

Exposé de clôture, Galois

Galois est un exemple rare, peut-être seulement égalé par certains poètes ou musiciens, d'un créateur qui, lors du 200-ème anniversaire de sa naissance nous paraisse toujours aussi jeune et fringant. En fait on peut arguer que sa théorie de l'ambiguïté, fruit de ses pensées mathématiques, est comme un animal sauvage qui n'a toujours pas été vraiment capturé par le formalisme moderne. Contraste saisissant entre le petit nombre de pages manuscrites que Galois a laissé à sa mort et leur éclatante influence sur les mathématiques.

Ainsi la fonction

$$(X_1 - X)(X_a - X)X_{a^2} - X) \dots$$

devra, quel que soit X , être connue.

Il *faut* donc et il *suffit* que l'équation qui donne cette fonction des racines admette, quel que soit X , une valeur rationnelle.

Si l'équation proposée a tous ses coefficients rationnels, l'équation auxiliaire qui donne cette fonction les aura tous aussi, et il suffira de reconnaître si cette équation auxiliaire du degré $1.2.3 \dots (n - 2)$ a ou non une racine rationnelle, ce que l'on sait faire.

C'est là le moyen qu'il faudrait employer dans la pratique. Mais nous allons présenter le théorème sous une autre forme.

PROPOSITION VIII.

THÉORÈME. « Pour qu'une équation irréductible de degré premier » soit soluble par radicaux, il *faut* et il *suffit* que deux quelconques » des racines étant connues, les autres s'en déduisent rationnelle- » ment. »

Premièrement, il le faut, car la substitution

$$x_k, \quad x_{a k + b}$$

ne laissant jamais deux lettres à la même place, il est clair qu'en adjoignant deux racines à l'équation, par la proposition IV, son groupe devra se réduire à une seule permutation.

En second lieu, cela suffit; car, dans ce cas, aucune substitution du groupe ne laissera deux lettres aux mêmes places. Par conséquent, le groupe contiendra tout au plus $n(n - 1)$ permutations. Donc il ne contiendra qu'une seule substitution circulaire (sans quoi il y aurait au moins n^2 permutations). Donc toute substitution du groupe, x_k, x_{fk} , devra satisfaire à la condition

$$f(k + c) = f^k + C,$$

Donc, etc.

Le théorème est donc démontré.

1) **Groupe de Galois cosmique**

Renormalisation et ambiguïté galoisienne.

2) **Corps de constantes en physique**

Anneaux de Fontaine à la place archimédienne.

3) **Limite $q \rightarrow 1$ des corps de Galois**

Fonction zêta de Soulé.

Références

- 1) A. Connes, M. Marcolli, *Noncommutative Geometry, Quantum Fields, and Motives*, Colloquium Publications, Vol.55, American Mathematical Society, 2008.
- 2) A. Connes, C. Consani, *Characteristic 1, entropy and the absolute point*; arXiv :0911.3537v1.
- 3) A. Connes, C. Consani, *Schemes over \mathbb{F}_1 and zeta functions*, Compositio Mathematica 146 (6), (2010) 1383–1415.

Groupe de Galois cosmique

“La parenté de plus en plus manifeste entre le groupe de Grothendieck–Teichmüller d’une part, et le groupe de renormalisation de la Théorie Quantique des Champs n’est sans doute que la première manifestation d’un groupe de symétrie des constantes fondamentales de la physique, une espèce de groupe de Galois cosmique !”

Pierre Cartier

Théorie des champs perturbative

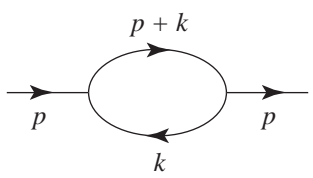
L'Amplitude de probabilité d'une configuration classique A est donnée par la formule de Dirac et Feynman

$$e^{i \frac{S(A)}{\hbar}}, \quad S(A) = \int \mathcal{L}(A) d^4x$$

On passe en Euclidien

$$Z(J_E) = \mathcal{N} \int \exp \left(- \frac{S(\phi_E) - \langle J_E, \phi_E \rangle}{\hbar} \right) \mathcal{D}[\phi_E]$$

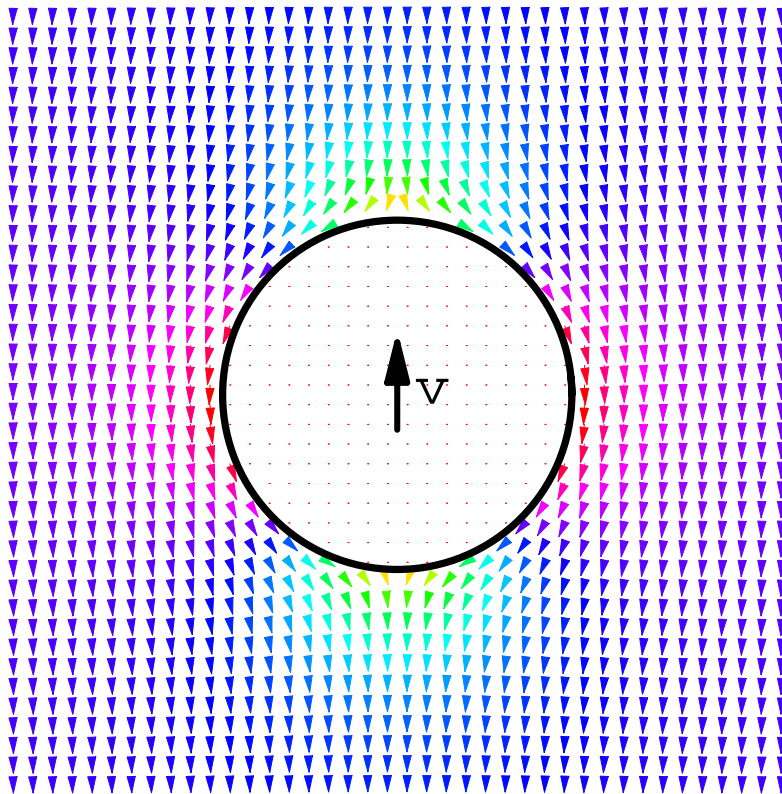
Développement perturbatif donne des **intégrales divergentes** indexées par des graphes de Feynman Γ



The diagram shows a bubble loop with two external lines. The left external line has momentum p entering the loop. The right external line has momentum p leaving the loop. The top arc of the loop has momentum $p+k$ flowing clockwise. The bottom arc has momentum k flowing counter-clockwise. To the right of the diagram is an equals sign.

$$\int \frac{1}{k^2 + m^2} \frac{1}{((p+k)^2 + m^2)} d^D k$$

Renormalisation



Green 1830

$$F = m a$$

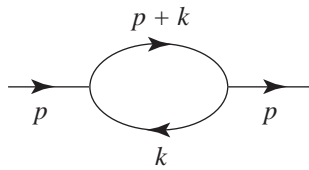
$$m \rightarrow m + \frac{1}{2}M$$

Dim-Reg

La formule de base

$$\int e^{-\lambda q^2} d^D q = \pi^{D/2} \lambda^{-D/2}$$

Exemple :



$$\rightarrow \int \frac{1}{k^2 + m^2} \frac{1}{((p+k)^2 + m^2)} d^D k.$$

$$\frac{1}{k^2 + m^2} \frac{1}{(p+k)^2 + m^2} =$$

$$\int_{s>0, t>0} e^{-s(k^2+m^2)-t((p+k)^2+m^2)} ds dt.$$

Dim-Reg, exemple

On diagonalise la forme quadratique $-Q(k)$ en exposant, avec $s = (1 - x)\lambda$, $t = x\lambda$,

$$-Q(k) = -\lambda ((k + xp)^2 + ((x - x^2)p^2 + m^2)),$$

On obtient en posant $q = k + xp$,

$$\begin{aligned} & \int_0^1 \int_0^\infty e^{-(\lambda(x-x^2)p^2 + \lambda m^2)} \int e^{-\lambda q^2} d^D q \lambda d\lambda dx \\ &= \pi^{D/2} \int_0^1 \int_0^\infty e^{-(\lambda(x-x^2)p^2 + \lambda m^2)} \lambda^{-D/2} \lambda d\lambda dx \\ &= \pi^{D/2} \Gamma(2-D/2) \int_0^1 ((x-x^2)p^2 + m^2)^{D/2-2} dx. \end{aligned}$$

Soustraction–Minimale (MS)

Préparation

On prépare d'abord un graphe Γ , en remplaçant la valeur non-renormalisée $U(\Gamma)$ par

$$\bar{R}(\Gamma) = U(\Gamma) + \sum_{\gamma \subset \Gamma} C(\gamma)U(\Gamma/\gamma)$$

Contre-termes

$$C(\Gamma) = -T(\bar{R}(\Gamma)) = \\ -T \left(U(\Gamma) + \sum_{\gamma \subset \Gamma} C(\gamma)U(\Gamma/\gamma) \right)$$

Valeur renormalisée

$$R(\Gamma) = \bar{R}(\Gamma) + C(\Gamma) = \\ U(\Gamma) + C(\Gamma) + \sum_{\gamma \subset \Gamma} C(\gamma)U(\Gamma/\gamma)$$

Algèbre de Hopf des graphes

(Dirk Kreimer \rightarrow arbres, ac + dk \rightarrow graphes)

Comme algèbre, \mathcal{H} est l'algèbre commutative libre engendrée par les graphes **1PI**.

Le **coproduit**

$$\Delta : \mathcal{H} \rightarrow \mathcal{H} \otimes \mathcal{H}$$

est spécifié sur les graphes **1PI** par

$$\Delta \Gamma = \Gamma \otimes 1 + 1 \otimes \Gamma + \sum_{\gamma \subset \Gamma} \gamma_{(i)} \otimes \Gamma / \gamma_{(i)}$$

Ici γ est un sous-ensemble non-trivial $\gamma \subset \tilde{\Gamma}$.

Coproduit

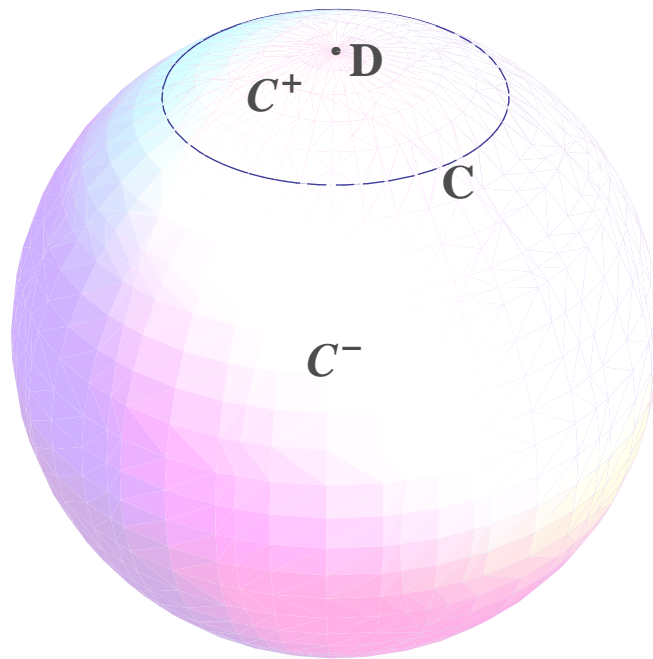
$$\Delta(-\bigcirc-) = -\bigcirc- \otimes 1 + 1 \otimes -\bigcirc-$$

$$\left\{ \begin{array}{l} \Delta(-\bigoplus-) = -\bigoplus- \otimes 1 + 1 \otimes -\bigoplus- + \\ 2 \text{---}\triangleleft \otimes -\bigcirc- \end{array} \right.$$

$$\left\{ \begin{array}{l} \Delta(-\diamond-) = -\diamond- \otimes 1 + 1 \otimes -\diamond- \\ + 2 \text{---}\triangleleft\!\!\!\diagup \otimes -\bigcirc- + 2 \text{---}\triangleleft \otimes -\bigoplus- \\ + \text{---}\triangleleft \text{---}\triangleleft \otimes -\bigcirc- \end{array} \right.$$

Fibrés sur $\mathbb{P}^1(\mathbb{C})$

$$\gamma(z) = \gamma_-(z)^{-1} \gamma_+(z) \quad z \in C$$



Décomposition de Birkhoff

Théorème (ac+dk)

Soit $\phi : \mathcal{H} \rightarrow K = \mathbb{C}\{z\}[z^{-1}]$ un homomorphisme d'algèbre. La décomposition de Birkhoff du lacet correspondant est donnée par récurrence par

$$\phi_{-}(X) = -T \left(\phi(X) + \sum \phi_{-}(X')\phi(X'') \right)$$

et

$$\phi_{+}(X) = \phi(X) + \phi_{-}(X) + \sum \phi_{-}(X')\phi(X'').$$

Cela coïncide avec le procédé récursif de MS !

$$\phi = U, \phi_{-} = C, \text{ et } \phi_{+} = R$$

⇒ compréhension conceptuelle du procédé récursif des physiciens

1. Il existe une unique application méromorphe $\gamma(z) \in G = \text{Hom}(\mathcal{H}, \mathbb{C})$, pour $z \in \mathbb{C}$, $z \neq 0$, de coordonnées $U(\Gamma)_{d=D-z}$.
2. La valeur renormalisée d'une observable est obtenue (pour Dim-Reg + MS) en remplaçant $\gamma(0)$ par $\gamma_+(0)$, où

$$\gamma(z) = \gamma_-(z)^{-1} \gamma_+(z)$$

est la décomposition de Birkhoff du lacet $\gamma(z)$ autour d'un cercle infinitésimal centré en $z = 0$.

Action sur les constantes de couplage

$$G \xrightarrow{\rho} \text{Diff}_{\mathbb{C}}$$

$$\left(g + \sum_{\text{diagram}} g^{2\ell+1} \frac{\Gamma}{S(\Gamma)} \right) \left(1 - \sum_{\text{diagram}} g^{2\ell} \frac{\Gamma}{S(\Gamma)} \right)^{-3/2}$$

Corollaire

Considérons la constante de couplage effective nonrenormalisée $g_{\text{eff}}(\varepsilon)$ comme une série formelle en g et soit

$$g_{\text{eff}}(\varepsilon) = g_{\text{eff}+}(\varepsilon) (g_{\text{eff}-}(\varepsilon))^{-1}$$

sa décomposition de Birkhoff (opposée) dans le groupe des difféomorphismes formels. Alors le lacet $g_{\text{eff}-}(\varepsilon)$ est la constante de couplage nue et $g_{\text{eff}+}(0)$ la constante de couplage renormalisée.

Groupe de renormalisation

L'analyse dimensionnelle introduit un paramètre de masse,

$$d^{D-z}k \mapsto \mu^z d^{D-z}k$$

La graduation par le nombre de boucles donne les automorphismes θ_t ,

$$\gamma_{e^t\mu}(z) = \theta_{tz}(\gamma_\mu(z)) \quad \forall t \in \mathbb{R}, \quad z = D - d$$

Le $\gamma_{\mu-}$ de la décomposition de Birkhoff

$$\gamma_\mu(z) = \gamma_{\mu-}(z)^{-1} \gamma_{\mu+}(z)$$

est **indépendant** de μ , $\frac{\partial}{\partial \mu} \gamma_{\mu-}(z) = 0$. La limite

$$F_t = \lim_{z \rightarrow 0} \gamma_{-}(z) \theta_{tz}(\gamma_{-}(z)^{-1})$$

définit un sous-groupe à un paramètre de $G(\mathbb{C})$.

$$\gamma_{e^t\mu+}(0) = F_t \gamma_{\mu+}(0), \quad \forall t \in \mathbb{R}.$$

$$\gamma_{-}(z) = \lim_{t \rightarrow \infty} e^{-t\left(\frac{\beta}{z} + Z_0\right)} e^{tZ_0}$$

Connections plates équisingulières

(ac + M. Marcolli)

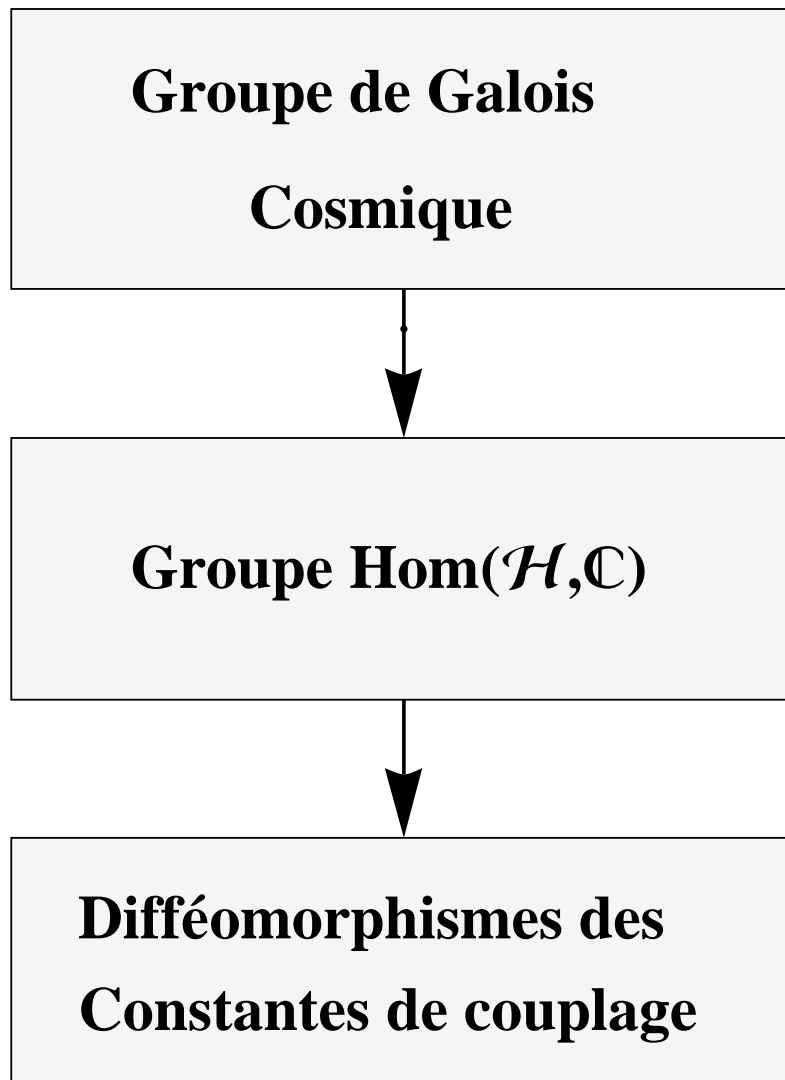
Une connexion plate ω définie sur $B^* = B \setminus V$, $B = \Delta \times \mathbb{G}_m$, $V = \{0\} \times \mathbb{G}_m$, est *équisingulière* si elle est invariante par \mathbb{G}_m et si la classe d'équivalence de sa restriction à une section $\sigma : \Delta \mapsto B$ ne dépend que de $\sigma(0)$.

Théorème

La catégorie des fibrés plats équisinguliers est équivalente à la catégorie des représentations de dimension finie d'un groupe algébrique affine U^* . Ce groupe est le produit semi-direct par \mathbb{G}_m (agissant par la graduation) du groupe pro-unipotent U dont l'algèbre de Lie

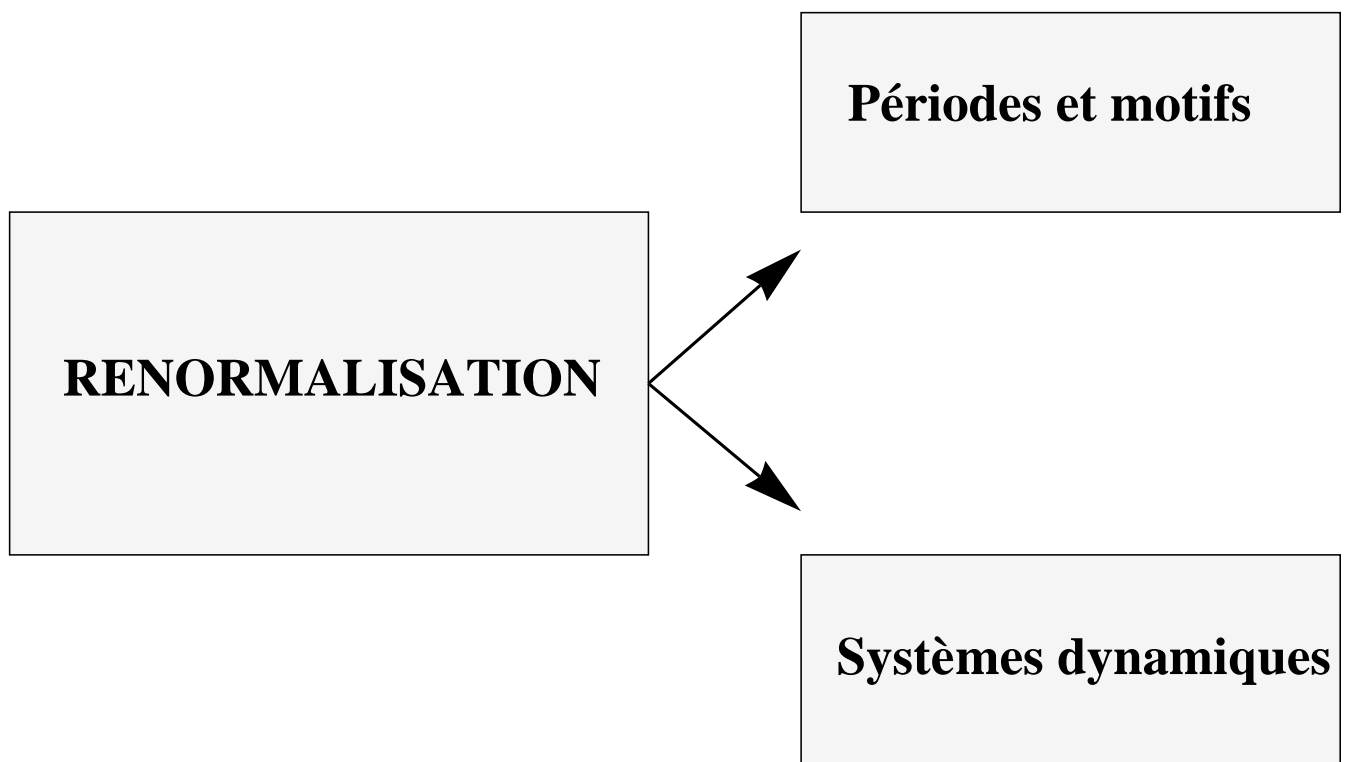
$$\mathrm{Lie}(U) = \mathcal{F}(1, 2, 3, \dots).$$

est librement engendrée par un générateur e_{-n} de degré n pour tout entier $n \geq 1$.



Motifs de Tate mixtes

- Motifs purs, catégorie Tannakienne \mathcal{M}_K (K corps de nombres). Sous-catégorie engendrée par les $\mathbb{Q}(m) = \mathbb{Q}(1)^m$, $m \in \mathbb{Z}$, $\mathbb{Q}(1) = \mathbb{L}^{-1}$, a pour groupe de Galois \mathbb{G}_m .
- Motifs mixtes, catégorie triangulée \mathcal{DM}_K , sous-catégorie $\mathcal{DM}\mathcal{T}_K$ engendrée par les $\mathbb{Q}(m)$ permet de définir une catégorie abélienne Tannakienne \mathcal{MT}_K des motifs de Tate mixtes.
- Le groupe de Galois de cette catégorie Tannakienne est de la forme $U \rtimes \mathbb{G}_m$ où le \mathbb{G}_m vient des motifs purs et le groupe unipotent U reflète les extensions non-triviales.



Grothendieck, dessins d'enfants

- C peut être définie sur $\bar{\mathbb{Q}}$
- C est la compactification d'un revêtement fini non-ramifié de $\mathbb{P}^1(\mathbb{C})$ dont on a enlevé les trois points $\{0, 1, \infty\}$.
- C est isomorphe à la compactification du quotient du demi-plan de Poincaré par un sous-groupe d'indice fini de $\mathrm{PSL}(2, \mathbb{Z})$.
- En tant que variété conforme C est obtenue en recollant entre eux un nombre fini de triangles équilatères (dotés de la structure conforme Euclidienne).

Schéma $X = \mathbb{P}^1 \setminus \{0, 1, \infty\}$

$$1 \rightarrow \pi_1^{\text{etale}}(X_{\bar{\mathbb{Q}}}) \rightarrow \pi_1^{\text{etale}}(X_{\mathbb{Q}}) \rightarrow \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \rightarrow 1$$

Théorème (Francis Brown)

Soit $G_{\mathcal{MT}}$ le groupe de Galois motivique de la catégorie $\mathcal{MT}(\mathbb{Z})$ des motifs de Tate mixtes non ramifiés sur \mathbb{Z} . Soit $\mathcal{MT}'(\mathbb{Z})$ la sous-catégorie pleine engendrée par le groupe fondamental motivique de $\mathbb{P}^1 \setminus \{0, 1, \infty\}$. L'application

$$G_{\mathcal{MT}} \rightarrow G_{\mathcal{MT}'}$$

est un isomorphisme.

Les périodes de $\mathcal{MT}(\mathbb{Z})$ sont les valeurs zêta multiples.

“Constantes” en physique

Les calculs des physiciens regorgent d'exemples de “constantes” telles les constantes de couplage g des interactions (électromagnétiques, faibles et fortes) qui n'ont de “constantes” que le nom. Elles dépendent, en réalité, du niveau d'énergie μ auquel les expériences sont réalisées et sont des fonctions $g(\mu)$, de sorte que les physiciens des hautes énergies étendent implicitement le “corps des constantes” avec lequel ils travaillent, passant du corps \mathbb{C} des scalaires à des fonctions $g(\mu)$. Le groupe d'automorphismes engendré par $\mu\partial/\partial\mu$ est le groupe d'ambiguïté de la théorie physique.

Pour obtenir le bon cadre mathématique, il faut “transposer” les constructions des anneaux de Fontaine de la théorie de Hodge p -adique à la place archimédienne (travail en cours avec C. Consani, *cf.* aussi réf. 2).

.

Anneaux de périodes (Fontaine)

On part du corps \mathbb{C}_p complétion d’une clôture algébrique de \mathbb{Q}_p ,

- Perfection universelle $F(\mathbb{C}_p)$.
- Anneaux de Witt $\mathbb{W}(\mathcal{O}_F) \subset \mathbb{W}(F)$.
- Anneau B^+ de fonctions analytiques rigides, complétion de $\mathbb{W}(\mathcal{O}_F)[\frac{1}{p}]$.
- Courbe X quotient du spectre de $B = B^+[\frac{1}{[a]}]$ par l’action du Frobenius (Fontaine + Fargues).

Perfection

La construction suivante donne un corps $F = F(\mathbb{C}_p)$ de caractéristique p ,

$$F = \{x = (x^{(n)})_{n \geq 0} \mid x^{(n)} \in \mathbb{C}_p, (x^{(n+1)})^p = x^{(n)}\}$$

avec les opérations ($x, y \in F$)

Addition

$$(x + y)^{(n)} = \lim_{m \rightarrow \infty} (x^{(n+m)} + y^{(n+m)})^{p^m}$$

Produit

$$(xy)^{(n)} = x^{(n)} y^{(n)}$$

Place archimédienne

Remplaçons \mathbb{C}_p par \mathbb{R} et soit $\kappa \in \mathbb{Q}_+$, impair ($|\kappa|_2 = 1$) avec $|\kappa|_\infty < 1$, considérons

$$F = \{x = (x^{(n)})_{n \geq 0} | x^{(n)} \in \mathbb{R}, (x^{(n+1)})^\kappa = x^{(n)}\}$$

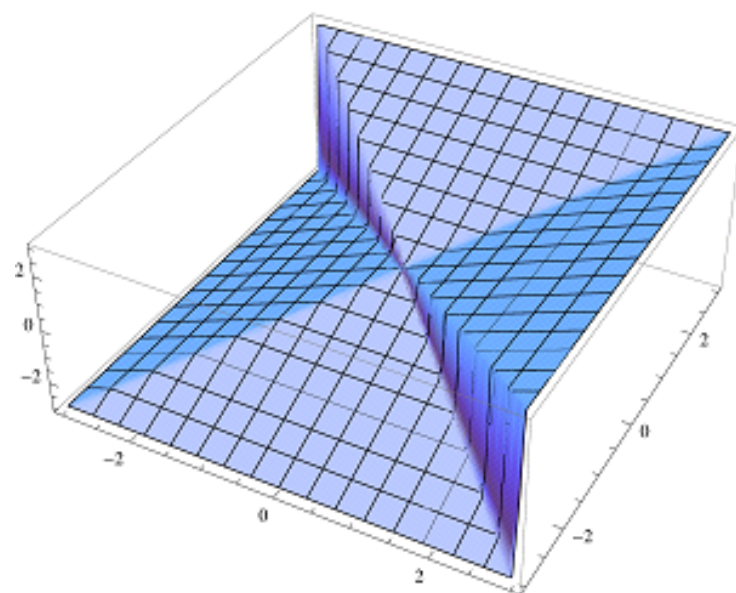
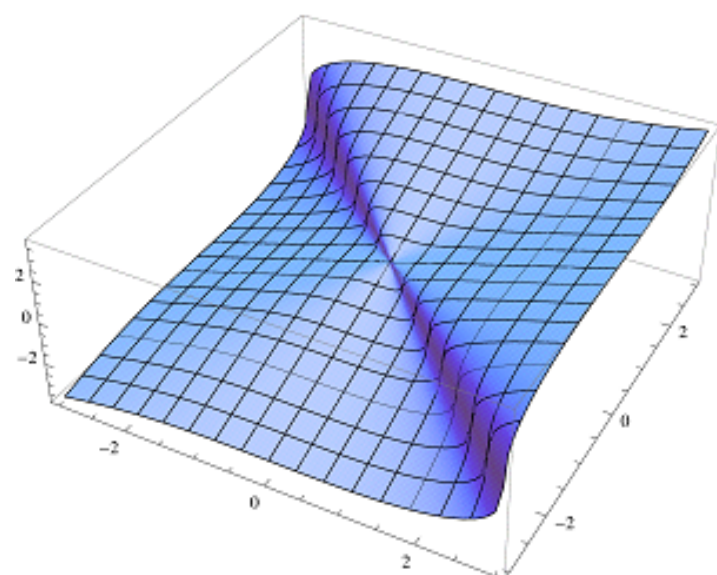
avec les opérations ($x, y \in F$)

Addition

$$(x + y)^{(n)} = \lim_{m \rightarrow \infty} (x^{(n+m)} + y^{(n+m)})^{\kappa^m}$$

Produit

$$(xy)^{(n)} = x^{(n)} y^{(n)}$$



Hypercorps \mathcal{TR} (Viro)

La limite des lois de corps définit un hypercorps au sens de Krasner.

(i) L'égalité $\theta_\lambda(x) = \text{sign}(x)|x|^\lambda$ définit un groupe d'automorphismes $\theta_\lambda \in \text{Aut}(\mathcal{TR})$, $\lambda \in \mathbb{R}_+^*$, et $\theta_\lambda(x) = x^\lambda$ pour $\lambda \in \mathbb{Q}_+^*$ impair.

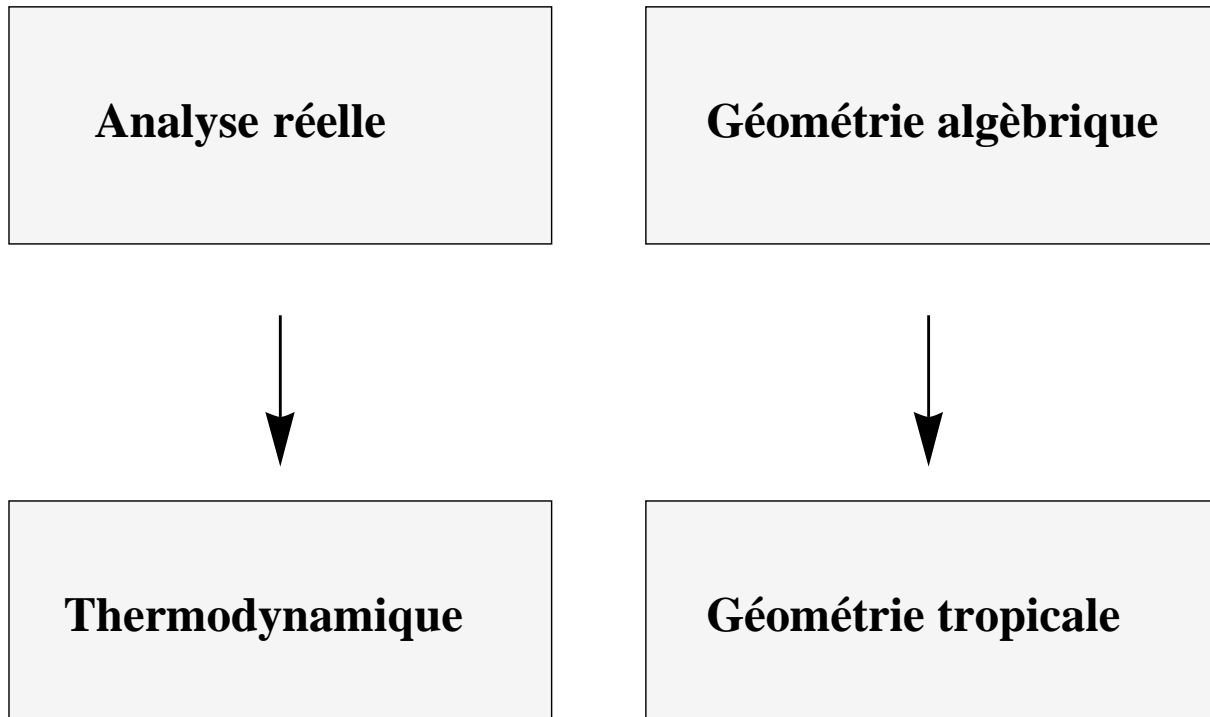
(ii) La partie positive \mathcal{TR}^+ de \mathcal{TR} est le semi-corps \mathbb{R}_+^{\max} (de la géométrie tropicale).

(iii) Le compact $[-1, 1] \subset \mathcal{TR}$ est le sous-anneau compact maximal $\mathcal{O}_{\mathcal{TR}}$ de \mathcal{TR} .

Cela me rappelle que reprendre aujourd'hui l'héritage de Galois, c'est sûrement aussi accepter le risque de la solitude qui a été sienne en son temps. Peut-être les temps changent-ils moins que nous ne le pensons, souvent ! Ce "risque" pourtant ne prend pas pour moi figure de menace. S'il m'arrive d'être peiné et frustré par l'affectation d'indifférence ou de dédain de ceux que j'ai aimés, jamais par contre depuis de longues années la solitude, mathématique ou autre, ne m'a-t-elle pesé. S'il est une amie fidèle que sans cesse j'aspire à retrouver quand je viens à la quitter, c'est elle !

A. Grothendieck

Dequantization (Maslov, Litvinov)



La transformation de Fourier devient la transformation de Legendre, la convolution de deux fonctions est

$$f \star g(z) = \sup_{x+y=z} f(x)g(y)$$

Caractéristique 1

Un semi-anneau A est un monoïde pour l'addition et la multiplication, avec éléments unité 0 et 1, et la multiplication est distributive par rapport à l'addition. Il est de *caractéristique 1* quand

$$x + x = x, \quad \forall x \in A$$

Un semi-anneau A est *simplifiable* si la multiplication par tout $x \neq 0$ est injective. Pour tout $n \in \mathbb{N}$, $n > 0$, l'application $\vartheta_n(x) = x^n$ est alors un endomorphisme injectif de A . Nous dirons que A est *parfait* quand ϑ_n est surjectif pour tout n . On a alors $\vartheta_\alpha \in \text{Aut}(A)$ pour tout $\alpha \in \mathbb{Q}_+$.

Coefficients $w(\alpha)$ (cf. Référence 2)

Pour obtenir l'analogie de la construction de l'anneau de Witt dans le cadre des semi-anneaux parfaits de caractéristique 1, on recherche les fonctions $w(\alpha) \in A$ définies pour $\alpha \in I = \mathbb{Q} \cap [0, 1]$ qui rendent associative et commutative l'opération

$$x +' y = \sum_{\alpha \in I} w(\alpha) x^\alpha y^{1-\alpha}$$

Outre la condition de symétrie $w(1-\alpha) = w(\alpha)$ on obtient l'équation fonctionnelle

$$w(\alpha)w(\beta)^\alpha = w(\alpha\beta)w(\gamma)^{(1-\alpha\beta)}, \quad \gamma = \frac{\alpha(1-\beta)}{1-\alpha\beta}.$$

Solution générale

$$I = \mathbb{Q} \cap [0, 1], \quad w : I \rightarrow G, \quad w(1 - \alpha) = w(\alpha),$$

$$w(\alpha)w(\beta)^\alpha = w(\alpha\beta)w(\gamma)^{(1-\alpha\beta)}, \quad \gamma = \frac{\alpha(1 - \beta)}{1 - \alpha\beta}.$$

La solution générale de cette équation à valeurs dans G groupe abélien uniquement divisible, est donnée par

$$w(\alpha) = \chi(\alpha)^\alpha \chi(1 - \alpha)^{1-\alpha}, \quad \forall \alpha \in (0, 1) \cap \mathbb{Q}$$

où $\chi : \mathbb{Q}_+^\times \rightarrow G$ est un homomorphisme de groupes.

(Relation au $1\frac{1}{2}$ -logarithme de Kontsevich).

Solution positive, Entropie

Soit G un groupe abélien ordonné uniquement divisible et tel que l'action $x \mapsto x^\alpha$ de \mathbb{Q}^\times sur G par divisibilité se prolonge en une action de \mathbb{R}^\times . Soit $w : I \rightarrow G$ une solution telle que

$$w(\alpha) \geq 1, \quad \forall \alpha \in I$$

Il existe alors $\rho \in G, \rho \geq 1$ tel que

$$w(\alpha) = \rho^{-\alpha \log \alpha - (1-\alpha) \log(1-\alpha)}, \quad \forall \alpha \in I$$

$$S(\alpha) = -\alpha \log \alpha - (1 - \alpha) \log(1 - \alpha)$$

Witt archimédien

La multiplication ne change pas

$$(fg)(T) = f(T)g(T)$$

L'addition est donnée par

$$(f_1 +_w f_2)(T) = \sum_I w(\alpha, T) f_1(T)^\alpha f_2(T)^{1-\alpha}$$

L'égalité

$$\log(e^a + e^b) = \sup_{\alpha \in [0,1]} S(\alpha) + \alpha a + (1 - \alpha)b$$

montre que

$$(f_1 +_w f_2)(T) = (f_1(T)^{1/T} + f_2(T)^{1/T})^T$$

L'exemple prototype de somme pour \dagger_w est donné par les intégrales fonctionnelles

$$Z(J_E) = \mathcal{N} \int \exp \left(-\frac{S(\phi_E) - \langle J_E, \phi_E \rangle}{\hbar} \right) \mathcal{D}[\phi_E]$$

où $S(\phi_E)$ est l'action Euclidienne, ϕ_E le champ classique, J_E la source qui est un élément du dual et \mathcal{N} est l'inverse de

$$\int \exp \left(-\frac{S(\phi_E)}{\hbar} \right) \mathcal{D}[\phi_E]$$

Witt archimédien

- La section de Teichmüller application multiplicative $[x](T) = x$.
- Les automorphismes de Frobenius F_λ pour $\lambda \in \mathbb{R}_+^*$,

$$F_\lambda(f)(T) = f(T/\lambda)^\lambda$$

- Les Verschiebung, applications additives V_λ , $\lambda \in \mathbb{R}_+^*$,

$$V_\lambda(f)(T) = \lambda^T f(\lambda T)^{1/\lambda}$$

- Les fonctions $T \mapsto x^T$ sont les point fixes des automorphismes F_λ . L'évaluation $f \mapsto \theta(f) = f(1)$ est un homomorphisme vers \mathbb{R} .

présenter par i la racine de cette équation, en sorte que

$$(i) \quad i^3 - i + 2 = 0,$$

et l'on aura toutes les imaginaires de la forme

$$a + a_1 i + a_2 i^2,$$

en élevant i à toutes les puissances, et réduisant par l'équation (i).

Le principal avantage de la nouvelle théorie que nous venons d'exposer est de ramener les congruences à la propriété (si utile dans les équations ordinaires) d'admettre précisément autant de racines qu'il y a d'unités dans l'ordre de leur degré.

La méthode pour avoir toutes ces racines sera très-simple. Premièrement on pourra toujours préparer la congruence donnée $Fx = 0$, de manière à ce qu'elle n'ait plus de racines égales, ou, en d'autres termes, à ce qu'elle n'ait plus de facteur commun avec $F'x = 0$, et le moyen de le faire est évidemment le même que pour les équations ordinaires.

Ensuite, pour avoir les solutions entières, il suffira, ainsi que M. Libri paraît en avoir fait le premier la remarque, de chercher le plus grand facteur commun à $Fx = 0$ et à $x^{p-1} = 1$.

Si maintenant on veut avoir les solutions imaginaires du second degré, on cherchera le plus grand facteur commun à $Fx = 0$ et à $x^{p-1} = 1$, et, en général, les solutions de l'ordre ν seront données par le plus grand commun diviseur à $Fx = 0$ et à $x^{p^\nu-1} = 1$.

C'est surtout dans la théorie des permutations, où l'on a sans cesse besoin de varier la forme des indices, que la considération des racines imaginaires des congruences paraît indispensable. Elle donne un moyen simple et facile de reconnaître dans quel cas une équation primitive est soluble par radicaux, comme je vais essayer d'en donner en deux mots une idée.

Soit une équation algébrique $fx = 0$ de degré p^ν ; supposons que les p^ν racines soient désignées par x_k , en donnant à l'indice k les p^ν valeurs déterminées par la congruence $k^{p^\nu} = k \pmod{p}$.

Prenons une fonction quelconque rationnelle V des p^ν racines x_k . Transformons cette fonction en substituant partout à l'indice k l'in-

dice $(ak + b)^{p^r}$, a, b, r étant des constantes arbitraires satisfaisant aux conditions de $a^{p^r-1} = 1$, $b^{p^r} = b \pmod{p}$ et de r entier.

En donnant aux constantes a, b, r toutes les valeurs dont elles sont susceptibles, on obtiendra en tout $p^r(p^r - 1) \nu$ manières de permuter les racines entre elles par des substitutions de la forme $[x_k, x_{(ak+b)^{p^r}}]$, et la fonction V admettra en général par ces substitutions $p^r(p^r - 1) \nu$ formes différentes.

Admettons maintenant que l'équation proposée $fx = 0$ soit telle, que toute fonction des racines invariable par les $p^r(p^r - 1) \nu$ permutations que nous venons de construire, ait pour cela même une valeur numérique rationnelle.

On remarque que, dans ces circonstances, l'équation $fx = 0$ sera soluble par radicaux, et, pour parvenir à cette conséquence, il suffit d'observer que la valeur substituée à k , dans chaque indice, peut se mettre sous les trois formes

$$(ak + b)^{p^r} = [a(k + b')]^{p^r} = a^r k^{p^r} + b'' = a'(k + b'')^{p^r}.$$

Les personnes habituées à la théorie des équations le verront sans peine.

Cette remarque aurait peu d'importance si je n'étais parvenu à démontrer que, réciproquement, une équation primitive ne saurait être soluble par radicaux, à moins de satisfaire aux conditions que je viens d'énoncer. (J'excepte les équations du neuvième et du vingt-cinquième degré.)

Ainsi, pour chaque nombre de la forme p^r , on pourra former un groupe de permutations tel, que toute fonction des racines invariable par ces permutations devra admettre une valeur rationnelle quand l'équation de degré p^r sera primitive et soluble par radicaux.

D'ailleurs, il n'y a que les équations d'un pareil degré p^r qui soient à la fois primitives et solubles par radicaux.

Le théorème général que je viens d'énoncer précise et développe les conditions que j'avais données dans le *Bulletin* du mois d'avril. Il indique le moyen de former une fonction des racines dont la valeur sera rationnelle, toutes les fois que l'équation primitive de degré p^r sera soluble par radicaux, et mène, par conséquent, aux caractères de réso-

Limite $q \rightarrow 1$ des corps de Galois

Fonction zêta de Soulé (motivée par Manin, Kurokawa, Deninger)

$N(q)$ donnée,

$$Z(q, T) = \exp \left(\sum_{r \geq 1} N(q^r) T^r / r \right)$$

$$\zeta_N(s) = \lim_{q \rightarrow 1} (q - 1)^\chi Z(q, q^{-s}), \quad \chi = N(1)$$

Problème : (cf. Référence 3, ac + C. Consani)

Existe t'il $N(q)$ telle que $\zeta_N(s)$ soit la fonction zêta de Riemann (complète)

$$\zeta_N(s) = \zeta_{\mathbb{Q}}(s) = \pi^{-s/2} \Gamma(s/2) \zeta(s)$$

Deux difficultés

1) D'après Soulé la valeur $N(1)$ est la caractéristique d'Euler de la "courbe" hypothétique $C = \overline{\text{Spec } \mathbb{Z}}$ sur \mathbb{F}_1 . Comme le genre de C est infini, on a $N(1) = -\infty$. En fait on montre

$$\frac{\partial_s \zeta_N(s)}{\zeta_N(s)} = - \int_1^\infty N(u) u^{-s} d^*u$$

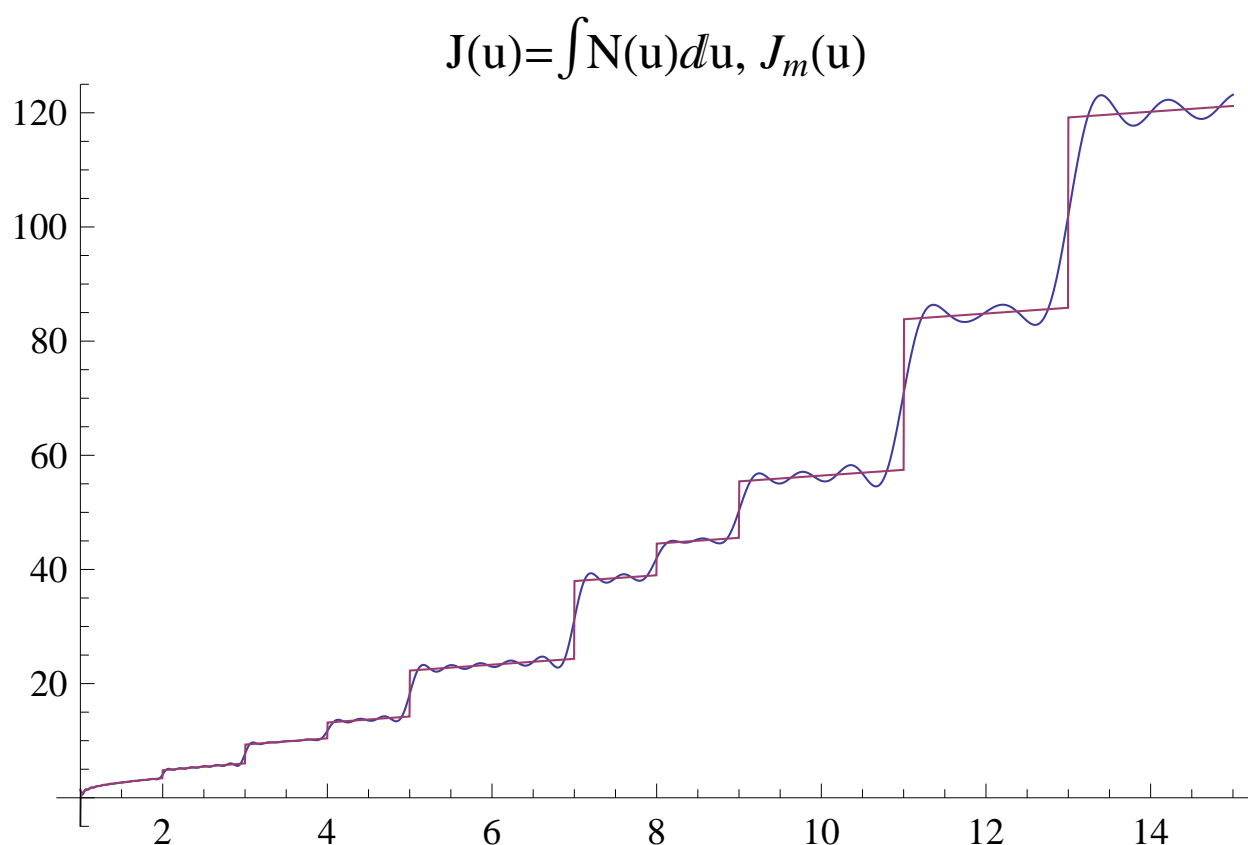
2) $N(1) = -\infty$ crée une tension avec la positivité de $N(q)$ pour $q > 1$. En fait la distribution $N(q)$ déterminée par

$$\frac{\partial_s \zeta_{\mathbb{Q}}(s)}{\zeta_{\mathbb{Q}}(s)} = - \int_1^\infty N(u) u^{-s} d^*u .$$

est positive pour $q > 1$ et pour $q = 1$ est donnée par

$$N(1) = \lim_{\epsilon \rightarrow 0} \frac{J(1 + \epsilon) - J(1)}{\epsilon} \\ \sim -\frac{1}{2} E \log E, \quad E = \frac{1}{\epsilon}$$

où $J(u)$ est une primitive de $N(u)$.



Primitive de $N(u)$ et approximation par

$$J_m(u) = \frac{u^2}{2} - \sum_{Z_m} \text{order}(\rho) \frac{u^{\rho+1}}{\rho+1} + u$$

$J(u)$ change de signe pour $u \sim 1.0050692$

Formules explicites pour $N(u)$

Théorème (ac + C. Consani) :

(1) La fonction $N(q)$ existe comme distribution et est donnée par

$$N(q) = q - \frac{d}{dq} \left(\sum_{\rho \in Z} \text{order}(\rho) \frac{q^{\rho+1}}{\rho+1} \right) + 1$$

où Z est l'ensemble des zéros non-triviaux de la fonction zêta de Riemann.

(2) La fonction $N(q)$ est positive (comme *distribution*) pour $q > 1$.

(3) La valeur $N(1)$ est égale à $-\infty$ et reflète la distribution des zéros de zêta en $E \log E$.

Courbe $C = \overline{\text{Spec } \mathbb{Z}}$?

La fonction $N(q)$ donne des renseignements précieux sur C . Dans le cas des variétés sur un corps fini, la fonction $N(q)$ est à valeurs entières. De plus $N(q^k) \leq N(q^\ell)$ quand k divise ℓ . Ceci n'est plus le cas pour $N(u)$ qui a une contribution de la forme

$$\kappa(u) = \frac{u^2}{u^2 - 1}$$

qui provient de

$$-\frac{\partial_s \zeta_{\mathbb{Q}}(s)}{\zeta_{\mathbb{Q}}(s)} = \sum_{n=1}^{\infty} \Lambda(n) n^{-s} + \int_1^{\infty} \kappa(u) u^{-s} d^* u ,$$

où $\Lambda(n)$ est la fonction de von-Mangoldt.