Vers les conjectures de Weil

Cécile Gachet, Yichen Qin, Élie Studnia,
sous la direction de Cyril Demarche

Résumé

La résolution d'équations polynomiales semble sous-tendre l'histoire des mathématiques, de l'époque pythagoricienne à la célèbre lettre de Galois, en passant par Cardan, Lagrange, Abel, Gauss. C'est en travaillant à la suite des intuitions de Galois, et en les cristallisant en ce qui deviendra peu à peu l'algèbre moderne, que les mathématiciens de la deuxième moitié du XIX$^{\text{e}}$ siècle déplacent le problème. Dès lors, la question n'est plus de résoudre des équations, mais d'étudier la structure des ensembles de solutions dans différents corps.

Parallèlement aux questions proprement galoisiennes de non-résolubilité, de nouveaux problèmes apparaissent au début du XIX$^{\text{e}}$ siècle, à mi-chemin entre algèbre et arithmétique : après avoir montré indépendamment la loi de réciprocité quadratique, Gauss, Jacobi étoffent leur théorie des résidus quadratiques, et deviennent ainsi à même de dénombrer des solutions de diverses équations polynomiales modulo p. Les ponts entre théorie des nombres et algèbre se multiplient tout au long du XIX$^{\text{e}}$ siècle jusqu'à l'avènement de la théorie algébrique des nombres et de la théorie analytique des nombres. Cependant, les outils arithmétiques élémentaires, les calculs astucieux et les questionnements naïfs des siècles passés tombent en désuétude. Si quelques mathématiciens se repenchent sur ces questions de comptage de solutions dans les années 1930-1940, ils ne s'y attardent pas et tentent surtout de relier ces problèmes au Graal de l'époque : l'hypothèse de Riemann. Lorsqu'André Weil publie, en 1949, l'article [Wei49], il va donc à l'encontre de la tendance contemporaine en se proposant de dénombrer le nombre de solutions à une équation de la forme $a_0 X_{n_0} + \ldots + a_r X^{n_r} = b$ dans $\mathbf{F}_q$, par des méthodes élémentaires.

Mais Weil va plus loin : en introduisant une série formelle associée à son problème de dénombrement, il remarque d'intéressantes propriétés, assez analogues à celles de la fonction zêta de Riemann. Il énonce alors trois conjectures sur la fonction zêta d'une variété algébrique générale. Ces conjectures suscitent l'engouement de la communauté mathématique, qui travaillera pendant une bonne partie du XX$^{\text{e}}$ siècle à développer l'analyse p-adique et surtout à créer des outils algébriques à la hauteur des espérances de Weil. La première conjecture de Weil est résolue par des méthodes analytiques par Bernard Dwork en 1960 dans [Dwo60], et finalement, Pierre Deligne propose en 1974 une preuve des trois conjectures de Weil basée sur les théories de Grothendieck.

On s'intéresse ici à établir les conjectures de Weil dans le cas particulier de [Wei49], et à présenter la preuve de la première conjecture de Weil donnée par Dwork en 1960, en s'appuyant essentiellement sur l'exposition de la preuve présentée dans [Tao]. En chemin, on développe par ailleurs quelques outils élémentaires d'arithmétique, comme les sommes de Gauss, plusieurs résultats de la théorie des corps finis, et des éléments d'analyse p-adique.

Les deux sections **1** et **2** sont largement indépendantes des sections **3** et **4**.

Table des matières

1 Quelques préliminaires de nature arithmétique

1.1 Des éléments de théorie des corps

Extensions de corps Soit $k \subset l$ deux corps. On voit alors que l est un k-espace vectoriel.

Définition On dit que l est une *extension*, ou un *surcorps* de k. Sa dimension comme k-espace vectoriel, si elle est finie, est le *degré* de l'extension de corps. On le note $[l : k]$.

On peut remarquer que la relation « être une extension de » est transitive. De plus, le degré, vu comme une application à valeurs dans $\mathbf{N} \cup \{\infty\}$, est multiplicatif : si on a une tour d'extensions $k \subset l \subset m$, alors $[m : l][l : k] = [m : k]$.

Exemple 1.1.1 Le corps $\mathbf{C}$ est une extension de $\mathbf{R}$ de degré deux. En revanche, $\mathbf{R}$ et l'ensemble des nombres algébriques sont tous deux des extensions de degré infini sur $\mathbf{Q}$: $\mathbf{R}$ pour une simple raison de cardinal, l'ensemble des nombres algébriques pour des raisons plus intéressantes [1].

Un polynôme à coefficients dans k peut aussi être vu comme un élément de $l[X]$. Ainsi, on peut au choix étudier ses racines dans k ou dans l, et arriver à des résultats très différents.

Exemple 1.1.2 Le polynôme $X^3 + X - 1$ est scindé dans $\mathbf{C}$, a une racine dans $\mathbf{R}$ et est irréductible dans $\mathbf{Q}$.

On peut aussi adopter le point de vue inverse et voir certains $x \in l$ comme racines de polynômes à coefficients dans $k[X]$ (on dit alors que x est *algébrique* sur k). Les éléments de l qui ne sont pas algébriques sont dits *transcendants*.

Les nombres algébriques sont un bon moyen de fabriquer des extensions de corps finies dont on connaît le degré.

Lemme 1.1.1 *Soit $x \in l$ algébrique sur k. Alors $k[x] := \{P(x) \mid P \in k[X]\}$ est un sous-corps de l, et on a $[k[x] : k] = \deg(\pi)$, où π engendre l'idéal $\{P \in k[X], \mid P(x) = 0\}$.*

Définition Un corps Ω est dit *algébriquement clos* lorsque tout polynôme de $\Omega[X]$ est scindé sur Ω.

Bien que tout corps ne soit pas algébriquement clos, on peut souvent se ramener à travailler dans un surcorps algébriquement clos, grâce à un théorème de Steinitz, ici admis, [2] qui nous servira dans la section **3** :

Théorème 1.1.1 *Soit k un corps. Il existe un surcorps algébriquement clos Ω de k, constitué d'éléments tous algébriques sur k, et il est unique à isomorphisme de corps k-linéaire près. On l'appelle la clôture algébrique de k.*

Cette première approche des extensions de corps est suffisante pour comprendre l'essentiel de l'exposé. Toutefois, certaines définitions et vérifications qui suivent peuvent sembler un peu arbitraires si on s'arrête en si bon chemin dans l'étude des extensions de corps... Le lecteur intéressé sera donc invité, plus loin, à lire un paragraphe d'introduction à la théorie de Galois.

Introduction aux corps finis Rappelons tout d'abord les indispensables, qui sont ici admis [3] :

Proposition 1.1.2 *Soit k un corps. Tout sous-groupe fini de k^* est cyclique.*

Citons un corollaire qui servira plus tard :

1. qu'on ne développera pas ici
2. pour une preuve, consulter [Tau08]
3. pour des preuves, consulter [Tau08]

Corollaire 1.1.3 *Soient K un corps de caractéristique nulle, $n \geq 1$. Supposons $X^n - 1$ scindé dans K. Alors il est scindé à racines simples et, pour $d \geq 0$,*

$$\sum_{\substack{x \in K \\ x^n = 1}} x^d = n \cdot \mathbb{1}(n \mid d)$$

Preuve La dérivée de $X^n - 1$ est nX^{n-1}, scindée dans K de seule racine nulle, et $0^n - 1 \neq 0$, donc $(X^n - 1)' \wedge X^n - 1 = 1$, d'où la simplicité des racines.

Soit $d \geq 0$. Si n divise d, le résultat est alors clair. Supposons donc que n ne divise pas d. Comme $\{x \in K \mid x^n = 1\}$ est un sous-groupe de cardinal n de K, il possède un générateur g, et $g^d \neq 1$. Dès lors,

$$\sum_{\substack{x \in K \\ x^n = 1}} x^d = \sum_{t=0}^{n-1} (g^t)^d = \sum_{t=0}^{n-1} (g^d)^t = \frac{1 - (g^d)^n}{1 - g^d} = 0.$$

□

La proposition 2 permet de plus d'établir l'existence et l'unicité des corps finis.

Proposition 1.1.4 *Soit q un entier naturel. Il existe un corps fini de cardinal q si et seulement s'il existe p premier, $n \in \mathbf{N}^*$ tels que $q = p^n$. De plus, un tel corps est unique à isomorphisme près.*

Définition On note ce corps $\mathbf{F}_q$, et on l'appelle à bon droit le corps à q éléments. Dorénavant, la lettre q est réservée aux puissances de nombres premiers.

Remarque 1.1.3 Puisqu'on a maintenant établi l'existence du corps fini $\mathbf{F}_q$, la proposition 2 implique que $\mathbf{F}_q^*$ est cyclique. Ce résultat fondamental sera fréquemment utilisé par la suite.

Proposition 1.1.5 *Pour tout p premier et tout k divisant $n \in \mathbf{N}^*$, on a $\mathbf{F}_{p^k} = \{x \in \mathbf{F}_{p^n} \mid x^{p^k} = x\}$. En particulier, $\mathbf{F}_{p^k} \subset \mathbf{F}_{p^n}$.*

Proposition 1.1.6 *Soit $l/k, m/k$ des extensions finies de degrés d_l, d_m sur un corps fini k. Soit n le plus petit surcorps engendré par l et m. Alors n/k est une extension finie de degré $\mathrm{ppcm}(d_l, d_m)$.*

Pour montrer tout cela, on utilise notamment les lemmes d'arithmétique admis suivants, qui resserviront aussi dans la section **2** :

Lemme 1.1.7 *Soit k un corps. Soit $n, m \in \mathbf{N}^*$. On a, dans $k[X]$: $X^n - 1 \mid X^m - 1$ ssi $n \mid m$.*

Lemme 1.1.8 *Soit $q \in \mathbf{N} \backslash \{0, 1\}$. Soit $n, m \in \mathbf{N}^*$. On a : $q^n - 1 \mid q^m - 1$ ssi $n \mid m$.*

On peut maintenant prouver la proposition 6.

Preuve Soit $x_1, \ldots, x_{d_l}$ une base de l sur k et $y_1, \ldots y_{d_m}$ une base de m sur k. Alors $n = k[x_1, \ldots, y_{d_m}]$ donc n/k est bien une extension finie.

Soit d son degré sur k. Par unicité des corps finis à unique isomorphisme près, on se ramène à la situation où $k = \mathbf{F}_q, l = \mathbf{F}_{q^{d_l}}, m = \mathbf{F}_{q^{d_m}}, n = \mathbf{F}_{q^d}$. De plus, par multiplicativité des degrés, $\mathrm{ppcm}(d_l, d_m)$ divise d.

D'autre part, l et m sont inclus dans le corps $\mathbf{F}_{q^{\mathrm{ppcm}(d_l, d_m)}}$, donc n aussi. Par conséquent, $d \mid \mathrm{ppcm}(d_l, d_m)$. □

Remarque 1.1.4 Ce résultat tombe en défaut pour des extensions de corps générales : par exemple, $\mathbf{Q}[i]$ et $\mathbf{Q}[\sqrt{2}]$ sont deux extensions finies de degré deux sur $\mathbf{Q}$ mais le surcorps qu'elles engendrent est $\mathbf{Q}[i, \sqrt{2}]$ qui est de degré quatre sur $\mathbf{Q}$.

On peut résumer les liens entre extensions de corps et corps finis par la figure 1.

Morphisme de Frobenius

Lemme 1.1.9 *Soit p un nombre premier, soit $1 \leq k < p$. Alors $\binom{p}{k}$ est divisible par p.*

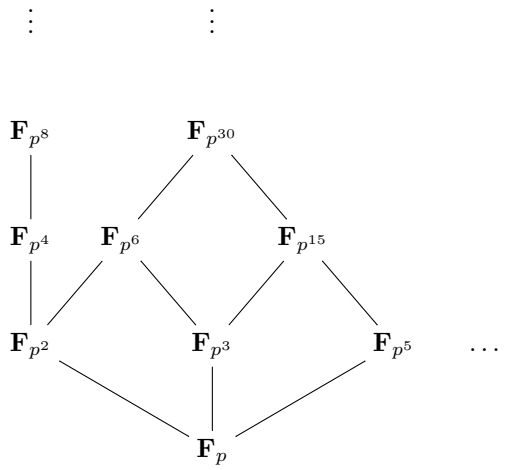

FIGURE 1 – Treillis de divisibilité et extensions de corps finis

Preuve Il suffit de constater que les coefficients binomiaux sont entiers, que $k\binom{p}{k} = p\binom{p-1}{k-1}$ et que k est premier avec p. □

Proposition 1.1.10 *Soient p un nombre premier, q, r deux puissances de p. Soit k le corps à q éléments. Alors $x \in k \longmapsto x^r \in k$ est un automorphisme.*

Preuve Il suffit de le montrer pour $r = p$, car notre application est une itérée de $f : x \longmapsto x^p$) (a fois, où $r = p^a$). Or f est clairement multiplicative, et d'après le lemme et la formule du binôme, f est additive, donc c'est un morphisme d'anneaux. Sa source est un corps, donc le morphisme est injectif, donc (k est fini) bijectif. □

Définition Soient q une puissance d'un nombre premier, $s \geq 1$. Alors l'application $x \in \mathbf{F}_{q^s} \longmapsto x^q \in \mathbf{F}_{q^s}$ est appelée à bon droit l'automorphisme de Frobenius de $\mathbf{F}_{q^s}$.

NORME ET TRACE DANS LES CORPS FINIS Les bases étant posées, on peut maintenant s'intéresser à deux applications particulièrement intéressantes sur un corps fini : la norme et la trace.

Définition Soit $\mathbf{F}_q$ un corps fini, $s \in \mathbf{N}^*$. On définit :

- la *norme* $\mathrm{nr}_{q^s,q} : x \in \mathbf{F}_{q^s}^* \mapsto x x^q x^{q^2} \cdots x^{q^{s-1}}$
- la *trace* $\mathrm{tr}_{q^s,q} : x \in \mathbf{F}_{q^s} \mapsto x + x^q + x^{q^2} + \ldots + x^{q^{s-1}}$

Lemme 1.1.11 *La norme est un morphisme de groupes surjectif de $\mathbf{F}_{q^s}^*$ dans $\mathbf{F}_q^*$. De plus, elle coïncide avec le morphisme $x \mapsto x^s$ sur $\mathbf{F}_q^*$.*

Preuve On fait les vérifications suivantes :

- la norme est à valeurs dans $\mathbf{F}_q^*$: soit $x \in \mathbf{F}_{q^s}^*$. Par définition des corps finis (proposition 5), il suffit de montrer que $\mathrm{nr}(x)^q = \mathrm{nr}(x)$. C'est bien le cas car $x^{q^s} = x$ et le produit est cyclique.
- la norme est clairement un morphisme ;
- soit $a \in \mathbf{F}_q^*$. Comme pour tout $k \in \mathbf{N}^*$, $a^{q^k} = (a^q)^{q^{k-1}} = a^{q^{k-1}} = a$, il vient $\mathrm{nr}(a) = a^s$;
- la norme est surjective : montrons que son noyau est de cardinal $\frac{|\mathbf{F}_{q^s}^*|}{|\mathbf{F}_q^*|} = \frac{q^s-1}{q-1}$. Soit $x \in \mathbf{F}_{q^s}^*$, notons le $x = \xi^j$ où ξ est un générateur de $\mathbf{F}_{q^s}^*$: $\mathrm{nr}(x) = 1$ équivaut à $q^s - 1 \mid \frac{j(q^s-1)}{q-1}$, ce qui a $\mathrm{pgcd}\left(\frac{q^s-1}{q-1}, q^s - 1\right) = \frac{q^s-1}{q-1}$ solutions.

□

Lemme 1.1.12 *La trace est une forme linéaire surjective de $\mathbf{F}_{q^s}$ dans $\mathbf{F}_q$.*

Preuve C'est le même genre de preuve que pour la norme :

- la trace est additive : c'est une somme d'itérées de morphismes de Frobenius, donc une somme de fonctions additives ;
- soient $a \in \mathbf{F}_q^*$, $x \in \mathbf{F}_{q^s}$. Comme pour tout $k \in \mathbf{N}^*$, $a^{q^k} = a$, il vient $\mathrm{tr}(ax) = a\mathrm{tr}(x)$;
- la trace est à valeurs dans $\mathbf{F}_q$: soit $x \in \mathbf{F}_{q^s}$. Par définition des corps finis (proposition 5), il suffit de montrer que $\mathrm{tr}(x)^q = \mathrm{tr}(x)$. C'est bien le cas car $x \in \mathbf{F}_{q^s} \longmapsto x^q$ est additive, $x^{q^s} = x$ et la somme est cyclique ;
- la trace est surjective : soit $x \in \mathbf{F}_{q^s}$, $\mathrm{tr}(x) = 0$ si et seulement si x est racine d'un certain polynôme de degré q^{s-1}. Donc le noyau de la trace est de cardinal au plus q^{s-1}, donc son image est de cardinal au moins q, donc c'est bien $\mathbf{F}_q$.

□

De telles vérifications « à la main » aboutissent certes à une preuve correcte, mais elles ne permettent pas vraiment de comprendre le bien-fondé des définitions de la norme et de la trace, qui semblent tout de même sortir *ex nihilo*... Pour mieux motiver ces définitions, on propose au lecteur intéressé le paragraphe suivant d'introduction à la théorie de Galois.

Bribes de théorie de Galois On rappelle ici quelques résultats de théorie de Galois, dans le but de définir la norme et la trace d'une extension de corps d'une façon plus satisfaisante. [4]

Soit l/k une extension de corps de degré fini.

Lemme 1.1.13 *Tout $x \in l$ est algébrique sur k. On définit le polynôme minimal de x, $P_x \in k[X]$, comme le polynôme unitaire de degré minimal tel que $P(x) = 0$. Il est irréductible.*

Définition Les autres racines de P dans la clôture algébrique de k sont appelées les *conjugués* de x. S'il y a exactement $\deg(P) - 1$ conjugués de x (ie P est à racines simples dans la clôture algébrique de k), le polynôme P et l'élément x sont dits *séparables*.

Définition L'extension de corps l/k est dite *galoisienne* si :

- elle est *séparable*, ie tout $x \in l$ est séparable ;
- elle est *normale*, ie pour tout $x \in l$, tous les conjugués de x sont aussi dans l.

Remarque 1.1.5 Une extension galoisienne est donc *algébrique* (tout $x \in l$ est algébrique sur k). En revanche, elle n'est pas nécessairement de degré fini, puisqu'on peut a priori trouver des éléments algébriques de degré arbitrairement grand dans l. On travaille désormais dans des extensions galoisiennes en toute généralité, les extensions de degré fini sur les corps finis en étant bien un cas particulier, d'après le lemme suivant.

Lemme 1.1.14 *Toute extension de corps algébrique l/k de degré fini, où k est un corps fini, est galoisienne.*

Preuve Notons p la caractéristique de k, $q = |k|$, $r = [l : k]$, de sorte que $k = \mathbf{F}_q$, $l = \mathbf{F}_{q^r}$, et notons Ω la clôture algébrique de k. Soit $P \in k[X]$ irréductible. Alors, $D = P' \wedge P \in k[X]$ est un diviseur de P.

Si $P' = 0$, alors $P \in k[X^p]$ donc, en vertu des propriétés du morphisme de Frobenius, P est une puissance p-ième donc n'est pas irréductible, absurde ! Supposons donc $P' \neq 0$.

4. ces définitions resserviront régulièrement par la suite, tout particulièrement dans la sous-section **3.5** pour construire des normes sur les extensions de $\mathbf{Q}_p$

Alors D est de degré strictement inférieur à celui de P, donc $D = 1$, donc toute racine z de P dans Ω est simple, donc P est séparable. Donc l/k est séparable.

Montrons maintenant le caractère normal de l'extension : soient $x \in l$, soit P son polynôme minimal sur k. Soit ω l'ordre multiplicatif de x. Comme ω divise $|l| - 1$, il est premier avec p, donc q est inversible dans $\mathbf{Z}/\omega\mathbf{Z}$: on peut donc définit α l'ordre multiplicatif de q modulo ω. On a alors $k[x] = \mathbf{F}_{q^\alpha}$: comme $x \in \mathbf{F}_{q^\alpha}$ on a l'inclusion directe, et x n'est inclus dans aucun $\mathbf{F}_{q^t}$, $0 < t < \alpha$, car si $x \in \mathbf{F}_{q^t}$, $x^{q^t-1} = 1$, donc $q^t = 1 \bmod \omega$, donc $\alpha \mid t$. Finalement, $\deg P = \alpha$, et en utilisant le morphisme de Frobenius, les x^{q^k}, $0 \leq k < \alpha$, sont α racines distinctes de P et sont bien dans l. □

Soit l/k une extension de corps.

Définition On définit :

- la *norme* $\mathrm{nr}_{l/k} : x \in l^* \mapsto \det(u_x)$, où $u_x : y \in l \mapsto xy$ automorphisme de k-espace vectoriel ;
- la *trace* $\mathrm{tr}_{l/k} : x \in l \mapsto \mathrm{tr}(u_x)$, pour le même u_x que *supra*.

Ainsi, la norme et la trace sont immédiatement des morphismes (de l^* dans k^* et de l dans k respectivement). Leur surjectivité est en revanche fausse dans le cas général.

Reste à faire le lien entre ces définitions et les définitions données pour les corps finis.

Proposition 1.1.15 *Soit l/k une extension de corps finie de degré n. Soit $x \in l, P$ son polynôme minimal sur k. Si $P = \sum_{i=0}^{d} a_i X^i$ avec $a_d = 1$, alors :*

$$\mathrm{nr}(x) = (-1)^n a_0^{n/d} \text{ et } \mathrm{tr}(x) = -\frac{n}{d} a_{d-1}.$$

Preuve Soit $s = \frac{n}{d}$ et soit $e_1, \ldots, e_s$ une base de l sur $k[x]$. Soit $E_i = k[x]e_i$ pour $1 \leq i \leq s$ une décomposition de l en sous-espaces stables par u_x. Dans chaque E_i, la matrice de u_x dans la base canonique est la matrice compagnon de P, d'où le résultat. □

Or $(-1)^d a_0$ (respectivement $-a_{d-1}$) est le produit (respectivement la somme) de x et de ses conjugués. Pour des corps finis, on a montré dans la preuve du lemme 14 que les conjugués de x sont exactement les x^{p^k} pour $0 \leq k \leq d-1$, où d est le degré du polynôme minimal de x, et restent dans le corps fini. D'où la définition de la norme dans les corps finis.

Le paragraphe suivant sert à établir une dernière propriété dite de transitivité de la norme et de la trace, qui sera très utile dans la suite.

Applications linéaires, extensions de corps, norme et trace

Soit l/k une extension finie de corps de degré d, $\mathscr{B}$ une base de l sur k. À $x \in l$ on associe la matrice M_x de l'endomorphisme u_x du paragraphe précédent. Soit $r \in \mathbf{N}^*$.

Définition À une matrice $A \in \mathscr{M}_r(l)$, on associe la matrice $T(A) \in \mathscr{M}_{rd}(k)$, définie en remplaçant dans A chaque $a_{i,j}$ par $M_{a_{i,j}}$.

Remarque 1.1.6 Comme $x \in l \longmapsto M_x$ soit un morphisme d'anneaux k-linéaire et par les propriétés du produit par blocs, $A \in \mathscr{M}_r(l) \longmapsto T(A) \in \mathscr{M}_{dr}(k)$ est un morphisme k-linéaire d'anneaux.

Lemme 1.1.16 *Si $A \in \mathscr{M}_r(l)$ est triangulaire supérieure (resp. inférieure), avec des 1 sur sa diagonale, il en est de même pour $T(A)$.*

Corollaire 1.1.17 *Si $A \in \mathscr{M}_r(l)$ est de déterminant 1, $T(A)$ aussi.*

Preuve Le groupe $\mathbf{SL}_r(l)$ est engendré par les matrices de transvection, qui sont triangulaires avec des 1 sur la diagonale. □

Lemme 1.1.18 *Si $A \in \mathscr{M}_r(l)$ est diagonale de déterminant δ, $T(A)$ est de déterminant $\mathrm{nr}_{l/k}(\delta)$.*

Preuve Cela découle des propriétés du déterminant diagonal par blocs, de la définition et de la multiplicativité de la norme. □

Corollaire 1.1.19 *Si $A \in \mathbf{GL}_r(l)$, $\det T(A) = \mathrm{nr}_{l/k}(\det A)$.*

Preuve Il suffit de décomposer A sous la forme $A = BC$ avec $B \in SL_r(l)$ et $C \in \mathscr{M}_r(l)$ diagonale. □

Proposition 1.1.20 *Pour tout $A \in \mathscr{M}_r(l)$, $\det T(A) = \mathrm{nr}_{l/k}(\det A)$.*

Preuve On écrit $A = PDQ$ avec $P, Q \in \mathbf{GL}_r(l)$ et $D \in \mathscr{M}_r(l)$ diagonale. □

Proposition 1.1.21 *Pour tout $A \in \mathscr{M}_r(l)$, on a $\mathrm{tr}\, T(A) = \mathrm{tr}_{l/k}(\mathrm{tr} A)$.*

Preuve En notant $A = (a_{i,j})$, on a $\mathrm{tr}\, T(A) = \sum_{i=1}^{r} \mathrm{tr} M_{a_{i,i}} = \sum_{i=1}^{r} \mathrm{tr}_{l/k}(a_{i,i}) = \mathrm{tr}_{l/k}(\mathrm{tr} A)$. □

Proposition 1.1.22 *Soit E un l-espace vectoriel de dimension finie. Soit $f : E \to E$ l-linéaire. Alors E est également un k-espace vectoriel de dimension finie, et f est un endomorphisme k-linéaire de E. On a $\mathrm{nr}_{l/k}(\det_l(f)) = \det_k(f)$, $\mathrm{tr}_{l/k}(\mathrm{tr}_l f) = \mathrm{tr}_k f$.*

Preuve Notons les vecteurs de la base $\mathscr{B} = (u_1, \ldots, u_d)$ de l sur k, et soit $\mathscr{C} = (e_1, \ldots, e_r)$ une l-base de E. On sait alors que $\mathscr{C}' = (u_1 e_1, u_2 e_1, \ldots, u_d e_1, u_1 e_2, \ldots, u_d e_2, \ldots, u_1 e_r, \ldots, u_d e_r)$ est une k-base de E. De plus, si A est la matrice de f dans la base $\mathscr{C}$, $T(A)$ est la matrice de f dans la base $\mathscr{C}'$. De la sorte, $\det_k f = \det T(A) = \mathrm{nr}_{l/k}(\det A) = \mathrm{nr}_{l/k}(\det_l f)$. On procède de même pour la trace. □

Proposition 1.1.23 *Soit m/l et l/k des extensions finies de corps. On a :*

- $\mathrm{nr}_{l/k} \circ \mathrm{nr}_{m/l} = \mathrm{nr}_{m/k}$;
- $\mathrm{tr}_{l/k} \circ \mathrm{tr}_{m/l} = \mathrm{tr}_{m/k}$.

Preuve Soit $x \in m$. On sait que m est un k-espace vectoriel de dimension finie, $f = x \cdot \mathrm{Id}_m$ est m-linéaire. Donc $\mathrm{nr}_{m/k}(x) = \det_k(f) = \mathrm{nr}_{l/k}(det_l(f)) = \mathrm{nr}_{l/k} \circ \mathrm{nr}_{m/l}(\det_m f) = \mathrm{nr}_{l/k} \circ \mathrm{nr}_{m/l}(x)$; on fait de même pour la trace. □

1.2 Un peu d'arithmétique élémentaire

Revenons maintenant à de l'arithmétique du XIX$^{\mathrm{e}}$ siècle. On rappelle ici la définition des caractères, et on introduit les sommes de Gauss et les sommes de Jacobi, dont on montre quelques propriétés.

Caractères On commence par quelques rappels et notations.

Définition Soit G un groupe. Un *caractère* de G est un morphisme de groupes $\chi : G \to \mathbf{C}^*$ (respectivement $\mathbf{C}$).

Fixons ξ un générateur de $\mathbf{F}_q^*$. Comme $\mathbf{F}_q^*$ est cyclique, on dispose de caractères multiplicatifs [5] non triviaux sur un corps fini, un caractère étant entièrement donné par le choix d'une racine $q-1$-ième de l'unité dans $\mathbf{C}$.

Ainsi, pour toute $(q-1)$-ième racine de l'unité $e^{2i\pi\alpha}$ (c'est-à-dire telle que $\alpha \mod 1 \in \{0, \frac{1}{q-1}, \ldots, \frac{q-2}{q-1}\} := \frac{1}{q-1}[\![0, q-2]\!]$), on note $\chi_\alpha^{\mathbf{F}_q}$ le caractère associé. Dans la suite, on s'autorise à confondre α et $\alpha \bmod 1$ et à omettre l'exposant $\mathbf{F}_q$ s'il n'y a pas ambiguïté.

Définition Si $\alpha \in \mathbf{Z}$, χ_α est appelé le *caractère trivial*.

On dispose d'un résultat général utile :

5. c'est-à-dire de caractères pour le groupe multiplicatif $(F_q^*, \cdot)$; on peut aussi définir les caractères additifs comme les caractères pour le groupe $(\mathbf{F}_q, +)$.

Proposition 1.2.24 *Si G est un groupe fini et χ un caractère sur G,*

$$\sum_{g\in G}\chi(g) = |G|\cdot \mathbb{1}(\chi \text{ est trivial})$$

Preuve Si χ est trivial, c'est bon. Sinon, soit $g\in G$ tel que $\chi(g)\neq 1$.
Soit $S=\sum_{h\in G}\chi(h)$. Comme $h\in G\longmapsto gh$ est une bijection de G dans lui-même,

$$S=\sum_{h\in G}\chi(gh)=\chi(g)\sum_{h\in G}\chi(h)=\chi(g)S$$

donc comme $\chi(g)\neq 1$, $S=0$, ce qui conclut. □

On pose enfin la convention suivante : $\chi_\alpha(0)=1$ si χ_α est trivial, 0 sinon. On a le premier résultat de comptage de racines suivant :

Proposition 1.2.25 *Soit $u\in\mathbf{F}_q, n\in\mathbf{N}^*$. Posons $d=\mathrm{pgcd}(n,q-1)$. Alors :*

$$|\{x\in\mathbf{F}_q|\, x^n=u\}| = \sum_{\alpha\in\frac{1}{d}[\![0,d-1]\!]}\chi_\alpha(u).$$

Preuve Si $u=0$, c'est vrai.
Notons $u=\xi^l$. Pour $x\in\mathbf{F}_q$,

$$x^n=u\Longleftrightarrow \exists\, j\in[\![0,q-1]\!] \text{ tq } x=\xi^j \text{ et } j\equiv (n/d)^{-1}(l/d) \mod (q-1)/d.$$

L'équation a donc d solutions si d divise l, aucune solution sinon. D'autre part, on a :

$$\sum_{\alpha\in\frac{1}{d}[\![0;d-1]\!]}\chi_\alpha(u)=\sum_{k=0}^{d-1}e^{2i\pi kl/d}=\begin{cases} d & \text{si } l/d \text{ entier}\\ 0 & \text{sinon.}\end{cases}$$

□

Sommes de Gauss Soit $\mathbf{F}_q$ un corps fini. On se donne ψ un caractère additif non trivial.
Définition Pour $\alpha\in\frac{1}{q-1}[\![0,q-2]\!]$, on pose :

$$g(\chi_\alpha)=\sum_{x\in\mathbf{F}_q}\chi_\alpha(x)\psi(x).$$

C'est la *somme de Gauss* associée au caractère χ_α.

Lemme 1.2.26 *Soit χ un caractère multiplicatif. Alors $|g(\chi)|^2=q$ et pour tout $t\in\mathbf{F}_q^*$, on a :*

$$\chi(t)=\frac{g(\chi)}{q}\sum_{x\in\mathbf{F}_q}\overline{\chi}(x)\overline{\psi}(tx).$$

Preuve C'est vrai si χ est trivial (d'après la proposition 24 appliquée au groupe $(\mathbf{F}_q,+)$).
Supposons χ non trivial. Comme le conjugué d'un complexe de module 1 est son inverse,

$$\begin{aligned} g(\chi)\overline{g(\chi)} &= \sum_{x,y\in\mathbf{F}_q^*}\chi(xy^{-1})\psi(x-y)\\ &= \sum_{u,y\in\mathbf{F}_q^*}\chi(u)\psi((u-1)y)\\ &= q-\sum_{u\in\mathbf{F}_q^*}\chi(u)=q.\end{aligned}$$

car, d'après la proposition 24, pour le groupe $(\mathbf{F}_q, +)$ et le caractère $\psi \circ ((u-1)\mathrm{Id})$,

$$\sum_{y \in \mathbf{F}_q^*} \psi((u-1)y) = \begin{cases} -1 & \text{si } u \neq 1, \\ q-1 & \text{si } u = 1. \end{cases}$$

On en déduit, pour tout $t \in \mathbf{F}_q^*$,

$$\frac{q}{g(\chi)} = \overline{g(\chi)} = \sum_{x \in \mathbf{F}_q} \overline{\chi}(tx)\overline{\psi}(tx) = \chi(t)^{-1} \sum_{x \in \mathbf{F}_q} \overline{\chi}(x)\overline{\psi}(tx).$$

□

Sommes de Jacobi On définit enfin les sommes de Jacobi de deux façons différentes, reliées par la proposition 27.

Définition Pour $a = (\alpha_0, \ldots, \alpha_r)$ tel que pour tout i, $\alpha_i \in \frac{1}{q-1}[\![1, q-2]\!]$ et $\alpha_0 + \ldots + \alpha_r$ entier, on définit :

$$j(a) = \frac{1}{q-1} \sum_{\substack{u_0, \ldots, u_r \in \mathbf{F}_q \\ u_0 + \ldots + u_r = 0}} \chi_{\alpha_0}(u_0) \cdots \chi_{\alpha_r}(u_r).$$

C'est la *somme de Jacobi* associée à a.

Remarque 1.2.7 En fait, un changement de variables permet de voir que $j(a)$ est toujours un entier algébrique :

$$\begin{aligned} j(a) &= \frac{1}{q-1} \sum_{\substack{u_0, \ldots, u_r \in \mathbf{F}_q \\ u_0 + \ldots + u_r = 0 \\ u_0 \neq 0}} \chi_{\alpha_0}(u_0) \cdots \chi_{\alpha_r}(u_r) \\ &= \frac{1}{q-1} \sum_{u_0 \in \mathbf{F}_q^*} \chi_{\alpha_0 + \ldots + \alpha_r}(u_0) \sum_{\substack{v_1, \ldots, v_r \in \mathbf{F}_q \\ v_1 + \ldots + v_r = -1}} \chi_{\alpha_1}(v_1) \cdots \chi_{\alpha_r}(v_r) \\ &\text{en posant } v_i = u_i u_0^{-1} \text{ pour tout } i. \\ &= \sum_{\substack{v_1, \ldots, v_r \in \mathbf{F}_q \\ v_1 + \ldots + v_r = -1}} \chi_{\alpha_1}(v_1) \cdots \chi_{\alpha_r}(v_r) \\ &\text{car } \chi_{\alpha_0 + \ldots + \alpha_r} = 1 \end{aligned}$$

Une racine de l'unité est un entier algébrique et un produit ou une somme d'entiers algébriques sont encore des entiers algébriques, d'où l'intégrité de $j(a)$. Ce résultat sera utile à la fin de la section **2**.

Proposition 1.2.27 *On a la formule :*

$$j(a) = \frac{1}{q} g(\chi_{\alpha_0}) \cdots g(\chi_{\alpha_r}).$$

Preuve On calcule, avec le lemme 26 :

$$\begin{aligned} (q-1)j(a) &= \sum_{\substack{u_0, \ldots, u_r \in \mathbf{F}_q \\ u_0 + \ldots + u_r = 0}} \chi_{\alpha_0}(u_0) \cdots \chi_{\alpha_r}(u_r) \\ &= \sum_{\substack{u_0, \ldots, u_r \in \mathbf{F}_q \\ u_0 + \ldots + u_r = 0}} g(\chi_{\alpha_0}) \cdots g(\chi_{\alpha_r}) q^{-r-1} \sum_{x_0, \ldots, x_r \in \mathbf{F}_q} \overline{\chi}_{\alpha_0(x_0)} \overline{\psi}(\alpha_0 x_0) \cdots \overline{\chi}_{\alpha_r}(x_r) \overline{\psi}(\alpha_r x_r) \\ &= q^{-r-1} \sum_{x_0, \ldots, x_r \in \mathbf{F}_q} g(\chi_{\alpha_0}) \overline{\chi}_{\alpha_0}(x_0) \cdots g(\chi_{\alpha_r}) \overline{\chi}_{\alpha_r}(x_r) \sum_{\substack{u_0, \ldots, u_r \in \mathbf{F}_q \\ u_0 + \ldots + u_r = 0}} \overline{\psi}(\alpha_0 x_0 + \cdots + \alpha_r x_r) \end{aligned}$$

Or, à x fixé, $\Psi : (u_0, \ldots, u_r) \mapsto \overline{\psi}(x_0u_0 + \ldots + x_ru_r)$ est un caractère du groupe $\{(u_0, \ldots, u_r) \in \mathbf{F}_{q^{r+1}} \mid u_0 + \ldots + u_r = 0\}$. Donc sa somme sur le groupe vaut q^r (ie le cardinal du groupe) s'il est le caractère trivial, zéro sinon. Déterminons à quelle condition sur x Ψ est trivial. Comme $\overline{\psi}$ est non trivial, il existe $z \in \mathbf{F}_q$ tel que $\overline{\psi}(z) = 1$, et le système linéaire suivant dans $\mathbf{F}_q$:

$$\begin{cases} \sum u_i = 0 \\ \sum x_i u_i = z \end{cases}$$

a une solution si et seulement si x n'est pas colinéaire à $(1, \ldots, 1)$. De fait, Ψ est finalement trivial si et seulement si x est colinéaire à $(1, \ldots, 1)$.

Donc :

$$\begin{aligned} q(q-1)j(a) &= \sum_{x \in \mathbf{F}_q} g(\chi_{\alpha_0})\overline{\chi}_{\alpha_0}(x) \cdots g(\chi_{\alpha_r})\overline{\chi}_{\alpha_r}(x) \\ &= (q-1)g(\chi_{\alpha_0}) \cdots g(\chi_{\alpha_r}) \end{aligned}$$

car $\overline{\chi}_{\alpha_0+\ldots+\alpha_r}$ est trivial. □

Corollaire 1.2.28 *En particulier,* $j(a)\overline{j(a)} = q^{r-1}$.

Remarque 1.2.8 On peut étendre la définition de la somme de Jacobi au cas où les α_i sont pour certains dans $\frac{1}{q-1}[\![1, q-2]\!]$ et pour d'autres dans $\frac{1}{q-1}[\![0, q-2]\!]$ (mais toujours de somme entière). On pose pour cela, pour $a = (\alpha_0, \ldots, \alpha_r)$ vérifiant les conditions *supra* et tel que $\alpha_i = 0 \Leftrightarrow i > r - s$:

$$j(a) = \frac{(-1)^s}{q-1} \sum_{\substack{u_0, \ldots, u_{r-s} \in \mathbf{F}_q \\ u_0 + \ldots + u_{r-s} = 0}} \chi_{\alpha_0}(u_0) \cdots \chi_{\alpha_{r-s}}(u_{r-s}).$$

On a alors la formule :

$$j(a) = \frac{(-1)^s}{q} g(\chi_{\alpha_0}) \cdots g(\chi_{\alpha_{r-s}}),$$

et en particulier, $j(a)\overline{j(a)} = q^{r-s-1}$.

1.3 Séries formelles

Les outils développés jusqu'ici permettent déjà d'obtenir une formule et un bon encadrement du nombre de points sur une hypersurface diagonale. Cette mise en œuvre est toutefois repoussée à la section **2**.

Avant cela, montrons un dernier résultat remarquable sur les sommes de Gauss, utilisé par Weil dans la deuxième moitié de l'article [Wei49] pour introduire la fonction zêta. Il s'agit du théorème de Hasse-Davenport, qui permet de faire le lien entre des sommes de Gauss dans un corps fini et dans une extension finie de ce corps (pour un choix de caractères multiplicatifs compatibles). La preuve de ce théorème est instructive, car elle réutilise les outils de la sous-section **1.2** ainsi qu'un nouveau type d'objet : les séries formelles. Ces séries formelles seront réutilisées par Weil à de nombreuses reprises (la fonction zêta est elle-même définie comme une série formelle), c'est pourquoi nous proposons ici une sous-section de rappels à leur sujet.

Toutes les preuves omises sont de simples calculs. Dans toute la sous-section, on fixe un corps K de caractéristique nulle.

Algèbre des séries formelles

Définition On appelle *série formelle* à coefficients dans K (ou sur K) (ou simplement série formelle quand il n'y a pas d'ambiguité) une suite $(a_n) \in K^{\mathbf{N}}$.

Définition Soient $a = (a_n), b = (b_n)$ deux séries formelles sur K, $\lambda \in K$. On définit les séries formelles sur K :

– $\lambda \cdot a := (\lambda a_n)_n$

– $a + b := (a_n + b_n)_n$

– $a \cdot b := \left(\sum_{k=0}^{n} a_k b_{n-k} \right)_n$

Proposition 1.3.29 *Muni de $+$ et $\cdot$ ainsi définies, l'ensemble des séries formelles à coefficients dans le corps K est une K-algèbre commutative, unitaire, notée $K[\![X]\!]$. L'élément neutre additif est la série $0 = (0)_n$, l'élément neutre multiplicatif est la série $1 = (\delta_{n,0})_n$.*

Définition On note X la série formelle $X = (\delta_{n,1})_n$.

Lemme 1.3.30 *Pour $k \geq 0$, $X^k = (\delta_{n,k})_n$.*

Corollaire 1.3.31 *Il existe un plongement naturel de K-algèbres de $K[X]$ vers $K[\![X]\!]$*

Remarque 1.3.9 On notera par conséquent $\sum a_n X^n$ la série formelle (a_n), par analogie avec les polynômes. De même, si $A = (a_n)_n$, on notera $A(0) = a_0$. On observera que $A \longmapsto A(0)$ est un morphisme d'algèbres.

Inversion des séries formelles

Proposition 1.3.32 *Soit $A \in K[\![X]\!]$. Il existe $B \in K[\![X]\!]$ tel que $AB = BA = 1$ si et seulement si $A(0) \neq 0$.*

Preuve Le sens direct est évident, voyons le sens réciproque. Notons $A = \sum a_n X^n$, on construit $b \in K^{\mathbf{N}}$ par récurrence par $b_0 = a_0^{-1}$, puis, si $n \geq 1$,

$$b_n = -a_0^{-1} \sum_{k=0}^{n-1} b_k a_{n-k}.$$

Par construction, $B = \sum b_n X^n$ convient. □

Topologie sur les séries formelles

Définition Soit $A = \sum a_n X^n \in K[\![X]\!]$. La *valuation* de A est la quantité $v(A) = \min\{k \in \mathbf{N},\ a_k \neq 0\} \in [\![0; \infty]\!]$.

Proposition 1.3.33 *Si $A, B \in K[\![X]\!]$, on a $v(AB) = v(A) + v(B)$, $v(A) = v(-A)$, $v(A + B) \geq \min(v(A), v(B))$, et $v(A) = \infty$ si et seulement si $A = 0$.*

Proposition 1.3.34 *On pose $d(A, B) = 2^{-v(A-B)}$ pour toutes séries formelles A et B. Alors d est une distance vérifiant l'inégalité ultramétrique sur $K[\![X]\!]$, donc elle munit cet espace d'une topologie.*

Remarque 1.3.10 Plus précisément, $|\cdot| : A \in K[\![X]\!] \longmapsto 2^{-v(A)}$ est une valeur absolue sur $K[\![X]\!]$, et on a construit la distance et la topologie associées à cette valeur absolue. Ce point de vue, développé dans les sections **3.1** et **3.4**, et brièvement utilisé dans la section **1.4** ne sert pas dans cette sous-section.

Proposition 1.3.35 *Soit $(A_n = \sum_p a_{n,p} X^p) \in K[\![X]\!]^{\mathbf{N}}$, $B = \sum_p b_p X^p \in K[\![X]\!]$. Alors $A_n \to B$ si, et seulement si, pour tout p dans $\mathbf{N}$, $(a_{n,p})_n$ stationne à b_p.*

Corollaire 1.3.36 *Une série d'éléments de $K[\![X]\!]$ converge au sens de d si et seulement si la valuation de son terme général tend vers $+\infty$.*

Remarque 1.3.11 Muni de cette distance, les considérations ci-dessus impliquent que $K[\![X]\!]$ est complet.

Dérivation des séries formelles

Définition Si $A = \sum a_n X^n$, on définit la *série formelle dérivée* par $A' = \sum (n+1)a_{n+1}X^n$.

Proposition 1.3.37 *$A \in K[\![X]\!] \longmapsto A'$ est K-linéaire, surjective, 2-lipschitzienne pour d et de plus, on a, pour $P, Q \in K[\![X]\!]$, $(PQ)' = PQ' + P'Q$.*

Exponentielle dans $K[\![X]\!]$

Proposition 1.3.38 *Soit $A \in K[\![X]\!]$ avec $A(0) = 0$. La valuation de $\frac{A^n}{n!}$ tend vers $+\infty$, de sorte que $\displaystyle\sum_{n\geq 0} \frac{A^n}{n!}$ converge dans $K[\![X]\!]$.*

Définition Pour $A \in K[\![X]\!]$ avec $A(0) = 0$, on pose à bon droit $\exp(A)$ la somme de cette série.

Proposition 1.3.39 *Soit $A \in K[\![X]\!]$ avec $A(0) = 0$. Alors $\exp(A)' = A' \exp(A)$, et de plus $\exp(A)(0) = 1$.*

Proposition 1.3.40 *Si $A, B \in K[\![X]\!]$ sont telles que $A(0) = B(0) = 0$, alors $\exp(A+B) = \exp(A)\exp(B)$.*

Preuve Elle est analogue au cas de l'exponentielle réelle, sauf que la propriété ultramétrique rend plus aisée l'obtention de la convergence. □

Propriétés de la dérivée logarithmique

Définition Soit A une série formelle avec $A(0)$ non nul. On définit la *dérivée logarithmique* de A par $DL(A) = \frac{A'}{A}$.

Proposition 1.3.41 *Si $A, B \in K[\![X]\!]$ vérifient que $A(0)$ et $B(0)$ sont non nuls, alors $DL(AB) = DL(A) + DL(B)$.*

Proposition 1.3.42 *Si $A \in K[\![X]\!]$ avec $A(0) = 0$, $A' = DL(\exp(A))$.*

Proposition 1.3.43 *Soient $A, B \in K[\![X]\!]$ avec $A(0)$ et $B(0)$ non nuls, et $DL(A) = DL(B)$. Alors, pour un $u \in K^*$, $A = uB$.*

Preuve On peut considérer la série $C = A \cdot B^{-1}$. On observe que $C(0)$ est non nul et que $CB = A$ donc en passant aux dérivées logarithmiques $DL(C) + DL(B) = DL(A)$, donc $DL(C) = 0$, donc $C' = 0$et $C = u$ pour un $u \in K^*$. □

Logarithme d'une série formelle

Définition Soit S une série formelle avec $S(0) = 1$. Alors on appelle $\log(S)$ la série formelle de $K[\![X]\!]$ telle que : $\log(S)' = DL(S)$, et $\log(S)(0) = 0$.

Lemme 1.3.44 *Soient S une série formelle avec $S(0) = 0$. Alors la série $\sum_{n\geq 0} S^n$ converge vers $(1-S)^{-1}$.*

Preuve

$$\sum_{n=0}^{N} S^n = (1-S)^{-1}(1-S)\sum_{n=0}^{N} S^n = (1-S)^{-1}(1-S^{N+1}) \underset{N\to\infty}{\longrightarrow} (1-S)^{-1}$$

□

Proposition 1.3.45 *Soit S une série formelle avec $S(0) = 0$. Alors la série $\sum_{n\geq 1} \frac{(-1)^{n-1}}{n} S^n$ converge et sa somme est $\log(1+S)$.*

Preuve La convergence de la série découle du fait que la valuation de son terme général est n fois celle de S, donc tend vers l'infini. Par continuité de la dérivation formelle, on a

$$\left(\sum_{n\geq 1} \frac{(-1)^{n-1}}{n} S^n\right)' = \sum_{n\geq 1} S'(-S)^{n-1} = \frac{(S+1)'}{1-(-S)},$$

ce qui conclut car la somme de la série est de terme constant nul. □

Corollaire 1.3.46 *Soit $\alpha \in K$. On a* $\log(1-\alpha X) = -\sum_{n\geq 1} \frac{\alpha^n}{n} X^n$.

Proposition 1.3.47 *Soient U, V deux séries formelles avec $U(0) = V(0) = 1$. Alors* $\log(UV) = \log(U) + \log(V)$

Preuve On observe que $(\log(U) + \log(V))(0) = 0$ et que $(\log(U) + \log(V))' = \log(U)' + \log(V)' = DL(U) + DL(V) = DL(UV)$, ce qui conclut. □

Proposition 1.3.48 *Soit S une série formelle avec $S(0) = 0$. Alors* $\exp(S)(0) = 1$ *: on peut définir* $\log(\exp(S))$. *On a* $\log(\exp(S)) = S$.

Preuve On a $S(0) = 0$, et $S' = DL(\exp(S))$. □

Exponentiation d'une série formelle

Définition Soit S une série formelle avec $S(0) = 0$, soit $t \in K$. On définit à bon droit la série formelle suivante :

$$(1+S)^t := \exp(t \log(1+S)).$$

Séries formelles en plusieurs variables

Soit $d \in \mathbf{N}^*$. On peut définir les séries formelles en d variables, comme les suites indexées sur $\mathbf{N}^d$. On définit la somme, la multiplication par un scalaire, le produit de séries formelles en d variables de façon similaire au cas d'une variable, et on vérifie qu'on définit ainsi une algèbre $K[\![X_1, \ldots, X_d]\!]$, qu'on pourra par la suite noter R s'il n'y a d'ambiguïté ni sur le corps K, ni sur d.

Par ailleurs, pour poursuivre l'analogie avec les polynômes, $K[X_1, \ldots, X_d]$ est une sous-algèbre de $K[\![X_1, \ldots, X_d]\!]$. On adopte donc la notation $X^w = X_1^{w_1} \cdots X_d^{w_d}$ pour tout $w = (w_1, \ldots, w_d) \in \mathbf{N}^d$.

On définit l'exponentiation pour les séries formelles de plusieurs variables.

Définition Soit $d \in \mathbf{N}^*$, $F \in K[\![X_1, \ldots, X_d]\!]$ une série formelle telle que $F(0) = 0$. Alors on définit la série formelle en $d+1$ variables suivante :

$$(1+F)^T := \sum_{i=0}^{\infty} \frac{T(T-1)\ldots(T-i+1)}{i!} F(X_1, \ldots, X_d)^i.$$

Preuve Cela définit bien une série formelle. En effet, fixons $(w,t) \in \mathbf{N}^d \times \mathbf{N}$. Le coefficient devant $X^w T^t$ dans le membre de droite ci-dessus est égal au coefficient devant $X^w T^t$ dans

$$\sum_{i=0}^{w_1+\ldots+w_d} \frac{T(T-1)\ldots(T-i+1)}{i!} F(X_1, \ldots, X_d)^i,$$

car pour tout $i > w_1 + \ldots + w_d + 1$, tous les monômes de $F(X_1, \ldots, X_d)^i$ sont de degré strictement supérieur au degré de X^w, et donc X^w n'apparaît pas dans $F(X_1, \ldots, X_d)^i$.

On peut donc « remonter le temps » : définir nos coefficients à l'aide des sommes finies puis établir l'identité formelle entre l'exponentiation pour ces sommes finies et l'exponentiation qu'on avait définie *a priori*. □

Remarque 1.3.12 Pour tout $(w,t) \in \mathbf{N}^d \times \mathbf{N}$, si $w_1 + \ldots + w_d < t$, le coefficient devant $X^w T^t$ vaut zéro.

1.4 Le théorème de Hasse-Davenport

Nous sommes maintenant suffisamment armés pour énoncer et démontrer le théorème de Hasse-Davenport. Soit k un corps fini, k'/k une extension de corps finie de degré ν.

Définition Deux caractères multiplicatifs (respectivement additifs) χ et χ' (respectivement ψ et ψ') sur k et k' sont dits *compatibles* si $\chi' = \chi \circ \mathrm{nr}_{k'/k}$ (respectivement $\psi' = \psi \circ \mathrm{tr}_{k'/k}$).

Soient χ, χ' (respectivement ψ, ψ') deux caractères multiplicatifs (respectivement additifs) compatibles sur k, k'.

Théorème 1.4.2 *Si on note $g(\chi)$ la somme de Gauss dans k associée à ψ et χ, $g'(\chi')$ dans k' avec ψ' et χ', on a :*

$$-g'(\chi') = [-g(\chi)]^{\nu}.$$

Preuve On procède en plusieurs étapes.
Première étape : lien entre norme, trace et polynôme minimal. On fait le constat suivant. Soit $\lambda : P = \sum_{i=0}^{d(P)} a_i X^i \in k[X]$ unitaire $\mapsto \chi((-1)^{d(P)} a_0)\psi(-a_{d(P)-1})$. Soit λ' défini de même sur $k'[X]$ avec χ' et ψ'. On observe que :

- λ est multiplicatif ;
- si on fixe $d \in \mathbf{N} \setminus \{0, 1\}$, la somme des $\lambda(P)$ pour P unitaire de degré d est nulle d'après la proposition 24 ;
- la somme des $\lambda(P)$ pour P unitaire de degré 1 vaut $g(\chi)$;
- si $x \in l$ (l extension finie arbitraire de k) a pour polynôme minimal P_x, alors $\lambda(P_x) = \chi(\mathrm{nr}_{l/k}(x))\psi(\mathrm{tr}_{l/k}(x))$, d'après la proposition 15. Cela nous motive pour étudier λ sur les polynômes irréductibles (qui sont potentiellement des polynômes minimaux).

Deuxième étape : soit $P \in k[X], P' \in k'[X]$ irréductibles tels que $P' \mid P$ dans $k'[X]$. Que dire de $\lambda(P)$ et de $\lambda'(P')$? Soit ξ une racine de P' (dans une extension de k' de dimension finie ; quitte à restreindre on peut supposer que cette extension est $k'(\xi)$). Soit $d = \mathrm{pgcd}(\deg(P), \nu)$. D'après la proposition 23, les caractères étant compatibles,

$$\begin{aligned}
\lambda'(P') &= \chi'(\mathrm{nr}_{k'(\xi)/k'}(\xi))\psi'(\mathrm{tr}_{k'(\xi)/k'}(\xi)) \\
&= \chi(\mathrm{nr}_{k'(\xi)/k}(\xi))\psi(\mathrm{tr}_{k'(\xi)/k}(\xi)) \\
&= \chi(\mathrm{nr}_{k(\xi)/k} \circ \mathrm{nr}_{k'(\xi)/k(\xi)}(\xi))\psi(\mathrm{tr}_{k(\xi)/k} \circ \mathrm{tr}_{k'(\xi)/k(\xi)}(\xi)) \\
&= (\chi(\mathrm{nr}_{k(\xi)/k}(\xi))\psi(\mathrm{tr}_{k(\xi)/k}(\xi)))^{\nu/d} \\
&= \lambda(P)^{\nu/d}
\end{aligned}$$

car puisque

$$[k'(\xi) : k(\xi)] = \frac{[k'(\xi) : k]}{[k(\xi) : k]} = \frac{\mathrm{ppcm}\,(\deg P, \nu)}{\deg P} = \frac{\nu}{d}$$

d'après la proposition 6 et la multiplicité des degrés (parce que P est le polynôme minimal de ξ sur k, et P' celui de ξ sur k'), $\mathrm{nr}_{k'(\xi)/k(\xi)}(\xi) = \xi^{\nu/d}$ et $\mathrm{tr}_{k'(\xi)/k(\xi)}(\xi) = \frac{\nu}{d}\xi$. On remarque par ailleurs que $\deg(P') = [k'(\xi) : k'] = \frac{\deg(P)}{d}$, ce qui resservira dans la quatrième étape.
Troisième étape : quid des sommes de Gauss ?

Cette étape est indépendante des deux précédentes et le résultat est prouvé dans un corps fini quelconque k muni de caractères non triviaux : χ multiplicatif, ψ additif. On l'appliquera donc légitimement à k et à k'. On utilise de façon légèrement anticipée les résultats de la section **3.4** *sur les produits infinis de séries formelles.*

Montrons l'identité formelle suivante :

$$1 + g(\chi)U = \prod_{P \text{ irréductible unitaire}} \frac{1}{1 - \lambda(P)U^{\deg(P)}}.$$

On remarque tout d'abord que le produit est bien défini, car pour tout $\varepsilon > 0$ et tout P irréductible unitaire, si on note d la distance précédemment introduite sur les séries formelles, $d\left(1, \frac{1}{1-\lambda(P)U^{\deg(P)}}\right) = 2^{-\deg P} \leq \varepsilon$ sauf si $\deg(P) > -\log_2(\varepsilon)$, ce qui ne laisse qu'un nombre fini de renégats.

Notons maintenant I_n l'ensemble des polynômes irréductibles unitaires de $k[X]$ de degré au plus n, pour $n \geq 1$. On a alors :

$$1 + g(\chi)U = 1 + \sum_{\substack{P \in k[X] \\ \deg(P) \geq 1 \\ P \text{unitaire}}} \lambda(P)U^{\deg(P)}$$

comme on l'a évoqué à la première étape,

$$= 1 + \sum_{\substack{k \in \mathbf{N}^*, \alpha_1, \ldots, \alpha_k \in \mathbf{N}^* \\ P_1, \ldots, P_k \in k[X] \text{ irr. unit. dist.}}} \lambda(P_1)^{\alpha_1} \cdots \lambda(P_k)^{\alpha_k} U^{\alpha_1 \deg(P_1) + \ldots + \alpha_k \deg(P_k)}$$

grâce à la décomposition unique d'un polynôme en produit d'irréductibles,

$$= \lim_{n \to \infty} \sum_{E \subset I_n} \sum_{\alpha \in (\mathbf{N}^*)^{|E|}} \prod_{P \in E} (\lambda(P)U^{\deg P})^{\alpha(P)}$$

en groupant par degré du plus grand facteur irréductible,

$$= \lim_{n \to \infty} \sum_{\alpha \in \mathbf{N}^{|I_n|}} \prod_{P \in I_n} (\lambda(P)U^{\deg P})^{\alpha(P)}$$

$$= \lim_{n \to \infty} \prod_{P \in I_n} \sum_{\alpha \in \mathbf{N}} (\lambda(P)U^{\deg P})^{\alpha}$$

d'après la factorisation 90,

$$= \lim_{n \to \infty} \prod_{P \in I_n} \frac{1}{1 - \lambda(P)U^{\deg P}}$$

$$= \prod_{P \text{ irr.}} \frac{1}{1 - \lambda(P)U^{\deg(P)}}$$

d'après le lemme 95.

Quatrième étape : polynômes irréductibles de $k[X]$, de $k'[X]$. Soit φ l'application de l'ensemble des irréductibles de $k'[X]$ dans l'ensemble des irréductibles de $k[X]$ qui à P' donné associe le polynôme minimal sur k d'une de ses racines. Elle est bien définie, surjective et telle que chaque polynôme P a exactement d antécédents $P_1, \ldots, P_d$ qui vérifient chacun :

$$\lambda'(P_i)U^{\nu \deg(P_i)} = \left(\lambda(P)U^{\deg(P)}\right)^{\nu/d},$$

et qui ne sont antécédents d'aucun autre polynôme, d'après la remarque sur le degré et la séparabilité de l'extension à la fin de la deuxième étape (prouvée par la proposition 14), qui donne le nombre d d'antécédents. Cela donne, dans l'identité formelle de la troisième étape, en remplaçant U par U^ν :

$$1 + g'(\chi')U^\nu = \prod_{\substack{P \in k[X] \\ \text{irréductible}}} \prod_{\varphi^{-1}(P) = \{P_1, \ldots, P_d\}} \frac{1}{1 - \lambda'(P_i)U^{\nu \deg(P_i)}}$$

$$= \prod_{\substack{P \in k[X] \\ \text{irréductible}}} \frac{1}{\left[1 - \left(\lambda(P)U^{\deg(P)}\right)^{\nu/d}\right]^d}$$

On peut alors montrer l'identité polynomiale suivante, pour $d = \mathrm{pgcd}(\nu, n)$:

$$(1 - X^{\nu/d})^d = \prod_{k=0}^{\nu-1}(1 - Xe^{2i\pi nk/\nu}),$$

dont on déduit :

$$\begin{aligned}
1 + g'(\chi')U^\nu &= \prod_{k=0}^{\nu-1} \prod_{\substack{P\in k[X] \\ \text{irréductible}}} \frac{1}{1 - \lambda(P)(Ue^{2ik\pi\deg(P)/\nu})^{\deg(P)}} \\
&\quad \text{d'après l'identité pour } n = \deg(P), X = \lambda(P)U^{\deg(P)}, \\
&= \prod_{k=0}^{\nu-1}(1 + g(\chi)e^{2i\pi k/\nu}U) \\
&= 1 + (-1)^{\nu-1}g(\chi)^\nu U^\nu \\
&\quad \text{d'après l'identité pour } n = 1, X = -g(\chi)U.
\end{aligned}$$

D'où le théorème. □

Une autre forme de Hasse-Davenport Dans la section **2**, on utilisera en fait le théorème de Hasse-Davenport sous la forme équivalente suivante :

Théorème 1.4.3 *Soit des entiers $n, m \geq 1$ avec $n \mid m$, ie $k_m := \mathbf{F}_{q^m}$ est une extension de $k_n := \mathbf{F}_{q^n}$. On se donne un caractère additif ψ de k_n, et on pose $\psi' = \psi \circ \mathrm{tr}_{k_m/k_n}$ caractère additif de k_m. Soit w, w' générateurs respectifs de k_n^* et k_m^* tels que $\mathrm{nr}_{k_m/k_n}(w') = w$. Soit $a \in \mathbf{R}$ tel que $(q^n - 1)a \in \mathbf{Z}$, donc $(q^m - 1)a \in \mathbf{Z}$. On peut définir les caractères multiplicatifs χ_a et χ'_a de k_n et k_m, envoyant respectivement w et w' sur $e^{2i\pi a}$. Partant, on définit les sommes de Gauss $g(\chi_a)$ et $g'(\chi'_a)$ associées à ces constructions sur k_n et k_m.*

On a alors :

$$-g'(\chi'_a) = (-g(\chi_a))^{\frac{m}{n}}.$$

Preuve Il suffit d'établir que $\chi_a \circ \mathrm{nr}_{k_m/k_n} = \chi'_a$. Or, il s'agit de deux morphismes de groupes, qui coïncident en w', générateur de k_m^*, et en 0, donc qui coïncident sur k_m. □

2 Étude des hypersurfaces diagonales

2.1 Calcul du nombre de points des hypersurfaces diagonales

Notations On se place dans un corps fini $k = \mathbb{F}_q$. On se donne $r \geq 1$ un entier, $n_0, \ldots, n_r$ des entiers strictement positifs et $a_0, \ldots, a_r \in k^*$. On considère l'équation polynomiale dans k^{r+1} :

$$\sum_{i=0}^{r} a_i X_i^{n_i} = 0$$

On note N le nombre de ses solutions.

On fixe un générateur de k, de sorte que l'on peut définir le caractère multiplicatif χ_α pour $\alpha \in \frac{1}{q}\mathbb{Z}$, comme vu précédemment. On pose, pour $0 \leq i \leq r$, $d_i = \text{pgcd}(n_i, q-1)$. Posons enfin, pour $u = (u_0, \ldots, u_r) \in k^{r+1}$, $L(u) = \sum_{i=0}^{r} a_i u_i$ et $L'(u) = \sum_{i=0}^{r} u_i$.

On se propose de montrer le théorème suivant :

Théorème 2.1.4 *On a :*

$$N = q^r + (q-1) \sum_{\substack{\alpha \in]0;1[^{r+1} \\ d_i\alpha_i \in \mathbf{Z} \\ \alpha_0 + \ldots + \alpha_r \in \mathbf{Z}}} j(\alpha) \prod_{i=0}^{r} \chi_{\alpha_i}(a_i^{-1})$$

.

Expression de N On a de façon immédiate :

$$N = \sum_{\substack{u \in k^{r+1} \\ L(u)=0}} \prod_{i=0}^{r} |\{x \in k \mid x^{n_i} = u_i\}|,$$

de sorte que, d'après la proposition 25,

$$N = \sum_{\substack{u \in k^{r+1} \\ L(u)=0}} \prod_{i=0}^{r} \sum_{\alpha_i \in \frac{1}{d_i}[\![0;d_i-1]\!]} \chi_{\alpha_i}(u_i),$$

donc en développant, et en intervertissant les sommes,

Proposition 2.1.49 *On a :*

$$N = \sum_{\substack{\alpha \in [0;1[^{r+1} \\ d_i\alpha_i \in \mathbf{Z}}} \sum_{\substack{u \in k^{r+1} \\ L(u)=0}} \prod_{i=0}^{r} \chi_{\alpha_i}(u_i).$$

Soit désormais $\alpha \in [0,1[^{r+1}$ tel que $d_i\alpha_i \in \mathbf{Z}$ pour tout i.

Quid des α_i nuls ? Si $\alpha_i = 0$ pour tout i, alors :

$$\sum_{\substack{u \in k^{r+1} \\ L(u)=0}} \prod_{i=0}^{r} \chi_{\alpha_i}(u_i) = |\{u \in k^{r+1} | L(u) = 0\}| = q^r,$$

parce que le cardinal est celui de $L^{-1}(0)$, donc, L étant une forme linéaire non nulle sur k^{r+1}, c'est celui d'un hyperplan de k^{r+1}, donc q^r.

Soit $I \subset [\![0,r]\!]$ tel que $i \in I$ si et seulement si $\alpha_i = 0$, supposons I stricte non vide. Alors :

$$S := \sum_{\substack{u\in k^{r+1}\\ L(u)=0}} \prod_{i=0}^{r} \chi_{\alpha_i}(u_i) = \sum_{\substack{u_j\in k\\ \text{pour } j\notin I}} \sum_{\substack{u_l\in k\\ \text{pour } l\in I\\ L(u)=0}} \prod_{i\notin I} \chi_{\alpha_i}(u_i).$$

Observons que la deuxième somme est somme d'un terme constant, sur un sous-espace affine de k^{r+1} de dimension $|I|-1$. En effet, lorsque les $u_i, i \notin I$ sont fixés, l'espace des indices est exactement $\{(v_i) \in k^{r+1} \mid \forall i \notin I,\, v_i = u_i \text{ et } \sum_{i\in I} a_i v_i = -\sum_{i\notin I} a_i u_i\}$, de sorte que :

$$S = \sum_{\substack{u_j\in k\\ \text{pour } j\notin I}} q^{|I|-1} \prod_{i\notin I} \chi_{\alpha_i}(u_i) = q^{|I|-1} \prod_{i\notin I} \sum_{u\in k} \chi_{\alpha_i}(u) = 0,$$

parce que I n'est pas de complémentaire vide et que les χ_{α_i} sont tous non triviaux pour $i \notin I$. Finalement,

Proposition 2.1.50

$$N = q^r + \sum_{\substack{\alpha\in]0;1[^{r+1}\\ d_i\alpha_i\in\mathbf{Z}}} \sum_{\substack{u\in k^{r+1}\\ L(u)=0}} \prod_{i=0}^{r} \chi_{\alpha_i}(u_i)$$

Pour conclure Les deux lemmes suivants exploitent deux changements de variables intéressants.

Lemme 2.1.51 *Soit $\alpha \in]0;1[^{r+1}$ satisfaisant $d_i\alpha_i \in \mathbf{Z}$ pour tout $0 \le i \le r$. On a*

$$\sum_{\substack{u\in k^{r+1}\\ L(u)=0}} \prod_{i=0}^{r} \chi_{\alpha_i}(u_i) = \prod_{i=0}^{r} \chi_{\alpha_i}(a_i^{-1}) \sum_{\substack{u\in k^{r+1}\\ L'(u)=0}} \chi_{\alpha_i}(u_i)$$

Preuve En posant $v_i = a_i u_i$ pour chaque i, on définit une bijection de k^{r+1} dans k^{r+1}. On note qu'on a $L(u) = 0$ si et seulement si $L'(v) = 0$.

Le membre gauche de l'égalité s'écrit donc, par changement de variable,

$$\sum_{\substack{v\in k^{r+1}\\ L'(v)=0}} \prod_{i=0}^{r} \chi_{\alpha_i}(a_i^{-1}v_i) = \prod_{i=0}^{r} \chi_{\alpha_i}(a_i^{-1}) \sum_{\substack{u\in k^{r+1}\\ L'(u)=0}} \chi_{\alpha_i}(u_i).$$

□

Lemme 2.1.52 *Soit $\alpha \in]0;1[^{r+1}$ satisfaisant $d_i\alpha_i \in \mathbf{Z}$ pour tout $0 \le i \le r$. Si $\beta = L'(\alpha)$ n'est pas entier, alors :*

$$\sum_{\substack{u\in k^{r+1}\\ L'(u_i)=0}} \chi_{\alpha_i}(u_i) = 0.$$

Preuve Comme les termes correspondant à $u_0 = 0$ sont nuls, on peut supposer qu'on a en fait sommé sur les indices pour lesquels $u_0 \neq 0$. Notons S le membre gauche. On a :

$$S = \sum_{u_0\in k^*} \sum_{\substack{u_1,\dots,u_r\in k\\ u_0+\dots+u_r=0}} \prod_{i=0}^{r} \chi_{\alpha_i}(u_i),$$

donc en effectuant le changement de variable $u_i = u_0 v_i$ pour $1 \leq i \leq r$, on trouve :

$$\begin{aligned} S &= \sum_{u_0 \in k^*} \sum_{\substack{v_1,\ldots,v_r \in k \\ v_1+\ldots+v_r=-1}} \prod_{i=0}^{r} \chi_{\alpha_i}(u_0) \prod_{i=1}^{r} \chi_{\alpha_i}(v_i) \\ &= \sum_{u \in k^*} \sum_{\substack{v \in k^r \\ v_1+\ldots+v_r=-1}} \chi_\beta(u) \prod_{i=1}^{r} \chi_{\alpha_i}(v_i) \\ &= \sum_{u \in k^*} \chi_\beta(u) \sum_{\substack{v \in k^r \\ v_1+\ldots+v_r=-1}} \prod_{i=1}^{r} \chi_{\alpha_i}(v_i) \end{aligned}$$

Le premier facteur, puisque β est non entier, d'où χ_β non trivial, est nul, de sorte que $S = 0$. □

Si l'on se souvient des sommes de Jacobi précédemment introduites, en sommant sur les $(r+1)$-uplets α dans le lemme 51, ce qui précède donne finalement :

Théorème 2.1.5 *On a :*

$$N = q^r + (q-1) \sum_{\substack{\alpha \in]0;1[^{r+1} \\ d_i \alpha_i \in \mathbf{Z} \\ \alpha_0+\ldots+\alpha_r \in \mathbf{Z}}} j(\alpha) \prod_{i=0}^{r} \chi_{\alpha_i}(a_i^{-1})$$

Cette expression donne par exemple, grâce aux estimations de la première section :

Proposition 2.1.53 *On a l'inégalité :*

$$|N - q^r| \leq q^{\frac{r+1}{2}} \prod_{i=0}^{r} n_i.$$

2.2 Fonction zêta d'une hypersurface diagonale

On fixe maintenant $q = p^\nu$, pour $\nu \geq 1$, p premier, et on note, pour $n \geq 1$, $k_n = \mathbf{F}_{q^n} \supset \mathbf{F}_q$, et $k = k_1 = \mathbf{F}_q$. On se donne $r \geq 1$, des entiers strictement positifs $n_0, \ldots, n_r$, $a_0, \ldots a_r$ des éléments de k^*. On considère, pour chaque $n \geq 1$, l'équation polynomiale suivante dans k_n :

$$\sum_{i=0}^{r} a_i x_i^{n_i} = 0,$$

dont on note N_n le nombre de solutions.

Remarque 2.2.13 Quitte à appliquer séparément aux inconnues l'automorphisme de Frobenius $x \in k_n \longmapsto x^p \in k_n$ (ce qui ne changera aucun des N_n), on peut supposer que p ne divise aucun des n_i.

Définition La *fonction zêta* du polynôme $P = \sum_{i=0}^{r} a_i X_i^{n_i}$ est la série formelle rationnelle

$$\zeta_P = \exp\left(\sum_{n=1}^{\infty} \frac{N_n X^n}{n} \right).$$

Pour travailler avec des caractères sur nos extensions de corps et pouvoir appliquer le théorème de Hasse-Davenport, on a tout d'abord besoin de construire des caractères additifs

et des caractères multiplicatifs (donc pour commencer des générateurs) compatibles sur tous nos k_n. C'est le but des deux résultats suivants.

Système de générateurs et caractères additifs compatibles

Lemme 2.2.54 *Soient $m, n \geq 1$ avec $n \mid m$. Soit w un générateur de k_n^*. Alors il existe un $w' \in k_m$ qui engendre k_m^* tel que $\mathrm{nr}_{k_m/k_n}(w') = w$.*

Preuve Soit w_0 un générateur de k_m^*, alors sa norme sur k_n, w_1, engendre k_n^* : en effet, ses puissances couvrent l'ensemble des normes des puissances de w_0, donc l'ensemble des normes des éléments de k_m^*, donc k_n^*.

On dispose d'entiers $a, a' > 0$ tels que $w = w_1^a$, $w_1 = w^{a'}$. Il s'ensuit $w_1^{aa'-1} = 1$, donc, w_1 étant un générateur de k_n^*, $q^n - 1 \mid aa' - 1$, de sorte que a et $q^n - 1$ sont premiers entre eux.

Supposons tout d'abord que pour tout $t \in \mathbf{Z}$, $a + t(q^n - 1)$ ne soit pas premier avec $q^m - 1$. Posons, pour chaque diviseur r premier de $q^m - 1$ divisant l'un des $a + t(q^n - 1)$ (notamment r et $q^n - 1$ sont premiers entre eux), $A_r = \{t \in \mathbf{Z},\, r \mid a + t(q^n - 1)\}$. Soient p comme ci-dessus, $t \in A_r$, $t' \in \mathbf{Z}$. Alors

$$t' \in A_r \Leftrightarrow r \mid a + t'(q^n - 1) - a - t(q^n - 1) \Leftrightarrow r \mid (t' - t)(q^n - 1) \Leftrightarrow r \mid t - t',$$

par lemme de Gauss, de sorte que A_r est une progression arithmétique de raison r et l'hypothèse signifie que les A_r recouvrent $\mathbf{Z}$. Or, soit, pour chaque r premier diviseur de $q^m - 1$ et divisant l'un des $a + t(q^n - 1)$, $t_r \in A_r$. Par le lemme chinois, puisque les tels r sont des premiers deux à deux distincts en nombre fini, il existe un entier t_0 congru à $t_r + 1$ modulo r pour chaque r. Comme chaque A_r est une progression arithmétique de raison r contenant t_r, elle ne peut contenir t_0. C'est absurde.

Ainsi, il existe un entier t tel que $a + t(q^n - 1)$ soit premier avec $q^m - 1$. Quitte à rajouter un multiple de $(q^m - 1)$ à t, on suppose $t > 0$, et on pose $b = a + t(q^n - 1)$. Alors $w' = w_0^b$ est un générateur de k_m^* (en effet, b est premier avec $q^m - 1$ donc, pour un entier c, $bc - 1$ est divisible par $q^m - 1$, de sorte que $w'^c = w_0$, et donc w' générateur) de norme $w_1^a(w_1^{q^n-1})^t = w$. □

Proposition 2.2.55 *Il existe des familles $(\psi_n)_{n\geq 1}$ et $(w_n)_{n\geq 1}$ telles que :*

- *pour tout $n \geq 1$, ψ_n est un caractère additif non trivial de k_n ;*
- *pour tous $m, n \geq 1$ avec $n \mid m$, $\psi_m = \psi_n \circ \mathrm{tr}_{k_m/k_n}$;*
- *pour tout $n \geq 1$, w_n est un générateur de k_n^* ;*
- *pour tous $n, m \geq 1$ avec $n \mid m$, $\mathrm{nr}_{k_m/k_n}(w_m) = w_n$.*

Preuve On va d'abord le faire pour les caractères additifs. On se donne un caractère additif non trivial ψ_1 de k_1. On pose, pour tout $n \geq 1$, $\psi_n = \psi_1 \circ \mathrm{tr}_{k_n/k_1}$. Comme la trace est toujours surjective, ψ_n est un caractère additif non trivial de k_n. De plus, si $n \mid m$, alors $\psi_m = \psi_1 \circ \mathrm{tr}_{k_m/k_1} = \psi_1 \circ \mathrm{tr}_{k_n/k_1} \circ \mathrm{tr}_{k_m/k_n} = \psi_n \circ \mathrm{tr}_{k_m/k_n}$. C'est bon.

Reste les générateurs. D'après le lemme précédent, on construit par récurrence une suite $(v_n)_{n\geq 1}$ telle que pour tout n, v_n soit un générateur de $k_{n!}$ et si $n \geq 1$, $\mathrm{nr}_{k_{(n+1)!}/k_{n!}}(v_{n+1}) = v_n$. Soient d un entier, $n \geq 1$ tel que $d \mid n!$. On a :

$$\mathrm{nr}_{k_{(n+1)!}/k_d}(v_{n+1}) = \mathrm{nr}_{k_{n!}/k_d}(\mathrm{nr}_{k_{(n+1)!}/k_{n!}}(v_{n+1})) = \mathrm{nr}_{k_{n!}/k_d}(v_n).$$

Par conséquent, pour tout entier d, la quantité $\mathrm{nr}_{k_{n!}/k_d}(v_n) \in k_d$ ne dépend pas de l'entier n tel que $d \mid n!$, on la note w_d. Notamment, $w_d = \mathrm{nr}_{k_{d!}/k_d}(v_d)$, engendre k_d^* par un raisonnement déjà fait ci-dessus.

Ainsi, soient $m, n \geq 1$ avec $n \mid m$. Alors

$$\mathrm{nr}_{k_m/k_n}(w_m) = \mathrm{nr}_{k_m/k_n}(\mathrm{nr}_{k_{m!}/k_m}(v_m)) = \mathrm{nr}_{k_{m!}/k_n}(v_m) = w_n,$$

parce que $n \mid m!$. □

Dans toute la suite, on figera de telles familles : alors les notations des caractères de k_n seront relatives au générateur w_n, les sommes de Gauss dans k_n seront relatives au caractère ψ_n.

Rationalité de ζ_P On observe que $DL(\zeta_P) = \sum_{n\geq 1} N_n X^{n-1}$. De la sorte,

$$X \cdot DL(\zeta_P) = \sum_{n\geq 1} X^n \left((q^n)^r + (q^n-1) \sum_{\substack{(\star) \\ (q^n-1)\alpha_i \in \mathbf{Z}}} j^{k_n}(\alpha) \prod_{i=0}^{r} \chi_{\alpha_i}^{k_n}(a_i^{-1}) \right),$$

où $(\star)$ correspond à sommer sur les $\alpha \in]0,1[^{r+1}$ tels que $L'(\alpha) \in \mathbf{Z}$ et $\forall\, i \in [\![0,r]\!]$, $n_i\alpha_i \in \mathbf{Z}$.
Définition Tout α vérifiant $(\star)$ est dit *sommé*. Pour α sommé, on pose :

$$S(\alpha) = \sum_{\substack{n\geq 1 \\ (q^n-1)\alpha_i \in \mathbf{Z}}} (q^n-1) X^n j^{k_n}(\alpha) \prod_{i=0}^{r} \chi_{\alpha_i}^{k_n}(a_i^{-1}).$$

Ainsi,

$$X \cdot DL(\zeta_P) = \frac{q^r X}{1-q^r X} + \sum_{(\star)} S(\alpha).$$

Lemme 2.2.56 *Soit α sommé. Alors il existe un entier $\mu(\alpha) \geq 1$ tel que :*

$$\{n \geq 1 \mid \forall\, i \in [\![0,r]\!],\ (q^n-1)\alpha_i \in \mathbf{Z}\} = \mu(\alpha)\mathbf{N}^*.$$

Preuve Soit $0 \leq i \leq r$. Constatons que dans $\mathbf{R}/\mathbf{Z}$, α_i est d'ordre fini (diviseur de n_i) : soit ω_i son ordre. Soit $X_i = \{n \geq 1 \mid (q^n-1)\alpha_i \in \mathbf{Z}\}$. Alors $X_i = \{n \geq 1,\ \omega_i \mid q^n-1\}$. Observons que $n_i \mid q^{\phi(n_i)}-1$, donc X_i est non vide. On dispose donc de $m_i = \min X_i$.

Si $a \in X_i$, alors ω_i divise q^a-1, $q^{m_i}-1$ donc d'après le lemme 8, si on note $d_i = \mathrm{pgcd}(a, m_i)$, on a $\omega_i \mid q^{d_i}-1$, d'où $d_i \in X_i$. On en déduit que $d_i \geq m_i$, donc $m_i \mid a$. Réciproquement, si $m_i \mid a$, $a \geq 1$, alors $\omega_i \mid q^{m_i}-1 \mid q^a-1$ donc $a \in X_i$, donc $X_i = m_i\mathbf{N}^*$. Finalement,

$$\{n \geq 1 \mid \forall\, i \in [\![0,r]\!],\ (q^n-1)\alpha_i \in \mathbf{Z}\} = \bigcap_{i=0}^{r} X_i = \bigcap_{i=0}^{r} m_i\mathbf{N}^* = \left(\operatorname*{ppcm}_{0\leq i\leq r} m_i\right)\mathbf{N}^*.$$

□

Lemme 2.2.57 *Soit α sommé. Soient $m = \mu(\alpha)$, $t \geq 1$, $n = tm$. Alors pour $0 \leq i \leq r$, $\chi_{\alpha_i}^{k_n}(a_i^{-1}) = \chi_{\alpha_i}^{k_m}(a_i^{-1})^t$, et $j^{k_n}(\alpha) = (-1)^{r-1}((-1)^{r-1}j^{k_m}(\alpha))^t$*

Preuve On a $\chi_{\alpha_i}^{k_n}(a_i^{-1}) = \chi_{\alpha_i}^{k_m}(\mathrm{nr}_{k_n/k_m}(a_i^{-1})) = \chi_{\alpha_i}^{k_m}(a_i^{-t}) = \chi_{\alpha_i}^{k_m}(a_i^{-1})^t$, parce que, par construction des générateurs, les caractères dans différents corps de même indice sont compatibles.

D'après la forme alternative du théorème de Davenport et Hasse,

$$g^{k_n}(\chi_{\alpha_i}) = (-1)^{t-1}(g^{k_m}(\chi_{\alpha_i}))^t.$$

En effectuant le produit, pour $0 \leq i \leq r$, on obtient $q^n j^{k_n}(\alpha) = (-1)^{(t-1)(r+1)}(q^m j^{k_m}(\alpha))^t$, donc finalement $j^{k_n}(\alpha) = (-1)^{(r-1)(t+1)}(j^{k_m}(\alpha))^t$, d'où le résultat. □

On peut maintenant calculer $S(\alpha)$ pour chaque α sommé. On a alors :

$$\begin{aligned}
S(\alpha) &= (-1)^{r-1}\sum_{t\geq 1}(q^{t\mu(\alpha)}-1)\left((-1)^{r-1}X^{\mu(\alpha)}j^{k_{\mu(\alpha)}}(\alpha)\prod_{i=0}^{r}\chi_{\alpha_i}^{k_{\mu(\alpha)}}(a_i^{-1})\right)^t \\
&= (-1)^{r-1}\left(\frac{q^{\mu(\alpha)}C(\alpha)X^{\mu(\alpha)}}{1-q^{\mu(\alpha)}C(\alpha)X^{\mu(\alpha)}}-\frac{C(\alpha)X^{\mu(\alpha)}}{1-C(\alpha)X^{\mu(\alpha)}}\right) \\
&\text{où } C(\alpha) := (-1)^{r-1}j^{k_{\mu(\alpha)}}(\alpha)\prod_{i=0}^{r}\chi_{\alpha_i}^{k_{\mu(\alpha)}}(a_i^{-1}) \\
&= \frac{(-1)^r}{\mu(\alpha)}X\left(DL\left(1-q^{\mu(\alpha)}C(\alpha)X^{\mu(\alpha)}\right)-DL\left(1-C(\alpha)X^{\mu(\alpha)}\right)\right)
\end{aligned}$$

Il reste encore à sommer sur α avant d'obtenir le résultat final.

Définition On appelle *quasi-sommé* un $(r+1)$-uplet α de non-entiers tel que pour chaque i, $n_i\alpha_i \in \mathbf{Z}$ et tel que $L'(\alpha) \in \mathbf{Z}$. On dit que deux quasi-sommés α et β sont *identiques* si $\alpha - \beta \in \mathbf{Z}^{r+1}$ (ie s'ils ont même réduction modulo 1).

On s'autorise à étendre les définitions des fonctions j, C, S aux quasi-sommés (de fait, si deux quasi-sommés sont identiques, les valeurs coïncident).

Remarque 2.2.14 On fait les constats suivants.

(*i*) Observons que si α est quasi-sommé, $q^t\alpha$ l'est également. En effet, soit $t \geq 1$: si $q^t\alpha_i \in \mathbf{Z}$, n_i étant par hypothèse premier avec p, l'est avec q^t, donc il existe $u, v \in \mathbf{Z}$ tels que $uq^t + vn_i = 1$, donc $\alpha_i = u(q^t\alpha_i) + v(n_i\alpha_i) \in \mathbf{Z}$, ce qui est impossible, et le reste est clair.

(*ii*) De plus, pour α quasi-sommé, $t > t' \geq 0$, on a $q^t\alpha$ et $q^{t'}\alpha$ identiques si et seulement si pour tout i, $(q^{t-t'}-1)q^{t'}\alpha_i \in \mathbf{Z}$, donc, comme précédemment, si et seulement si $(q^{t-t'}-1)\alpha_i \in \mathbf{Z}$ pour chaque i, donc si, et seulement si $t = t' \mod \mu(\alpha)$. Notons que cette propriété implique que $\mu(q\alpha) = \mu(\alpha)$.

(*iii*) Enfin, lorsque α est un quasi-sommé, comme $a_i^q = a_i$, et puisque $x \longmapsto x^q$ est un automorphisme de corps de chaque k_n, on a $j^{k_{\mu(q\alpha)}}(q\alpha) = j^{k_{\mu(\alpha)}}(\alpha)$, et il s'ensuit que $C(q\alpha) = C(\alpha)$, et finalement que $S(q\alpha) = S(\alpha)$.

Finalement, en regroupant les $q^t\alpha$ pour chaque sommé, qui sont exactement au nombre de $\mu(\alpha)$, on obtient que la somme des $S(\alpha)$ pour α sommé est une somme de termes de la forme $(-1)^r X \cdot DL\left(\frac{1-q^{\mu(\alpha)}C(\alpha)X^{\mu(\alpha))}}{1-C(\alpha)X^{\mu(\alpha)}}\right)$. Finalement,

$$DL(\zeta_P) = -DL\left(\frac{1}{1-q^rX}\right) + (-1)^r DL\left(\prod_{\alpha}\frac{1-q^{\mu(\alpha)}C(\alpha)X^{\mu(\alpha)}}{1-C(\alpha)X^{\mu(\alpha)}}\right).$$

On a effectué le produit sur l'ensemble des sommés α quotienté par la relation d'équivalence « être identiques ou différer multiplicativement d'une puissance de q ». Par unicité de la « primitive logarithmique » à facteur constant près, on a donc établi la rationalité de la fonction ζ pour les hypersurfaces diagonales.

En notant de plus que $j(\alpha), \chi(\alpha), C(\alpha)$ sont toujours des entiers algébriques et que $C(\alpha)$ est de module $q^{\mu(\alpha)\frac{r-1}{2}}$, on établit le :

Théorème 2.2.6 *Pour une hypersurface diagonale P, ζ_P est une fraction rationnelle à coefficients entiers dont les pôles et les zéros sont des inverses d'entiers algébriques de module $q^{-\frac{r\pm 1}{2}}$ ou q^{-r}.*

Remarque 2.2.15 Le fait que les coefficients de la fraction rationnelle soient entiers découle du fait qu'ils soient entiers algébriques (comme produits, sommes, d'entiers algébriques) et

rationnels (quitte à redévelopper la fraction rationnelle en la série formelle qui définit ζ_P et qui est, elle, à coefficients rationnels).

Remarque 2.2.16 Dans l'article [Wei49] , Weil étudie une fonction ζ légèrement différente : il impose l'homogénéité du polynôme P et note N_n le nombre de zéros de P dans l'espace projectif de dimension r associé à l'équation. Le problème est essentiellement le même.

2.3 Vers une généralisation

Partant de ces propriétés remarquables de la fonction ζ associée à une hypersurface diagonale, Weil formule trois conjectures, que nous sommes maintenant en mesure d'énoncer.

Énoncé des conjectures de Weil Soit I un idéal de l'anneau $\mathbf{F}_q[X_0, \ldots, X_r]$. On dispose de $P_1, \ldots, P_m$ qui engendrent I d'après le théorème de la base de Hilbert. Supposons que les P_i sont homogènes et que, pour tout x annulant tous les P_i, la matrice $\left(\frac{\partial P_i}{\partial X_j}(x)\right)_{i,j}$ est de rang maximal. Pour $n \in \mathbf{N}^*$, notons N_n le cardinal de $\{x \in (\mathbf{F}_{q^n}^{r+1} \setminus \{0\})/\mathbf{F}_{q^n}^* \mid \forall\, P \in I,\ P(x) = 0\}$ et définissons la fonction zêta de I :

$$\zeta(X) = \exp\left(\sum_{n\geq 1} N_n \frac{X^n}{n}\right).$$

On a alors :

Rationalité ζ est une fraction rationnelle à coefficients entiers. On peut la factoriser :

$$\zeta(X) = \frac{\prod(1-\alpha_i X)}{\prod(1-\beta_j X)}.$$

Les α_i et β_j sont appelées les *valeurs caractéristiques* de la fonction ζ.

Hypothèse de Riemann Les modules des valeurs caractéristiques sont de la forme $q^{h/2}$ pour $h \in [\![1, 2d-1]\!]$ pour un certain d entier minimal (avec h pair pour les α_i, h impair pour les β_j). Si on note b_h le degré du polynôme à coefficients entiers

$$P_h = \begin{cases} \displaystyle\prod_{|\alpha_i| = q^{h/2}} (1-\alpha_i X) & \text{si } h \text{ pair,} \\ \displaystyle\prod_{|\beta_j| = q^{h/2}} (1-\beta_j X) & \text{sinon,} \end{cases}$$

on définit $\chi := \sum(-1)^h b_h$ la *caractéristique d'Euler-Poincaré* associée à I.

Équation fonctionnelle Il existe $\varepsilon \in \{\pm 1\}$ tel que :

$$\zeta_P\left(\frac{1}{q^d X}\right) = \varepsilon q^{d\chi/2} X^{\chi_P} \zeta_P(X).$$

Remarque 2.3.17 La première conjecture est vraie, plus généralement, dans le cadre affine : pour I un idéal de $\mathbf{F}_{q^n}[X_1, \ldots, X_r]$ sans condition de non-singularité, et N_n le cardinal de $\{x \in \mathbf{F}_{q^n}^r \mid \forall\, P \in I,\ P(x) = 0\}$.

Tous ces résultats ont également été prouvés pour des courbes avec des méthodes « élémentaires ». [6] La fin du rapport est dévouée à la preuve du premier point. Les deux suivants ont été prouvés avec des outils de géométrie algébrique par Pierre Deligne en 1973. Une preuve reposant sur des méthodes p-adiques a été proposée récemment [7] par Kiran Kedlaya dans [Ked02], mais nous ne l'avons pas étudiée.

6. Weil y fait déjà référence dans l'article de 1949.
7. en 2001

3 Quelques résultats d'analyse p-adique

3.1 Des rudiments sur les anneaux valués

Valeur absolue sur un anneau

Dans ce paragraphe, on considère des anneaux intègres (c'est-à-dire commutatifs et sans diviseurs de zéro) qui seront la plupart du temps des corps. Le cas des anneaux est évoqué seulement en vue de l'étude de produits infinis dans section **3.4**, qui permet de justifier le calcul délicat de la section **1.4**.

Définition Soit A un anneau. On appelle *valeur absolue* sur A une application $|\cdot| : A \to \mathbf{R}^+$ satisfaisant :

- $\forall\, x \in A,\ |x| = 0 \Leftrightarrow x = 0$
- $\forall\, x, y \in A,\ |xy| = |x||y|$
- $\forall\, x, y \in A,\ |x + y| \leq |x| + |y|$

Remarque 3.1.18 Si A est un anneau et $|\cdot|$ une valeur absolue sur A, $|1| = |-1| = 1$.

Remarque 3.1.19 Soient A un anneau, $|\cdot|$ une valeur absolue sur A,

$$d : (x, y) \in A^2 \longmapsto |x - y|$$

est une distance sur A. A et, plus généralement, tous les A^n sont donc naturellement munis d'une structure d'espace métrique, donc topologique, pour laquelle toutes les opérations sont continues.

En particulier toutes les applications polynomiales sur A^n sont continues, et $|\cdot| : A \to \mathbf{R}^+$ est 1-lipschitzienne.

Définition Une valeur absolue $|\cdot|$ sur l'anneau A est *ultramétrique* si on a :

$$\forall x, y \in A,\ |x + y| \leq \max(|x|, |y|).$$

Dorénavant et dans toute la sous-section, on ne considère que des corps.

Complété d'un corps muni d'une valeur absolue

Lorsqu'un corps est muni d'une valeur absolue, on peut se demander s'il est complet, ou du moins si *a minima* on peut le plonger [8] dans un surcorps complet. De telles interrogations doivent être familières au lecteur habitué à construire $\mathbf{R}$ comme complété de $\mathbf{Q}$ pour la valeur absolue usuelle. Sans grande surprise, le théorème suivant dit que ce résultat se généralise à K et $|\cdot|$ quelconques.

Théorème 3.1.7 *Soient K un corps, $|\cdot|$ une valeur absolue sur K. Il existe un corps L, une application $i : K \to L$, et une valeur absolue $||\cdot||$ sur L tels que :*

(i) L est complet pour la métrique induite par $||\cdot||$;

(ii) $i : (K, |\cdot|) \to (L, ||\cdot||)$ est un morphisme isométrique d'anneaux ;

(iii) $i(K)$ est dense dans L.

8. tout en préservant sa structure et sa valeur absolue bien sûr

De plus, si deux triplets $(L_1, i_1, ||\cdot||_1)$ et $(L_2, i_2, ||\cdot||_2)$ vérifient cela, il existe un isomorphisme isométrique $\phi : L_1 \to L_2$ tel que $\phi \circ i_1 = i_2$.

Définition Le corps L, muni du morphisme i et de la valeur absolue $||\cdot||$, est appelé le *complété* de K pour la valeur absolue $|\cdot|$. On verra toujours K comme un sous-corps dense de L.

Un élément de preuve du théorème est le lemme topologique suivant. Une fois établie l'existence d'un complété métrique de K, il permet en effet de prolonger continûment les opérations de K à son complété métrique. On obtient alors les propriétés des opérations dans ledit complété par densité.

Lemme 3.1.58 *Soient A, C deux espaces métriques, B une partie dense de A, $f : B \to C$. On suppose que f envoie toute suite (à valeurs dans B) convergeant dans A sur une suite convergente dans C. Alors il existe $g : A \to C$ continue prolongeant f.*

Remarque 3.1.20 Noter que la valeur absolue obtenue sur le complété est ultramétrique si, et seulement si, la valeur absolue sur le corps de départ l'était.

On va montrer que le passage au complété, qui est un phénomène topologique, préserve une importante propriété algébrique : celle d'être algébriquement clos.

Lemme 3.1.59 *Soient K un corps, $|\cdot|$ une valeur absolue sur K,*

$$P = X^d + \sum_{k=0}^{d-1} a_k X^k \in K[X],$$

$z \in K$ avec $P(z) = 0$. Alors

$$|z| \leq \max\left(1, \sum_{k=0}^{d-1} |a_k|\right).$$

Si $|\cdot|$ est ultramétrique, on a même $|z| \leq \max\limits_{0 \leq i \leq d} a_i$.

Théorème 3.1.8 *Soient K un corps algébriquement clos, $|\cdot|$ une valeur absolue sur K, $L \supset K$ son complété, pour la valeur absolue $||\cdot||$. Alors L est algébriquement clos.*

Preuve Soit $P = X^d + \sum\limits_{k=0}^{d-1} b_k X^k \in L[X]$. Pour $0 \leq k \leq d-1$, on dispose d'une suite $(a_{k,n})_n \in K^{\mathbf{N}}$ de limite b_k. Cette suite est majorée par un certain $M_k \geq 0$. Soient :

$$B = 1 + \sum_{k=0}^{d-1} M_k \geq 1, \quad P_n = X^d + \sum_{k=0}^{d-1} a_{k,n} X^k \in K[X].$$

Notons $z_{1,n}, \ldots z_{d,n}$ les zéros de P_n ; d'après le lemme 59, $||z_{k,n}|| \leq B$ pour tous k, n.

Observons de plus que, si $m, n \in \mathbf{N}$, $1 \leq k \leq d$, on a $(\star)$:

$$\begin{aligned}
\min_{1 \leq i \leq d} ||z_{k,m} - z_{i,n}|| &\leq \left(\prod_{i=1}^{d} ||z_{k,m} - z_{i,n}||\right)^{1/d} \\
&= ||P_n(z_{k,m}) - P_m(z_{k,m})||^{1/d} \\
&\leq \left(\sum_{i=0}^{d-1} ||a_{i,m} - a_{i,n}||\, ||z_{k,m}||^i\right)^{1/d} \\
&\leq B \left(\sum_{i=0}^{d-1} ||a_{i,m} - b_i|| + ||b_i - a_{i,n}||\right)^{1/d}.
\end{aligned}$$

Pour $p \in \mathbf{N}$, on dispose d'un entier N_p tel que pour tout $q \geq N_p$ et tout i,

$$||b_i - a_{i,q}|| \leq \frac{1}{dB^d 2^{pd+1}}.$$

Quitte à augmenter artificiellement N_p, on peut supposer (N_p) strictement croissante. Soit (i_n) définie par récurrence par $i_0 \in [\![1, d]\!]$, et $i_{p+1} \in [\![1, d]\!]$ tel que $||z_{i_{p+1},N_{p+1}} - z_{i_p,N_p}||$ soit minimal. Alors, par $(\star)$, $||z_{i_{p+1},N_{p+1}} - z_{i_p,N_p}|| \leq \frac{1}{2^p}$, de sorte que $(z_{i_p,N_p})_p$ est de Cauchy dans L, donc converge vers un $\zeta \in L$.

Dès lors, pour $p, q \in \mathbf{N}, q \geq N_p$, on a par $(*)$: $||P_q(z_{i_p,N_p})|| \leq 2^{-pd}$, donc en faisant tendre q vers l'infini, $||P(z_{i_p,N_p})|| \leq 2^{-pd}$, puis en faisant tendre p vers l'infini, $||P(\zeta)|| = 0$, donc P possède une racine (dans L). □

Espaces vectoriels de dimension finie sur un corps localement compact

On fixe un corps K et une valeur absolue $|\cdot|$ sur K non constante sur K^*. On se propose ici de généraliser les résultats de topologie usuels sur des espaces vectoriels de dimension finie sur $\mathbf{R}$ et $\mathbf{C}$ à des espaces vectoriels de dimension finie sur des corps plus généraux. On commence par étudier les corps localement compacts, puis les normes sur les espaces vectoriels de dimension finie sur de tels corps.

Admettons tout d'abord ce lemme, qui resservira par la suite.

Lemme 3.1.60 *$\{|x| \mid x \in K^*\}$ est un sous-groupe de $\mathbf{R}^{+*}$ auquel 0 et ∞ sont adhérents.*

Proposition 3.1.61 *S'équivalent :*

(i) K est localement compact

(ii) Dans K, 0 possède un voisinage compact.

(iii) Les parties bornées de K sont relativement compactes.

Preuve Que (i) implique (ii) est évident. Que (iii) implique (i) l'est aussi (car les $\{x \in K \mid |x - a| \leq \varepsilon\}$ pour $a \in K$ fixe, $\varepsilon > 0$, forment un système fondamental de voisinages fermés bornés de a).

Supposons donc que 0 possède un voisinage compact V. Alors, pour un $r > 0$, l'ensemble $\{x \in K \mid |x| \leq r\}$ est une partie fermée (dans K donc dans V) du compact V, donc est compacte. Soit maintenant $B \subset K$ bornée. Alors $\overline{B}$ est fermée, bornée, donc incluse dans un $W = \{x \mid |x| \leq R\}$ pour un $R > 0$. Soit $\lambda \in K^*$ avec $|\lambda| > \frac{R}{r}$, alors W est un fermé inclus dans λV, qui est image du compact V par l'application continue $x \in K \longmapsto \lambda x$, donc est compact. W est un fermé inclus dans un compact, donc est compact, donc $\overline{B}$ est également compact. □

Dans la suite du paragraphe, on suppose K localement compact. On veut établir sur les K-espaces vectoriels de dimension finie les mêmes résultats que dans les cas réel et complexe.

Définition Soit E un K-espace vectoriel. On appelle *norme* sur E toute application $N : E \to \mathbf{R}^+$ telle que :

(i) $\forall x \in E,\ N(x) = 0 \Leftrightarrow x = 0.$

(ii) $\forall x \in E,\ \forall \lambda \in K, N(\lambda x) = |\lambda| N(x).$

(iii) $\forall x, y \in E,\ N(x + y) \leq N(x) + N(y).$

Remarque 3.1.21 Soient E un K-espace vectoriel, N norme sur E, alors

$$(a, b) \in E^2 \longmapsto N(a - b)$$

est une distance sur E, qui munit donc E d'une topologie telle que toutes les opérations usuelles d'espace vectoriel (en un nombre fini d'arguments, qu'ils soient dans E, dans K, ou les deux) sont continues.

Définition Soient E un K-espace vectoriel de dimension finie, $(e_i)_{1\leq i\leq d}$ une base de E. On considère

$$||\cdot||_\infty : \sum_{i=1}^{d} \lambda_i e_i \in E \longmapsto \max_{1\leq k\leq d} |\lambda_i| \in \mathbf{R}_+.$$

Cette application est une norme sur E, pour laquelle les parties compactes sont exactement les parties fermées bornées. On l'appelle la *norme infinie* subordonnée à $|\cdot|$ sur E.

Preuve Soit $X \subset E$ fermée bornée, montrons qu'elle est compacte. Soit $(x_n) = \left(\sum \lambda_{i,n} e_i\right)_n$ une suite dans $X \subset \{x \mid ||x||_\infty \leq M\}$ pour un certain $M \geq 0$. Alors, à i fixé, les suites $(\lambda_{i,n})$, sont bornées par M dans K et en nombre fini : on dispose d'une extractrice ϕ telle que pour chaque i, $(\lambda_{i,\phi(n)})$ converge vers un $\mu_i \in K$. Par continuité des opérations, $(x_{\phi(n)})$ converge vers $y := \sum \mu_i e_i$. Comme X est fermée, $y \in X$, donc $(x_{\phi(n)})$ converge dans X. □

Théorème 3.1.9 *Soit E un K-espace vectoriel de dimension finie.*

(i) Si N, N' sont deux normes sur E, il existe $A, B > 0$ telles que $AN' \leq N \leq BN'$, autrement dit ces deux normes sont équivalentes*.*

(ii) Toutes les normes définissent la même topologie sur E, appelée topologie naturelle de K-espace vectoriel de dimension finie. Toutes les normes sur E définissent les mêmes parties bornées.

(iii) Pour la topologie naturelle de E, les parties compactes sont exactement les parties fermées bornées.

(iv) Si F est un K-espace vectoriel normé de dimension finie, si $f \in \mathcal{L}(E, F)$, f est continue pour les topologies naturelles.

(v) Si F est un sous-espace de E, sa topologie naturelle est induite par la topologie naturelle de E.

(vi) Si F est un sous-espace de E, F est fermé dans E.

Preuve Montrons tout d'abord (i). Fixons une base $(e_1, \ldots, e_d)$ de E, et considérons la norme $||\cdot||_\infty$ du lemme précédent. Soit N une norme sur E.

Pour $x_1, \ldots x_d \in K$, on a

$$N\left(\sum_{i=1}^{d} x_i e_i\right) \leq \sum_{i=1}^{d} |x_i| N(e_i) \leq \sum_{i=1}^{d} N(e_i) ||x||_\infty.$$

On dispose donc de $C > 0$ tel que $N \leq C||\cdot||_\infty$. Par conséquent, pour la topologie induite par $||\cdot||_\infty$, N est continue. Elle envoie $\{x \in E \mid ||x||_\infty = 1\}$ (fermé borné de E pour $||\cdot||_\infty$ donc compact, qui ne contient pas 0) sur un compact de $\mathbf{R}_+^*$. En particulier, il existe $C' > 0$ tel que, si $||x||_\infty = 1$, $N(x) \geq C'$. Soit enfin $x = \sum x_i e_i \in E$ non nul : il existe i tel que $|x_i| = ||x||_\infty \neq 0$, donc :

$$N(x) = |x_i| \cdot ||x_i^{-1} x||_\infty \geq |x_i| C' = C' ||x||_\infty.$$

Finalement, pour les constantes $C, C' < 0$, $C'||\cdot||_\infty \leq N \leq C||\cdot||_\infty$.

Si N' est une autre norme sur E, on a également des constantes $D, D' > 0$ telles que $D'||\cdot||_\infty \leq N' \leq D||\cdot||_\infty$. Il s'ensuit que

$$\frac{D'}{C} N \leq N' \leq \frac{D}{C'} N.$$

Les points (ii) et (iii) découlent du lemme et du premier point. Montrons les trois points restants :

(iv) : soient N norme sur E, N' norme sur F : alors on vérifie que $x \in E \longmapsto N(x)+N'(f(x))$ est une norme sur E, donc est majorée par un $A \cdot N$ pour un $A > 0$. Ainsi, on a $N'(f(x)-f(y)) = N'(f(x-y)) \leq AN(x-y)$, donc f est continue (car lipschitzienne) pour les normes données. On conclut par (ii).

(v) : si N est une norme sur E, la restriction de N à F est une norme sur F, donc induit sur F la topologie naturelle, mais aussi la restriction de la topologie naturelle de E, d'où le résultat.

(vi) : soit Y un supplémentaire de F. Soit $p \in \mathcal{L}(E,Y)$ la projection sur Y parallèlement à F. Comme Y et E sont de dimension finie, p est continue, donc $F = \text{Ker } p$ est fermé.

□

3.2 Le corps $\mathbf{Q}_p$

On a évoqué dans le paragraphe précédent la construction de $\mathbf{R}$ comme complété de $\mathbf{Q}$ pour la valeur absolue usuelle. Dans cette sous-section, on construit un nouveau corps complet, $\mathbf{Q}_p$, comme complétion de $\mathbf{Q}$ pour une autre valeur absolue : la valeur absolue p-adique. Jusqu'à la fin de la section **3**, p désigne un nombre premier quelconque.

Construction de $\mathbf{Q}_p$

Définition Pour un entier $n \in \mathbf{Z}$, et un nombre premier p, on note $v_p(n)$ le plus grand $r \in \mathbf{N} \cup \{\infty\}$ tel que $p^r \mid n$. C'est la *valuation p-adique* de n. On munit $\mathbf{N} \cup \{\infty\}$ des opérations d'addition, de soustraction et de multiplication usuelles. Pour $x = \frac{a}{b}$ un rationnel écrit sous forme irréductible, on pose $v_p(x) = v_p(a) - v_p(b)$.

On admet les lemmes d'arithmétique élémentaire suivants :

Lemme 3.2.62 *Si $a, b \in \mathbf{Z}$, $v_p(ab) = v_p(a) + v_p(b)$, et $v_p(a+b) \geq \min(v_p(a), v_p(b))$.*

Lemme 3.2.63 *Si $a, b \in \mathbf{Z}$, $b \neq 0$, $v_p\left(\frac{a}{b}\right) = v_p(a) - v_p(b)$.*

Proposition 3.2.64 *$|\cdot|_p : x \in \mathbf{Q} \longmapsto p^{-v_p(x)}$ est une valeur absolue ultramétrique sur $\mathbf{Q}$.*

Preuve Si $x, y \in \mathbf{Q}$, on peut écrire $x = \frac{u}{w}, v = \frac{v}{w}$, $u, v, w \in \mathbf{Z}, w \geq 1$. Alors

$$\begin{aligned} v_p(x+y) &= v_p\left(\frac{u+v}{w}\right) \\ &= v_p(u+v) - v_p(w) \\ &\geq \min(v_p(u), v_p(v)) - v_p(w) \\ &= \min(v_p(u) - v_p(w), v_p(v) - v_p(w)) \\ &= \min(v_p(x), v_p(y)). \end{aligned}$$

D'autre part,

$$v_p(xy) = v_p\left(\frac{uv}{w^2}\right) = v_p(uv) - v_p(w^2) = v_p(u) - v_p(w) + v_p(v) - v_p(w) = v_p(x) + v_p(y).$$

Pour conclure, on multiplie ces deux résultats membre à membre par $-\log(p)$ et on applique l'exponentielle. □

Définition On note $\mathbf{Q}_p$ le complété de $\mathbf{Q}$ pour la valeur absolue p-adique $|\cdot|_p$ sur $\mathbf{Q}$. Dans la suite, on voit $\mathbf{Q}$ comme un sous-corps dense de $\mathbf{Q}_p$. On note alors, sans ambiguïté, $|\cdot|_p$ la valeur absolue ultramétrique induite sur $\mathbf{Q}_p$.

Topologie de $\mathbf{Q}_p$

Il s'agit ici de montrer que $\mathbf{Q}_p$ est localement compact. On en profite pour établir en cours de route plusieurs résultats intéressants sur sa topologie naturelle.

Lemme 3.2.65 *On a l'égalité* $\{|x|_p \mid x \in \mathbf{Q}_p\} = \{|x|_p \mid x \in \mathbf{Q}\} = \{p^a \mid -\infty \leq a < +\infty\}$.

Preuve Remarquons que comme $\mathbf{Q}$ est dense dans $\mathbf{Q}_p$, $\{|x|_p \mid x \in \mathbf{Q}_p\} \subset \overline{\{|x|_p \mid x \in \mathbf{Q}\}}$. Or $\{|x|_p \mid x \in \mathbf{Q}\} = \{p^a \mid a \in \mathbf{Z} \cup \{-\infty\}\}$, donc cet ensemble est fermé. □

Proposition 3.2.66 *Soit* (x_n) *suite d'éléments de* $\mathbf{Q}_p$ *convergeant vers un* $y \in \mathbf{Q}_p^*$. *Alors* $(|x_n|_p)$ *stationne à* $|y|_p$.

Preuve Le seul point d'accumulation de l'espace topologique $\{|z|_p \mid z \in \mathbf{Q}_p\}$ est zéro. □

Proposition 3.2.67 $\mathbf{Q}_p$ *est totalement discontinu.*

Preuve Supposons l'inverse : il existe $a, b \in \mathbf{Q}_p$ distincts contenus dans un connexe C de $\mathbf{Q}_p$. Alors $C' = \frac{1}{b-a}(C - a)$ est connexe et contient 0 et 1. Pour $x \in \mathbf{Q}_p$, $C_x = xC'$ est connexe et contient 0 et x, donc x est dans la composante connexe de 0. Ainsi, $\mathbf{Q}_p$ est connexe. Or, son image par $|\cdot|_p$, qui est continue, est totalement discontinue et non réduite à un point : c'est absurde. □

Définition Pour $a \in \mathbf{Q}, r \in \mathbf{R}_+$, on note $\mathcal{B}(a; r) := \{x \in \mathbf{Q} \mid |x - a|_p \leq r\}$ la *boule fermée* de centre a et de rayon r pour la valeur absolue p-adique $|\cdot|_p$ dans $\mathbf{Q}$.

Lemme 3.2.68 *Munissons* $\mathbf{Q}$ *de sa valeur absolue p-adique. Alors* $\mathcal{B}(0; 1)$ *est recouverte par p boules fermées de rayon* $\frac{1}{p}$.

Preuve Soit $r = \frac{a}{b}$ un rationnel écrit sous forme irréductible, avec $|r|_p \leq 1 : v_p(a) \geq v_p(b)$. Comme a et b sont premiers entre eux, $v_p(b) = 0$, donc b est premier avec p, donc possède un inverse modulo p, noté c. Soit $d \in [\![0, p-1]\!]$ le reste de ac modulo p :

$$|r - d|_p \leq \max\left(\left|\frac{a}{b} - ac\right|_p, |ac - d|_p\right).$$

Or, $|ac - d|_p \leq \frac{1}{p}$ car $p \mid ac - d$. D'autre part, b étant un entier premier avec p, $|b|_p = 1$; a étant entier, $|a|_p \leq 1$, de sorte que $\left|\frac{a}{b} - ac\right|_p \leq |1 - bc|_p \leq \frac{1}{p}$, car $1 - bc$ est un entier divisible par p. Finalement,

$$\frac{a}{b} \in \bigcup_{d=0}^{p-1} \mathcal{B}\left(d; \frac{1}{p}\right).$$

□

Lemme 3.2.69 *Soit* $a \in \mathbf{Z}$. *Une boule de rayon* p^a *dans* $\mathbf{Q}$ *pour la valeur absolue p-adique peut être recouverte par p boules de rayon* p^{a-1}.

Preuve On applique une transformation affine pour ramener le[9] centre de la boule à 0, et le rayon de la boule à 1. On utilise ensuite le lemme précédent. □

Corollaire 3.2.70 *Soient* $a \in \mathbf{Z}, r \in \mathbf{N}$. *Toute boule fermée dans* $\mathbf{Q}$ *de rayon* p^a *peut être couverte par* p^r *boules de rayon* p^{a-r}.

Tous les résultats que nous venons d'établir sont également valables pour des boules ouvertes de $\mathbf{Q}$. Que peut-on dire des boules dans $\mathbf{Q}_p$?

Lemme 3.2.71 *Soient* $q \in \mathbf{Q}$, $r > 0$. *La boule* $\mathcal{B}_p$ *fermée de* $\mathbf{Q}_p$ *de centre q et de rayon r est l'adhérence dans* $\mathbf{Q}_p$ *de la boule* $\mathcal{B}$ *fermée dans* $\mathbf{Q}$ *de centre q et de rayon r*.

Preuve Notons $\overline{\mathcal{B}}$ l'adhérence dans $\mathbf{Q}_p$ de $\mathcal{B}$. Comme $\mathcal{B}_p$ est un fermé de $\mathbf{Q}_p$ contenant $\mathcal{B}$, on a l'inclusion indirecte : $\mathcal{B}_p \supset \overline{\mathcal{B}}$.

Inversement, soit $z \in \mathbf{Q}_p$ avec $|z - q|_p \leq r$. Si $z = q$, $z \in \overline{\mathcal{B}}$. Supposons $z - q \neq 0$: on dispose d'une suite (r_n) de rationnels de limite z, et on a $r_n - q \longrightarrow z - q \neq 0$, donc la suite

9. ou plutôt « un », *cf* proposition 85

$(|r_n - q|_p)$ stationne à $|z-q|_p \leq r$, de sorte qu'à partir d'un certain rang r_n est dans $\mathcal{B}$, donc z est dans $\overline{\mathcal{B}}$. □

On peut en venir au résultat désiré :

Théorème 3.2.10 *$\mathbf{Q}_p$ est localement compact.*

Preuve Il suffit de montrer que la boule fermée de centre 0 et de rayon 1 de $\mathbf{Q}_p$ est précompacte : en effet, le cas échéant, comme c'est un fermé du complet $\mathbf{Q}_p$, elle est complète donc elle serait compacte. 0 possèderait donc un voisinage compact, ce qui conclurait.

Soit $r > 0$. Soit $a \in \mathbf{Z}_-$ avec $p^a \leq r$. D'après le corollaire 70, la boule fermée de centre 0 et de rayon 1 de $\mathbf{Q}$ est incluse dans une réunion finie de boules fermées de centre rationnel et de rayon p^a, mettons :

$$\mathcal{B}_{\mathbf{Q}}(0;1) \subset \bigcup_{i=1}^{s} \mathcal{B}_{\mathbf{Q}}(q_i; p^a).$$

Passons aux adhérences dans $\mathbf{Q}_p$: par le lemme précédent et comme cette opération préserve les unions finies, on a :

$$\mathcal{B}_{\mathbf{Q}_p}(0;1) \subset \bigcup_{i=1}^{s} \mathcal{B}_{\mathbf{Q}_p}(q_i; p^a) \subset \bigcup_{i=1}^{s} \mathcal{B}_{\mathbf{Q}_p}(q_i, r),$$

ce qui conclut. □

Entiers p-adiques

On peut légitimement s'interroger sur la notation $\mathbf{Q}_p$. En effet, pourquoi parler de « rationnels » p-adiques si l'on n'a pas de notion d'entiers p-adiques ? Dans ce paragraphe, on comble cette lacune en définissant $\mathbf{Z}_p$ et en indiquant ses liens avec $\mathbf{Q}_p$.

Définition On définit l'ensemble $\mathbf{Z}_p$ des *entiers p-adiques* comme l'adhérence dans $\mathbf{Q}_p$ de son sous-anneau $\mathbf{Z}$.

Lemme 3.2.72 *$\mathbf{Z}_p \subset \{n \in \mathbf{Q}_p \mid |n|_p \leq 1\}$ est un sous-anneau compact de $\mathbf{Q}_p$.*

Preuve L'inclusion et la compacité sont claires.

D'autre part, soient $x, y \in \mathbf{Z}_p$. x et y sont limites p-adiques respectivement des suites $(u_n) \in \mathbf{Z}^{\mathbf{N}}$, $(v_n) \in \mathbf{Z}^{\mathbf{N}}$. Alors $x-y, xy \in \mathbf{Q}_p$ sont limites des suites d'entiers $u-v$, uv, donc sont dans $\mathbf{Z}_p$. Enfin, $1 \in \mathbf{Z} \subset \mathbf{Z}_p$, ce qui conclut. □

Lemme 3.2.73 *Pour tout $n \geq 1$, si on munit $\mathbf{Z}/p^n\mathbf{Z}$ de la topologie discrète, il existe un morphisme continu d'anneaux $r_n : \mathbf{Z}_p \to \mathbf{Z}/p^n\mathbf{Z}$, dit de réduction modulo p^n, satisfaisant :*

- *si $n \geq 1$, $x \in \mathbf{Z}$, $r_n(x)$ est la réduction modulo p^n de x ;*
- *si $n \geq m \geq 1$, si $p_{n,m}$ est la projection de $\mathbf{Z}/p^n\mathbf{Z}$ dans $\mathbf{Z}/p^m\mathbf{Z}$, on a $p_{n,m} \circ r_n = r_m$.*

Preuve On observe que la réduction modulo p^n « naturelle » de $\mathbf{Z}$ dans $\mathbf{Z}/p^n\mathbf{Z}$ envoie une suite de Cauchy de $(\mathbf{Z}, |\cdot|_p)$ sur une suite stationnaire de $\mathbf{Z}/p^n\mathbf{Z}$. On applique le lemme topologique de prolongement 58 pour passer de $\mathbf{Z}$ à $\mathbf{Z}_p$. Les propriétés voulues sont vraies dans $\mathbf{Z}$ et continues, par densité de $\mathbf{Z}$ dans $\mathbf{Z}_p$ elles sont donc vraies dans $\mathbf{Z}_p$. □

Le théorème suivant caractérise complètement la structure d'anneau topologique de $\mathbf{Z}_p$ en tant que la « limite projective » des $\mathbf{Z}/p^n\mathbf{Z}$. L'idée en est la suivant : un entier p-adique est entièrement déterminé par la suite de ses réductions modulo p^n, pour peu que celles-ci soient compatibles au sens du second point du lemme 73.

Théorème 3.2.11 *Soit $P = \{(u_n)_{n\geq 1} \in \prod_{n\geq 1} \mathbf{Z}/p^n\mathbf{Z} \mid \forall n \geq m \geq 1,\ p_{n,m}(u_n) = u_m\}$. On le munit de la topologie induite par la topologie produit et de la structure de sous-anneau induite par la structure d'anneau produit de $\prod_{n\geq 1} \mathbf{Z}/p^n\mathbf{Z}$.*

Alors l'application $\phi : x \in \mathbf{Z}_p \longmapsto (r_n(x))_{n\geq 1} \in P$ est un homéomorphisme et un isomorphisme d'anneaux.

Preuve Puisque $\mathbf{Z}_p$ est compact et que P est sous-espace d'un produit d'espaces séparés, donc est séparé, et que notre application est clairement continue et clairement un morphisme d'anneaux par la proposition précédente, il suffit d'en montrer la bijectivité.

Soit $(u_n)_{n\geq 1} \in P$; soit, pour $n \geq 1$, $b_n \in [\![0, p^n[\![$ congru à u_n modulo p^n. Alors, si $m \geq n$, comme $p_{m,n}(u_m) = u_n$, b_n et b_m sont congrus modulo p^n. Donc $|b_n - b_m|_p \leq p^{-\min(m,n)}$ pour tous $m, n \geq 1$. Ainsi b est de Cauchy, notons $l \in \mathbf{Z}_p$ sa limite. Si $m \geq n$, $r_n(b_m) = u_n$ par construction, donc en passant à la limite $r_n(l) = u_n$ pour tout n, et $\phi(l) = u$, d'où la surjectivité.

Pour l'injectivité, soit $l \in \mathbf{Z}_p \cap \ker \phi$, on dispose d'une suite $(b_n) \in \mathbf{Z}^{\mathbf{N}}$ d'entiers de limite l dans $(\mathbf{Z}_p, |\cdot|_p)$. Si $n \geq 1$, $r_n(l) = 0$, donc $r_n(b_m) \underset{m\to+\infty}{\longrightarrow} 0$. Comme $\mathbf{Z}/p^n\mathbf{Z}$ est discret, $p^n \mid b_m$, ie $|b_m|_p \leq p^{-n}$, pour m assez grand. Donc $|l|_p \leq p^{-n}$, donc $l = 0$. □

Remarque 3.2.22 C'est ce résultat qui sert parfois de définition aux entiers p-adiques, notamment dans les nombreux ouvrages où l'on fait remarquer qu'un entier p-adique est un entier dont l'écriture en base p a potentiellement « une infinité de chiffres à gauche ». Pour une telle exposition des p-adiques, partant de $\mathbf{Z}_p$ pour définir $\mathbf{Q}_p$ puis montrer qu'il s'agit de la complétion de $\mathbf{Q}$ pour la valeur absolue p-adique, le lecteur curieux peut se référer à [Ami75].

Proposition 3.2.74 *Les inversibles de $\mathbf{Z}_p$ sont exactement les $l \in \mathbf{Z}_p$ tels que $r_1(l) \neq 0$.*

Preuve D'après le théorème 11, on peut raisonner dans P. Soit $(u_n)_{n\geq 1} \in P$. Si u_1 est nul, clairement u n'est pas inversible dans P.

Si u_1 est non nul, alors, pour $n \geq 1$, soit $b_n \in \mathbf{Z}$ un représentant de u_n modulo p^n. On a $r_1(b_n) = u_1 \neq 0$ donc b_n et p sont premiers entre eux, donc u_n possède un inverse $v_n \in \mathbf{Z}/p^n\mathbf{Z}$, et $(v_n)_{n\geq 1} \in P$ (il vérifie bien la condition de recollement par unicité de l'inverse) et $uv = 1_P$, ce qui conclut. □

Lemme 3.2.75 *$p\mathbf{Z}_p$ est exactement l'ensemble des $x \in \mathbf{Z}_p$ tels que $r_1(x) = 0$.*

Preuve Soit $x \in Z_p$ avec $r_1(x) = 0$. Pour $n \geq 1$, soit b_n un représentant de $r_n(x)$ modulo p^n. Comme $r_1(b_n) = 0$, b_n s'écrit $c_{n-1}p$, pour tout $n \geq 2$. Soient $m \geq n \geq 2$. Comme $c_{n-1}p = b_n$ et $c_{m-1}p = b_m$ sont congrus l'un à l'autre modulo p^n, c_{n-1} et c_{m-1} sont congrus modulo p^{n-1}. Soit $y \in \mathbf{Z}_p$ défini par $\phi(y) = (r_n(c_n))_{n\geq 1}$. On vérifie sans peine que $x = py \in p\mathbf{Z}_p$.

D'autre part, si $y \in \mathbf{Z}_p$, $r_1(py) = r_1(p)r_1(y) = 0$, ce qui conclut. □

Le prochain corollaire donne une structure très générale et très intéressante sur $\mathbf{Z}_p$, celle d'anneau local, qu'on ne présentera pas dans son cadre général ici. [10]

Corollaire 3.2.76 *$p\mathbf{Z}_p$ est le plus grand des idéaux propres de $\mathbf{Z}_p$.*

Preuve C'est un idéal propre (il ne contient pas 1, car p n'est pas inversible) qui contient tous les non-inversibles, et maximal puisque tout idéal propre d'un anneau est inclus dans l'ensemble des non-inversibles. □

Le théorème suivant détaille le lien entre $\mathbf{Q}_p$ et $\mathbf{Z}_p$.

Théorème 3.2.12 *$\mathbf{Z}_p$ est l'ensemble des $x \in \mathbf{Q}_p$ avec $|x|_p \leq 1$.*

Preuve L'inclusion directe a déjà été évoquée avec le lemme 72.

Voyons la réciproque : soit $x \in \mathbf{Q}_p$ avec $|x|_p \leq 1$. Si $x = 0$, $x \in \mathbf{Z}_p$. Sinon, x est limite p-adique de rationnels $r_n = \frac{a_n}{b_n}$ avec a_n et b_n premiers entre eux et $b_n > 0$. Pour n assez grand, on a alors $|r_n|_p = |x|_p \leq 1$. Par conséquent, comme $|a_n|_p, |b_n|_p \leq 1$ et que l'un des deux vaut 1, on doit avoir $|b_n|_p = 1$. Donc p ne divise pas b_n, donc $r_1(b_n) \neq 0$, donc $b_n^{-1} \in \mathbf{Z}_p$, donc $r_n \in \mathbf{Z}_p$, et $\mathbf{Z}_p$ est fermé, donc on a bien $x \in \mathbf{Z}_p$. □

Corollaire 3.2.77 *Soit $x \in \mathbf{Z}_p$. x est inversible dans $\mathbf{Z}_p$ si, et seulement si, $|x|_p = 1$.*

Preuve Si $|x|_p = 1$, $x \neq 0$ et $|x^{-1}|_p = 1$ donc $x^{-1} \in \mathbf{Z}_p$. Si $x \in (\mathbf{Z}_p)^*$, $|x^{-1}|_p \leq 1$, donc $|x|_p \geq 1$, donc $|x|_p = 1$. □

10. même si on la rencontrera à nouveau dans la sous-section **3.5**

Corollaire 3.2.78 *Soit $x \in \mathbf{Q}_p$ non nul. Il existe un unique couple $(n,u) \in \mathbf{Z} \times (\mathbf{Z}_p)^*$ avec $x = p^n u$.*

Preuve Si $x = p^n u = p^m v$ sont deux telles décompositions, on a $p^{-n} = |p^n|_p = |p^n u|_p = |p^m v|_p = |p^m|_p = p^{-m}$ donc $m = n$, donc $u = v$, d'où l'unicité.

Pour l'existence, soit n tel que $p^n = |x|_p$, alors $|p^n x|_p = 1$ donc $p^n x \in (\mathbf{Z}_p)^*$, de sorte que $x = p^{-n}(p^n x)$. □

Corollaire 3.2.79 *$\mathbf{Q}_p$ est le corps des fractions de $\mathbf{Z}_p$.*

3.3 Polynômes dans $\mathbf{Z}_p$ et $\mathbf{Q}_p$

On prouve quelques résultats sur les polynômes sur $\mathbf{Q}_p$, qui serviront par la suite.

Lemme 3.3.80 *Soit $P \in \mathbf{Z}_p[X]$ irréductible. Alors P est aussi irréductible dans $\mathbf{Q}_p[X]$.*

Preuve Par l'absurde, supposons $P = QR$ avec $Q, R \in \mathbf{Q}_p[X]$ chacun de degré non nul. Tout élément de $\mathbf{Q}_p^*$ s'écrivant $x = up^v$, où $u \in \mathbf{Z}_p$ est inversible dans $\mathbf{Z}_p$ et $v \in \mathbf{Z}$ est la valuation p-adique de x, on peut poser m et n entiers minimaux tels que $\tilde{Q} := p^n Q, \tilde{R} := p^m R \in \mathbf{Z}_p[X]$.

Alors $p^{m+n} P = \tilde{Q}\tilde{R}$: si $m + n \leq 0$, c'est gagné. Sinon, on réduit l'égalité dans $\mathbf{F}_p[X]$, où $\tilde{Q}$ et $\tilde{R}$ sont non nuls par hypothèse de minimalité de n, m. Or, leur produit est nul, ce qui contredit l'intégrité de $\mathbf{F}_p[X]$.

Donc P est bien irréductible dans $\mathbf{Q}_p[X]$. □

Par ailleurs, on aura besoin par la suite du lemme de Hensel. Il s'agit d'un résultat permettant de relever de racine d'un polynôme d'un corps résiduel dans le corps de base, sous certaines conditions. On l'énonce ici dans un cas un peu particulier.

Lemme 3.3.81 *Soit K un corps complet muni d'une valeur absolue ultramétrique telle que $|p| = p^{-1}$ et que tout $x \in K^*$ a pour valeur absolue une puissance entière de p. Introduisons son sous-anneau $A = \{x \in K \mid |x| \leq 1\}$ et $M = \{x \in K \mid |x| < 1\}$ l'unique idéal maximal de A.*[11] *Alors, si $P \in A[X]$ admet une racine γ dans A/M telle que $P'(\gamma) \neq 0$ dans A/M, il existe un unique $x \in A$ relevant γ tel que $P(x) = 0$ (dans K).*

Preuve Pour l'existence, on va construire une suite de Cauchy qui tend vers la solution. Posons $x_1 \in \gamma$, et définissons par récurrence $x_{k+1} = x_k - P'(x_k)^{-1} P(x_k) \in A$ pour tout $k \in \mathbf{N}$. On montre par récurrence que la suite est bien définie, que $P(x_k) \in p^k A$ et que $P'(x_k) \in A \setminus M$ pour tout $k \in \mathbf{N}^*$.

C'est bon pour $k = 1$. Soit $k \in \mathbf{N}^*$ vérifiant cela. Alors $P'(x_k)$ est de valeur absolue 1, donc inversible dans A, donc x_{k+1} est bien défini et dans A. D'après la formule de Taylor polynomiale,

$$\begin{aligned} P(x_{k+1}) &= P(x_k) + (x_{k+1} - x_k)P'(x_k) + \sum_{i \geq 2} (x_{k+1} - x_k)^i \frac{P^{(i)}(x_k)}{i!} \\ &= \sum_{i \geq 2} (x_{k+1} - x_k)^i \frac{P^{(i)}(x_k)}{i!}, \end{aligned}$$

ce qui appartient à $p^{2k} A \subset p^{k+1} A$ car, pour $i \geq 2$, $\frac{P^{(i)}(x_k)}{i!}$ est dans A (en effet, si $P = \sum_t a_t X^t$, alors $\frac{1}{i!} P^{(i)}(x_k) = \sum_t \binom{t+i}{i} a_{t+i} x_k^t$).

De façon analogue, on voit que $P'(x_{k+1}) - P'(x_k) \in pA$, d'où $|P'(x_{k+1})| = 1$. La récurrence se propage. Finalement, pour tout $k, n \in \mathbf{N}^*$,

$$|x_{n+k} - x_k| \leq p^{-k}$$

11. la définition de ces objets A et M est établie en détail dans le second paragraphe de la sous-section **3.5**

donc la suite (x_k) est de Cauchy, donc elle converge vers un certain $x \in A$ tel que

$$P(x) \in \bigcap \overline{p^k A} = \{0\}$$

(vu la définition de $p^k A$ avec la valeur absolue), et $|x - x_1| < 1$ donc $x \in [x_1] = \gamma$. On note que $P'(x) \in A$ par continuité de P' et de la valeur absolue.

Pour l'unicité, on raisonne par l'absurde, on écrit la formule de Taylor pour nos deux racines x et y, on divise tout par $y - x$ et on obtient une identité qui contredit l'inversibilité de $P'(x)$. □

3.4 Topologie, sommation et produits dans un anneau valué ultramétrique

Compléments de topologie ultramétrique

Ce paragraphe donne un bref aperçu des propriétés singulières des valeurs absolues ultramétriques. On considère un anneau intègre A muni d'une valeur absolue ultramétrique $|\cdot|$.

Lemme 3.4.82 *Soient $x_1, x_2, x_3 \in A$ de somme nulle. L'ensemble des i tels que $|x_i|$ est maximal est de cardinal au moins deux.*

Preuve Cet ensemble est clairement non vide. On peut quitte à renommer dire que le maximum est atteint en $i = 1$. Alors $|x_1| = |x_2 + x_3| \leq \max(|x_2|, |x_3|)$, donc $|x_1| \leq |x_i|$ pour un i égal à 2 ou 3, de sorte que $|x_2|$ ou $|x_3|$ est également le maximum. □

Corollaire 3.4.83 *Tout triangle de A est isocèle. D'autre part, si $x, y \in A$ vérifient $|x| \neq |y|$, alors $|x + y| = \max(|x|, |y|)$.*

Preuve Le premier point est une interprétation du lemme.

Pour le second, quitte à renommer on peut supposer $|x| > |y|$. Soit $z = -x - y$: on sait que le maximum des modules de x,y,z est atteint par au moins deux des trois : or $|x| > |y|$, donc $|y|$ n'est pas ce maximum, donc il s'ensuit que $\max(|x|, |y|) = |x| = |z| = |x + y|$. □

Mentionnons un autre corollaire, qui généralise un résultat vu dans la section **3.2** :

Corollaire 3.4.84 *Si $a \in A^{\mathbf{N}}$ tend vers $b \in A$ non nul, alors $(|a_n|)_n$ stationne à $|b|$.*

Preuve Pour n assez grand, $|a_n - b| < |b|$, donc $|a_n| = |b + (a_n - b)| = |b|$. □

Proposition 3.4.85 *Soient $x \in A$, $r > 0$, $y \in \mathcal{B}(x; r)$, alors $\mathcal{B}(x; r) = \mathcal{B}(y; r)$, et de même pour les boules ouvertes.*

Preuve On le fait seulement pour les boules fermées, c'est la même preuve pour les boules ouvertes. Soit $z \in \mathcal{B}(x; r)$. Alors $|y - z| \leq \max(|y - x|, |x - z|) \leq r$ (car y, z sont dans la boule de centre x et de rayon r, donc $z \in \mathcal{B}_f(y; r)$). Finalement, $\mathcal{B}(x; r) \subset \mathcal{B}(y; r)$. Donc $x \in \mathcal{B}_f(y; r)$, de sorte que comme ci-dessus $\mathcal{B}(y; r) \subset \mathcal{B}(x; r)$, ce qui conclut. □

Un réel intérêt topologique des valeurs absolues ultramétriques apparaît dans la proposition suivante, qui est évidemment fausse pour la valeur absolue usuelle sur $\mathbf{R}$ ou $\mathbf{C}$:

Proposition 3.4.86 *Supposons A complet. Soit $\sum_{n \geq 0} a_n$ une série à coefficients dans A. Cette série est convergente si et seulement si $|a_n| \to 0$. Le cas échéant, si on note S sa somme, on a en outre*

$$|S| \leq \sup_{n \geq 0} |a_n|.$$

Preuve Le sens direct est clair. Pour le sens réciproque, il suffit d'appliquer le critère de Cauchy et l'inégalité ultramétrique. Enfin, on a

$$\left| \sum_{i=0}^{n} a_i \right| \leq \max_{0 \leq i \leq n} |a_i| \leq \sup_{i \in \mathbf{N}} |a_i|,$$

et on passe à la limite. □

Attention : on est tenté de penser qu'on vient de montrer que la série harmonique [12] posséderait enfin une limite dans $\mathbf{Q}_p$. C'est un raisonnement très hâtif ! En effet, la notion de convergence est radicalement différente dans $\mathbf{Q}$ pour la valeur absolue usuelle et la valeur absolue p-adique : un rationnel est « p-adiquement petit » s'il est « très divisible par p », ce qui est complètement indépendant de la question de son module. On va lister quelques exemples :

(*i*) (q^{-n}), pour un entier $q \geq 2$, tend vers l'infini dans $\mathbf{Q}_p$ si $p \mid q$ et est de norme constante égale à 1 sinon (et ne converge pas car $|q^{-n} - q^{-n-1}|_p = |q|_p^{-n-1}|q-1|_p = |q-1|_p$). En revanche, cette suite tend vers 0 dans $\mathbf{Q}$ pour la valeur absolue usuelle (qu'on appelle la *valeur absolue archimédienne*) sur $\mathbf{Q}$;

(*ii*) $(n!)$ tend vers 0 dans $\mathbf{Q}_p$ car pour $n \geq p^2$, la formule de Legendre permet de montrer que $|n!|_p \leq (p^{-1/p})^n$;

(*iii*) $\left(\frac{1}{n}\right)$ est minorée en valeur absolue par 1, en particulier la série harmonique diverge dans $\mathbf{Q}_p$;

(*iv*) Si $q > p$ est premier, $\left(\left(\frac{p}{q}\right)^n\right)$ tend vers 0 dans $\mathbf{Q}$ au sens des valeurs absolues p-adique et archimédienne ;

(*v*) $\left(\left(1 + \frac{1}{p^n-1}\right)^{p^n-1}\right)$ tend vers $e \notin \mathbf{Q}$ pour la valeur absolue archimédienne, mais vers 0 pour la valeur absolue p-adique ;

(*vi*) $(u_n) = \left(\left(1 + \frac{1}{p^n-1}\right)^n\right)$ tend vers 1 pour la valeur absolue archimédienne mais vers 0 au sens p-adique. A l'inverse, $(1-u_n)$ tend vers 1 au sens p-adique mais vers 0 au sens archimédien.

Sommabilité dans un anneau complet ultramétrique

Dans cette section, on considère un anneau (comme toujours, commutatif, unitaire, intègre) A muni d'une valeur absolue ultramétrique $|\cdot|$ qui le rend complet, par exemple $A = \mathbf{Q}_p, A = \mathbf{C}_p, A = K[\![X]\!]$, où K est un corps de caractéristique nulle. On cherche à utiliser la caractérisation des séries convergentes et l'inégalité ultramétrique pour aboutir, comme dans $\mathbf{R}$ ou $\mathbf{C}$, à une théorie des familles sommables. Néanmoins, cette théorie s'avère bien plus simple dans ce cadre que dans le cas archimédien. Dans tout le paragraphe, on se donne D un ensemble dénombrable infini. [13]

Proposition 3.4.87 *Soient $u \in A^{\mathbf{N}}$ de limite nulle, $f : \mathbf{N} \longmapsto \mathbf{N}$ une bijection. Alors les séries $\sum_{n\geq 0} u_n$ et $\sum_{n\geq 0} u_{f(n)}$ convergent et possèdent la même somme.*

Preuve Comme $f(n) \underset{n\to\infty}{\longrightarrow} +\infty$, $u_{f(n)}$ tend vers zéro, d'où la convergence.

Soit $\varepsilon > 0$. Soit $N_0 \geq 0$ tel que si $n \geq N_0$, $|u_n| \leq \varepsilon$. Soit $N = \max\left(\max f^{-1}([\![0, N_0]\!]), N_0\right)$. Soit $N_1 = \max\left(\max f([\![0, N]\!]), N\right)$. Soit $p \geq N_1$. Par inégalité ultramétrique,

$$\left|\sum_{n=0}^{p} u_n - \sum_{n=0}^{N_1} u_n\right| \leq \varepsilon, \text{ d'où } \left|\sum_{n=0}^{\infty} u_n - \sum_{n=0}^{N_1} u_n\right| \leq \varepsilon.$$

D'autre part,

$$\left|\sum_{n=0}^{N_1} u_n - \sum_{n=0}^{N} u_{f(n)}\right| = \left|\sum_{n\in[\![0;N_1]\!]\setminus f([\![0;N]\!])} u_n\right| \leq \sup_{n\in[\![0;N_1]\!]\setminus f([\![0;N]\!])} |u_n|.$$

12. par exemple
13. toutes les propositions qu'on établies ici étant par ailleurs clairement vraies pour un ensemble fini

Soit donc $n \in [\![0; N_1]\!] \backslash f([\![0; N]\!])$. Alors, $n \notin f([\![0; N]\!]) \supset f(f^{-1}([\![0; N_0]\!]))$ donc $n > N_0$ et $|u_n| \leq \varepsilon$. D'autre part, si $p > N$, $f(p) \geq N_0$, donc $|u_{f(p)}| \leq \varepsilon$. Finalement, pour $p \geq N$, on déduit par inégalité ultramétrique :

$$\left| \sum_{n=0}^{+\infty} u_n - \sum_{n=0}^{p} u_{f(n)} \right| \leq \varepsilon,$$

ce qui conclut. □

Corollaire 3.4.88 *Soit $u \in A^D$. Supposons que u tend vers 0 au sens où, pour tout $\varepsilon > 0$, il existe $F \subset D$ finie telle que pour tout $n \notin F$, $|u_n| \leq \varepsilon$.*

Alors il existe une quantité $S \in A$, telle que pour toute bijection f de $\mathbf{N}$ dans D, $\sum_{n \geq 0} u_{f(n)}$ converge et soit de somme S. On note $S = \sum_{n \in D} u_n$.

Preuve Comme $f, g : \mathbf{N} \to D$ sont bijectives, $(u_{f(n)})$ et $(u_{g(n)})$ tendent vers 0, et $u_{g(n)} = u_{f(f^{-1} \circ g(n))}$, où $f^{-1} \circ g$ est une bijection de $\mathbf{N}$ dans $\mathbf{N}$. On conclut par la proposition. □

Remarque 3.4.23 La formule de changement de variable est inchangée : soit E dénombrable, $u \in A^E$ tendant vers 0, $f : D \to E$ bijective. Alors $(u_{f(n)})_{n \in D}$ tend vers 0 et

$$\sum_{n \in D} u_{f(n)} = \sum_{n \in E} u_n$$

Remarque 3.4.24 L'application

$$(u \in A^D \text{ tendant vers } 0) \longmapsto \sum_{n \in D} u_n$$

est linéaire et 1-lipschitzienne pour la norme infinie au départ.

Lemme 3.4.89 *Soit (F_n) une suite croissante de parties finies de D avec $\bigcup_{n \geq 0} F_n = D$, $u \in A^D$ tendant vers 0. Alors :*

$$\sum_{p \in F_n} u_p \underset{n \to +\infty}{\to} \sum_{d \in D} u_d.$$

Preuve Quitte à appliquer une bijection de $\mathbf{N}$ sur D, on peut supposer que $D = \mathbf{N}$. Soit $\varepsilon > 0$, soit $N_0 \in \mathbf{N}$ tel que si $n \geq N_0$, $|u_n| \leq \varepsilon$. Soit $N_1 \in \mathbf{N}$ tel que $[\![0, N_0 - 1]\!] \subset F_{N_1}$. Pour $p \geq \max F_{N_1}$, on a :

$$\left| \sum_{i=0}^{p} u_i - \sum_{i \in F_{N_1}} u_i \right| = \left| \sum_{i \in [\![0;p]\!] \backslash F_{N_1}} \right| \leq \max_{i \in [\![0;p]\!] \backslash F_{N_1}} |u_i| \leq \max_{i \geq N_0} |u_i| \leq \varepsilon,$$

donc en faisant tendre p vers l'infini il vient

$$\left| \sum_{n \in \mathbf{N}} u_n - \sum_{n \in F_{N_1}} u_i \right| \leq \varepsilon$$

□

Ce lemme a deux conséquences : le corollaire juste ci-dessous, et le résultat [14] dit « d'associativité des sommes » qui correspond à la proposition 91. Il est beaucoup plus simple à énoncer et à manipuler pour une valeur absolue ultramétrique que pour une valeur absolue archimédienne.

14. important dans le cas archimédien

Corollaire 3.4.90 *Soient F un ensemble fini, D un ensemble fini ou dénombrable, $(a_{i,d}) \in A^{F\times D}$. Supposons que pour chaque $i \in F$, $(a_{i,d})_d$ tende vers 0. Alors la famille $\left(\prod_{i\in F} a_{i,d}\right)_d \in A^D$ tend vers 0, et*

$$\sum_{d\in D}\prod_{i\in F} a_{i,d} = \prod_{i\in F}\sum_{d\in D} a_{i,d}$$

Preuve Pour chaque $i \in F$, l'ensemble des $d \in D$ tels que $|a_{i,d}| \leq 1$ est fini, donc sauf pour un nombre fini d'indices j, $|a_j| \leq 1$. Ainsi, pour un $B > 1$, $|a_j| \leq B$ pour tout $j \in F \times D$. Soit donc $\varepsilon > 0$, soit $r > 0$ avec $B^{|F|-1}r < \varepsilon$. Fixons $i_0 \in F$: comme $(a_{i_0,d})$ tend vers 0, on a $|a_{i,d}| < r$ pour tout $d \in D$ sauf un nombre fini d'entre eux. Donc pour tout $d \in D$ hormis un nombre fini de renégats, $\left|\prod_{i\in F} a_{i,d}\right| \leq B^{|F|-1}r < \varepsilon$, donc la famille tend bien vers 0.

Soit $X \subset D$ finie, on a

$$\sum_{d\in X}\prod_{i\in I} a_{i,d} = \prod_{i\in F}\sum_{d\in X} a_{i,d},$$

et on conclut en « passant à la limite » d'après le lemme (et la continuité du produit). □

Proposition 3.4.91 *Soient D un ensemble dénombrable, union disjointe des I_δ, $\delta \in \Delta$. Soit $u \in A^{\mathbf{N}}$ de limite nulle. Alors :*

- *$(u_n)_{n\in I_\delta}$, est de limite nulle, donc $\left(\sum_{n\in I_\delta} u_n\right)_{\delta\in\Delta}$ existe ;*
- *cette famille tend vers 0, et*

$$\sum_{\delta\in\Delta}\sum_{n\in I_\delta} u_n = \sum_{n\in D} u_n.$$

Preuve Soient $\delta \in \Delta$, $\varepsilon > 0$. On dispose d'une partie finie F de D telle que si $n \notin F$, $|u_n| \leq \varepsilon$. Donc si $n \in I_\delta$ n'appartient pas à $I_\delta \cap F$ (partie finie de I_δ), $|u_n| \leq \varepsilon$, ce qui assure le premier point.

De plus, comme les I_δ partitionnent D, l'ensemble D' des $\delta \in \Delta$ tels que F rencontre I_δ est fini, donc si $\delta \notin D'$, pour chaque $n \in I_\delta$, $|u_n| \leq \varepsilon$ donc $\left|\sum_{n\in I_\delta} u_n\right| \leq \varepsilon$, d'où la sommabilité de la seconde famille.

Supposons maintenant Δ fini et montrons le résultat (cela nous servira dans le cas infini). Pour $\delta \in \Delta$, on dispose d'une suite $(F_{n,\delta})_n$ croissante de parties finies de I_δ d'union cet ensemble. Alors, si $G_n = \bigcup_{\delta\in\Delta} F_{n,\delta}$ (l'union est une union disjointe de parties finies), (G_n) est une suite croissante de parties finies de D d'union D. Ainsi, les deuxième et trisième égalités s'expliquant par la finitude de Δ,

$$\sum_{n\in D} u_n = \lim_{n\to+\infty}\sum_{d\in G_n} u_d = \lim_{n\to+\infty}\sum_{\delta\in\Delta}\sum_{d\in F_{n,\delta}} u_d = \sum_{\delta\in\Delta}\sum_{d\in I_\delta} u_d.$$

Passons au cas général. Soit X une partie finie de D. Toutes les sommabilités utilisées étant de simples vérifications, et d'après le cas Δ fini (relation de Chasles), (pour la première égalité, on sépare les $\delta \in \Delta$ tels que I_δ rencontre X les uns des autres et des autres éléments de Δ),

$$\begin{aligned}\left|\sum_{d\in X} u_d - \sum_{\delta\in\Delta}\sum_{n\in I_\delta} u_n\right| &= \left|\sum_{\delta\in\Delta}\sum_{n\in I_\delta\setminus X} u_n\right| \\ &\leq \sup_{\delta\in\Delta}\left|\sum_{n\in I_\delta\setminus X} u_n\right| \\ &\leq \sup_{\delta\in\Delta}\sup_{n\in I_\delta\setminus X}|u_n| \\ &\leq \sup_{n\in D\setminus X}|u_n|.\end{aligned}$$

et d'autre part,

$$\left|\sum_{d\in X} u_d - \sum_{d\in D} u_d\right| = \left|\sum_{n\in D\setminus X} u_n\right| \leq \sup_{n\in D\setminus X} |u_n|$$

de sorte que pour tout $X \subset D$ fini,

$$\left|\sum_{\delta\in\Delta}\sum_{n\in I_\delta} u_n - \sum_{n\in D} u_n\right| \leq \sup_{n\in D\setminus X} |u_n|,$$

ce qui conclut en posant, pour $\varepsilon > 0$, $X = \{n \in D,\ |u_n| > \varepsilon\}$ fini. □

Corollaire 3.4.92 *Soient D fini ou dénombrable, (F_n) une suite croissante de parties de D d'union D. Soit $a \in A^D$ tendant vers 0. Alors*

$$\sum_{d\in F_n} a_d \underset{n\to\infty}{\longrightarrow} \sum_{d\in D} a_d$$

Preuve Utiliser la « partition » de D en $I_0, I_1\setminus I_0, \ldots, I_{n+1}\setminus I_n, \ldots$ et le théorème d'associativité. □

Produits infinis dans un anneau complet ultramétrique

Dans $\mathbf{C}$, par exemple, on peut étudier des produits infinis de complexes, et même de fonctions holomorphes, qui jouent un rôle central dans cette théorie. On se donne donc un anneau intègre A de caractéristique nulle muni d'une valeur absolue $|\cdot|$ qui le rend complet ; on veut étudier les produits infinis dans A. Le schéma est similaire à celui des sommes.

Le premier résultat est un lemme technique, analogue à l'inégalité ultramétrique.

Lemme 3.4.93 *Soient F un ensemble fini, $\varepsilon \in]0,1]$, $a \in A^F$. Supposons que pour tout $n \in F$, $|a_n| \leq \varepsilon$. Alors*

$$\left|\prod_{n\in F}(1+a_n) - 1\right| \leq \varepsilon$$

Preuve Développer puis appliquer l'inégalité ultramétrique. □

Théorème 3.4.13 *Soit $a \in A^{\mathbf{N}}$. La suite $\prod_{0\leq k\leq n} a_k$ converge $x \neq 0$ si et seulement si $a_n \to 1$ et (a_n) ne s'annule pas. Dans ce cas,*

$$\left(\prod_{k=0}^{n} |a_k|\right)_n \text{ stationne à } |x|.$$

En particulier, la suite tend vers 0 si et seulement si $\prod_{n\geq 0} |a_n|$ tend vers 0. On dit alors que le produit infini diverge vers 0.

Preuve D'après le corollaire 84, il suffit de prouver la première équivalence. Le sens direct est immédiat ; voyons le sens réciproque : si (a_n) tend vers 1, elle est bornée en valeur absolue par un $B > 1$ et à partir d'un certain rang $E \geq 1$, $|a_n| = 1$ pour tout n (d'après le corollaire 84), de sorte que $|a_n - 1| \leq 1$. Soit $C = B^E$. Soit $\varepsilon > 0$. Soit $0 < \varepsilon_1 < \frac{\min(1,\varepsilon)}{C} < 1$. Soit $N \geq E$ tel que si $n \geq N$, $|a_n - 1| \leq \varepsilon_1$. Alors, pour $n \geq m \geq N$, d'après le lemme 93,

$$\left|\prod_{i=0}^{m} a_i - \prod_{i=0}^{n} a_i\right| = \prod_{i=0}^{E-1} |a_i| \prod_{i=E}^{m} |a_i| \left|\prod_{i=m+1}^{n} a_i - 1\right| \leq C\varepsilon_1 \leq \varepsilon$$

□

La proposition suivante permet la définition de produits infinis dans A non ordonnés.

Proposition 3.4.94 *Soient $a \in A^{\mathbf{N}}$ tendant vers 1, f une bijection de $\mathbf{N}$ dans $\mathbf{N}$. Les suites $\prod_{n\geq 0} a_n$ et $\prod_{n\geq 0} a_{f(n)}$ convergent vers la même limite non nulle ; on dit que c'est le produit des a_n.*

Preuve Comme ci-dessus, on se donne $B > 1$ bornant (a_n), $E \geq 0$ tel que si $n \geq E$, $|a_n| = 1$ donc $|a_n - 1| \leq 1$, $C = B^E$. Soit $\varepsilon > 0$, soit $\varepsilon_1 > 0$ inférieur à 1 et à ε/C. Soit $N_1 \geq E$ tel que pour tout $n \geq N_1$, $|a_n - 1| \leq \varepsilon_1$. Soit $N \geq N_1$ tel que si $n \leq N_1$, $f^{-1}(n) \leq N$. Pour $t \geq N$, on a

$$\prod_{i=0}^{t} a_i - \prod_{i=0}^{t} a_{f(i)} = \prod_{i=0}^{N_1} a_i \left(\left(\prod_{i=N_1+1}^{t} a_i - 1 \right) - \left(\prod_{\substack{0\leq i\leq t \\ f(i)>N_1}} a_{f(i)} - 1 \right) \right),$$

de sorte que, d'après le lemme 93,

$$\left| \prod_{i=0}^{t} a_i - \prod_{i=0}^{t} a_{f(i)} \right| \leq \prod_{i=0}^{E-1} |a_i| \prod_{i=E}^{N_1} |a_i| \max \left(\left| \prod_{i=N_1+1}^{t} a_i - 1 \right|, \left| \prod_{\substack{0\leq i\leq t \\ f(i)>N_1}} a_{f(i)} - 1 \right| \right) \leq C \cdot \varepsilon_1 \leq \varepsilon.$$

□

Définition Soient D un ensemble dénombrable, $a \in A^D$ tendant vers 1 au sens des suites généralisées (*ie* pour tout $\varepsilon > 0$, l'ensemble des $n \in D$ tels que $|a_n - 1| \geq \varepsilon$ est fini). On définit le produit $\prod_{n\in D} a_n \in A$ comme la limite de la suite

$$\left(\prod_{i=0}^{n} a_{f(n)} \right),$$

pour n'importe quelle bijection $f : \mathbf{N} \to D$. Cette limite est non nulle si et seulement chaque a_n est non nul. La définition est naturelle dans le cas de D fini.

Remarque 3.4.25 Soient E, D finis ou dénombrables, $f : E \to D$ bijective, $a \in A^D$ tendant vers 1, alors $a \circ f \in A^E$ tend vers 1 et par définition :

$$\prod_{n\in E} a_{f(n)} = \prod_{n\in D} a_n$$

La proposition ci-dessous justifie la notation :

Proposition 3.4.95 *Soient D un ensemble fini ou dénombrable, $a \in A^D$ tendant vers 1. Soit (F_n) une suite croissante de parties finies de D d'union D. Alors*

$$\prod_{i\in F_n} a_i \underset{n\to\infty}{\longrightarrow} \prod_{i\in D} a_i$$

Preuve On construit aisément une suite croissante d'entiers (p_n) et une bijection $f : \mathbf{N} \to D$ telle que $f(\llbracket 0; p_n \rrbracket) = F_n$, ce qui conclut d'après la définition. □

Corollaire 3.4.96 *Soient $a \in A^D$ avec D un ensemble fini ou dénombrable, a tend vers 1. Soit $(E_i)_{1\leq i\leq N}$ une famille de parties deux à deux disjointes de D et de réunion D. Alors, pour tout $1 \leq i \leq N$, $(a_p)_{p\in E_i} \in A^{E_i}$ tend vers 1, et*

$$\prod_{n\in D} a_n = \prod_{i=1}^{N} \prod_{n\in E_i} a_n$$

Preuve Le premier point est clair ; voyons le second. Par récurrence immédiate, il suffit de traiter le cas $N = 2$, ie $D = E \cup F$ avec E, F disjoints. Alors, E et F étant finis ou dénombrables, on dispose de suites $(E_n), (F_n)$ croissantes de parties finies de E et F d'unions respectives E et F. Soit, pour $n \geq 0$, $D_n = E_n \cup F_n$. (D_n) est une suite croissante de parties finies de D d'union D. Par conséquent, en appliquant à D, puis à E et F la proposition 95,

$$\prod_{i\in D} a_i = \lim_{n\to\infty} \prod_{i\in D_n} a_i = \lim_{n\to\infty} \prod_{i\in E_n} a_i \prod_{i\in F_n} a_i = \prod_{i\in E} a_i \prod_{i\in F} a_i$$

□

Enfin, comme pour les familles sommables, on dispose d'un « théorème d'associativité », qui sera démontré après avoir énoncé un lemme technique :

Lemme 3.4.97 *Soient D fini ou dénombrable, $\varepsilon \in]0,1]$, $a \in A^D$ tendant vers 1. Supposons que pour tout $d \in D$, $|a_d - 1| \leq \varepsilon$. Alors*

$$\left| \prod_{d\in D} a_i - 1 \right| \leq \varepsilon.$$

Preuve C'est vrai pour les parties finies d'après le lemme 93, il suffit de passer à la limite d'après la proposition 95. □

Théorème 3.4.14 *Soient D, Δ deux ensembles finis ou dénombrables, $(I_\delta)_{\delta\in\Delta}$ une famille de parties deux à deux disjointes de D de réunion D. Soit $a \in A^D$ tendant vers 1. Alors pour tout $\delta \in \Delta$, $(a_i)_{i\in I_\delta}$ tend vers 1 ; de plus, $\left(\prod_{i\in I_\delta} a_i\right)_{\delta\in\Delta}$ tend vers 1 ; enfin,*

$$\prod_{\delta\in\Delta} \prod_{i\in I_\delta} a_i = \prod_{i\in D} a_i$$

Preuve Le premier point est clair. Le deuxième découle du lemme 97, puisque pour $\varepsilon \in]0,1]$, sauf sur un nombre fini de $\delta \in \Delta$, pour tout $n \in I_\delta$, $|a_n - 1| < \varepsilon$.

Reste le troisième point. Soit F finie telle que si $f \notin F$, $|a_f - 1| < 1$. Pour toute partie finie $G \subset \Delta$ contenant l'ensemble des δ tels que I_δ rencontre F, on a

$$\prod_{d\in F} a_d \prod_{\delta\in G} \prod_{i\in I_\delta\setminus F} a_i = \prod_{\delta\in G} \prod_{i\in I_\delta} a_i,$$

donc en passant « à la limite »,

$$\prod_{d\in F} a_d \prod_{\delta\in\Delta} \prod_{i\in I_\delta\setminus F} a_i = \prod_{\delta\in\Delta} \prod_{i\in I_\delta} a_i.$$

Donc, quitte à remplacer D par $D\setminus F$, on peut supposer $|a_d - 1| < 1$ pour tout $d \in D$. Soit X une partie finie de D. Alors, toutes les questions de limites étant de simples vérifications découlant des résultats 95, 97, comme fait ci-dessus, et d'après le lemme 97,

$$\begin{aligned}
\left| \prod_{d\in X} a_d - \prod_{\delta\in\Delta} \prod_{i\in I_\delta} a_i \right| &= \left| \prod_{\delta\in\Delta} \prod_{i\in I_\delta\setminus X} a_i - 1 \right| \\
&\leq \sup_{\delta\in\Delta} \left| \prod_{i\in I_\delta\setminus X} a_i - 1 \right| \\
&\leq \sup_{\substack{\delta\in\Delta \\ i\in I_\delta\setminus X}} |a_i - 1| \\
&\leq \sup_{d\in D\setminus X} |a_d - 1|
\end{aligned}$$

D'autre part,

$$\left|\prod_{d\in D} a_d - \prod_{d\in X} a_d\right| = \left|\prod_{d\in D\setminus X} a_d - 1\right| \leq \sup_{d\in D\setminus X} |a_d - 1|,$$

de sorte que finalement, pour tout $\varepsilon > 0$, $X = \{d \in D, |a_d - 1| > \varepsilon\}$ étant fini, on en déduit par inégalité ultramétrique :

$$\left|\prod_{d\in D} a_d - \prod_{\delta\in\Delta}\prod_{i\in I_\delta} a_i\right| \leq \varepsilon.$$

□

3.5 Extensions de corps valués ultramétriques

Prolongement d'une valeur absolue à une extension de corps

On se donne pour l'instant un corps K, muni d'une valeur absolue $|\cdot|$ non triviale, et on prend une de ses clôtures algébriques L.

Proposition 3.5.98 *Soit $x \in L$. On dispose d'un sous-corps M de L qui est une extension de dimension d de K et qui contient x. La quantité $|\mathrm{nr}_{M/K}(x)|^{1/d}$ ne dépend que de x, pas du choix du corps M.*

Preuve Pour l'existence de M, $K[x]$ convient. Pour la norme, on a vu dans la proposition 15 que, si on note c_0 le coefficient constant du polynôme minimal de x, de degré δ, on a $\mathrm{nr}_{M/K}(x) = (-1)^d c_0^{d/\delta}$. La quantité qui nous intéresse est donc $|c_0^{d/\delta}(-1)^d|^{1/d} = |c_0|^{1/\delta}$, indépendante de M. □

Définition Soit $x \in L$. On note $||x||$ la quantité distinguée par la proposition précédente.

Proposition 3.5.99 *L'application $||\cdot||$ est multiplicative de L dans $\mathbf{R}^+$, s'annule en zéro seul et coïncide avec $|\cdot|$ sur K.*

Preuve Pour le troisième point, il suffit de prendre comme extension finie de K le corps K lui-même. D'autre part, si $||x|| = 0$, la preuve de la proposition précédente nous dit que le polynôme minimal de x s'annule en zéro. Ce dernier étant irréductible, il est égal à X, et donc $x = 0$.

Voyons le second point : soient $x, y \in L$, prenons $M = K[x, y]$, qui est bien de dimension finie d sur K. On a alors

$$||xy|| = |\mathrm{nr}_{M/K}(xy)|^{1/d} = |\mathrm{nr}_{M/K}(x)|^{1/d}|\mathrm{nr}_{M/K}(y)|^{1/d} = ||x|| \cdot ||y||.$$

□

On aimerait donc bien prouver que $||\cdot||$ est une valeur absolue sur L. Malheureusement, cela marche assez mal.

Non-exemple 3.5.26 Si on garde cette définition, $3 \pm 2\sqrt{2} = (1 \pm \sqrt{2})^2$ devrait être de valeur absolue 1, car le polynôme minimal de $1 \pm \sqrt{2}$ est $(X-1)^2 - 2 = X^2 - 2X - 1$. Mais $3 + 2\sqrt{2} + 3 - 2\sqrt{2}$ vaut 6, ce qui empêche toute forme d'inégalité triangulaire.

Cependant, il existe des cas dans lesquels $||\cdot||$ est tout de même une valeur absolue. Pour les étudier, on aura besoin d'un petit lemme technique :

Lemme 3.5.100 *Soit $(a_n) \in K^{\mathbf{N}}$ une suite de limite nulle. Pour tout $\varepsilon > 0$, il existe un $N \geq 1$ tel que pour tous entiers $k, l \geq 1$, si $k + l \geq N$, alors*

$$\left|\frac{ka_k + la_l}{k+l}\right| \leq \varepsilon.$$

Preuve Soit $\varepsilon > 0$. On dispose de $N_0 \geq 1$ tel que si $n \geq N_0$, $|a_n| \leq \frac{\varepsilon}{2}$. Soit de plus M tel que pour tout $n \geq 1$, $|a_n| \leq M$. Posons $N \geq 1$ tel que $\frac{MN_0}{N} \leq \frac{\varepsilon}{2}$. Soit $k, l \in \mathbf{N}^*$ tels que $k + l \geq N$. Alors :

$$\begin{cases} \frac{k|a_k|}{k+l} \leq |a_k| \leq \frac{\varepsilon}{2} & \text{si } k \geq N_0, \\ \frac{k|a_k|}{k+l} \leq \frac{MN_0}{N} \leq \frac{\varepsilon}{2} & \text{sinon,} \end{cases}$$

et de même pour $l|a_l|$, ce qui conclut par inégalité triangulaire. □

Théorème 3.5.15 *Supposons K localement compact et sa valeur absolue ultramétrique. Alors $||\cdot||$ est une valeur absolue ultramétrique sur L.*

Preuve Il suffit de montrer que si $M \subset L$ est une extension de K, si $a, b \in M$, on a $||a + b|| \leq \max(||a||, ||b||)$. Soit donc $M \subset L$ une extension de dimension d sur K. Soit $(e_1, \ldots, e_d)$ une K-base de M, soit $||\cdot||_\infty$ la norme infinie subordonnée à la valeur absolue de K pour cette base. Cette norme satisfait l'inégalité ultramétrique. On pose alors, pour A endomorphisme de M,

$$||A||_{\text{op}} = \sup_{||y||_\infty \leq 1} ||A(y)||_\infty.$$

On pose aussi, pour $a \in M$, $|a|_{\text{op}} = ||P_a||_{\text{op}}$, où $P_a : b \in M \longmapsto ab$. On vérifie que $||\cdot||_{\text{op}}$ est une norme sur l'espace vectoriel des endomorphismes de M, ultramétrique et sous-multiplicative (et $|\cdot|_{\text{op}}$ aussi).

Soit $I = [A_0; B_0]$ un segment de $\mathbf{R}^{+*}$ contenant 1 et un $|u| > 1$ pour un $u \in K$. Alors, comme $|u|^n I \supset [|u|^n; |u|^{n+1}]$ pour tout $n \in \mathbf{Z}$,

$$\bigcup_{n \in \mathbf{Z}} |u|^n I = \mathbf{R}_+^*.$$

Par conséquent, si $x \in M^*$, il existe $t \in K^*$ tel que $|tx|_{\text{op}} \in I$.

L'ensemble $S = \{z \in M : |z|_{\text{op}} \in I\}$ est un fermé borné de M de dimension finie, donc un compact pour l topologie induite par $|\cdot|_{\text{op}}$. Comme $z \in E \mapsto \det(P_z)$ est continue (composé d'une application linéaire entre espaces de dimension finie sur un corps localement compact et du déterminant, qui est polynomial sur l'espace des endomorphismes de M donc continu), $\{|\det P_z| \mid z \in S\} \subset \mathbf{R}^{+*}$ est compact. Il existe donc une constante $C_1 > 0$ telle que :

$$\forall\, |z|_{\text{op}} \in I, \quad C_1^{-1} < |\det(P_z)| = ||z||^d < C_1.$$

Soit $z \in M$ non nul, on dispose de $t \in K^*$ tel que $|t^{-1}z|_{\text{op}} \in I$. Alors :

$$C_1^{-1} < |\det(P_{t^{-1}z})| = |t|^{-d}||z||^d < C_1.$$

Donc, comme $|t^{-1}z|_{\text{op}} \in I$, $A_0 \leq |t|^{-1}|z|_{\text{op}} \leq B_0$, d'où $B_0^{-1}|z|_{\text{op}} \leq |t| \leq A_0^{-1}|z|_{\text{op}}$, pour les constantes strictement positives $A = B_0^{-1}C_1^{-1/d}$, $B = A_0^{-1}C_1^{1/d}$,

$$A|z|_{\text{op}} \leq ||z|| \leq B|z|_{\text{op}}.$$

Finalement, on a montré que la « norme » $||\cdot||$ est « équivalente » à la norme ultramétrique d'opérateur sur M. C'est l'ingrédient clé pour montrer que $||\cdot||$ est ultramétrique : en effet, on n'a plus qu'à « se débarrasser » des constantes dans cette inégalité, ce pourquoi on fait la remarque suivante : de la multiplicativité de $||\cdot||$ s'ensuit que $|z^n|_{\text{op}}^{1/n} \to ||z||$.

Soient $a, b \in M$, $A = \max(||a||, ||b||)$. On dispose d'une suite (r_k) de limite nulle avec $|a^k|_{\text{op}} \leq (A + r_k)^k$ et $|b^k|_{\text{op}} \leq (A + r_k)^k$ pour tout k. En utilisant la formule du binôme et la propriété ultramétrique de $|\cdot|_{\text{op}}$, on en déduit que pour $n \geq 1$, il existe $0 \leq k_n \leq n$ tel que

$$|(a+b)^n|_{\text{op}}^{1/n} \leq |a^{k_n}|_{\text{op}}^{1/n} |b^{n-k_n}|_{\text{op}}^{1/n} \leq A + \frac{k_n r_{k_n} + (n - k_n) r_{n-k_n}}{n},$$

par inégalité arithmético-géométrique et propriété de la suite r. Le membre droit tend vers A d'après le lemme 100, et le terme gauche tend vers $||a + b||$, ce qui conclut. □

On applique immédiatement ce théorème à $\mathbf{Q}_p$, ce qui nous donne une valeur absolue ultramétrique sur $\overline{\mathbf{Q}_p}$.

Structure de certaines extensions primitives de $\mathbf{Q}_p$

Ce paragraphe sert d'étude préliminaire de certaines extensions de $\mathbf{Q}_p$, qui seront introduites de façon plus légitime dans la sous-section **4.3** pour montrer l'existence d'un relèvement de Teichmüller.

Définition Pour K un corps muni d'une valuation $|\cdot|$ ultramétrique, on définit son *anneau de valuation* $A := \{x \in K \mid |x| \leq 1\}$, et *son grand idéal de valuation*[15] $M := \{x \in K \mid |x| < 1\}$.

Lemme 3.5.101 *Avec les notations de la définition, A est bien un anneau, et M est le seul idéal maximal de A. Donc l'anneau quotient A/M est un corps.*

Preuve Le 1 de K n'est pas dans M, donc M est strict. L'inégalité ultramétrique et la multiplicativité des valeurs absolues assurent que M est bien un idéal de A.

Vérifions la maximalité de M : soit $x \in A \setminus M$, par multiplicativité de la valeur absolue $x^{-1} \in A$ donc, si on note I l'idéal de A engendré $M \cup \{x\}$, on a $1 = x^{-1}x \in I$. Finalement, il vient $I = A$. D'ailleurs, la même raison montre que tout idéal maximal I_{max} de A ne contient aucun x de valeur absolue 1, donc est inclus dans M, d'où l'unicité de M. □

Prenons désormais p premier, $n \in \mathbf{N}^*$, α un générateur de $\mathbf{F}_{p^n}^*$. Soit P son polynôme minimal sur $\mathbf{F}_p$, il est irréductible de degré n. Soit $\tilde{P}$ un relèvement quelconque de P dans $\mathbf{Z}_p[X] \subset \mathbf{Q}_p[X]$. Soit β une racine de $\tilde{P}$.

Lemme 3.5.102 *$\tilde{P}$ est irréductible dans $\mathbf{Q}_p[X]$, et proportionnel au polynôme minimal sur $\mathbf{Q}_p$ de β.*

Preuve D'après le lemme 80, il suffit de prouver que $\tilde{P}$ est irréductible dans $\mathbf{Z}_p[X]$. Supposons donc $\tilde{P} = QR$, Q, R dans $\mathbf{Z}_p[X]$ de degrés q et r, avec $1 \leq q, r < n$. Réduisons Q, R en $\overline{Q}, \overline{R}$ modulo p : comme $\tilde{P}$ est de degré n et relève dans $\mathbf{Z}_p$ un polynôme unitaire de $\mathbf{F}_p$ de degré n, son coefficient dominant est inversible, il en est donc de même pour ceux de Q et R, de sorte que leurs réductions modulo p sont $\overline{Q}$ de degré q et $\overline{R}$ de degré r, et on a $P = \overline{QR}$ en réduisant dans $\mathbf{F}_p$. Or, les deux facteurs sont non constants et P est irréductible, c'est absurde. □

Proposition 3.5.103 *Dans ce cas particulier, si on considère $K = \mathbf{Q}_p(\beta)$, $A/M \simeq \mathbf{F}_{p^n}$.*

Pour prouver ce résultat, on introduit plusieurs lemmes.

Lemme 3.5.104 *On a $|\beta|_p = 1$.*

Preuve $\tilde{P}$ a tous ses coefficients de valeur absolue inférieure ou égale à 1,[16] donc par la version ultramétrique de la proposition 59, toutes les racines de $\tilde{P}$ dans $\overline{\mathbf{Q}_p}$ sont de valeur absolue plus petite que 1. Mais leur produit est de valeur absolue 1 (car $P(0) \neq 0$ dans $\mathbf{F}_p$ car P irréductible, donc $\tilde{P}(0)$ est inversible dans $\mathbf{Z}_p$ donc est de valeur absolue 1). Donc toutes les racines sont de valeur absolue 1, de sorte que $|\beta|_p = 1$. □

Définition On note maintenant, à bon droit, $\mathbf{F}_p([\beta])$ le sous-corps de A/M engendré par $\mathbf{F}_p \subset A/M$ et par $[\beta] \in A/M$ (le lemme 104 assure que $\beta \in A$). On peut aussi le voir comme l'image du sous-anneau $\mathbf{Z}_p(\beta)$ de K inclus dans A par la réduction modulo M.

Lemme 3.5.105 *On a $\mathbf{F}_p([\beta]) \simeq \mathbf{F}_{p^n}$.*

Preuve On sait que $[\beta]$ est une racine de $\tilde{P}$, or le polynôme $\tilde{P} - P$ est à coefficients dans $p\mathbf{Z}_p$, ensemble dont la réduction modulo M est nulle. Donc $P([\beta]) = 0 \mod M$, et P est irréductible de degré n sur $\mathbf{F}_p$, d'où $\mathbf{F}_p([\beta]) \simeq \mathbf{F}_{p^n}$. □

Lemme 3.5.106 *Soit $R \in \mathbf{Z}_p[X]$ de réduction dans $\mathbf{F}_p$ non nulle de degré inférieur ou égal à $n-1$. Alors $|R(\beta)|_p = 1$.*

15. terminologie non standard
16. car P peut avoir des coefficients nuls, donc de relèvement de valeur absolue strictement inférieure à 1

Preuve L'inégalité ultramétrique donne $|R(\beta)|_p \leq 1$.

Pour l'autre sens, on se propose de trouver $U \in \mathbf{Z}_p[X]$ tel que $U(\beta)R(\beta) = 1$: alors, en passant cette égalité à la valeur absolue, on obtiendrait $|R(\beta)|_p \geq 1$, ce qui conclut. Un bon candidat est donné par l'identité de Bézout dans $\mathbf{Q}_p[X]$: on dispose en effet de $U, V \in \mathbf{Q}_p[X]$ tels que

$$UR + V\tilde{P} = 1,$$

où $\tilde{P}$ désigne toujours le polynôme minimal de β, et U est choisi de degré strictement inférieur à n. Si $U \in \mathbf{Z}_p[X]$, c'est gagné. Sinon, soit par l'absurde $\alpha \geq 1$ minimal tel que $U_1 := p^\alpha U$ et $V_1 := p^\alpha V$ soient à coefficients dans $\mathbf{Z}_p$. En réduisant modulo $p\mathbf{Z}_p[X]$ l'identité de Bézout multipliée par p^α, il vient :

$$\overline{U_1}\,\overline{R} + \overline{V_1}\,\overline{\tilde{P}} = 0,$$

et comme $\overline{\tilde{P}} = P$ irréductible de degré n (avec les notations de début de paragraphe), il est premier avec $\overline{R}$ qui est non nul de degré strictement inférieur, donc divise $\overline{U_1}$, qui est de degré strictement inférieur, donc nul. Finalement, $\overline{V_1}\overline{\tilde{P}} = 0$, d'où $\overline{V_1} = 0$, ce qui contredit la minimalité de α.

On avait donc bien $U \in \mathbf{Z}_p[X]$, d'où s'ensuit le résultat voulu. □

On peut maintenant démontrer la proposition 103.

Preuve Il suffit, d'après le lemme 105, de prouver que $A/M = \mathbf{F}_p([\beta])$. Soit $[x] \in A/M$. On note $x = Q(\beta)$ où $Q \in \mathbf{Q}_p[X]$ de degré inférieur ou égal à $n-1$. On veut montrer l'existence de $R \in \mathbf{F}_p[X]$ tel que $x - R(\beta) = 0 \mod M$. Remarquons tout d'abord que, quitte à modifier le polynôme Q en enlevant les monômes $a_i\beta^i$ qui sont dans M, on peut supposer que tous les coefficients non nuls de Q sont de valeur absolue supérieure ou égale à 1.

En distinguant les coefficients de valeur absolue 1 (qui sont donc des éléments inversibles de $\mathbf{Z}_p$, c'est-à-dire des sommes d'un élément de $\mathbf{F}_p$ et d'un élément de $p\mathbf{Z}_p \subset M$), on peut donc écrire $Q = R + p^{-m}S$, modulo M, pour $R \in \mathbf{F}_p[X]$, $m \in \mathbf{N}$ minimal et $S \in \mathbf{Z}_p[X]$. Par minimalité de m, si $S \in p\mathbf{Z}_p[X]$, $m = 0$, donc $Q \in \mathbf{Z}_p[X]$ et $x \in \mathbf{F}_p([\beta])$. Donc, d'après le lemme 106, $|S(\beta)|_p = 1$ donc, si $m > 0$, d'après l'égalité dans l'inégalité ultramétrique (*ie* le corollaire 83), $|x|_p = |Q(\beta)|_p = p^m$ donc $x \notin A$, ce qui est absurde ; si $m = 0$, $Q \in \mathbf{Z}_p[X]$ donc $[x] \in \mathbf{F}_p([\beta])$. □

Restons dans ce cas particulier pour K. Non seulement on connait bien la structure du corps résiduel A/M (qu'on identifie dorénavant systématiquement à $\mathbf{F}_{p^n}$), mais la proposition et le corollaire suivants nous montre que la structure de M ne fait guère plus de mystère :

Proposition 3.5.107 *Soit $x \in K^*$. Il existe $k \in \mathbf{Z}$ tel que $|x|_p = p^k$.*

Preuve Soit $(e_1, \ldots, e_n)$ la famille $(1, \ldots, \beta^{n-1})$. On a modulo M : $([e_1], \ldots, [e_n])$ base de A/M sur $\mathbf{F}_p$ d'après ce qui précède. En outre, comme $\tilde{P}$ est irréductible d'après le lemme 80, c'est le polynôme minimal de β sur $\mathbf{Q}_p$ et donc la famille $(e_1, \ldots, e_n)$ est libre sur $\mathbf{Q}_p$. Comme $\mathbf{Q}_p(\beta)$ est de degré n sur $\mathbf{Q}_p$, x s'écrit donc comme combinaison linéaire à coefficients dans $\mathbf{Q}_p$ des (e_i) : $x = \sum \lambda_i e_i$. Or tous les e_i sont de valeur absolue 1 d'après le lemme 104. Donc quitte à factoriser par une puissance entière de p, on peut supposer que chaque λ_i est de valeur absolue au plus 1 (donc est entier p-adique) et que 1 est atteint.

Soit alors $F(X) = \sum_{i=0}^{n-1} \lambda_i X^i \in \mathbf{Z}_p[X]$. On a donc $x = F(\beta)$, et la réduction modulo p de F est non nulle. D'après le lemme 106, $|x|_p = |F(\beta)|_p = 1$, ce qui conclut. □

Corollaire 3.5.108 *On a $M = pA$.*

Preuve Il suffit de montrer que si $x \in M$, $x \in pA$. Soit $x \in M$. D'après la proposition précédente, $|x|_p \leq p^{-1}$. Donc $xp^{-1} \in A$. □

Remarque 3.5.27 En conclusion, dans ce paragraphe, (en gardant toujours les mêmes notations), on a identifié $\mathbf{F}_{p^n}$ à A/pA.

3.6 Le corps $\mathbf{C}_p$

Définition On se place maintenant dans le cas $K = \mathbf{Q}_p$. Comme on l'a fait dans la dernière partie de la sous-section précédente, on note $\overline{\mathbf{Q}_p}$ une clôture algébrique de $\mathbf{Q}_p$, que l'on munit de la valeur absolue donnée par le théorème 15, puis on définit $\mathbf{C}_p$ le complété de $\overline{\mathbf{Q}_p}$. Ainsi, d'après le théorème 8, $\mathbf{C}_p$ est un corps complet et algébriquement clos contenant $\mathbf{Q}_p$.

Remarque 3.6.28 Le corps $\mathbf{C}_p$ est de caractéristique nulle. On peut donc tout à fait étudier des séries formelles à coefficients dans $\mathbf{C}_p$.

3.7 Lemme de préparation de Weierstrass

Définition Une fonction $f : \mathbf{C}_p \to \mathbf{C}_p$ est dite *entière* si elle s'écrit :

$$f(T) = \sum_{i \geq 0} a_i T^i$$

avec $a_i \in \mathbf{C}_p$ et $|a_n|_p^{1/n} \underset{n\to\infty}{\longrightarrow} 0$.

Remarquons qu'en effet, la série définissant f converge alors normalement sur tout borné de $\mathbf{C}_p$ (exactement comme dans le cas complexe). Démontrons d'abord un résultat de construction de zéros localisés d'une fonction entière sur $\mathbf{C}_p$.

Proposition 3.7.109 *Soit $f(T) = 1+a_1T+a_2T^2\ldots$ une fonction entière sur $\mathbf{C}_p$. Supposons que $|a_m|_p^{1/m} \geq 1/R$ pour des $m \geq 1$, $R > 0$. Alors f possède un zéro $z \in \mathbf{C}_p$ avec $|z|_p \leq R$.*

Preuve On considère d'abord le polynôme $f_n(T) = 1 + a_1T + \ldots + a_nT^n$, pour $n \geq 0$ fixé. Puisque $\mathbf{C}_p$ est algébriquement clos, f_n a une décomposition

$$f_n(T) = (1 - \beta_{n,1}T)\ldots(1 - \beta_{n,n}T),$$

pour des $\beta_{n,1}, \ldots, \beta_{n,n} \in \mathbf{C}_p$. Soient $n \geq k \geq 0$. Alors $(-1)^k a_k$ est le k-ième polynôme symétrique en les $\beta_{n,i}$, de sorte que :

$$\left(\max_{1\leq i\leq n} |\beta_{n,i}|_p\right) \geq \max_{\substack{X\subset[\![1;n]\!]\\|X|=k}} \left|\prod_{i\in X}\beta_{n,i}\right|_p^{1/k} \geq \left|(-1)^k \sum_{\substack{X\subset[\![1;n]\!]\\|X|=k}} \prod_{i\in X}\beta_{n,i}\right|_p^{1/k} = |a_k|_p^{1/k}.$$

De $|a_m|_p \geq 1/R^m$, il découle donc qu'au moins un i vérifie $|\beta_{n,i}|_p \geq 1/R$, pour tout $n \geq m$. Ainsi l'ensemble $J_n = \{i \in [\![1, n]\!] \mid |\beta_{n,i}|_p \geq 1/R\}$ est non vide pour tout $n > m$; soit $C_n \geq 1$ son cardinal.

Majorons uniformément C_n. On remarque que si $n \geq k \geq 1$, si $R' > 0$, et si, parmi les $\beta_{n,i}$, exactement k sont de valeur absolue supérieure à $1/R'$, alors leur produit π est de valeur absolue strictement plus grande que tout autre produit de k facteurs $\beta_{n,i}$ (avec des indices i distincts), de sorte que $|(-1)^k a_k - \pi|_p < |\pi|_p$, donc

$$|a_k|_p = |((-1)^k a_k - \pi) + \pi|_p = |\pi|_p \geq 1/R'^k.$$

Puisque $|a_n|_p^{1/n} \to 0$, on obtient que pour tout $R' > 0$, il existe $N_{R'} > 0$ tel que $C_n(R') \leq N_{R'}$ pour tout n.

On obtient également que, si $|\beta_{n,i}|_p \geq B$, alors il existe un k tel que $|a_k|_p^{1/k} \geq B$. Notamment, avec $B = 1 + \sup_{n\geq 1} |a_n|_p^{1/n}$, on a, pour tous n, i, $|\beta_{n,i}|_p < B$.

Soient $n' \geq n \geq 1$, soit $i \in [\![1; n]\!]$ tel que $|\beta_{n,i}|_p \geq 1/R$. On a $f_n(1/\beta_{n,i}) = 0$, d'où :

$$f_{n'}\left(\frac{1}{\beta_{n,i}}\right) = \sum_{k=n+1}^{n'} a_k \beta_{n,i}^k, \text{ donc } \left|f_{n'}\left(\frac{1}{\beta_{n,i}}\right)\right|_p \leq \max_{n<k\leq n'} (|a_k|_p^{1/k} B)^k.$$

Soit $M_0 > N_R$ tel que pour tout $k > M_0$, $|a_k|_p^{1/k} B < 1$. Soit $n' \geq n \geq M_0$. On a :

$$\left| f_{n'} \left(\frac{1}{\beta_{n,i}} \right) \right|_p \leq B \sup_{k>n} |a_k|_p^{1/k}.$$

Pour $i \in J_n$, $j \in [\![1, n']\!] \setminus J_{n'}$, $\frac{\beta_{n',j}}{\beta_{n,i}}$ est donc de valeur absolue strictement inférieure à 1, d'où $\left|1 - \frac{\beta_{n',j}}{\beta_{n,i}}\right|_p = 1$. Dès lors,

$$\begin{aligned}
\min_{j \in J_{n'}} (|\beta_{n,i} - \beta_{n',j}|_p) &\leq \left(\prod_{j \in J_{n'}} |\beta_{n,i} - \beta_{n',j}|_p \right)^{1/C_{n'}} \\
&\leq B \left| \prod_{j \in J_{n'}} \left(1 - \frac{\beta_{n',j}}{\beta_{n,i}} \right) \right|_p^{1/C_{n'}} \\
&\leq B \left| f_{n'} \left(\frac{1}{\beta_{n,i}} \right) \right|_p^{1/C_{n'}} \\
&\leq B \left(B \sup_{k>n} |a_k|_p^{1/k} \right)^{1/C_{n'}} \\
&\leq B^2 \left(\sup_{k>n} |a_k|_p^{1/k} \right)^{1/N_R}
\end{aligned}$$

On dispose par ailleurs d'une suite strictement croissante (Q_n) tendant vers $+\infty$ et minorée par M_0 telle que si $q \geq Q_n$, $|a_q|^{1/q} \leq \left(\frac{1}{2^n B^2}\right)^{N_R}$. Construisons la suite (i_n) par récurrence telle que $i_0 \in J_{Q_0}$ et pour tout $n \in \mathbf{N}$, $i_{n+1} \in J_{Q_{n+1}}$ minimise $|\beta_{Q_n,i_n} - \beta_{Q_{n+1},i_{n+1}}|$. D'après le calcul précédent, on a, pour $n \in \mathbf{N}$, $|\beta_{Q_{n+1},i_{n+1}} - \beta_{Q_n,i_n}| \leq \frac{1}{2^n}$, de sorte que $(\beta_{Q_n,i_n})_n$ est de Cauchy, donc converge vers un $z \in \mathbf{C}_p$.

Pour chaque n, par construction, $|\beta_{Q_n,i_n}|_p^{-1} \leq R$, donc $z \in \mathbf{C}_p^*$ et $|z^{-1}|_p \leq R$. D'autre part, pour $n \in \mathbf{N}, q \geq Q_n$, $\left| f_q \left(\frac{1}{\beta_{Q_n,i_n}} \right) \right|_p \leq 2^{-n}$ (toujours d'après le calcul précédent), donc, en faisant tendre q vers $+\infty$, puis n vers $+\infty$, on obtient $f(z^{-1}) = 0$. □

On peut maintenant prouver une première forme du théorème de préparation de Weierstrass, qu'on pourrait qualifier de forme exponentielle du résultat.

Proposition 3.7.110 *Soit $f(T) = 1 + \sum_{n \geq 1} a_n T^n$ une fonction entière sur $\mathbf{C}_p$, et soit $R > 0$. Alors il existe $\beta_1, ..., \beta_d \in \mathbf{C}_p$ tels que l'on ait $f(T) = g(T) \prod_{i=1}^d (1 - \beta_i T)$, où la fonction $g(T) = 1 + \sum b_n T^n$ est entière et telle que $|b_n|_p \leq R^{-n}$ pour tout entier n.*

Preuve Posons $a_0 = 1$. Comme f est entière, on dispose d'un entier m minimal tel que $R^m |a_m|_p \geq R^n |a_n|_p$ pour tout $n \in \mathbf{N}$. On procède alors par récurrence sur m.

Le résultat est immédiat lorsque $m = 0$. Supposons donc $m \geq 1$ et supposons le résultat prouvé pour tout $k < m$. On a alors $R^m |a_m|_p > 1$ (sans égalité par minimalité de m), donc $|a_m|^{1/m} \geq \frac{1}{R'}$ pour un $R' < R$. Par la proposition précédente, il existe donc $z \in \mathbf{C}_p$ avec $|z| \leq R' < R$, et $f(z) = 0$, en particulier $z \neq 0$. On peut donc écrire $f(T) = \left(1 - \frac{T}{z}\right) h(T)$, où $h(T) = 1 + \sum_{n \geq 1} b_i T^i$, $b_0 = 1$, $b_n = z^{-n} \sum_{k=0}^n a_k z^k$. Puisque $f(z) = 0$, on a également, avec convergence, $b_n = -\sum_{k \geq 1} z^k a_{k+n}$.

Reste à montrer que cette première factorisation nous a permis d'avancer dans le problème : essayons d'encadrer les coefficients de $h(T)$. Soient alors $k \geq 1$, $n \geq 0$. On

$$|z^k a_{k+n}|_p \leq |z|_p^k |a_m|_p R^{m-k-n} \leq |z a_m|_p R^{m-n-1},$$

on a en sommant $|b_n|_p \leq |z a_m|_p R^{m-n-1}$. Or $|z a_m|_p = |b_{m-1}|_p$: en effet, si $k \geq 2$,

$$|z^k a_{k+m-1}|_p \leq |z|_p^k |a_m|_p R^{1-k} \leq |z|_p^2 R^{-1} |a_m|_p < |z a_m|_p,$$

donc il y a bien égalité dans l'inégalité ultramétrique quand on somme pour retrouver b_{m-1}, d'après la proposition 83. Finalement, si $n \geq 0$,

$$R^n |b_n|_p \leq R^{m-1} |b_{m-1}|_p,$$

ce qui conclut par hypothèse de récurrence. □

Coefficients du logarithme et théorème de préparation de Weierstrass

Définition Posons, pour tout $n \geq 1$,

$$L_n(X_1, \ldots, X_n) = \sum_{k \geq 1} \frac{(-1)^{k-1}}{k} \sum_{\substack{p_1, \ldots, p_k \in \mathbf{N}^* \\ p_1 + \ldots + p_k = n}} \prod_{i=1}^{k} X_{p_i},$$

la somme étant finie et définissant un polynôme rationnel en n variables.

De simples calculs aboutissent à la proposition et au lemme suivants :

Proposition 3.7.111 *Soient K un corps de caractéristique nulle, $(a_n)_{n \geq 1} \in K^{\mathbf{N}^*}$, alors*

$$\log\left(1 + \sum_{n \geq 1} a_n X^n\right) = \sum_{n \geq 1} L_n(a_1, \ldots, a_n) X^n.$$

Lemme 3.7.112 *Soient K un corps de caractéristique nulle muni d'une valeur absolue $|\cdot|$ ultramétrique, $(a_n) \in K^{\mathbf{N}^*}$, $r > 0$. Supposons que pour tout $n \geq 1$, $|a_n| \leq r^n$. Alors pour tout $n \geq 1$, $|L_n(a_1, \ldots, a_n)| \leq r^n \sup_{1 \leq k \leq n} \left|\frac{1}{k}\right|$.*

Théorème 3.7.16 *Soit $(a_n)_{n \geq 1}$ une suite à valeurs dans $\mathbf{C}_p$ telle que la série formelle*

$$\exp\left(\sum_{n \geq 1} \frac{a_n}{n} X^n\right)$$

définisse une fonction entière sur $\mathbf{C}_p$. Soit $A > 0$. Il existe $\beta_1, \ldots, \beta_m \in \mathbf{C}_p$ tels que pour tout n,

$$\left| a_n + \sum_{i=1}^{m} \beta_i^n \right|_p \leq p^{-An}.$$

Preuve Observons d'emblée que si $1 \leq k \leq n$, $\left|\frac{1}{k}\right|_p \leq p^n$. [17] Soit $R = p^{-A'}$, où $A' = A + 1$.

D'après la proposition 110, on dispose de $\beta_1, \ldots, \beta_m \in \mathbf{C}_p$, et d'une série formelle $g(X) = \sum b_n X^n$ à coefficients dans $\mathbf{C}_p$ avec $|b_n|_p \leq p^{-A'n}$ et $b_0 = 1$ tels que :

$$\exp\left(\sum_{n \geq 1} \frac{a_n}{n} X^n\right) = \prod_{i=1}^{m} (1 - \beta_i X) g(X).$$

Passons au logarithme : si $c_n = L_n(b_1, \ldots, b_n)$, on a $|c_n|_p \leq p^n p^{-A'n} = p^{-An}$, et on a :

$$\sum_{n \geq 1} \frac{a_n}{n} X^n = \sum_{i=1}^{m} \log(1 - \beta_i X) + \log(g(X)) = \sum_{n \geq 1} X^n \left(c_n - \sum_{i=1}^{m} \frac{\beta_i^n}{n}\right),$$

donc finalement, pour tout $n \geq 1$, $\left| a_n + \sum_{i=1}^{m} \beta_i^n \right|_p = |n|_p |c_n|_p \leq p^{-An}$, ce qu'on voulait établir. □

17. c'est extrêmement brutal, mais cela importe peu

4 Rationalité de la fonction zêta

Dans toute cette section, on pose q une puissance d'un nombre premier p, r un entier supérieur ou égal à 1, $I \subset \mathbf{F}_q[X_1, \ldots, X_r]$ un idéal. On note :

$$N_n = |\{x \in \mathbf{F}_{q^n}^r \mid \forall P \in I,\ P(x) = 0\}|.$$

Soit ζ_I la fonction zêta associée à I.

4.1 Un plan d'attaque

On se propose ici de montrer le :

Théorème 4.1.17 *Il existe deux ensembles à multiplicité disjoints d'entiers algébriques $(\alpha_i)_{i\in[\![1,k]\!]}$ et $(\beta_j)_{j\in[\![1,k']\!]}$ tels que pour tout $n \in \mathbf{N}^*$:*

$$N_n = \sum_{1\leq j\leq k'} \beta_j^n - \sum_{1\leq i\leq k} \alpha_i^n.$$

Montrons que ce théorème équivaut à la première conjecture de Weil.

Preuve Si la première conjecture de Weil est vraie, $\zeta_I(X) = \frac{\prod(1-\alpha_i X)}{\prod(1-\beta_j X)}$, pour α_i, β_j des entiers algébriques. On peut supposer $\alpha_i \neq \beta_j$ pour tous i, j. On a donc :

$$\begin{aligned}\sum_{n\geq 1} N_n X^n &= X \cdot DL(\zeta_I(X)) \\ &= -\sum_i \frac{\alpha_i X}{1-\alpha_i X} + \sum_j \frac{\beta_j X}{1-\beta_j X} \\ &= \sum_{n\geq 1} \left(\sum_j \beta_j^n - \sum_i \alpha_i^n \right) X^n.\end{aligned}$$

en développant les séries géométriques et en échangeant les sommes.

Réciproquement, si le théorème est vrai, on pose :

$$\tilde{\zeta_I}(X) = \frac{\prod_{1\leq i\leq k}(1-\alpha_i X)}{\prod_{1\leq j\leq k'}(1-\beta_j X)}.$$

Les mêmes calculs établissent que $DL(\zeta_I(X)) = DL(\tilde{\zeta_I}(X))$. D'où $\zeta_I(X) = \lambda\tilde{\zeta_I}(X)$, d'où, comme $\zeta_I(0) = \tilde{\zeta_I}(0) = 1$, $\zeta_I(X) = \tilde{\zeta_I}(X)$. Dès lors, ζ_I est une fraction rationnelle à pôles et zéros entiers algébriques, et à coefficients entiers d'après la remarque 15. □

Pour montrer le théorème, on s'appuie sur les deux propositions suivantes :

Proposition 4.1.113 *Il existe $C, A > 0$ telles que :*

$$\forall\, n \in \mathbf{N} \quad |N_n|_\infty \leq C q^{An},$$

où $|\cdot|_\infty$ est la valeur absolue archimédienne sur $\mathbf{Q}$.

Proposition 4.1.114 *Soit p la caractéristique de $\mathbf{F}_q$. Pour tout $A > 0$, il existe $\alpha_1, \ldots, \alpha_k$ et $\beta_1, \ldots, \beta_{k'} \in \mathbf{C}_p$ tels que :*

$$\forall\, n \in \mathbf{N} \quad \left| N_n - \sum_{1\leq j\leq k'} \beta_j + \sum_{1\leq i\leq k} \alpha_i \right|_p \leq q^{-An}.$$

La proposition 113 donne un contrôle évident [18] de la valeur absolue archimédienne de N_n. Conjointement, la proposition 114 contrôle la valeur absolue p-adique de N_n. Toutefois, elle est plus difficile à montrer. Elle repose sur deux arguments importants de nature très différentes, à savoir la proposition 115 *infra* et le théorème 16 établi précédemment.

Proposition 4.1.115 *Il existe $k \in \mathbf{N}^*$, et pour tout $i \in [\![1,k]\!]$, $\lambda_i \in \mathbf{Z}$, $(N_n^i)_n \in \mathbf{C}_p^{\mathbf{N}^*}$ telles que $N_n = \sum_{1\leq i\leq k} \lambda_i N_n^i$ pour tout $n \in \mathbf{N}^*$, et pour tout i,*

$$\zeta_I^i(X) := \exp\left(\sum_{n\geq 1} \frac{N_n^i}{n} X^n\right)$$

est entière dans $\mathbf{C}_p$.

Cette proposition permet de décomposer la fonction ζ_I en produit de fonctions entières de $\mathbf{C}_p$. Or, le théorème de préparation de Weierstrass établit l'analogue de la proposition 114 pour chaque terme de la décomposition séparément. Par inégalité ultramétrique (et le fait que si $n \in \mathbf{Z}$, $|n|_p \leq 1$), ces deux résultats impliquent directement la proposition 114.

Dès lors, voici notre plan d'attaque pour prouver la rationalité de la fonction zêta : d'une part, le fait que les propositions 113 et 114 impliquent le théorème est établi dans la sous-section **4.2**, et d'autre part, la proposition 115 est démontrée dans la sous-section **4.5**, à l'aide d'outils présentés dans les sous-sections **4.3** et **4.4**.

4.2 Lien entre majorations de $|N_n|_\infty, |N_n|_p$ et rationalité de la fonction zêta

L'intérêt d'étudier à la fois la valeur absolue archimédienne et la valeur absolue p-adique de N_n pour un certain p est donné par le lemme suivant.

Lemme 4.2.116 *Soit p un nombre premier, $n \in \mathbf{Z}^*$. On a $|n|_\infty \cdot |n|_p \geq 1$.*

Preuve Pour $n = 1$, c'est bon. Sinon, on voit en décomposant $|n|$ en produit de facteurs premiers que $|n|_\infty \cdot |n|_p = |n|p^{-v_p(n)} \geq 1$. □

Dorénavant, p désigne la caractéristique de $\mathbf{F}_q$, et on admet les propositions 113 et 114. On voudrait appliquer judicieusement le lemme ; or les propositions sus-citées et le critère de rationalité du théorème 17 font intervenir des éléments de $\mathbf{C}_p$ qui n'ont aucune raison d'être des entiers. Pour commencer, on se propose donc d'énoncer un nouveau critère de rationalité, dans $\mathbf{Q}$.

Un nouvel espoir On a le résultat suivant :

Proposition 4.2.117 *Soit $(c_n) \in \mathbf{Q}^{\mathbf{N}}$. S'équivalent :*

(i) la série $\sum c_n X^n$ est une fraction rationnelle ;

(ii) il existe $m \in \mathbf{N}$ et $(a_i)_{i\in[\![0,m]\!]} \in \mathbf{Q}^{m+1}$ (non nul) tels que pour tout n assez grand,

$$\sum_{0\leq i\leq m} a_i c_{n+i} = 0\,;$$

(iii) il existe $m \in \mathbf{N}$ tel que, pour tout n assez grand, $\det(c_{n+i+j})_{0\leq i,j\leq m} = 0$.

Preuve On a clairement $(i) \Leftrightarrow (ii) \Rightarrow (iii)$. Montrons $(iii) \Rightarrow (ii)$. Pour $n, m \in \mathbf{N}$, notons $M_{n,m}$ la matrice $(c_{n+i+j})_{0\leq i,j\leq m}$.

18. prendre $A = r$.

Observons que les m dernières colonnes de $M_{n,m}$ sont exactement les m premières de $M_{n+1,m}$, que la sous-matrice $m \times m$ « en haut à gauche » dans $M_{n,m}$ est $M_{n,m-1}$, et que la sous-matrice $m \times m$ « en haut à droite » dans $M_{n,m}$ est $M_{n+1,m-1}$.

Notons $(C^i_{n,m})_{0 \leq i \leq m}$ les colonnes de $M_{n,m}$. Soit $m \in \mathbf{N}$ minimal tel que $\det(M_{n,m}) = 0$ pour n assez grand. Si $m = 0$, c'est fini. Supposons $m \neq 0$.

Supposons qu'on dispose d'un entier N tel que $\det(M_{n,m}) = 0$ pour tout $n \geq N$, et $\det(M_{N,m-1}) = 0$. Alors $\det(M_{n,m-1}) = 0$ pour tout $n \geq N$: montrons-le par récurrence. Soit n vérifiant la propriété, c'est-à-dire tel que $\det(M_{p,m}) = 0$ si $p \geq n$ et $\det(M_{n,m-1}) = 0$, et montrons que $\det(M_{n+1,m-1}) = 0$.

On dispose de $(\lambda_i)_{i \in [\![0,m]\!]}, (\mu_i)_{i \in [\![0,m-1]\!]}$ tous deux non nuls tels que :

$$\sum_{i=0}^{m} \lambda_i C^i_{n,m} = 0 \text{ et } \sum_{i=0}^{m-1} \mu_i C^i_{n,m-1} = 0.$$

Si $\lambda_0 = 0$, il suffit d'enlever la dernière ligne de la première combinaison linéaire pour obtenir une dépendance non triviale entre les colonnes de $M_{n+1,m-1}$. De même si $\mu_0 = 0$. Supposons λ_0 et μ_0 non nuls. Comme pour tout $i \in [\![0, m-1]\!]$, $C^i_{n,m} = \begin{pmatrix} C^i_{n,m-1} \\ c_{n+m+i} \end{pmatrix}$, on a $(\star)$:

$$\begin{aligned} \mu_0 C^0_{n,m} &= \begin{pmatrix} -\sum_{i=1}^{m-1} \mu_i C^i_{n,m-1} \\ \mu_0 c_{n+m} \end{pmatrix} \\ &= \sum_{i=1}^{m-1} -\mu_i C^i_{n,m} + \begin{pmatrix} 0 \\ \vdots \\ 0 \\ \beta \end{pmatrix} \\ \text{où } \beta &= \sum_{i=0}^{m-1} \mu_i c_{n+m+i}. \end{aligned}$$

La multilinéarité du déterminant par rapport aux colonnes, ainsi que son caractère alterné, donnent :

$$0 = \mu_0 \det(M_{n,m}) = \det \begin{pmatrix} 0 & & \\ \vdots & C^1_{n,m} & \cdots & C^m_{n,m} \\ 0 & & \\ \beta & & \end{pmatrix} = (-1)^m \beta \det(M_{n+1,m-1}).$$

Donc si $\beta \neq 0$, $\det(M_{n+1,m-1}) = 0$ et si $\beta = 0$, il suffit d'enlever la première ligne de la combinaison linéaire $(\star)$ pour trouver une dépendance non triviale entre les colonnes de $M_{n+1,m-1}$ (c'est en effet la matrice $m \times m$ « en bas à gauche » dans $M_{n,m}$). Ainsi, $\det M_{n+1,m-1} = 0$ et la récurrence se propage bien.

Cela contredit la minimalité de m. Donc, contrairement à ce qu'on avait supposé, on dispose de N tel que pour tout $n \geq N$, $\det(M_{n,m-1}) \neq 0$. Ainsi pour tout $n \geq N$, $\operatorname{rg} M_{n,m} = m$. L'espace engendré par ses m premières colonnes est donc de dimension m, c'est le même que l'espace engendré par ses m dernières colonnes (ces deux sous-matrices possédant un mineur d'ordre m non nul) : par une récurrence immédiate, c'est donc un hyperplan de $\mathbf{Q}^{m+1}$ qui ne dépend pas de n. Cet hyperplan s'écrit :

$$\{(x_0, \ldots, x_m) \in \mathbf{Q}^{m+1} \mid a_0 x_0 + \ldots + a_m x_m = 0\},$$

d'où (ii) avec ces mêmes (a_i). □

Rationalité de $DL(\zeta)$ Ce critère, conjugué avec les propositions 113 et 114 permet de montrer la rationalité de la série formelle $\sum N_n X^n$.

En effet, soit A tel que $\forall\, n \in \mathbf{N}$, $|N_n|_\infty \leq q^{An}$. Alors, avec les notations de la preuve précédente (c'est la suite N qui joue le rôle de c), $|\det(M_{n,m})|_\infty \leq (m+1)!\, q^{A(n(m+1)+m(m+1)/2)}$ pour tous $n, m \in \mathbf{N}$.

D'autre part, on dispose de $\alpha_1, \ldots, \alpha_k, \beta_1, \ldots, \beta_{k'}$ tels que pour tout n,

$$\left| N_n - \sum_j \beta_j^n + \sum_i \alpha_i^n \right|_p \leq q^{-(A+1)n}.$$

Donc :

$$M_{n,m} = \sum_j B_{n,m}^j - \sum_i A_{n,m}^i + E_{n,m}$$

avec $A_{n,m}^i = (\alpha_i^{n+k})_{0\leq k\leq m}$, $B_{n,m}^j = (\beta_j^{n+k})_{0\leq k\leq m}$ et $E_{n,m}$ une matrice d'erreur dont tous les coefficients sont de valeur absolue p-adique inférieure à $q^{-(A+1)n}$. Par multilinéarité du déterminant par rapport aux colonnes, il vient, et en remarquant que deux colonnes de la même matrice $A_{n,m}^i$ ou $B_{n,m}^i$ sont toujours liées :

$$|\det(M_{n,m})|_p = \left| \sum_{\substack{I\subset[\![0,m]\!] \\ |I|\leq k+k'}} \sum_{\substack{\sigma: I\to[\![1,k+k']\!] \\ \text{injective}}} \det\left(M_{I,\sigma}\right) \right|_p$$

où $M_{I,\sigma}$ est la matrice dont la i-ième colonne

$$\text{est} \begin{cases} \text{la } i\text{-ième colonne de } -A_{n,m}^{\sigma(i)} & \text{si } i \in I \text{ et } \sigma(i) \leq k, \\ \text{la } i\text{-ième colonne de } B_{n,m}^{\sigma(i)-k} & \text{si } i \in I \text{ et } \sigma(i) > k, \\ \text{la } i\text{-ième colonne de } E_{n,m} & \text{sinon,} \end{cases}$$

où I correspond aux rangs des colonnes qui seront des colonnes de matrices $A_{n,m}^i$ ou $B_{n,m}^i$, σ choisit dans quelle matrice on pioche ces colonnes, son injectivité résulte de la remarque,

$$\leq \max_{\substack{I\subset[\![0,m]\!] \\ |I|\leq k+k' \\ \sigma: I\to[\![1,k+k']\!] \\ \text{injective}}} |\det(M_{I,\sigma})|_p$$

Or, soient $I \subset [\![0; m]\!]$ avec $|I| \leq k + k'$, puis $\sigma : I \longmapsto [\![1; k + k']\!]$ injective. On a par inégalité ultramétrique :

$$|\det(M_{I,\sigma})|_p \leq \max_{f\in\mathfrak{S}([\![0,m]\!])} \prod_{i=0}^m |[M_{I,\sigma}]_{i,f(i)}|_p$$

Soit donc $f \in \mathfrak{S}([\![0; m]\!])$, on a, pour $C = 1 + \max\left(\max_i |\alpha_i|_p, \max_j |\beta_j|_p\right)$,

$$\begin{aligned} \prod_{i=0}^m |[M_{I,\sigma}]_{i,f(i)}|_p &\leq \prod_{i\notin I} |[M_{I,\sigma}]_{i,f(i)}|_p \prod_{i\in I} |[M_{I,\sigma}]_{i,f(i)}|_p \\ &\leq \prod_{i\notin I} q^{-(A+1)n} \prod_{i\in I} C^{n+i+f(i)} \\ &\leq C^{n|I|+2|I|m} q^{-(A+1)n(m+1-|I|)} \\ &\leq C^{(n+2m)(k+k')} q^{-(A+1)n(m+1-k-k')} \end{aligned}$$

Ainsi,

$$|\det(M_{n,m})|_\infty \cdot |\det(M_{n,m})|_p \leq C^{(n+2m)(k+k')}(m+1)! q^{A[n(m+1)+m(m+1)/2]-(A+1)n(m+1-k-k')}.$$

Figeons $m \geq 1$ assez grand pour que $(A+1)(m+1-k-k') > A(m+1)+(k+k')\log_q(C)$. Soit $\delta = C^{k+k'} q^{-(A+1)(m+1-k-k')} q^{A(m+1)} < 1$, on a :

$$|\det(M_{n,m})|_\infty \cdot |\det(M_{n,m})|_p \leq C^{2m(k+k')}(m+1)!\, q^{m(m+1)/2}\delta^n < 1$$

si n est assez grand, donc pour n assez grand, par le lemme 116, $\det(M_{n,m}) = 0$.

D'après la proposition 117, la série formelle $\sum N_n X^n$ est donc rationnelle.

Raffinements pour la rationalité de ζ

L'argument développé *supra* ne suffit pas à conclure immédiatement car $\frac{\zeta'}{\zeta}$ rationnelle n'implique pas ζ rationnelle. Plus que la rationalité de $DL(\zeta)$, il faut donc en retenir le fait qu'il existe $(a_i)_{0\leq i\leq m} \in \mathbf{Z}^{m+1}$ tels que

$$\sum_{i=0}^{m} a_i N_{n+i} = 0$$

pour tout n assez grand. On peut supposer $a_m \neq 0$ et noter $\pi \in \mathbf{Z}[X]$ un polynôme caractéristique associé à cette relation de récurrence.

Lemme 4.2.118 *Soient $r > 0$, K un corps muni d'une valeur absolue $|\cdot|$, $c_1, \ldots, c_d \in K$, $u_1, \ldots, u_d \in K$. Supposons que les u_i soient deux à deux distincts et que*

$$\left|\sum_{k=1}^{d} c_k u_k^n\right| \underset{n\to+\infty}{=} O(r^n)$$

Alors, pour tout $1 \leq i \leq d$, si $c_i \neq 0$, alors $|u_i| \leq r$.

Preuve On raisonne par l'absurde. Quitte à enlever les termes $c_i u_i^n$, quand $|u_i| \leq r$ ou $c_i = 0$, on peut supposer que pour tout i, $|u_i| > r$ et $c_i \neq 0$. On suppose également que d est le plus petit entier pour lequel le résultat est invalidé. Clairement, on ne peut pas avoir $d = 1$, donc $d \geq 2$. On a alors

$$\left|\sum_{k=1}^{d-1} c_k(u_k - u_d)u_k^n\right| = \left|\sum_{k=1}^{d} c_k u_k^{n+1} - u_d \sum_{k=1}^{d} c_k u_k^n\right| \underset{n\to+\infty}{=} O(r^n)$$

par inégalité triangulaire. Or, les u_i, $1 \leq i < d$ sont deux à deux distincts, de module minoré strictement par r, et on a, pour chaque $1 \leq i < d$, $c_i(u_i - u_d) \neq 0$, ce qui contredit la minimalité de d, ce qui achève la preuve. □

Corollaire 4.2.119 *Soient $\alpha_1, \ldots, \alpha_d \in \mathbf{C}_p^*$, deux à deux distincts, $n_1, \ldots n_d \in \mathbf{Z} \setminus \{0\}$ et $A > 0$ tels que pour chaque i, $|\alpha_i|_p > q^{-A}$, et*

$$\forall n \geq 1, \left|N_n - \sum_{i=1}^{d} n_i \alpha_i^n\right|_p \leq q^{-An}.$$

Soit $A' > A$. Soient $\beta_1, \ldots, \beta_g \in \mathbf{C}_p^*$, deux à deux distincts, $m_1, \ldots, m_g \in \mathbf{Z} \setminus \{0\}$ tels que pour chaque i, $|\beta_i|_p > q^{-A'}$, et

$$\forall n \geq 1, \left|N_n - \sum_{i=1}^{g} m_i \beta_i^n\right|_p \leq q^{-A'n}.$$

Alors il existe une bijection $f : [\![1;d]\!] \to \{j \in [\![1;g]\!] \mid |\beta_j|_p > q^{-A}\}$, *telle que* $\alpha_i = \beta_{f(i)}$ *et* $n_i = m_{f(i)}$.

Preuve Il suffit d'observer que par inégalité ultramétrique,

$$\forall n \geq 1, \left| \sum_{i=1}^{d} n_i \alpha_i^n - \sum_{j=1}^{g} m_j \beta_j^n \right|_p \leq q^{-An},$$

et d'appliquer le lemme. □

Proposition 4.2.120 *Soient* $\alpha_1, \dots, \alpha_d \in \mathbf{C}_p^*$, *deux à deux distincts,* $n_1, \dots n_d \in \mathbf{Z} \setminus \{0\}$ *et* $A > 0$ *tels que pour chaque* i, $|\alpha_i|_p > q^{-A}$, *et*

$$\forall n \geq 1, \left| N_n - \sum_{i=1}^{d} n_i \alpha_i^n \right|_p \leq q^{-An}.$$

Alors $\pi(\alpha_i) = 0$ *pour tout* i.

Preuve Notons $\pi(X) = \sum_{j=0}^{m} a_j X^j$. Alors, pour tout n assez grand,

$$\left| \sum_{i=1}^{d} n_i \alpha_i^n \pi(\alpha_i) \right|_p \leq \left| \sum_{i=1}^{d} \sum_{j=0}^{m} n_i a_j \alpha_i^{n+j} - \sum_{j=0}^{m} a_j N_{n+j} \right|_p \leq \max_{0 \leq j \leq m} |a_j|_p q^{-A(n+j)} = O(q^{-An}).$$

D'après le lemme 118, comme $|\alpha_i|_p > q^{-A}$ pour tout i, on en déduit que pour tout i, $n_i \pi(\alpha_i) = 0$, donc $\pi(\alpha_i) = 0$. □

Corollaire 4.2.121 *Notons* $\pi = \sum_{i=0}^{m} a_i X^i \in \mathbf{Z}[X]$ *un polynôme caractérisant la relation de récurrence satisfaite par* (N_n). *Notons* $\alpha_1, \dots \alpha_a$ *ses racines non nulles dans* $\mathbf{C}_p$. *Pour tout* $A > 0$, *il existe* $(n_i(A)) \in \mathbf{Z}^a$ *tel que*

$$\forall n \geq 1, \left| N_n - \sum_{i=1}^{a} n_i(A) \alpha_i^n \right|_p \leq q^{-An}$$

Preuve Découle immédiatement de ce qui précède et de la proposition 114. □

Corollaire 4.2.122 *Soient* $0 < A < A'$. *Supposons que pour tout* i, $|\alpha_i|_p > q^{-A}$. *Alors* $n_i(A) = n_i(A')$ *pour chaque* i.

Preuve Découle du corollaire 119. □

Ainsi, en admettant la proposition 115, on établit la première conjecture de Weil :

Théorème 4.2.18 ζ_I *est rationnelle.*

Preuve Ce qui précède immédiatement permet d'assurer qu'il existe $n_1, \dots, n_a \in \mathbf{Z}$ tels que pour tout $A > 0$ assez grand, pour tout $n \in \mathbf{N}^*$,

$$\left| N_n - \sum_{i=1}^{a} n_i \alpha_i^n \right|_p \leq q^{-An}.$$

En faisant tendre A vers $+\infty$, on en déduit que

$$\forall n \geq 1, N_n = \sum_{i=1}^{a} n_i \alpha_i^n,$$

ce qui conclut d'après le premier résultat de la section. □

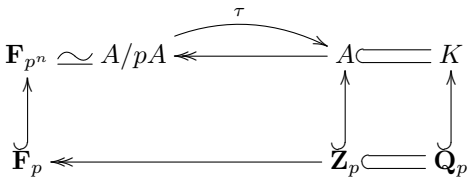

FIGURE 2 – Extensions et corps résiduels

4.3 Relèvement de Teichmüller

Dans tout cette sous-section, on se donne p premier et χ un caractère de $\mathbf{F}_p$ dans $\mathbf{C}_p^*$.

Définition On note $\overline{\mathbf{F}_p}$ la clôture algébrique de $\mathbf{F}_p$.

Remarque 4.3.29 C'est la « réunion » des $\mathbf{F}_{p^n}$, recollés par les morphismes d'inclusion qu'on a exhibé lors de l'étude des corps finis dans la proposition 5. Attention, $\overline{\mathbf{F}}_p$ est notamment plus compliquée qu'une simple limite projective.

Définition Pour tout $n \in \mathbf{N}^*$, on note μ_n le groupe des n-racines de l'unité dans $\mathbf{C}_p$.

Définition Par ailleurs, on se munit dorénavant et jusqu'à la fin de la section de la notation vectorielle des opérations : si E, F sont des ensembles, $f : E \to F$ une application, $d \in \mathbf{N}$, $x = (x_1, \dots, x_d) \in E^d$, on note $f(x) = (f(x_1), \dots, f(x_d)) \in F^d$.

On se propose d'établir le théorème suivant, qui est central pour montrer la formule des traces dans la sous-section **4.4**, et partant pour prouver l'existence d'une décomposition de la fonction zêta dans la sous-section **4.5**.

Théorème 4.3.19 *Il existe une application $\tau : \overline{\mathbf{F}_p}^* \to \mathbf{C}_p^*$, appelée morphisme relevant de Teichmüller, avec les propriétés suivantes :*

- *l'application τ est un morphisme (multiplicatif) et pour tout $n \in \mathbf{N}^*$, sa restriction sur $\mathbf{F}_{p^n}^*$ co-restreinte à μ_{p^n-1} est un isomorphisme,*
- *il existe une série formelle*

$$\Theta(X) = \sum_0^\infty a_k X^k$$

avec $|a_k|_p \leq p^{-k/p-1}$ pour tout $k \in \mathbf{N}$, telle que, pour tout $n \in \mathbf{N}^*$ et tout $x \in \mathbf{F}_{p^n}$:

$$\chi \circ \mathrm{tr}_n(x) = \Theta(\tau(x))\Theta(\tau(x)^p) \cdots \Theta(\tau(x)^{p^{n-1}}).$$

Remarque 4.3.30 Clairement, si on tel τ existe, il n'est pas unique : tous les τ^{p^k} sont aussi des morphismes relevant de Teichmüller.

Preuve La preuve se déroule en trois étapes : on commence par définir, pour $n \in \mathbf{N}^*$ fixé, un isomorphisme $\tau_n : \mathbf{F}_{p^n}^* \to \mu_{p^n-1}$. On vérifie ensuite la compatibilité des τ_n, et on définit donc immédiatement leur recollement τ. Enfin, on définit la série formelle Θ, et on majore la valuation p-adique de ses coefficients comme dans l'énoncé.

Première étape : Construction de τ_n

Soit $\alpha \in \mathbf{F}_{p^n}^*$ un générateur. Soit P unitaire de degré n son polynôme minimal sur $\mathbf{F}_p$ et $\tilde{P}$ un relèvement de P dans $\mathbf{Z}_p[X]$. Soit β une racine de $\tilde{P}$, d'après la remarque 27, si on note A l'anneau de valuation de $\mathbf{Q}_p(\beta)$, on a un isomorphisme ι_n de $\mathbf{F}_{p^n}$ dans A/pA.

Soit $\gamma \in \mathbf{F}_{p^n}^*$, on a $\gamma^{p^n-1} = 1$. En appliquant le lemme de Hensel, alias le lemme 81, au polynôme $X^{p^n-1} - 1$ de $A[X]$ avec la racine $\iota_n(\gamma)$, on peut trouver un unique relèvement $\tau_n(\gamma) \in \mathbf{Q}_p(\beta)$ de $\iota_n(\gamma)$ tel que $\tau_n(\gamma)^{p^n-1} = 1$, ie $\tau_n(\gamma) \in \mu_{p^n-1} \subset A$. Par construction,

τ_n est injective, et par égalité des cardinaux, τ_n est une bijection de $\mathbf{F}_{p^n}^*$ dans μ_{p^n-1}. La bijection réciproque est une restriction de la projection $A \to A/pA$, composée avec ι_n^{-1}, c'est un morphisme de groupes. Donc τ_n est également un morphisme de groupes.

Deuxième étape : Construction de τ par recollement des τ_n

On procède en deux temps, avec le même principe que dans la preuve de la proposition 55 :

Lemme 4.3.123 *Si $d, n \in \mathbf{N}^*$ tels que $d \mid n$. Si $\tilde{\tau_d}$ est un isomorphisme de $\mathbf{F}_{p^d}^*$ dans μ_{p^d-1}, il existe un isomorphisme de $\mathbf{F}_{p^n}^*$ dans μ_{p^n-1}, noté $\tilde{\tau_n}$, qui prolonge $\tilde{\tau_d}$.*

Preuve Soit τ_n le morphisme qu'on vient de définir, il vérifie la condition d'isomorphisme et il envoie donc l'ensemble des éléments d'ordre multiplicatif divisant $p^d - 1$ de $\mathbf{F}_{p^d}^*$ sur le même ensemble dans μ_{p^n-1}, c'est-à-dire que τ_n induit un isomorphisme de $\mathbf{F}_{p^d}^*$ sur μ_{p^d-1}.

Soit α un générateur de $\mathbf{F}_{p^d}^*$. Posons $\beta = \tau_n(\alpha)$, c'est un générateur de μ_{p^d-1}, on a donc $\{\beta^k \mid 1 \leq k \leq p^d - 1 \text{ premier avec } p^d - 1\}$ égal (pour des raisons d'inclusion et de cardinal) à l'ensemble des générateurs de μ_{p^d-1}. Soit finalement k premier avec $p^d - 1$ tel que $\beta^k = \tilde{\tau_d}(\alpha)$. Comme on l'a déjà vu dans la preuve du lemme 54, on dispose de $t \in \mathbf{Z}$ tel que $k + t(p^d - 1)$ soit premier avec $p^n - 1$. On pose $\tilde{\tau_n} = \tau_n^{k+t(p^d-1)}$, et cela convient. □

On pose donc à bon droit τ l'application de $\overline{\mathbf{F}_p}$ dans $\mathbf{C}_p^*$ obtenue par prolongements successifs des morphismes $(\tau_{d!})$. [19]

Lemme 4.3.124 *Cette application τ est un morphisme et pour tout $n \in \mathbf{N}$, elle induit une bijection de $\mathbf{F}_{p^n}^*$ dans μ_{p^n-1}.*

Preuve Soit $n \in \mathbf{N}$. On a $d \in \mathbf{N}$ tel que $n \mid d!$. On sait que τ induit une bijection de $\mathbf{F}_{p^{d!}}^*$ dans $\mu_{p^{d!}-1}$ par définition, donc dans ces groupes les ensembles des éléments d'ordre $p^n - 1$ sont envoyés l'un sur l'autre, donc τ induit bien une bijection de $\mathbf{F}_{p^n}^*$ dans μ_{p^n-1}. □

Intermezzo : Une propriété utile de τ

Avant de définir Θ, attardons-nous sur un point de théorie de Galois qui resservira par la suite. Soit $x \in \overline{\mathbf{F}_p}^*$, et $n \in \mathbf{N}^*$ minimal tel que $x \in \mathbf{F}_{p^n}^*$. On connaît bien les conjugués de Galois de x sur $\mathbf{F}_p$; mais qu'en est-il des conjugués de Galois de $\tau(x)$ sur $\mathbf{Q}_p$?

Lemme 4.3.125 *Les conjugués de Galois de $\tau(x)$ sur $\mathbf{Q}_p$ sont les $\tau(x)^p, \ldots, \tau(x)^{p^{n-1}}$.*

Preuve Écrivons un peu mieux dans quels corps et avec quelles extensions nous travaillons. Reprenons pour ce faire les notations de la section **3.5** : soit P le polynôme minimal de x. Or, x engendrant $\mathbf{F}_{p^n}$ en tant que corps, P est de degré n. On relève P en un $\tilde{P}$ de $\mathbf{Z}_p[X]$. Soit β une racine de $\tilde{P}$ dans $\overline{\mathbf{Q}_p}$, posons $K = \mathbf{Q}_p(\beta)$, A son anneau de valuation. On a en pratique $x \in A/pA$ et $\tau(x) \in A$, et les divers objets qui leur sont reliés vivent essentiellement dans les corps et anneaux représentés sur le diagramme commutatif 2.

Soit $Q \in \mathbf{Q}_p[X]$ le polynôme minimal de $\tau(x) \in Q_p(\beta)$ sur $\mathbf{Q}_p$, alors Q est de degré au plus n. Comme $\tau(x)$ est un élément de μ_{p^n-1}, Q divise $X^{p^n-1} - 1$ donc toutes ses racines sont de valeur absolue 1. Les coefficients de Q sont donnés, au signe près, par les polynômes symétriques élémentaires en les racines, donc par inégalité ultramétrique, ils sont de valeur absolue inférieure ou égale à 1. Ainsi, Q est à coefficients dans $\mathbf{Z}_p$. De plus, sa réduction modulo p est unitaire et annule x, donc est divisible par P, mais est de degré inférieur au degré de P (regarder dans le diagramme commutatif 2, où les flèches verticales et les flèches qui vont vers la gauche sont bien toutes des morphismes d'anneau). Comme les deux polynômes sont unitaires, P est la réduction modulo p de Q et Q est de degré n.

Or, toujours comme Q divise $X^{p^n-1} - 1$, les conjugués de Galois de $\tau(x)$ sont de la forme $\tau(y)$ pour $y \in \mathbf{F}_{p^n}^*$. Soit y tel que $\tau(y)$ soit effectivement un conjugué de Galois de $\tau(x)$. On a, en réduisant dans notre diagramme, $P(y) = 0$. Donc y est un conjugué de Galois de x, d'où $y = x^{p^m}$ pour un $m \in [\![0, n-1]\!]$.

19. en toute rigueur, il s'agit plutôt de la suite définie par récurrence dont le premier terme est τ_1 et le $(d+1)$-ième terme est le prolongement du d-ième terme de $\mathbf{F}_{p^{(d+1)!}}^*$ dans $\mu_{p^{(d+1)!}-1}$.

Or Q est de degré n et irréductible dans $\mathbf{Q}_p$ donc à racines simples (voir la première partie de la preuve de 14, qui se simplifi car on est en caractéristique nulle), donc cette condition nécessaire est suffisante, et les conjugués de Galois de $\tau(x)$ sont exactement les $\tau(x^{p^m})$ pour $m \in [\![0; n-1]\!]$. □

Troisième étape : Définition de Θ

On pose[20] $\lambda = \chi(1) - 1 \in \mathbf{C}_p$ et $\Theta(T) = F(T, \lambda)$, où $F(T, Y)$ est la série formelle en deux variables définie par :

$$F(T,Y) = (1+Y)^T \prod_{j=1}^{\infty} (1+Y^{p^j})^{(T^{p^j}-T^{p^{j-1}})/p^j}.$$

On vérifie tout d'abord un certain nombre de propriétés de bonne définition.

Lemme 4.3.126 *$F(T, Y)$ est effectivement bien définie en tant que série formelle.*

Preuve D'après la définition de l'exponentiation dans le paragraphe « Séries formelles en plusieurs variables » de la section **1.3**, $(1+Y)^T$ et chaque terme $(1+Y^{p^j})^{(T^{p^j}-T^{p^{j-1}})/p^j}$ sont bien définis comme séries formelles de plusieurs variables. On remarque par ailleurs que, pour $j \in \mathbf{N}^*$, tous les monômes de la série entière $(1+Y^{p^j})^{(T^{p^j}-T^{p^{j-1}})/p^j} - 1$ ont un degré en l'indéterminée Y supérieur ou égal à p^j.

Soit $(y, t) \in \mathbf{N}^2$. On pose $a_{t,y}$ le coefficient devant $T^t Y^y$ dans la série formelle

$$(1+Y)^T \prod_{j=1}^{\lceil \log_p(y) \rceil} (1+Y^{p^j})^{(T^{p^j}-T^{p^{j-1}})/p^j}.$$

On définit ainsi une nouvelle série formelle $\sum a_{t,y} T^t Y^y$, et on vérifie formellement qu'il s'agit bien de F. □

Dorénavant, on note effectivement $F(T, Y) = \sum a_{t,y} T^t Y^y$.

Lemme 4.3.127 *Soit $t \in \mathbf{C}_p$. $F(t, Y)$ est bien définie en tant que série formelle en Y.*

Preuve Chaque terme du produit est bien défini d'après le paragraphe « Exponentiation d'une série formelle » de la sous-section **1.3**. On vérifie que la distance (au sens de la sous-section **1.3**) de chaque facteur à 1 tend vers 0. On conclut à l'aide de la section **3.4** □

Lemme 4.3.128 *Soit $y \in \mathbf{C}_p$. $F(T, y)$ est bien définie en tant que série formelle en T, et pour tout $n \in \mathbf{N}$, son coefficient t_n devant T^n vérifie $|t_n|_p \leq p^{-n/(p-1)}$.*

Preuve Un changement d'un indice dans la définition de F permet d'établir que :

$$F(T^p, Y^p) = F(T,Y)^p \frac{(1+Y^p)^T}{(1+Y)^{pT}}.$$

D'autre part, il existe $G \in \mathbf{Z}_p[Y]$ tel que $1 + Y^p = pYG(Y) + (1+Y)^p$, de sorte que, comme $(1+Y)^{-p}$ définit une série formelle à coefficients dans $\mathbf{Z}_p$, on pose $H(Y) = G(Y)(1+Y)^{-p}$ série formelle à coefficients dans $\mathbf{Z}_p$ telle que :

$$F(T^p, Y^p)^p = F(T,Y)^p (1 + pYH(Y))^T,$$

donc, en développant, il existe $S(T, Y)$ série formelle à coefficients dans $\mathbf{Z}_p$ telle que $S(0, 0) = 0$ et :

$$F(T^p, Y^p)^p = F(T,Y)^p (1 + pS(T,Y)).$$

20. un peu miraculeusement, il est vrai...

En effet,

$$(1+pYH(Y))^T = 1+\sum_{i=1}^{\infty} \underbrace{\frac{p^i}{i!}}_{\substack{\in \mathbf{Z}_p \text{ d'après} \\ \text{la formule} \\ \text{de Legendre}}} Y^i H(Y)^i T(T+1)\cdots(T+i-1).$$

Notons $S(T,Y) = \sum s_{t,y} T^t Y^y$. On a, pour tout $(a,b) \in \mathbf{N}^2$, l'équation suivante :

$$\mathbb{1}(p \mid a \text{ et } p \mid b) a_{a/p,b/p} = \sum_{\substack{t_1+\ldots+t_p=a \\ y_1+\ldots+y_p=b}} a_{t_1,y_1}\ldots a_{t_p,y_p} + p \sum_{\substack{t_1+\ldots+t_p+t'=a \\ y_1+\ldots+y_p+y'=b}} a_{t_1,y_1}\ldots a_{t_p,y_p} s_{t',y'}.$$

Montrons par récurrence (pour l'ordre lexicographique sur les couples d'indices) que les coefficients $a_{a,b}$ sont tous dans $\mathbf{Z}_p$.

Si a ou b n'est pas divisible par p, alors, comme $a_{0,0} = 1$, $a_{a,b}$ apparaît exactement p fois dans le membre de droite et tous les autre termes apparaissent un nombre multiple de p fois (c'est clair pour la deuxième somme : pour les termes de la première somme, on voit en permutant les indices de sommation sous l'action de $\mathbf{Z}/p\mathbf{Z}$ qu'un produit donné apparaît p fois, sauf si tous les indices sont égaux : $(t_i,y_i) = (t_j,y_j)$ pour tous i,j, *ie* $(t_i,y_i) = (a/p, b/p)$ pour tout i, et on a déjà exclus ce cas). Donc $pa_{a,b} \in p\mathbf{Z}_p$, d'où $a_{a,b} \in \mathbf{Z}_p$.

Si a et b sont divisibles par p, le même argument que précédemment aboutit à : $a_{a/p,b/p} = pa_{a,b} + a_{a/p,b/p}$ + un élément de $p\mathbf{Z}_p$. Donc là encore, $a_{a,b} \in \mathbf{Z}_p$.

D'autre part, $(1+\lambda)^p = 1$ et $\lambda \neq 0$, donc λ a pour polynôme annulateur sur $\mathbf{Q}_p$ le polynôme :

$$X^{p-1} + X^{p-2}\binom{p}{p-1} + \ldots + X\binom{p}{2} + p,$$

qui est même son polynôme minimal d'après le critère d'irréductibilité d'Eisenstein [21] dans $\mathbf{F}_p$ et d'après le lemme 80 pour remonter l'irréductibilité dans $\mathbf{Q}_p$. Donc le produit des $p-1$ conjugués de Galois de λ est de valeur absolue p-adique p^{-1}, donc $|\lambda|_p = p^{-1/(p-1)}$, par définition du prolongement de la norme.

Ainsi, en combinant les deux points qu'on vient de montrer, uniformément en $n \in \mathbf{N}$,

$$|a_{n,y}\lambda^y|_p \leq p^{-y/(p-1)} \underset{y\to\infty}{\longrightarrow} 0,$$

donc $\sum a_{n,y}\lambda^y$ converge dans $\mathbf{C}_p$. Donc $\Theta(T) = F(T,\lambda)$ est bien définie.

De surcroît, comme le stipule la remarque 12, si on écrit $\Theta(T) = \sum t_n T^n$, on a en fait

$$|t_n|_p = \left|\sum_{y\geq n} a_{n,y}\lambda^y\right|_p \leq |\lambda^n|_p = p^{-n/(p-1)},$$

ce qui conclut la preuve du lemme. □

Tout cela nous a largement permet de montrer que Θ est bien défini. Vérifions maintenant son équation fonctionnelle. Soit $n \in \mathbf{N}^*$, $x \in \mathbf{F}_{p^n}^*$. Comme $\tau(x)^{p^n} = \tau(x)$, un télescopage donne :

$$F(\tau(x),Y)F(\tau(x)^p,Y)\ldots F(\tau(x)^{p^{n-1}},Y) = (1+Y)^{\tau(x)+\tau(x)^p+\ldots+\tau(x)^{p^{n-1}}}.$$

On évalue alors en λ défini au début de l'étape, et il vient :

$$\Theta(\tau(x))\Theta(\tau(x)^p)\cdots\Theta(\tau(x)^{p^{n-1}}) = \chi(\tau(x)+\tau(x)^p+\ldots+\tau(x)^{p^{n-1}}).$$

21. pour un énoncé et une preuve de ce critère, voir [GFN01]

Il reste néanmoins à justifier la possibilité de faire les évaluations dans cet ordre. Pour $|a|_p \leq 1$,

$$\Theta(a) = \sum_{n\geq 1} t_n a^n = \sum_{n\geq 1}\sum_{y\geq 1} a_{n,y} a^n \lambda^y.$$

Pour que l'interversion soit licite, il suffit que la famille étudiée soit sommable, *ie* qu'elle tend vers zéro au sens des suites généralisées. Si $|a|_p \leq 1$, comme $|a_{n,y}\lambda^y|_p \leq p^{-y/(p-1)}$, c'est gagné.

Or $\tau(x) + \tau(x)^p + \ldots + \tau(x)^{p^{n-1}} \in \mathbf{Q}_p$, puisque c'est l'opposé du coefficient devant X^{n-1} du polynôme minimal de $\tau(x)$, d'après l'intermezzo. De plus, cet élément de $\mathbf{Q}_p$ est de valeur absolue inférieure ou égale à 1, donc c'est un entier p-adique. Donc on a, modulo $p\mathbf{Z}_p$,

$$\tau(x) + \tau(x)^p + \ldots + \tau(x)^{p^{n-1}} = x + x^p + \ldots + x^{p^{n-1}} = \mathrm{tr}_{\mathbf{F}_{p^n}/\mathbf{F}_p}(x).$$

Finalement, $\chi(\tau(x) + \tau(x)^p + \ldots + \tau(x)^{p^{n-1}}) = \chi \circ \mathrm{tr}_{\mathbf{F}_{p^n}/\mathbf{F}_p}(x)$, ce qui conclut la preuve d'existence d'un morphisme relevant de Teichmüller. □

4.4 Formule des traces

Pour pouvoir établir l'existence d'une décomposition de la fonction ζ comme produit de fonctions entières dans la section **4.5**, on doit connaître des fonctions entières qui ressemblent à la fonction ζ. Même si la ressemblance n'est pas encore frappante, on va relier ζ à une fonction de la forme :

$$\exp\left(-\sum_{n=1}^{\infty} \frac{\mathrm{tr}_R(\Psi^n)X^n}{n}\right),$$

pour un certain opérateur Ψ sur un certain espace vectoriel de séries formelles R, avec une certaine fonction tr_R qu'on note abusivement comme une trace. Or le maillon essentiel de ce lien est la formule dite des traces, que nous allons énoncer et démontrer dans cette sous-section.

Soit $d \in \mathbf{N}^*$, on travaille ici avec des séries formelles en d variables sur $\mathbf{C}_p$. On s'autorise l'abus de notation suivant : quand on définit une série formelle avec une somme sans bornes précisées et avec une variable muette, il faut sommer la variable muette sur $\mathbf{N}^d$. On garde également la notation vectorielle des opérations introduite à l'orée de la sous-section **4.3**.

Définition Pour $w = (w_1, \ldots, w_d) \in \mathbf{N}^d$, on définit l'application $\mathbf{N}$-linéaire [22] de *poids* par $|w| = w_1 + \ldots + w_d$.

Pour commencer, nous allons définir un espace de séries entières en d variables qui nous intéresse, et définir, pour chaque série entière G de cet espace, un certain opérateur linéaire Ψ_G sur $\mathbf{C}_p[\![X_1, \ldots, X_d]\!]$, dit l'*opérateur associé* à G.

Série formelle rapidement décroissante et opérateur associé

Définissons une classe un peu restreinte de séries formelles, comme les séries formelles susceptibles de converger quand on les spécialise :

Définition Une série formelle $G(X) = \sum_{n\in\mathbf{N}^d} a_n X^n$ sur $\mathbf{C}_p$ est dite *rapidement décroissante* ou encore *à décroissance rapide* s'il existe $M > 0$ tel que pour tout $n \in \mathbf{N}^d$, $|a_n|_p \leq p^{-M|n|}$.

L'ensemble des séries formelles à décroissance rapide a un peu de structure, comme le montrent les résultats suivants :

Lemme 4.4.129 *Soient $G(X)$ une série formelle à décroissance rapide, $m \in \mathbf{N}^*$. Alors $G(X^m) := G(X_1^m, \ldots, X_d^m)$ est à décroissance rapide.*

Preuve Si $G(X) = \sum a_w X^w$ avec, pour un $M > 0$, pour tout $w \in \mathbf{N}^d$, $|a_w|_p \leq p^{-M|w|}$, alors $G(X^m) = \sum \mathbb{1}(m \mid w) a_{w/m} X^w$.

22. c'est-à-dire qui respecte l'addition de $\mathbf{N}^d$ et la multiplication par un élément de $\mathbf{N}$.

Soit donc $w \in \mathbf{N}^d$. Si m divise w (coordonnée par coordonnée),

$$|\mathbb{1}(m \mid w) a_{w/m}|_p \leq |a_{w/m}|_p \leq p^{-|w|M/m};$$

cette inégalité est vraie *a fortiori* si m ne divise pas w, ce qui conclut. □

Lemme 4.4.130 *Soient $F(X) = \sum a_w X^w$, $G(X) = \sum b_w X^w$ deux séries formelles dans $\mathbf{C}_p$ à décroissance rapide. Alors $(FG)(X)$ est aussi à décroissance rapide.*

Preuve Si $M_1, M_2 > 0$ sont associés aux décroissances rapides de F et de G, soit $M = \min(M_1, M_2)$, $(FG)(X) = \sum c_w X^w$, où $c_w = \sum_{u+v=w} a_u b_v$. Par conséquent,

$$|c_w|_p \leq \sup_{u+v=w} |a_u|_p |b_v|_p \leq \sup_{u+v=w} p^{-M|u|} p^{-M|v|} \leq p^{-M|w|}.$$

□

Lemme 4.4.131 *Soient $z \in \mathbf{C}_p$ de valeur absolue 1, $F(X)$ série formelle dans $\mathbf{C}_p$ en d variables et rapidement décroissante. Alors $F(zX)$ est rapidement décroissante.*

Pour pouvoir énoncer la formule des traces, on introduit encore les opérateurs suivants sur les séries formelles :

Définition Soit $n \geq 2$. Si $F(X) = \sum a_w X^w$ est une série formelle en d variables sur $\mathbf{C}_p$, on pose $T_n(F) = \sum a_{nw} X^w$. T_n est un endomorphisme de $\mathbf{C}_p[\![X_1, \ldots, X_d]\!]$.

Lemme 4.4.132 *Soient $n, m \geq 2$. On a $T_n \circ T_m = T_{nm}$.*

Définition Soient $G(X)$ une série formelle sur $\mathbf{C}_p$ à décroissance rapide, $n \geq 2$. On pose $\Psi_{n,G} = F \longmapsto T_n(F(X)G(X))$ endomorphisme de $\mathbf{C}_p[\![X_1, \ldots, X_d]\!]$. Il s'agit de l'*opérateur associé* à G pour l'entier n.

Expression des itérées d'un opérateur associé

On fixe, dans ce paragraphe, un entier $m \geq 2$, une série formelle $G(X) = \sum c_w X^w$ en d variables sur $\mathbf{C}_p$ à décroissance rapide, $M > 0$ fixé associé par la définition de la décroissance rapide, $\Psi = \Psi_{m,G}$ l'opérateur associé.

Posons, pour $i, j \in \mathbf{N}^d$, $g_{i,j}^{(1)} = \mathbb{1}(qj - i \in \mathbf{N}^d) c_{qj-i}$.

Lemme 4.4.133 *Soient $m \geq 1$, $i, j \in \mathbf{N}^d$.*

Il y a un nombre fini de suites $i = v_0, v_1, \ldots, v_{m-1}, v_m = j \in \mathbf{N}^d$ telles que pour chaque $0 \leq t < m$, $g_{v_t, v_{t+1}}^{(1)}$ soit non nul. Ce nombre est nul si $q^n j - i \notin \mathbf{N}^d$.

Preuve Si on prend une telle suite, de $g_{v_t,v_{t+1}}^{(1)}$ non nul s'ensuit $v_t \leq q v_{t+1}$. Par récurrence, on obtient $v_t \leq q^{m-t} j$, et finalement pour chaque $t \in [\![0; m]\!]$, $v_t \leq q^m j$ (et notamment $i \leq q^m j$ pour qu'une telle suite existe). Notre ensemble est donc inclus dans l'ensemble des m-uplets d'éléments d'une partie bornée, donc finie, de $\mathbf{N}^d$, donc il est fini. □

Définition On pose donc à bon droit, pour $i, j \in \mathbf{N}^d$, $m \geq 1$,

$$g_{i,j}^{(m)} = \sum_{\substack{v_0, \ldots, v_m \in \mathbf{N}^d \\ v_0 = i \\ v_m = j}} g_{v_0, v_1}^{(1)} \cdots g_{v_{m-1}, v_m}^{(1)}$$

Proposition 4.4.134 *Pour $m \geq 1$, pour $i, j \in \mathbf{N}^d$, la somme étant finie,*

$$g_{i,j}^{(m+1)} = \sum_{w \in \mathbf{N}^d} g_{i,w}^{(m)} g_{w,j}^{(1)}.$$

Preuve La finitude de la somme découle du fait que $g_{w,j}^{(1)}$ est nul si qj n'est pas supérieur à w. Pour le reste, il suffit juste de regrouper les termes en fonction de la valeur du v_m dans la somme définissant $g_{i,j}^{(m+1)}$. □

Corollaire 4.4.135 *Si $F(X) = \sum_{w\in\mathbf{N}^d} a_w X^w$ est une série formelle, pour tout $m \geq 1$,*

$$\Psi^m(F(X)) = \sum_{w\in\mathbf{N}^d} \sum_{\substack{u\in\mathbf{N}^d \\ (u\leq qw)}} a_u g_{u,w}^{(m)} X^w$$

Corollaire 4.4.136 *Pour tout $i \in \mathbf{N}^d$,*

$$\Psi^m(X^i) = \sum_{j\in\mathbf{N}^d} g_{i,j}^{(m)} X^j$$

.

Remarque 4.4.31 On vient de prouver que, si on définit *a contrario* la quantité $g_{i,j}^{(m)}$ comme le coefficient de X^j dans la série formelle $\Psi^m(X^i)$, on a bien la formule du corollaire 135. [23]

Trace d'une itérée

On garde des notations similaires au paragraphe précédent.

Définition On pose à bon droit $\mathrm{tr}_R(\Psi^m) = \sum_{w\in\mathbf{N}^d} g_{w,w}^{(m)}$, pour tout $m \geq 1$.

Preuve On montre par récurrence sur $m \in \mathbf{N}^*$ que pour tous $i, j \in \mathbf{N}^l$ et tout $m \in \mathbf{N}^*$, $|g_{i,j}^{(m)}|_p \leq p^{-M(q|j|-|i|)}$. En effet, pour $m = 1$, il s'agit juste de la définition de $g_{i,j}^{(1)}$ et de la décroissance rapide de G ; soit $m \in \mathbf{N}^*$ satisfaisant l'hypothèse de récurrence ; soient $i, j \in \mathbf{N}^d$. On a :

$$\begin{aligned}
|g_{i,j}^{(m+1)}|_p &= \left| \sum_{\alpha,w\in\mathbf{N}^d} c_w \mathbb{1}(w+\alpha = qj) g_{i,\alpha}^{(m)} \right|_p \\
&\leq \sup_{w+\alpha=qj} |c_w|_p |g_{i,\alpha}^{(m)}|_p \\
&\leq \sup_{w+\alpha=qj} p^{-M(|w|+q|\alpha|-|i|)} \\
&\leq p^{-M(q|j|-|i|)}.
\end{aligned}$$

Donc, pour tout $m \in \mathbf{N}^*$, quand $|i|$ croît et tend vers l'infini, $|g_{i,i}^{(m)}|_p \leq p^{-M(q-1)|i|}$ tend vers zéro, donc la série de terme général $g_{i,i}^{(m)}$ converge dans $\mathbf{C}_p$. □

Remarque 4.4.32 Observer que la trace est bien seulement dépendante de Ψ en tant qu'opérateur : avec la notation, si $\Psi_{a,A}^{\alpha} = \Psi_{b,B}^{\beta}$, alors $\mathrm{tr}(\Psi_{a,A}^{\alpha}) = \mathrm{tr}(\Psi_{b,B}^{\beta})$.

Réexpression de la trace

Lemme 4.4.137 *Soient $G(X)$ une série formelle à décroissance rapide en d variables dans $\mathbf{C}_p$, $n, m \geq 1$. Soit $H_m(X) = G(X)G(X^n)\dots G(X^{n^{m-1}})$. H_m est bien à décroissance rapide d'après les lemmes 129 et 130), et on a :*

$$\Psi_{n,G(X)}^m = \Psi_{n^m,H_m(X)}.$$

23. ce qui n'est pas immédiat puisque Ψ linéaire ne permet d'accéder qu'aux sommes finies

Preuve On observe que si A, B sont des séries formelles en d variables dans $\mathbf{C}_p$,

$$A(X)T_k(B(X)) = T_k(A(X^k)B(X)),$$

pour $k \geq 2$. On montre alors le résultat par récurrence sur m.

Si $m = 1$, c'est bon. Soit donc $m \in \mathbf{N}^*$ tel que le résultat soit vrai. Alors, si $F(X)$ est une série formelle,

$$\begin{aligned}
\Psi^{m+1}_{n,G(X)}(F(X)) &= \Psi_{n,G(X)}\left(\Psi_{n^m,H_m(X)}(F(X))\right) \\
&= T_n\left(G(X)T_{n^m}(H_m(X)F(X))\right) \\
&= T_n \circ T_{n^m}\left(H_m(X)G(X^{n^m})F(X)\right) \\
&= T_{n^{m+1}}(H_{m+1}(X)F(X)) \\
&= \Psi_{n^{m+1},H_{m+1}(X)},
\end{aligned}$$

d'après le lemme 132. □

Lemme 4.4.138 *Soient $r \geq 1$, $q = p^r$, $G = \sum a_w X^w$ une série formelle à décroissance rapide en d variables. Alors, si $x = (x_1, \ldots, x_d) \in \mathbf{C}_p^d$ vérifie $|x_i|_p \leq 1$ pour tout x, la série définissant $G(x)$ converge. De plus, on a, tout étant bien défini,*

$$(q-1)^d \mathrm{tr}(\Psi_{q,G}) = \sum_{x \in \mu_{q-1}^d} G(x).$$

Preuve Si $x = (x_1, \ldots, x_d) \in \mathbf{C}_p$ avec $|x_i|_p \leq 1$, on a, si $G(X) = \sum a_w X^w$, on a, pour $w \in \mathbf{N}^d$ et un certain $M > 0$, $|a_w x^w|_p \leq p^{-M|w|} \longrightarrow 0$, d'où la convergence de la série. D'autre part, on a, si $x = (x_1, \ldots, x_d) \in \mu_{q-1}^d$, pour chaque i, $|x_i|_p = 1$, donc la série définissant $G(x)$ converge.

Enfin, on peut calculer :

$$\begin{aligned}
\sum_{x \in \mu_{q-1}^d} G(x) &= \sum_{\substack{w \in \mathbf{N}^d \\ w=(w_1,\ldots,w_d)}} \sum_{\substack{x \in \mu_{q-1}^d \\ x=(x_1,\ldots,x_d)}} a_w x_1^{w_1} \ldots x_d^{w_d} \\
&= \sum_{\substack{w \in \mathbf{N}^d \\ w=(w_1,\ldots,w_d)}} a_w \prod_{i=1}^{d} \sum_{x \in \mu_{q-1}} x^{w_i} \\
&= \sum_{\substack{w \in \mathbf{N}^d \\ w=(w_1,\ldots,w_d)}} a_w \prod_{i=1}^{d} (q-1)\mathbb{1}(q-1 \mid w) \\
&\quad \text{d'après le lemme 3,} \\
&= (q-1)^d \sum_{\substack{w \in \mathbf{N}^d \\ q-1 \mid w}} a_w \\
&= (q-1)^d \sum_{w \in \mathbf{N}^d} a_{qw-w}.
\end{aligned}$$

Or a_{qw-w} étant le coefficient de $\Psi(X^w)$ selon X^w, le membre droit vaut $(q-1)^d \mathrm{tr}(\Psi_{q,G})$, d'où le résultat. □

Lemme 4.4.139 *Soient $r \geq 1$, $q = p^r$, $n \geq 1$, G série formelle dans $\mathbf{C}_p$ à décroissance rapide en d variables. Alors, tout étant bien défini,*

$$(q^n-1)^d \mathrm{tr}(\Psi^n_{q,G}) = \sum_{x \in \mu_{q^n-1}^d} G(x)G(x^q)\ldots G(x^{q^{n-1}}).$$

Preuve D'après le lemme 138, le membre droit est $(q^n-1)^d \mathrm{tr}(\Psi_{q^n,G(X)G(X^q)\dots G(X^{q^{n-1}})})$. D'après le lemme 137, c'est donc exactement $(q^n-1)^d \mathrm{tr}(\Psi^n_{q,G})$. □

Formule des traces

On est maintenant en mesure d'énoncer et de prouver la formule des traces. On se donne un entier $r \geq 1$, $q = p^r$, un polynôme P en d variables sur $\mathbf{F}_q$, et un caractère χ associé de $\mathbf{F}_p$ dans $\mathbf{C}_p^*$. Notons τ un morphisme relevant de Teichmüller construit dans la sous-section précédente et $\Theta = \sum t_k X^k$ la série formelle de $\mathbf{C}_p[\![X]\!]$ associée, pour le caractère χ.

Théorème 4.4.20 *Il existe G série formelle à d variables de la forme*

$$G(X) = \sum_{w \in \mathbf{N}^d} c_w X^w$$

et $M > 0$ telles que $\forall\, w \in \mathbf{N}^d, \quad |c_w|_p \leq p^{-M|w|}$ et que l'opérateur Ψ associé vérifie pour tout $n \in \mathbf{N}^*$:

$$\sum_{x \in (\mathbf{F}_{q^n}^*)^d} \chi(\mathrm{tr}_{\mathbf{F}_{q^n}/\mathbf{F}_p}(P(x))) = (q^n-1)^d \mathrm{tr}_R(\Psi^n).$$

Preuve Notons $W \subset \mathbf{N}^d$ un certain ensemble fini, $a_w \in \mathbf{F}_q^*$ pour $w \in W$ tels que :

$$P(X) = \sum_{w \in W} a_w X^w.$$

Observons que les $\tau(a_w)$ sont dans μ_{q-1} donc sont de module 1.

Ainsi, si $w \in W$ n'est pas nul et $0 \leq s < r$,

$$\Theta(\tau(a_w)^{p^s} X^{p^s w}) = \sum_{u \in \mathbf{N}^d} \mathbb{1}(u \in p^s w \mathbf{N}^d) t_{u/p^s w} \tau(a_w)^{u/w} X^u$$

est une série formelle rapidement décroissante car $|t_{u/p^s w}|_p \leq p^{-i/((p-1)p^s w)}$ par construction de Θ. Si $w = 0$, c'est une constante de valeur absolue inférieur ou égale à 1, donc *a fortiori* une série formelle rapidement décroissante. Soit $G(X)$ le produit de ces séries (sur $w \in W$ et $0 \leq s < r$). Par le lemme 130, $G(X)$ est rapidement décroissante.

D'autre part, on a, pour tout $x \in (\mathbf{F}_{q^n}^*)^d$, comme les a_w sont dans $\mathbf{F}_q$,

$$\begin{aligned}
G(\tau(x))G(\tau(x)^q)\dots G(\tau(x)^{q^{n-1}}) &= \prod_{w \in W} \prod_{i=0}^{n-1} \prod_{s=0}^{r-1} \Theta(\tau(a_w)^{p^s} \tau(x^{q^i})^{p^s w}) \\
&= \prod_{w \in W} \prod_{i=0}^{n-1} \prod_{s=0}^{r-1} \Theta(\tau(a_w^{q^i})^{p^s} \tau(x)^{p^{ri+s} w}) \\
&= \prod_{w \in W} \prod_{i=0}^{n-1} \prod_{s=0}^{r-1} \Theta((\tau(a_w)\tau(x)^w)^{p^{ri+s}}) \\
&= \prod_{w \in W} \prod_{i=0}^{nr-1} \Theta(\tau(a_w x^w)^{p^i}) \\
&= \prod_{w \in W} \chi(\mathrm{tr}_{\mathbf{F}_{q^n}/\mathbf{F}_p}(a_w x^w)) \\
&= \chi \circ \mathrm{tr}_{\mathbf{F}_{q^n}/\mathbf{F}_p} \left(\sum_{w \in W} a_w x^w \right) \\
&= \chi \circ \mathrm{tr}_{\mathbf{F}_{q^n}/\mathbf{F}_p}(P(x)),
\end{aligned}$$

et on conclut en sommant sur les $x \in (\mathbf{F}_{q^n}^*)^d$, en notant que τ induit un isomorphisme de $(\mathbf{F}_{q^n}^*)^d$ sur $\mu_{q^n-1}^d$, et en utilisant le lemme 139. □

4.5 Décomposition de la fonction zêta

On procède en deux temps. Tout d'abord, on montre à l'aide de la formule des traces (théorème 20) que, pour tout caractère non trivial χ de $\mathbf{F}_p$ dans $\mathbf{C}_p^*$, pour tout entier d et pour tout polynôme Q, on peut « décomposer » la suite

$$\left(\sum_{x \in (\mathbf{F}_{q^n}^*)^d} \chi \circ \mathrm{tr}_{\mathbf{F}_{q^n}/\mathbf{F}_p}(Q(x)) \right)_{n \in \mathbf{N}^*}$$

au sens de la proposition 140 *infra*. On en déduit ensuite par des réductions plus élémentaires l'existence d'une décomposition de ζ au sens de la proposition 115.

Proposition 4.5.140 *Soit $d \in \mathbf{N}^*$, $Q \in \mathbf{F}_{q^n}[X_1, \ldots, X_l]$, χ un caractère non trivial de $\mathbf{F}_p$ dans $\mathbf{C}_p^*$. Alors il existe I fini, $\lambda_i \in \mathbf{Z}$, $(S_n^i) \in \mathbf{C}_p^{\mathbf{N}}$ tels que pour tout $i \in I$, $\exp\left(\sum_{n\geq 1} \frac{S_n^i}{n} X^n\right)$ entière, et :*

$$\forall\, n \in \mathbf{N}, \quad \sum_{x \in (\mathbf{F}_{q^n}^*)^d} \chi(\mathrm{tr}_{\mathbf{F}_{q^n}/\mathbf{F}_p}(Q(x))) = \sum_{i \in I} \lambda_i S_n^i.$$

Fixons nous $d \in \mathbf{N}^*$, $Q \in \mathbf{F}_{q^n}[X_1, \ldots, X_l]$, χ un caractère non trivial de $\mathbf{F}_p$ dans $\mathbf{C}_p^*$. Soit G une série formelle à décroissance rapide et Ψ l'opérateur associé à G pour l'entier q, donnés par la formule des traces pour le polynôme Q et le caractère χ.

Montrons tout d'abord la :

Proposition 4.5.141 *La fonction* $\exp\left(-\sum_{n=1}^{\infty} \frac{\mathrm{tr}_R(\Psi^n) X^n}{n}\right)$ *est entière.*

Pour ce faire, on se donne tout d'abord les outils pour énoncer rigoureusement la proposition suivante, et on la démontre :

Proposition 4.5.142 *On a*

$$\exp\left(-\sum_{n\geq 1} \frac{\mathrm{tr}(\Psi^n)}{n} X^n\right) = \sum_{n \geq 0} b_n(\Psi) X^n,$$

où, pour $n \geq 0$,

$$b_n(\Psi) = (-1)^n \sum_{\substack{I \subset \mathbf{N}^d \\ |I| = n \\ s \in \mathfrak{S}(I)}} \varepsilon_I(s) \prod_{i \in I} g_{i,s(i)}^{(1)},$$

la série étant convergente.

Signature d'une permutation abstraite

On se propose ici de justifier l'existence d'une signature abstraite d'une permutation d'un ensemble, indépendamment de la façon dont on énumère ses éléments, afin de donner un sens à la fonction ε_I de la proposition précédente.

Proposition 4.5.143 *Pour chaque ensemble fini E, il existe un morphisme canonique surjectif ε_E de l'ensemble de bijections de E dans E, noté $\mathfrak{S}(E)$, dans $\{\pm 1\}$ tel que :*

- *$\varepsilon_{[\![1,n]\!]}$ est la signature usuelle sur $\mathfrak{S}_n$.*
- *Si $f : E \to F$ est une bijection et si $s \in \mathfrak{S}(E)$, alors $\varepsilon_F(s) = \varepsilon_E(f^{-1} \circ s \circ f)$.*

- *Si E est un ensemble fini, F une partie non vide de E, $f \in \mathfrak{S}(E)$ telle que $f|_{E\setminus F} = id_{E\setminus F}$ (donc en particulier $f(F) = F$), alors $\varepsilon_E(f) = \varepsilon_F(f|_F)$.*

Preuve Soient $f, g : [\![1; |E|]\!] \to E$ deux bijections, on a pour tout $s \in \mathfrak{S}(E)$, $f^{-1}g \in \mathfrak{S}_{|E|}$ et

$$f^{-1}sf = f^{-1}g(g^{-1}sg)(f^{-1}g)^{-1},$$

de sorte que la quantité $\varepsilon(f^{-1}sf)$ ne dépend pas du choix de $f : [\![1; |E|]\!]$ bijective. On note ladite quantité $\varepsilon_E(s)$.

Remarquons que si f est comme ci-dessus, $s \longmapsto f^{-1}sf$ est un isomorphisme de $\mathfrak{S}(E)$ sur $\mathfrak{S}_{|E|}$, ε_E est bien un morphisme surjectif de $\mathfrak{S}(E)$ sur $\{\pm 1\}$.

De cette définition découlent aisément les autres propriétés. □

Cas d'un endomorphisme en dimension finie

Pour montrer la proposition 141, on en établit tout d'abord un analogue en dimension finie.

Proposition 4.5.144 *Soient K un corps de caractéristique nulle, $A \in \mathscr{M}_n(K)$. La matrice $I_n - AX$ est à coefficients dans l'anneau $K[X]$, donc on peut calculer son déterminant, qui est dans $K[X]$. On a*

$$\det(I_n - AX) = \sum_{k=0}^{n} b_k(A)X^k,$$

où pour $0 \leq m \leq n$,

$$b_m(A) = (-1)^m \sum_{\substack{I \subset [\![1,n]\!] \\ |I|=m \\ s \in \mathfrak{S}(I)}} \varepsilon_I(s) \prod_{i \in I} A_{i,s(i)}.$$

Preuve On a par définition :

$$\det(I_n - AX) = \sum_{s \in \mathfrak{S}_n} \varepsilon(s) \prod_{i=1}^{n} (\delta_{i,s(i)} - A_{i,s(i)}X)$$

donc $\det(I_n - AX)$ est combinaison linéaire de polynômes de degré au plus n, donc est un polynôme de degré au plus n.

Soit $s \in \mathfrak{S}_n$, déterminons le coefficient $b_m(A)$ devant X^m dans $\prod_{i=1}^{n} (\delta_{i,s(i)} - A_{i,s(i)}X)$. Notons que si s a strictement moins de $n - m$ points fixes, ce produit contient strictement plus de m monômes de degré 1 donc son coefficient de degré m est nul. Si s a $n - m$ points fixes, notons S son support (de cardinal au plus m). Alors le coefficient devant X^m du produit s'écrit comme $c \cdot (-1)^{|S|} \prod_{i \in S} A_{i,s(i)}$, où c est le coefficient devant $X^{m-|S|}$ de $\prod_{i \notin S} (1 - A_{i,s(i)}X)$. Par conséquent,

$$c = (-1)^{m-|S|} \sum_{\substack{Y \subset [\![1;n]\!] \\ Y \cap S = \varnothing \\ |Y|+|S|=m}} \prod_{y \in Y} A_{y,s(y)},$$

d'où il s'ensuit que

$$\begin{aligned} b_m(A) &= (-1)^m \sum_{\substack{s\in\mathfrak{S}_n \\ Y\subset[\![1;n]\!] \\ |Y|=m \\ |Y|\supset \mathrm{Supp}(s)}} \varepsilon(s) \prod_{y\in Y} A_{s,s(y)} \\ &= \sum_{\substack{Y\subset[\![1;n]\!] \\ |Y|=m}} \sum_{\substack{s\in\mathfrak{S}_n \\ \mathrm{Supp}(s)\subset Y}} \varepsilon_Y(s_{|Y}) \prod_{y\in Y} A_{y,s(y)} \\ &= \sum_{\substack{Y\subset[\![1;n]\!] \\ |Y|=m \\ s\in\mathfrak{S}(Y)}} \varepsilon_Y(s) \prod_{y\in Y} [A]_{y,s(y)}. \end{aligned}$$

□

D'autre part, on montre aussi les résultats suivants :

Lemme 4.5.145 *On a l'identité formelle :*

$$1 - X = \exp\left(-\sum_{n=1}^{\infty} \frac{X^n}{n}\right).$$

Lemme 4.5.146 *Pour $A \in \mathscr{M}_n(\mathbf{C})$, $\exp(\mathrm{tr}(A)) = \det(\exp(A))$.*

Preuve C'est vrai pour les matrices triangulaires, le problème est invariant par similitude, et A est trigonalisable. □

À partir de là, intuitivement, il suffit de spécialiser l'identité formelle en AX dans $\mathscr{M}_n(\mathbf{C}_p[X])$ et de prendre le déterminant pour conclure que :

$$\exp\left(-\sum_{n=1}^{\infty} \frac{\mathrm{tr}(A^n)X^n}{n}\right) = \sum_{m=0}^{n} b_m(A)X^m,$$

pour les coefficients $b_m(A)$ définis dans la proposition 144.

Reste à justifier cette spécialisation et cette identification hâtives. Pour faire cela proprement, on ajoute tout d'abord quelques notations, en explicitant les coefficients du terme de gauche.

Définition Pour $n \geq 1$, on pose

$$E_n(X_1, \ldots, X_n) = \sum_{\substack{1\leq k\leq n \\ p_1,\ldots,p_k\in\mathbf{N}^* \\ p_1+\ldots+p_k=n}} \frac{1}{k!} \prod_{i=1}^{k} X_{p_i}.$$

On pose $E_0 = 1$.

Proposition 4.5.147 *E_n est un polynôme rationnel en n variables à coefficients positifs, et on a, sur tout corps K de caractéristique nulle et toute suite $(a_n)_{n\geq 1} \in K^{\mathbf{N}^*}$, l'identité formelle :*

$$\exp\left(\sum_{n\geq 1} a_n X^n\right) = \sum_{n\geq 0} E_n(a_1, \ldots, a_n)X^n$$

Preuve Développer formellement. □

Ainsi, avec cette « identification » on veut juste montrer que

$$\forall\, n \in \mathbf{N},\ \forall\, A \in \mathscr{M}_n(\mathbf{C}_p), \quad E_n\left(-\mathrm{tr}(A), \ldots, -\frac{\mathrm{tr}(A^n)}{n}\right) = b_n(A),$$

avec $b_n(A)$ défini précédemment. Comme les termes de gauche et de droite sont polynomiaux en les coefficients de A, il suffit de montrer qu'ils coïncident pour tout choix de coefficients dans $\mathbf{Q}$. Pour des raisons de confort, on va le montrer pour tout choix de coefficients dans $\mathbf{C}$.

Théorème 4.5.21 *Soient $M > 0$, $u \in \mathscr{M}_n(\mathbf{C})$ tel que $\|u\| < \frac{1}{2M}$, $(a_n) \in \mathbf{C}^{\mathbf{N}}$ avec $|a_n| \leq M^n$. Alors la série*

$$\sum_{n\geq 1} E_n(a_1, \ldots, a_n)\, u^n$$

converge dans $\mathscr{M}_n(\mathbf{C})$, et sa somme est $\exp\left(\sum_{n\geq 1} a_n u^n\right)$, qui est bien définie.

Pour montrer cela, on admet provisoirement la proposition 150 de combinatoire établie dans l'antépénultième paragraphe de cette section.

Preuve Le dernier point étant clair, on observe que, comme E_n est à coefficients positifs, si $r = M||u|| < 1/2$,

$$\begin{aligned}\sum_{n\geq 1} \sum_{\substack{k\geq 1 \\ p_1,\ldots,p_k\in\mathbf{N}^* \\ p_1+\ldots+p_k=n}} \frac{1}{k!}|a_{p_1}|\ldots|a_{p_k}|\cdot||u^n|| &\leq \sum_{n\geq 1}\sum_{k\geq 1}\frac{1}{k!}\binom{n-1}{k-1} r^n \\ &\leq r\sum_{n\geq 1}\sum_{k\geq 1}\binom{n-1}{k-1} r^{n-1} \\ &\leq r\sum_{n\geq 1}(2r)^{n-1} < +\infty\end{aligned}$$

Ainsi, la famille

$$\left(\frac{1}{k!}\prod_{i=1}^{k} a_{p_i} u^n\right)_{\substack{n,k\geq 1 \\ p_1,\ldots,p_k\geq 1 \\ p_1+\ldots+p_k=n}}$$

est sommable, notons S sa somme. En sommant d'abord sur les p_i et sur k, puis sur n, on obtient que $S+1 = \sum_{n\geq 0} E_n(a_1,\ldots,a_n)u^n$, le membre droit étant absolument convergent.

D'autre part, en sommant d'abord sur n, puis sur les p_i, puis sur k,

$$\begin{aligned}S+1 &= 1+\sum_{k\geq 1}\frac{1}{k!}\sum_{p_1,\ldots,p_k\in\mathbf{N}^*}\prod_{i=1}^{k} a_{p_i}X^{p_i} \\ &= 1+\sum_{k\geq 1}\frac{1}{k!}\left(\sum_{p\geq 1} a_p u^p\right)^k \\ &= \exp\left(\sum_{n\geq 1} a_n u^n\right),\end{aligned}$$

ce qui conclut. □

Corollaire 4.5.148 *Soit $n \geq 2$. On a $E_n\left(-1, -\frac{1}{2}, \ldots, -\frac{1}{n}\right) = 0$. On a aussi $E_1(X_1) = X_1$.*

Preuve Le deuxième point est clair.

D'autre part, par la proposition, la série entière réelle $\sum_{n\geq 0} E_n\left(-1\ldots, -\frac{1}{n}\right)x^n$ a un rayon de convergence d'au moins $1/2$, et, si on note $S(x)$ sa somme pour $x \in]-1/2, 1/2[$,

on a, quand $|2x| < 1$,

$$S(x) = \exp\left(-\sum_{n\geq 1}\frac{x^n}{n}\right) = \exp((\ln(1-x)) = 1-x,$$

et on conclut par unicité du développement en série entière. □

Corollaire 4.5.149 *Soit $A \in \mathscr{M}_n(\mathbf{C})$, $z \in \mathbf{C}$ tels que $|z| < \frac{1}{2C||A||}$, où $C \geq 1$ majore la norme d'opérateur de* tr. *Alors*

$$\det(I_n - Az) = \exp\left(-\sum_{n\geq 1}\frac{\mathrm{tr}(A^n)z^n}{n}\right) = \sum_{m\geq 0} E_m\left(-\mathrm{tr}(A), \ldots, -\frac{\mathrm{tr}(A^m)}{m}\right) z^m.$$

Donc, par identification, $b_m(A) = E_m\left(-\mathrm{tr}(A), \ldots, -\frac{\mathrm{tr}(A^m)}{m}\right)$ pour tout $m \in [\![0, n]\!]$.

Preuve C'est une conséquence du théorème 21, du corollaire 148 et du lemme 146. □

Remarque 4.5.33 Le cas des matrices étudié ci-dessus nous a montré pourquoi la proposition 144, bien qu'elle ne légifère que sur les cas de dimension finie, était pertinente ; pour la montrer effectivement, il ne reste qu'à vérifier quelques questions de convergence de séries. Quant à la proposition 141, elle revient aussi à une question d'estimation asymptotique : il s'agit de montrer que $|b_n(\Psi)|_p^{1/n} \to 0$ quand $n \to \infty$. Finalement, on veut juste estimer les $b_n(\Psi)$, qui sont de nature des objets combinatoires. C'est ainsi que nous appelons de nos vœux le paragraphe suivant :

Un peu de combinatoire

Voici tout d'abord la proposition utilisée dans la preuve du théorème 21.

Proposition 4.5.150 *Soient $k, n \in \mathbf{N}^*$. Le nombre de solutions entières strictement positives à l'équation $a_1 + \ldots + a_k = n$ est $\binom{n-1}{k-1}$.*

Preuve Notons S l'ensemble des k-uplets d'entiers strictement positifs des solutions de l'équation. Notons I l'ensemble des suites à $k-1$ éléments strictement croissantes, chaque élément appartenant à $[\![1, n-1]\!]$. Clairement, I est en bijection avec l'ensemble des parties à $k-1$ éléments de $[\![1, n-1]\!]$, de sorte que $|I| = \binom{n-1}{k-1}$. D'autre part,

$$(a_i) \in S \longmapsto \left(\sum_{t=1}^{i} a_t\right)_{1\leq i\leq k-1}$$

est clairement une bijection de S dans I, d'où le résultat. □

De façon analogue, on a :

Proposition 4.5.151 *Soient $k, n \in \mathbf{N}^*$. Le nombre de solutions entières positives à l'équation $a_1 + \ldots + a_k = n$ est $\binom{n+k-1}{k-1}$.*

Preuve Notons S l'ensemble des k-uplets d'entiers naturels solutions de l'équation, T l'ensemble des k-uplets d'entiers strictement positifs solutions de l'équation $b_1 + \ldots + b_k = n+k$. On sait que $|T| = \binom{n+k-1}{k-1}$. Or,

$$(a_i) \in S \longmapsto (a_i + 1)_{1\leq i\leq k}$$

est une bijection entre S et T, ce qui conclut. □

Corollaire 4.5.152 *Dans $\mathbf{N}^d$, il existe exactement $\binom{n+d-1}{d-1}$ éléments x de poids n.*

Définition Soit $d \geq 1$. Pour une partie finie $I \subset \mathbf{N}^d$, on définit son *poids total* par la formule : $w(I) = \sum_{i\in I} |i|$. Notons de plus $w_n = \inf_{\substack{X\subset\mathbf{N}^d \\ |X|=n}} w(X)$.

Lemme 4.5.153 *Si* $n = \binom{t+d}{d}$, *alors* $w_n = d\binom{d+t}{d+1}$

Preuve On observe que

$$n = \sum_{k=0}^{t} \binom{k+d}{d} - \binom{k+d-1}{d} = \sum_{k=0}^{t} \binom{k+d-1}{d-1} = |\{x \in \mathbf{N}^d,\ |x| \leq t\}|,$$

donc l'ensemble de cardinal n et de poids total minimal dans $\mathbf{N}^d$ est $\{x \in \mathbf{N}^d,\ |x| \leq t\}$, d'où

$$\begin{aligned} w_n &= \sum_{k=0}^{t} k|\{x \in \mathbf{N}^d,\ |x| = k\}| \\ &= \sum_{k=1}^{t} k\frac{(k+d-1)!}{k!(d-1)!} \\ &= d\sum_{k=1}^{t} \frac{(k+d-1)!}{(k-1)!d!} \\ &= d\sum_{k=1}^{t} \binom{k+d}{d+1} - \binom{k+d-1}{d+1} \\ &= d\binom{t+d}{d+1}. \end{aligned}$$

□

Remarque 4.5.34 (w_n) est croissante.

Proposition 4.5.154 *Pour* n *assez grand,* $w_n \geq \frac{d}{4d+4}\, n^{1+1/d}$.

Preuve Pour $n \geq 1$, on dispose de t tel que $\binom{t+d}{d} \leq n \leq \binom{t+d+1}{d} \leq (t+d+1)^d$. De la sorte, on a $d\binom{d+t}{d+1} \leq w_n \leq d\binom{d+t+1}{d+1}$. Supposons donc que $n \geq (2d+2)^d$, alors $t \geq d+1$ et $t \geq \frac{1}{2}(t+d+1)$. Alors

$$\begin{aligned} \frac{w_n}{n} &\geq d\binom{d+t}{d+1}\binom{d+t+1}{d}^{-1} \\ &\geq \frac{dt(t+1)}{(t+d+1)(d+1)} \geq \frac{d}{4(d+1)}(t+d+1) \\ &\geq \frac{d}{4d+4} n^{1/d}. \end{aligned}$$

□

Preuve des propositions 141 et 142

Nous avons maintenant tous les outils nécessaires pour cette preuve.

Preuve Observons que si $X \subset \mathbf{N}^d$ est de cardinal $n \geq 0$, si $s \in \mathfrak{S}(X)$,

$$|\varepsilon_X(s) \prod_{x \in X} g_{x,s(x)}| \leq \prod_{x \in X} p^{-M(q|x|-|s(x)|)} = p^{-M(q-1)w(X)}$$

de sorte que si X contient au moins un élément de $\mathbf{N}^d$ de poids supérieur à $R > 0$ (ce qui arrive pour toutes les parties de cardinal n de $\mathbf{N}^d$ sauf un nombre fini d'entre elles),

$$\left|\varepsilon_X(s) \prod_{x \in X} g^{(1)}_{x,s(x)}\right| \leq p^{-MR(q-1)},$$

et $p^{-MR(q-1)} \underset{R\longrightarrow+\infty}{\longrightarrow} 0$. Ainsi la somme est convergente, donc la famille est sommable au sens p-adique.

Il s'agit de prouver que $b_n(\Psi) = E_n\left(\left(-\frac{\mathrm{tr}(\Psi^k)}{k}\right)_{1\leq k\leq n}\right)$ ie, si une bijection $\phi : \mathbf{N} \to \mathbf{N}^d$ est fixée, que

$$E_n\left(\left(-\frac{1}{k}\sum_{v_1,\dots v_k\in\mathbf{N}} g^{(1)}_{\phi(v_1),\phi(v_2)}\cdots g^{(1)}_{\phi(v_k),\phi(v_1)}\right)_{1\leq k\leq n}\right) = b_n(\Psi),$$

la sommabilité des familles correspondantes se montrant comme le théorème 21 pour le membre de gauche, celle du membre de droite venant juste d'être vue.

L'identité est vraie pour $n = 0$: on suppose donc $n \geq 1$.
Le membre gauche est la limite quand $N \to +\infty$ de

$$u_N = E_n\left(\left(-\frac{1}{k}\sum_{0\leq v_1,\dots v_k\leq\mathbf{N}} g^{(1)}_{\phi(v_1),\phi(v_2)}\cdots g^{(1)}_{\phi(v_k),\phi(v_1)}\right)_{1\leq k\leq n}\right).$$

Or, on a vu précédemment que pour $N \geq n$,

$$u_N = (-1)^n \sum_{\substack{X\subset[\![0;N]\!]\\|X|=n\\s\in\mathfrak{S}(X)}} \varepsilon_X \prod_{x\in X} g_{\phi(x),\phi(s(x))}{}^{(1)} = (-1)^n \sum_{\substack{X\subset\phi([\![0;N]\!])\\|X|=n\\s\in\mathfrak{S}(X)}} \varepsilon_X(s) \prod_{x\in X} g^{(1)}_{x,s(x)}.$$

En faisant tendre N vers l'infini, en utilisant la sommabilité de la famille dont la somme définit b_n (et en disant que toute partie de $\mathbf{N}^d$ de cardinal n est incluse dans un $\phi([\![0,N]\!])$ pour N assez grand), on conclut.

Reste à prouver que $|b_n|^{1/n} \to 0$. Puisque $\mathbf{C}_p$ est ultramétrique, il suffit d'établir que

$$\left(\sup_{\substack{X\subset\mathbf{N}^d\\|X|=n\\s\in\mathfrak{S}(X)}}\left(\prod_{x\in X}|g^{(1)}_{x,s(x)}|\right)\right)^{1/n} \underset{n\to+\infty}{\to} 0.$$

Soient $n \geq 1$, $X \subset \mathbf{N}^d$ de cardinal n, $s \in \mathfrak{S}(X)$. On a déjà vu que

$$\left(\prod_{x\in X}|g^{(1)}_{x,s(x)}|\right)^{1/n} \leq p^{-M(q-1)w(X)/n} \leq p^{-M(q-1)w_n/n} \underset{n\to\infty}{\longrightarrow} 0,$$

avec les notations du paragraphe de combinatoire, ce qui conclut. □

Décomposition de la fonction zêta

On se fixe une fois pour toutes un corps $\mathbf{F}_q$ de caractéristique p.

Remarque 4.5.35 Attention, dans ce paragraphe, on s'autorise à faire varier le polynôme qu'on considère afin de montrer l'existence d'une décomposition de la fonction zêta de tout polynôme, et même à choisir à notre convenance l'espace des polynômes considérés (nombre de variables).

Introduisons pour le confort cette définition (non standard).

Définition Une suite $(a_n)_{n\geq1}$ d'éléments de $\mathbf{C}_p$ est *quasi-finie* si l'égalité formelle

$$\exp\left(\sum_{n\geq0}\frac{a_n}{n}X^n\right) = \sum_{n\geq0} b_n X^n$$

définit une fonction entière au sens de $\mathbf{C}_p$, ie si $|b_n|_p^{1/n}$ tend vers 0 quand $n \to \infty$.

Lemme 4.5.155 *Soient $(a_n)_{n\geq 1}$ quasi-finie, $t \in \mathbf{C}_p$. Alors $(a_n t^n)$ est quasi-finie.*

Preuve On a

$$\begin{aligned}\exp\left(\sum_{n\geq 1}\frac{a_n t^n}{n}X^n\right) &= \exp\left(\sum_{n\geq 1}\frac{a_n}{n}(tX)^n\right)\\ &= \sum_{n\geq 0} b_n (tX)^n\\ &= \sum_{n\geq 0} b_n t^n X^n,\end{aligned}$$

où (b_n) est associée à (a_n) comme dans la définition.
Alors $(|b_n t^n|^{1/n}) = (|t|\cdot|b_n|^{1/n})$ est de limite nulle. □

Corollaire 4.5.156 *Si (a_n) est quasi-finie, $d \geq 1$, $t \in \mathbf{C}_p$, alors $((t^n-1)^d a_n)_n$ est combinaison linaire finie à coefficients entiers de suites quasi-finies.*

Preuve Pour $n \in \mathbf{N}^*$,

$$(t^n-1)^d a_n = \sum_{k=0}^{d}\binom{d}{k}(-1)^{d-k}(t^k)^n a_n,$$

ce qui conclut. □

Proposition 4.5.157 *Soient Q un polynôme à d variables sur $\mathbf{F}_q$, χ un caractère non trivial de $\mathbf{F}_p$ dans $\mathbf{C}_p^*$. La suite*

$$n \longmapsto \sum_{x\in(\mathbf{F}_{q^n}^*)^d} \chi\circ \mathrm{tr}_{\mathbf{F}_{q^n}/\mathbf{F}_p}(Q(x))$$

se décompose comme combinaison linéaire finie à coefficients entiers de suites dans $\mathbf{C}_p$ quasi-finies.

Preuve Cela résulte du corollaire 156, de la formule des traces et de la proposition 141. □

Proposition 4.5.158 *Soient Q un polynôme à $d \geq 1$ variables sur $\mathbf{F}_q$, χ un caractère non trivial de $\mathbf{F}_p$ dans $\mathbf{C}_p^*$. La suite*

$$u : n \longmapsto \sum_{x\in\mathbf{F}_{q^n}^d} \chi\circ \mathrm{tr}_{\mathbf{F}_{q^n}/\mathbf{F}_p}(Q(x))$$

est combinaison linéaire finie à coefficients entiers de suites quasi-finies.

Preuve On observe que cette suite s'écrit

$$u_n = \sum_{I\subset[\![1,d]\!]}\sum_{x\in(\mathbf{F}_{q^n}^*)^{|I|}} \chi\circ \mathrm{tr}_{\mathbf{F}_{q^n}/\mathbf{F}_p}(Q_I(x)),$$

où, pour une partie I de $[\![1,d]\!]$ de cardinal k, Q_I est le polynôme en $|I|$ variables à coefficients dans $\mathbf{F}_q$ défini en substituant, dans l'écriture de Q, 0 à chaque X_i pour $i \notin I$, et en renumérotant de 1 à k les X_i, $i \in I$, par ordre croissant d'indice i. □

Lemme 4.5.159 *Soient χ un caractère non trivial de $\mathbf{F}_p$ dans $\mathbf{C}_p^*$, $d \geq 1$, $x \in \mathbf{F}_{q^n}^d$. Alors*

$$\sum_{y\in\mathbf{F}_{q^n}^d} \chi\circ \mathrm{tr}_{\mathbf{F}_{q^n}/\mathbf{F}_p}(xy) = q^{dn}\delta_{x,0}.$$

Preuve On peut, la trace étant additive, séparer les contributions des différentes coordonnées en factorisant. Il suffit donc de traiter le cas $d = 1$. Le membre de gauche est la somme sur $\mathbf{F}_{q^n}$ des valeurs images par un certain morphisme de $\mathbf{F}_{q^n}$ dans $\mathbf{C}_p^*$. D'après la proposition 24, c'est donc q^n si le morphisme est trivial (si et seulement si $x = 0$, par surjectivité de la trace), 0 sinon. □

Nous pouvons enfin démontrer la proposition 115 qui restait la seule pièce manquante de la preuve.

Théorème 4.5.22 *On se donne $P_1, \dots, P_m$ des polynômes à coefficients dans $\mathbf{F}_q$ en d variables. Pour $n \in \mathbf{N}^*$, on note $N_n = |\{x \in \mathbf{F}_{q^n}^d \mid \forall\, i \in [\![1, m]\!],\ P_i(x) = 0\}|$. Alors (N_n) est combinaison linéaire finie à coefficients entiers de suites d'éléments de $\mathbf{C}_p$ quasi-finies.*

Preuve Soit χ un caractère non trivial de $\mathbf{F}_p$ dans $\mathbf{C}_p^*$. Par le lemme 159,

$$\begin{aligned} N_n &= \frac{1}{q^{mn}} \sum_{x \in \mathbf{F}_{q^n}^d} q^{mn} \mathbb{1}(\forall\, i \in [\![1, m]\!],\ P_i(x) = 0) \\ &= \frac{1}{q^{mn}} \sum_{x \in \mathbf{F}_{q^n}^d} \sum_{y \in \mathbf{F}_{q^n}^m} \chi \circ \mathrm{tr}_{\mathbf{F}_{q^n}/\mathbf{F}_p} \left(\sum_{i=1}^m y_i P_i(x) \right) \\ &= \frac{1}{q^{mn}} \sum_{z \in \mathbf{F}_{q^n}^{d+m}} \chi \circ \mathrm{tr}_{\mathbf{F}_{q^n}/\mathbf{F}_p}(\Pi(z)) \end{aligned}$$

où $\Pi(X_1, \dots, X_d, Y_1, \dots, Y_m) = \sum_{i=1}^m Y_i P_i(X_1, \dots, X_d)$ est à coefficients dans $\mathbf{F}_q$ et en $d+m$ variables, ce qui conclut d'après la proposition 158 et le lemme 155. □

Références

[Ami75] Yvette Amice : *Les nombres p-adiques*, chapitre 1. Presses universitaires de France, 1975.

[Dwo60] Bernard Dwork : On the rationality of the zeta function of an algebraic variety. *American Journal of Mathematics*, 82:631–648, 1960.

[GFN01] Hervé Gianella, Serge Francinou et Serge Nicolas : *Oraux X-ENS : Algèbre 1*, chapitre 5.12. Cassini, 2001.

[IR90] Kenneth Ireland et Michael Rosen : *A classical Introduction to Modern Number Theory*, volume 84. Springer-Verlag, 1990.

[Ked02] Kiran Kedlaya : Fourier transforms and p-adic "Weil II". *ArXiv Mathematics e-prints*, 2002.

[Tao] Terence Tao : Dwork's proof of rationality of the zeta function over finite fields. *Page éditée le 13 mai 2014, consultée le 26 avril 2017 :* https://terrytao.wordpress.com/2014/05/13/dworks-proof-of-rationality-of-the-zeta-function-over-finite-fields/.

[Tau08] Patrice Tauvel : *Corps commutatifs et théorie de Galois*. Calvage et Mounet, 2008.

[Wei49] André Weil : Number of solutions of equations in finite fields. *Bulletin of the American Mathematical Society*, 55:497–508, 1949.