Sur le corps à un élément
(exposé donné à l'Arbeitstagung[1], Bonn, juin 1999)

Christophe Soulé

Cnrs et Ihés

1. Soit G un schéma en groupes de Chevalley sur $\mathbb{Z}$, et $\mathbb{F}_q$ le corps fini à q éléments. Il a été remarqué depuis quelques temps que, lorsque q tend vers 1, la cardinalité du groupe de points de G dans $\mathbb{F}_q$ se comporte comme suit :

$$\text{card } \mathrm{G}(\mathbb{F}_q) \underset{q\to 1}{\sim} (q-1)^r \times \text{card } \mathrm{W},$$

où r est le rang de G et W est son groupe de Weyl. En 1957, Tits [1] a proposé de penser à W comme au groupe de points of G dans “le corps de caractéristique un” :

$$\mathrm{G}(\mathbb{F}_1) := \mathrm{W}. \tag{1}$$

Il a aussi argumenté sur le fait que les géométries finies attachées à chaque groupe G ont une limite quand q tend vers 1, notamment la géométrie finie attachée au groupe de Coxeter W.

En 1993, Manin [2] a écrit quelques exposés au sujet des fonctions zeta dans lesquels il mentionne le corps à un élément. Il propose de développer la géométrie algébrique sur $\mathbb{F}_1$, et il prédit que les variétés sur ce corps ont des fonctions zeta simples. Par exemple

$$\zeta_{\mathrm{P}^N_{\mathbb{F}_1}}(s) = s(s-1)(s-2)\ldots(s-N). \tag{2}$$

Il note également que l'équation (1) pour $\mathrm{G} = \mathrm{SL}_N$ amène au fait que la K-théorie la plus haute de $\mathbb{F}_1$ doit être l'homotopie des groupes de sphères. En effet, par le théorème de Barratt-Priddy-Quillen, on obtient

$$\mathrm{K}_m(\mathbb{F}_1) = \pi_m \mathrm{BGL}(\mathbb{F}_1)^+ := \pi_m B \textstyle\sum_\infty^+ = \pi_m^s. \tag{3}$$

Plus tard, Smirnov et Kapranov-Smirnov (preprints non publiés) ont étudié la question plus avant. Entre autres choses, ils ont développé l'algèbre linéaire sur $\mathbb{F}_1$ (un espace vectoriel étant un ensemble fini pointé), et ont obtenu de cette manière une description de la loi de réciprocité de Gauss similaire à la description donnée plus tôt par Arbarello, De Concini et Kac de la loi de réciprocité de Weil sur les courbes au moyen des déterminants des espaces vectoriels.

2. L'analogie entre les corps de nombres et les corps de fonctions trouve une limitation de base avec le manque d'un corps de base. On dit que Spec($\mathbb{Z}$) (avec un point ajouté à l'infini, comme c'est l'habitude en théorie d'Arakelov) est comme une courbe (complète) ; mais sur quel corps ? En particulier, on devrait rêver d'avoir un objet comme

$$\mathrm{Spec}(\mathbb{Z}) \times_{\mathrm{Spec}(\mathbb{F}_1)} \mathrm{Spec}(\mathbb{Z}),$$

[1] L'Arbeitstagung est une rencontre État de l'art de mathématiciens de haut niveau ayant lieu à Bonn, annuellement depuis 1957, et fondée par Hirzebruch.

Article : IHES/M/99/55, Scan-9911017 des bibliothèques du CERN à Genève.

Traduction : Denise Vella-Chemla, juillet 2023.

puisque la preuve de Weil de l'hypothèse de Riemann pour une courbe sur un corps fini utilise le produit de deux copies de cette courbe. Je n'ai rien à dire sur cette question. Le fait simple que la fonction zeta de Riemann ait une infinité de zéros indique que $\mathrm{Spec}(\mathbb{Z})$ ne peut être regardé comme un objet de type fini sur $\mathbb{F}_1$, par conséquent $\mathrm{Spec}(\mathbb{Z}) \times_{\mathrm{Spec}(\mathbb{F}1)} \mathrm{Spec}(\mathbb{Z})$ ne peut être une honnête variété algébrique sur $\mathbb{Z}$.

D'un autre côté, si X est une variété de type fini sur $\mathbb{F}_1$, son changement de base $X_{\mathbb{Z}} = X \otimes_{\mathbb{F}_1} \mathbb{Z}$ vers $\mathbb{Z}$ doit être une variété de type fini sur $\mathbb{Z}$. Il y a donc un espoir de décrire de tels objets X en utilisant la géométrie algébrique habituelle, et on peut se poser la :

Question : Quelles variétés sur $\mathbb{Z}$ sont obtenues par changement de base de $\mathbb{F}_1$ à $\mathbb{Z}$?

Par exemple, quand X est lisse sur $\mathbb{F}_1$, $X_{\mathbb{Z}}$ sera lisse sur $\mathbb{Z}$, ce qui est déjà une contrainte forte.

3. Notre point de départ pour une tentative de définition des variétés sur $\mathbb{F}_1$ est la définition courte des schémas qui dit qu'un schéma est un foncteur covariant des anneaux vers les ensembles qui est localement représentable par un anneau. Dans ce langage, le changement de base d'un corps k vers une k-algèbre Λ est décrite par le lemme facile suivant. Étant donnée une variété X sur k (resp. une k-algèbre A), soit $X_\Lambda = X \otimes_k \Lambda$ (resp. $A_\Lambda = A \otimes_k A$).

Lemme 1 :

i) Il y a une inclusion canonique $X(A) \subset X_\Lambda(A_\Lambda)$.

ii) Étant donnée une variété S sur Λ et n'importe quelle transformation naturelle de foncteurs (des k-algèbres vers les ensembles)

$$\phi \ : \ (A \mapsto X(A)) \longrightarrow (A \mapsto S(A_\Lambda))$$

il existe un unique morphisme canonique

$$\widetilde{\phi} : X_\Lambda \mapsto S$$

induisant ϕ sur chaque ensemble $X(A)$.

Nous aimerions avoir une situation similaire avec $k = \mathbb{F}_1$ et $\Lambda = \mathbb{Z}$. Mais personne ne nous dit quelles sont les Λ-algèbres provenant de k.

4. Une définition

4.1. Pour tout entier $n \geq 1$, un corps fini $\mathbb{F}_q$ a une extension finie $\mathbb{F}_{q^n}$ de degré n, obtenue en adjoignant les racines de l'unité. Comme Kapranov et Smirnov le suggèrent, $\mathbb{F}_1$ devrait avoir une extension $\mathbb{F}_{1^n}$ de degré n, et on décide que

$$\mathbb{F}_{1^n} \otimes_{\mathbb{F}_1} \mathbb{Z} = \mathbb{Z}[T]/(T^n - 1).$$

En d'autres termes, $\mathbb{F}_{1^n} \otimes_{\mathbb{F}_1} \mathbb{Z}$ est l'anneau R_n de fonctions sur le schéma de groupe affine des n-ièmes racines de l'unité.

Soit $\mathcal{R}$ la sous-catégorie pleine de Anneaux avec comme objets les anneaux $R_n, n \geq 1$, et leurs produits tensoriels finis. Soit également $\mathcal{R}'$ la catégorie pleine de Anneaux contenant comme objets les produits tensoriels des anneaux dans $\mathcal{R}$ avec les anneaux $\mathbb{Z}[1/N], N \geq 1$.

Définition : Une *variété sur* $\mathbb{F}_1$ est un foncteur covariant X de $\mathcal{R}$ vers les ensembles finis, équipé des inclusions naturelles $X(R) \subset X_{\mathbb{Z}}(R), R \in \mathrm{Ob}\mathcal{R}$, où $X_{\mathbb{Z}}$ est une variété sur $\mathbb{Z}$, et tel que la propriété suivante (U) est vérifiée : pour toute variété S sur $\mathbb{Z}$ et n'importe quelle "bonne" transformation de foncteurs (de $\mathcal{R}$ vers les ensembles)

$$\phi \ : \ (R \mapsto X(R)) \longrightarrow (R \mapsto S(R))$$

il existe un unique groupe algébrique

$$\widetilde{\phi} : X_{\mathbb{Z}} \mapsto S$$

induisant sur chaque ensemble $X(R), R \in \mathrm{Ob}\mathcal{R}$.

4.2. Voici trois possibilités de ce que "bon" pourrait vouloir dire dans la définition précédente :

(G0) Soit $X(\mathbb{C})$ l'union des sous-ensembles $\sigma(X(R)) \subset X_{\mathbb{Z}}(\mathbb{C})$, où R parcourt tous les anneaux dans $\mathcal{R}$ et σ parcourt tous les morphismes de R vers $\mathbb{C}$. Il y a une application continue $\phi_{\mathbb{C}}$ de la fermeture topologique de $X(\mathbb{C})$ (dans $X_{\mathbb{Z}}(\mathbb{C})$) vers $S(\mathbb{C})$ telle que, pour tout R et σ comme ci-dessus,

$$\sigma \circ \phi = \phi_{\mathbb{C}} \circ \sigma$$

(G1) Même définition que (G0), mais maintenant $\phi_{\mathbb{C}}$ est holomorphe sur la fermeture holomorphe de $X(\mathbb{C})$ dans $X_{\mathbb{Z}}(\mathbb{C})$.

(G2) Le foncteur X s'étend à un foncteur de $\mathcal{R}'$ vers les ensembles, et ϕ s'étend à une transformation des foncteurs sur $\mathcal{R}'$. Alors (G0) est vérifiée, et, de plus, la même assertion est vraie quand $\mathbb{C}$ (resp. $\mathcal{R}$) est remplacé par n'importe quelle extension finie d'un corps p-adique (resp. par $\mathcal{R}'$).

5. Exemples

5.0. Quand $X_{\mathbb{Z}} = \mathrm{Spec}(\mathbb{Z})$ et $X(R) = X_{\mathbb{Z}}(R)$, on dit que $X = \mathrm{Spec}(\mathbb{F}_1)$.

5.1. Quand $X_{\mathbb{Z}}(R) = R^*$ et $X(R)$ est l'ensemble $\mu(R)$ des racines de l'unité dans R, on dit que $X = \mathrm{G}_m/\mathbb{F}_1$.

Lemme 2 : La propriété (U) est vérifiée quand S est affine et satisfait (G0).

Esquisse de la démonstration : On prouve l'existence de $\widetilde{\phi}$ quand S est la droite affine (regarder les coordonnées réduit la preuve à ce cas). Pour tout $n \geq 1$, l'application ϕ envoie l'élément $T \in \mu(R_n)$ vers un polynôme $\sum_{i=0}^{n-1} a_i(n)T^i$ dans R_n. D'un autre côté, la fermeture topologique de $X(\mathbb{C})$ est le cercle S^1. L'application continue $\phi_{\mathbb{C}}$ du cercle vers $\mathbb{C}$ peut être écrite comme une série de Laurent

$$\phi_{\mathbb{C}}(z) = \sum_{-\infty}^{+\infty} \alpha_i z^i.$$

Lorsque n tend vers l'infini, le coefficient

$$a_i(n) = \sum_{\zeta^n=1} \phi_{\mathbb{C}}(\zeta)\zeta^{-i}/n$$

tend vers

$$\alpha_i = \int_{S^1} \phi_{\mathbb{C}}(z)z^{-i}d\theta.$$

Puisque tous les $a_i(n)$ sont entiers, la séquence $a_i(n), n \geq 1$, doit être stationnaire, par conséquent, $\phi_{\mathbb{C}}$ est un polynôme de Laurent $\widetilde{\phi} \in \mathbb{Z}[T, T^{-1}] = Hom(\mathrm{G}_m, A_1)$.

5.2. Quand, pour tout $R \in \mathcal{R}, X_{\mathbb{Z}}(R) = R$ et $X(R)$ est l'ensemble $\mu(R) \cup \{0\}$, on dit que $X = A_1/\mathbb{F}_1$. Quand $R \in \mathrm{Ob}(\mathcal{R}')$, si $\sum = Hom(R, \mathbb{C})$ a pour cardinalité N, on dénote par $X(R)$ l'ensemble des éléments $x \in R$ tels que

$$\sum_{\sigma \in \sum} |\sigma(x)|^2 \leq \ N.$$

La propriété (U) est vérifiée si S est affine et satisfait (G1) ou (G2).

5.3. Plus généralement, si $X_{\mathbb{Z}}$ est une variété torique lisse sur $\mathbb{Z}$, on peut l'écrire comme une union disjointe de produits de copies de A_1 avec des copies de G_m. En imposant que les coordonnées correspondantes soient dans $\mu(R) \cup \{0\}$, on obtient un sous-ensemble $X(R) \subset X_{\mathbb{Z}}(R)$, qui satisfait (U) quand S est affine et ϕ satisfait (G1) ou (G2).

5.4. Soit $E \simeq \mathbb{Z}^N$ un réseau équipé d'un produit scalaire hermitien h sur $E \otimes \mathbb{C}$, et $\|\cdot\|$ la norme correspondante. Il est habituel en théorie d'Arakelov de voir la paire $\overline{E} = (E, h)$ comme un fibré[2] sur la courbe $\mathrm{Spec}(\mathbb{Z}) \cup \{\infty\}$, dont les sections globales sont les éléments de E de norme inférieure à un.

Si on définit $X(R)$ comme l'ensemble des éléments $x \in E \otimes R$ tels que

$$\sum_{\sigma \in \sum} \|\sigma(x)\|^2 \leq N,$$

on peut à nouveau montrer que la propriété (U) est vérifiée (pour une certaine variété $X_{\mathbb{Z}}$) si S est affine et si ϕ satisfait (G1) ou (G2).

5.5. Quand $X_{\mathbb{Z}} = \mathrm{G}$ est un groupe de Chevalley comme dans le §1, il semble naturel de définir $X(R)$ comme l'ensemble des éléments $g \in \mathrm{G}(R)$ qui sont envoyés vers le sous-groupe compact standard maximal de $\mathrm{G}(\mathbb{C})$ par tous les $\sigma \in \sum$. Le groupe $\mathrm{G}(\mathbb{F}_1)$ sera alors une extension de W par un 2-groupe élémentaire fini abélien. Je n'ai pas vérifié si la propriété (U) était satisfaite.

[2] bundle ?

6. Fonction zeta

Soit X une variété sur $\mathbb{F}_1$. Pour tout $n \geq 1$, soit $q = 2n + 1$, et

$$N(q) := \text{card } X(R_n).$$

Dans tous les cas considérés dans le §5, $N(q)$ s'avère être un polynôme en q à coefficients entiers (c'est facile à montrer, mais assez surprenant dans le cas 5.4). On peut alors définir

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

En remplaçant T par q^{-s} et en laissant tendre q vers 1, on obtient

$$\mathbb{Z}(q, q^{-s}) \underset{q\to 1}{\sim} (q-1)^{\chi}\zeta_X(s),$$

où χ est la caractéristique d'Euler-Poincaré de $X_{\mathbb{Z}}(\mathbb{C})$ et

$$\zeta_X(s) = \mathrm{P}(s)/\mathrm{Q}(s),$$

où P et Q sont des polynômes avec à la fois des coefficients et des racines entières.

Par exemple, quand $X = \mathrm{P}^N_{\mathbb{F}_1}$ (défini comme dans 5.3, i.e. $X(R)$ est constitué des points dans $\mathrm{P}^N(R)$ ayant des coordonnées homogènes dans $\mu(R) \cup \{0\}$), la formule (2) est vérifiée.

7. Motifs

7.1. Soit T un tore séparé[3] sur $\mathbb{C}$, M une variété T-torique, et $r > 1$ un entier. L'endomorphisme qui envoie $t \in T$ sur sa r-ième puissance s'étend à un endomorphisme Φ_r, sur M. Totaro a noté dans un article récent [3] que le sous-espace de la cohomologie rationnelle de M où Φ_r agissant par multiplication par r^i fournit une séparation canonique de la filtration poids (de degré i).

En termes de motifs mélangés (encore une notion conjecturale), M donne naissance à des extensions (plusieurs) de motifs de Tate à cause de la stratification mentionnée au §5.3), et leurs classes $e \in \mathrm{Ext}(\mathbb{Z}(i), \mathbb{Z}(i+n))$ sont éliminées par le plus grand commun diviseur de $r^{i+n} - r^i > 1$, i.e. (essentiellement) le dénominateur de B_n/n, où B_n est le n-ième nombre de Bernoulli.

7.2. D'un autre côté, Beilinson propose la formule

$$K_{2n-1}(\mathbb{Z}) = \mathrm{Ext}_{\mathcal{M}/Z}(\mathbb{Z}, \mathbb{Z}(n))$$

décrivant la K-théorie de $\mathbb{Z}$ comme des extensions de motifs de Tate sur Spec($\mathbb{Z}$). À cause de (3), on pourrait spéculer que

$$\pi^s_{2n-1} = \mathrm{Ext}_{\mathcal{M}/\mathbb{F}_1}(\mathbb{Z}, \mathbb{Z}(n)).$$

[3] split ?

Si la variété torique M est définie et lisse sur $\mathbb{Z}$, l'exemple du §5.3 indique que les classes d'extension e ci-dessus devraient vivre dans l'image du morphisme $\pi^s_{2n-1} \to K_{2n-1}(\mathbb{Z})$. C'est un théorème de Quillen et Mitchell que cette image est (à 2-torsion près) le groupe cyclique $\mathrm{Im}(J)_{2n-1}$, dont l'ordre est le dénominateur de B_n/n. Ceci est assez consistant avec la remarque de Totaro.

Il serait intéressant de vérifier si cette borne sur e est pointue, i.e. si tous les éléments dans $\mathrm{Im}(J)_{2n-1}$ peuvent être interprétés en termes de variétés toriques.

Références

[1] Tits, J. : *Sur les analogues algébriques des groupes semi-simples complexes.* Colloque d'algèbre supérieure, Bruxelles, 1956, pp. 261-289. Centre Belge de Recherches Mathématiques. Gauthier-Villars, (1957).

[2] Manin, Y. : *Lectures on zeta functions and motives (according to Deninger and Kurokawa).* Columbia University Number Theory Seminar (New York, 1992). Astérisque no. 228 (1995), 4, 121-163.

[3] Totaro, B. : *Chow groups, Chow cohomology, and linear varieties*, preprint (1998).

IHES
35 route de Chartres 91440 Bures/s/Yvette
France