Le logarithme $1\frac{1}{2}$

(Appendice de l'article "On poly(ana)logs i" de P. Elbaz-Vincent et H. Gangl)

Maxim Kontsevich

Cet appendice à l'article de Elbaz-Vincent et Gangl est inclus pour fournir des éléments d'Histoire des mathématiques. Il reproduit un texte de 1995, initialement écrit pour le livret privé "Hommage à Friedrich Hirzebruch".

Soit $p > 2$ un nombre premier. Définissons une application de $\mathbb{Z}/p\mathbb{Z}$ dans lui-même par la formule

$$H_p(x) = \sum_{k=1}^{p-1} \frac{x^k}{k} = x + \frac{x^2}{2} + \cdots + \frac{x^{p-1}}{p-1} \pmod{p}.$$

Cette fonction apparaît dans les formules explicites pour les extensions abéliennes de corps cyclotomiques.

Elle ressemble à une version tronquée de $\log(\frac{1}{1-x})$. Bien sûr, ça ne pourrait pas être un logarithme parce qu'il n'y a pas d'homomorphisme non nul de $(\mathbb{Z}/p\mathbb{Z})^\times \simeq \mathbb{Z}/(p-1)\mathbb{Z}$ vers $\mathbb{Z}/p\mathbb{Z}$.

Je prétends que H_p est analogue à une autre fonction bien connue d'une variable réelle. Je déduirai cette analogie en écrivant plusieurs équations fonctionnelles pour H_p. Ces équations seront indépendantes de p et je supprimerai l'indice p des notations.

(A) : $$H(1-x) = H(x).$$

Preuve : on peut calculer explicitement les coefficients du polynôme $H(1-x)$.

Tout d'abord, son zéro-ième coefficient est $H(1) = 1 + \frac{1}{2} + \ldots \frac{1}{p-1} = 1 + 2 + \cdots + (p-1) = \frac{p(p-1)}{2} = 0 \pmod{p}$.

Pour l compris entre 1 et $p-1$, le l-ième coefficient de $H(1-x)$ est égal à

$$\begin{aligned}\sum_{k=1}^{p-1} \frac{1}{k} (-1)^l \frac{k(k-1)\ldots(k-l+1)}{l!} &= \frac{(-1)^l}{l!} \sum_{k=1}^{p-1} (k-1)\ldots(k-l+1) \\ &= -\frac{(-1)^l}{l!}(0-1)(0-2)\ldots(0-l+1) = \frac{(l-1)!}{l!} = \frac{1}{l}.\end{aligned}$$

On utilise ici le fait standard que

$$\sum_{k=0}^{p-1} P(k) = 0$$

Appendice de la référence : https://arxiv.org/pdf/math/0008089 , 2000.
Traduction : Denise Vella-Chemla, 26 février 2025.

pour tout polynôme $P \in \mathbb{Z}/p\mathbb{Z}[x]$ de degré au plus $p-2$. □

Une généralisation simple de l'argument précédent montre que

$$\text{(B)} : \qquad H(x+y) = H(y) + (1-y)\, H\left(\frac{x}{1-y}\right) + y\, H\left(-\frac{x}{y}\right) \text{ pour } y \neq 0,\, 1.$$

Il y a également une identité élémentaire

$$\text{(C)} : \qquad x\, H\left(\frac{1}{x}\right) = -H(x) \text{ pour } x \neq 0$$

Assertion : il y a seulement une solution continue non nulle (à un facteur scalaire près) des équations (A), (B), (C) en fonctions de $\mathbb{R}$ dans lui-même. C'est

$$H_\infty(x) = -\left(x\ \log|x| + (1-x)\ \log|1-x|\right) .$$

La fonction H_p est également l'unique solution (à un facteur scalaire près) en applications de $\mathbb{Z}/p\mathbb{Z}$ dans lui-même.

Interprétation cohomologique des équations fonctionnelles. Soit F un corps et supposons que $H : F \to F$ satisfasse (A) et (B). L'équation (C) sera non pertinente.

On associe à H une fonction homogène $\phi : F \times F \to F$ de degré 1:

$$\phi(x,y) := \begin{cases} (x+y)\, H\left(\dfrac{x}{x+y}\right) & \text{si} \quad x+y \neq 0\,, \\ 0 & \text{si} \quad x+y = 0\,. \end{cases}$$

L'équation (A) implique que $\phi(x,y) = \phi(y,x)$. L'équation (B) est équivalente à l'identité

$$\phi(x,y) - \phi(x,y+z) + \phi(x+y,z) - \phi(y,z) = 0\,.$$

Par conséquent, ϕ est un 2-cocycle du groupe abélien F (le groupe additif du corps) avec des coefficients dans lui-même comme module trivial. Parce que ce cocycle est invariant selon l'action habituelle du groupe multiplicatif $F^\times$ (agissant à la fois sur le groupe et sur les coefficients), on obtient un 2-cocycle du groupe des transformations affines de la droite sur F

$$\mathrm{Aff}(1,F) = \{t \mapsto at+b \mid a \in K^\times, b \in K\}$$

avec des coefficients dans la représentation 1-dimensionnelle non triviale donnée par le premier coefficient.

Ce 2-cocycle définit une extension de $\mathrm{Aff}(1,F)$ par F. Le groupe résultant G peut être identifié à un ensemble avec $F \times F \times F^\times$.

Maintenant considérons le cas de $F = \mathbb{R}$ et supposons que H est une application mesurable.

Il y a des classes de cohomologie mesurables non triviales dans $H^2(\mathbb{R},\mathbb{R})$, par conséquent, ϕ devrait être une cofrontière. Cela signifie qu'il existe une fonction $\psi : \mathbb{R} \to \mathbb{R}$ telle que

$$\phi(x,y) = \psi(x) + \psi(y) - \psi(x+y)\,.$$

L'homogénéité de ϕ implique que pour tout $\lambda \neq 0$, la fonction $\psi_\lambda(x) := \psi(\lambda x) - \lambda\psi(x)$ est additive dans x. Si l'on a affaire qu'à des applications mesurables alors ψ_λ est une fonction linéaire.

De cela, on peut facilement déduire que

$$\psi(x)/x = a\,\log|x| + b$$

pour certains $a, b \in \mathbb{R}$. Ainsi on obtient la solution des équations fonctionnelles pour $F = \mathbb{R}$.

Maintenant voyons le cas $F = \mathbb{Z}/p\mathbb{Z}$. Si la classe de cohomologie dans $H^2(F,F) \simeq \mathbb{Z}/p\mathbb{Z}$ correspondant à H est nulle, alors par des arguments similaires aux arguments précédents, on obtient un homomorphisme de $(\mathbb{Z}/p\mathbb{Z})^\times$ dans $\mathbb{Z}/p\mathbb{Z}$. Cet homomorphisme (un "logarithme") s'évanouit inévitablement, fournissant ainsi l'unicité de H à un facteur scalaire près.

Le groupe G dans le cas où $F = \mathbb{R}$ est un groupe de Lie résoluble 3-dimensionnel. L'algèbre de Lie de G est définie sur $\mathbb{Z}$ et elle a une base x, y, z dans laquelle les relations de commutation sont

$$[x,y] = y,\ \ [x,z] = y + z,\ \ [y,z] = 0.$$

Cette algèbre de Lie ne peut pas être l'algèbre de Lie de n'importe quel groupe sur $\mathbb{Z}$ ou sur $\mathbb{Q}$.

Néanmoins, nous avons défini des groupes de points sur $\mathbb{R}$ et sur $\mathbb{Z}/p\mathbb{Z}$ pour tous les nombres premiers impairs p.

Entropie. La fonction H est l'entropie d'une variable aléatoire prenant deux valeurs. Plus généralement, si ξ prend un nombre fini de valeurs avec les probabilités $p_1, \dots, p_k$, $\sum p_i = 1$ alors l'entropie de ξ est définie comme

$$H(\xi) := -\sum_{i=1}^{k} p_i\ \log(p_i)\,.$$

On considèrera l'entropie également comme une fonction de la collection de probabilités des événements élémentaires, $H(\xi) = H(p_*)$. La principale propriété de l'entropie est que si une variable aléatoire (disons ξ) est une fonction d'une autre variable aléatoire (disons η) alors l'entropie de η peut être calculée comme suit. Dénotons les probabilités de toutes les valeurs possibles de η par $p_{1,1}, p_{1,2}, \dots, p_{1,l_1}; p_{2,1}, \cdots : \dots p_{k,l_k}$ de telle façon que $p_{1,1} + p_{1,2} + \cdots + p_{1,l_1} = p_1$ etc.

Alors on a k distributions de probabilités conditionnelles $p_{i,*}/p_i$ pour chaque $i \leq k$. La principale identité des entropies est

$$H(p_{*,*}) = H(p_*) + \sum_{i=1}^{k} p_i H(\frac{p_{i,*}}{p_i})\,, \quad H(\eta) = H(\xi) + H_\xi(\eta)\,.$$

Le dernier terme dans la formule ci-dessus est la valeur moyenne des entropies de η avec des valeurs données de ξ et on l'appelle l'entropie relative.

En utilisant l'identité principale, on peut réduire par induction le calcul de l'entropie de n'importe quelle variable aléatoire au cas d'une variable à deux valeurs, i.e. notre fonction $H(x)$. On peut facilement vérifier que l'entropie des variables aléatoires calculées en utilisant $H(x)$ est bien définie si et seulement si les équations fonctionnelles (A) et (B) sont satisfaites.

Conclusion : Si on a une variable aléatoire ξ qui prend un nombre fini de valeurs avec toutes les probabilités dans $\mathbb{Q}$, alors on peut définir non seulement le nombre transcendant $H(\xi)$ mais également ses "restes modulo p" pour presque tous les nombres premiers p !

Je propose d'appeler les fonctions H_p des "logarithmes $1\frac{1}{2}$," parce que leur équation fonctionnelle contient 4 termes, et 4 est compris entre 3 (le logarithme) et 5 (le dilogarithme fournissant un élément dans $H^3(Sl(2,\mathbb{C}),\mathbb{R})$).

La question naturelle est de trouver des équations fonctionnelles pour l'application $x \mapsto \sum_{k=1}^{p-1} x^k/k^2$ de $\mathbb{Z}/p\mathbb{Z}$ dans lui-même. Je ne sais pas comment faire cela.