Quelques identités combinatoires en faveur de l'existence du corps à un élément

Xavier Caruso

Mai 2006

Résumé

Dans cette note, on présente une version modifiée des entiers (qui dépend d'un paramètre q) qui amène à définir par analogie certaines quantités combinatoires moins usuelles. On montre toutefois que ces nombres apparaissent naturellement dans certaines formules (et notamment la formule du binôme) et qu'ils sont également reliés de très près à des problèmes de dénombrement. L'existence de ces entiers modifiés et la similarité de certaines formules avec les formules usuelles de combinatoire amènent à penser qu'il doit exister « un corps à un élément » (qui n'est pas l'anneau nul !) et une géométrie sur celui-ci.

Mots-clés : formule du binôme, corps finis, grassmaniennes, hypothèse de Riemann.

Table des matières

Tout au long de cet article, nous fixons q un nombre réel[1] et pour tout entier n, nous considérons le *q-entier* $[n]_q$ défini par la formule suivante :

$$[n]_q = 1 + q + q^2 + \cdots + q^{n-1} = \frac{q^n - 1}{q - 1}$$

la dernière égalité n'étant valable que pour $q \neq 1$. Lorsque $q = 1$, on retrouve les entiers usuels. À partir de la définition précédente, on introduit la notion de *q-factorielle* et de *q-coefficients binômiaux* (ou plus simplement *q-binômiaux*) en posant :

$$[n]_q! = [1]_q \cdot [2]_q \cdots [n-1]_q \cdot [n]_q$$

et :

$$\left[\begin{array}{c} n \\ k \end{array} \right]_q = \frac{[n]_q!}{[k]_q! \cdot [n-k]_q!}.$$

[1]Nous imposons à q d'être réel simplement pour fixer les idées. En réalité, dans la partie purement algébrique de l'article, il peut être n'importe quel élément d'un anneau commutatif, alors que pour la partie combinatoire, on sera contraint de supposer qu'il est une puissance d'un nombre premier.

Dans la première partie de ce texte, nous expliquons pourquoi ces nombres sont la généralisation naturelle des coefficients binômiaux usuels, en montrant qu'ils apparaissent dans une formule du binôme du Newton valable dans un cadre non commutatif.

Dans la seconde partie, nous nous attardons sur d'autres propriétés plus combinatoires de ces nombres. Nous sommes amenés pour cela à nous restreindre au cas où q est une puissance d'un nombre premier p et à considérer des espaces vectoriels sur le corps fini à q éléments $\mathbb{F}_q$. Précisément, nous montrons que les q-binômiaux (et plus généralement les q-multinômiaux) correspondent aux cardinaux de certains « espaces de drapeaux ».

1 Avant-propos algébrique

Avant de se lancer dans la formule du binôme, on remarque que les q-binômiaux vérifient des relations semblables à celles valables pour les coefficients binômiaux usuels. Par exemple, comme le lecteur le vérifiera facilement, on a :

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \begin{bmatrix} n \\ n-k \end{bmatrix}_q \tag{1}$$

et la relation de récurrence fondamentale :

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \begin{bmatrix} n-1 \\ k \end{bmatrix}_q + q^{n-k} \begin{bmatrix} n-1 \\ k-1 \end{bmatrix}_q = q^k \begin{bmatrix} n-1 \\ k \end{bmatrix}_q + \begin{bmatrix} n-1 \\ k-1 \end{bmatrix}_q. \tag{2}$$

Voici la proposition qui généralise la formule du binôme de Newton à une situation non commutative :

Proposition 1. *Soient A une $\mathbb{R}$-algèbre*[2]*, et x et y deux éléments de A qui vérifient la relation de commutation $yx = qxy$. Alors, pour tout entier $n \geqslant 0$, on a la formule :*

$$(x+y)^n = \sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix}_q x^k y^{n-k}.$$

La preuve de cet énoncé se fait par récurrence et est très facile à partir de la relation (2) ; nous laissons donc le lecteur la mener à bien lui-même. De même, il est aisé d'en déduire une formule plus générale, dite du multinôme, donnée par la proposition suivante :

Proposition 2. *Soient A une $\mathbb{R}$-algèbre, et $x_1, \ldots, x_s$ des éléments de A tels que $x_j x_i = q x_i x_j$ pour des indices $i < j$. Alors, pour tout entier $n \geqslant 0$, on a :*

$$(x_1 + \cdots + x_s)^n = \sum_{d_1+\ldots+d_s=n} \frac{[n]_q!}{[d_1]_q! \cdot [d_2]_q! \cdots [d_s]_q!} x_1^{d_1} x_2^{d_2} \cdots x_s^{d_s}.$$

Le facteur $\frac{[n]_q!}{[d_1]_q! \cdot [d_2]_q! \cdots [d_s]_q!}$ est un *q-multinômial* et sera noté par la suite plus simplement $M_q(d_1, \ldots, d_s)$. (Notez que les d_i déterminent n par la relation $n = d_1 + \cdots + d_s$.)

2 Grassmaniennes et variétés de drapeaux

On cherche désormais à obtenir une interprétation plus combinatoire des q-binômiaux (et éventuellement aussi des q-multinômiaux) : ces coefficients dénombrent-ils certains espaces naturels ? Pour obtenir une réponse positive à cette question, on suppose que q est une puissance d'un nombre premier p. On rappelle alors l'existence d'un corps fini (unique à isomorphisme – non unique – près) à q éléments que l'on désigne généralement par le symbole $\mathbb{F}_q$. Il n'est pas nécessaire pour la suite de l'exposé de connaître des propriétés fines de ce corps ; nous allons nous borner à considérer des espaces vectoriels sur $\mathbb{F}_q$, et la théorie (existence de bases, matrices, *etc.*) est alors en tout point semblable à celle des espaces vectoriels réels (ou complexes).

[2]Nous considérons une algèbre sur le corps des nombres réels car nous avons choisi de prendre pour q un nombre réel. Si q avait été choisi dans un anneau de base (commutatif) R, on aurait dû considérer pour A une R-algèbre.

2.1 Le cas des q-binômiaux

Un premier décompte crucial est celui du cardinal de l'ensemble des matrices inversibles de taille $n \times n$ à coefficients dans $\mathbb{F}_q$, c'est-à-dire du groupe $\mathrm{GL}_n(\mathbb{F}_q)$. S'en donner un élément revient à se donner une base, ou encore une famille libre de cardinal n, de l'espace vectoriel $\mathbb{F}_q^n$. Pour calculer le nombre de telles familles libres, on estime le nombre de choix que l'on a successivement pour chaque vecteur : le premier vecteur peut être n'importe quel vecteur non nul de l'espace, il y a donc $(q^n - 1)$ choix ; le second vecteur, quant à lui, ne doit pas appartenir à la droite engendrée par le premier, ceci ne laisse que $(q^n - q)$ possibilités ; de même le troisième vecteur ne doit pas être dans le plan engendré par les deux premiers, ce qui amène à un total de $(q^n - q^2)$; et ainsi de suite. Au final, le cardinal de $\mathrm{GL}_n(\mathbb{F}_q)$ est donné par la formule :

$$(q^n - 1)(q^n - q)(q^n - q^2) \cdots (q^n - q^{n-1}) = q^{n(n-1)/2}(q-1)^n \cdot [n]_q!$$

et l'on observe déjà l'apparition d'un q-entier.

Exercice. Montrer que $n!$ divise $(q^n - 1)(q^n - q)(q^n - q^2) \cdots (q^n - q^{n-1})$. Le résultat reste-t-il valable lorsque q n'est pas une puissance d'un nombre premier ?

Proposition 3. *Soient $k \leqslant n$ des entiers positifs ou nuls. Le nombre de sous-espaces vectoriels de $\mathbb{F}_q^n$ de dimension k est $\left[\begin{array}{c} n \\ k \end{array} \right]_q$.*

Plusieurs remarques s'imposent avant même de donner la preuve de ce résultat. Tout d'abord, comme cela sera détaillé dans la section 3, il faut mettre en parallèle l'énoncé précédent avec le fait que $\binom{n}{k}$ dénombre les parties à k éléments de l'ensemble $\{1, \ldots, n\}$. Ensuite, une question de terminologie : l'espace des sous-espaces vectoriels de $\mathbb{F}_q^n$ de dimension k est couramment appelé une *grassmanienne* et noté $\mathrm{Gr}_{n,k}(\mathbb{F}_q)$. Ceux qui connaissent noteront que, lorsque $k = 1$, la grassmanienne s'identifie à l'espace projectif de dimension $n - 1$.

Démonstration. Un sous-espace de dimension k de $\mathbb{F}_q^n$ est certainement déterminé par une de ses bases. Celles-ci sont les familles libres de k vecteurs de $\mathbb{F}_q^n$. En reprenant l'argument utilisé pour le calcul du cardinal de $\mathrm{GL}_n(\mathbb{F}_q)$, on prouve que l'ensemble de ces familles a pour cardinal :

$$(q^n - 1)(q^n - q)(q^n - q^2) \cdots (q^n - q^{k-1}) = q^{k(k-1)/2}(q-1)^k \cdot \frac{[n]_q!}{[n-k]_q!}.$$

Toutefois, deux familles fournissent le même sous-espace si les matrices obtenues en écrivant en colonne les vecteurs qui les constituent se déduisent l'une de l'autre par multiplication par un élément de $\mathrm{GL}_k(\mathbb{F}_q)$. Pour obtenir le cardinal de la grassmanienne $\mathrm{Gr}_{n,k}(\mathbb{F}_q)$, il faut donc diviser le nombre précédent par le cardinal de $\mathrm{GL}_k(\mathbb{F}_q)$, ce qui fournit le résultat annoncé. $\square$

2.2 Retour sur la formule du binôme

Dans le cas commutatif, il est possible et souvent jugé élégant de donner une démonstration combinatoire directe de la formule du binôme. On dit pour cela que lorsque l'on développe $(x+y)^n$, on doit choisir un x ou un y dans chacun des facteurs et, par suite, que le coefficient devant $x^k y^{n-k}$ correspond au nombre de façons de choisir k fois la lettre x et $n-k$ fois la lettre y, c'est-à-dire au nombre de parties à k éléments (les positions des facteurs dans lesquels on a choisi x) de $\{1, \ldots, n\}$, soit encore $\binom{n}{k}$.

On aimerait obtenir une démonstration de la proposition 1 fondée sur un argument de ce type : elle utiliserait uniquement le fait que le nombre $\left[\begin{array}{c} n \\ k \end{array} \right]_q$ compte les sous-espaces vectoriels de dimension k de $\mathbb{F}_q^n$. Pour cela, on reprend les notations et les hypothèses de la proposition 1. Tout d'abord, il est clair que, si l'on ne fait aucune simplification, le développement de $(x+y)^n$ donne la somme de tous les mots de n lettres écrits dans l'alphabet $\{x, y\}$. La relation de commutation $yx = qxy$ ne modifiant ni le nombre de x, ni le nombre de y, les mots parmi les précédents qui contribuent à un terme en $x^k y^{n-k}$ sont exactement ceux qui comportent k fois la lettre x et $n-k$ fois la lettre y. De plus, le coefficient qu'un tel mot apporte est q^N où N est le nombre de couples (i, j), avec $i < j$, pour lesquels la i-ième lettre est y et la j-ième x. La stratégie consiste à associer à un élément de $\mathrm{Gr}_{n,k}(\mathbb{F}_q)$ un mot de n lettres comportant k occurrences de x et $n-k$ de y, ceci étant fait de telle façon qu'il corresponde à un mot donné exactement q^N éléments de la grassmanienne (N étant défini comme précédemment).

Pour ce faire, on commence par fixer un drapeau complet de $\mathbb{F}_q^n$, c'est-à-dire une suite d'espaces vectoriels $0 = E_0 \subset E_1 \subset E_2 \subset \cdots \subset E_n = \mathbb{F}_q^n$ tels que $\dim E_i = i$ et $(e_1, \ldots, e_n)$ une base de $\mathbb{F}_q^n$ avec $e_i \in E_i$. Soit F un sous-espace vectoriel de $\mathbb{F}_q^n$ de dimension k. Pour tout $i \in \{0, 1, \ldots, n\}$, notons $F_i = F \cap E_i$. Les F_i forment une suite croissante de sous-espaces vectoriels de F telle que $F_0 = 0$, $F_n = F$ et $\dim F_{i+1} \leqslant \dim F_i + 1$. (La dernière inégalité se vérifie sans mal en écrivant la formule de Grassmann pour la dimension de F_i et celle de F_{i+1}.) Le mot associé à F est alors déterminé de la façon suivante : sa i-ième lettre est x si F_i est strictement plus grand que F_{i-1}, elle est y sinon. Un argument direct de dimension assure que le mot obtenu contient bien k fois la lettre x et $n-k$ fois la lettre y.

Reste à voir qu'étant donné un tel mot m, exactement q^N sous-espaces lui correspondent (où N désigne toujours le nombre de couples (i, j), avec $i < j$, pour lesquels la i-ième lettre de m est y et sa j-ième lettre x). Notons $i_1, \ldots, i_k$ les positions des occurrences (rangées par ordre croissant) de x dans m. Soit F un sous-espace correspondant au mot m. Les espaces $F_{i_1}, F_{i_2}, \ldots, F_{i_k}$ forment un drapeau complet de F. Ainsi il existe une base $(f_1, \ldots, f_k)$ de F avec $f_s \in F_{i_s}$. Écrivons ces vecteurs dans la base $(e_1, \ldots, e_n)$. Le premier a nécessairement une composante non nulle sur e_{i_1} (car sinon $F_{i_1 - 1}$ serait égal à F_{i_1} et il n'y aurait pas de x à la position i_1 dans le mot m). Quitte à le multiplier par une constante adéquate, on peut supposer que cette composante vaut exactement e_{i_1}. De $F_{i_1} \subset E_{i_1}$, on déduit aussi que f_1 n'a pas de composante sur les vecteur e_i avec $i > i_1$. Ainsi, f_1 est représenté par un vecteur ligne de la forme :

$$\begin{array}{cc} & e_1 \text{ —— } e_{i_1} \text{ —— } e_n \\ f_1 & \begin{pmatrix} \star \cdots \star & 1 & 0 \cdots 0 \end{pmatrix} \end{array}$$

En outre, avec la condition de normalisation, le vecteur f_1 est uniquement déterminé. Le même raisonnement vaut pour le vecteur f_2, pour lequel on peut également s'arranger, quitte à lui retrancher un multiple de f_1, pour qu'il n'ait pas de composante sur e_{i_1}. Avec ces contraintes, f_2 est uniquement déterminé. Visuellement, la famille (f_1, f_2) est représentée par une matrice de la forme :

$$\begin{array}{cc} & e_1 \text{ —— } e_{i_1} \text{ ——— } e_{i_2} \text{ —— } e_n \\ \begin{matrix} f_1 \\ f_2 \end{matrix} & \begin{pmatrix} \star \cdots \star & 1 & \multicolumn{3}{c}{0 \cdots\cdots\cdots\cdots 0} \\ \star \cdots \star & 0 & \star \cdots \star & 1 & 0 \cdots 0 \end{pmatrix} \end{array}$$

Réitérant le raisonnement pour les vecteurs f_i suivants, on conclut que la famille $(f_1, \ldots, f_d)$ est entièrement décrite par une unique matrice à k lignes et n colonnes comprenant des 1 aux entrées (s, i_s) $(1 \leqslant s \leqslant k)$ et des 0 à droite et en dessous des coefficients précédents. Les entrées non encore remplies de la matrice, que l'on appellera *entrées libres*, peuvent être renseignées par des coefficients quelconques.

Dès lors, il suffit de s'assurer que le nombre de ces entrées libres est exactement N. Cette dernière étape peut se traiter sans difficulté en examinant les définitions, mais il est sans doute plus intéressant de remarquer qu'elle se déduit directement de la relation $yx = qxy$. En effet, on est directement ramené à démontrer que si m est un mot de la forme $\ldots yx \ldots$ et si m' se déduit de m en remplaçant le yx par xy, alors la matrice associée à m' a une entrée libre de moins que celle associée à m. C'est une conséquence directe de la constatation suivante : si i indique la position du y de yx dans m, alors les entrées libres sur les colonnes j avec $j \neq i, i+1$ restent inchangées et celles des colonnes i et $i+1$ sont permutées à l'exception de l'une d'entre elles (celle qui est la plus haute) qui disparaît.

Remarque. De même, les relations (1) et (2) s'interprètent de façon combinatoire. Pour la première, il suffit de remarquer, qu'ayant fixé une forme bilinéaire non dégénérée sur $\mathbb{F}_q^n$, la fonction qui à un sous-espace associe son orthogonal réalise une bijection (involutive) entre $\mathrm{Gr}_{n,k}(\mathbb{F}_q)$ et $\mathrm{Gr}_{n,n-k}(\mathbb{F}_q)$. Pour (2), on commence par fixer H un hyperplan de $\mathbb{F}_q^n$. On sépare les sous-espaces de F_q^n de dimension k, on distingue deux catégories : ceux qui sont inclus dans H qui sont au nombre de $\begin{bmatrix} n-1 \\ k \end{bmatrix}_q$ et les autres qui sont au nombre de $q^{n-k}\begin{bmatrix} n-1 \\ k-1 \end{bmatrix}_q$ (en effet, se donner un tel espace revient à se donner son intersection avec H (qui est de dimension $k-1$) et un vecteur supplémentaire dont $n-k$ coordonnées ne sont pas fixées). La seconde inégalité se déduit en échangeant les rôles de k et $n-k$.

2.3 Le cas général des q-multinômiaux

Soit $(d_1, \dots, d_s)$ une partition de l'entier n, c'est-à-dire une suite d'entiers strictement positifs telle que $d_1 + \cdots + d_s = n$. Un *drapeau de type* $(d_1, \dots, d_s)$ de F_q^n est (dans cette note) une suite croissante d'espaces vectoriels $V_1 \subset V_2 \subset \cdots \subset V_s \subset \mathbb{F}_q^n$ avec $\dim V_t = d_1 + d_2 + \cdots + d_t$ pour tout $t \in \{1, \dots, s\}$. Les q-multinômiaux dénombrent ces ensembles de drapeaux. Précisément :

Proposition 4. *Soit $(d_1, \dots, d_s)$ une partition de l'entier n. Le nombre de drapeaux de type $(d_1, \dots, d_s)$ est donné par $M_q(d_1, \dots, d_s)$.*

Démonstration. Elle procède par récurrence sur s. Lorsque $s = 2$, c'est exactement le résultat de la proposition 3. Sinon, on note qu'étant donné V un sous-espace vectoriel de E, la donnée d'un espace W vérifiant $V \subset W \subset E$ est équivalente à la donnée d'un sous-espace (quelconque) $\bar{W}$ du quotient E/V, avec en outre $\dim \bar{W} = \dim W + \dim V$. Ainsi se donner drapeau de type $(d_1, \dots, d_s)$, c'est exactement se donner un sous-espace V_1 de dimension d_1 et un drapeau de type $(d_2, \dots, d_s)$. L'hypothèse de récurrence permet de conclure. □

Là encore, il est possible de fabriquer une démonstration purement combinatoire de la proposition 2 qui donnait le développement de l'expression $(x_1 + \cdots + x_s)^n$. La démarche est la même que celle élaborée en 2.2, et de fait, nous n'allons pas la détailler à nouveau entièrement mais expliquer comment associer à un drapeau de type $(d_1, \dots, d_s)$ un mot de n lettres sur l'alphabet $\{x_1, \dots, x_s\}$ comprenant exactement d_i fois la lettre x_i. On fixe comme précédemment $E_0 \subset E_1 \subset \cdots \subset E_n$ un drapeau complet de $\mathbb{F}_q^n$. Étant donné $(V_1, \dots, V_s)$ un drapeau de type $(d_1, \dots, d_s)$, on note $V_{t,i} = V_t \cap E_i$ ($1 \leqslant t \leqslant s, 0 \leqslant i \leqslant n$). On obtient une suite double à la fois croissante en t et en i qui vérifie les conditions limites $V_{0,i} = V_{s,0} = 0$, $V_{s,i} = E_i$ et $V_{t,n} = V_t$. Le mot associé est alors obtenu en plaçant à la i-ième position la lettre x_t si t est le plus petit indice pour lequel $V_{t,i} \neq V_{t,i-1}$.

3 Le rêve du corps à un élément

Au vu des analogies mises en évidence précédemment[3] entre combinatoire et « q-combinatoire », certains auteurs croient en l'existence d'un objet mystérieux (et pas encore défini à ce jour) baptisé *corps à un élément* et noté $\mathbb{F}_1$, ainsi que d'une géométrie sur cet hypothétique corps (voir [3] pour un historique et une tentative de construction de cette géométrie). De façon spéculative, un espace vectoriel sur $\mathbb{F}_1$ ne devrait être rien d'autre qu'un ensemble, et une application linéaire

[3]Ainsi que de certaines autres non mentionnées dans cet article.

une application ensembliste partiellement définie (voir par exemple [4] ou [1]). De même, un sous-espace vectoriel serait simplement un sous-ensemble, une somme d'espaces vectoriels une union, la dimension devrait correspondre au cardinal, *etc.*

Cette hypothèse est en accord avec la proposition 3 puisque les sous-$\mathbb{F}_1$-espaces vectoriels de dimension k (*i.e.* les sous-ensembles de cardinal k) de $\mathbb{F}_1^n$ (*i.e.* de $\{1,\ldots,n\}$) sont bien comptés par les coefficients binômiaux usuels. La proposition 4 corrobore également ces idées osées puisqu'un $\mathbb{F}_1$-drapeau de $\{1,\ldots,n\}$ de type $(d_1,\ldots,d_t)$ est simplement une suite $E_1 \subset E_2 \subset \cdots \subset E_t$ de sous-ensembles de $\{1,\ldots,n\}$ avec $\mathrm{Card}\,(E_s) = d_1 + \cdots + d_s$. Et il est facile de voir que leur nombre est le coefficient multinômial usuel. En effet, se donner un tel drapeau revient à choisir un sous-ensemble E_1 de $\{1,\ldots,n\}$ de cardinal d_1, puis un sous-ensemble $E_2 \backslash E_1$ de $\{1,\ldots,n\}\backslash E_1$ (qui est de cardinal $n-d_1$) de cardinal d_2 et ainsi de suite. Leur nombre est donc :

$$\binom{n}{d_1} \cdot \binom{n-d_1}{d_2} \cdot \binom{n-d_1-d_2}{d_3} \cdots \binom{n-d_1-\cdots-d_{t-1}}{d_t} = \frac{n!}{d_1! \cdot d_2! \cdots d_t!}.$$

L'analogie est encore plus marquée lorsque l'on s'intéresse aux groupes $\mathrm{GL}_n(\mathbb{F}_q)$ et S_n (qui devrait correspondre à $\mathrm{GL}_n(\mathbb{F}_1)$, puisqu'un isomorphisme de $\mathbb{F}_1^n$ n'est autre qu'une bijection de $\{1,\ldots,n\}$). D'une part, l'étude des classes de conjugaison fait intervenir des deux côtés de façon centrale la notion de partition ordonnée[4] de l'entier n : les classes de conjugaison de S_n correspondent bijectivement à ces partitions, alors que celles de $\mathrm{GL}_n(\mathbb{F}_q)$ correspondent par la théorie des invariants de similitude aux t-uplets de polynômes unitaires $(P_1,\ldots,P_t)$ avec $\deg P_1 + \ldots + \deg P_t = n$, et pour tout i, $P_i(0) \neq 0$ et P_i divise P_{i+1} ; la partition est bien entendu obtenue en isolant la famille des $d_i = \deg P_i$. Poursuivant l'analogie, cela pourrait suggérer qu'il y ait un unique polynôme unitaire à coefficients dans $\mathbb{F}_1$ pour chaque degré.

L'étude des représentations complexes irréductibles des groupes $\mathrm{GL}_n(\mathbb{F}_q)$ et S_n conduit également à des coïncidences surprenantes, sans doute encore plus frappantes que celles que nous avons évoquées jusqu'à présent. Toutefois, cela nous mènerait bien trop loin de les détailler dans cet article. Le lecteur intéressé pourra par exemple consulter [5] ou [6] pour une étude dans un cas plus général avec d'autres groupes.

Une des motivations pour construire la géométrie sur le corps $\mathbb{F}_1$ est un possible lien avec l'hypothèse de Riemann. Si q est une puissance d'un nombre premier p, on sait associer à toute courbe[5] sur $\mathbb{F}_q$ (vérifiant certaines hypothèses) une fonction ζ dont on sait montrer que les zéros sont sur la droite de partie réelle $\frac{q}{2}$. Certains espoirs laissent penser que l'anneau des entiers relatifs $\mathbb{Z}$ pourrait définir une courbe sur le corps $\mathbb{F}_1$ dont la fonction ζ s'identifierait à la fonction ζ de Riemann classique. Une stratégie pour prouver l'hypothèse de Riemann serait alors d'adapter les idées de la preuve que l'on connaît sur $\mathbb{F}_q$ au corps à un élément $\mathbb{F}_1$. Pour une explication plus détaillée de ce dernier espoir, on pourra se reporter à [2].

Bibliographie

[1] M. Karpanov et A. Smirnov, *Cohomology determinants and reciprocity laws : number field case*, prépublication

[2] Y. Manin, *Lectures on zêta fonctions and motives (according to Deninger and Kurokawa)*, Astérisque **228** (1995), pp 121–163

[3] C. Soulé, *Les variétés sur le corps à un élément*, prépublication. Disponible sur `http://www.arxiv.org/abs/math.AG/0304444`.

[4] C'est-à-dire une partition $(d_1,\ldots,d_t)$ de n avec $d_1 \leqslant d_2 \leqslant \cdots \leqslant d_t$.

[5] Peu importe de savoir précisément ce que l'on entend par ce terme, ainsi d'ailleurs que les hypothèses dont on a besoin. Sachez simplement qu'une variété sur un corps k est définie grosso modo comme un recollement de sous-ensembles de k^n défini par l'annulation d'une famille de polynômes. Pour ces objets, on a une notion de dimension et une courbe est par définition une variété de dimension 1.

[4] A. Smirnov, *Hurwitz inequalities for number fields*, St. Petersbg. Math **4** No 2 (1993), pp 357–375

[5] R. Steinberg, *A geometric approch to the representations of the full linear group over a Galois field*, Trans. Amer. Math. Soc **71** (1951), pp 274–282

[6] J. Tits, *Sur les analogues algébriques des groupes semi-simples complexes*, Colloque d'algèbre supérieure - Bruxelles (1956), pp 261–289