Algèbres de Hopf et Problèmes Diophantiens

Michel Waldschmidt

Groupes algébriques - linéaires, commutatifs, sur $\overline{\mathbf{Q}}$

Polynômes exponentiels

Transcendance de valeurs de polynômes exponentiels

Algèbres de Hopf - commutatives, co-commutatives, de type fini

Algèbre des nombres multizêta

Groupes algébriques - linéaires, commutatifs, sur $\overline{\mathbf{Q}}$

$G = \mathbf{G}_a^{d_0} \times \mathbf{G}_m^{d_1} \qquad d = d_0 + d_1$

$$G(\overline{\mathbf{Q}}) = \overline{\mathbf{Q}}^{d_0} \times (\overline{\mathbf{Q}}^{\times})^{d_1}$$

$$\exp_G : T_e(G) = \mathbf{C}^d \longrightarrow G(\mathbf{C}) = \mathbf{C}^{d_0} \times (\mathbf{C}^{\times})^{d_1}$$

$$(z_1, \ldots, z_d) \longmapsto (z_1, \ldots, z_{d_0}, e^{z_{d_0+1}}, \ldots, e^{z_d})$$

Pour α_j et β_i dans $\overline{\mathbf{Q}}$,

$$\exp_G(\beta_1, \ldots, \beta_{d_0}, \log\alpha_1, \ldots, \log\alpha_{d_1}) \in G(\overline{\mathbf{Q}})$$

Théorème de Baker. *Si*

$$\beta_0 + \beta_1 \log\alpha_1 + \cdots + \beta_n \log\alpha_n = 0$$

avec β_i *et* α_j *algébriques, alors*

1. $\beta_0 = 0$

2. Si $(\beta_1, \ldots, \beta_n) \neq (0, \ldots, 0)$, *alors* $\log\alpha_1, \ldots, \log\alpha_n$ *sont linéairement dépendants sur* $\mathbf{Q}$.

3. Si $(\log\alpha_1, \ldots, \log\alpha_n) \neq (0, \ldots, 0)$, *alors* $\beta_1, \ldots, \beta_n$ *sont linéairement dépendants sur* $\mathbf{Q}$.

Exemple: $(3-2\sqrt{2})\log 2+\sqrt{2}\log 4-\log 8=0.$

Corollaires.

1. *Hermite-Lindemann* $(n=1)$: transcendance de

$$e, \quad \pi, \quad \log 2, \quad e^{\sqrt{2}}.$$

2. *Gel'fond-Schneider* $(n=2)$: transcendance de

$$2^{\sqrt{2}}, \quad \log 2/\log 3, \quad e^{\pi}.$$

(cf. exposé de Noriko Hirata Kohno le 21 mai)

Théorème fort des six exponentielles. *Si x_1, x_2 sont deux nombres complexes linéairement indépendants sur $\mathbf{Q}$, si y_1, y_2, y_3 sont trois nombres complexes linéairement indépendants sur $\mathbf{Q}$, et si β_{ij} sont six nombres algébriques tels que*

$$e^{x_i y_j - \beta_{ij}} \in \overline{\mathbf{Q}} \quad \textit{pour} \quad i = 1, 2,\ j = 1, 2, 3,$$

alors $x_i y_j = \beta_{ij}$ pour $i = 1, 2,\ j = 1, 2, 3$.

Corollaire 1 (Théorème des six exponentielles). *Un au moins des six nombres*

$$e^{x_i y_j} \quad i = 1, 2,\ j = 1, 2, 3$$

est transcendant.

Corollaire 2 (Théorème des cinq exponentielles). *Si x_1, x_2 sont deux nombres complexes linéairement indépendants sur $\mathbf{Q}$, si y_1, y_2 sont deux nombres complexes linéairement indépendants sur $\mathbf{Q}$ et si γ est un nombre algébrique non nul, alors un au moins des cinq nombres*

$$e^{x_1y_1},\ e^{x_1y_2},\ e^{x_2y_1},\ e^{x_2y_2},\ e^{\gamma x_2/x_1}$$

est transcendant.

Démonstration. Poser $y_3 = \gamma/x_1$ de sorte que

$$x_1y_3 = \gamma \quad \text{et} \quad x_2y_3 = \gamma x_2/x_1.$$

Énoncé plus général (D. Roy). *Si x_1, x_2 sont deux nombres complexes linéairement indépendants sur $\overline{\mathbf{Q}}$ et si y_1, y_2, y_3 sont trois nombres complexes linéairement indépendants sur $\overline{\mathbf{Q}}$, un au moins des six nombres*

$$x_i y_j \quad (i = 1, 2,\ j = 1, 2, 3)$$

n'est pas de la forme

$$\beta_{ij} + \sum_{h=1}^{\ell} \beta_{ijh} \log \alpha_h.$$

Valeurs de polynômes exponentiels

Démonstration du Théorème de Baker. On suppose

$$\beta_0 + \beta_1 \log \alpha_1 + \cdots + \beta_{n-1} \log \alpha_{n-1} = \log \alpha_n$$

Méthode (B_1) (Gel'fond–Baker)

Fonctions: $z_0,\ e^{z_1},\ \ldots,\ e^{z_{n-1}},\ e^{\beta_0 z_0 + \beta_1 z_1 + \cdots + \beta_{n-1} z_{n-1}}$

Points: $\mathbf{Z}(1, \log \alpha_1, \ldots, \log \alpha_{n-1}) \in \mathbf{C}^n$

Dérivées: $\partial/\partial z_i$, $(0 \leq i \leq n-1)$.

Autre démonstration du Théorème de Baker. On suppose encore

$$\beta_0 + \beta_1 \log \alpha_1 + \cdots + \beta_{n-1} \log \alpha_{n-1} = \log \alpha_n$$

Méthode (B_2) (Généralisation de la méthode de Schneider)

Fonctions: $z_0,\ z_1,\ \ldots, z_{n-1},$

$$e^{z_0}\alpha_1^{z_1}\cdots\alpha_{n-1}^{z_{n-1}} = \exp\{z_0 + z_1\log\alpha_1 + \cdots + z_{n-1}\log\alpha_{n-1}\}$$

Points: $\{0\} \times \mathbf{Z}^{n-1} + \mathbf{Z}(\beta_0, , \ldots, \beta_{n-1}) \in \mathbf{C}^n$

Dérivée: $\partial/\partial z_0$.

Démonstration du Théorème fort des six exponentielles

On suppose que $x_1, \ldots, x_a$ sont des nombres complexes linéairement indépendants sur $\mathbf{Q}$, $y_1, \ldots, y_b$ sont des nombres complexes linéairement indépendants sur $\mathbf{Q}$, et β_{ij} sont des nombres algébriques tels que

$$e^{x_i y_j - \beta_{ij}} \in \overline{\mathbf{Q}} \quad \text{pour} \quad i = 1, \ldots, a, \; j = 1, \ldots, b$$

avec $ab > a + b$.

Fonctions: $z_i, \; e^{x_i(z_{a+1}+z_1)-z_i} \quad (1 \le i \le a)$

Points: $(\beta_{1j}, \ldots, \beta_{aj}, y_j - \beta_{1j}) \in \mathbf{C}^{a+1} \quad (1 \le j \le b)$

Dérivées: $\partial/\partial z_i$ $(2 \le i \le a)$ et $\partial/\partial z_{a+1} - \partial/\partial z_1$.

Théorème du sous-groupe linéaire

$G = \mathbf{G}_a^{d_0} \times \mathbf{G}_m^{d_1} \qquad d = d_0 + d_1$

$W \subset T_e(G)$ sous-$\mathbf{C}$-espace vectoriel rationnel sur $\overline{\mathbf{Q}}$, de dimension ℓ_0.

$Y \subset T_e(G)$ sous groupe de type fini, tel que $\Gamma = \exp(Y)$ soit contenu dans $G(\overline{\mathbf{Q}}) = \overline{\mathbf{Q}}^{d_0} \times (\overline{\mathbf{Q}}^{\times})^{d_1}$. Soit ℓ_1 le rang de Γ.

$V \subset T_e(G)$ sous-$\mathbf{C}$- espace vectoriel contenant W et Y. Soit n la dimension de V.

Hypothèse:

$$\boxed{n(\ell_1 + d_1) < \ell_1 d_1 + \ell_0 d_1 + \ell_1 d_0}$$

	d_0	d_1	ℓ_0	ℓ_1	n
Baker B_1	1	n	n	1	n
Baker B_2	n	1	1	n	n
Six exponentielles	a	a	a	b	$a+1$

Baker:

$$n(\ell_1 + d_1) = n^2 + n$$

$$\ell_1 d_1 + \ell_0 d_1 + \ell_1 d_0 = n^2 + n + 1$$

Six exponentielles: $a + b < ab$

$$n(\ell_1 + d_1) = a^2 + ab + a + b$$

$$\ell_1 d_1 + \ell_0 d_1 + \ell_1 d_0 = a^2 + 2ab$$

Dualité de Fourier-Borel:

$$(d_0, d_1, \ell_0, \ell_1) \longleftrightarrow (\ell_0, \ell_1, d_0, d_1)$$

$$\left(\frac{d}{dz}\right)^s \left(z^t e^{xz}\right)_{z=y} = \left(\frac{d}{dz}\right)^t \left(z^s e^{yz}\right)_{z=x}.$$

$$\mathsf{L}_{sy} : f \longmapsto \left(\frac{d}{dz}\right)^s f(y).$$

$$f_\zeta(z) = e^{z\zeta}, \qquad \mathsf{L}_{sy}(f_\zeta) = \zeta^s e^{y\zeta}.$$

$$\mathsf{L}_{sy}(z^t f_\zeta) = \left(\frac{d}{d\zeta}\right)^t \mathsf{L}_{sy}(f_\zeta).$$

Pour $\underline{v} = (v_1, \ldots, v_n) \in \mathbf{C}^n$, on pose

$$D_{\underline{v}} = v_1 \frac{\partial}{\partial z_1} + \cdots + v_n \frac{\partial}{\partial z_n}.$$

Soient $\underline{w}_1, \ldots, \underline{w}_{\ell_0}$, $\underline{u}_1, \ldots, \underline{u}_{d_0}$, $\underline{x}$ et $\underline{y}$ dans $\mathbf{C}^n$, $\underline{t} \in \mathbf{N}^{d_0}$ et $\underline{s} \in \mathbf{N}^{\ell_0}$. Pour $\underline{z} \in \mathbf{C}^n$, écrivons

$$(\mathbf{u}\underline{z})^{\underline{t}} = (\underline{u}_1\underline{z})^{t_1} \cdots (\underline{u}_{d_0}\underline{z})^{t_{d_0}} \qquad \text{et} \qquad D_{\mathbf{w}}^{\underline{s}} = D_{\underline{w}_1}^{s_1} \cdots D_{\underline{w}_{\ell_0}}^{s_{\ell_0}}.$$

Alors

$$\boxed{D_{\mathbf{w}}^{\underline{s}}\Big((\mathbf{u}\underline{z})^{\underline{t}} e^{\underline{x}\underline{z}}\Big)\Big|_{\underline{z}=\underline{y}} = D_{\mathbf{u}}^{\underline{t}}\Big((\mathbf{w}\underline{z})^{\underline{s}} e^{\underline{y}\underline{z}}\Big)\Big|_{\underline{z}=\underline{x}}}$$

Algèbres de Hopf

Algèbres

Une k-algèbre A est un k-module muni d'une multiplication $m : A \otimes A \to A$ et d'une unité $\eta : k \longrightarrow A$ qui sont k-linéaires et telles que les diagrammes suivants commutent

(Associativité)

$$\begin{array}{ccc} A \otimes A \otimes A & \xrightarrow{m \otimes \mathrm{Id}} & A \otimes A \\ \mathrm{Id} \otimes m \downarrow & & \downarrow m \\ A \otimes A & \xrightarrow[m]{} & A \end{array}$$

$$\begin{array}{ccccc} k \otimes A & \xrightarrow{\eta \otimes \mathrm{Id}} & A \otimes A & \xleftarrow{\mathrm{Id} \otimes \eta} & A \otimes k \\ \downarrow & & \downarrow m & & \downarrow \\ A & = & A & = & A \end{array}$$

Cogèbres

Une k-cogèbre A est un k-module muni d'une comultiplication $\Delta : A \to A \otimes A$ et d'une counité $\epsilon : A \longrightarrow k$ qui sont k-linéaires telles que les diagrammes suivants commutent

(Coassociativité)

$$\begin{array}{ccc} A & \xrightarrow{\Delta} & A \otimes A \\ \Delta \downarrow & & \downarrow \Delta \otimes \mathrm{Id} \\ A \otimes A & \xrightarrow[\mathrm{Id} \otimes \Delta]{} & A \otimes A \otimes A \end{array}$$

$$\begin{array}{ccccc} A & = & A & = & A \\ \downarrow & & \downarrow \Delta & & \downarrow \\ k \otimes A & \xleftarrow[\epsilon \otimes \mathrm{Id}]{} & A \otimes A & \xrightarrow[\mathrm{Id} \otimes \epsilon]{} & A \otimes k \end{array}$$

Bigèbres

Une bigèbre est une k-algèbre (A, m, η) avec une structure de cogèbre (A, Δ, ϵ) qui est *compatible*: Δ et ϵ sont des morphismes d'algèbres

$$\Delta(xy) = \Delta(x)\Delta(y), \quad \epsilon(xy) = \epsilon(x)\epsilon(y).$$

Algèbres de Hopf

Une algèbre de Hopf est une bigèbre munie d'une *antipode* $S : A \longrightarrow A$ qui est k-linéaire et telle que le diagramme suivant commute:

$$
\begin{array}{ccccc}
A \otimes A & \stackrel{\Delta}{\longleftarrow} & A & \stackrel{\Delta}{\longrightarrow} & A \otimes A \\
\mathrm{Id}\otimes S \downarrow & & \eta\circ\epsilon \downarrow & & \downarrow S\otimes\mathrm{Id} \\
A \otimes A & \underset{m}{\longrightarrow} & A & \underset{m}{\longleftarrow} & A \otimes A
\end{array}
$$

Dans une algèbre de Hopf les éléments *primitifs*

$$\Delta(x) = x \otimes 1 + 1 \otimes x$$

forment une algèbre de Lie pour le crochet

$$[x, y] = xy - yx$$

et les éléments *group-like*

$$\Delta(x) = x \otimes x$$

forment un groupe.

Exemples

$H = \mathbf{C}[\mathbf{G}_a]$, $\Delta(x) = x \otimes 1 + 1 \otimes x$, $\epsilon(x) = 0$, $S(x) = -x$.

$H = \mathbf{C}[\mathbf{G}_m]$, $\Delta(x) = x \otimes x$, $\epsilon(x) = 1$, $S(x) = x^{-1}$.

La catégorie des groupes algébriques linéaires commutatifs est anti-équivalente à celle des algèbres de Hopf de type fini, commutatives et co-commutatives

$$H = \mathbf{C}[\mathbf{G}_a^{d_0} \times \mathbf{G}_m^{d_1}].$$

Autres exemples

Si W est un $\mathbf{C}$-espace vectoriel, $\mathrm{Sym}(W)$ est une algèbre de Hopf de type fini commutative et co-commutative.

Si Γ est un $\mathbf{Z}$-module de type fini, l'algèbre $\mathbf{C}\Gamma$ du groupe Γ est aussi une algèbre de Hopf de type fini commutative et co-commutative.

Enfin $\mathrm{Sym}(W) \otimes \mathbf{C}\Gamma$ est encore une algèbre de Hopf de type fini commutative et co-commutative.

Interprétation de la dualité en termes d'Algèbres de Hopf

d'après Stéphane Fischler

Soit H une algèbre de Hopf sur $\overline{\mathbf{Q}}$ de type fini et abélienne (commutative et cocommutative).

Soit W le $\overline{\mathbf{Q}}$-espace vectoriel formé des éléments primitifs et Γ le groupe des éléments group-like.

On note

$$d_0 = \dim_{\overline{\mathbf{Q}}} W, \quad d_1 = \mathrm{rang}_{\mathbf{Z}} \Gamma.$$

Soit H' une autre algèbre de Hopf sur $\overline{\mathbf{Q}}$ de type fini et abélienne, W' ses éléments primitifs et Γ' ses éléments group-like. On note

$$\ell_0 = \dim_{\overline{\mathbf{Q}}} W', \quad \ell_1 = \mathrm{rang}_{\mathbf{Z}} \Gamma'.$$

Soit

$$\langle \cdot \rangle : H \times H' \longrightarrow \overline{\mathbf{Q}}$$

un produit bilinéaire telle que

$$\langle x, yy' \rangle = \langle \Delta x, y \otimes y' \rangle \quad \text{et} \quad \langle xx', y \rangle = \langle x \otimes x', \Delta y \rangle.$$

La dualité revient à permuter H et H'.

Algèbre des nombres multizêta

Soit $X = \{x_0, x_1\}$ un alphabet à deux lettres et $\mathfrak{H} = \overline{\mathbf{Q}}\langle X\rangle$ l'algèbre libre sur X (polynômes non commutatifs en x_0 et x_1, $\overline{\mathbf{Q}}$-espace vectoriel de base le monoïde X^*).

On code les suites $\underline{s} = (s_1, \ldots, s_k) \in \mathbf{N}^k$ avec $s_1 \geq 2$, $s_i \geq 1$ $(2 \leq i \leq k)$ par les mots

$$y_{\underline{s}} = x_0^{s_1-1}x_1 \cdots x_0^{s_k-1}x_1$$

de $x_0X^*x_1$. Pour $y_{\underline{s}} \in x_0X^*x_1$, on pose

$$\hat{\zeta}(y_{\underline{s}}) = \zeta(\underline{s}) = \sum_{n_1 > \cdots > n_k \geq 1} n_1^{-s_1} \cdots n_k^{-s_k}.$$

On prolonge $\hat{\zeta}$ en une application $\overline{\mathbf{Q}}$-linéaire $\mathfrak{H} \to \mathbf{R}$.

Une structure naturelle d'algèbre de Hopf non commutative sur $\mathfrak{H}$ est donnée par le coproduit

$$\Delta P = P(x_0 \otimes 1 + 1 \otimes x_0, x_1 \otimes 1 + 1 \otimes x_1)$$

la co-unité $\epsilon(x) = 0$ et l'antipode $(Sf)(x) = f(x^{-1})$ pour $x \in X$.

Critère de Friedrichs. Les éléments primitifs de $\mathfrak{H}$ constituent l'algèbre de Lie libre $\mathrm{Lie}(X)$ sur X.

En notant

$$P = \sum_{u \in X^*} (P|u)u$$

on a

$$\Delta P = \sum_{u,v \in X^*} (P|u ш v) u \otimes v.$$

Donc

$$P \in \mathrm{Lie}(X) \Longleftrightarrow (P|u ш v) = 0 \quad \text{pour tout } u,\ v \text{ dans } X^* \setminus \{e\}.$$

Dual de la concaténation: $\Phi : \mathfrak{H} \to \mathfrak{H} \otimes \mathfrak{H}$ défini par

$$\langle \Phi(w) | u \otimes v \rangle = \langle w | uv \rangle.$$

Séries formelles non commutatives.

Algèbre de Hopf de factorisation :

$$(\hat{\mathfrak{H}}, ш, \epsilon, \Phi, e, S)$$

Algèbre de Hopf de décomposition:

$$(\hat{\mathfrak{H}}, \cdot, \epsilon, \Delta, e, S)$$

Algèbre Harmonique *M. Hoffmann*

On code les suites $\underline{s} = (s_1, \ldots, s_k) \in \mathbf{N}^k$ par les mots

$$y_{\underline{s}} = y_{s_1} \cdots y_{s_k} \in x_0 X^* x_1 = Y^*$$

sur l'alphabet $Y = \{y_2, y_3, \ldots\}$ avec $y_s = x_0^{s-1} x_1$.

Algèbre de Hopf de quasi-mélange sur $\overline{\mathbf{Q}}\langle Y\rangle$*:*

$$\Delta(y_i) = y_i \otimes 1 + 1 \otimes y_i,$$

$$\epsilon(P) = (P|1),$$
$$S(y_{i_1} \cdots y_{i_r}) = (-1)^r y_{i_r} \cdots y_{i_1}.$$