égaux à 1. La seule nouvelle règle que l'on ajoute est la règle suivante

$$1 + 1 = X - 1. \tag{5.2}$$

En appliquant (5.2), on ajoute deux polynômes de degré 0 en utilisant la table suivante

$+$	-1	0	1
-1	$1-X$	-1	0
0	-1	0	1
1	0	1	$X-1$

Pour spécifier la somme de trois polynômes de degré 0, il suffit de savoir comment ajouter au polynôme $X-1$ les éléments de $\{-1, 0, 1\}$. En utilisant l'associativité de la somme et (5.2), on a

$$(X-1)+1 = X, \qquad (X-1)-1 = X-(1+1) = X-(X-1) = 1.$$

Il s'ensuit alors que, comme requis, la somme de 3 polynômes de degré 0 est un polynôme de degré $\leqslant 1$. Le résultat suivant détermine la somme de n'importe quelle somme de polynômes selon (5.2).

PROPOSITION 5.1. *Soit $P(X)$ et $Q(X)$ deux polynômes tels que dans (5.1), de degrés au plus n. Alors il existe un unique polynôme de degré au plus $n+1$ qui coïncide, en utilisant la règle (5.2), avec la somme $P(X)+Q(X)$.*

PREUVE : Supposons (par induction) que l'assertion est vérifiée pour n'importe quels polynômes de degrés $< n$ et considérons une paire $P(X)$, $Q(X)$ tous les deux de degré n. On décompose $P(X) = P_1(X) + \alpha_n X^n$, $Q(X) = Q_1(X) + \beta_n X^n$, avec $\alpha_n, \beta_n \in \{-1, 0, 1\}$. Alors

$$P(X) + Q(X) = P_1(X) + Q_1(X) + (\alpha_n + \beta_n)X^n,$$

où $P_1(X) + Q_1(X)$ est, par induction, la somme d'un polynôme de degré $n-1$ avec un terme γX^n, $\gamma \in \{-1, 0, 1\}$. Alors, de la spécification de la somme de trois polynômes de degré zéro, on a $\alpha_n + \beta_n + \gamma = \delta + \epsilon X$, avec $\delta, \epsilon \in \{-1, 0, 1\}$. Ainsi la somme $P(X) + Q(X)$ peut s'écrire comme un polynôme de degré au plus $n+1$, où les termes de degré $\geqslant n$ sont $\delta X^n + \epsilon X^{n+1}$. □

On obtient la conclusion intrigante suivante

PROPOSITION 5.2. *L'ensemble des polynômes tels que dans (5.1), avec la règle d'addition fournie dans la Proposition 5.1, et l'unique produit associé, forme un anneau isomorphe à $\mathbb{Z}$.*

PREUVE : L'application

$$\theta : \sum \alpha_j X^j \mapsto \sum \alpha_j 3^j$$

est une bijection de l'ensemble des polynômes tels que dans (5.1) vers les entiers. Cette application est compatible avec l'addition et la multiplication vues dans la Proposition 5.1. □

Il y a une fonction qui permet de calculer effectivement des sommes de polynômes comme ci-dessus. C'est une fonction de trois variables α, β, γ dans $\{-1, 0, 1\}$ qui spécifie leur somme comme étant un polynôme de degré au plus 1 dans X. Pour déterminer $\alpha + \beta + \gamma$ on peut y penser comme à une somme de 3 nombres réels et écrire l'ensemble $\{-1, 0, 1\} + \gamma$ auquel cette somme appartient, pour obtenir le coefficient de X. Au niveau algébrique, $\alpha + \beta + \gamma$ peut être écrit explicitement en utilisant le corps fini $\mathbb{F}_3 = \{-1, 0, 1\}$ comme suit

$$\alpha + \beta + \gamma = \overline{\alpha + \beta + \gamma} + \overline{\sigma(\alpha, \beta, \gamma)}\ X$$

où $\overline{m}$ est le reste de m modulo 3 et

$$\sigma(\alpha, \beta, \gamma) := \alpha\beta\gamma - \alpha^2\beta - \alpha^2\gamma - \alpha\beta^2 - \alpha\gamma^2 - \beta^2\gamma - \beta\gamma^2.$$

Cela détermine l'expression algébrique pour la somme de trois polynômes de degré 0 comme dans la preuve de la Proposition [5.1]. Alors, par induction sur n, on obtient une expression algébrique pour les coefficients de X^n dans la somme $\sum_j \alpha_j X^j + \sum_j \beta_j X^j$ de deux polynômes. En effet, on définit par induction les polynômes $s_n(\alpha_0, \ldots, \alpha_{n-1}, \beta_0, \ldots, \beta_{n-1})$ à coefficients dans $\mathbb{F}_3$ comme suit

$$s_0 := 0, \quad s_n = \sigma(\alpha_{n-1}, \beta_{n-1}, s_{n-1}).$$

Alors le coefficient de X^n dans la somme $\sum_j \alpha_j X^j + \sum_j \beta_j X^j = \sum_j \gamma_j X^j$ est donné par

$$\gamma_n = \alpha_n + \beta_n + s_n. \tag{5.3}$$

Cette construction fournit une séquence de polynômes $\gamma_n(\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_n)$ et finalement, on a le

LEMME 5.3. *Le polynôme $\gamma_n(\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_n)$ s'évanouit à condition que les composants α_n, α_{n-1} et β_n, β_{n-1} s'évanouissent tous.*

PREUVE : Il suffit de montrer que $s_n = 0$ si $\alpha_{n-1} = 0$ et $\beta_{n-1} = 0$. Cela découle de la définition inductive de $s_n = \sigma(\alpha_{n-1}, \beta_{n-1}, s_{n-1})$. □

Puisqu'on travaille sur $\mathbb{F}_3$, $x^n = x$ si n est un nombre impair, alors que $x^n = x^2$ si n est un nombre pair non nul. Ainsi on peut réduire les exposants des variables dans les polynômes γ_n de façon à ce qu'ils soient au plus égaux à 2.

On a $s_1(\alpha_0, \beta_0) = -\alpha_0\beta_0^2 - \alpha_0^2\beta_0$, alors que s_2 en forme réduite est égal à

$$\begin{aligned} s_2(\alpha_0, \alpha_1, \beta_0, \beta_1) = {} & \alpha_1\alpha_0^2\beta_0^2 + \alpha_0^2\beta_0\beta_1^2 + \alpha_1^2\alpha_0^2\beta_0 + \alpha_0^2\beta_0^2\beta_1 - \alpha_1\alpha_0^2\beta_0\beta_1 \\ & + \alpha_1^2\alpha_0\beta_0^2 + \alpha_0\beta_0^2\beta_1^2 + \alpha_1\alpha_0\beta_0 - \alpha_1\alpha_0\beta_0^2\beta_1 + \alpha_0\beta_0\beta_1 - \alpha_1\beta_1^2 - \alpha_1^2\beta_1 \end{aligned}$$

Écrire complètement $s_3(\alpha_0, \alpha_1, \alpha_2, \beta_0, \beta_1, \beta_2)$ nécessiterait plusieurs lignes.

Conceptuellement, on voit que la construction ci-dessus est décrite par la règle d'addition de deux vecteurs de Witt sur $\mathbb{F}_3$. Le nombre 3 est le seul nombre premier pour lequel les vecteurs de Witt avec seulement un nombre fini de composants non nuls forment un sous-groupe additif de l'anneau de Witt. Plus précisément, on peut énoncer la proposition suivante

PROPOSITION 5.4. *Les vecteurs de Witt avec seulement un nombre fini de composants non nuls forment un sous-anneau de l'anneau $\mathbf{W}(\mathbb{F}_3)$. Ce sous-anneau est isomorphe à $\mathbb{Z} \subset \mathbb{Z}_3$.*

PREUVE : Pour tout nombre premier p, on sait que l'application

$$\mathbf{W}(\mathbb{F}_p) \ni \xi = (\xi_j) \mapsto \tilde{\tau}(\xi) := \sum_{j=0}^{\infty} \tau(\xi_j) p^j,$$

où τ est le relèvement de Teichmüller est un isomorphisme d'anneaux entre l'anneau de Witt $\mathbf{W}(\mathbb{F}_p)$ et l'anneau $\mathbb{Z}_p$ des entiers p-adiques. Pour $p = 3$, $\tau(\mathbb{F}_3) = \{-1, 0, 1\} \subset \mathbb{Z} \subset \mathbb{Z}_3$, ainsi $\tilde{\tau}$ envoie les vecteurs de Witt avec seulement un nombre fini de composants non nuls dans le sous-anneau $\mathbb{Z} \subset \mathbb{Z}_3$. Cette application est un homomorphisme injectif d'anneaux et elle envoie surjectivement sur $\mathbb{Z}$ puisque par la Proposition 5.2, tout entier peut être écrit comme une somme finie de puissances de 3 avec coefficients dans $\{-1, 0, 1\}$. □

Références

[1] A. Connes, C. Consani, *Riemann Roch for $\overline{Spec\ \mathbb{Z}}$*, Preprint (2022). Available at https://arxiv.org/abs/2205.01391.