Analyse et géométrie

M. Alain Connes, membre de l'Institut
(Académie des sciences), professeur

Anneaux de Witt et mécanique statistique quantique

Introduction

Mon cours cette année portait sur les résultats récents (obtenus en collaboration avec C. Consani [4]) sur les relations entre le système de mécanique statistique quantique construit dans [2] (appelé système BC) et la construction de l'anneau universel de Witt pour une clôture algébrique $\bar{\mathbb{F}}_p$ du corps fini $\mathbb{F}_p$. Pour p premier et σ un isomorphisme du groupe multiplicatif de $\bar{\mathbb{F}}_p$ avec le groupe des racines de l'unité (dans $\mathbb{C}$) d'ordre premier à p, nous construisons une représentation p-adique indécomposable π_σ du système BC (défini sur $\mathbb{Z}$) comme endomorphismes additif de l'anneau de Witt universel de $\bar{\mathbb{F}}_p$. Les représentations obtenues sont les analogues p-adiques des représentations irréductibles complexes associées aux états extrémaux KMS_∞ du système BC. Le rôle de la fonction zêta de Riemann comme fonction de partition dans le cas complexe est tenu dans le cas p-adique par les fonctions L p-adiques et les relations de division des polylogarithmes p-adiques permettent de démontrer l'analogue p-adique de la condition KMS. Nous montrons que la théorie d'Iwasawa permet d'étendre la théorie KMS à un revêtement du groupe additif de $\mathbb{C}_p$ (complétion d'une clôture algébrique de $\mathbb{Q}_p$).

Présentation du système BC

Le système BC est un anneau noncommutatif dont la construction est semblable à celle de l'anneau des opérateurs de Hecke à partir des double classes de $\mathrm{GL}_2(\mathbb{Z})$ dans $\mathrm{GL}_2(\mathbb{Q})$. On remplace GL_2 par le groupe affine $P =$ "$ax + b$". L'algèbre de Hecke $\mathcal{H}_\mathbb{Z}$ obtenue est hautement non-triviale même sur $\mathbb{C}$ et sa représentation régulière engendre un facteur de type III_1 et une « évolution dans le temps » $\sigma_t \in \mathrm{Aut}(\mathcal{H}_\mathbb{C})$.

L'étude des états KMS a montré que :

1. La fonction de partition est la fonction zêta de Riemann.
2. Au pôle de zêta on a une transition de phase avec brisure de symétrie spontanée.

3. Les états de vide (température nulle) donnent l'isomorphisme du corps de classe global pour $\mathbb{Q}$.

L'algèbre de Hecke $\mathcal{H}_{\mathbb{Z}}$ contient l'algèbre de groupe $\mathbb{Z}[\mathbb{Q}/\mathbb{Z}]$. Soient $e(r) \in \mathbb{Z}[\mathbb{Q}/\mathbb{Z}]$, les générateurs canoniques pour $r \in \mathbb{Q}/\mathbb{Z}$. Pour $n \in \mathbb{N}$, on définit un endomorphisme σ_n de $\mathbb{Z}[\mathbb{Q}/\mathbb{Z}]$ tel que $\sigma_n(e(\gamma)) = e(n\gamma)$ pour tout $\gamma \in \mathbb{Q}/\mathbb{Z}$ et une application additive $\tilde{\rho}_n$ telle que

$$\tilde{\rho}_n : \mathbb{Z}[\mathbb{Q}/\mathbb{Z}] \to \mathbb{Z}[\mathbb{Q}/\mathbb{Z}], \ \tilde{\rho}_n(e(\gamma)) = \sum_{n\gamma'=\gamma} e(\gamma').$$

Ces applications vérifient les relations de compatibilité suivantes

$$\sigma_{nm} = \sigma_n\sigma_m, \tilde{\rho}_{mn} = \tilde{\rho}_m\tilde{\rho}_n, \quad \forall m,n \in \mathbb{N} \tag{1}$$

$$\tilde{\rho}_m(\sigma_m(x)y) = x\tilde{\rho}_m(y), \quad \forall x,y \in \mathbb{Z}[\mathbb{Q}/\mathbb{Z}] \tag{2}$$

$$\sigma_c\,\tilde{\rho}_b = (b,c)\tilde{\rho}_{b'}\sigma_{c'} \tag{3}$$

où $(b,c) = \gcd(b,c)$ est le plus grand diviseur commun de b et c, $b' = b/(b,c)$, $c' = c/(b,c)$.

L'algèbre de Hecke $\mathcal{H}_{\mathbb{Z}}$ admet une présentation comme produit croisé $\mathbb{Z}[\mathbb{Q}/\mathbb{Z}] \rtimes_{\tilde{\rho}} \mathbb{N}$. Elle est engendrée par $\mathbb{Z}[\mathbb{Q}/\mathbb{Z}]$, et les éléments $\tilde{\mu}_n$, μ_n^*, pour $n \in \mathbb{N}$, qui vérifient les relations

$$\tilde{\mu}_n x \mu_n^* = \tilde{\rho}_n(x), \mu_n^* x = \sigma_n(x)\mu_n^*, x\tilde{\mu}_n = \tilde{\mu}_n\sigma_n(x),$$

$$\tilde{\mu}_{nm} = \tilde{\mu}_n\tilde{\mu}_m, \mu_{nm}^* = \mu_n^*\mu_m^*, \mu_n^*\tilde{\mu}_n = n,$$

ainsi que $\tilde{\mu}_n\mu_m^* = \mu_m^*\tilde{\mu}_n$ pour $(n,m) = 1$. Tout élément de $\mathcal{H}_{\mathbb{Z}}$ s'écrit de manière unique comme somme finie de monômes

$$\tilde{\mu}_a x \mu_b^*, \quad (a,b) = 1, \ x \in \mathbb{Z}[\mathbb{Q}/\mathbb{Z}],$$

où par convention $\tilde{\mu}_1 = \mu_1^* = 1$.

Système BC, $\mathbb{W}_0(\overline{\mathbb{F}}_p)$ et représentations *p*-adiques

Le point de départ de notre travail est la similitude entre les relations (1), (2) et (3) et celles que satisfont les endomorphismes de Frobenius F_n et les « Verschiebung » V_n dans la construction de Witt universelle (*cf.* [3]).

Le foncteur $\mathbb{W}_0$ de Witt

L'incarnation la plus simple de la construction de Witt universelle est le foncteur qui associe à l'anneau commutatif A l'anneau $\mathbb{W}_0(A) = K_0(\underline{\mathrm{End}}_A)/K_0(A)$ qui classifie les endomorphismes (E,f) où E désigne un module projectif de type fini sur A et $f \in \mathrm{End}_A(E)$ un endomorphisme de E. Les opérations dans $\mathbb{W}_0(A)$ sont celles de somme directe et de produit tensoriel sur les endomorphismes. Les structures importantes sont

- la section de Teichmüller application multiplicative $\tau : A \to \mathbb{W}_0(A)$, $f \mapsto \tau(f) = [f] = (A,f)$;
- les endomorphismes de Frobenius F_n pour $n \in \mathbb{N}$, avec $F_n(E,f) = (E,f^n)$;

• les Verschiebung, applications additives V_n, $n \in \mathbb{N}$, où $V_n(f)$ est la matrice compagnon du polynôme $X^n - f$;

• les composantes fantôme $\mathrm{gh}_n : \mathbb{W}_0(A) \to A$ pour $n \in \mathbb{N}$, $\mathrm{gh}_n(E, f) = \mathrm{Trace}(f^n)$.

Parmi les nombreuses propriétés générales de cette construction, notons les relations suivantes,

(1) $F_n \circ V_n(x) = nx$.

(2) $V_n(F_n(x)y) = xV_n(y)$.

(3) Si $(m,n) = 1$, $V_m \circ F_n = F_n \circ V_m$.

(4) Pour $n \in \mathbb{N}$, $V_n(x)V_n(y) = nV_n(xy)$.

(5) Pour $n \in \mathbb{N}$, $F_n(\tau(f)) = \tau(f^n)$.

(6) Pour $n, m \in \mathbb{N}$, $\mathrm{gh}_n(F_m(f)) = \mathrm{gh}_{nm}(f)$.

(7) $\mathrm{gh}_n(V_m(f)) = \begin{cases} m\mathrm{gh}_{n/m}(f) & \text{si } m|n \\ 0 & \text{sinon.} \end{cases}$

Soit k un corps algébriquement clos. On a alors un isomorphisme canonique de l'anneau de groupe $\mathbb{Z}[k^\times]$ avec $\mathbb{W}_0[k]$ qui associe au diviseur $\sum n_j(x_j) \in \mathbb{Z}[k^\times]$ la somme des relevés de Teichmüller $\sum n_j \tau(x_j) \in \mathbb{W}_0[k]$. L'endomorphisme de Frobenius F_n correspond à l'endomorphisme $g \mapsto g^n$ dans le groupe multiplicatif de k.

Soit $k = \overline{\mathbb{F}}_p$ une clôture algébrique du corps fini $\mathbb{F}_p$. Le groupe multiplicatif de k est isomorphe non canoniquement au groupe $\mu^{(p)}$ des racines de l'unité (dans $\mathbb{C}$) d'ordre premier à p, que l'on identifiera au sous groupe $(\mathbb{Q}/\mathbb{Z})^{(p)}$ de $\mathbb{Q}/\mathbb{Z}$ des fractions dont le dénominateur est premier à p. On note r la projection naturelle de $\mathbb{Q}/\mathbb{Z}$ sur $(\mathbb{Q}/\mathbb{Z})^{(p)}$. Soit X_p l'ensemble des isomorphismes du groupe multiplicatif de $\overline{\mathbb{F}}_p$ avec $\mu^{(p)}$. On obtient la relation suivante entre $\mathbb{W}_0(\overline{\mathbb{F}}_p)$ et le système BC.

Théorème 3.1 *À tout $\sigma \in X_p$, $\sigma : \overline{\mathbb{F}}_p^\times \sim \mu^{(p)} \subset \mathbb{C}^\times$, correspond un isomorphisme d'anneaux, $\tilde{\sigma}$*

$$\mathbb{W}_0(\overline{\mathbb{F}}_p) \xrightarrow{\tilde{\sigma}} \mathbb{Z}[(\mathbb{Q}/\mathbb{Z})^{(p)}] \subset \mathbb{Z}[\mathbb{Q}/\mathbb{Z}] \xrightarrow{r} \mathbb{Z}[(\mathbb{Q}/\mathbb{Z})^{(p)}]$$

Les Frobenius F_n et Verschiebung V_n de $\mathbb{W}_0(\overline{\mathbb{F}}_p)$ sont les restrictions des endomorphismes σ_n et des $\tilde{\rho}_n$ de $\mathbb{Z}[\mathbb{Q}/\mathbb{Z}]$ par

$$\tilde{\sigma} \circ F_n = \sigma_n \circ \tilde{\sigma}, \ \tilde{\sigma} \circ V_n = r \circ \tilde{\rho}_n \circ \tilde{\sigma} \tag{4}$$

On en déduit une représentation $\pi_{p,\sigma}$ du système BC, *i.e.* de $\mathcal{H}_\mathbb{Z}$ sur $\mathbb{W}_0(\overline{\mathbb{F}}_p)$, on a

$$\pi_{p,\sigma}(x)\xi = \tilde{\sigma}^{-1}(r(x))\xi, \tag{5}$$

pour tous $\xi \in \mathbb{W}_0(\overline{\mathbb{F}}_p)$, $x \in \mathbb{Z}[\mathbb{Q}/\mathbb{Z}]$ et, pour $n \in \mathbb{N}$

$$\pi_{p,\sigma}(\mu_n^*) = F_n, \ \pi_{p,\sigma}(\tilde{\mu}_n) = V_n. \tag{6}$$

Le foncteur $\mathbb{W}(A)$

Nous utilisons les résultats de P. Cartier (*cf.* [3]) sur l'anneau universel $\mathbb{W}(A)$ pour A une $\mathbb{F}_p$ algèbre, ce qui donne l'isomorphisme

$$\mathbb{W}(\overline{\mathbb{F}}_p) = (\mathbb{W}_{p^\infty}(\overline{\mathbb{F}}_p))^{I(p)} \tag{7}$$

où $I(p) \subset \mathbb{N}$ est l'ensemble des entiers premiers à p et $\mathbb{W}_{p^\infty}$ la construction de Witt isotypique. Cet isomorphisme nous permet de prolonger la représentation $\pi_{p,\sigma}$ en une représentation p-adique.

L'anneau universel $\mathbb{W}(A)$ défini dans [3] s'obtient par complétion de $\mathbb{W}_0(A)$ mais la structure uniforme impliquée dépend de la structure algébrique de A et pas seulement de l'anneau $\mathbb{W}_0(A)$, même si l'on tient compte des structures supplémentaires données par les F_n et V_n. Soit $\Lambda(A) = 1 + tA[[t]]$ le groupe multiplicatif des séries formelles à coefficients dans A. On peut introduire l'anneau universel $\mathbb{W}(A)$ comme complétion de $\mathbb{W}_0(A)$ en utilisant un résultat de G. Almkvist [1] qui montre que le polynôme caractéristique des endomorphismes donne un invariant complet

$$L : \mathbb{W}_0(A) \to \Lambda(A), \quad L(E,f) = \det(1 - tM(f))^{-1}$$

dont l'image est le groupe multiplicatif des fractions rationnelles à coefficients dans A de la forme $(1+\sum a_n t^n)/(1+\sum b_n t^n)$. L'anneau $\mathbb{W}(A)$ des vecteurs de Witt s'obtient alors en prolongeant les opérations de $\mathbb{W}_0(A)$ au groupe formel $\Lambda(A) = 1 + tA[[t]]$ des séries formelles à coefficients dans A et en utilisant la bijection $\varphi_A : \mathbb{W}(A) \to \Lambda(A)$, qui associe au vecteur de Witt $(x_n)_{n\in\mathbb{N}}$ le produit $f_x(t) = \prod_{\mathbb{N}}(1 - x_n t^n)^{-1}$. L'addition et la multiplication des vecteurs de Witt sont données en composantes par des polynômes universels à coefficients entiers. Les endomorphismes de Frobenius F_n sont eux aussi donnés par des polynômes et l'on a par exemple

$$\begin{aligned}
F_3(x)_1 &= x_1^3 + 3x_3\\
F_3(x)_2 &= x_2^3 - 3x_1^3x_3 - 3x_3^2 + 3x_6\\
F_3(x)_3 &= -3x_1^6x_3 - 9x_1^3x_3^2 - 8x_3^3 + 3x_9
\end{aligned}$$

soit $\mathbb{Z}_{(p)}$ le localisé de $\mathbb{Z}$ en p. L'exponentielle de Artin-Hasse a un sens dans $\Lambda(\mathbb{Z}_{(p)})$

$$E_p(t) = \text{hexp}(t) = \exp\left(t + \frac{t^p}{p} + \frac{t^{p^2}}{p^2} + \cdots\right) \in \Lambda(\mathbb{Z}_{(p)})$$

et de plus,

(1) $E_p(t)$ est un idempotent de $\Lambda(\mathbb{Z}_{(p)})$.

(2) Pour $n \in I(p)$, la série

$$E_p(n)(t) = \frac{1}{n} V_n(E_p)(t) \in \Lambda(\mathbb{Z}_{(p)})$$

détermine un idempotent. Quand n varie dans $I(p)$, les $E_p(n)$ forment une partition de l'unité.

(3) Pour $n \notin p^{\mathbb{N}}$, $F_n(E_p)(t) = 1 (= 0_\Lambda)$ et $F_{p^k}(E_p)(t) = E_p(t)$, $\forall k \in \mathbb{N}$.

Addition et multiplication des vecteurs de Witt se localisent à tout sous-ensemble de $\mathbb{N}$ stable par l'opération $n \to$ diviseurs de n. On note $\mathbb{W}_{p^\infty}$ le foncteur de Witt pour l'ensemble des puissances de p. Soit A une $\mathbb{Z}_{(p)}$-algèbre, l'application

$$\psi_A : \mathbb{W}_{p^\infty}(A) \to \Lambda(A)_{E_p},$$

$$x = (x_{p^n})_{n\in\mathbb{N}} \mapsto \psi_A(x)(t) = h_x(t) = \prod_{\mathbb{N}} E_p(x_{p^n} t^{p^n})$$

est un isomorphisme sur l'algèbre réduite $\Lambda(A)_{E_p}$. Pour $n \in I(p)$, $\psi_A^{-1} \circ F_n$ est un isomorphisme de $\Lambda(A)_{E_p(n)}$ avec $\mathbb{W}_{p^\infty}(A)$. On obtient ainsi un isomorphisme $\Theta_A : \mathbb{W}(A) \to \mathbb{W}_{p^\infty}(A)^{I(p)}$ qui est donné en composantes par

$$(\Theta_A(x)_n)_{p^k} = F_n(x)_{p^k}, \quad \forall x \in \mathbb{W}(A), \quad \forall n \in I(p).$$

On applique ce résultat à $A = \overline{\mathbb{F}}_p$. On sait alors que, comme A est parfait de caractéristique p, l'anneau $\mathbb{W}_{p^\infty}(A)$ est l'unique p-anneau strict R (R séparé complet pour la topologie p-adique, p non diviseur de zéro) de corps résiduel $\overline{\mathbb{F}}_p$. Notons $\mathbb{C}_p$ la complétion p-adique d'une clôture algébrique de $\mathbb{Q}_p$. Soit $\widehat{\mathbb{Q}_p^{\mathrm{ur}}} \subset \mathbb{C}_p$ la complétion de l'extension $\mathbb{Q}_p^{\mathrm{ur}}$ non ramifiée maximale de $\mathbb{Q}_p$. Alors $\mathbb{W}_{p^\infty}(\overline{\mathbb{F}}_p)$ est l'anneau des entiers

$$\mathcal{O} = \mathcal{O}_{\widehat{\mathbb{Q}_p^{\mathrm{ur}}}} \subset \widehat{\mathbb{Q}_p^{\mathrm{ur}}}$$

complétion du sous anneau engendré par les racines de l'unité. On a donc un isomorphisme canonique

$$\mathbb{W}(\overline{\mathbb{F}}_p) \to \mathcal{O}^{I(p)},\ x \mapsto (F_n(x))\big|_{p\mathbb{N}}. \tag{8}$$

Notons ε_m, $m \in I(p)$ les vecteurs de composantes toutes nulles sauf une, égale à 1. Notons $\mathbb{Q}^{\mathrm{cyc}}$ le corps cyclotomique abstrait, quotient de l'anneau de groupe $\mathbb{Q}[\mathbb{Q}/\mathbb{Z}]$ par l'idéal J engendré par les $\pi_n = \frac{1}{n}\sum_{j=0}^{n-1} e\left(\frac{j}{n}\right)$, pour $n \geq 2$. Soit $\mathbb{Q}^{\mathrm{cyc,p}} \subset \mathbb{Q}^{\mathrm{cyc}}$ le sous-corps de $\mathbb{Q}^{\mathrm{cyc}}$ engendré sur $\mathbb{Q}$ par le groupe $\mu^{(p)} \subset \mathbb{Q}^{\mathrm{cyc}}$ des racines de l'unité d'ordre premier à p. À tout $\sigma \in X_p$ correspond un unique plongement $\rho : \mathbb{Q}^{\mathrm{cyc,p}} \to \mathbb{C}_p$ qui donne l'inverse de σ au niveau résiduel. On peut alors prolonger la représentation $\pi_{p,\sigma}$ du système BC de (5) et l'on obtient,

Théorème 3.2 *Soit* $\sigma \in X_p$ *et* $\rho : \mathbb{Q}^{\mathrm{cyc,p}} \to \mathbb{C}_p$ *le plongement associé. La représentation* $\pi_{p,\sigma}$ *de l'algèbre* $\mathcal{H}_{\mathbb{Z}}$ *se prolonge à* $\mathbb{W}(\overline{\mathbb{F}}_p)$*. Pour* $n \in I(p)$*, les* $\pi_\sigma(\mu_n)$ *et pour* $x \in \mathbb{Z}[\mathbb{Q}/\mathbb{Z}]$*, les* $\pi_\sigma(x)$ *sont des opérateurs* $\mathcal{O}$*-linéaires tels que*

$$\pi_\sigma(\mu_n)\varepsilon_m = \varepsilon_{nm}, \quad \pi_\sigma(e(a/b))\varepsilon_m = \rho(\zeta_{a/b}^m)\varepsilon_m, \quad \forall n \in \mathbb{N},\ m, b \in I(p).$$

De plus

$$\pi_\sigma(\mu_p) = \mathrm{Fr}^{-1}$$

est l'inverse du Frobenius.

Soit $\mathcal{J}_p \subset \mathcal{H}_{\mathbb{Z}}$ l'idéal bilatère engendré par les $1-e(p^{-k})$, $k \in \mathbb{N}$. C'est le noyau de la représentation π_σ indépendamment de σ. Soit $\mathcal{H}_{\mathbb{Z}}^{(p)}$ le quotient par $\mathcal{J}_p$ de la sous-algèbre de $\mathcal{H}_{\mathbb{Z}}$ engendrée par $\mathbb{Z}[\mathbb{Q}/\mathbb{Z}]$, $\tilde{\mu}_n$, μ_n^* pour $n \in I(p)$. L'algèbre $\mathcal{H}_{\mathbb{Z}}^{(p)}$ est engendrée par $\mathbb{Z}[(\mathbb{Q}/\mathbb{Z})^{(p)}]$, et les $\tilde{\mu}_n$, μ_n^* pour $n \in I(p)$. Il existe un unique automorphisme $\mathrm{Fr} \in \mathrm{Aut}(\mathcal{H}_{\mathbb{Z}}^{(p)})$ de cette algèbre tel que

$$\mathrm{Fr}(e(\gamma) = e(\gamma)^p, \quad \forall \gamma \in \mu^{(p)}, \ \mathrm{Fr}(\tilde{\mu}_n) = \tilde{\mu}_n, \ \mathrm{Fr}(\mu_n^*) = \mu_n^*, \quad \forall n \in I(p)$$

L'on retrouve le quotient $\mathcal{H}_{\mathbb{Z}} / \mathcal{J}_p$ comme un produit croisé de la forme

$$\mathcal{H}_{\mathbb{Z}} / \mathcal{J}_p = \mathcal{H}_{\mathbb{Z}}^{(p)} \rtimes_{\mathrm{Fr},p} \mathbb{Z}.$$

Le choix de $\sigma \in X_p$ intervient de manière essentielle dans cette construction comme le montre le résultat suivant,

Théorème 3.3 *Soit* $\sigma \in X_p$ et $\rho : \mathbb{Q}^{\mathrm{cyc,p}} \to \mathbb{C}_p$ *le plongement associé. Les représentations* π_σ *restreintes à* $\mathcal{H}_{\mathbb{Z}}^{(p)}$ *sont* $\mathcal{O}$*-linéaires, indécomposables et deux à deux inéquivalentes. Les représentations* π_σ *de* $\mathcal{H}_{\mathbb{Z}}$ *sont* $\mathbb{Z}_p$*-linéaires, indécomposables et* π_σ *et* $\pi_{\sigma'}$ *sont équivalentes sur* $\mathbb{Z}_p$ *si et seulement si il existe* $\alpha \in \mathrm{Aut}(\overline{\mathbb{F}}_p)$ *tel que* $\sigma' = \sigma \circ \alpha$.

Condition KMS, analyse *p*-adique et polylogarithmes

La formulation algébrique de la condition KMS est l'égalité

$$\varphi(x\sigma_\beta(y)) = \varphi(yx), \quad \forall x, y \in \mathcal{A}, \tag{9}$$

où φ est une forme linéaire sur l'algèbre $\mathcal{A}$ et $\sigma_\beta \in \mathrm{Aut}(\mathcal{A})$ est un automorphisme.

Le cas complexe

Les résultats de [2] montrent que les états KMS_β extrémaux sont, pour $\beta > 1$ de la forme

$$\varphi_{\beta,\rho}(X) = \frac{\mathrm{Tr}(\pi_\rho(X)e^{-\beta H})}{\mathrm{Tr}(e^{-\beta H})}, \quad \forall X \in \mathcal{H}_{\mathbb{Z}} \tag{10}$$

où H est l'Hamiltonien, opérateur de multiplication par $\log n$ dans la base canonique ε_n de l'espace de Hilbert $\ell^2(\mathbb{N})$ et π_ρ la représentation irréductible de $\mathcal{H}_{\mathbb{Q}}$ donnée par

$$\pi_\rho(\mu_n)\varepsilon_m = \varepsilon_{nm}, \ \pi_\rho(\mu_n^*) = \pi_\rho(\mu_n)^*, \pi_\rho(e(a/b))\varepsilon_m = \rho(\zeta_{a/b}^m)\varepsilon_m, \tag{11}$$

où $\rho \in \widehat{\mathbb{Z}}^*$ détermine un plongement dans $\mathbb{C}$ du corps cyclotomique $\mathbb{Q}^{\mathrm{cyc}}$.

Dans notre cas l'algèbre est

$$\mathcal{A} = \mathcal{H}_{\mathbb{C}_p}^{(p)} = \mathcal{H}_{\mathbb{Z}}^{(p)} \otimes_{\mathbb{Z}} \mathbb{C}_p. \tag{12}$$

L'analogue du Hamiltonien qui dans le cas complexe est simplement $H\varepsilon_n = \log(n)\varepsilon_n$ s'obtient dans le cas p-adique en utilisant le logarithme d'Iwasawa, $\log_p$,

$$-\log_p(1-x) = \sum_{n=1}^{\infty} \frac{x^n}{n}, \quad \forall x, |x|_p < 1$$

qui se prolonge à $\mathbb{C}_p$ de telle sorte que $\log_p(p) = 0$ et

$$\log_p(xy) = \log_p(x) + \log_p(y), \quad \forall x, y \in \mathbb{C}_p.$$

Les automorphismes $\sigma^{(\beta)} \in \mathrm{Aut}(\mathcal{H}_{\mathbb{C}_p}^{(p)})$

Pour p premier on note $q = 4$ si $p = 2$, $q = p$ si $p \neq 2$, et $\tilde{q} = \frac{q}{p}(p-1)$ l'indicatrice d'Euler de q. Le domaine naturel qui remplace dans le cas p-adique le groupe additif $\mathbb{C}$ des « températures inverses » β de la condition KMS_β est le groupe additif

$$D_p = \{\beta \in \mathbb{C}_p \,\|\beta|_p < qp^{-1/(p-1)}\}.$$

Soit $\mathbb{Z}_{(p)}^{\times} \subset \mathbb{Q}^{\times}$ le groupe multiplicatif des fractions rationnelles de numérateur et dénominateur premiers à p.

Lemme 4.1 *Soit* $r \in \mathbb{Z}_{(p)}^{\times}$. *Il existe une unique fonction analytique* $D_p \to \mathbb{C}_p$, $\beta \mapsto r^{(\beta)}$ *telle que* $r^{(\beta)} = r^{\beta}$ *pour tout* $\beta = 1 - k\tilde{q}$ *avec* k entier. On a

$$r^{(\beta)} := r\exp((\beta-1)\log_p(r)), \quad \forall \beta \in D_p. \tag{13}$$

Pour $\beta \in D_p$, l'application

$$\mathbb{Z}_{(p)}^{\times} \ni r \mapsto r^{(\beta)} \in \mathbb{C}_p^{\times} \tag{14}$$

est un homomorphisme de groupes. De plus pour $r \in \mathbb{Z}_{(p)}^{\times}$

$$r^{(\beta_1)} r^{(\beta_2)} = r^{(\beta_1+\beta_2)} r^{(0)}, \quad \forall \beta_j \in D_p \tag{15}$$

Proposition 4.2 (1) *Pour* $\beta \in D_p$ *il existe un unique automorphisme* $\sigma^{(\beta)} \in \mathrm{Aut}(\mathcal{H}_{\mathbb{C}_p}^{(p)})$ *tel que*

$$\sigma^{(\beta)}(\tilde{\mu}_a e(\gamma)\mu_b^*) = \left(\frac{b}{a}\right)^{(\beta)} \tilde{\mu}_a e(\gamma)\mu_b^*, \quad \forall a, b \in I(p), \gamma \in (\mathbb{Q}/\mathbb{Z})^{(p)}. \tag{16}$$

(2) *On a*

$$\sigma^{(\beta_1)} \circ \sigma^{(\beta_2)} = \sigma^{(\beta_1+\beta_2)} \circ \sigma^{(0)}, \quad \forall \beta_j \in D_p \tag{17}$$

et $\sigma^{(0)}$ *est un automorphisme d'ordre fini* $\tilde{q}$.

Pour construire les états KMS_β, *i.e.* les formes linéaires $\varphi : \mathcal{H}_{\mathbb{C}_p}^{(p)} \to \mathbb{C}_p$, $\varphi(1) = 1$, telles que

$$\varphi(x\sigma^{(\beta)}(y)) = \varphi(yx), \quad \forall x, y \in \mathcal{H}_{\mathbb{C}_p}^{(p)},$$

il faut donner, pour $\rho:\mathbb{Q}^{\mathrm{cyc,p}}\to\mathbb{C}_p$, un sens à la somme formelle, analogue du cas complexe,

$$Z(\tfrac{a}{b},\beta)=\sum_{m\in I(p)}\rho(\zeta_{a/b}^{m})m^{-\beta},\ \beta\in D_p$$

dans le domaine p-adique. On utilise pour cela la construction classique, [5], où les B_j sont les nombres de Bernoulli. On note $\langle a\rangle=\exp(\log_p(a))$.

Lemme 4.3 *Pour $f\in\mathbb{N}$, $f\neq 0$, multiple de bq, l'expression*

$$Z_\rho(\tfrac{a}{b},\beta,f):=\frac{1}{f}\sum_{\substack{1\le c<f\\ c\notin p\mathbb{N}}}\rho(\zeta_{a/b}^{c})\frac{\langle c\rangle^{1-\beta}}{\beta-1}\sum_{j=0}^{\infty}\binom{1-\beta}{j}\left(\frac{f}{c}\right)^{j}B_j,\qquad \beta\in D_p,\tag{18}$$

définit une fonction méromorphe (avec au plus un pôle simple en $\beta=1$) dans le disque D_p et ne dépend pas du choix de f.

On note $Z_\rho(\dfrac{a}{b},\beta)=Z_\rho(\dfrac{a}{b},\beta,f)$ indépendamment du choix de f.

Polylogarithme et cyclotomie

La vérification de la condition KMS_β pour tout β se ramène par analyticité au cas où β est un entier négatif de la forme $1-k\tilde{q}$. Dans ce cas on utilise les relations de division des polylogarithmes. On définit des fractions rationnelles $\ell_\beta(z)$ pour β entier négatif, par les égalités

$$z\partial_z\ell_\beta(z)=\ell_{\beta-1}(z),\ \ell_0(z)=\frac{z}{1-z}.$$

Lemme 4.4 *Soient $n>1$, $a,b\in\mathbb{N}$. Alors*

$$b^{n-1}\sum_{j=0}^{b-1}\zeta_{a/b}^{j}B_n(\frac{j}{b})=\begin{cases}-n\ell_{1-n}(\zeta_{a/b}), & si\ \zeta_{a/b}\neq 1\\ B_n, & si\ \zeta_{a/b}=1.\end{cases}$$

On pose

$$Y_n(a/b)=f^{\,n-1}\sum_{j=0}^{f-1}\zeta_{a/b}^{j}B_n(\frac{j}{f}),\quad \forall f\in b\mathbb{N},\ f\neq 0$$

Lemme 4.5 *Soit β un entier négatif de la forme $\beta=1-m=1-k\tilde{q}$, on a alors*

$$Z_\rho(\frac{a}{b},\beta)=-\frac{1}{m}\rho\left(Y_m\left(\frac{a}{b}\right)-p^{m-1}Y_m\left(\frac{pa}{b}\right)\right).\tag{19}$$

Ce lemme ramène la démonstration du lemme 4.7 ci-dessous à la vérification des relations de division des polylogarithmes.

Condition KMS$_\beta$

Le théorème suivant donne la construction de formes linéaires vérifiant la condition KMS$_\beta$. On définit une forme linéaire $\varphi_{\beta,\rho}$ sur $\mathcal{H}^{(p)}_{\mathbb{C}_p}$ pour tout $\beta \in D_p$ par (avec $n,m \in I(p)$ premiers entre eux),

$$\varphi_{\beta,\rho}(\tilde{\mu}_n e(\frac{a}{b})\mu_m^*) = \begin{cases} Z_\rho(\frac{a}{b},\beta), & si\ n=m=1, \\ 0, & sinon. \end{cases}$$

Théorème 4.6 *Pour tout $\beta \in D_p$, $\beta \neq 1$, et $\rho \in Hom(\mathbb{Q}^{\mathrm{cyc,p}},\mathbb{C}_p)$ la forme linéaire $\varphi_{\beta,\rho}$ vérifie la condition KMS$_\beta$:*

$$\varphi_{\beta,\rho}(x\sigma_{(\beta)}(y)) = \varphi_{\beta,\rho}(yx), \quad \forall x,y \in \mathcal{H}^{(p)}_{\mathbb{C}_p}.$$

La fonction de partition est la fonction L (p-adique) pour le caractère $\chi = 1$,

$$Z(\beta) = L_p(\beta,1).$$

On a $Z(\beta) \neq 0$ pour $\beta \in D_p$ et un pôle en $\beta = 1$ de résidu $\frac{p-1}{p}$.

La démonstration utilise le lemme suivant sur les applications $\tilde{\rho}_n$.

Lemme 4.7 *Pour tout $n \in I(p)$ et $\beta \in D_p$, $\beta \neq 1$, on a*

$$\varphi_{\beta,\rho}(\tilde{\rho}_n(X)) = \langle n\rangle^{1-\beta}\varphi_{\beta,\rho}(X), \quad \forall X \in \mathbb{Z}[\mu^{(p)}] \tag{20}$$

Pour normaliser les formes linéaires $\varphi_{\beta,\rho}$ il faut étudier la fonction de partition et ses zéros. Elle est donnée par

$$Z(\beta) := \varphi_{\beta,\rho}(1) = \frac{1}{q}\sum_{\substack{1\le c<q \\ c\notin p\mathbb{N}}} \frac{\langle c\rangle^{1-\beta}}{\beta-1}\sum_{j=0}^{\infty}\binom{1-\beta}{j}\left(\frac{q}{c}\right)^j B_j. \tag{21}$$

C'est la fonction L : $Z(\beta) = L_p(\beta,1)$ pour le caractère $\chi = 1$. Elle a un pôle en $\beta = 1$ de résidu

$$\frac{1}{q}\sum_{\substack{1\le c<q \\ c\notin p\mathbb{N}}} 1 = \frac{\tilde{q}}{q} = \frac{p-1}{p}.$$

La théorie d'Iwasawa donne une série formelle $\eta(T) \in \mathcal{O}_p[[T]]$ telle que

$$((1+q)^{1-\beta}-1)Z(\beta) = \eta((1+q)^\beta - 1) \tag{22}$$

Pour $\beta = 0$ on a

$$Z(0) = -\frac{1}{q}\sum_{\substack{1\le c<q \\ c\notin p\mathbb{N}}} \langle c\rangle(1-\frac{q}{2c}).$$

Pour $p > 2$ on a $q = p$ et le résidu de $\eta(0)$ vaut $p-1$. Pour $p = 2$ on a aussi

$$\frac{1}{2}\eta(T) \in \mathcal{O}_p[[T]]^{\times}$$

de sorte que $Z(\beta)$ ne s'annule pas. Cela permet de normaliser les formes linéaires $\varphi_{\beta,\rho}$ et de déterminer la limite des états associés quand $\beta \to 1$.

Proposition 4.8 Quand $\beta \to 1$ on a

$$\lim_{\beta\to 1} Z(\beta)^{-1} Z_\rho(\frac{a}{b},\beta) = \begin{cases} 1 & si\ \frac{a}{b} \in \mathbb{Z} \\ 0 & sinon. \end{cases} \tag{23}$$

On obtient ainsi la représentation régulière et dans ce cas l'automorphisme $\sigma_{(1)}$ prend la forme très simple

$$\sigma_{(1)}(\tilde{\mu}_a e(\gamma)\mu_b^*) = \frac{b}{a}\,\tilde{\mu}_a e(\gamma)\mu_b^*$$

Dans le cas p-adique l'analogue de la brisure de symétrie du cas complexe résulte du lemme suivant,

Lemme 4.9 *Soit $p > 2$ et $\theta \in \mathrm{Aut}((\mathbb{Q}/\mathbb{Z})^{(p)})$. Si $\theta \in \{\pm 1\}$ on a*

$$Z_\rho(\frac{a}{b},\beta) = Z_{\theta\circ\rho}(\frac{a}{b},\beta), \quad \forall a/b \in (\mathbb{Q}/\mathbb{Z})^{(p)}, \beta \in D_p. \tag{24}$$

Si $\theta \notin \{\pm 1\}$ et $\beta = 1 - m = 1 - k\tilde{q}$, $k > 0$, alors les formes linéaires $\varphi_{\beta,\rho}$ et $\varphi_{\beta,\theta\circ\rho}$ sont distinctes.

Ainsi dans le cas p-adique et contrairement au cas complexe, le groupe de symétrie $\mathrm{Aut}((\mathbb{Q}/\mathbb{Z})^{(p)})$ n'est pas totalement brisé et il reste une invariance non-triviale par le sous-groupe $\theta \in \{\pm 1\}$. Cela correspond en fait a la nullité des fonctions L pour les caractères impairs dans le cas p-adique.

Prolongement au revêtement

Le bon cadre pour la théorie KMS s'obtient en exploitant la théorie d'Iwasawa des fonction L. Le domaine naturel pour la variable β est le revêtement M du groupe additif de $\mathbb{C}_p$ décrit dans (25). La formule

$$((1+q)^{1-\beta} - 1)Z(\beta) = \eta((1+q)^\beta - 1)$$

montre que $\lambda = (1+q)^\beta$ est un meilleur paramètre que β. Nous montrons que la construction des états KMS_β, $\varphi_{\beta,\rho}$, pour $\beta \in D_p$, se prolonge naturellement au revêtement de $\mathbb{C}_p$ donné par l'homomorphisme de groupes

$$M = D(1,1^-) \ni \lambda \mapsto \beta = \ell(\lambda) = \frac{\log_p \lambda}{\log_p(1+q)} \in \mathbb{C}_p \tag{25}$$

où $M = D(1,1^-)$ est le disque ouvert dans $\mathbb{C}_p$ de rayon 1, vu comme groupe multiplicatif. Cet homomorphisme est surjectif et de noyau le groupe μ_{p^∞} des racines de l'unité d'ordre une puissance de p. Il définit par restriction une bijection

$$\ell : \{\lambda \in M \| \lambda - 1|_p < p^{-1/(p-1)}\} \xrightarrow{\sim} D_p \tag{26}$$

dont l'inverse est donné par

$$D_p \ni \beta \mapsto \psi(\beta) = (1+q)^\beta = \exp(\beta \log_p(1+q)). \tag{27}$$

Ceci permet de considerer D_p comme sous-groupe de M. La construction des automorphismes $\sigma_{(\beta)}$ et des états KMS_β se prolonge au revêtement M de $\mathbb{C}_p$. Ainsi pour $\lambda \in M$, il existe un unique automorphisme $\sigma[\lambda] \in \mathrm{Aut}(\mathcal{H}^{(p)}_{\mathbb{C}_p})$ tel que

$$\sigma[\lambda](\tilde{\mu}_a e(\gamma)\mu_b^*) = \omega(b/a)\lambda^{i_p(b/a)}\tilde{\mu}_a e(\gamma)\mu_b^*, \quad \forall a,b \in I(p), \gamma \in (\mathbb{Q}/\mathbb{Z})^{(p)}, \tag{28}$$

où $\omega(r)$ est la notation standard pour $r^{(0)}$ et

$$i_p(r) = \frac{\log_p(r)}{\log_p(1+q)} \in \mathbb{Z}_p \tag{29}$$

définit un homomorphisme de $\mathbb{Z}^\times_{(p)}$ vers le groupe additif $\mathbb{Z}_p$. On a alors

Théorème 4.10 *Il existe une famille analytique de formes linéaires $\psi_{\lambda,\rho}$, $\lambda \in M$, sur $\mathcal{H}^{(p)}_{\mathbb{C}_p}$ telles que*

- $\psi_{\lambda,\rho}(1) = 1$.
- $\psi_{\lambda,\rho}$ *vérifie la condition KMS*

$$\psi_{\lambda,\rho}(x\sigma[\lambda](y)) = \psi_{\lambda,\rho}(yx), \quad \forall x,y \in \mathcal{H}^{(p)}_{\mathbb{C}_p}. \tag{30}$$

- *Pour $\beta \in D_p$ et $\lambda = (1+q)^\beta$ on a*

$$\psi_{\lambda,\rho} = Z(\beta)^{-1}\varphi_{\beta,\rho}.$$

On obtient le résultat en comparant

$$Z_\rho(\frac{a}{b},\beta) := \frac{1}{f}\sum_{\substack{1\le c<f \\ c\notin p\mathbb{N}}} \rho(\zeta^c_{a/b})\frac{\langle c\rangle^{1-\beta}}{\beta-1}\sum_{j=0}^{\infty}\binom{1-\beta}{j}\left(\frac{f}{c}\right)^j B_j$$

avec les fonctions L (p-adiques)

$$L_p(\beta,\chi) := \frac{1}{f}\sum_{\substack{1\le c<f \\ c\notin p\mathbb{N}}} \chi(c)\frac{\langle c\rangle^{1-\beta}}{\beta-1}\sum_{j=0}^{\infty}\binom{1-\beta}{j}\left(\frac{f}{c}\right)^j B_j$$

où χ est un caractère de Dirichlet primitif.

Lemme 4.11 *Soit $a/b \in \mu^{(p)}$, il existe $c(d,\chi) \in \mathbb{C}_p$ tels que*

$$Z_\rho(\frac{a}{b},\beta) = \sum_{d|b} c(d,\chi) L_p(\beta,\chi) d^{-1} \langle d \rangle^{1-\beta} \prod (1-\chi(\ell)\ell^{-1}\langle \ell \rangle^{1-\beta})$$

où d divise b, χ est un caractère primitif de conducteur f qui divise $m = b/d$ et ℓ varie parmi les diviseurs premiers de m/f premiers à f.

Références

[1] Almkvist G., « The Grothendieck ring of the category of endomorphisms », *J. of Algebra*, 28, 1974, 375-388.

[2]. Bost J.B, Connes A., « Hecke algebras, Type III factors and phase transitions with spontaneous symmetry breaking in number theory », *Selecta Math. (New Series)*, vol. 1, 1995, n° 3, 411-457.

[3] Cartier P., « Groupes formels associés aux vecteurs de Witt généralisés », *Compt. Rend. Acad. Sci*. Paris, Ser. A-B 265, 1967, A49-A52.

[4] Connes A., Consani C., « On the arithmetic of the BC-system », arXiv:1103.4672.

[5] Washington L., *Introduction to cyclotomic fields* (second edition), Graduate Texts in Mathematics, 83, Springer-Verlag, New York, 1997.

Conférences

- Septembre 2010, une conférence à Rome, Academia dei lincei.
- Novembre 2010, une conférence à IHP, Paris.
- Janvier 2011, une conférence à IHES.
- Mars 2011, deux conférences à John's Hopkins University.
- Mai 2011, cinq conférences à Vanderbilt University.
- Mai 2011, une conférence à Tours.

Publications

Connes A., « The BC-system and L-functions », *Japan. J. Math*., 6, 2011, 1-44.

Connes A., « The Witt construction in characteristic one and quantization. Noncommutative geometry and Global Analysis », *Contemporary Mathematics*, 546, 2011.

Connes A., Consani C., « On the arithmetic of the BC-system », arXiv:1103.4672.

Connes A., Chamseddine A., « Spectral action for Robertson-Walker metrics », arXiv:1105.4637.