DÉMONSTRATION DE LA CONJECTURE DE CATALAN

par

Henri Cohen

Table des matières

1. Introduction aux corps de nombres

1.1. Propriétés en tant que corps. — Il n'est pas exagéré de dire que la théorie des corps de nombres a été inventée (dans un langage un peu différent) par Kummer, Dedekind, Dirichlet, et bien d'autres, dans le seul but de résoudre le « grand » théorème de Fermat, du moins dans les cas où ceci est possible avec ces méthodes. Rappelons de quoi il s'agit. Fermat a affirmé qu'il n'existe pas d'entiers non nuls x, y et z tels que $x^n + y^n = z^n$ pour $n \geqslant 3$. Il a lui-même démontré (par une

méthode dite de descente infinie) que cette équation est effectivement impossible pour $n = 4$. Il en résulte qu'il suffit de démontrer son impossibilité pour $n = p$ premier impair, et par homogénéité on peut également supposer que x, y et z sont premiers entre eux deux à deux.

L'idée fondamentale de la démonstration, peut-être imaginée par Fermat, mais en tous cas explicitée par Kummer, est de *factoriser* l'équation. On peut le faire partiellement sur $\mathbb{Z}$ en mettant $x + y$ en facteur, mais ce n'est pas suffisant. Il est donc nécessaire d'agrandir le corps sur lequel on travaille : cela conduit à la notion *d'adjonction*. Soit ζ une racine primitive p-ième de l'unité et $K = \mathbb{Q}(\zeta)$ le corps obtenu par adjonction de ζ à $\mathbb{Q}$, c'est-à-dire l'ensemble des fractions rationnelles en ζ à coefficients dans $\mathbb{Q}$. On peut maintenant complètement factoriser l'équation de Fermat comme suit :

$$(x + y)(x + \zeta y) \cdots (x + \zeta^{p-1} y) = z^p.$$

L'idée est alors la suivante : si les facteurs du membre de gauche sont « premiers entre eux » deux à deux en un sens convenable, alors ils doivent tous être des puissances p-ièmes, et on peut espérer en déduire une contradiction.

Cette idée fondamentale est correcte à la base, mais se heurte à plusieurs obstacles. Tout d'abord la notion de « premiers entre eux » n'a de sens que dans un anneau principal, ce qui n'est pas nécessairement le cas. Ceci va donc conduire les auteurs ci-dessus à introduire la notion *d'idéal*, pour essayer de s'affranchir de cette restriction. Ensuite, même si cette étape peut être franchie, il n'est pas tout à fait exact de dire que les facteurs doivent être des puissances p-ièmes : ce sera des puissances p-ièmes multiplié par des éléments *inversibles* (qui dans $\mathbb{Z}$ ne sont autres que ± 1), et il va donc falloir aussi s'occuper de cet aspect. Enfin, il se peut que les facteurs ne soient pas premiers entre eux, mais dans ce cas il faut faire appel à des techniques spécifiques au théorème de Fermat, et donc que nous ne considérerons pas ici.

Tout ceci conduit donc aux définitions suivantes, volontairement biaisées vers les équations diophantiennes.

Définition 1.1. — Soit $T(X)$ un polynôme irréductible de degré n à coefficients rationnels, et soit $\theta \in \mathbb{C}$ une racine complexe de T. On note $K = \mathbb{Q}(\theta)$ l'ensemble des *fractions rationnelles* en θ à coefficients dans $\mathbb{Q}$, et on l'appelle corps obtenu par *adjonction* de θ à $\mathbb{Q}$.

Il est évident que K est un corps. De plus, si $P(\theta)/Q(\theta)$ est une fraction rationnelle en θ avec $Q(\theta) \neq 0$, les polynômes $T(X)$ et $Q(X)$ sont premiers entre eux, donc par « Bezout » il existe des polynômes $U(X)$ et $V(X)$ tels que $U(X)T(X)+V(X)Q(X) = 1$, donc $1/Q(\theta) = V(\theta)$. Il en résulte que tout élément de K s'exprime de manière unique comme *polynôme* en θ de degré inférieur ou égal à $n-1$. En particulier K est un $\mathbb{Q}$-espace vectoriel de dimension n, une base étant $1, \theta, \ldots, \theta^{n-1}$. Un corps obtenu par adjonction d'un élément θ comme ci-dessus sera appelé *corps de nombres*. Le *théorème de l'élément primitif* (dont nous ne nous servirons pas) affirme que tout $\mathbb{Q}$-espace vectoriel de dimension finie est un corps de nombres.

Si $\theta_1 = \theta, \ldots, \theta_n$ sont les n racines complexes de $T(X)$, il est clair que l'application σ_i telle que $\sigma_i(A(\theta)) = A(\theta_i)$ est un plongement complexe de K dans $\mathbb{C}$, et il est évident que tout plongement est de cette forme. De plus, si $\theta_i \in K$ pour tout i, on dira que K est une extension *galoisienne* de $\mathbb{Q}$. Dans ce cas σ_i est non seulement un plongement de K dans $\mathbb{C}$ mais un *automorphisme* de K, et l'ensemble de ces automorphismes forme donc un groupe d'ordre n appelé *groupe de Galois* de $K/\mathbb{Q}$.

Définition 1.2. — Soit $\alpha \in K = \mathbb{Q}(\theta)$. On appelle *norme* de α et on note $\mathcal{N}_{K/\mathbb{Q}}(\alpha)$, ou simplement $\mathcal{N}(\alpha)$ lorsqu'il n'y aura pas d'ambiguïté, le déterminant de l'application $\mathbb{Q}$-linéaire $x \mapsto \alpha x$ de K dans K.

Il est clair par définition que la norme est *multiplicative* : $\mathcal{N}(\alpha\beta) = \mathcal{N}(\alpha)\,\mathcal{N}(\beta)$, et que $\mathcal{N}(\alpha) = \prod_{1 \leqslant i \leqslant n} \sigma_i(\alpha)$.

1.2. Propriétés en tant qu'anneau. — Soit $K = \mathbb{Q}(\theta)$ un corps de nombres comme ci-dessus, où θ est racine de $T(X) \in \mathbb{Q}[X]$. Pour faire de l'arithmétique dans K, ce qui est nécessaire pour les équations diophantiennes, nous devons agrandir $\mathbb{Z}$, comme nous avons agrandi $\mathbb{Q}$. Toutefois il n'est pas toujours vrai que ceci se fasse par adjonction. La définition est la suivante.

Définition 1.3. — On dit que $\alpha \in K$ est un entier algébrique s'il est racine d'un polynôme *unitaire* (c'est-à-dire de coefficient dominant égal à 1) à coefficients dans $\mathbb{Z}$ (et pas seulement dans $\mathbb{Q}$). L'ensemble des entiers algébriques de K est noté $\mathbb{Z}_K$.

C'est un exercice classique et facile de montrer que $\mathbb{Z}_K$ est un *anneau*. Si on choisit $T(X)$ unitaire à coefficients entiers pour définir le corps K (ce qu'on peut toujours facilement faire), il est donc clair que $\mathbb{Z}[\theta] \subset \mathbb{Z}_K$, et il est facile de voir que l'indice $[Z_K : \mathbb{Z}[\theta]]$ est *fini*. En fait, dans les applications que nous avons en vue, K sera un corps cyclotomique (voir ci-dessous), et on aura $\mathbb{Z}_K = \mathbb{Z}[\theta]$, mais ceci n'est pas vrai en général.

Définition 1.4

(1) On dit qu'un sous-ensemble $\mathfrak{a}$ de $\mathbb{Z}_K$ est un *idéal* de $\mathbb{Z}_K$ si c'est un sous-groupe additif stable par multiplication externe par $\mathbb{Z}_K$.

(2) On dit que $\mathfrak{a}$ est un idéal *principal* s'il est de la forme $\mathfrak{a} = \alpha\mathbb{Z}_K$ pour $\alpha \in \mathbb{Z}_K$.

(3) On dit qu'un idéal $\mathfrak{p}$ est *premier* s'il est différent de l'anneau tout entier et si pour tout α et β dans $\mathbb{Z}_K$, $\alpha\beta \in \mathfrak{p}$ implique que α ou β appartient à $\mathfrak{p}$ ou, de manière équivalente, si $\mathbb{Z}_K/\mathfrak{p}$ est un anneau intègre.

On conviendra toujours d'exclure l'idéal nul. Si $\mathfrak{a}$ et $\mathfrak{b}$ sont deux idéaux, on appellera produit de $\mathfrak{a}$ et de $\mathfrak{b}$, et on notera $\mathfrak{ab}$, l'ensemble des *combinaisons linéaires* finies $\sum_i a_i b_i$ avec $a_i \in \mathfrak{a}$ et $\mathfrak{b}_i \in \mathfrak{b}$. Il est clair que c'est un idéal.

Le résultat suivant est immédiat, puisque tout anneau fini intègre est un corps.

Proposition 1.5. — *Si $\mathfrak{a}$ est un idéal (non nul) l'anneau quotient $\mathbb{Z}_K/\mathfrak{a}$ est* fini. *En particulier, $\mathfrak{p}$ est un idéal premier non nul si et seulement si $\mathbb{Z}_K/\mathfrak{p}$ est un corps fini.*

Ceci conduit donc à la définition suivante.

Définition 1.6. — Si $\mathfrak{a}$ est un idéal non nul de $\mathbb{Z}_K$ on appelle *norme* de $\mathfrak{a}$, et on note $\mathcal{N}(\mathfrak{a})$, le nombre d'éléments de l'anneau quotient $\mathbb{Z}_K/\mathfrak{a}$.

Le résultat suivant n'est pas difficile mais est essentiel.

Proposition 1.7

(1) *La norme est multiplicative sur les idéaux : $\mathcal{N}(\mathfrak{ab}) = \mathcal{N}(\mathfrak{a})\,\mathcal{N}(\mathfrak{b})$.*

(2) *Si $\mathfrak{a} = \alpha\mathbb{Z}_K$ est un idéal principal on a $\mathcal{N}(\mathfrak{a}) = |\mathcal{N}(\alpha)|$.*

(3) *Si* $\mathfrak{p}$ *est un idéal premier, on a* $\mathcal{N}(\mathfrak{p}) = p^f$*, où* p *est la caractéristique du corps fini* $\mathbb{Z}_K/\mathfrak{p}$*, et* $f = \dim_{\mathbb{Z}/p\mathbb{Z}}(\mathbb{Z}_K/\mathfrak{p})$.

Quand on travaille dans les corps de nombres, il est essentiel de généraliser très légèrement la définition d'un idéal. Si $\mathfrak{a}$ est un idéal de $\mathbb{Z}_K$ et $m \in \mathbb{Z}_{>0}$, on dira par abus que $\mathfrak{a}/m$ est un idéal (appelé idéal fractionnaire pour ne pas confondre, les idéaux ordinaires étant appelés les idéaux entiers) de $\mathbb{Z}_K$. Toutes les notions ci-dessus se généralisent immédiatement aux idéaux fractionnaires. Toutefois, la raison principale pour laquelle nous avons besoin de cette notion est le théorème suivant, qui regroupe les propriétés essentielles des idéaux.

Théorème 1.8

(1) *L'ensemble des idéaux (fractionnaires) non nuls de* K *est un* groupe *abélien* $I(K)$ *pour la multiplication des idéaux.*

(2) *Tout idéal (non nul)* $\mathfrak{a}$ *de* K *s'écrit de manière* unique *sous la forme* $\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{a})}$*, où les idéaux* $\mathfrak{p}$ *sont des idéaux premiers distincts de* $\mathbb{Z}_K$ *et* $v_{\mathfrak{p}}(\mathfrak{a}) \in \mathbb{Z}$.

(3) *Si on note* $\mathrm{Pr}(K)$ *le sous-groupe de* I *formé des idéaux principaux, le groupe quotient* $\mathrm{Cl}(K) = I(K)/\mathrm{Pr}(K)$ *est un groupe abélien* fini*, appelé groupe de classes d'idéaux de* K.

Ce théorème nous montre donc plusieurs choses. Tout d'abord, bien que l'existence et l'unicité de la décomposition en facteurs premiers ne soit pas vraie en général dans $\mathbb{Z}_K$ (c'est équivalent au fait que $\mathbb{Z}_K$ soit un anneau principal), c'est vrai pour les *idéaux*. D'autre part le groupe de classes $\mathrm{Cl}(K)$ mesure exactement « l'obstruction » de $\mathbb{Z}_K$ à être un anneau principal. Le fait qu'il soit fini montre que cette obstruction n'est pas si grave que cela. L'un des thèmes du présent exposé est de montrer comment contourner cette obstruction. Notons immédiatement le résultat suivant :

Proposition 1.9. — *Soit* $h(K) = |\mathrm{Cl}(K)|$ *le* nombre de classes *de* K. *Pour tout idéal* $\mathfrak{a}$ *de* K *l'idéal* $\mathfrak{a}^{h(K)}$ *est un idéal principal.*

Démonstration. — C'est clair, mais très important. □

Un autre groupe indissolublement lié au groupe de classes est le groupe des unités :

Définition 1.10. — On dira que $u \in \mathbb{Z}_K$ est une *unité* si u est inversible dans $\mathbb{Z}_K$. Le groupe des unités sera noté $U(K)$.

Il est immédiat de voir que *si* $u \in \mathbb{Z}_K$ alors u est une unité si et seulement si $\mathcal{N}(u) = \pm 1$. L'importance du groupe des unités réside dans le fait évident que deux éléments α et β engendrent le même idéal principal si et seulement si α/β est une unité.

Le théorème fondamental sur les unités, dû à Dirichlet, et qui se démontre simultanément avec le théorème sur la finitude du groupe de classes $\mathrm{Cl}(K)$, est le suivant.

Théorème 1.11. — *Soit K un corps de nombres de degré n, soit r_1 le nombre de ses plongements complexes σ_i tels que $\sigma_i(K) \subset \mathbb{R}$, et posons $2r_2 = n - r_1$ et $r = r_1 + r_2 - 1$. Il existe une racine de l'unité $\zeta \in K$ d'ordre $w \in \mathbb{Z}_{>0}$, et des unités $\varepsilon_1, \dots, \varepsilon_r$ tels que toute unité $u \in U(K)$ s'écrive de manière* unique

$$u = \zeta^j \prod_{1 \leqslant i \leqslant r} \varepsilon_i^{x_i} \quad \textit{avec } x_i \in \mathbb{Z} \textit{ et } 0 \leqslant j < w.$$

1.3. Les corps cyclotomiques. — Les corps de nombres qui pour nous seront les plus importants sont les corps dits *cyclotomiques*, car provenant de la division du cercle. Soit ζ_n une racine primitive n-ième de l'unité dans $\mathbb{C}$. On appelle n-ième corps cyclotomique le corps de nombres obtenu en adjoignant ζ_n à $\mathbb{Q}$. Pour simplifier nous nous restreindrons au cas où $n = p$ est un nombre premier. Le théorème suivant résume les propriétés de base et n'est pas difficile.

Théorème 1.12. — *Soit $p \geqslant 3$ un nombre premier, $\zeta = \zeta_p$ une racine primitive p-ième de l'unité et $K = \mathbb{Q}(\zeta)$.*

(1) *Le polynôme minimal de ζ est le polynôme $(X^p - 1)/(X - 1) = X^{p-1} + \cdots + X + 1$.*

(2) *Le corps K est galoisien. Les automorphismes de K sont les applications σ_j de K dans K laissant fixe $\mathbb{Q}$ et envoyant ζ sur ζ^j, où $1 \leqslant j \leqslant p - 1$, et donc $\mathrm{Gal}(K/\mathbb{Q}) = (\mathbb{Z}/p\mathbb{Z})^*$.*

(3) *L'idéal principal $\mathfrak{p} = (1 - \zeta)\mathbb{Z}_K$ est un idéal premier de $\mathbb{Z}_K$ de norme p, et c'est le seul idéal premier divisant $p\mathbb{Z}_K$. Plus précisément on a $p\mathbb{Z}_K = \mathfrak{p}^{p-1}$.*

(4) *On a $\mathbb{Z}_K = \mathbb{Z}[\zeta]$.*

(5) *Le groupe des racines de l'unité de K est engendré par $-\zeta$, en d'autres termes une racine de l'unité de K est de la forme $\pm\zeta^k$ pour un certain signe $\pm$ et $0 \leqslant k < p$.*

(6) *Les éléments $u_{i,j} = (1-\zeta^i)/(1-\zeta^j)$ pour $1 \leqslant i, j \leqslant p-1$ sont des unités de $\mathbb{Z}_K$.*

Un autre résultat sur les unités est crucial bien que facile.

***Proposition 1.13* (Kronecker).** — *Soit $u \in \mathbb{Z}_K$ un* entier algébrique *de K. Supposons que $|\sigma_i(u)| = 1$ pour tout plongement σ_i de K dans $\mathbb{C}$. Alors u est une racine de l'unité.*

Démonstration. — La démonstration est très simple et je l'esquisse ici. Soit $A(X) = \prod_i (X - \sigma_i(\alpha))$ le polynôme caractéristique de u, qui est donc dans $\mathbb{Z}[X]$. Pour tout $k \in \mathbb{Z}_{>0}$ considérons le polynôme $A_k(X) = \prod_i (X - \sigma_i(\alpha)^k)$. Les coefficients de A_k sont des polynômes symétriques en $\sigma_i(\alpha)$ à coefficients entiers, donc sont des polynômes à coefficients entiers dans les coefficients de A, donc sont dans $\mathbb{Z}$. De plus, puisque $|\sigma_i(\alpha)^k| = 1$ pour tout i le coefficient de X^{n-m} dans $A_k(X)$ est borné en valeur absolue par $\binom{n}{m}$. Il ne peut donc y avoir qu'un nombre *fini* de polynômes distincts $A_k(X)$, et donc qu'un nombre fini de $\sigma_i(\alpha)^k$. Il est aisé d'en déduire que α est une racine de l'unité. □

***Corollaire 1.14*.** — *Soit $K = \mathbb{Q}(\zeta)$ un corps cyclotomique avec $\zeta = \zeta_p$ et $p \neq 2$.*

(1) *Si $u \in U(K)$ alors $u/\overline{u}$ est une racine de l'unité, où u désigne la conjugaison complexe.*

(2) *Si $u \in U(K)$ il existe $k \in \mathbb{Z}$ tel que $u/\zeta^k \in \mathbb{R}$.*

Démonstration. — (1) résulte immédiatement du résultat ci-dessus puisque $K/\mathbb{Q}$ est galoisien de groupe de Galois abélien, et que la conjugaison complexe appartient à ce groupe. (2) n'est pas difficile et laissé en exercice. □

1.4. Retour au théorème de Fermat. — Avant de passer à l'équation de Catalan, voyons comment utiliser les outils que nous avons introduits pour le théorème de Fermat, qui est à l'origine de la théorie algébrique des nombres. Considérons donc notre équation $x^p + y^p = z^p$ avec $p \geqslant 3$ et $xyz \neq 0$. Comme il a déjà été mentionné,

on peut supposer x, y et z premiers entre eux deux à deux. Puisque p est impair on peut écrire

$$x^p + y^p = \prod_{0 \leqslant j \leqslant p-1} (x + \zeta^j y).$$

Supposons tout d'abord que l'anneau $\mathbb{Z}_K = \mathbb{Z}[\zeta]$ soit un anneau *principal*. Parmi les propriétés essentielles et caractéristiques des anneaux principaux figurent l'existence d'un PGCD défini à multiplication près par un élément inversible de l'anneau, donc par une *unité*, et l'existence et l'unicité (à permutation et unités près) de la décomposition en éléments premiers. Revenant au produit ci-dessus, puisque les puissances de ζ sont des unités il est clair que le PGCD de $x + \zeta^j y$ et $x + \zeta^k y$ doit diviser $(1 - \zeta^{k-j})y = \zeta^{-j}(x + \zeta^j y - (x + \zeta^k y))$ ainsi que $(1 - \zeta^{k-j})x = (x + \zeta^k y - \zeta^{k-j}(x + \zeta^j y))$, et donc puisque x et y sont premiers entre eux (dans $\mathbb{Z}$, mais *a fortiori* dans $\mathbb{Z}_K$) il doit diviser $1 - \zeta^{k-j}$. Or si $k \not\equiv j \pmod{p}$ on a vu (et il est immédiat de le vérifier) que $(1 - \zeta^{k-j})/(1 - \zeta)$ est une unité, donc comme le PGCD est défini à une unité près il doit diviser $1 - \zeta$.

Comme $(1 - \zeta)\mathbb{Z}_K$ est idéal premier et qu'il divise p, il en résulte que (à une unité près bien sûr) le PGCD ne peut qu'être égal à 1 ou à $1 - \zeta$, ce dernier cas ne pouvant de produire que si $p \mid z$. On est donc amené à considérer deux cas dans le théorème de Fermat : le premier cas où $p \nmid z$, et le deuxième où $p \mid z$. Le deuxième cas étant plus difficile, et de toutes façons le théorème de Fermat n'étant pas notre but principal, nous allons nous limiter au premier cas $p \nmid xyz$. Il résulte donc de la discussion ci-dessus que les facteurs $x + \zeta^j y$ de z^p sont premiers entre eux deux à deux. Remarquons alors que le cas $p = 3$ est immédiat : comme $x^3 \equiv 0$ ou ± 1 modulo 9 on ne peut pas avoir $x^3 + y^3 = z^3$ sans que $3 \mid xyz$. Nous supposerons donc $p \geqslant 5$ (on verra ci-dessous où cela intervient).

Utilisant l'existence et l'unicité de la décomposition en facteurs premiers dans $\mathbb{Z}_K$ il en résulte que chaque $x + \zeta^j y$ *individuellement* est une puissance p-ième dans $\mathbb{Z}_K$ à une unité près, en d'autres termes que pour chaque j il existe $\alpha_j \in \mathbb{Z}_K$ et une unité u_j tels que $x + \zeta^j y = u_j \alpha_j^p$. En particulier nous pouvons écrire $x + \zeta y = u\alpha^p$ pour une certaine unité u, et un $\alpha \in \mathbb{Z}_K$.

Avant de poursuivre, voyons maintenant ce qu'on peut faire si on ne suppose plus que $\mathbb{Z}_K$ est principal. Le seul outil à notre disposition est maintenant la notion d'idéal : on a existence et unicité de la décomposition en produit *d'idéaux* premiers, et la notion de PGCD a un sens en tant qu'idéal. Le raisonnement ci-dessus montre donc que les *idéaux* principaux $(x+\zeta^j y)\mathbb{Z}_K$ sont premiers entre eux deux à deux (si on suppose $p \nmid z$), et donc qu'ils sont individuellement égaux à une puissance p-ième d'un *idéal* : $(x+\zeta^j y)\mathbb{Z}_K = \mathfrak{a}_j^p$ pour un certain idéal $\mathfrak{a}_j$.

Nous voulons maintenant « tuer » l'obstruction provenant du fait que le groupe des classes n'est pas forcément réduit à l'élément neutre. La manière la plus simple (mais non la seule comme nous le verrons) est d'utiliser le fait mentionné ci-dessus que $\mathfrak{a}_j^{h(K)}$ est un idéal principal. Supposons que p ne divise pas $h(K)$ (nous reviendrons ci-dessous sur cette hypothèse). Par « Bezout » il existe des entiers u et v tels que $up + vh(K) = 1$. Il en résulte que $\mathfrak{a}_j = (\mathfrak{a}_j^p)^u(\mathfrak{a}_j^{h(K)})^v$ est un idéal principal ! Si on écrit $\mathfrak{a}_j = \alpha_j\mathbb{Z}_K$, on a donc $(x+\zeta^j y)\mathbb{Z}_K = \alpha_j^p\mathbb{Z}_K$. Nous avons donc deux générateurs du même idéal principal, et donc il existe une unité $u_j \in U(K)$ telle que $x+\zeta^j = u_j\alpha_j^p$. Nous aboutissons donc à exactement *la même* conclusion qu'en supposant $\mathbb{Z}_K$ principal, ce qui est remarquable.

Reste à voir dans quelle mesure la condition $p \nmid h(K)$ est restrictive. Un nombre premier vérifiant cette condition est dit *régulier*. Parmi les 24 nombres premiers impairs inférieurs à 100, seuls les trois nombres $p = 37$, 59 et 67 ne le sont pas, ce qui est bon signe. Toutefois il faut noter que bien que l'on sache montrer qu'il existe une infinité de nombres premiers *irréguliers*, on ne sait pas montrer qu'il en existe une infinité de réguliers, bien que cela semble être le cas (et on conjecture beaucoup plus).

Bref, si on se limite aux exposants premiers $p \leqslant 100$, le travail que nous avons fait ci-dessus est applicable pour 21 des 24 valeurs possibles.

Pour terminer la démonstration du premier cas du théorème de Fermat pour les exposants réguliers, il faut maintenant s'occuper des unités. C'est un phénomène tout à fait général : quand on utilise des méthodes de théorie algébrique des nombres pour étudier une équation diophantienne, on commence par utiliser les idéaux et la structure du

groupe de classes d'idéaux, puis les propriétés des unités. Puisque notre but est Catalan et pas Fermat, le lecteur peut sauter ce qui suit sans que cela nuise à la compréhension.

Soit $\mathfrak{p} = (1-\zeta)\mathbb{Z}_K$ comme ci-dessus l'unique idéal premier divisant p, qui est tel que $\mathfrak{p}^{p-1} = p\mathbb{Z}_K$. Notons tout d'abord que pour tout j on a $\overline{\zeta^j} = \zeta^{p-j} \equiv \zeta^j \pmod{\mathfrak{p}}$, donc par linéarité, pour tout $\alpha \in \mathbb{Z}_K$ on a $\overline{\alpha} \equiv \alpha \pmod{\mathfrak{p}}$. D'après ce que nous avons dit ci-dessus on a $x+\zeta^j y = u_j \alpha_j^p$ pour certains $\alpha_j \in \mathbb{Z}_K$ et certaines unités u_j. Posons $\alpha = \alpha_1$ et $u = u_1$. Comme $z^p/\alpha \in \mathbb{Z}_K$ et que $p \nmid z$ par hypothèse, on a nécessairement $\mathfrak{p} \nmid \alpha$, donc $\alpha/\overline{\alpha} \equiv 1 \pmod{\mathfrak{p}}$, en d'autres termes il existe $\beta \in K$ tel que $\alpha/\overline{\alpha} = 1+(1-\zeta)\beta$, où $v_{\mathfrak{p}}(\beta) \geqslant 0$ (noter que β n'est pas nécessairement dans $\mathbb{Z}_K$, mais ce n'est pas important). Si on élève cette égalité à la puissance p et qu'on utilise le fait que les coefficients binomiaux $\binom{p}{k}$ pour $1 \leqslant k \leqslant p-1$ sont divisibles par p, donc par $(1-\zeta)^{p-1}$, on obtient

$$\alpha^p/\overline{\alpha^p} = 1 + (1-\zeta)^p\gamma,$$

où $v_{\mathfrak{p}}(\gamma) \geqslant 0$. Or par définition on a $x+\zeta y = u\alpha^p$, donc $x+\zeta^{-1}y = \overline{u}\overline{\alpha^p}$, et donc on obtient

$$(x+\zeta y)/(x+\zeta^{-1}y) = (u/\overline{u})(1+(1-\zeta)^p\gamma),$$

en d'autres termes

$$x+\zeta y - (u/\overline{u})(x+\zeta^{-1}y) \equiv 0 \pmod{\mathfrak{p}^p},$$

où nous pouvons à nouveau mettre des congruences puisque tout est dans $\mathbb{Z}_K$, u étant inversible.

D'après le corollaire énoncé ci-dessus comme conséquence du théorème de Kronecker, $\overline{u}/u$ est une racine de l'unité dans K, donc on a $u/\overline{u} = \pm\zeta^m$ pour un certain signe et un entier m tel que $0 \leqslant m < p$, donc que

$$x+\zeta y \mp \zeta^m(x+\zeta^{-1}y) \equiv 0 \pmod{\mathfrak{p}^p}.$$

J'affirme que $m = 1$. En effet, supposons le contraire. Si $m = 0$ on multiplie la congruence par ζ, et si $m = p-1$ on la multiplie par ζ^2, et sinon on ne fait rien. Nous voyons donc qu'il existe un polynôme $f(T) \in \mathbb{Z}[T]$ de degré au plus égal à $p-2 \geqslant 3$ (puisque nous avons supposé que $p \geqslant 5$), non divisible par p, et tel que $f(\zeta) \equiv 0 \pmod{\mathfrak{p}^p}$. Posons $g(X) = f(1-X)$, qui est aussi de degré au plus égal à $p-2$ et non divisible par p, et tel que $g(\pi) \equiv 0 \pmod{\mathfrak{p}^p}$.

Toutefois, comme $v_{\mathfrak{p}}(p) = p - 1$, il est clair que les différents monômes non nuls intervenant dans $g(\pi)$ ont des valuations qui ne sont pas congrues entre elles modulo $p - 1$, et qui sont donc distinctes. La valuation de $g(\pi)$ est donc égale à la valuation du monôme de plus petite valuation. Comme le degré de g est au plus $p - 2$ et que $v_{\mathfrak{p}}(g(\pi)) \geqslant p$ il en résulte que pour tous les coefficients g_i de g on a $v_{\mathfrak{p}}(g_i) \geqslant 1$, donc $v_p(g_i) \geqslant 1$, ce qui contredit l'hypothèse que les coefficients ne sont pas tous divisibles par p. Il en résulte que la seule possibilité est $m = 1$, et donc que notre congruence s'écrit

$$x + \zeta y \mp (x\zeta + y) = (x \mp y)(1 \mp \zeta) \equiv 0 \pmod{\mathfrak{p}^p},$$

et donc puisque $\mathfrak{p}^{p-1} = p\mathbb{Z}_K$ et $v_{\mathfrak{p}}(1 \mp \zeta) \leqslant 1$ on doit avoir $x \mp y \equiv 0 \pmod{p}$. Toutefois $x + y \equiv 0 \pmod{p}$ est impossible, sinon $p \mid z$. Il en résulte que $y \equiv x \pmod{p}$.

Nous pouvons maintenant appliquer le même raisonnement à l'équation $(-x)^p + z^p = y^p$ et en déduire que $-z \equiv x \pmod{p}$. Il en résulte que $0 = x^p + y^p - z^p \equiv 3x^p \pmod{p}$, et puisque $p \nmid x$, on obtient $p = 3$, qui a été exclu car traité directement. Ceci termine la démonstration du premier cas du théorème de Fermat dans le cas d'un exposant premier régulier. La démonstration ci-dessus est essentiellement due à Kummer.

Remarques

(1) En utilisant des techniques semblables mais un peu plus compliquées, on peut démontrer que le deuxième cas du théorème de Fermat est aussi valable pour un exposant régulier.

(2) En utilisant d'autres outils, et en particulier la loi de réciprocité d'Eisenstein, on peut démontrer la validité du premier cas pour tous les $p < 10^{18}$. Ces outils seront implicitement utilisés aussi dans la démonstration de la conjecture de Catalan.

(3) Par contre, on ne sait démontrer le deuxième cas de manière algébrique que si certaines conditions sont remplies, ce qui a été le cas dans tous les exemples étudiés.

(4) Bien entendu, le théorème de Fermat a finalement été démontré en 1995 par Wiles, Taylor et Ribet en utilisant des techniques complètement différentes et nettement plus sophistiquées.

2. La conjecture de Catalan : exposants pairs

2.1. Introduction : le théorème de V. Lebesgue. — La conjecture de Catalan, démontrée en 2003 par P. Mihăilescu, est l'énoncé suivant.

Théorème 2.1. — *Soient m et n deux entiers supérieurs ou égaux à 2. Les seules solutions en entiers non nuls x et y de l'équation*

$$x^m - y^n = 1$$

sont $(m, n, x, y) = (2, 3, \pm 3, 2)$.

Remarquons que l'exposant 2 n'est pas exclu. De ce fait, nous devons démontrer trois résultats bien distincts :

Théorème 2.2 **(V. Lebesgue).** — *Si $p \geqslant 2$ est premier, l'équation $x^p - y^2 = 1$ n'a pas de solution non triviale.*

Théorème 2.3 **(Ko Chao).** — *Si $q \geqslant 2$ est premier, les seules solutions non triviales de l'équation $x^2 - y^q = 1$ sont $(q, x, y) = (3, \pm 3, 2)$.*

Théorème 2.4 **(Mihăilescu).** — *Si p et q sont deux nombres premiers impairs, l'équation $x^p - y^q = 1$ n'a pas de solution non triviale.*

Avant d'attaquer le vif du sujet, remarquons que le théorème de V. Lebesgue (1850) se démontre sans difficulté par des méthodes semblables à celles que nous avons vues ci-dessus pour le théorème de Fermat. Par contre, il est à noter que le théorème de Ko Chao (1965) n'a été démontré que plus d'un siècle plus tard, bien que les méthodes soient analogues mais plus subtiles. Enfin le théorème de Mihăilescu (2003) utilise toute la puissance de la théorie des corps cyclotomiques et est beaucoup plus complexe. C'est d'ailleurs un peu miraculeux que les techniques des corps cyclotomiques suffisent pour démontrer Catalan complètement (les techniques de Ribet–Wiles sont inapplicables).

Nous commençons donc par démontrer le théorème de V. Lebesgue. Noter qu'il ne s'agit pas de l'inventeur de l'intégrale du même nom.

Démonstration du théorème de Lebesgue. — Notons tout d'abord que si y est impair on a $y^2+1 \equiv 2 \pmod 8$ ce qui est impossible pour une puissance p-ième avec $p \geqslant 2$. Il en résulte que y est pair, donc que x est impair. D'autre part il est clair que l'équation n'a pas de solution non triviale pour $p=2$, et nous supposerons donc p impair. Écrivant notre équation sous la forme $y^2+1=x^p$, nous la *factorisons* dans le corps des nombres de Gauss $K=\mathbb{Q}(i)$, dont l'anneau d'entiers $\mathbb{Z}_K=\mathbb{Z}[i]$ est l'anneau des entiers de Gauss, qui est principal et dont les unités sont i^k pour $0 \leqslant k \leqslant 3$. De la factorisation $(y+i)(y-i)=x^p$ on déduit, puisque x est impair, que les deux facteurs sont premiers entre eux, donc qu'ils sont égaux à une puissance p-ième, à une unité près. Il existe donc $\alpha \in \mathbb{Z}[i]$ et un entier k tel que $y+i=i^k\alpha^p$. Mais comme p est premier à 4, par « Bezout » on peut écrire $up+4v=1$ donc $i=(i^4)^v(i^u)^p=(i^u)^p$, donc i est une puissance p-ième. Donc quitte à modifier α on a $y+i=\alpha^p$.

Écrivons $\alpha=a+ib$. On a $\alpha^p=A+iB$ avec en particulier

$$B=\sum_{k=0}^{(p-1)/2}\binom{p}{2k}a^{2k}b^{p-2k}(-1)^{(p-1)/2-k}.$$

En particulier on voit que $b \mid B$. Comme $B=1$ on a donc $b=\pm 1$, d'où la relation

$$\sum_{k=0}^{(p-1)/2}\binom{p}{2k}a^{2k}(-1)^{(p-1)/2-k}=\pm 1.$$

Puisque $p \mid \binom{p}{2k}$ pour $1 \leqslant k \leqslant (p-1)/2$ on en déduit, en regardant modulo p, que le membre de droite est congru à $(-1)^{(p-1)/2}$ modulo p, donc qu'il est égal à cette quantité. On a donc

$$L=\sum_{k=1}^{(p-1)/2}\binom{p}{2k}a^{2k}(-1)^k=0.$$

J'affirme que a est pair. En effet, sinon en considérant l'équation modulo 2 on obtiendrait

$$\sum_{k=0}^{(p-1)/2}\binom{p}{2k}(-1)^k \equiv 1 \pmod 2,$$

ce qui est absurde puisque le membre de gauche est égal à 2^{p-1} qui est pair.

Posons maintenant

$$u_k = \binom{p}{2k} a^{2k} = \frac{p(p-1)}{2k(2k-1)} \binom{p-2}{2k-2} a^{2k}.$$

Puisque $u_1 = p(p-1)a^2/2$ on a

$$\frac{u_k}{u_1} = \frac{1}{k(2k-1)} \binom{p-2}{2k-2} a^{2k-2},$$

ce qui implique que pour $k > 1$ (donc pour $p > 3$) on a

$$v_2(u_k) - v_2(u_1) \geqslant (2k-2)v_2(a) - v_2(k) \geqslant (2k-2) - v_2(k)$$

puisque a est pair. On vérifie immédiatement que cette dernière expression est toujours plus grande ou égale à 1, et donc que $v_2(u_k) > v_2(u_1)$ pour $k > 1$. Puisque $L = \sum_{k=1}^{(p-1)/2} (-1)^k u_k$ il en résulte que $v_2(L) = v_2(u_1) = v_2((p(p-1)/2)a^2)$, ce qui est impossible pour $a \neq 0$ puisque $L = 0$. On doit donc avoir $a = 0$, donc $\alpha = \pm i$, et donc $y = 0$, montrant qu'il n'y a pas de solution non triviale. □

2.2. Les théorèmes de Nagell et Ko Chao. — Notre but est maintenant de démontrer le théorème de Ko Chao, en d'autres termes de montrer que les seules solutions non triviales de l'équation $x^2 - y^q = 1$ sont $(q, x, y) = (3, \pm 3, 2)$. Le fait qu'il *existe* des solutions est une indication que la démonstration sera (un peu) plus difficile. Nous commençons par démontrer le résultat préliminaire suivant, dû à Nagell. C'est la partie la plus délicate.

***Proposition 2.5* (Nagell).** — *Si x et y sont des entiers non nuls et q un nombre premier tel que $x^2 - y^q = 1$ alors $2 \mid y$ et $q \mid x$.*

Démonstration. — Comme nous l'avons déjà vu, on peut supposer que $q \neq 2$, et puisque $xy \neq 0$ on a $y > 0$, et nous pouvons bien sûr supposer que $x > 0$. Si y est impair x est pair, donc $x - 1$ et $x + 1$ sont premiers entre eux, et puisque $(x-1)(x+1) = y^q$, ceci implique que $x - 1$ et $x + 1$ sont tous deux des puissances q-ièmes, ce qui est impossible puisque deux puissances q-ièmes distinctes ne peuvent pas différer de 2. Il en résulte que y est pair, donc que x est impair.

Supposons par l'absurde que $q \nmid x$. On utilise ici la factorisation dans $\mathbb{Q}$

$$x^2 = (y+1)((y^q+1)/(y+1)) = Y((Y-1)^q + 1)/Y = Yr(Y),$$

où $Y = y + 1$. Il est clair que

$$r(Y) = ((Y-1)^q + 1)/Y = \sum_{1 \leqslant k \leqslant q} (-1)^{q-k} \binom{q}{k} Y^{k-1},$$

donc que $\operatorname{pgcd}(r(Y), Y) = \operatorname{pgcd}(q, Y) = \operatorname{pgcd}(q, y+1)$. Comme $q \nmid x$ on ne peut pas avoir $q \mid y+1$, donc Y et $r(Y)$ sont premiers entre eux. Il en résulte que chacun d'eux est un carré (car nous avons choisi $y > 0$). Écrivons donc $y + 1 = a^2$, $(y^q + 1)/(y + 1) = b^2$, et donc $x = ab$, avec $a > 0$, $b > 0$. Puisque $y \neq 0$, notons en particulier que y n'est pas un carré.

Soit $K = \mathbb{Q}(\sqrt{y})$ le corps de nombres obtenu en adjoignant $\sqrt{y}$ à $\mathbb{Q}$, qui est donc différent de $\mathbb{Q}$, et posons $\alpha = x + y^{(q-1)/2}\sqrt{y} \in \mathbb{Z}[\sqrt{y}]$. Notons que l'anneau $A = \mathbb{Z}[\sqrt{y}]$ est un sous-anneau de $\mathbb{Z}_K$, mais n'est pas égal à $\mathbb{Z}_K$ en général.

La norme de α dans K est égale à $x^2 - y^q$ donc à 1, et α est un entier algébrique. C'est donc une *unité* de A. Puisque $y^2 + 1 = a^2$, il n'est pas difficile de démontrer dans ce cas particulier (nous l'admettrons) que toute unité u de A s'écrit de manière unique $u = \pm(a + \sqrt{y})^k$ pour un $k \in \mathbb{Z}$ et un signe uniques. Comme nous avons supposé $x > 0$ et $y > 0$, il en résulte qu'il existe $k > 0$ tel que

$$\alpha = x + y^{(q-1)/2}\sqrt{y} = (a + \sqrt{y})^k.$$

Regardons tout d'abord cette équation modulo l'idéal yA. On obtient $x \equiv a^k + ka^{k-1}\sqrt{y} \pmod{yA}$, en d'autres termes $y \mid a^k - x$ et $y \mid ka^{k-1}$, et puisque y et a sont premiers entre eux (puisque $y^2 + 1 = a^2$) on a $y \mid k$. Puisque y est pair, il en résulte que k est pair.

Nous regardons maintenant l'égalité ci-dessus modulo l'idéal aA, en utilisant le fait que $x = ab \equiv 0 \pmod{a}$ et $y = a^2 - 1 \equiv -1 \pmod{a}$. On obtient

$$(-1)^{(q-1)/2}\sqrt{y} \equiv y^{k/2} \equiv (-1)^{k/2} \pmod{aA},$$

ce qui implique que $a \mid 1$, donc que $a = 1$, ce qui contredit l'hypothèse $y \neq 0$. □

Nous pouvons maintenant démontrer le théorème de Ko Chao.

Démonstration du théorème de Ko Chao. — Nous supposerons tout d'abord $q \geqslant 5$. D'après le résultat de Nagell nous savons que x est impair, et on peut supposer $x > 0$. Soit $\varepsilon = \pm 1$ choisi tel que $x \equiv \pm 1$

(mod 4). Comme on peut écrire $x^2-1=(x-\varepsilon)(x+\varepsilon)$ et que $(x+\varepsilon)/2$ est *impair*, un raisonnement analogue à ceux que nous avons fait à plusieurs reprises montre qu'il existe des entiers a et b (que l'on peut supposer strictement positifs) tels que $x-\varepsilon=2^{q-1}a^q$ et $x+\varepsilon=2b^q$. Puisque $q\geqslant 5$ on a $a^q=(b^q-\varepsilon)/2^{q-2}<b^q$, et donc $a<b$ (en fait il est immédiat de voir que ceci est encore vrai pour $q=3$). D'autre part on a

$$(b^2-2\varepsilon a)\frac{b^{2q}-(2\varepsilon a)^q}{b^2-2\varepsilon a}=b^{2q}-(2\varepsilon a)^q=\left(\frac{x+\varepsilon}{2}\right)^2-2\varepsilon(x-\varepsilon)$$
$$=\left(\frac{x-3\varepsilon}{2}\right)^2.$$

D'après le résultat de Nagell nous savons que $q\mid x$. Puisque $q\geqslant 5$ (ici c'est essentiel), il en résulte que $q\nmid(x-3\varepsilon)/2$, et donc, par un raisonnement analogue à celui fait pour le théorème de Nagell on en déduit que les deux facteurs du membre de gauche sont premiers entre eux, donc sont des carrés parfaits. Toutefois puisque $0<a<b$ on a

$$(b-1)^2=b^2-2b+1<b^2-2a<b^2<b^2+2a<b^2+2b+1=(b+1)^2,$$

ce qui montre que $b^2-2\varepsilon a$ ne peut pas être un carré, contradiction.

Il reste à traiter le cas $q=3$, qui est plus simple mais nécessite une technique un peu différente due à Skolem, donc bien antérieure. Comme ci-dessus nous savons qu'il existe deux entiers a et b tels que $x-\varepsilon=4a^3$ et $x+\varepsilon=2b^3$, donc $b^3-2a^3=\pm1$. Ici il est naturel de travailler dans le corps de nombres $K=\mathbb{Q}(\theta)$, où θ est la racine cubique réelle de 2. Notre nouvelle équation signifie que $\alpha=b-a\theta$ est un entier algébrique de norme ±1, c'est-à-dire une *unité* de K. D'après le théorème de Dirichlet sur la structure du groupe des unités, il est facile de voir qu'il existe $k\in\mathbb{Z}$ tel que $\alpha=b-a\theta=\pm(\theta-1)^k$. Ce qui est remarquable dans cette égalité est le fait que le coefficient de θ^2 soit nul. En la considérant modulo des puissances de 3, Skolem démontre qu'il ne peut exister qu'au plus une valeur de $k\neq 0$ pour laquelle ceci se produit (nous admettrons ce résultat). Comme $k=1$ convient, correspondant à $(a,b)=\mp(1,1)$, on en déduit qu'il n'y a pas d'autres solutions. Par contre, $(a,b)=\mp(1,1)$ conduit aux solutions $(x,y)=(\pm3,2)$. □

3. La conjecture de Catalan : les résultats de Cassels

3.1. Énoncés et réductions préliminaires. — Grâce aux résultats de V. Lebesgue et de Ko Chao, il suffit maintenant de considérer l'équation de Catalan $x^p - y^q = 1$ avec p et q nombres premiers *impairs*. Il est important de noter que si (p, q, x, y) est une solution, alors $(q, p, -y, -x)$ en sera une. Bien entendu cette réduction n'est possible que grâce au fait que nous avons traité les exposants pairs.

La démonstration de la conjecture de Catalan finalement obtenue par P. Mihăilescu repose de manière essentielle sur des résultats préliminaires obtenus par Cassels en 1960, qui généralisent le résultat de Nagell ci-dessus.

Le but des paragraphes qui suivent va être la démonstration du théorème suivant.

***Théorème 3.1* (Cassels).** — *Soient p et q des nombres premiers impairs et x et y des entiers non nuls tels que $x^p - y^q = 1$.*

(1) *On a $q \mid x$ et $p \mid y$.*

(2) *Plus précisément il existe des entiers non nuls a et b et des entiers positifs u et v tels que $q \nmid u$, $p \nmid v$ et vérifiant*

$$x = qbu,\ x - 1 = p^{q-1}a^q,\ \frac{x^p - 1}{x - 1} = pv^q,$$
$$y = pav,\ y + 1 = q^{p-1}b^p,\ \frac{y^q + 1}{y + 1} = qu^p.$$

Montrons tout de suite que (1) implique (2), l'inverse étant trivial. Comme d'habitude on écrit $y^q = (x-1)r(x)$, avec $r(x) = (x^p - 1)/(x - 1)$ et, en développant avec la formule du binôme, on a donc comme ci-dessus

$$r(x) = \sum_{0 \leqslant k \leqslant p-1} \binom{p}{k+1} (x-1)^k = p + \binom{p}{2}(x-1) + \cdots + \binom{p}{p}(x-1)^p.$$

Comme $p \mid y$, on en déduit que $p \mid (x - 1)$ ou $p \mid r(x)$, et dans ce dernier cas la formule ci-dessus montre que l'on a encore $p \mid (x - 1)$. En appliquant à nouveau cette formule, on en déduit que $r(x) \equiv p \pmod{p^2}$, et donc que $v_p(r(x)) = 1$. Puisque $v_p(x - 1) + v_p(r(x)) = qv_p(y)$, il en résulte que $v_p(x-1) \equiv q-1 \pmod{q}$. Comme la formule ci-dessus montre que $\operatorname{pgcd}(x - 1, r(x)) = p$, on en déduit donc qu'il existe a et v avec $p \nmid v$ tels que $x - 1 = p^{q-1}a^q$ et $r(x) = pv^q$, et alors

$y = pav$. Les autres formules en résultent par symétrie en changeant (p, q, x, y) en $(q, p, -y, -x)$, ce qu'on peut faire puisque p et q sont impairs.

Pour la même raison de symétrie il suffit de prouver que $p \mid y$. Notons que, puisque deux puissances q-ièmes ne peuvent différer de 1 que quand l'une est nulle, on a $p \neq q$. Nous allons considérer séparément les cas $p < q$ et $p > q$, qui sont, comme nous allons le voir, de difficultés assez différentes.

3.2. Preuve du théorème de Cassels pour $p < q$. — Nous avons d'abord besoin du petit lemme suivant, dont la démonstration facile est laissée au lecteur :

Lemme 3.2

(1) *Pour tout $x \in \mathbb{R}_{>0}$ on a $(x+1)\log(x+1) > x\log(x)$.*

(2) *Soit $b \in \mathbb{R}_{>1}$. La fonction $(b^t+1)^{1/t}$ est une fonction décroissante de $\mathbb{R}_{>0}$ dans $\mathbb{R}_{>0}$ et la fonction $(b^t-1)^{1/t}$ est une fonction croissante de $\mathbb{R}_{>0}$ dans $\mathbb{R}_{>0}$.*

(3) *Supposons que $0 < p < q$ soient des nombres réels. Si $a \in \mathbb{R}_{\geqslant 1}$ alors $(a^q+1)^p < (a^p+1)^q$ et si $a \in \mathbb{R}_{>1}$ alors $(a^q-1)^p > (a^p-1)^q$.*

Le théorème de Cassels pour $p < q$ est donc le résultat suivant :

Proposition 3.3. — *Si p et q sont des nombres premiers impairs tels $p < q$ et x et y des entiers non nuls tels que $x^p - y^q = 1$ alors $p \mid y$.*

Démonstration. — Supposons par l'absurde que $p \nmid y$. D'après le raisonnement fait ci-dessus, les entiers $x-1$ et $r(x) = (x^p-1)/(x-1)$ sont premiers entre eux et, comme leur produit est égal à y^q, chacun d'eux est une puissance q-ième. Écrivons donc $x - 1 = a^q$ pour un entier a, avec $a \neq 0$ (sinon $y = 0$) et $a \neq -1$ (sinon $x = 0$), et donc $(a^q+1)^p - y^q = 1$. Considérons la fonction $f(z) = (a^q+1)^p - z^q - 1$, qui est trivialement une fonction strictement décroissante. Supposons tout d'abord que $a \geqslant 1$. Alors $f(a^p) = (a^q+1)^p - a^{pq} - 1 > 0$ d'après la formule du binôme, alors que $f(a^p+1) = (a^q+1)^p - (a^p+1)^q - 1 < 0$ d'après (3) du lemme ci-dessus. Puisque f est strictement décroissante, il en résulte que la valeur de y telle que $f(y) = 0$ n'est pas un entier, contradiction. De manière analogue, supposons que $a < 1$, donc que $a \leqslant -2$ d'après la remarque ci-dessus, et posons $b = -a$.

Puisque p et q sont impairs on a $f(a^p) = (a^q+1)^p - a^{pq} - 1 = -((b^q-1)^p - b^{pq}+1) > 0$ par la formule du binôme, alors que $f(a^p+1) = (a^q+1)^p - (a^p+1)^q - 1 = -((b^q-1)^p - (b^p-1)^q+1) < 0$, à nouveau grâce au lemme ci-dessus puisque $b \geqslant 2$. On obtient à nouveau une contradiction, ce qui démontre la proposition et donc le résultat de Cassels pour $p < q$. □

Avant d'attaquer le cas plus difficile $p > q$, nous démontrons une inégalité due à S. Hyyrö dont nous aurons besoin.

Corollaire 3.4. — *Avec les mêmes hypothèses que ci-dessus, et en particulier en supposant toujours que $p < q$, on a $|y| \geqslant p^{q-1} + p$.*

Démonstration. — Grâce à la proposition que nous venons de démontrer nous savons que $p \mid y$, et donc, comme dans la démonstration de (1) implique (2) du théorème de Cassels donnée ci-dessus, on en déduit qu'il existe des entiers a et v tels que $a \neq 0$, $v > 0$ et $p \nmid v$ tels que $x - 1 = p^{q-1}a^p$, $(x^p-1)/(x-1) = pv^q$ et $y = pav$. Nous avons vu ci-dessus que

$$(x^p-1)/(x-1) = p + \sum_{1 \leqslant k \leqslant p-1} \binom{p}{k+1} (x-1)^k \equiv p \pmod{(x-1)},$$

donc que

$$p^{q-1} \mid (x-1) \mid (x^p-1)/(x-1) - p = p(v^q-1).$$

Il en résulte que $v^q \equiv 1 \pmod{p^{q-2}}$. Toutefois l'ordre du groupe multiplicatif $(\mathbb{Z}/p^{q-2}\mathbb{Z})^*$ est égal à $p^{q-3}(p-1)$, et puisque $p < q$, ceci est premier à q. Si k est l'ordre de v dans ce groupe, on a donc $k \mid \operatorname{pgcd}(q, p^{q-3}(p-1)) = 1$, donc $v \equiv 1 \pmod{p^{q-2}}$.

J'affirme que $v > 1$. En effet supposons par l'absurde que $v = 1$, donc que $x^{p-1} + \cdots + x + 1 = p$. Si $x > 1$ alors $2^{p-1} > p$, donc ceci est impossible. Puisque p et q sont premiers impairs et $a \neq 0$ on a $|x-1| = p^{q-1}|a|^p \geqslant 9$, donc si $x \leqslant 1$ nous devons avoir en fait $z = -x \geqslant 8$. Mais alors, puisque $p-1$ est pair, on a

$$p = z^{p-1} - z^{p-2} + \cdots + 1 \geqslant z^{p-1}(z-1) \geqslant z^{p-1} \geqslant 2^{p-1},$$

une contradiction qui démontre que $v > 1$. Puisque $v \equiv 1 \pmod{p^{q-2}}$ il en résulte que $v \geqslant p^{q-2}+1$, et donc que $|y| = pav \geqslant pv \geqslant p^{q-1}+p$. □

Remarque. — Une fois démontré le théorème de Cassels il n'est pas difficile de montrer que le résultat ci-dessus reste vrai sans l'hypothèse $p < q$. La démonstration est laissée au lecteur.

3.3. Preuve du théorème de Cassels pour $p > q$. — Nous pouvons maintenant aborder la démonstration du théorème de Cassels pour $p > q$. Nous avons vu que, dans le cas $p < q$, nous avons eu besoin d'une petite inégalité analytique facile à démontrer (et d'ailleurs laissée au lecteur). Ici nous avons besoin d'une telle inégalité, mais elle est un peu plus délicate donc nous la démontrons complètement.

Lemme 3.5. — *Supposons que $p > q$, posons $F(t) = ((1+t)^p - t^p)^{1/q}$, soit $m = \lfloor p/q \rfloor + 1$ la partie entière de p/q plus 1, et appelons $F_m(t)$ la somme des termes de degré au plus égaux à m dans le développement en série de Taylor de $F(t)$ autour de $t = 0$. Alors, pour tout $t \in \mathbb{R}$ tel que $|t| \leqslant 1/2$, on a*

$$|F(t) - F_m(t)| \leqslant \frac{|t|^{m+1}}{(1-|t|)^2}.$$

(Je conseille au lecteur « taupinal » de démontrer ce résultat tout seul au lieu de lire la démonstration qui suit).

Démonstration. — Posons $G(t) = (1+t)^{p/q}$. Il est clair que les coefficients de Taylor de $F(t)$ et de $G(t)$ autour de $t = 0$ coïncident à tout ordre $k < p$, et en particulier à l'ordre m puisque $m \leqslant p/3 + 1 < p$ (puisque $q \geqslant 3$ donc $p \geqslant 5$). Dans ce qui suit, supposons que $|t| < 1$. Par la formule de Taylor–Lagrange appliquée aux fonctions $x^{1/q}$ et $G(x)$ respectivement, il existe t_1 et t_2 tels que

$$\begin{aligned}|F(t) - F_m(t)| &\leqslant |F(t) - G(t)| + |G(t) - F_m(t)| \\ &\leqslant \frac{|t|^p}{q} t_1^{1/q-1} + |t|^{m+1} \frac{1}{(m+1)!} G^{(m+1)}(t_2) \\ &\leqslant \frac{|t|^p}{q} t_1^{1/q-1} + |t|^{m+1} \binom{p/q}{m+1} (1+t_2)^{p/q-m-1},\end{aligned}$$

où t_1 est entre $(1+t)^p$ et $(1+t)^p - t^p$, et t_2 entre 0 et t. Puisque $p/q < m \leqslant p/q + 1$ on a $-1 \leqslant p/q - m < 0$, et pour tout $j \geqslant 1$ on a $0 < p/q - (m-j) = j - (m - p/q) < j$. Il en résulte que

$$0 < \prod_{1 \leqslant j \leqslant m} (p/q - (m-j)) < \prod_{1 \leqslant j \leqslant m} j = m!,$$

et donc que

$$\left|\binom{p/q}{m+1}\right| = \frac{(m-p/q)}{m+1}\frac{\prod_{1\leqslant j\leqslant m}(p/q-(m-j))}{m!} \leqslant \frac{1}{m+1}.$$

Puisque $1/q-1<0$ et $p/q-m-1<0$, nous devons trouver des bornes *inférieures* pour t_1 et $1+t_2$. Si $t>0$, $(1+t)^p$ et $(1+t)^p-t^p$ sont tous deux strictement plus grands que 1, donc $t_1>1>1-t^p$. Si $t<0$ alors $(1+t)^p=(1-|t|)^p$ et $(1+t)^p-t^p=(1-|t|)^p+|t|^p>(1-|t|)^p$, et donc $t_1>(1-|t|)^p$ dans tous les cas. D'autre part on a trivialement $|1+t_2|\geqslant 1-|t|$. En regroupant ces inégalités on obtient

$$|F(t)-F_m(t)| \leqslant \frac{|t|^p}{q}(1-|t|)^{-p+p/q}+\frac{|t|^{m+1}}{m+1}(1-|t|)^{p/q-m-1},$$

cette inégalité étant valable pour tout $t\in\mathbb{R}$ tel que $|t|<1$. Si nous supposons de plus que $|t|\leqslant 1/2$ alors $|t|^{p-m-1}\leqslant(1-|t|)^{p-m-1}$ (puisque $m\leqslant p-1$), et donc

$$|t|^p(1-|t|)^{-p+p/q}\leqslant|t|^{m+1}(1-|t|)^{p/q-m-1}.$$

Il en résulte que

$$|F(t)-F_m(t)|\leqslant\left(\frac{1}{q}+\frac{1}{m+1}\right)|t|^{m+1}(1-|t|)^{p/q-m-1}.$$

Puisque $p/q-m-1\geqslant -2$ et $1/q+1/(m+1)\leqslant 1$, on obtient le résultat voulu. □

En plus de ce lemme donnant une inégalité de nature *analytique*, nous avons également besoin d'un lemme donnant une inégalité de nature *arithmétique*.

Rappelons que si $a\in\mathbb{C}$ et $k\in\mathbb{Z}_{\geqslant 0}$, on peut définir les coefficients du binôme généralisés $\binom{a}{k}$ par la formule

$$\binom{a}{k}=a(a-1)\cdots(a-k+1)/k!.$$

Ce sont les coefficients du développement de Taylor à l'origine de $(1+t)^a$.

Lemme 3.6. — *Soient p et q deux nombres premiers distincts, et posons $w(k)=k+v_q(k!)$. Alors $q^{w(k)}\binom{p/q}{k}$ est un entier non divisible par q, et $w(k)$ est une fonction strictement croissante de k.*

(À nouveau, le lecteur est invité à démontrer ce résultat tout seul sans lire ce qui suit).

Démonstration. — La démonstration qui suit pourra paraître artificielle, mais c'est en fait la plus naturelle qui soit quand on considère l'aspect « p-adique ». Fixons k et posons $P(x) = \binom{x}{k}$. C'est un polynôme de degré k en x à coefficients rationnels. Soit maintenant ℓ un nombre premier différent de q. Pour tout N entier, soit x_N un entier positif tel que $qx_N \equiv p \pmod{\ell^N}$, qui existe puisque q est premier à ℓ^N. D'après la formule de Taylor on peut écrire

$$P(x_N) = P(p/q) + \sum_{1 \leqslant j \leqslant k} (x_N - p/q)^j \frac{P^{(j)}(p/q)}{j!}.$$

Soit M le plus grand exposant de ℓ figurant au dénominateur des coefficients $P^{(j)}(p/q)/j!$. Puisque $q \neq \ell$, il est clair que, pour $N \geqslant M$, aucun des dénominateurs des nombres rationnels figurant dans la somme de droite ne sera divisible par ℓ. Comme il en va de même pour $P(x_N)$ puisque $P(x_N) \in \mathbb{Z}$, il en résulte que ℓ ne figure pas au dénominateur du nombre rationnel $P(p/q)$. Il résulte de ceci que $\binom{p/q}{k} = n/q^{w(k)}$ pour un entier n premier à q. Le calcul de l'exposant exact $w(k)$ est immédiat : on a

$$\binom{p/q}{k} = \frac{p(p-q)\cdots(p-q(k-1))}{q^k k!}.$$

Comme p et q sont premiers entre eux, le numérateur est premier à q, et donc $w(k) = v_q(q^k k!) = k + v_q(k!)$, ce qui démontre la première assertion. La deuxième est évidente puisque $w(k+1) = 1 + v_q(k+1) + w(k)$. □

Nous sommes maintenant en mesure de démontrer le théorème de Cassels pour $p > q$.

Proposition 3.7. — *Si p et q sont des nombres premiers impairs tels $p > q$ et x et y des entiers non nuls tels que $x^p - y^q = 1$ alors $p \mid y$.*

Démonstration. — Nous conservons les notations du lemme 3.5, et nous commençons comme pour le cas $p < q$: on suppose par l'absurde que $p \nmid y$, et on en déduit qu'il existe $a \in \mathbb{Z} \setminus \{0\}$ tel que $x - 1 = a^q$, et donc $y^q = (a^q+1)^p - 1$, d'où $y = a^p F(1/a^q)$, où F est comme dans le lemme 3.5. Il en résulte que si on pose $z = a^{mq-p}y - a^{mq}F_m(1/a^q)$ on a

$z = a^{mq}(F(1/a^q) - F_m(1/a^q))$. Comme dans beaucoup de problèmes diophantiens, nous allons démontrer que pour un certain entier non nul D on a $Dz \in \mathbb{Z}$, et que par ailleurs $|Dz| < 1$, ce qui montrera que $z = 0$ et conduira à une contradiction.

Nous appliquons le lemme 3.5 à $t = 1/a^q$ (qui vérifie bien $|t| \leqslant 1/2$ puisque $a \neq \pm 1$), et on obtient donc

$$|z| \leqslant \frac{|a|^q}{(|a|^q - 1)^2} \leqslant \frac{1}{|a|^q - 2} \leqslant \frac{1}{|x| - 3}.$$

D'après la formule de Taylor on a $t^m F_m(1/t) = \sum_{0 \leqslant j \leqslant m} \binom{p/q}{j} t^{m-j}$, et d'après le lemme 3.6 $D = q^{m+v_q(m!)}$ est un dénominateur commun de tous les coefficients binomiaux $\binom{p/q}{j}$ pour $0 \leqslant j \leqslant m$. Il en résulte que $Da^{mq}F_m(1/a^q) \in \mathbb{Z}$, et puisque $mq \geqslant p$, que $Dz \in \mathbb{Z}$.

Nous allons maintenant borner $|Dz|$. D'après le résultat de Hyyrö (corollaire 3.4), avec (p, q, x, y) remplacé par $(q, p, -y, -x)$ pour que l'inégalité $p > q$ soit renversée, on a $|x| \geqslant q^{p-1} + q \geqslant q^{p-1} + 3$, et donc d'après l'inégalité pour $|z|$ obtenue ci-dessus on a

$$|Dz| \leqslant \frac{D}{|x| - 3} \leqslant q^{m+v_q(m!)-(p-1)}.$$

Or il est bien connu et facile que pour $m \geqslant 1$ on a $v_q(m!) < m/(q-1)$, et puisque $m < p/q + 1$ on a

$$m + v_q(m!) - (p-1) < m\frac{q}{q-1} - (p-1) = \frac{3 - (p-2)(q-2)}{q-1} \leqslant 0,$$

puisque $q \geqslant 3$ et $p \geqslant 5$ (noter qu'il est absolument essentiel que l'inégalité obtenue ci-dessus soit stricte). Il en résulte que $|Dz| < 1$, et puisque $Dz \in \mathbb{Z}$ on a donc $Dz = 0$. Ceci va rapidement conduire à une contradiction : en effet on a

$$Dz = Da^{mq-p}y - \sum_{0 \leqslant j \leqslant m} D\binom{p/q}{j} a^{q(m-j)},$$

et d'après le lemme 3.6 on a aussi

$$v_q\left(\binom{p/q}{j}\right) < v_q\left(\binom{p/q}{m}\right) = v_q(D)$$

pour $0 \leqslant j \leqslant m-1$, et donc $0 = Dz \equiv D\binom{p/q}{m} \not\equiv 0 \pmod{q}$ toujours d'après le même lemme. Cette contradiction termine la démonstration de la proposition et donc du théorème de Cassels. □

3.4. Conséquence des formules de Cassels. — Nous conservons les notations du théorème de Cassels, et en particulier p et q sont des nombres premiers *impairs et distincts*. Comme pour le théorème de Fermat nous allons maintenant factoriser l'équation de Catalan dans le corps cyclotomique $K = \mathbb{Q}(\zeta)$, où $\zeta = \zeta_p$ est une racine primitive p-ième de l'unité. Rappelons que dans ce contexte on a $\mathbb{Z}_K = \mathbb{Z}[\zeta]$, et que $\mathfrak{p} = (1-\zeta)\mathbb{Z}_K$ est l'unique idéal premier divisant p, et qu'on a $\mathfrak{p}^{p-1} = p\mathbb{Z}_K$. Enfin, soient x et y des entiers non nuls tels que $x^p - y^q = 1$.

Lemme 3.8. — *Pour tout i tel que $1 \leqslant i \leqslant p-1$ posons $\beta_i = (x-\zeta^i)/(1-\zeta^i)$. Alors les β_i sont des entiers algébriques non divisibles par $\mathfrak{p}$, et les idéaux principaux qu'ils engendrent sont premiers entre eux deux à deux et égaux à des puissances q-ièmes d'idéaux.*

Démonstration. — D'après le théorème de Cassels on a $p \mid (x-1)$, donc $v_{\mathfrak{p}}(x-1) \geqslant p-1 \geqslant 2$, et donc $v_{\mathfrak{p}}(\beta_i - 1) = v_{\mathfrak{p}}(x-1) - v_{\mathfrak{p}}(1-\zeta^i) \geqslant 1$. Il en résulte que $v_{\mathfrak{p}}(\beta_i) = 0$, et puisque $(1-\zeta^i)\mathbb{Z}_K = \mathfrak{p}$, on voit que β_i est un entier algébrique premier à $\mathfrak{p}$. De plus, $(1-\zeta^i)\beta_i - (1-\zeta^j)\beta_j = \zeta^j - \zeta^i$, et puisque $(\zeta^j - \zeta^i)\mathbb{Z}_K = \mathfrak{p}$ pour tout $i \not\equiv j \pmod{p}$ il en résulte que pour $1 \leqslant i \neq j \leqslant p-1$ les idéaux $\beta_i\mathbb{Z}_K$ et $\beta_j\mathbb{Z}_K$ sont premiers entre eux. Enfin, en utilisant l'identité polynomiale $\prod_{1\leqslant i\leqslant p-1}(X-\zeta^i) = (X^p-1)/(X-1)$ et le théorème de Cassels on a

$$\prod_{1\leqslant i\leqslant p-1} \beta_i = \frac{\prod_{1\leqslant i\leqslant p-1}(x-\zeta^i)}{\prod_{1\leqslant i\leqslant p-1}(1-\zeta^i)} = \frac{x^p-1}{p(x-1)} = v^q$$

pour un $v \in \mathbb{Z}_{>0}$. Puisque les $\beta_i\mathbb{Z}_K$ sont premiers entre eux deux à deux, il en résulte que chacun d'eux est individuellement la q-ième puissance d'un idéal. □

Pour simplifier, dans la suite nous poserons $\beta = \beta_1 = (x-\zeta)/(1-\zeta)$, et donc il existe un idéal $\mathfrak{b}$ tel que $\beta\mathbb{Z}_K = \mathfrak{b}^q$.

Nous pourrions maintenant continuer la démonstration d'une manière similaire à celle que nous avons utilisée pour le théorème de Fermat : si on suppose que q ne divise pas le nombre de classes $h_p = |\operatorname{Cl}(K)|$ de K, on déduit de ce que nous venons de montrer que l'idéal $\mathfrak{b}$ est principal, et donc qu'il existe $\gamma \in \mathbb{Z}_K$ et une unité u tels que $(x-\zeta)/(1-\zeta) = u\gamma^q$. En continuant de cette manière on

arrive effectivement ainsi à un théorème, dû à Inkeri, qui affirme que, si $q \nmid h_p$ et si $p^{q-1} \not\equiv 1 \pmod{q^2}$, alors l'équation $x^p - y^q = 1$ n'a pas de solutions non triviales.

Ceci est un résultat très similaire à celui de Kummer énoncé pour le théorème de Fermat. Les conditions d'Inkeri sont peu restrictives mais, comme pour Fermat, il est peu probable qu'elles puissent conduire (du moins directement) à une démonstration complète de la conjecture de Catalan.

L'idée fondamentale de Mihăilescu est de reconsidérer la démonstration ci-dessus : la seule raison pour laquelle nous avons introduit le nombre de classes de K a été pour « tuer » l'obstruction à la principalité des idéaux, grâce à la remarque triviale que $\mathfrak{a}^h$ est principal pour tout idéal $\mathfrak{a}$. Il n'y a toutefois pas de raison de n'utiliser que cet annulateur du groupe de classes : en effet, un remarquable (mais assez ancien, puisqu'il date de 1890) théorème dû à Stickelberger donne un annulateur plus « fin ». C'est celui-ci que Mihăilescu utilise de manière fondamentale, et qui conduit à des résultats bien meilleurs. En particulier, les restrictions sur le nombre de classes disparaissent complètement.

La démonstration du théorème de Stickelberger nécessite de nombreux préparatifs, auxquels nous consacrons les paragraphes qui suivent. La théorie est de toutes façons intéressante en elle-même, indépendamment de ses applications.

4. Sommes de Gauss

4.1. Définitions et propriétés de base. — Soit $\mathbb{F}_Q$ un corps fini de caractéristique q, donc ayant $Q = q^f$ éléments pour un certain entier $f = [\mathbb{F}_Q : \mathbb{F}_q]$.

Définition 4.1

(1) On appelle *caractère additif* (resp., multiplicatif) sur $\mathbb{F}_Q$ tout homomorphisme de groupes du groupe additif $\mathbb{F}_Q$ (resp., du groupe multiplicatif $\mathbb{F}_Q^*$) dans le groupe multiplicatif $\mathbb{C}^*$.

(2) Si ψ est un caractère additif et χ un caractère multiplicatif, on appelle *somme de Gauss* associée à ces deux caractères le nombre

complexe

$$\tau(\chi,\psi)=\sum_{x\in\mathbb{F}_Q^*}\chi(x)\psi(x).$$

Puisque $\mathbb{F}_Q$ est isomorphe à $(\mathbb{Z}/q\mathbb{Z})^f$ en tant que groupe additif, il est clair qu'un caractère additif est à valeurs dans les racines q-ièmes de l'unité et un caractère multiplicatif est clairement à valeurs dans les racines $(Q-1)$-ièmes de l'unité.

Nous dirons qu'un caractère est *trivial* si son image est réduite à 1, et nous supposerons *toujours* implicitement par la suite que les caractères additifs ψ sont non triviaux. Par contre, il sera nécessaire de considérer des caractères multiplicatifs triviaux.

Les sommes de Gauss possèdent des propriétés tout à fait remarquables. Comme ce sont des sommes finies, la plupart de ces propriétés se démontrent par des manipulations algébriques convenables. Toutefois les plus subtiles d'entre elles n'ont pas de démonstration vraiment « élémentaire ». Les résultats les plus importants dont nous ayons besoin concernent les valuations « archimédiennes » et « $\mathfrak{p}$-adiques » de ces sommes (nous verrons ci-dessous la signification de ces termes).

Proposition 4.2. — *Soit ψ un caractère additif (non trivial) et χ un caractère multiplicatif.*

(1) *Si χ est trivial on a $\tau(\chi,\psi)=-1$.*
(2) *On a $\tau(\chi^{-1},\psi)=\chi(-1)\overline{\tau(\chi,\psi)}$.*
(3) *Si χ est non trivial on a $|\tau(\chi,\psi)|=Q^{1/2}$.*

Démonstration

(1) Si χ est trivial on a

$$\tau(\chi,\psi)=\sum_{x\in\mathbb{F}_Q^*}\psi(x)=-1+\sum_{x\in\mathbb{F}_Q}\psi(x).$$

Or il est bien connu que la somme des valeurs d'un caractère non trivial d'un groupe abélien est nulle : si S désigne la somme ci-dessus et si $a\in\mathbb{F}_Q$ est tel que $\psi(a)\neq 1$, alors comme l'application $x\mapsto x+a$ est une bijection de $\mathbb{F}_Q$ et que ψ est un caractère, on voit que $S=\psi(a)S$ donc que $S=0$.

(2) Puisque $1=\psi(0)=\psi(x)\psi(-x)$ on a $\psi(-x)=\overline{\psi(x)}$ puisque c'est une racine de l'unité. Puisque $\chi^{-1}(x)=\overline{\chi(x)}$ (pour la même

raison) on a

$$\overline{\tau(\chi^{-1},\psi)} = \sum_{x\in\mathbb{F}_Q^*} \chi(x)\overline{\psi(x)} = \sum_{y\in\mathbb{F}_Q^*} \chi(-y)\psi(y) = \chi(-1)\tau(\chi,\psi),$$

ce qui démontre (2).

(3) Posant $z = xy^{-1}$, on a

$$|\tau(\chi,\psi)|^2 = \tau(\chi,\psi)\overline{\tau(\chi,\psi)} = \sum_{x,y\in\mathbb{F}_Q^*} \chi(x)\overline{\chi}(y)\psi(x)\overline{\psi}(y)$$
$$= \sum_{z\in\mathbb{F}_Q^*} \chi(z) \sum_{y\in\mathbb{F}_Q^*} \psi(y(z-1)).$$

Il est clair que $y \mapsto \psi(y(z-1))$ est un caractère additif, qui est non trivial si et seulement si $(z-1) \in \mathbb{F}_Q^*$ (puisque dans ce cas l'application $y \mapsto y(z-1)$ est une bijection de $\mathbb{F}_Q^*$ dans lui-même). Il en résulte comme dans (1) que $\sum_{y\in\mathbb{F}_Q} \psi(y(z-1)) = 0$ quand $z \neq 1$, et donc que

$$|\tau(\chi,\psi)|^2 = \chi(1)(Q-1) + \sum_{z\in\mathbb{F}_Q^*,\ z\neq 1} (-1)\chi(z) = Q - \sum_{z\in\mathbb{F}_Q^*} \chi(z) = Q,$$

utilisant à nouveau le résultat sur la somme des valeurs d'un caractère, mais cette fois-ci appliqué au caractère non trivial χ. □

Une propriété importante et très légèrement plus délicate est la suivante.

Lemme 4.3

(1) *Si χ_1 et χ_2 sont des caractères multiplicatifs d'ordre divisant m alors*

$$\tau(\chi_1,\psi)\tau(\chi_2,\psi)/\tau(\chi_1\chi_2,\psi) \in \mathbb{Q}(\zeta_m).$$

(2) *Si χ est un caractère multiplicatif d'ordre divisant m alors*

$$\tau(\chi,\psi)^m \in \mathbb{Q}(\zeta_m).$$

Démonstration. — Les résultats sont évidents si l'un des caractères qui interviennent est trivial. Sinon, pour (1), un argument combinatoire très simple laissé au lecteur montre que

$$\frac{\tau(\chi_1,\psi)\tau(\chi_2,\psi)}{\tau(\chi_1\chi_2,\psi)} = \sum_{x\neq 0,1} \chi_1(x)\chi_2(x).$$

Pour (2), un argument analogue montre que

$$\tau(\chi,\psi)^m = Q\chi(-1)\sum_{\substack{x_1+\cdots+x_{k-1}=1\\ x_i\neq 0}}\chi(x_1\cdots x_{k-1}).$$

Dans les deux cas le résultat est démontré puisque les valeurs de χ appartiennent à $\mathbb{Q}(\zeta_m)$. □

Les sommes qui apparaissent ci-dessus, et que nous rencontrerons à nouveau, s'appellent des sommes de Jacobi.

4.2. Instanciation des sommes de Gauss. — Pour poursuivre notre étude des sommes de Gauss, il est indispensable de pouvoir préciser les caractères χ et ψ que nous utilisons. Bien qu'*a priori* il n'y ait rien de « canonique », on va voir que l'on peut quand même obtenir ce qu'on veut.

Tout d'abord, comme $\mathbb{F}_Q$ est une $\mathbb{F}_q$-algèbre, la multiplication par $x\in\mathbb{F}_Q$ est une application linéaire de $\mathbb{F}_Q$ dans lui-même, et on peut donc parler de sa trace, appelée trace de x et notée $\mathrm{Tr}(x)$, et de son déterminant, appelé *norme* de x et noté $\mathcal{N}(x)$. La trace et la norme sont donc des éléments de $\mathbb{F}_q$. De fait, il est facile de voir que le polynôme caractéristique de notre application est $\prod_{0\leqslant i<f}(X-x^{q^i})$, et donc en particulier que $\mathrm{Tr}(x)=\sum_{0\leqslant i<f}x^{q^i}$ et que $\mathcal{N}(x)=x^{(Q-1)/(q-1)}$.

Soit ζ_q une racine primitive q-ième de l'unité. Il est évident que l'application $x\mapsto\zeta_q^{\mathrm{Tr}(x)}$ est un caractère additif, étant bien entendu que l'élévation de ζ_q à une puissance un élément de $\mathbb{F}_q$ a bien un sens. Il est un tout petit peu moins évident de voir que ce caractère est non trivial : de fait, le polynôme $T(X)=\sum_{0\leqslant i<f}X^{q^i}$ est de degré q^{f-1}, et donc il existe $a\in\mathbb{F}_Q$ (qui possède q^f éléments) tel que $\mathrm{Tr}(a)=T(a)=c\neq 0$. Il en résulte par $\mathbb{F}_q$-linéarité que $\mathrm{Tr}(a/c)=1$, donc notre caractère est différent de 1 pour $x=a/c$.

Si maintenant $b\in\mathbb{F}_Q$ est quelconque, l'application $x\mapsto\zeta_q^{\mathrm{Tr}(bx)}$ est encore un caractère additif, que nous noterons ψ_b. Le caractère ci-dessus est donc ψ_1. C'est maintenant un exercice très facile que nous laissons au lecteur de voir que l'application $b\mapsto\psi_b$ est un isomorphisme de groupes entre le groupe additif $\mathbb{F}_Q$ et le groupe multiplicatif des caractères additifs de $\mathbb{F}_Q$. En particulier tout caractère additif est de la forme ψ_b pour un unique $b\in\mathbb{F}_Q$.

Nous laissons au lecteur le soin de démontrer les résultats très simples suivants, le deuxième provenant du fait que $\mathrm{Tr}(x^q) = \mathrm{Tr}(x)$.

Lemme 4.4

(1) *On a* $\tau(\chi, \psi_b) = \chi(b)^{-1}\tau(\chi, \psi_1)$.
(2) *On a* $\tau(\chi^q, \psi_b) = \chi^{1-q}(b)\tau(\chi, \psi_b) = \tau(\chi, \psi_{b^{q-1}})$.

Les caractères additifs de $\mathbb{F}_Q$ sont maintenant sous contrôle. Nous devons faire de même pour les caractères multiplicatifs, et c'est légèrement plus délicat. Pour cela nous utiliserons quelques notions supplémentaires très simples sur les corps de nombres.

Considérons le corps $L = \mathbb{Q}(\zeta_q, \zeta_{Q-1})$ obtenu en adjoignant à $\mathbb{Q}$ la racine primitive q-ième de l'unité ζ_q, et une racine primitive $(Q-1)$-ième de l'unité ζ_{Q-1} (en fait $L = \mathbb{Q}(\zeta_{q(Q-1)})$ est un corps cyclotomique, mais nous n'utiliserons pas ce fait). L'une des raisons pour lesquelles on introduit ce corps est que $\tau(\chi, \psi) \in L$ puisque les valeurs de ψ sont dans $\mathbb{Q}(\zeta_q)$ et celles de χ dans $\mathbb{Q}(\zeta_{Q-1})$. Comme on l'a vu ci-dessus dans l'étude du théorème de Fermat (avec q remplacé par p), il existe un unique idéal premier $\mathfrak{q}$ de $K_q = \mathbb{Q}(\zeta_q)$ divisant q, et on a $\mathfrak{q} = (1-\zeta_q)\mathbb{Z}_{K_q}$ et $\mathfrak{q}^{q-1} = q\mathbb{Z}_{K_q}$. Il est facile de montrer (mais nous l'admettrons, cela fait partie des résultats standards sur les corps de nombres) que la décomposition de $\mathfrak{q}\mathbb{Z}_L$ en produit d'idéaux premiers est $\mathfrak{q}\mathbb{Z}_L = \prod_{1\leqslant i\leqslant g}\mathfrak{P}_i$, où les $\mathfrak{P}_i$ sont des idéaux premiers distincts de L tels que $[\mathbb{Z}_L/\mathfrak{P}_i : \mathbb{Z}_{K_q}/\mathfrak{q}] = f$ (rappelons que $Q = q^f$), et $g = \phi(Q-1)/f$, où ϕ est la fonction d'Euler (nous n'aurons pas besoin de g). En particulier, on voit que $\mathbb{Z}_L/\mathfrak{P}_i$ est un corps fini à $Q = q^f$ éléments. Nous allons donc *choisir* (ce n'est bien sûr pas canonique) un idéal premier $\mathfrak{P}$ parmi les $\mathfrak{P}_i$, et *instancier* $\mathbb{F}_Q$ en posant $\mathbb{F}_Q = \mathbb{Z}_L/\mathfrak{P}$. Il sera indispensable de se rappeler que tout ce que nous allons faire à partir de maintenant dépend (un peu) du choix de cet idéal $\mathfrak{P}$.

Lemme 4.5. — *Soit* $\mu_{Q-1} = \{\zeta_{Q-1}^j,\ 0 \leqslant j < Q-1\} \subset L$ *le groupe multiplicatif des racines* $(Q-1)$*-ièmes de l'unité dans* L*. L'application* $u_{\mathfrak{P}}$ *qui envoie* $x \in \mu_{Q-1}$ *sur sa classe modulo* $\mathfrak{P}$ *dans* $\mathbb{F}_Q^* = (\mathbb{Z}_L/\mathfrak{P})^*$ *est un isomorphisme de groupes.*

Démonstration. — Il est clair que c'est un homomorphisme, et puisque μ_{Q-1} et $\mathbb{F}_Q^*$ ont le même nombre d'éléments il suffit de

montrer que son noyau est trivial. Or on a

$$\prod_{1\leqslant k\leqslant Q-2}(x-\zeta_{Q-1}^k)=\frac{x^{Q-1}-1}{x-1},$$

donc $\prod_{1\leqslant k\leqslant Q-2}(1-\zeta_{Q-1}^k)=Q-1$. Mais $u_{\mathfrak{P}}(\zeta_{Q-1}^k)=1$ signifie que $\mathfrak{P}\mid(\zeta_{Q-1}^k-1)$, donc si $1\leqslant k\leqslant Q-2$ ceci implique que $\mathfrak{P}\mid(Q-1)$, ce qui est absurde puisque $\mathfrak{P}\mid q$ et q est premier à $Q-1=q^f-1$. □

Définition 4.6. — On définit $\omega_{\mathfrak{P}}$ comme étant l'isomorphisme réciproque $u_{\mathfrak{P}}^{-1}$, en d'autres termes comme l'unique isomorphisme de groupes de $\mathbb{F}_Q^*=(\mathbb{Z}_L/\mathfrak{P})^*$ sur μ_{Q-1} tel que $\omega_{\mathfrak{P}}(x)\equiv x \pmod{\mathfrak{P}}$.

Il est clair que $\omega_{\mathfrak{P}}$ est un caractère multiplicatif de $\mathbb{F}_Q$ d'ordre exactement égal à $Q-1$ puisque c'est un isomorphisme. Comme $\mathbb{F}_Q^*$ est un groupe cyclique d'ordre $Q-1$, et donc son groupe de caractères également, il en résulte que tout caractère multiplicatif χ de $\mathbb{F}_Q$ est de la forme $\omega_{\mathfrak{P}}^{-r}$ pour un unique entier r défini modulo $Q-1$ (on inclut un signe $-$ pour simplifier certaines formules).

En résumé toute somme de Gauss sur $\mathbb{F}_Q$ est de la forme $\tau(\omega_{\mathfrak{P}}^{-r},\psi_b)$ pour un unique $r\in\mathbb{Z}/(Q-1)\mathbb{Z}$ et un unique $b\in\mathbb{F}_Q$. Ceci ne dépend donc maintenant que du triplet $(\mathfrak{P},r,b)$ et nous avons fini l'instanciation des sommes de Gauss. En fait, puisque d'après le lemme ci-dessus on a $\tau(\omega_{\mathfrak{P}}^{-r},\psi_b)=\omega_{\mathfrak{P}}^r(b)\tau(\omega_{\mathfrak{P}}^{-r},\psi_1)$, on pourra donc toujours se ramener au cas $b=1$, et dans ce cas nous omettrons d'indiquer ψ_1 dans la notation. Il est également très facile de voir la dépendance en $\mathfrak{P}$. En effet, la théorie de Galois très simple montre que tous les $\mathfrak{P}_i$ sont de la forme $\sigma(\mathfrak{P})$ pour $\sigma\in\mathrm{Gal}(L/K_q)$, et on montre alors aisément le lemme suivant, dont la démonstration est laissée au lecteur :

Lemme 4.7

(1) *Pour tout* $\sigma\in\mathrm{Gal}(L/\mathbb{Q})$ *on a*

$$\omega_{\sigma(\mathfrak{P})}=\sigma\circ\omega_{\mathfrak{P}}\circ\sigma^{-1}.$$

(2) *Pour tout* $\sigma\in\mathrm{Gal}(L/\mathbb{Q})$ *et tout* $r\in\mathbb{Z}$ *on a*

$$\tau(\omega_{\sigma(\mathfrak{P})}^{-r})=\sigma(\tau(\omega_{\mathfrak{P}}^{-r})).$$

L'argument véritablement important est donc r.

Lemme 4.8. — *Soit p un diviseur premier de $Q-1$ et $d=(Q-1)/p$. Le nombre $\tau(\omega_{\mathfrak{P}}^{-d})^p$ appartient à $K=\mathbb{Q}(\zeta_p)$ et ne dépend que de l'idéal premier de K en dessous de $\mathfrak{P}$, et non de $\mathfrak{P}$ lui-même.*

Démonstration. — D'après le lemme 4.3 nous savons que $\tau(\omega_{\mathfrak{P}}^{-d})^p \in K$. Si $\mathfrak{P}_1$ est un autre idéal premier de L au-dessus du même idéal premier $\mathfrak{q}$ de K en dessous de $\mathfrak{P}$, par la théorie de Galois il existe $\sigma \in \mathrm{Gal}(L/K)$ tel que $\mathfrak{P}_1 = \sigma(\mathfrak{P})$. Il résulte du lemme ci-dessus que $\tau(\omega_{\mathfrak{P}_1}^{-d})^p = \sigma(\tau(\omega_{\mathfrak{P}}^{-d})^p)$. Puisque par définition σ laisse K invariant, il n'agit pas sur les valeurs des caractères multiplicatifs, mais seulement sur les caractères additifs. Il en résulte que pour un certain a premier à q (déterminé par σ) on a

$$\sigma(\tau(\omega_{\mathfrak{P}}^{-d})^p) = \tau(\omega_{\mathfrak{P}}^{-d}, \psi_a)^p = (\omega_{\mathfrak{P}}(a)^d \tau(\omega_{\mathfrak{P}}^{-d}))^p = \tau(\omega_{\mathfrak{P}}^{-d})^p,$$

puisque $\omega_{\mathfrak{P}}(a)$ est une racine $(Q-1)$-ième de l'unité. □

4.3. Le théorème de Stickelberger. — Nous pouvons enfin démontrer le premier théorème de Stickelberger.

Définition 4.9. — On définit la fonction arithmétique $s(r)$ de la manière suivante. Quand $0 \leqslant r < Q-1$, on pose $s(r) = \sum_{0 \leqslant j \leqslant f-1} r_j$, où $r = \sum_{0 \leqslant j \leqslant f-1} r_j q^j$ est l'écriture habituelle de r en base q, avec $0 \leqslant r_j \leqslant q-1$. Pour un $r \in \mathbb{Z}$ quelconque on pose $s(r) = s(r \bmod (Q-1))$, où $r \bmod (Q-1)$ désigne le reste de la division euclidienne de r par $Q-1$.

***Théorème 4.10* (Stickelberger).** — *Pour tout caractère additif non trivial ψ on a*

$$v_{\mathfrak{P}}(\tau(\omega_{\mathfrak{P}}^{-r}, \psi)) = s(r).$$

Démonstration. — Posons $v(r) = v_{\mathfrak{P}}(\tau(\omega_{\mathfrak{P}}^{-r}))$. On a le lemme suivant.

Lemme 4.11

(1) $v(0) = 0$.
(2) $v(a+b) \equiv v(a) + v(b) \pmod{q-1}$.
(3) $v(qa) = v(a)$.
(4) $\sum_{1 \leqslant a \leqslant Q-2} v(a) = f(q-1)(Q-2)/2$.

Démonstration. — Tout ceci est très facile : (1) est trivial, (2) résulte du lemme 4.3, (3) résulte également de ce lemme puisque si $x \in K$ on a $v_{\mathfrak{P}}(x) = (q-1)v_{\mathfrak{q}}(x)$, où $\mathfrak{q}$ est l'idéal de K en dessous de $\mathfrak{P}$, (4) résulte du lemme 4.4 (2). Enfin, d'après le résultat sur le module des sommes de Gauss (proposition 4.2) on vérifie que $v(a)+v(Q-1-a) = v_{\mathfrak{P}}(Q) = (q-1)f$. En regroupant les termes de la somme deux par deux on en déduit (5). □

Le résultat vraiment crucial est la deuxième assertion du lemme suivant.

Lemme 4.12. — *Si $r \not\equiv 0 \pmod{Q-1}$ on a $v(r) > 0$, et d'autre part $v(1) = 1$.*

Démonstration. — Notons que $\pi_q = 1 - \zeta_q$ engendre l'unique idéal premier divisant q dans $\mathbb{Q}(\zeta_q)$, qui divise donc nécessairement $\mathfrak{P}$, donc $\pi_q \in \mathfrak{P}$. Il en résulte que

$$\tau(\omega_{\mathfrak{P}}^{-r}, \psi_1) = \sum_{x \in \mathbb{F}_Q^*} \omega_{\mathfrak{P}}^{-r}(x)\zeta_q^{\mathrm{Tr}(x)} \equiv \sum_{x \in \mathbb{F}_Q^*} \omega_{\mathfrak{P}}^{-r}(x) \equiv 0 \pmod{\mathfrak{P}}$$

puisque la somme des valeurs d'un caractère non trivial est nulle, et donc $v(r) > 0$. D'autre part, par la formule du binôme

$$\begin{aligned}\tau(\omega_{\mathfrak{P}}^{-1}, \psi_1) &= \sum_{x \in \mathbb{F}_Q^*} \omega_{\mathfrak{P}}^{-1}(x)(1-\pi_q)^{\mathrm{Tr}(x)} \equiv \sum_{x \in \mathbb{F}_Q^*} \omega_{\mathfrak{P}}^{-1}(x)(1-\pi_q \,\mathrm{Tr}(x)) \\ &\equiv -\pi_q \sum_{x \in \mathbb{F}_Q^*} \omega_{\mathfrak{P}}^{-1}(x)\,\mathrm{Tr}(x) \pmod{\mathfrak{P}^2}.\end{aligned}$$

Or nous avons mentionné que $\mathrm{Tr}(x) = \sum_{0 \leqslant j \leqslant f-1} x^{q^j}$, où x est vu comme un élément de $\mathbb{F}_Q = \mathbb{Z}_L/\mathfrak{P}$. On a donc par définition de $\omega_{\mathfrak{P}}$

$$\sum_{x \in \mathbb{F}_Q^*} \omega_{\mathfrak{P}}^{-1}(x)\,\mathrm{Tr}(x) \equiv \sum_{\substack{y \in \mathbb{Z}_L \smallsetminus \mathfrak{P} \\ y \bmod \mathfrak{P}}} y^{-1}(y + y^q + \cdots + y^{q^{f-1}}) \pmod{\mathfrak{P}}.$$

Mais il est classique et facile de démontrer que $\sum_{x \in \mathbb{F}_Q^*} x^m = 0$ (dans $\mathbb{F}_Q$) pour $1 \leqslant m < Q-1$, et est égal à -1 si $m = 0$. Il en résulte que

$$\sum_{x \in \mathbb{F}_Q^*} \omega_{\mathfrak{P}}^{-1}(x)\,\mathrm{Tr}(x) \equiv -1 \pmod{\mathfrak{P}},$$

ce qui démontre que $\tau(\omega_{\mathfrak{P}}^{-1}(x), \psi_1) \equiv \pi_q \pmod{\mathfrak{P}^2}$, et puisque $v_{\mathfrak{P}}(\pi_q) = 1$, que $v(1) = 1$. □

Il est maintenant facile de terminer la démonstration du théorème de Stickelberger.

Démonstration du théorème de Stickelberger. — Nous pouvons bien entendu supposer que $\psi = \psi_1$, et par périodicité que $0 \leqslant r < Q-1$. D'après le lemme ci-dessus combiné avec les résultats (1), (2) et (3) du lemme 4.11, il est clair que $v(r) = r = s(r)$ pour $0 \leqslant r \leqslant q-2$. Si $Q = q$, c'est-à-dire $f = 1$, c'est terminé. Sinon on a $v(q-1) > 0$ d'après le lemme ci-dessus, et on en déduit de même que $v(q-1) = q-1$. Les assertions (2) et (4) du lemme 4.11 entraînent évidemment que $v(r) \leqslant s(r)$. Quand r parcourt l'ensemble des entiers de l'intervalle $[0, Q-1]$, chaque coefficient du développement en base q prend chacune des valeurs de 0 à $q-1$ exactement q^{f-1} fois, et donc

$$\sum_{0 \leqslant r \leqslant Q-1} s(r) = f q^{f-1} \frac{q(q-1)}{2} = fQ(q-1)/2.$$

Comme $s(Q-1) = (q-1)f$ on a donc

$$\sum_{0 \leqslant r \leqslant Q-2} s(r) = f(q-1)(Q-2)/2 = \sum_{0 \leqslant r \leqslant Q-2} v(r)$$

d'après (5) du lemme 4.11 et, puisque $v(r) \leqslant s(r)$ pour tout r, on a donc $v(r) = s(r)$. □

Corollaire 4.13. — *Soit p un diviseur premier de $Q-1$, posons $d = (Q-1)/p$, et soit $\mathfrak{P}_p$ un idéal premier de $L_p = \mathbb{Q}(\zeta_q, \zeta_p) \subset L$ en dessous de $\mathfrak{P}$ (et donc au-dessus de q). Pour tout r on a $v_{\mathfrak{P}_p}(\tau(\omega_{\mathfrak{P}}^{-rd})) = s(rd)$.*

Démonstration. — C'est clair, puisque $\tau(\omega_{\mathfrak{P}}^{-rd}) \in L_p$ et que $v_{\mathfrak{P}}(\mathfrak{P}_p) = 1$ comme on le voit aisément. □

Maintenant que nous avons calculé la valuation de la somme de Gauss $\tau(\omega_{\mathfrak{P}}^{-rd})$ pour l'idéal premier $\mathfrak{P}_d$ lui-même, il est très facile de le faire pour les autres idéaux premiers. Le résultat est le suivant :

Corollaire 4.14. — *Gardons les mêmes hypothèses que le corollaire précédent. Pour t premier à p, soit $\sigma_t \in \mathrm{Gal}(L_p/\mathbb{Q})$ l'automorphisme de L_p laissant $\mathbb{Q}$ et ζ_q invariant, et envoyant ζ_p sur ζ_p^t. On a*

$$v_{\sigma_t^{-1}(\mathfrak{P}_p)}(\tau(\omega^{-rd})) = s(rtd).$$

Démonstration. — Résulte immédiatement du lemme 4.7 et laissé au lecteur. □

Remarque. — Dans les énoncés ci-dessus nous avons toujours utilisé un diviseur *premier* p de $Q-1$, car c'est dans ce contexte que nous en aurons besoin, mais bien entendu les résultats sont vrais en toute généralité.

4.4. Réinterprétation en termes de théorie de Galois

Nous commençons par réinterpréter le résultat ci-dessus en termes de théorie de Galois.

Proposition 4.15. — *Gardons toutes les notations ci-dessus. Alors*

$$\tau(\omega_{\mathfrak{P}}^{-rd})\mathbb{Z}_{L_p} = \prod_{t\in(\mathbb{Z}/p\mathbb{Z})^*/\langle q\rangle} \sigma_t^{-1}(\mathfrak{P}_p)^{s(rtd)},$$

où $\langle q\rangle$ désigne le sous-groupe engendré par (la classe de) q.

Démonstration. — Il est clair que $\tau(\omega_{\mathfrak{P}}^{-rd}) \in \mathbb{Z}_{L_p}$, donc l'idéal principal du membre de gauche a bien un sens. Un raisonnement très simple de théorie de Galois montre que les idéaux de L_p au-dessus de l'unique idéal premier $\mathfrak{q}$ de $\mathbb{Q}(\zeta_q)$ au-dessus de q sont obtenus une fois et une seule comme $\sigma_t^{-1}(\mathfrak{P}_p)$ pour $\sigma_t \in \mathrm{Gal}(L_p/\mathbb{Q}(\zeta_q))/H$, où H est le sous-groupe des $\sigma_t \in \mathrm{Gal}(L_p/\mathbb{Q}(\zeta_q))$ tel que $\sigma_t(\mathfrak{P}_p) = \mathfrak{P}_p$. Dans l'isomorphisme canonique $\mathrm{Gal}(L_p/\mathbb{Q}(\zeta_q)) \simeq (\mathbb{Z}/p\mathbb{Z})^*$ il est facile de voir que le sous-groupe H correspond aux classes modulo p des puissances de q, donc $\mathrm{Gal}(L_p/\mathbb{Q}(\zeta_q))/H \simeq (\mathbb{Z}/p\mathbb{Z})^*/\langle q\rangle$. Enfin, remarquons que puisque $|\tau(\omega_{\mathfrak{P}}^{-rd})|^2 = Q = q^f$, les seuls idéaux premiers pouvant diviser $\tau(\omega_{\mathfrak{P}}^{-rd})$ sont ceux au-dessus de q, et la proposition est donc démontrée. □

Corollaire 4.16. — *Gardons les mêmes hypothèses, et en particulier soit $\mathfrak{q}$ l'idéal premier de K en dessous de $\mathfrak{P}$ (et donc au-dessus de q). On a*

$$\tau(\omega_{\mathfrak{P}}^{-d})^p\mathbb{Z}_K = \prod_{t\in(\mathbb{Z}/p\mathbb{Z})^*/\langle q\rangle} \sigma_t^{-1}(\mathfrak{q})^{v_t}, \quad \text{où}$$

$$v_t = \frac{p}{q-1}s\left(t\frac{Q-1}{p}\right) = p\sum_{0\leqslant i<f}\left\{\frac{q^i t}{p}\right\}.$$

Démonstration. — D'après le lemme 4.3 nous savons que $\tau(\omega_{\mathfrak{P}}^{-d})^p \in K$. Puisque $v_{\mathfrak{P}_p}(\mathfrak{q}) = q-1$ on a

$$v_{\mathfrak{q}}(\tau(\omega_{\mathfrak{P}}^{-d})^p) = (p/(q-1))v_{\mathfrak{P}_p}(\tau(\omega_{\mathfrak{P}_p}^{-d})),$$

et nous obtenons donc la formule du corollaire avec la première expression pour v_t. La seconde formule pour v_t est un exercice facile sur les développements en base q et laissée au lecteur. □

4.5. L'élément de Stickelberger. — Il va être indispensable de reformuler le théorème de Stickelberger en termes d'algèbres de groupes. Définissons cette notion, dans le contexte des groupes abéliens puisque ce sera le seul considéré.

Définition 4.17. — Soit G un groupe abélien et A un anneau (commutatif unitaire). On appelle *algèbre de groupe* de G sur A et on note $A[G]$ l'ensemble des combinaisons linéaires formelles finies $\alpha = \sum_{g\in G} n_g g$ avec $n_g \in A$, muni de l'addition en tant que A-module, et de la multiplication induite par la loi de groupe sur G.

En d'autres termes, $\sum_g n_g g + \sum_g m_g g = \sum_g (n_g+m_g)g$ et

$$\Big(\sum_g n_g g\Big)\Big(\sum_h m_h h\Big) = \sum_g \sum_h n_g m_h (gh) = \sum_g \Big(\sum_h n_h m_{gh^{-1}}\Big) g.$$

En particulier $\mathbb{Z}[G]$ s'appelera *l'anneau de groupes* associé à G.

Proposition 4.18. — *Soit G un groupe abélien et E un ensemble sur lequel G opère. Alors E possède une structure naturelle de $\mathbb{Z}[G]$-module.*

Si $x \in E$ et $\alpha \in \mathbb{Z}[G]$, on a coutume d'écrire l'action de α sur x sous forme *exponentielle*, c'est-à-dire sous la forme x^α. L'intérêt est que $x^{\alpha\beta} = (x^\alpha)^\beta$. Notons au passage que la proposition ci-dessus n'a plus de sens si on remplace $\mathbb{Z}[G]$ par $\mathbb{Q}[G]$ par exemple.

Pour la conjecture de Catalan nous utiliserons principalement le groupe $G = \mathrm{Gal}(K/\mathbb{Q})$. Rappelons que les éléments de G sont les automorphismes σ_t pour $1 \leqslant t \leqslant p-1$ laissant invariant $\mathbb{Q}$ et tels que $\sigma_t(\zeta) = \zeta^t$. En particulier G est canoniquement isomorphe à $(\mathbb{Z}/p\mathbb{Z})^*$. Le groupe G opère naturellement sur à peu près tout ce qu'on peut considérer : éléments, idéaux, classes d'idéaux, unités, racines de l'unité, etc.

Dans le langage de l'anneau de groupe, regardons quelques annulateurs évidents du groupe des classes $\mathrm{Cl}(K)$. Rappelons que par définition l'annulateur $I = \mathrm{Ann}_{\mathbb{Z}[G]}(/\,\mathrm{Cl}(K))$ de $\mathrm{Cl}(K)$ est l'ensemble des éléments $\alpha \in \mathbb{Z}[G]$ tels que $\alpha\,\mathrm{Cl}(K) = 1$, en d'autres termes tels que $\alpha(\overline{\mathfrak{a}}) = 1$ pour toute classe $\overline{\mathfrak{a}}$, en désignant par 1 la classe triviale. C'est évidemment un idéal de $\mathbb{Z}[G]$. Tout d'abord si $h(K)$ est le nombre de classes on a $\overline{\mathfrak{a}}^{h(K)} = 1$, donc $h(K)\mathbb{Z}[G] \subset I$. D'autre part, $\mathcal{N}(\mathfrak{a})$ est un idéal de $\mathbb{Z}$, donc est principal. Il en résulte que si on pose par abus de notation $\mathcal{N} = \sum_{t\in(\mathbb{Z}/p\mathbb{Z})^*} \sigma_t$ on a aussi $\mathcal{N} \in I$ (donc $\mathcal{N}\mathbb{Z}[G] \in I$). Les résultats ci-dessus sont valables pour tout corps de nombres. Nous allons voir que le théorème de Stickelberger entraîne immédiatement que dans le cas d'un corps cyclotomique on peut faire beaucoup mieux. Tout d'abord en termes d'anneau de groupe le corollaire 4.16 peut se réécrire de la manière suivante.

Proposition 4.19. — *Posons*

$$\Theta = \frac{1}{p} \sum_{1\leqslant t\leqslant p-1} t\sigma_t^{-1} \in \mathbb{Q}[G].$$

Avec les mêmes notations que ci-dessus on a

$$\tau(\omega_{\mathfrak{P}}^{-d})^p\mathbb{Z}_K = \mathfrak{q}^{p\Theta}.$$

Démonstration. — C'est uniquement une question d'interprétation des définitions. Soit T un système de représentants de $(\mathbb{Z}/p\mathbb{Z})^*$ modulo le sous-groupe engendré par q. On peut reformuler le corollaire 4.16 en disant que $\tau(\omega_{\mathfrak{P}}^{-d})^p\mathbb{Z}_K = \mathfrak{q}^{p\theta}$, où

$$\theta = \sum_{t\in T} \sum_{0\leqslant i<f} \{q^i t/p\}\sigma_t^{-1}$$

(noter que cela n'aurait aucun sens de remplacer T par $(\mathbb{Z}/p\mathbb{Z})^*/\langle q\rangle$ dans l'expression ci-dessus car σ_t ne serait pas défini). Par définition, quand t parcourt T et i va de 0 à $f-1$ les éléments $q^i t$ modulo p parcourent $(\mathbb{Z}/p\mathbb{Z})^*$, donc

$$\theta = \sum_{t\in(\mathbb{Z}/p\mathbb{Z})^*} \{t/p\}\sigma_{t_1}^{-1},$$

où t_1 est le représentant de la classe de t dans T. D'autre part il est facile de montrer que le sous-groupe des éléments de $\mathrm{Gal}(K/\mathbb{Q})$

laissant $\mathfrak{q}$ fixe est le sous-groupe cyclique engendré par σ_q, et il en résulte donc que $\mathfrak{q}^{p\theta} = \mathfrak{q}^{p\Theta}$, où Θ est comme indiqué. □

L'élément $\Theta \in \mathbb{Q}[G]$ s'appelle *l'élément de Stickelberger*.

Grâce à la proposition ci-dessus, nous pouvons maintenant donner un élément de l'annulateur de $\mathrm{Cl}(K)$ beaucoup moins trivial que ceux que nous avons donné ci-dessus. Toutefois nous verrons au paragraphe suivant que l'on peut faire *encore* mieux.

***Théorème 4.20* (Stickelberger).** — *L'élément $p\Theta$ appartient à l'annulateur I du groupe des classes d'idéaux de K, en d'autres termes pour tout idéal $\mathfrak{a}$ de K l'idéal $\mathfrak{a}^{p\Theta}$ est un idéal principal.*

Démonstration. — D'après une version du théorème chinois, il n'est pas difficile de montrer que pour tout idéal $\mathfrak{a}$ il existe un élément $\beta \in K$ tel que l'idéal $\beta\mathfrak{a}$ soit premier à p. Il suffit donc de démontrer le résultat pour un idéal $\mathfrak{a}$ premier à p. D'autre part puisque tout idéal est un produit de puissances d'idéaux premiers, par multiplicativité il suffit de démontrer le résultat quand $\mathfrak{a} = \mathfrak{q}$ est un idéal premier distinct de $\mathfrak{p}$, donc divisant un nombre premier q distinct de p. Nous avons déjà mentionné que $Q = \mathcal{N}(\mathfrak{q}) = q^f$, où $f = [\mathbb{Z}_K/\mathfrak{q} : \mathbb{Z}/q\mathbb{Z}]$. J'affirme que $Q \equiv 1 \pmod{p}$. En effet, considérons $\zeta \in \mathbb{Z}_K$. Comme $\zeta^p = 1$, la classe de ζ dans $(\mathbb{Z}_K/\mathfrak{q})^*$ est d'ordre 1 ou p, et comme on ne peut pas avoir $\zeta \equiv 1 \pmod{\mathfrak{q}}$ (sinon $\mathcal{N}(\mathfrak{q}) \mid \mathcal{N}(1-\zeta) = p$ ce qui est exclu puisque $q \neq p$) la classe de ζ est d'ordre p. Comme le cardinal du groupe $(\mathbb{Z}_K/\mathfrak{q})^*$ est par définition égal à $Q-1$ il en résulte que $p \mid (Q-1)$, donc que $Q \equiv 1 \pmod{p}$ comme annoncé (en fait il est facile de montrer que f est le plus petit entier strictement positif tel que $q^f \equiv 1 \pmod{p}$, mais nous n'en aurons pas besoin). Puisque $p \mid (Q-1)$ nous pouvons appliquer toute la technologie que nous avons développée jusqu'ici. En particulier la proposition 4.19 montre bien que $\mathfrak{q}^{p\Theta} = \alpha\mathbb{Z}_K$ est un idéal principal, avec $\alpha = \tau(\omega_{\mathfrak{P}}^{-d})^p \in \mathbb{Z}_K$ d'après le lemme 4.3. □

4.6. L'idéal de Stickelberger. — Les développements ci-dessus sont tout à fait remarquables, puisqu'il est loin d'être trivial que $p\Theta$ soit un annulateur. Toutefois, on peut tirer encore plus d'informations de ce fait. En effet, la présence du facteur p dans $p\Theta$ présente de nombreux inconvénients, et on aimerait bien s'en débarrasser. Bien

évidemment il serait absurde de vouloir que $\Theta \in I$ puisque Θ n'est pas à coefficients entiers et $\mathbb{Q}[G]$ n'opère pas sur le groupe de classes en général. Toutefois, on va faire du mieux que l'on peut : puisque l'annulateur est un idéal, il est raisonnable de considérer les éléments de $\Theta\mathbb{Z}[G]$ pour lesquels on a une action naturelle sur le groupe de classes, c'est-à-dire tout simplement $\Theta\mathbb{Z}[G] \cap \mathbb{Z}[G]$. Il est évident que c'est un idéal de $\mathbb{Z}[G]$, appelé *idéal de Stickelberger* et noté I_s.

Définition 4.21. — Si b est un entier non divisible par p on définit $\Theta_b = (\sigma_b - b)\Theta \in \mathbb{Q}[G]$.

Les résultats qui suivent se démontent de manière combinatoire et simple, et donc leur démonstration est laissée au lecteur.

Proposition 4.22

(1) *On a $\Theta_b \in I_s$, et plus précisément*

$$\Theta_b = -\sum_{1 \leqslant t \leqslant p-1} \left\lfloor \frac{bt}{p} \right\rfloor \sigma_t^{-1},$$

où $\lfloor x \rfloor$ désigne le plus grand entier inférieur ou égal à x.

(2) *L'idéal I_s de $\mathbb{Z}[G]$ est engendré comme $\mathbb{Z}$-module (et donc a fortiori comme $\mathbb{Z}[G]$-module) par les Θ_b pour $1 \leqslant b \leqslant p-1$ ainsi que par Θ_{p+1}.*

Le lemme essentiel qui va conduire au renforcement du théorème de Stickelberger est le suivant :

Lemme 4.23. — *Pour tout b non divisible par p on a*

$$\tau(\omega_{\mathfrak{P}}^{-d})^{\sigma_b - b} \in K.$$

Démonstration. — Rappelons que $L_p = \mathbb{Q}(\zeta_q, \zeta_p)$ et $K = \mathbb{Q}(\zeta_p)$. Puisque p et q sont premiers entre eux le groupe de Galois $\mathrm{Gal}(L_p/K)$ est le groupe cyclique d'ordre $q-1$ formé des automorphismes α_k tels que $\alpha_k(\zeta_q) = \zeta_q^k$ et $\alpha_k(\zeta_p) = \zeta_p$ pour $k \in (\mathbb{Z}/q\mathbb{Z})^*$ (noter qu'on ne peut pas utiliser la notation σ_k qui est réservée aux éléments de $\mathrm{Gal}(L/K_q)$, donc qui fixent ζ_q). D'après la théorie de Galois, pour montrer le lemme nous devons montrer que le membre de gauche est invariant par tous les α_k. Puisque $\omega_{\mathfrak{P}}^{-d}$ est d'ordre p et le caractère

additif implicite ψ_1 est d'ordre q nous avons, en utilisant les propriétés élémentaires des sommes de Gauss données au début

$$\alpha_k(\tau(\omega_{\mathfrak{P}}^{-d})) = \tau(\omega_{\mathfrak{P}}^{-d}, \psi_k) = \omega_{\mathfrak{P}}(k)^d \tau(\omega_{\mathfrak{P}}^{-d}),$$

et donc, puisque α_k et σ_b commutent

$$\alpha_k(\tau(\omega_{\mathfrak{P}}^{-d})^{\sigma_b - b}) = \omega_{\mathfrak{P}}(k)^{d(b-\sigma_b)} \tau(\omega_{\mathfrak{P}}^{-d})^{\sigma_b - b}.$$

Le lemme en résulte puisque $\omega_{\mathfrak{P}}(k)^d$ est une puissance de ζ_p donc $\omega_{\mathfrak{P}}(k)^{d\sigma_b} = \omega_{\mathfrak{P}}(k)^{db}$. □

Il est maintenant facile de démontrer le résultat principal sur l'idéal de Stickelberger, à savoir qu'il est inclus dans l'annulateur I de $\mathrm{Cl}(K)$:

***Théorème 4.24* (Stickelberger).** — *L'idéal de Stickelberger annule le groupe de classes de K, en d'autres termes pour tout $\gamma \in I_s$ et pour tout idéal $\mathfrak{a}$ de K l'idéal $\mathfrak{a}^\gamma$ est principal.*

Démonstration. — Comme dans la démonstration du théorème 4.20 il suffit de montrer que $\mathfrak{q}^\gamma$ est un idéal principal pour tout $\gamma \in I_s$ et tout idéal $\mathfrak{q}$ premier à p. Pour cela, soit b non divisible par p et élevons à la puissance $\sigma_b - b$ l'égalité de la proposition 4.19. On obtient

$$\mathfrak{q}^{p\Theta_b} = \tau(\omega_{\mathfrak{P}}^{-d})^{p(\sigma_b - b)} \mathbb{Z}_K = \alpha^p \mathbb{Z}_K,$$

où $\alpha = \tau(\omega_{\mathfrak{P}}^{-d})^{\sigma_b - b} \in K$ d'après le lemme ci-dessus. Puisque $\mathfrak{q}^{\Theta_b}$ et $\alpha\mathbb{Z}_K$ sont des idéaux de K dont les p-ième puissances sont égales, d'après l'unicité de la décomposition en *idéaux* premiers dans $\mathbb{Z}_K$ on en déduit qu'ils sont égaux. Remarquez la force remarquable de ce raisonnement, qui nous permet de nous débarrasser des facteurs p dans les exposants. Nous en déduisons donc que $\mathfrak{q}^{\Theta_b} = \alpha\mathbb{Z}_K$ est un idéal principal, et comme les Θ_b engendrent I_s il en résulte que $\mathfrak{q}^\gamma$ est aussi un idéal principal pour tout $\gamma \in I_s$. □

Remarque. — Soit $K^+ = K \cap \mathbb{R} = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$ (parmi bien d'autres propriétés) le sous-corps totalement réel maximal de K. La théorie classique des corps cyclotomiques montre que le groupe de classes $\mathrm{Cl}(K)$ est composé en fait de deux morceaux : le groupe de classes $\mathrm{Cl}(K^+)$, et le groupe de classes « relatif », noté $\mathrm{Cl}^-(K)$ et défini comme $\mathrm{Cl}(K)/\mathrm{Cl}(K^+)$ (il faut bien sûr montrer que ceci a un sens, ce que nous ferons ci-dessous). Il est facile de montrer que le théorème de Stickelberger ne donne de renseignements utiles que sur $\mathrm{Cl}^-(K)$. Plus

précisément, l'action d'un élément de I_s sur une classe dans $\mathrm{Cl}(K^+)$ est toujours égale à une puissance de la norme, donc le théorème de Stickelberger est trivial sur cette partie là. Par contre, on peut montrer que I_s est une grosse partie de l'annulateur de $\mathrm{Cl}^-(K)$.

5. Le premier théorème de Mihăilescu : les paires de Wieferich

Après ces très longs préliminaires sur l'idéal de Stickelberger (dont le lecteur paresseux pourra ne retenir que la définition de I_s et le théorème 4.24), nous pouvons enfin revenir à la conjecture de Catalan. Comme nous l'avons mentionné, l'idée fondamentale de Mihăilescu est de ne pas utiliser le fait que le groupe de classes est annulé par $h(K)$, ce qui fait intervenir des conditions difficiles à manier, mais d'utiliser le fait qu'il est annulé par l'idéal de Stickelberger I_s. Noter que le fait que $h(K)$ annule le groupe de classes est une propriété valable pour tout corps de nombres, et peut donc s'utiliser très généralement, alors que l'idéal de Stickelberger ne peut se définir que pour un sous-corps d'un corps cyclotomique (ou de manière équivalente, par un célèbre théorème dû à Kronecker–Weber, pour une extension galoisienne de $\mathbb{Q}$ de groupe de Galois abélien).

Nous reprenons les notations de la conjecture de Catalan. En particulier on rappelle que $x^p - y^q = 1$, que l'on a posé $\beta = (x-\zeta)/(1-\zeta)$ (où nous écrivons à nouveau ζ à la place de ζ_p), et qu'il existe un idéal $\mathfrak{b}$ tel que $\beta\mathbb{Z}_K = \mathfrak{b}^q$. Nous noterons ι la conjugaison complexe, considéré comme un élément du groupe de Galois de $K/\mathbb{Q}$ (nous devons lui donner un nom et ne pas simplement la noter $\overline{\ }$ puisque nous la considérons maintenant comme élément d'un ensemble). Le premier lemme fondamental de Mihăilescu est le suivant.

Lemme 5.1. — *Pour tout $\theta \in (1-\iota)I_s$ l'élément $(x-\zeta)^\theta$ est une puissance q-ième dans K.*

Démonstration. — Écrivons $\theta = (1-\iota)\theta_1$ avec $\theta_1 \in I_s$. Puisque $\beta\mathbb{Z}_K = \mathfrak{b}^q$, d'après le théorème de Stickelberger il existe $\alpha \in K$ tel que $\mathfrak{b}^{\theta_1} = \alpha\mathbb{Z}_K$. Il en résulte que $\alpha^q\mathbb{Z}_K = \mathfrak{b}^{q\theta_1} = \beta^{\theta_1}\mathbb{Z}_K$, et donc il existe une unité $u \in U(K)$ telle que $\beta^{\theta_1} = u\alpha^q$ (noter la ressemblance

de ce raisonnement avec celui utilisé avec $h(K)$). On peut donc écrire

$$(x-\zeta)^\theta = \left(\frac{1-\zeta}{1-\iota(z)}\right)^{\theta_1} \frac{u}{\iota(u)} \left(\frac{\alpha}{\iota(\alpha)}\right)^q.$$

Or $(1-\zeta)/(1-\iota(z)) = -\zeta$, et d'après le corollaire 1.14 (c'est-à-dire essentiellement le théorème de Kronecker) $u/\iota(u)$ est aussi une racine de l'unité. Les deux premiers facteurs sont donc des racines de l'unité dans K, donc des racines $2p$-ièmes de l'unité. Comme q et $2p$ sont premiers entre eux, d'après « Bezout » ce sont des puissances q-ièmes, ce qui démontre le lemme. □

Nous avons aussi besoin d'un lemme totalement élémentaire et complètement indépendant de tout le reste, mais qui est crucial.

Lemme 5.2. — *Soit K un corps de nombres, q un nombre premier, et $\mathfrak{q}$ un idéal premier de $\mathbb{Z}_K$ divisant q. Alors si α et β sont dans $\mathbb{Z}_K$ les trois propriétés suivantes sont équivalentes :*

(1) $\alpha \equiv \beta \pmod{\mathfrak{q}}$.
(2) $\alpha^q \equiv \beta^q \pmod{\mathfrak{q}}$.
(3) $\alpha^q \equiv \beta^q \pmod{\mathfrak{q}^2}$.

Démonstration. — Écrivons $\alpha = \beta + \pi$. D'après la formule du binôme on a donc

$$\alpha^q = \beta^q + \pi^q + \sum_{1 \leqslant i \leqslant q-1} \binom{q}{i} \pi^i \beta^{q-i}.$$

Puisque $q \mid \binom{q}{i}$ pour $1 \leqslant i \leqslant q-1$ et que $\mathfrak{q}$ divise q on en déduit que $\alpha^q \equiv \beta^q + \pi^q \pmod{\mathfrak{q}\pi}$. Il en résulte que si $\alpha^q \equiv \beta^q \pmod{\mathfrak{q}}$ on a $\pi^q \in \mathfrak{q}$, et *comme $\mathfrak{q}$ est un idéal premier* que $\pi \in \mathfrak{q}$, en d'autres termes que $\alpha \equiv \beta \pmod{\mathfrak{q}}$, donc (2) implique (1). D'autre part si $\alpha \equiv \beta \pmod{\mathfrak{q}}$ on a $\pi \in \mathfrak{q}$ donc la même congruence obtenue ci-dessus montre que $\alpha^q \equiv \beta^q + \pi^q \equiv \beta^q \pmod{\mathfrak{q}^2}$, puisque $q \geqslant 2$, donc (1) implique (3), et enfin (3) implique (2) est trivial. □

Corollaire 5.3. — *Supposons que $\mathfrak{q}^2$ ne divise pas l'idéal $q\mathbb{Z}_K$ de $\mathbb{Z}_K$ (on dit alors que q est* non ramifié *dans K). Les propriétés ci-dessus sont alors vraies en remplaçant $\mathfrak{q}$ par $q\mathbb{Z}_K$*

Démonstration. — En effet dans ce cas $q\mathbb{Z}_K$ est un produit d'idéaux premiers *distincts* $\mathfrak{q}_i$, auxquels on peut appliquer le lemme. On en

déduit le résultat par une application directe du théorème chinois pour les idéaux. □

Noter que ce résultat est *faux* en général si q est ramifié.

Après ces préliminaires nous pouvons aisément démontrer le premier résultat de Mihăilescu sur la conjecture de Catalan :

***Théorème 5.4* (Mihăilescu).** — *Si p et q sont des nombres premiers impairs et x et y des entiers non nuls tels que $x^p - y^q = 1$ alors*

$$p^2 \mid y, \quad q^2 \mid x, \quad q^{p-1} \equiv 1 \pmod{p^2} \quad \textit{et} \quad p^{q-1} \equiv 1 \pmod{q^2}.$$

Démonstration. — Si $\mathfrak{m} \subset \mathbb{Z}_K$ est un idéal nous utiliserons la notation (standard) $u \equiv v \pmod{{}^*\mathfrak{m}}$ pour signifier que $v_{\mathfrak{q}}(u-v) \geqslant v_{\mathfrak{q}}(\mathfrak{m})$ pour tous les idéaux premiers $\mathfrak{q} \mid \mathfrak{m}$, ce qui permet de travailler sur des congruences entre nombres algébriques qui ne sont pas nécessairement des *entiers* algébriques. Puisque $(1-x\zeta^{-1}) = (-\zeta^{-1})(x-\zeta)$ et puisque $(-\zeta^{-1})^\theta$ est une racine $2p$-ième de l'unité, donc une q-ième puissance dans K, il résulte du lemme 5.1 que pour tout $\theta \in (1-\iota)I_s$ le nombre $(1-x\zeta^{-1})^\theta$ est une puissance q-ième dans K. D'autre part, d'après le théorème de Cassels, on a $q \mid x$, et donc $(1-x\zeta^{-1})^\theta \equiv 1 \pmod{{}^*q\mathbb{Z}_K}$. Puisque q est non ramifié dans K, il résulte du corollaire 5.3 que $(1-x\zeta^{-1})^\theta \equiv 1 \pmod{{}^*q^2\mathbb{Z}_K}$ (en toute rigueur nous n'avons pas démontré le résultat dans le contexte des congruences généralisées de ce type, mais il est facile de voir que le raisonnement est toujours valable). D'autre part, si nous écrivons $\theta = \sum_{\sigma\in G} a_\sigma \sigma$ avec $a_\sigma \in \mathbb{Z}$, il est clair en développant et en utilisant le fait que $q \mid x$ que

$$(1-x\zeta^{-1})^\theta = 1 - xS \pmod{{}^*q^2\mathbb{Z}_K} \quad \text{avec} \quad S = \sum_{\sigma\in G} a_\sigma \sigma(\zeta^{-1}).$$

Il résulte de la combinaison de ces deux congruences que $xS \equiv 0 \pmod{{}^*q^2\mathbb{Z}_K}$. Nous allons commencer par démontrer que $q^2 \mid x$. Si par l'absurde nous supposons le contraire on a donc $S \equiv 0 \pmod{{}^*q\mathbb{Z}_K}$. Comme les $\sigma(\zeta^{-1})$ forment une permutation des ζ^j pour $1 \leqslant j \leqslant p-1$, ils forment une $\mathbb{Z}$-base de $\mathbb{Z}_K = \mathbb{Z}[\zeta]$, et donc par unicité $q \mid a_\sigma$ pour tout $\sigma \in G$. Toutefois, rappelons nous que l'on a seulement demandé à θ d'appartenir à $(1-\iota)I_s$, donc que nous avons un grand choix pour obtenir une contradiction. Par exemple, si on choisit $\theta = (1-\iota)\Theta_2$

(où Θ_b est défini ci-dessus), il est immédiat de voir que

$$\theta = -\sum_{1\leqslant j\leqslant (p-1)/2} \sigma_j^{-1} + \sum_{(p+1)/2\leqslant j\leqslant p-1} \sigma_j^{-1},$$

et cet élément de $(1-\iota)I_s$ ne satisfait clairement pas à la condition $q \mid a_\sigma$ pour tout $\sigma \in G$, contradiction.

Nous avons donc démontré que $q^2 \mid x$, ce qui est un renforcement crucial du théorème de Cassels, et nous permet aisément de prouver les autres conditions du théorème : puisque $q^2 \mid x$, d'après le théorème de Cassels dont on reprend les notations, on a $p^{q-1}a^q = x - 1 \equiv -1 \pmod{q^2}$, et puisque d'après le « petit » théorème de Fermat on a $p^{q-1} \equiv 1 \pmod{q}$, on en déduit que $a^q \equiv (-1)^q \pmod{q}$. En utilisant à nouveau le lemme crucial 5.2 (mais cette fois-ci dans le corps $\mathbb{Q}$) on en déduit que $a^q \equiv -1 \pmod{q^2}$, et en remplaçant dans le théorème de Cassels on obtient $p^{q-1} \equiv 1 \pmod{q^2}$. Comme nous l'avons déjà remarqué dans la démonstration du théorème de Cassels, p et q étant impairs jouent des rôles symétriques (changer (p, q, x, y) en $(q, p, -y, -x)$), ce qui démontre les résultats obtenus en échangeant p et q. □

Remarques

(1) Un résultat important dû à Wieferich affirme que le premier cas du théorème de Fermat est vrai dès que $2^{p-1} \not\equiv 1 \pmod{p^2}$ (les seuls contre-exemples connus sont $p = 1093$ et 3511, pour lesquels on démontre le premier cas de Fermat avec des résultats analogues). On a donc coutume d'appeler un couple de nombres premiers (p, q) tels que l'on ait simultanément $p^{q-1} \equiv 1 \pmod{q^2}$ et $q^{p-1} \equiv 1 \pmod{p^2}$ une *paire de Wieferich*. Le premier théorème de Mihăilescu ci-dessus implique donc que si (p, q) n'est *pas* une paire de Wieferich (avec p et q premiers impairs) alors l'équation de Catalan est impossible pour cette paire d'exposants. Les seules paires de Wieferich connues au moment de la rédaction de ce texte sont $(2, 1093)$, $(3, 1006003)$, $(5, 1645333507)$, $(5, 188748146801)$, $(83, 4871)$, $(911, 318917)$ et $(2903, 18787)$ (voir **[2]**), la plus grande ayant été obtenue en 2004. Toutefois par un raisonnement probabiliste très raisonnable, on s'attend à ce qu'il y en ait une infinité, et en fait même à p fixé.

(2) Le théorème ci-dessus a été démontré par Mihăilescu en 2001. Il est tout à fait surprenant qu'il ait fallu attendre si tard pour obtenir cette démonstration : la clef est le lemme 5.1, mais on voit que la démonstration de ce lemme est immédiate en utilisant le théorème de Stickelberger, démontré en 1890, couplée avec le théorème de Cassels qui date de 1960. On aurait donc pu s'attendre à obtenir la démonstration ci-dessus peu après celle du théorème de Cassels, c'est-à-dire dans les années 1960. C'est d'autant plus étonnant que le critère de Wieferich pour premier cas du théorème de Fermat, qui a un énoncé très analogue, se démontre *aussi* grâce au théorème de Stickelberger, à travers ce qu'on appelle la loi de réciprocité d'Eisenstein, qui en est une conséquence. L'histoire des mathématiques n'est pas toujours logique.

La suite de la démonstration de la conjecture de Catalan se fait à travers trois théorèmes plus ou moins indépendants. Les deux premiers ne sont pas véritablement essentiels, mais aident à obtenir une démonstration n'utilisant ni outil informatique, ni outils analytiques sophistiqués sur les formes linéaires en logarithmes de nombres algébriques. Par contre le dernier théorème est tout à fait extraordinaire et très difficile, et en toute honnêteté, bien que je comprenne la démonstration « localement » comme on dit, je ne peux pas dire que je comprenne le pourquoi et le comment. Ce dernier théorème est basé à nouveau sur une idée forcément géniale et naturelle de Mihăilescu : puisque l'utilisation du théorème de Stickelberger, qui décrit très précisément l'annulateur de $\mathrm{Cl}^-(K)$ a si bien marché, ne pourrait-on pas maintenant utiliser aussi l'annulateur de $\mathrm{Cl}(K^+)$ et obtenir des informations complémentaires qui résoudraient la conjecture ? C'est bien sûr une très bonne idée, mais qui se heurte à un obstacle de taille. Autant on contrôle fort bien $\mathrm{Cl}^-(K)$ (il existe par exemple une formule très simple pour calculer son cardinal), autant $\mathrm{Cl}(K^+)$ est beaucoup plus mystérieux, principalement à cause de la présence d'unités. Le lecteur ayant déjà un peu manipulé les corps quadratiques peut imaginer sans peine qu'il est beaucoup plus facile de travailler dans $\mathbb{Q}(\sqrt{-6})$ (qui ne possède pas d'unités autres que ± 1) que dans $\mathbb{Q}(\sqrt{6})$, dont le groupe des unités est infini, même si les deux anneaux d'entiers correspondants sont principaux, c'est-à-dire ont un nombre de classes

égal à 1. De fait, dans toutes les démonstrations que nous avons faites ci-dessus, nous avons évacué sans difficulté le problème des unités dans K en remarquant que si u est une telle unité alors $u/\overline{u} = u/\iota(u)$ est une racine de l'unité, donc entièrement sous contrôle. Mais clairement cette opération « tue » les unités réelles, c'est-à-dire les unités de K^+, et il faudrait donc les récupérer d'une manière ou d'une autre.

Contrairement au cas de $\mathrm{Cl}^-(K)$, le problème du calcul de l'annulateur de $\mathrm{Cl}(K^+)$ demeure un problème difficile, et le restera probablement à tout jamais. Heureusement pour nous, pour Mihăilescu et pour la conjecture de Catalan, il existe un remarquable théorème dû au mathématicien Brésilien F. Thaine et démontré en 1988, qui donne une réponse *partielle* à la question. Bien que partiel, ce théorème a eu des conséquences extrêmement importantes dans plusieurs branches de la théorie des nombres. Par exemple, c'est grâce à lui que Kolyvagin et Rubin ont montré la validité de la conjecture de Birch et Swinnerton-Dyer sur les courbes elliptiques de rang analytique 0 ou 1, et en particulier la finitude de leur groupe de Tate-Shafarevitch, qui n'était connu auparavant pour *aucune* courbe elliptique (je ne définis pas toutes ces notions). Et donc c'est également grâce au théorème de Thaine que en 2003 Mihăilescu a pu finir la démonstration de la conjecture de Catalan.

Comme expliqué ci-dessus, la suite de la démonstration est plus ardue. Bien que le titre l'exposé oral ait été « premières approches » de la démonstration, ce qui dans mon esprit s'arrête ici, je vais donner ci-dessous la démonstration complète. Celle-ci est la traduction quasiment littérale d'un chapitre d'un livre que j'espère publier en 2006, et est fortement inspiré de **[3]**. Toutefois, je tiens à avertir le lecteur qu'un certain nombre de notions ne seront pas définies, et que le niveau d'abstraction est plus élevé. Il est donc prié, s'il le désire, de se référer aux nombreux excellents ouvrages existants de théorie algébrique des nombres.

6. Le deuxième théorème de Mihăilescu : $p \mid h_q^-$ et $q \mid h_p^-$

6.1. L'inclusion $\mathrm{Cl}(K^+) \subset \mathrm{Cl}(K)$. — Comme annoncé ci-dessus nous allons devoir maintenant considérer encore plus en détail l'action de la conjugaison complexe sur tous les objets que nous étudierons.

Nous appelons donc K^+ le sous-corps de $K = \mathbb{Q}(\zeta)$ fixé par la conjugaison complexe, en d'autres termes le sous-corps (totalement) réel maximal de K. On sait que $K^+ = \mathbb{Q}(\zeta + \zeta^{-1})$. On désigne par h_p^+ son nombre de classes d'idéaux. Nous allons montrer ci-dessous que h_p^+ divise le nombre de classes d'idéaux h_p de K, et on posera donc $h_p^- = h_p/h_p^+$. Il faut se rendre compte que h_p^- est *facile* à calculer bien qu'il soit exponentiellement grand en p (nous donnerons des formules ci-dessous), alors que h_p^+ est très difficile à calculer (on ne connaît pas sa valeur pour $p > 500$ par exemple), bien qu'il soit conjecturalement très petit.

Proposition 6.1. — *L'application qui envoie un idéal* $\mathfrak{a}$ *de* $\mathbb{Z}_{K^+}$ *vers* $\mathfrak{a}\mathbb{Z}_K$ *induit un homomorphisme* injectif *de* $\mathrm{Cl}(K^+)$ *dans* $\mathrm{Cl}(K)$. *En particulier* h_p^+ *divise* h_p.

Démonstration. — Puisqu'elle passe aux idéaux principaux, il est clair que cette application induit un homomorphisme de groupes de $\mathrm{Cl}(K^+)$ dans $\mathrm{Cl}(K)$, et on doit montrer qu'elle est injective. Soit donc $\mathfrak{a}$ un idéal (entier) de $\mathbb{Z}_{K^+}$ tel que $\mathfrak{a}\mathbb{Z}_K = \alpha\mathbb{Z}_K$ soit un idéal principal de K. Puisque $\iota(\mathfrak{a}) = \mathfrak{a}$ on en déduit que $\iota(\alpha)\mathbb{Z}_K = \alpha\mathbb{Z}_K$, et donc que $\alpha/\iota(\alpha)$ est une unité de K. Il résulte de la démonstration du corollaire 1.14 (1), qui n'utilise que le fait que $u/\iota(u)$ est un entier algébrique, que $\alpha/\iota(\alpha)$ est une racine de l'unité, en d'autres termes que $\alpha/\iota(\alpha) = (-\zeta)^j$ pour un certain entier j. J'affirme que j est *pair*. En effet, si on pose comme d'habitude $\pi = 1 - \zeta$ et $\mathfrak{p} = \pi\mathbb{Z}_K$, et si $\mathfrak{p}^+ = \mathfrak{p} \cap \mathbb{Z}_{K^+}$ est l'idéal premier de K^+ en dessous de $\mathfrak{p}$, alors comme $p\mathbb{Z}_K = \mathfrak{p}^{p-1}$ on doit avoir $\mathfrak{p}^+\mathbb{Z}_K = \mathfrak{p}^2$. Il en résulte que $v_{\mathfrak{p}}(\mathfrak{a}\mathbb{Z}_K) = 2v_{\mathfrak{p}^+}(\mathfrak{a}) \equiv 0 \pmod 2$, et donc que $v_{\mathfrak{p}}(\alpha) \equiv 0 \pmod 2$. Puisque $\pi/\iota(\pi) = (1-\zeta)/(1-\zeta^{-1}) = -\zeta$, on a $\alpha/\iota(\alpha) = (\pi/\iota(\pi))^j$ donc si on pose $\beta = \alpha\iota(\pi)^j$ on a $\beta = \iota(\beta)$, en d'autres termes $\beta \in K^+$. On en déduit à nouveau que $v_{\mathfrak{p}}(\beta) \equiv 0 \pmod 2$, et donc $j = v_{\mathfrak{p}}(\iota(\pi)^j) = v_{\mathfrak{p}}(\beta) - v_{\mathfrak{p}}(\alpha) \equiv 0 \pmod 2$, ce qui démontre mon assertion.

Posant $j = 2i$ et $\gamma = \alpha(-\zeta)^{-i}$, on voit donc que $\iota(\gamma) = \iota(\alpha)(-\zeta)^i = \gamma(\iota(\alpha)/\alpha)(-z)^j = \gamma$, et donc $\gamma \in K^+$. Puisque α et γ ne diffèrent que par une unité on a $\mathfrak{a}\mathbb{Z}_K = \alpha\mathbb{Z}_K = \gamma\mathbb{Z}_K$. Puisque $\mathfrak{a}$ et $\gamma\mathbb{Z}_{K^+}$ sont des idéaux de $\mathbb{Z}_{K^+}$, en intersectant avec K^+ il en résulte que $\mathfrak{a} = \gamma\mathbb{Z}_{K^+}$ (exercice : si L/K est une extension de corps de nombres et $\mathfrak{a}$ et $\mathfrak{b}$ des

idéaux de K, alors on a $\mathfrak{a}\mathbb{Z}_L = \mathfrak{b}\mathbb{Z}_L$ si et seulement si $\mathfrak{a} = \mathfrak{b}$. Pour cela on montrera que $\mathfrak{a}\mathfrak{b}^{-1}$ et $\mathfrak{b}\mathfrak{a}^{-1}$ sont des idéaux entiers). Il en résulte donc que $\mathfrak{a}$ est bien un idéal principal de K^+. □

6.2. Diagonalisation de l'élément de Stickelberger

À un unique endroit ci-dessous nous allons avoir besoin d'un résultat d'injectivité (le lemme 6.3) qui se démontre par des voies analytiques. Le but de ce paragraphe est donc de démontrer ce résultat.

Notons $\widehat{G}$ le groupe des caractères de $G \simeq (\mathbb{Z}/p\mathbb{Z})^*$, qui est non canoniquement isomorphe à G. Pour $\chi \in \widehat{G}$ on pose

$$e_\chi = \frac{1}{p-1} \sum_{\sigma \in G} \chi(\sigma)\sigma^{-1} \in \mathbb{C}[G].$$

On vérifie immédiatement que les e_χ forment un *système complet d'idempotents orthogonaux*, en d'autres termes que $e_\chi^2 = e_\chi$, que $e_{\chi_1} e_{\chi_2} = 0$ quand $\chi_1 \neq \chi_2$, et que $\sum_{\chi \in \widehat{G}} e_\chi = 1$. Comme conséquence immédiate on en déduit que

$$\mathbb{C}[G] = \bigoplus_{\chi \in \widehat{G}} e_\chi \mathbb{C}[G].$$

Puisque $e_\chi \neq 0$ tous les $e_\chi\mathbb{C}[G]$ sont non nuls, et d'autre part le nombre de termes dans la somme est égal à $|\widehat{G}| = |G| = \dim_{\mathbb{C}} \mathbb{C}[G]$. Il en résulte que tous les termes sont de dimension égale à 1, et donc que $e_\chi\mathbb{C}[G] = \mathbb{C}e_\chi$, donc que les e_χ forment une $\mathbb{C}$-base de $\mathbb{C}[G]$. D'autre part puisque $e_\chi\mathbb{C}[G]$ est l'idéal principal de $\mathbb{C}[G]$ engendré par e_χ, il en résulte que $\mathbb{C}e_\chi$ est un idéal de $\mathbb{C}[G]$.

Lemme 6.2. — *Appelons j l'isomorphisme canonique de $(\mathbb{Z}/p\mathbb{Z})^*$ dans G tel que $j(t) = \sigma_t$, et comme d'habitude notons $\iota = \sigma_{-1}$ la conjugaison complexe. On a $\Theta e_\chi = \lambda_\chi e_\chi$ avec*

$$\lambda_\chi = \begin{cases} (p-1)/2 & \text{si } \chi \text{ est le caractère trivial} \\ 0 & \text{si } \chi(\iota) = 1 \text{ et } \chi \text{ est non trivial} \\ L(\overline{\chi \circ j}, 0) & \text{si } \chi(\iota) = -1. \end{cases}$$

Ici, $L(\overline{\chi \circ j}, 0)$ est défini comme la valeur en 0 du prolongement analytique de la fonction $L(\overline{\chi \circ j}, s)$ définie pour $\mathrm{Re}(s) > 1$ par

$$L(\overline{\chi \circ j}, s) = \sum_{n \geqslant 1} \frac{\overline{\chi \circ j}(n)}{n^s}.$$

Démonstration. — Par définition de e_χ on a

$$\sigma_t e_\chi = \frac{1}{p-1}\sum_{\sigma\in G}\chi(\sigma)\sigma_t\sigma^{-1} = \frac{1}{p-1}\sum_{\sigma\in G}\chi(\sigma\sigma_t)\sigma^{-1} = \chi(\sigma_t)e_\chi.$$

Ainsi $\Theta e_\chi = \lambda_\chi e_\chi$, où

$$\lambda_\chi = \frac{1}{p}\sum_{1\leqslant t\leqslant p-1} t\overline{\chi(\sigma_t)}.$$

Il est clair que $\lambda_\chi = (p-1)/2$ quand χ est le caractère trivial, et en regroupant les termes en t et en $p-t$ il est également évident que $\lambda_\chi = 0$ si $\chi(\iota) = 1$ avec χ non trivial, puisque la somme des valeurs d'un caractère non trivial est nul. Enfin, si $\chi(\iota) = -1$, la théorie (tout à fait élémentaire, mais que nous ne ferons pas ici) du prolongement des fonctions L de Dirichlet montre que $\lambda_\chi = L(\overline{\chi\circ j}, 0)$. □

Remarque. — Le fait que $\lambda_\chi = 0$ quand χ est un caractère pair non trivial est une autre manière de dire que l'idéal de Stickelberger ne donne de renseignements que sur la partie $-$ du groupe de classes, comme nous l'avons signalé à plusieurs reprises. De fait, si on pose

$$\mathbb{C}[G]^- = \{x\in\mathbb{C}[G],\ \iota x = -x\} = (1-\iota)\mathbb{C}[G]$$

(où la dernière égalité est évidente), nous avons en fait le résultat suivant, qui est le but de ce paragraphe.

Lemme 6.3

(1) *Les e_χ pour lesquels $\chi(\iota) = -1$ (en d'autres termes tels que $\chi\circ j$ soit un caractère impair) forment une $\mathbb{C}$-base de $\mathbb{C}[G]^-$.*

(2) *La multiplication par Θ induit une application $\mathbb{C}$-linéaire* bijective *de $\mathbb{C}[G]^-$ dans lui-même.*

Démonstration

(1) Puisque $\sigma_t e_\chi = \chi(\sigma_t)e_\chi$ on a $\iota e_\chi = \chi(\iota)e_\chi = -e_\chi$ quand $\chi(\iota) = -1$, donc de tels e_χ appartiennent à $\mathbb{C}[G]^-$. Or le nombre de caractères impairs modulo p est égal à $(p-1)/2$. D'autre part puisque $\iota\sigma_t = \sigma_{-t}$, $\sum_{t\in(\mathbb{Z}/p\mathbb{Z})^*} a_t\sigma_t \in \mathbb{C}[G]^-$ si et seulement si $a_{-t} = -a_t$, et donc les σ_t pour $1\leqslant t\leqslant (p-1)/2$ forment une base de $\mathbb{C}[G]^-$, donc $\dim_{\mathbb{C}}\mathbb{C}[G]^- = (p-1)/2$, ce qui démontre (1) puisque les e_χ sont $\mathbb{C}$-linéairement indépendants.

(2) D'après le lemme ci-dessus, sur la $\mathbb{C}$-base $(e_\chi)_{\chi(\iota)=-1}$ de $\mathbb{C}[G]^-$ la matrice de la multiplication par Θ est diagonale, les éléments diagonaux étant le s $L(\overline{\chi \circ j}, 0)$ pour $\chi(\iota) = -1$. Or un théorème très important et pas tout à fait évident de théorie analytique des nombres affirme que toutes ces valeurs en 0 sont *non nulles* (le théorème est habituellement énoncé pour les valeurs en 1, mais il est facile de voir que dans notre cas la non nullité en 0 est équivalente). Noter que c'est ce même théorème qui permet de démontrer le théorème de Dirichlet sur l'infinité des nombres premiers dans les progressions arithmétiques. En tous cas ce théorème montre que la matrice de la multiplication par Θ sur la base des e_χ est une matrice diagonale avec des éléments diagonaux non nuls, et est donc inversible, ce qui démontre le lemme. □

Remarque. — On peut montrer que le déterminant de l'application multiplication par Θ de $\mathbb{C}[G]^-$ dans lui-même est égal à $2^{(p-3)/2} h_p^- / p$. Il est à noter que ceci donne une manière tout à fait élémentaire de calculer h_p^-.

6.3. Les sous-espaces + et −. — Soit R un anneau commutatif et M un $R[G]$-module. Nous poserons $M^\pm = \{x \in M,\ \iota(x) = \pm x\}$. Si 2 est inversible dans R (ce qui n'est *pas* le cas pour $R = \mathbb{Z}$ par exemple), nous poserons $\varepsilon^\pm = (1 \pm \iota)/2 \in R[G]$. Il est clair que les $\varepsilon^\pm$ sont des *projecteurs complémentaires*, en d'autres termes que $(\varepsilon^\pm)^2 = \varepsilon^\pm$, $\varepsilon^+ + \varepsilon^- = 1$ et $\varepsilon^+ \varepsilon^- = 0$. Il est également évident que $M^\pm = \varepsilon^\pm M$ et que $M = M^+ \oplus M^-$. Si 2 n'est pas inversible dans R (donc par exemple pour $R = \mathbb{Z}$) nous poserons $\varepsilon^\pm = 1 \pm \iota$, et nous avons seulement les inclusions $\varepsilon^\pm M \subset M^\pm$ et $M^+ \oplus M^- \subset M$, les indices étant des puissances de 2. Toutefois, dans le cas particulier où $M = R[G]$ nous avons le résultat suivant :

Lemme 6.4. — *On a $\varepsilon^\pm R[G] = R[G]^\pm$, et ce sont des R-modules libres de dimension $(p-1)/2$.*

Démonstration. — Le membre de gauche est toujours un sous-module de celui de droite. Ainsi, soit $x = \sum_{1 \leqslant t \leqslant p-1} a_t \sigma_t \in R[G]^\pm$. Puisque $\iota \sigma_t = \sigma_{p-t}$ on a donc $a_{p-t} = \pm a_t$. Il en résulte que si l'on pose $y = \sum_{1 \leqslant t \leqslant (p-1)/2} a_t \sigma_t$ on aura $x = \varepsilon^\pm y$. La dernière assertion est évidente puisque $a_{p-t} = \pm a_t$. □

Exercice. — Montrer que l'indice de $\mathbb{Z}[G]^+ \oplus \mathbb{Z}[G]^-$ dans $\mathbb{Z}[G]$ est égal à $2^{(p-1)/2}$.

Rappelons que l'élément de Stickelberger est défini par

$$\Theta = \frac{1}{p} \sum_{1 \leqslant t \leqslant p-1} t\sigma_t^{-1} \in \mathbb{Q}[G],$$

et que l'idéal de Stickelberger I_s est défini par $I_s = \Theta\mathbb{Z}[G] \cap \mathbb{Z}[G]$. Nous poserons

$$I = (1-\iota)I_s = \varepsilon^- I_s \subset I_s^- = I_s \cap \mathbb{Z}[G]^- = I_s \cap \varepsilon^-\mathbb{Z}[G],$$

où la dernière égalité résulte du lemme ci-dessus (noter que nous avons déjà utilisé l'idéal I dans le lemme 5.1). D'après la proposition 4.22 (2), I_s est engendré par Θ_{p+1} et par les Θ_b pour $1 \leqslant b \leqslant p-1$. Posons $g_b = -\Theta_b$ pour $1 \leqslant b \leqslant p-1$ et $g_p = -\Theta_{p+1}$. D'après la proposition 4.22 (1) nous avons $g_b = \sum_{1 \leqslant t \leqslant p-1} \lfloor bt/p \rfloor \sigma_t^{-1}$, y compris quand $b = p$ puisque $\lfloor (p+1)t/p \rfloor = t$ pour $1 \leqslant t \leqslant p-1$. Enfin, pour $1 \leqslant i \leqslant p-1$ posons

$$f_i = g_{i+1} - g_i = \sum_{1 \leqslant t \leqslant p-1} \left(\left\lfloor \frac{t(i+1)}{p} \right\rfloor - \left\lfloor \frac{ti}{p} \right\rfloor \right) \sigma_t^{-1},$$

où nous notons que le coefficient de σ_t^{-1} est égal à 0 ou à 1. Puisque les g_i pour $1 \leqslant i \leqslant p$ engendrent I_s et que $g_1 = 0$, il en résulte que les f_i pour $1 \leqslant i \leqslant p-1$ engendrent aussi I_s. De plus, puisque $\lfloor tp/p \rfloor = t$ et $\lfloor t(p-1)/p \rfloor = t-1$ pour $1 \leqslant t \leqslant p-1$ on a donc $f_{p-1} = \sum_{1 \leqslant t \leqslant p-1} \sigma_t$. Ceci est exactement l'élément *norme* $\mathcal{N}$ de l'anneau de groupe $\mathbb{Z}[G]$ vu ci-dessus, que nous noterons ici $s(G)$ (somme des éléments de G), et qui vérifie $\alpha^{s(G)} = \mathcal{N}(\alpha)$.

Définition 6.5. — Si $f = \sum_{1 \leqslant t \leqslant p-1} a_t\sigma_t \in \mathbb{Z}[G]$ on pose

$$\|f\| = \sum_{1 \leqslant t \leqslant p-1} |a_t|.$$

Il est clair que $\|f\| \geqslant 0$, que $\|f\| = 0$ si et seulement si $f = 0$, et on vérifie immédiatement que $\|fg\| \leqslant \|f\|\|g\|$, et qu'il y a égalité quand tous les coefficients de f et de g sont positifs ou nuls.

Lemme 6.6

(1) *Pour* $1 \leqslant i \leqslant p-2$ *on a* $\|f_i\| = (p-1)/2$.

(2) *L'idéal I_s est un $\mathbb{Z}$-module libre de dimension $(p+1)/2$ engendré par les f_i pour $1 \leqslant i \leqslant (p-1)/2$ et par $f_{p-1} = s(G)$.*

(3) *L'idéal I est un $\mathbb{Z}$-module libre de dimension $(p-1)/2$ engendré par les e_i pour $1 \leqslant i \leqslant (p-1)/2$, où on pose $e_i = \varepsilon^- f_i$.*

(4) *Pour $1 \leqslant i \leqslant (p-1)/2$ les coefficients de e_i sont tous égaux à ± 1, et en particulier $\|e_i\| = p-1$.*

Démonstration

(1) et (4). Pour $1 \leqslant t \leqslant p-1$ et $1 \leqslant i \leqslant p-1$ nous avons

$$\lfloor ti/p \rfloor + \lfloor (p-t)i/p \rfloor = \lfloor ti/p \rfloor + i - \lceil ti/p \rceil = i - 1$$

puisque $p \nmid ti$. Il en résulte que

$$\sum_{1 \leqslant t \leqslant p-1} \lfloor ti/p \rfloor = \sum_{1 \leqslant t \leqslant (p-1)/2} (\lfloor ti/p \rfloor + \lfloor (p-t)i/p \rfloor) = (i-1)(p-1)/2.$$

Puisque les coefficients de f_i valent 0 ou 1, pour $1 \leqslant i \leqslant p-2$ on a $\|f_i\| = i(p-1)/2 - (i-1)(p-1)/2 = (p-1)/2$, ce qui démontre (1) (noter que ceci est faux pour $i = p-1$ puisque pour cette valeur de i le calcul ci-dessus n'est pas valable pour $i+1 = p$, et de fait nous savons que $\|f_{p-1}\| = \|s(G)\| = p-1$). La démonstration de (4) résulte immédiatement de (1) et est laissée au lecteur.

(2) et (3). En échangeant i et t dans la première égalité prouvée dans (1) nous voyons que

$$\lfloor it/p \rfloor + \lfloor (p-i)t/p \rfloor = t - 1 = \lfloor (i+1)t/p \rfloor + \lfloor (p-i-1)t/p \rfloor,$$

en d'autres termes que

$$\lfloor (p-i)t/p \rfloor - \lfloor (p-i-1)t/p \rfloor = \lfloor (i+1)t/p \rfloor - \lfloor it/p \rfloor.$$

Il en résulte que $f_{p-1-i} = f_i$, et donc que les f_i pour $1 \leqslant i \leqslant (p-1)/2$ ainsi que $s(G)$ engendrent I_s.

Posons $e_i = \varepsilon^- f_i$. Puisqu'on a trivialement $\varepsilon^-(s(G)) = 0$ et que $I = \varepsilon^- I_s$, il en résulte que les e_i pour $1 \leqslant i \leqslant (p-1)/2$ engendrent I. Supposons que nous ayons démontré (3), c'est-à-dire que nous sachions que les e_i forment une $\mathbb{Z}$-base de I. Il est alors évident que les f_i pour $1 \leqslant i \leqslant (p-1)/2$ ainsi que $s(G)$ forment une $\mathbb{Z}$-base de I_s : en effet, si nous avions une relation $\sum_{1 \leqslant i \leqslant (p-1)/2} \lambda_i f_i + \lambda s(G) = 0$, appliquant ε^- on en déduirait $\sum_{1 \leqslant i \leqslant (p-1)/2} \lambda_i e_i = 0$, donc $\lambda_i = 0$, et donc aussi $\lambda = 0$, ce qui démontre (2).

Reste à démontrer (3), ce que nous allons faire de manière indirecte. Puisque I_s est un $\mathbb{Z}$-module de type fini et sans torsion il est libre, ainsi que ses sous-modules. Montrer (3) est donc équivalent à montrer que la $\mathbb{Z}$-dimension de I est égale à $(p-1)/2$. Or d'après le lemme 6.4 on a $\dim_{\mathbb{Z}} \mathbb{Z}[G]^- = (p-1)/2$. D'après le lemme 6.3, que nous utilisons de manière cruciale et uniquement ici, la multiplication par $p\Theta$ est une application injective de $\mathbb{Z}[G]^-$ dans $\mathbb{Z}[G]^-$, et donc $\dim_{\mathbb{Z}} p\Theta\mathbb{Z}[G]^- = (p-1)/2$. Or puisque par définition $I_s = \Theta\mathbb{Z}[G]\cap\mathbb{Z}[G]$ on a donc $I_s^- = \Theta\mathbb{Z}[G]\cap\mathbb{Z}[G]^-$. Puisque $p\Theta \in \mathbb{Z}[G]$ nous avons la chaîne d'inclusions

$$p\Theta\mathbb{Z}[G]^- = p\Theta\mathbb{Z}[G]^- \cap \mathbb{Z}[G]^- \subset \Theta\mathbb{Z}[G]^- \cap \mathbb{Z}[G]^- \subset I_s^- \subset \mathbb{Z}[G]^-.$$

Puisque les extrémités de cette chaîne sont de $\mathbb{Z}$-dimension égale à $(p-1)/2$ on en déduit que c'est le cas pour tous les termes, et donc en particulier que $\dim_{\mathbb{Z}}(I_s^-) = (p-1)/2$. Finalement, notons que si $x \in I_s^-$ alors $\varepsilon^- x \in I$, mais que d'autre part $\varepsilon^- x = x + x = 2x$. Il en résulte que $2I_s^- \subset I \subset I_s^-$, et donc que $\dim_{\mathbb{Z}}(I) = \dim_{\mathbb{Z}}(I_s^-) = (p-1)/2$, ce qui finit la démonstration du lemme. □

Remarque. — Il résulte de ce lemme que les e_i pour $1 \leqslant i \leqslant (p-1)/2$ sont $\mathbb{Z}$-linéairement indépendants. Nous laissons en exercice au lecteur le soin de démontrer que ceci est équivalent au fait que la matrice carrée $M = (m_{i,j})_{1\leqslant i,j\leqslant(p-1)/2}$ d'ordre $(p-1)/2$ définie par $m_{i,j} = \lfloor (i+1)(j+1)/p \rfloor$ a un déterminant non nul. Ceci peut se faire sans trop de mal en montrant que $\det(M)$ est égal au déterminant de l'application multiplication par Θ de $\mathbb{C}[G]^-$ dans lui-même, multiplié par $p/(2^{(p-3)/2})$. Comme nous l'avons déjà remarqué après le lemme 6.3, on a donc $h_p^- = |\det(M)|$, d'où une formule immédiatement implantable pour h_p^-.

6.4. Le groupe S. — Le lecteur aura pu remarquer que les résultats obtenus ci-dessus n'ont pour l'instant rien à voir avec Catalan. Nous nous en approchons maintenant en introduisant un nombre premier impair q différent de p. Rappelons que $\pi = 1 - \zeta$ est le générateur de l'unique idéal premier $\mathfrak{p}$ au-dessus de p dans K, qui vérifie $\mathfrak{p}^{p-1} = p\mathbb{Z}_K$.

Définition 6.7

(1) Nous définissons $E = \{u\pi^k,\ u \in U(K),\ k \in \mathbb{Z}\}$.

(2) Soit V le groupe des éléments $\alpha \in K^*$ tels que $v_{\mathfrak{r}}(\alpha) \equiv 0 \pmod{q}$ pour tous les idéaux premiers $\mathfrak{r} \neq \mathfrak{p}$. On pose $S = V/K^{*q}$.

Remarque. — Nous pourrions faire toute la démonstration en utilisant $U(K)$ à la place de E, et en effectuant les modifications correspondantes pour les groupes S, etc., mais nous avons un peu plus de liberté en autorisant également des puissances de π. Le prix à payer est que nous devons travailler dans $\mathbb{Z}[\zeta_p, 1/p]$ au lieu de $\mathbb{Z}[\zeta_p]$.

Proposition 6.8

(1) *E est un $\mathbb{Z}[G]$-module et $E = \mathbb{Z}[\zeta_p, 1/p]^*$.*

(2) *$\alpha \in V$ si et seulement si il existe un idéal $\mathfrak{a}$ et $k \in \mathbb{Z}$ tels que $\alpha\mathbb{Z}_K = \pi^k \mathfrak{a}^q$.*

(3) *S est un $\mathbb{Z}[G]$-module annulé par $q\mathbb{Z}[G]$, donc S est un $\mathbb{F}_q[G]$-module.*

Démonstration. — Conséquences immédiates des définitions et laissé au lecteur. □

Nous poserons $G^+ = \mathrm{Gal}(K^+/\mathbb{Q}) = G/\langle\iota\rangle$, qui est de cardinal $(p-1)/2$. Le groupe $\mathrm{Cl}(K)$ est un $\mathbb{Z}[G]$-module, donc nous pouvons parler de $\mathrm{Cl}(K)^{\pm}$. Par définition $\mathrm{Cl}(K)^+$ est le sous-groupe des classes d'idéaux invariantes par la conjugaison complexe ι. Il est important de noter que ceci n'est en général *pas* égal à $\mathrm{Cl}(K^+)$, mais d'après la proposition 6.1 l'application naturelle de $\mathrm{Cl}(K^+)$ vers $\mathrm{Cl}(K)^+$ est injective, donc $\mathrm{Cl}(K^+)$ peut être considéré comme un sous-groupe de $\mathrm{Cl}(K)^+$, et en particulier $h_p^+ \mid |\mathrm{Cl}(K)^+|$. De plus, d'après les considérations générales du début du paragraphe 6.3, on a $\mathrm{Cl}(K)^- \oplus \mathrm{Cl}(K)^+ \subset \mathrm{Cl}(K)$. Il en résulte qu'il existe une injection naturelle de $\mathrm{Cl}(K)^-$ vers $\mathrm{Cl}(K)/\mathrm{Cl}(K)^+$, et qu'en particulier

$$|\mathrm{Cl}(K)^-| \mid (h_p/|\mathrm{Cl}(K)^+|) \mid (h_p/h_p^+) = h_p^-.$$

De la même manière, ne pas confondre $\mathrm{Cl}^-(K)$ défini comme $\mathrm{Cl}(K)/\mathrm{Cl}(K^+)$ avec $\mathrm{Cl}(K)^-$.

Pour le lemme qui suit rappelons la notation suivante : si A est un groupe abélien $A[q]$ est l'ensemble des $x \in A$ tels que $x^q = 1$ (ou $qx = 0$ en notation additive). Rappelons aussi qu'une suite $M_1 \to M_2 \to M_3 \cdots$ de modules et d'homomorphismes de modules est dite

exacte si l'image de chaque homomorphisme est égale au noyau de l'homomorphisme qui le suit.

Lemme 6.9

(1) *Il existe une suite exacte de* $\mathbb{F}_q[G]$*-modules*

$$0 \longrightarrow E/E^q \longrightarrow S \longrightarrow \mathrm{Cl}(K)[q].$$

(2) E/E^q *est invariant par* ι*, donc est un* $\mathbb{F}_q[G^+]$*-module.*

(3) *On a* $S^- \simeq \mathrm{Cl}(K)[q]^- = \mathrm{Cl}(K)^-[q]$*, et il existe une suite exacte de* $\mathbb{F}_q[G^+]$*-modules*

$$0 \longrightarrow E/E^q \longrightarrow S^+ \longrightarrow \mathrm{Cl}(K)[q]^+.$$

(4) S *est annulé par* I*.*

Démonstration. — (1) est immédiat : si $\overline{\alpha} \in S$ alors $\alpha\mathbb{Z}_K = \pi^k\mathfrak{a}^q$ pour un idéal $\mathfrak{a}$, et nous envoyons $\overline{\alpha}$ sur la classe d'idéaux de $\mathfrak{a}$. Il est clair qu'on aboutit dans $\mathrm{Cl}[q]$, que c'est indépendant du représentant choisi pour $\overline{\alpha}$ (le changement de α en $\alpha\gamma^q$ change $\mathfrak{a}$ en $\gamma\mathfrak{a}$, qui est dans la même classe d'idéaux). Son noyau est l'ensemble des $\overline{\alpha}$ tels que $\alpha\mathbb{Z}_K = \pi^k\gamma^q\mathbb{Z}_K$ pour un certain γ, donc $\alpha = \pi^k\gamma^q u$ pour un $u \in U(K)$, donc $\alpha/\gamma^q \in E$ est tel que $\overline{\alpha/\gamma^q} = \overline{\alpha}$. Finalement l'application est surjective puisque si $\mathfrak{a}^q = \alpha\mathbb{Z}_K$ la classe de $\mathfrak{a}$ est l'image de la classe de α.

(2) Soit $\alpha = \pi^k u \in E$. Puisque $\iota(\pi) = 1 - \zeta^{-1} = -z^{-1}\pi$ et $-\zeta^{-1}$ est une puissance q-ième (comme q et $2p$ sont premiers entre eux) il en résulte que $\iota(\pi)/\pi \in E^q$. De plus si $u \in U(K)$ alors, par le corollaire 1.14, $\iota(u)/u$ est une racine $2p$-ième de l'unité, donc $\iota(u)/u \in E^q$, ce qui montre (2).

(3) Puisque q est impair, 2 est inversible dans $\mathbb{F}_q$, donc pour tout $\mathbb{F}_q[G]$-module M on a $M = M^+ \oplus M^-$. En particulier prendre les parties $+$ et $-$ dans une suite exacte de $\mathbb{F}_q[G]$-modules conserve l'exactitude. Puisque d'après (2) on a $(E/E^q)^+ = E/E^q$ et $(E/E^q)^- = 0$, en prenant la partie $-$ de la suite exacte de (1) on obtient $S^- \simeq \mathrm{Cl}(K)[q]^-$, qui est clairement égal à $\mathrm{Cl}(K)^-[q]$, et en prenant la partie $+$ on obtient la suite exacte de (3).

(4) D'après le théorème de Stickelberger on sait que I_s annule $\mathrm{Cl}(K)$ et donc $\mathrm{Cl}(K)[q]$, et d'après (3) que ε^- annule E/E^q, où

$\varepsilon^- = 1 - \iota$. Puisque $I = \varepsilon^- I_s$ il en résulte que I annule à la fois $\mathrm{Cl}(K)[q]$ et E/E^q, et donc aussi S grâce à la suite exacte de (1). □

Nous revenons maintenant vraiment à la conjecture de Catalan. Soit donc à nouveau p et q des nombres premiers impairs distincts et x et y des entiers non nuls tels que $x^p - y^q = 1$. Nous avons déjà vu et utilisé le fait qu'il existe un idéal entier $\mathfrak{b}$ tel que $((x-\zeta)/(1-\zeta))\mathbb{Z}_K = \mathfrak{b}^q$.

Lemme 6.10

(1) *La classe de $x - \zeta$ appartient à S.*
(2) *Si de plus $q \nmid h_p^-$, la classe de $(x-\zeta)^{1-\iota}$ dans S est triviale.*

Démonstration. — (1) résulte de $((x-\zeta)/(1-\zeta))\mathbb{Z}_K = \mathfrak{b}^q$ et de la définition de S. Pour (2), d'après les remarques précédant le lemme 6.9 on sait que $|\mathrm{Cl}(K)^-| \mid h_p^-$, donc si $q \nmid h_p^-$ *a fortiori* $q \nmid |\mathrm{Cl}(K)^-|$, donc $\mathrm{Cl}(K)^-[q] = 0$. D'après le lemme 6.9 on en déduit que $S^- = 0$, ce qui démontre (2) puisque la classe de $(x-\zeta)^{1-\iota}$ appartient à S^-. □

6.5. Démonstration du théorème. — Pour démontrer le deuxième théorème de Mihăilescu nous devrons démontrer la proposition technique mais essentielle suivante, donc la démonstration est assez longue. Il est clair qu'elle sera en contradiction avec le lemme 6.10 (2) quand $q \nmid h_p^-$.

Proposition 6.11. — *Si p et q sont des nombres premiers et x et y des entiers non nuls tels que $x^p - y^q = 1$ alors la classe de $(x-\zeta)^{1-\iota}$ dans S est non triviale.*

Démonstration. — Supposons le contraire, en d'autres termes que $(x-\zeta)^{1-\iota} \in K^{*q}$, et donc qu'il existe $\alpha \in K^*$ tel que $(x-\zeta)/(x-\zeta^{-1}) = \alpha^q$. Posons $\mu = (x-1)/(1-\zeta) = (x-1)/\pi$. D'après le théorème de Cassels nous savons que $x \equiv 1 \pmod{p^{q-1}}$, donc $v_{\mathfrak{p}}(\mu) \geqslant (p-1)(q-1) - 1 \geqslant 4$ puisque p et q sont des premiers impairs distincts. De plus $1 + \mu = (x-\zeta)/(1-\zeta)$, donc il existe $\beta \in K^*$ tel que $(1+\mu)/(1+\overline{\mu}) = -\zeta^{-1}\alpha^q = \beta^q$, puisque $-\zeta^{-1}$ est une puissance q-ième. Plus précisément, si $r \in \mathbb{Z}$ est tel que $qr \equiv -1 \pmod{2p}$ alors $-\zeta^{-1} = (-\zeta)^{qr}$, donc on peut choisir $\beta = (-\zeta)^r\alpha = -\zeta^r\alpha$.

J'affirme que $\beta \equiv 1 \pmod{\mathfrak{p}\mathbb{Z}_\mathfrak{p}}$ (nous devons ici introduire un peu de p-adique, sans définitions, mais vraiment en quantité minimale) : en effet, puisque $v_\mathfrak{p}(\mu) \geqslant 1$ et $v_\mathfrak{p}(\overline{\mu}) \geqslant 1$ on a $\beta^q \equiv 1 \pmod{\mathfrak{p}\mathbb{Z}_\mathfrak{p}}$, et en particulier β est premier à $\mathfrak{p}$. Puisque $\mathbb{Z}_K/\mathfrak{p} \simeq \mathbb{Z}/p\mathbb{Z}$ il en résulte qu'il existe $b \in \mathbb{Z}$ tel que $\beta \equiv b \pmod{\mathfrak{p}\mathbb{Z}_\mathfrak{p}}$, et donc $b^q \equiv 1 \pmod{\mathfrak{p}}$. De plus $\beta\overline{\beta} = 1$, donc $b^2 \equiv 1 \pmod{\mathfrak{p}}$. Puisque q et 2 sont premiers entre eux il en résulte que $\beta \equiv b \equiv 1 \pmod{\mathfrak{p}\mathbb{Z}_\mathfrak{p}}$, comme annoncé.

Dans une extension convenable L de K soit ρ_1 tel que $\rho_1^q = 1+\mu$. Si on pose $\rho_2 = \rho_1/\beta$ il est clair que $\rho_2^q = (1+\mu)/\beta^q = 1+\overline{\mu}$. Finalement, posons

$$\eta = (\rho_1 + \zeta^r\rho_2)^q,$$

où r est comme ci-dessus. Puisque

$$\eta = \rho_2^q(\rho_1/\rho_2 + \zeta^r)^q = (1+\overline{\mu})(\beta+\zeta^r)^q,$$

il est clair que $\eta \in K$. De plus

$$\rho_1^q + (\zeta^r\rho_2)^q = 1 + \mu + \zeta^{-1}(1+\overline{\mu}) = \frac{x-\zeta}{1-\zeta} + \frac{x-\zeta^{-1}}{\zeta-1} = \zeta^{-1}\frac{1-\zeta^2}{1-\zeta},$$

qui est une unité. Puisque $(\rho_1^q + (\zeta^r\rho_2)^q)/\eta$ est un entier algébrique, il en résulte que η est aussi une unité, en d'autres termes que $\eta \in U(K)$. En particulier $\mathcal{N}_{K/\mathbb{Q}}(\eta) = \pm 1$, et puisque les plongements de K dans $\mathbb{C}$ vont par paires car il n'y en a aucun de réel toute norme est positive ou nulle, donc $\mathcal{N}_{K/\mathbb{Q}}(\eta) = 1$.

Puisque $v_\mathfrak{p}(\mu) \geqslant 4$ et $p \neq q$, le développement en série entière de $(1+\mu)^{1/q}$ converge $\mathfrak{p}$-adiquement dans $\mathbb{Q}_p(\zeta_p)$ (il n'y a pas besoin de savoir grand-chose sur les p-adiques pour comprendre le raisonnement qui va suivre). Nous choisissons donc $L = \mathbb{Q}_p(\zeta_p)$ et nous *définissons* ρ_1 par ce développement en série, et donc en particulier on a $\rho_1 \equiv 1 \pmod{\mathfrak{p}\mathbb{Z}_\mathfrak{p}}$. J'affirme que ρ_2 est égal à la somme du développement en série entière de $(1+\overline{\mu})^{1/q}$, qui bien entendu converge également. En effet, si on définit ρ_2 de cette manière on a $\rho_1/\rho_2 \equiv 1 \pmod{\mathfrak{p}}$ et $(\rho_1/\rho_2)^q = (1+\mu)/(1+\overline{\mu}) = \beta^q$, donc $\rho_1/\rho_2 = \varepsilon\beta$ pour une certaine racine q-ième de l'unité ε dans $\mathbb{Q}_p(\zeta_p)$. Puisqu'on a vu ci-dessus que $\beta \equiv 1 \pmod{\mathfrak{p}}$, et puisque $\rho_1/\rho_2 \equiv 1 \pmod{\mathfrak{p}\mathbb{Z}_\mathfrak{p}}$ par construction, il en résulte que $\varepsilon \equiv 1 \pmod{\mathfrak{p}\mathbb{Z}_\mathfrak{p}}$. Toutefois il est facile de montrer que si $p \not\equiv 1 \pmod{q}$ la seule racine q-ième de l'unité dans $\mathbb{Q}_p(\zeta_p)$ est égale à 1, donc $\rho_1/\rho_2 = \beta$ comme annoncé. D'autre part, si $p \equiv 1 \pmod{q}$ il existe maintenant q racines q-ièmes de l'unité

distinctes ε dans $\mathbb{Q}_p(\zeta_p)$, qui relèvent les racines q-ièmes de l'unité de $\mathbb{Z}_\mathfrak{p}/\mathfrak{p}$, et qui sont donc distinctes modulo $\mathfrak{p}$. Il en résulte que le seul ε tel que $\varepsilon \equiv 1 \pmod{\mathfrak{p}\mathbb{Z}_\mathfrak{p}}$ est $\varepsilon = 1$, d'où la conclusion également dans ce cas.

Ainsi, en utilisant les définitions de ρ_1 et ρ_2 par des séries entières nous posons $u = \rho_1 + \zeta^r \rho_2$, en se rappelant que par définition $\eta = u^q \in U(K)$. Notons que $\overline{\mu}/\mu = (1-\zeta)/(1-\zeta^{-1}) = -\zeta$. Ainsi, en utilisant les développements en série donnant ρ_1 et ρ_2 on a

$$\begin{aligned} u &\equiv 1 + \frac{\mu}{q} + \zeta^r \left(1 + \frac{\overline{\mu}}{q}\right) \equiv (1+\zeta^r)\left(1 + \frac{\mu + \zeta^r \overline{\mu}}{q(1+\zeta^r)}\right) \\ &\equiv (1+\zeta^r)\left(1 + \mu \frac{1-\zeta^{r+1}}{q(1+\zeta^r)}\right) \pmod{\mu^2 \mathbb{Z}_\mathfrak{p}} \end{aligned}$$

avec des notations évidentes. Noter que $1 + \zeta^r = (1-\zeta^{2r})/(1-\zeta^r)$ est une unité, et est donc de norme 1. D'où, en prenant les normes on obtient

$$\mathcal{N}_{K_\mathfrak{p}/\mathbb{Q}_p}(u) \equiv 1 + \frac{x-1}{q} \sum_{\zeta \neq 1} \frac{1-\zeta^{r+1}}{(1-\zeta)(1+\zeta^r)} \pmod{\mu^2},$$

où la somme est de manière implicite sur toutes les racines p-ièmes de l'unité différentes de 1. Noter qu'il y a ici un léger abus de notation puisque μ dépend de ζ, mais la valuation $\mathfrak{p}$-adique de μ n'en dépend pas.

Puisque $\zeta \equiv 1 \pmod{\mathfrak{p}}$ nous avons $(1-\zeta^{r+1})/(1-\zeta) = \sum_{0 \leqslant j \leqslant r} \zeta^j \equiv (r+1) \pmod{\mathfrak{p}}$, et $1 + \zeta^r \equiv 2 \pmod{\mathfrak{p}}$, donc

$$\mathcal{N}_{K_\mathfrak{p}/\mathbb{Q}_p}(u) \equiv 1 + \frac{x-1}{q} \frac{(r+1)(p-1)}{2} \pmod{(x-1)\mathfrak{p}\mathbb{Z}_\mathfrak{p}}$$

puisque l'on remarque que $v_\mathfrak{p}(\mu^2) = 2(v_\mathfrak{p}(x-1)-1) \geqslant v_p(x-1)+1$, ceci étant équivalent à $v_\mathfrak{p}(x-1) \geqslant 3$. En élevant à la puissance q et en remarquant que $v_\mathfrak{p}((x-1)^j) \geqslant v_\mathfrak{p}(\mathfrak{p}(x-1))$ pour $j \geqslant 2$ nous avons donc

$$\begin{aligned} 1 = \mathcal{N}_{K/\mathbb{Q}}(\eta) &= \mathcal{N}_{K_\mathfrak{p}/\mathbb{Q}_p}(u)^q \\ &\equiv 1 + (x-1)(r+1)(p-1)/2 \pmod{(x-1)\mathfrak{p}\mathbb{Z}_\mathfrak{p}}, \end{aligned}$$

donc $\mathfrak{p} \mid r+1$ c'est-à-dire $r \equiv -1 \pmod{p}$ puisque $r \in \mathbb{Z}$. Comme par définition $qr \equiv -1 \pmod{p}$ il en résulte que $q \equiv 1 \pmod{p}$. Donc si $q \not\equiv 1 \pmod{p}$ nous avons obtenu une contradiction. Pour le reste de la démonstration nous pouvons donc supposer que $q \equiv 1$

(mod p), en d'autres termes que l'on peut choisir $r=-1$. Nous allons maintenant calculer le développement de u modulo μ^3 au lieu de μ^2. En remarquant que $\mu+\zeta^{-1}\overline{\mu}=0$ on a donc

$$\begin{aligned} u &\equiv 1+\frac{\mu}{q}+\binom{1/q}{2}\mu^2+\zeta^{-1}\left(1+\frac{\overline{\mu}}{q}+\binom{1/q}{2}\overline{\mu}^2\right)\\ &\equiv (1+\zeta^{-1})\left(1+\frac{(1-q)(x-1)^2}{2q^2}\frac{\zeta}{(1-\zeta)^2}\right) \pmod{\mu^3}. \end{aligned}$$

Prenant les normes et en raisonnant comme ci-dessus on obtient

$$\begin{aligned} \mathcal{N}_{K_{\mathfrak{p}}/\mathbb{Q}_p}(u) &\equiv 1+\frac{(1-q)(x-1)^2}{2q^2}\sum_{\zeta\neq 1}\frac{\zeta}{(1-\zeta)^2}\\ &\equiv 1+\frac{(q-1)(p^2-1)(x-1)^2}{24q^2} \pmod{\mu^3}, \end{aligned}$$

(le calcul des sommes sur les racines de l'unité qui interviennent ci-dessus est un joli exercice laissé au lecteur). Donc à nouveau en élevant à la puissance q et en notant que $v_{\mathfrak{p}}((x-1)^4)\geqslant v_{\mathfrak{p}}(\mu^3)$ on obtient

$$1\equiv 1+\frac{(q-1)(p^2-1)(x-1)^2}{24q} \pmod{\mu^3}.$$

On a donc $v_{\mathfrak{p}}((q-1)(x-1)^2/24)\geqslant v_{\mathfrak{p}}(\mu^3)$, en d'autres termes

$$v_{\mathfrak{p}}((q-1)/3)+2v_{\mathfrak{p}}(x-1)\geqslant 3(v_{\mathfrak{p}}(x-1)-1),$$

ce qui implique $v_{\mathfrak{p}}((q-1)/3)\geqslant v_{\mathfrak{p}}(x-1)-3$. Or d'après le théorème de Cassels nous savons que $x\equiv 1 \pmod{p^{q-1}}$. Il en résulte que $v_{\mathfrak{p}}(x-1)\geqslant (p-1)(q-1)$, et nous en déduisons donc que $(p-1)v_p((q-1)/3)\geqslant (p-1)(q-1)-3$, et donc que $v_p(q-1)\geqslant (q-1)+v_p(3)-3/(p-1)$. Puisque pour tout p impair on a $v_p(3)-3/(p-1)>-1$, il en résulte que $v_p(q-1)\geqslant q-1$, ce qui est trivialement impossible puisque le membre de droite est bien plus grand, et ce qui termine la démonstration de cette proposition très technique. □

Théorème 6.12 **(Mihăilescu).** — *Soient p et q des nombres premiers impairs distincts. Si $p\nmid h_q^-$ ou $q\nmid h_p^-$ l'équation $x^p-y^q=1$ n'a pas de solutions avec $xy\neq 0$.*

Démonstration. — C'est maintenant évident : par symétrie on peut supposer que $q\nmid h_p^-$, et alors le lemme 6.10 (2) et la proposition ci-dessus se contredisent. □

Corollaire 6.13. — *Si p et q sont des nombres premiers distincts et si p ou q est inférieur ou égal à 43 l'équation $x^p - y^q = 1$ n'a pas de solutions avec $xy \neq 0$.*

Démonstration. — Grâce au théorème ci-dessus il suffit de vérifier que pour tout p et q tels que $\min(p, q) \leqslant 43$ on a $p \nmid h_q^-$ ou $q \nmid h_p^-$. Nous devons tout d'abord calculer h_p^- pour de petites valeurs de p, ce qui se fait très facilement comme nous l'avons expliqué ci-dessus. Sous forme complètement factorisée on trouve que $h_p^- = 1$ pour $p \leqslant 19$, et que $h_{23}^- = 3$, $h_{29}^- = 2^3$, $h_{31}^- = 3^2$, $h_{37}^- = 37$ (qui provient du fait que 37 est un nombre premier irrégulier), $h_{41}^- = 11^2$ et $h_{43}^- = 211$. Par symétrie on peut supposer que $3 \leqslant p < q$. De la liste ci-dessus on déduit que, en dehors du cas $p = 43$ on a $q \nmid h_p^-$ puisque tous les diviseurs premiers de h_p^- sont inférieurs ou égaux à p. Pour $p = 43$ on a également $q \mid h_{43}^-$ pour $q = 211$, et nous devons donc vérifier que $43 \nmid h_{211}^-$, ce qui est bien le cas puisqu'on calcule que

$$h_{211}^- = 3^2 \cdot 7^2 \cdot 41 \cdot 71 \cdot 181 \cdot 281 \cdot 421 \cdot 1051 \cdot 12251 \cdot 113981701 \cdot 4343510221$$

(le fait qu'il y ait beaucoup de petits facteurs premiers n'est pas un hasard, et bien entendu nous n'avons pas besoin de la factorisation complète simplement pour vérifier que $43 \nmid h_{211}^-$). □

Remarques

(1) La raison pour laquelle nous nous arrêtons à 43 est que pour $p = 47$ et $q = 139$ on peut vérifier que $q \mid h_p^-$ et $p \mid h_q^-$, donc le théorème n'est pas applicable dans ce cas. De toutes façons la démonstration complète n'utilise ce théorème que pour $\min(p, q) \leqslant 11$.

(2) Nous avons maintenant deux critères différents nous permettant de conclure que l'équation de Catalan n'a pas de solutions non nulles : les théorèmes 5.4 et 6.12. Il est très probable qu'il n'existe pas de couples (p, q) satisfaisant les deux, mais ceci n'est pas démontré. Toutefois, grâce au théorème de Baker et successeurs sur les formes linéaires en logarithmes, il n'est pas difficile de montrer que les deux théorèmes ci-dessus suffisent à démontrer la conjecture de Catalan complète, moyennant une quantité finie et pas complètement déraisonnable de calculs sur ordinateur. Ceux-ci ont d'ailleurs été commencés, mais ils n'ont pas été achevés, tout d'abord parce qu'ils seraient très longs, mais surtout parce que grâce aux deux autres théorèmes

de Mihăilescu (qui évitent même tout recours aux formes linéaires de logarithmes) ils ne sont pas nécessaires.

7. Le troisième théorème de Mihăilescu : $p < 4q^2$ et $q < 4p^2$

Bien qu'assez longue, ceci n'est pas vraiment une partie importante de la démonstration de la conjecture de Catalan, et n'a en fait été trouvée qu'après. Son seul avantage est d'éviter complètement l'utilisation de formes linéaires en logarithmes et des calculs assez longs sur ordinateur.

Nous gardons les notations ci-dessus, et pour simplifier nous écrirons $\mathcal{N}$ à la place de $\mathcal{N}_{K/\mathbb{Q}}$. Si $u \in V$ nous noterons $[u]$ sa classe dans $S = V/K^{*q}$. Rappelons que d'après le lemme 6.10, si $x^p - y^q = 1$ on a $[x - \zeta_p] \in S$.

Définition 7.1. — Nous appellerons X l'annulateur de $[x - \zeta_p]$ dans $\mathbb{Z}[G]$, en d'autres termes l'ensemble des $\theta \in \mathbb{Z}[G]$ tels que $(x - \zeta_p)^\theta = \alpha^q$ pour un $\alpha \in K^*$.

Il est clair que X est un idéal de $\mathbb{Z}[G]$.

Lemme 7.2. — *L'application qui à $\theta \in X$ associe $\alpha \in K^*$ tel que $(x - \zeta_p)^\theta = \alpha^q$ est bien définie et est un homomorphisme de groupes injectif.*

Démonstration. — Puisque $K = \mathbb{Q}(\zeta_p)$ ne contient aucune racine q-ième de l'unité autre que 1 il est clair que l'application est bien définie, et il est évident que c'est un homomorphisme de groupes du groupe additif X dans le groupe multiplicatif K^*. Montrons qu'il est injectif : soit $\theta \in X$ tel que $(x - \zeta_p)^\theta = 1$. Pour tout $\sigma \in G$ on a donc $(x - \sigma(\zeta_p))^\theta = \sigma(1) = 1$, et donc $\mathcal{N}(x - \zeta_p)^\theta = 1$. Si $\theta = \sum_{\sigma \in G} a_\sigma \sigma$, puisque $\mathcal{N}(x - \zeta_p) \in \mathbb{Z}$, il en résulte que $\mathcal{N}(x - \zeta_p)^s = 1$, où $s = \sum_{\sigma \in G} a_\sigma$. Or nous savons que $(x - \zeta_p)/(1 - \zeta_p) \in \mathbb{Z}_K$, et puisque $\mathcal{N}(1 - \zeta_p) = p$ il en résulte que $p \mid \mathcal{N}(x - \zeta_p)$, et en particulier $\mathcal{N}(x - \zeta_p) \geqslant p$, et est donc différent de 1. Nous avons donc $s = \sum_{\sigma \in G} a_\sigma = 0$, donc nous pouvons écrire

$$1 = \frac{(x - \zeta_p)^\theta}{(1 - \zeta_p)^s} = \prod_{\sigma \in G} \left(\frac{x - \sigma(\zeta_p)}{1 - \zeta_p} \right)^{a_\sigma},$$

et puisque $(1-\sigma(\zeta_p))/(1-\zeta_p)$ est une unité pour tout $\sigma \in G$ il en résulte que $\prod_{\sigma\in G}\sigma(\beta)^{a_\sigma}$ est une unité, où nous avons posé comme d'habitude $\beta = (x-\zeta_p)/(1-\zeta_p)$. Or d'après le lemme 3.8 nous savons que les idéaux $\mathfrak{b}_\sigma = \sigma(\beta)\mathbb{Z}_K$ sont entiers et premiers entre eux deux à deux. Puisque $\prod_{\sigma\in G}\mathfrak{b}_\sigma^{a_\sigma} = \mathbb{Z}_K$ il en résulte que $a_\sigma = 0$ pour tout $\sigma \in G$, en d'autres termes que $\theta = 0$, ce qui démontre l'injectivité. □

Proposition 7.3. — *Supposons que* $\min(p,q) \geqslant 11$. *Soit* $\theta = \sum_{\sigma\in G} a_\sigma\sigma \in X \cap (1-\iota)\mathbb{Z}[G]$, *soit* $\alpha \in K^*$ *tel que* $(x-\zeta_p)^\theta = \alpha^q$, *et supposons que* $\|\theta\| = \sum_{\sigma\in G}|a_\sigma| \leqslant 3q/(p-1)$. *Alors pour tout* $\tau \in G$ *on a*

$$|\operatorname{Arg}(\tau(\alpha)^q)| \leqslant \frac{\|\theta\|}{|x|-1} \quad et \quad |\operatorname{Arg}(\tau(\alpha))| > \frac{\pi}{q},$$

où $\operatorname{Arg}(z)$ *désigne la détermination principale de l'argument, c'est-à-dire telle que* $-\pi < \operatorname{Arg}(z) \leqslant \pi$.

Démonstration. — Puisque $\theta \in (1-\iota)\mathbb{Z}[G]$ on a $\iota\theta = -\theta$, donc pour tout $\tau \in G$

$$|\tau(\alpha)|^{2q} = |(x-\zeta_p)^{\tau\theta}|^2 = (x-\zeta_p)^{\tau\theta}(x-\zeta_p)^{\tau\iota\theta} = (x-\zeta_p)^{\tau\theta}(x-\zeta_p)^{-\tau\theta} = 1,$$

et donc $|\tau(\alpha)| = 1$. Pour la même raison on a $a_{\iota\sigma} = -a_\sigma$, donc $s = \sum_{\sigma\in G} a_\sigma = 0$. Il en résulte que

$$\begin{aligned}\alpha^q = (x-\zeta_p)^\theta &= \prod_{\sigma\in G}(x-\sigma(\zeta_p))^{a_\sigma} \\ &= x^s\prod_{\sigma\in G}(1-\sigma(\zeta_p)/x)^{a_\sigma} = \prod_{\sigma\in G}(1-\sigma(\zeta_p)/x)^{a_\sigma}.\end{aligned}$$

Fixons un $\tau \in G$ et posons $\zeta = \tau(\zeta_p)$. Nous avons donc

$$\tau(\alpha)^q = \prod_{\sigma\in G}(1-\sigma(\zeta)/x)^{a_\sigma}.$$

Notons Log la détermination principale du logarithme complexe, donc telle que $\operatorname{Log}(z) = \log(|z|) + i\operatorname{Arg}(z)$, et soit f *une* détermination du logarithme, ce qui fait que $f(z) - \operatorname{Log}(z) \in 2i\pi\mathbb{Z}$. On a donc

$$\sum_{\sigma\in G} a_\sigma \operatorname{Log}(1-\sigma(\zeta)/x) = f(\tau(\alpha)^q).$$

Comme $|x| > 1$ nous avons

$$|\operatorname{Log}(1-\sigma(\zeta)/x)| = \left|\sum_{k\geqslant 1}\sigma(\zeta)^k/(kx^k)\right| \leqslant \sum_{k\geqslant 1}|x|^{-k} = 1/(|x|-1).$$

Notons que pour tout z on a $f(z)=\log(|z|)+i(\mathrm{Arg}(z)+2k\pi)$ pour un certain $k\in\mathbb{Z}$, donc $|f(z)|\geqslant|\mathrm{Arg}(z)+2k\pi|$. Si $k=0$ cela donne $|f(z)|\geqslant|\mathrm{Arg}(z)|$, et si $k\neq0$ cela donne

$$|f(z)|\geqslant|2k\pi|-|\mathrm{Arg}(z)|\geqslant(2|k|-1)\pi\geqslant\pi\geqslant|\mathrm{Arg}(z)|$$

puisque $|\mathrm{Arg}(z)|\leqslant\pi$, ce qui montre qu'on a toujours $|f(z)|\geqslant|\mathrm{Arg}(z)|$. Ainsi

$$|\mathrm{Arg}(\tau(\alpha)^q)|\leqslant|f(\tau(\alpha)^q)|\leqslant\frac{1}{|x|-1}\sum_{\sigma\in G}|a_\sigma|\leqslant\frac{\|\theta\|}{|x|-1},$$

ce qui démontre la première inégalité. Supposons maintenant par l'absurde que $|\mathrm{Arg}(\tau(\alpha))|\leqslant\pi/q$. On vérifie immédiatement que dans ce cas on a $|\mathrm{Arg}(\tau(\alpha)^q)|=q|\mathrm{Arg}(\tau(\alpha))|$, et donc que $|\mathrm{Arg}(\tau(\alpha))|\leqslant\|\theta\|/(q(|x|-1))$. De plus si on pose $\phi=\mathrm{Arg}(\tau(\alpha))$, comme $|\tau(\alpha)|=1$ on a $\tau(\alpha)=\cos(\phi)+i\sin(\phi)$, donc

$$\tau(\alpha)-1=2\sin(\phi/2)(-\sin(\phi/2)+i\cos(\phi/2)),$$

d'où

$$|\tau(\alpha)-1|=2|\sin(\phi/2)|\leqslant|\phi|=|\mathrm{Arg}(\tau(\alpha))|.$$

Nous avons donc $|\tau(\alpha)-1|\leqslant\|\theta\|/(q(|x|-1))$, et donc en prenant le produit sur tous les $\sigma\in G$ on obtient

$$|\mathcal{N}(\alpha-1)|=|\tau(\alpha)-1|^2\prod_{\substack{\sigma\in G\\ \sigma\neq\tau,\ \sigma\neq\iota\tau}}|\sigma(\alpha)-1|\leqslant\left(\frac{\|\theta\|}{q(|x|-1)}\right)^2 2^{p-3},$$

puisque $|\sigma(\alpha)-1|\leqslant|\sigma(\alpha)|+1=2$.

Posons $\theta^+=\sum_{\sigma\in G,\ a_\sigma\geqslant0}a_\sigma\sigma$ et $\theta^-=\sum_{\sigma\in G,\ a_\sigma\leqslant0}(-a_\sigma)\sigma$, ce qui fait que $\theta=\theta^+-\theta^-$. Puisque $a_{\iota\sigma}=-a_\sigma$ on a $\iota\theta^+=\theta^-$ donc $\alpha^q=(x-\zeta_p)^\theta=\beta/\iota(\beta)$, où $\beta=(x-\zeta_p)^{\theta^+}$ est un *entier* algébrique. Or

$$\begin{aligned}\mathcal{N}(\beta^2)&=\mathcal{N}(\beta)\mathcal{N}(\iota(\beta))=\mathcal{N}(\beta\iota(\beta))\\&=\mathcal{N}_{K/Q}\Big(\prod_{\sigma\in G}(x-\sigma(\zeta_p))^{|a_\sigma|}\Big)\leqslant(|x|+1)^{\|\theta\|(p-1)},\end{aligned}$$

et donc $\mathcal{N}(\beta)\leqslant(|x|+1)^{\|\theta\|(p-1)/2}$. Écrivons $\alpha\mathbb{Z}_K=\mathfrak{a}/\mathfrak{b}$, où $\mathfrak{a}$ et $\mathfrak{b}$ sont des idéaux entiers premiers entre eux. On a $\mathfrak{a}^q/\mathfrak{b}^q=(\beta/\iota(\beta))\mathbb{Z}_K$, donc $\mathfrak{a}^q\iota(\beta)=\mathfrak{b}^q\beta$, et puisque $\mathfrak{a}$ et $\mathfrak{b}$ sont premiers entre eux il en résulte que $\mathfrak{b}^q\mid\iota(\beta)\mathbb{Z}_K$. En particulier $\mathcal{N}(\mathfrak{b}^q)\leqslant\mathcal{N}(\iota(\beta))=\mathcal{N}(\beta)$, donc $\mathcal{N}(\mathfrak{b})\leqslant(|x|+1)^{\|\theta\|(p-1)/(2q)}$. Or d'après le lemme 7.2, puisque

nous avons choisi $\theta \neq 0$ nous avons $\alpha \neq 1$. Puisque $\mathfrak{b}\alpha = \mathfrak{a}$ et $\mathfrak{b}$ sont des idéaux entiers il en résulte que $\mathfrak{a}_1 = \mathfrak{b}(\alpha - 1) = \{x\alpha - x,\ x \in \mathfrak{b}\}$ est aussi un idéal entier, et donc que $1 \leqslant \mathcal{N}(\mathfrak{a}_1) = \mathcal{N}(\mathfrak{b})|\mathcal{N}(\alpha - 1)|$. En combinant toutes les inégalités obtenues ci-dessus on a donc

$$1 \leqslant (|x| + 1)^{\|\theta\|(p-1)/(2q)} \left(\frac{\|\theta\|}{q(|x| - 1)}\right)^2 2^{p-3}.$$

Cette égalité va nous donner une contradiction. Puisque $|x| \geqslant 6$ (voir ci-dessous), on a $(1 + |x|)^2 \leqslant 2(|x| - 1)^2$, donc

$$(1 + |x|)^{2-\|\theta\|(p-1)/(2q)} \leqslant 2^{p-1}(\|\theta\|/q)^2,$$

et donc d'après l'hypothèse de la proposition $\|\theta\| \leqslant 3q/(p - 1)$ et le fait que $p \geqslant 5$ on en déduit que

$$(1 + |x|)^{1/2} \leqslant 2^{p-1}(3/(p - 1))^2 \leqslant 2^{p-1} = 4^{(p-1)/2}.$$

Or d'après la remarque que nous avons faite après la démonstration du résultat de Hyrrö (corollaire 3.4), nous savons que $|x| \geqslant q^{p-1} + q$ (ce qui montre au passage que $|x| \geqslant 6$). Il en résulte que $q^{(p-1)/2} < (1 + |x|)^{1/2} \leqslant 4^{(p-1)/2}$, ce qui est absurde puisque par hypothèse $q \geqslant 5$. □

Pour démontrer le résultat important suivant, à savoir la proposition 7.6, nous avons besoin de plusieurs lemmes.

Lemme 7.4. — *Le nombre de k-uplets d'entiers positifs ou nuls λ_i tels que $\sum_{1 \leqslant i \leqslant k} \lambda_i \leqslant s$ est égal à $\binom{s+k}{s} = \binom{s+k}{k}$.*

Démonstration. — C'est classique : il est facile de voir que l'application qui à $(\lambda_i)_{1 \leqslant i \leqslant k}$ associe l'ensemble des $\sum_{1 \leqslant i \leqslant j}(\lambda_i + 1)$ pour $1 \leqslant j \leqslant k$ est une bijection de l'ensemble des k-uplets de somme s dans l'ensemble des parties de $[1, s + k]$ ayant k éléments. □

Lemme 7.5. — *Supposons que* $\min(p, q) \geqslant 11$ *et que $q > 4p^2$. Il existe* au moins $q + 1$ *éléments $\theta \in I$ tels que $\|\theta\| \leqslant 3q/(2(p - 1))$.*

Démonstration. — Rappelons que le lemme 6.6 nous dit que I a une base formée d'éléments e_i pour $1 \leqslant i \leqslant (p-1)/2$ tels que $\|e_i\| = p-1$. Considérons l'ensemble des $\theta = \sum_{1 \leqslant i \leqslant (p-1)/2} \lambda_i e_i$, où $\lambda_i \in \mathbb{Z}_{\geqslant 0}$ et $\sum_i \lambda_i \leqslant s = \lfloor 3q/(2(p - 1)^2) \rfloor$. Pour un tel θ on a

$$\|\theta\| \leqslant (p - 1) \sum_i \lambda_i \leqslant (p - 1)s \leqslant 3q/(2(p - 1)).$$

D'après le lemme ci-dessus le nombre de tels θ est égal à $\binom{s+(p-1)/2}{s}$. Puisque nous pouvons aussi considérer les $-\theta$ quand $\theta \neq 0$, il en résulte que nous construisons de cette manière $2\binom{s+(p-1)/2}{s}-1$ éléments distincts θ. Montrons que ce nombre est supérieur ou égal à $q+1$. On note tout d'abord que

$$\frac{\binom{s+(p-1)/2}{s}}{p^2(s+1)} = \frac{\prod_{2\leqslant j\leqslant (p-1)/2}(s+j)}{p^2((p-1)/2)!},$$

qui est évidemment une fonction croissante de s. Puisque $q \geqslant 4p^2 \geqslant 4(p-1)^2$ on a $s \geqslant 6$, et donc $\binom{s+(p-1)/2}{s}/(s+1) \geqslant \binom{6+(p-1)/2}{6}/(7p^2) = f(p)$, disons. On calcule que $f(p)/f(p-2) = (p+11)(p-2)^2/(p^2(p-1))$, et on vérifie immédiatement que ceci est plus grand que 1 dès que $p \geqslant 5$, ce qui montre que $f(p)$ est une fonction croissante de p. En particulier on a $f(11) = 6/11 > 1/3$. Ainsi, si $p \geqslant 11$ on a

$$\binom{s+(p-1)/2}{s} > \frac{p^2(s+1)}{2} > \frac{p^2 q}{2(p-1)^2} \geqslant \frac{q+2}{2},$$

la dernière égalité étant évidente puisque $q > 4p^2$. Nous avons donc bien construit au moins $q+1$ éléments θ distincts qui conviennent. □

Proposition 7.6. — *Supposons que* $\min(p,q) \geqslant 11$ *et que* $q > 4p^2$. *Pour tout* $\tau \in G$ *il existe* $\theta \in I$ *non nul tel que* $\|\theta\| \leqslant 3q/(p-1)$ *et tel que* $|\operatorname{Arg}(\tau(\alpha))| \leqslant \pi/q$, *où* $\alpha \in K^*$ *est l'élément tel que* $(x-\zeta_p)^\theta = \alpha^q$.

Démonstration. — D'après le lemme ci-dessus il existe au moins $q+1$ éléments $\theta \in I$ tels que $\|\theta\| \leqslant 3q/(2(p-1))$. Pour un tel θ il existe un unique α tel que $(x-\zeta_p)^\theta = \alpha^q$. Puisque $\theta \in I \subset (1-\iota)\mathbb{Z}[G]$, d'après la première inégalité de la proposition 7.3 on en déduit que $|\operatorname{Arg}(\tau(\alpha)^q)| \leqslant \|\theta\|/(|x|-1)$. Or il existe un entier k tel que $\operatorname{Arg}(\tau(\alpha)^q) = q\operatorname{Arg}(\tau(\alpha)) + 2k\pi$, d'où $2k\pi = -q\operatorname{Arg}(\tau(\alpha)) + \operatorname{Arg}(\tau(\alpha)^q)$, et puisque Arg est toujours entre $-\pi$ et π on a $2|k|\pi < (q+1)\pi$. Il en résulte que $2|k| \leqslant q$ et donc que $|k| \leqslant (q-1)/2$ puisque q est impair. Comme il y a exactement q entiers k tels que $-(q-1)/2 \leqslant k \leqslant (q-1)/2$ et que nous avons au moins $q+1$ éléments θ distincts qui conviennent, il résulte du principe des tiroirs qu'il existe θ_1 et θ_2 distincts qui conviennent et qui de plus correspondent à la même valeur de k. Pour $i = 1$ et 2 écrivons $(x-\zeta_p)^{\theta_i} = \alpha_i^q$ et $\theta = \theta_1 - \theta_2$, ce qui fait que $(x-\zeta_p)^\theta = \alpha^q$,

où $\alpha = \alpha_1/\alpha_2$, et évidemment $\|\theta\| \leqslant \|\theta_1\| + \|\theta_2\| \leqslant 3q/(p-1)$. Puisque

$$\operatorname{Arg}(\tau(\alpha_i)) = \frac{\operatorname{Arg}(\tau(\alpha_i)^q)}{q} - \frac{2k\pi}{q}$$

on a

$$|\operatorname{Arg}(\tau(\alpha_2)) - \operatorname{Arg}(\tau(\alpha_1))| = \frac{1}{q}|\operatorname{Arg}(\tau(\alpha_2)^q) - \operatorname{Arg}(\tau(\alpha_1)^q)| \leqslant 2\pi/q < \pi,$$

donc $\operatorname{Arg}(\tau(\alpha)) = \operatorname{Arg}(\tau(\alpha_2)) - \operatorname{Arg}(\tau(\alpha_1))$. En utilisant les inégalités $\|\theta\| \leqslant 3q/(2(p-1))$ et $|x| - 1 > q^{p-1}$ on a donc

$$\begin{aligned}
|\operatorname{Arg}(\tau(\alpha))| &= |\operatorname{Arg}(\tau(\alpha_2)) - \operatorname{Arg}(\tau(\alpha_1))| \\
&\leqslant |\operatorname{Arg}(\tau(\alpha_2)) + 2k\pi/q| + |\operatorname{Arg}(\tau(\alpha_1)) + 2k\pi/q| \\
&\leqslant (|\operatorname{Arg}(\tau(\alpha_2)^q)| + |\operatorname{Arg}(\tau(\alpha_1)^q)|)/q \\
&\leqslant 2\|\theta\|/(q(|x|-1)) \leqslant 3/((p-1)q^{p-1}) < \pi/q,
\end{aligned}$$

ce qui démontre la proposition. □

Il est maintenant immédiat de démontrer le troisième théorème de Mihăilescu.

Théorème 7.7. — *Soient p et q des nombres premiers impairs distincts tels que $\min(p,q) \geqslant 11$, et soient x et y des entiers non nuls tels que $x^p - y^q = 1$. On a alors $p < 4q^2$ et $q < 4p^2$.*

Démonstration. — Par symétrie il suffit de démontrer que $q < 4p^2$. Supposons par l'absurde que $q > 4p^2$. D'après la proposition ci-dessus, pour tout $\tau \in G$ il existe $\theta \in I$ non nul tel que $\|\theta\| \leqslant 3q/(p-1)$ avec $|\operatorname{Arg}(\tau(\alpha))| \leqslant \pi/q$, où $(x - \zeta_p)^\theta = \alpha^q$. D'après le lemme 6.9 (4), S est annulé par I, donc $[x - \zeta_p]$ est annulé par I et donc $I \subset X$. Puisque par définition $I = (1-\iota)I_s \subset (1-\iota)\mathbb{Z}[G]$ il en résulte que $\theta \in X \cap (1-\iota)\mathbb{Z}[G]$, et puisque $\|\theta\| \leqslant 3q/(p-1)$ on déduit de la proposition 7.3 que $|\operatorname{Arg}(\tau(\alpha))| > \pi/q$, ce qui contredit l'inégalité de la proposition 7.6 et démontre le théorème. □

8. Le quatrième théorème de Mihăilescu : $p \equiv 1 \pmod q$ ou $q \equiv 1 \pmod p$

Ceci est la partie la plus délicate de la démonstration. Jusqu'à présent nous n'avons en fait utilisé que des propriétés simples et très classiques des corps cyclotomiques (bien que certaines démonstrations

soient très techniques), l'outil principal étant le théorème de Stickelberger et les propriétés de la partie − du groupe de classes. Comme nous l'avons déjà mentionné, le quatrième théorème de Mihăilescu repose au contraire sur les propriétés de la partie + du groupe de classes, qui est beaucoup moins bien comprise. L'utilisation du théorème de Thaine, que nous ne démontrerons pas (voir **[3]** ou la deuxième édition de **[4]**), qui est un analogue plus faible du théorème de Stickelberger pour la partie +, va se révéler indispensable.

Dans les trois premières parties nous démontrons les résultats dont nous aurons besoin sur la partie +, et qui sont complètement indépendants de l'équation de Catalan. Nous aurons bien sûr besoin du théorème de Thaine à un moment crucial. Nous donnerons ensuite la démonstration du quatrième théorème de Mihăilescu, qui finira la démonstration de la conjecture de Catalan.

8.1. Préliminaires d'algèbre commutative

Lemme 8.1. — *Soit R un anneau commutatif, $\mathfrak{b}$ un idéal de R, M un R-module de type fini et ϕ un R-endomorphisme de M tel que $\phi(M) \subset \mathfrak{b}M$. Il existe un polynôme unitaire non nul $P \in R[X]$ tel que $P(\phi) = 0$, et tel que tous les coefficients de P autres que le coefficient dominant appartiennent à $\mathfrak{b}$.*

Rappelons que dans l'énoncé ci-dessus $\mathfrak{b}M$ est le R-module des *combinaisons linéaires* de produits d'un élément de $\mathfrak{b}$ par un élément de M, et que pour tout endomorphisme ϕ on convient que ϕ^0 est l'identité.

Démonstration. — Soit $(m_i)_{1\leqslant i\leqslant n}$ un système générateur de M, et soient $b_{i,j} \in \mathfrak{b}$ tels que $\phi(m_j) = \sum_{1\leqslant i\leqslant n} b_{i,j}m_i$ pour $1 \leqslant j \leqslant n$. La loi $A(\phi)\cdot m = A(\phi)(m)$ pour $A \in R[X]$ et $m \in M$ permet de considérer M comme un $R[\phi]$-module. Si on pose $B = (b_{i,j})_{1\leqslant i,j\leqslant n}$ et si on désigne par I_n la matrice identité d'ordre n nous pouvons donc écrire dans l'anneau des matrices à coefficients dans $R[\phi]$ l'équation $(\phi I_n - B)V = 0$, où V est le vecteur (colonne) des m_i. En multipliant par la comatrice de $\phi I_n - B$ on en déduit que $\det(\phi I_n - B)V = 0$, en d'autres termes que $\det(\phi I_n - B)m_i = 0$ pour tout i. Comme les m_i engendrent M ceci signifie que (en tant qu'élément de $R[\phi]$, c'est-à-dire en tant qu'endomorphisme) on a $\det(\phi I_n - B) = 0$, et ceci est

évidemment un polynôme unitaire non nul en ϕ dont les coefficients sont dans $\mathfrak{b}$, en dehors du coefficient dominant. □

Nous noterons comme il est l'usage $\mathrm{Ann}_R(M)$ l'annulateur d'un R-module M, en d'autres termes l'ensemble des $x \in R$ tels que $xM = 0$. C'est évidemment un idéal de R.

Lemme 8.2. — *Soit R un anneau commutatif, $\mathfrak{b}$ un idéal de R, M un R-module de type fini, et notons ψ la surjection canonique de R dans $R/\mathfrak{b}$. Si $R/(\mathrm{Ann}_R(M) + \mathfrak{b})$ n'a pas d'éléments nilpotents non nuls alors*

$$\psi(\mathrm{Ann}_R(M)) = \mathrm{Ann}_{R/\mathfrak{b}}(M/\mathfrak{b}M).$$

Démonstration. — L'inclusion $\subset$ est triviale, montrons l'autre. Soit $\psi(\alpha) \in \mathrm{Ann}_{R/\mathfrak{b}}(M/\mathfrak{b}M)$, en d'autres termes soit $\alpha \in R$ tel que $\alpha M \subset \mathfrak{b}M$. Appliquant le lemme précédent à l'endomorphisme multiplication par α on en déduit qu'il existe des $b_i \in \mathfrak{b}$ tels que l'application multiplication par $\beta = \alpha^n + b_{n-1}\alpha^{n-1} + \cdots + b_0$ soit l'application nulle de M dans M, en d'autres termes tels que $\beta \in \mathrm{Ann}_R(M)$. Puisque $b_i \in \mathfrak{b}$ il en résulte que $\alpha^n \in \mathrm{Ann}_R(M) + \mathfrak{b}$, et puisque $R/(\mathrm{Ann}_R(M) + \mathfrak{b})$ n'a pas d'éléments nilpotents non nuls on doit donc avoir $\alpha \in \mathrm{Ann}_R(M) + \mathfrak{b}$, donc $\psi(\alpha) \in \psi(\mathrm{Ann}_R(M))$. □

Lemme 8.3. — *Soit H un groupe cyclique d'ordre n, et supposons que $q \nmid n$. Posons $s = \sum_{\sigma \in H} \sigma \in \mathbb{F}_q[H]$. Les anneaux $\mathbb{F}_q[H]$ et $\mathbb{F}_q[H]/(s\mathbb{F}_q[H])$ n'ont pas d'éléments nilpotents non nuls.*

Démonstration. — Puisque H est cyclique, on a

$$\mathbb{F}_q[H] \simeq \mathbb{F}_q[X]/((X^n - 1)\mathbb{F}_q[X])$$

et

$$\mathbb{F}_q[H]/(s\mathbb{F}_q[H]) \simeq \mathbb{F}_q[X]/((X^{n-1} + \cdots + X + 1)\mathbb{F}_q[X]),$$

donc

$$\begin{aligned}\mathbb{F}_q[H] &\simeq (\mathbb{F}_q[X]/((X-1)\mathbb{F}_q[X])) \\ &\qquad \times \mathbb{F}_q[H]/((X^{n-1} + \cdots + X + 1)\mathbb{F}_q[H]) \\ &\simeq \mathbb{F}_q \times \mathbb{F}_q[H]/(s\mathbb{F}_q[H])\end{aligned}$$

si $(X - 1)$ et $X^{n-1} + \cdots + X + 1$ sont premiers entre eux, ce qui est le cas puisque $q \nmid n$. Si η est un élément nilpotent de $\mathbb{F}_q[H]/(s\mathbb{F}_q[H])$, alors par cet isomorphisme $(0, \eta)$ sera un élément nilpotent de $\mathbb{F}_q[H]$,

donc il suffit de montrer qu'il n'y en a pas dans cet anneau. Or $\mathbb{F}_q[H] \simeq \mathbb{F}_q[X]/((X^n-1)\mathbb{F}_q[X])$, donc si la classe de $A(X) \in \mathbb{F}_q[X]$ est nilpotente on doit avoir $(X^n-1) \mid A(X)^k$ pour un certain $k \geqslant 1$. Toutefois les racines de X^n-1 dans une clôture algébrique de $\mathbb{F}_q$ sont distinctes puisque sa dérivée vaut nX^{n-1} qui est non nulle puisque $q \nmid n$. Il en résulte que $X^n-1 \mid A(X)$, donc que la classe de A est nulle. □

Nous terminons cette partie en rappelant sans démonstration des résultats de base sur les modules et anneaux semi-simples que l'on peut trouver dans tout bon livre sur les sujet, et en particulier dans Bourbaki.

Définition 8.4

(1) Un anneau commutatif R sera dit semi-simple si c'est un produit fini de corps.

(2) Un R-module M est simple si ses seuls sous-modules sont 0 et M, et il est semi-simple s'il est somme directe de modules simples.

(3) Un R-module M est cyclique s'il est engendré en tant que R-module par un seul élément, en d'autres termes s'il existe $a \in M$ tel que $M = aR$.

Lemme 8.5. — *Soit H un groupe cyclique d'ordre n, et supposons que $q \nmid n$. Alors l'anneau $\mathbb{F}_q[H]$ est semi-simple.*

Démonstration. — Soit $X^n-1 = \prod_{1 \leqslant i \leqslant g} P_i^{e_i}(X)$ la décomposition de X^n-1 comme produit de puissances de polynômes irréductibles unitaires distincts dans $\mathbb{F}_q[X]$. Puisque $q \nmid n$, comme nous l'avons déjà mentionné les racines de X^n-1 dans une clôture algébrique sont distinctes, donc $e_i = 1$ pour tout i. D'après le lemme ci-dessus on a donc

$$\mathbb{F}_q[H] \simeq \mathbb{F}_q[X]/((X^n-1)\mathbb{F}_q[X]) \simeq \prod_{1 \leqslant i \leqslant g} K_i,$$

où $K_i = \mathbb{F}_q[X]/(P_i(X)\mathbb{F}_q[X])$ est un corps, donc $\mathbb{F}_q[H]$ est bien semi-simple. □

La proposition suivante résume les résultats dont nous aurons besoin.

Proposition 8.6. — *Soit R un anneau semi-simple. Alors :*

(1) *Tout R-module est semi-simple.*

(2) *Toute suite exacte de R-modules est scindée.*

(3) *Pour tout R-module M il existe $\alpha \in M$ tel que $\mathrm{Ann}_R(\alpha) = \mathrm{Ann}_R(M)$, donc M contient le sous-module cyclique aR qui est isomorphe au module quotient $R/\mathrm{Ann}_R(M)$.*

(4) *Si R et M sont finis alors $|M| \geqslant |R/\mathrm{Ann}_R(M)|$ avec égalité si et seulement si M est cyclique.*

(5) *Soit M un module cyclique. Tout sous-module M' de M est aussi cyclique, $\mathrm{Ann}_R(M) = \mathrm{Ann}_R(M') \cdot \mathrm{Ann}_R(M/M')$, et les idéaux $\mathrm{Ann}_R(M)$ et $\mathrm{Ann}_R(M/M')$ sont premiers entre eux (c'est-à-dire de somme égale à R).*

Noter que (2) signifie que si $0 \to M_1 \to M_2 \to M_3 \to 0$ est une suite exacte alors $M_2 \simeq M_1 \oplus M_3$.

8.2. Préliminaires sur la partie plus. — Rappelons que l'on note $G^+ = \mathrm{Gal}(K^+/\mathbb{Q}) = G/\langle\iota\rangle$, et que le corollaire 1.14 nous dit que $U(K) = \langle\zeta_p\rangle U(K^+)$. Rappelons enfin que d'après la proposition 6.1 l'application naturelle de $\mathrm{Cl}(K^+)$ dans $\mathrm{Cl}(K)$ est injective.

Lemme 8.7. — *On a $\mathrm{Cl}(K^+)[q] = \mathrm{Cl}(K)[q]^+$.*

Bien observer la position des $+$, et se rappeler que ce résultat est faux en général si on enlève les $[q]$.

Démonstration. — Par abus de notation, d'après la proposition 6.1 on peut écrire $\mathrm{Cl}(K^+)[q] \subset \mathrm{Cl}(K)[q]$, et puisque $\mathrm{Cl}(K^+)$ est trivialement invariant par ι on a $\mathrm{Cl}(K^+)[q] \subset \mathrm{Cl}(K)[q]^+$. Réciproquement, soit $\mathfrak{a}$ un représentant d'une classe de $\mathrm{Cl}(K)[q]^+$. Puisque $\mathrm{Cl}(K)[q]$ est un $\mathbb{F}_q[G]$-module et que 2 est inversible dans $\mathbb{F}_q$, il en résulte que $\mathrm{Cl}(K)[q]^+$ est égal au noyau de la multiplication par $(1-\iota)/2$ (ou par $1-\iota$) de $\mathrm{Cl}(K)[q]$ dans lui-même. Ainsi il existe α et β dans K^* tels que $\mathfrak{a}\iota(\mathfrak{a})^{-1} = \alpha\mathbb{Z}_K$ et $\mathfrak{a}^q = \beta\mathbb{Z}_K$. Soit $\mathfrak{b}$ l'idéal de K^+ défini par $\mathfrak{b} = \mathcal{N}_{K/K^+}(\mathfrak{a})$. Nous avons $\mathfrak{b}\mathbb{Z}_K = \mathfrak{a}\iota(\mathfrak{a})$, donc $\mathfrak{b}^q\mathbb{Z}_K = \mathfrak{a}^q\iota(\mathfrak{a}^q) = \beta\iota(\beta)\mathbb{Z}_K = \mathcal{N}_{K/K^+}(\beta)\mathbb{Z}_K$, et donc en intersectant avec K^+ on en déduit que $\mathfrak{b}^q = \mathcal{N}_{K/K^+}(\beta)K^+$, donc la classe de $\mathfrak{b}$ appartient à $\mathrm{Cl}(K^+)[q]$. De plus, en posant $m = (q+1)/2$ on voit que

$$\mathfrak{b}^m\mathbb{Z}_K = \mathfrak{a}^m\iota(\mathfrak{a})^m = \mathfrak{a}^m(\mathfrak{a}\alpha^{-1})^m = \mathfrak{a}^{q+1}\alpha^{-m} = \mathfrak{a}\beta\alpha^{-m},$$

et donc la classe de $\mathfrak{a}$ est égale à celle de $\mathfrak{b}^m\mathbb{Z}_K$, ce qui démontre le lemme. □

Rappelons (définition 6.7) que l'on a posé

$$E = \{u\pi^k,\ u \in U(K),\ k \in \mathbb{Z}\} = \mathbb{Z}[\zeta_p, 1/p]^*.$$

C'est un $\mathbb{Z}[G]$-module, donc E/E^q est un $\mathbb{F}_q[G]$-module. Puisque $\pi = 1 - \zeta_p$, d'après le corollaire 1.14 pour tout $x \in E$ la quantité $\iota(x)/x$ est une racine $2p$-ième de l'unité, donc comme d'habitude une puissance q-ième. Il en résulte que E/E^q est invariant sous l'action de ι, donc que c'est en fait un $\mathbb{F}_q[G^+]$-module. Le lemme suivant décrit très précisément sa structure.

Lemme 8.8. — *Supposons que* $p \not\equiv 1 \pmod q$.

(1) *On a* $|E/E^q| = q^{(p-1)/2}$.

(2) *Si on pose* $V = U(K^+)/\{\pm 1\}$, *alors* $\mathrm{Ann}_{\mathbb{Z}[G^+]}(V) = s\mathbb{Z}[G^+]$, *où* $s = \sum_{\sigma\in G^+}\sigma$.

(3) *On a* $\mathrm{Ann}_{\mathbb{F}_q[G^+]}(V/V^q) = s\mathbb{F}_q[G^+]$.

(4) *On a* $\mathrm{Ann}_{\mathbb{F}_q[G^+]}(E/E^q) = 0$.

(5) E/E^q *est un* $\mathbb{F}_q[G^+]$*-module libre de rang* 1.

Noter que le V de ce lemme n'a rien à voir avec le V utilisé ci-dessus pour définir le groupe S.

Démonstration

(1) L'application (u, k) de $U(K) \times \mathbb{Z}$ dans E est un isomorphisme puisque k est déterminé de manière unique comme la valuation $\mathfrak{p}$-adique de $u\pi^k$. D'après le théorème de Dirichlet donnant la structure du groupe des unités, on en déduit que comme groupe abélien on a $E \simeq \mu_{2p} \times \mathbb{Z}^{(p-1)/2}$ puisque le rang du groupe des unités de K est égal à $(p-3)/2$. Puisque $2p$ est premier à q il en résulte que $E/E^q \simeq (\mathbb{Z}/q\mathbb{Z})^{(p-1)/2}$, ce qui montre (1).

(2) Soit $\sum_{\sigma\in G^+} a_\sigma\sigma$ un élément de $\mathrm{Ann}_{\mathbb{Z}[G^+]}(V)$, en d'autres termes tel que $\prod_{\sigma\in G^+}\sigma(\varepsilon)^{a_\sigma} = \pm 1$ pour tout $\varepsilon \in U(K^+)$, et soit $(\varepsilon_i)_{1\leqslant i\leqslant(p-3)/2}$ un système d'unités fondamentales de K^+. En prenant les logarithmes, on a $\sum_{\sigma\in G^+} a_\sigma \log(|\sigma(\varepsilon_i)|) = 0$ pour tout i. Par ailleurs, toujours d'après le théorème de Dirichlet, la matrice $((p-3)/2) \times ((p-1)/2)$ des $\sigma(\varepsilon_i)_{i\leqslant(p-3)/2,\sigma\in G^+}$ est de rang $(p-3)/2$, et donc son noyau est de dimension 1. Puisque l'on a

$\sum_{\sigma\in G^+}\log(|\sigma(\varepsilon_i)|)=0$, ce noyau est engendré sur $\mathbb{R}$ par le vecteur colonne dont les $(p-1)/2$ coordonnées sont égales à 1. Il en résulte que $a_\sigma = a$ pour tout σ, donc que $\sum_{\sigma\in G^+} a_\sigma\sigma = a\cdot s$, comme annoncé.

(3) D'après le lemme 8.3 appliqué à $H = G^+$, on voit que, si $p\not\equiv 1 \pmod q$, l'anneau $\mathbb{F}_q[G^+]/(s\mathbb{F}_q[G^+])$ n'a pas d'éléments nilpotents non nuls. Posons temporairement $I = s\mathbb{Z}[G^+] + q\mathbb{Z}[G^+]$. Il est clair que $\mathbb{Z}[G^+]/I \simeq \mathbb{F}_q[G^+]/(s\mathbb{F}_q[G^+])$, et donc n'a pas de nilpotents non nuls. D'après (2) il est clair que $s\mathbb{F}_q[G^+]\subset \mathrm{Ann}_{\mathbb{F}_q[G^+]}(V/V^q)$. Montrons l'inclusion inverse. Soit $\theta\in\mathrm{Ann}_{\mathbb{F}_q[G^+]}(V/V^q)$, en d'autres termes soit $\theta\in\mathbb{F}_q[G^+]$ tel que $V^\theta\subset V^q$. Nous appliquons le lemme 8.2 à $R=\mathbb{Z}[G^+]$, $\mathfrak{b}=q\mathbb{Z}[G^+]$ et $M=V$, où nous rappelons que l'action de R sur M est bien évidemment multiplicative, alors qu'elle est écrite additivement dans le lemme. Puisque d'après (2) on a $\mathrm{Ann}_R(M)=sR$ on voit que puisque $R/(\mathrm{Ann}_R(M)+\mathfrak{b})$ n'a pas de nilpotents non nuls on a $\psi(\mathrm{Ann}_R(M)) = \mathrm{Ann}_{R/\mathfrak{b}}(M/\mathfrak{b}M)$. Traduisant ceci dans notre contexte signifie que $s\mathbb{F}_q[G^+]=\mathrm{Ann}_{\mathbb{F}_q[G^+]}(V/V^q)$.

(4) Calculons l'image et le noyau de l'application naturelle de $U(K^+)$ dans $U(K)/U(K)^q$. Comme nous l'avons rappelé ci-dessus, tout $u\in U(K)$ peut s'écrire $u=\zeta\varepsilon$, où $\varepsilon\in U(K^+)$ et ζ une racine $2p$-ième de l'unité, donc une puissance q-ième. La classe de u dans $U(K)/U(K)^q$ est donc égale à la classe de ε, ce qui montre que l'application est surjective. Soit maintenant $\varepsilon\in U(K^+)$ dans le noyau, en d'autres termes tel que $\varepsilon=u^q$ pour un $u\in U(K)$. On a donc $\varepsilon=\iota(u)^q=u^q$, donc $\iota(u)=u$ (il n'y a pas de racines q-ièmes de l'unité non triviales dans K), d'où $u\in U(K^+)$, et donc le noyau est égal à $U(K^+)^q$. Il résulte de ceci que

$$U(K)/U(K)^q \simeq U(K^+)/U(K^+)^q \simeq V/V^q,$$

et donc que $E/E^q\simeq V/V^q\times\mathbb{Z}/q\mathbb{Z}$. Noter que tous les isomorphismes ci-dessus sont canoniques, et en particulier sont des isomorphismes de $\mathbb{F}_q[G^+]$-modules. Il résulte donc de (3) que

$$\mathrm{Ann}_{\mathbb{F}_q[G^+]}(E/E^q)\subset\mathrm{Ann}_{\mathbb{F}_q[G^+]}(V/V^q)\subset s\mathbb{F}_q[G^+].$$

Remarquons maintenant que pour tout $\sigma\in G^+$ on a $s\sigma=s$. Il en résulte que $s\mathbb{F}_q[G^+]=\mathbb{F}_q s$. Ainsi, soit $\overline{a}s\in\mathrm{Ann}_{\mathbb{F}_q[G^+]}(E/E^q)$ avec $a\in\mathbb{Z}$. Puisque $\pi=1-\zeta_p\in E$ on a $\pi^{as}\in E^q$, donc $v_{\mathfrak{p}}(\pi^{as})\equiv 0 \pmod{\mathfrak{q}}$ par définition de E. D'autre part, pour tout $\sigma\in G$ on a

$\pi^\sigma = u_\sigma \pi$ pour une certaine unité u_σ, et donc $\pi^s = u\pi^{(p-1)/2}$ pour une unité u. Il en résulte que $v_{\mathfrak{p}}(\mathfrak{p}^{as}) = a(p-1)/2$. Comme $q \nmid (p-1)/2$ on doit donc avoir $q \mid a$, donc $\overline{a} = 0$, ce qui démontre (4).

(5) D'après la proposition 8.6 (3) appliquée à l'anneau semi-simple $R = \mathbb{F}_q[G^+]$ et à $M = E/E^q$ il existe $\alpha \in M$ tel que $\mathrm{Ann}_R(\alpha) = \mathrm{Ann}_R(M)$, et donc $\mathrm{Ann}_R(\alpha) = 0$ d'après (4). Ceci signifie que l'application $x \mapsto x \cdot \alpha$ de R dans M est un homomorphisme injectif de R-modules. Or d'après (1) on a $|M| = |E/E^q| = q^{(p-1)/2} = |\mathbb{F}_q[G^+]| = |R|$. Il en résulte que cet homomorphisme est une bijection, et donc que R et M sont des R-modules isomorphes. □

Définition 8.9

(1) Pour simplifier les notations on posera $R_p = \mathbb{Z}[\zeta_p, 1/p]$, d'où $E = R_p^*$.

(2) Rappelons que l'on écrit $[\alpha]$ pour la classe de α dans S modulo les puissances q-ièmes. On définit le groupe des éléments *q-primaires* de S comme suit :

$$S_q = \{[\alpha] \in S,\ \alpha \equiv \beta^q \pmod{q^2 R_p},\ \beta \text{ inversible modulo } q^2 R_p\},$$

et $E_q = \{u \in E,\ [u] \in S_q\}$.

Lemme 8.10. — *On a*

$$E_q = \{u \in E,\ u \equiv \beta^q \pmod{q^2 R_p}\}.$$

Démonstration. — Si u appartient au membre de droite alors $u \in E$, $u \equiv \beta^q \pmod{q^2 R_p}$, donc β^q modulo q^2 est égal à u. Comme les éléments de E sont inversibles dans R_p (ce sont d'ailleurs exactement ceux qui le sont), il en résulte que β^q modulo q^2 est inversible, et donc β aussi, ce qui montre que $u \in E_q$. Réciproquement soit $u \in E_q$, donc tel que $u \in E$ et $[u] \in S_q$. Par définition de S_q il existe $\alpha \in K^*$ et β, $\gamma \in R_p$ tels que $u\alpha^q = \beta^q + q^2\gamma$, et β inversible modulo $q^2 R_p$. Soit $\mathfrak{q}$ un idéal premier de $\mathbb{Z}_K$ différent de $\mathfrak{p} = \pi\mathbb{Z}_K$. On a donc $v_{\mathfrak{q}}(u) = 0$, et puisque β et γ sont dans R_p et $\mathfrak{q} \neq \mathfrak{p}$ on a $v_{\mathfrak{q}}(\beta) \geqslant 0$ et $v_{\mathfrak{q}}(\gamma) \geqslant 0$. Il en résulte que $v_{\mathfrak{q}}(\alpha) \geqslant 0$ pour tous les idéaux premiers $\mathfrak{q} \neq \mathfrak{p}$, en d'autres termes que $\alpha \in R_p$. Or modulo $q^2 R_p$ on a $\overline{u\alpha}^q = \overline{\beta}^q$. Puisque $\overline{\beta}$ est inversible il en résulte que $\overline{\alpha}$ est aussi inversible et $\overline{u} = (\overline{\beta}\overline{\alpha}^{-1})^q$. Donc si $\beta_0 \in R_p$ est un représentant de $\overline{\beta}\overline{\alpha}^{-1}$ on a

$\overline{u} = \overline{\beta_0}^q$, en d'autres termes $u = \beta_0^q + q^2\gamma_0$ pour un $\gamma_0 \in R_p$, ce qui démontre l'inclusion réciproque et donc le lemme. □

8.3. Unités cyclotomiques et le théorème de Thaine

Définition 8.11. — Le groupe C des unités p-cyclotomiques de K est le sous-groupe multiplicatif de K^* engendré par les racines de l'unité et les $1 - \zeta_p^k$ pour $k \in \mathbb{Z}$. On pose $C_q = C \cap E_q$ et on appelle les éléments de C_q les unités p-cyclotomiques q-primaires.

Lemme 8.12. — *Si p et q sont des nombres premiers impairs distincts, l'égalité $C = C_q$ implique que $p < q$.*

Démonstration. — Soit ζ une racine primitive p-ième de l'unité *quelconque*, pas nécessairement égale à ζ_p. Puisque $1 + \zeta^q = (1 - \zeta^{2q})/(1 - \zeta^q) \in C$ on a $1 + \zeta^q \in C_q$. De plus j'affirme que $R_p/q^2R_p \simeq \mathbb{Z}[\zeta_p]/q^2\mathbb{Z}[\zeta_p]$: en effet, soit ϕ l'application qui envoie $x \in \mathbb{Z}[\zeta_p]$ sur sa classe dans R_p/q^2R_p. Son noyau est égal à $q^2R_p \cap \mathbb{Z}[\zeta_p] = q^2\mathbb{Z}[\zeta_p]$, donc il suffit de montrer que ϕ est surjective. Soit donc $y/p^n \in R_p = \mathbb{Z}[\zeta_p, 1/p]$ avec $y \in \mathbb{Z}[\zeta_p]$. Puisque p^n et q^2 sont premiers entre eux, il existe u et v dans $\mathbb{Z}$ tels que $up^n + vq^2 = 1$. Il en résulte que $y/p^n = uy + vyq^2/p^n$, donc que la classe de y/p^n dans R_p/q^2R_p est égale à celle de $uy \in \mathbb{Z}[\zeta_p]$, et donc elle est dans l'image de ϕ, ce qui démontre mon assertion.

Puisque $1 + \zeta^q \in C_q \subset E_q$ on peut écrire $1 + \zeta^q = \beta^q + q^2\gamma$ avec β et γ dans R_p et donc, grâce à l'isomorphisme ci-dessus, en changeant si nécessaire β et γ par un élément de q^2R_p, on peut supposer que β et γ appartiennent à $\mathbb{Z}[\zeta_p]$. Il en résulte que $1 + \zeta^q \equiv \beta^q \pmod{q^2\mathbb{Z}[\zeta_p]}$. D'après la formule du binôme on a donc $(1 + \zeta)^q \equiv 1 + \zeta^q \equiv \beta^q \pmod{q\mathbb{Z}[\zeta_p]}$. Puisque q est non ramifié dans K, il résulte du corollaire 5.3 que $(1 + \zeta)^q \equiv \beta^q \pmod{q^2\mathbb{Z}[\zeta_p]}$. Ainsi $(1 + \zeta)^q \equiv 1 + \zeta^q \pmod{q^2\mathbb{Z}[\zeta_p]}$, et donc $F(\zeta) \in q\mathbb{Z}[\zeta_p]$, où $F(X) = ((1 + X)^q - 1 - X^q)/(qX)$, qui est évidemment un polynôme de degré $q - 2$ à coefficients entiers. Notons $\overline{F} \in \mathbb{F}_q[X]$ la réduction de F modulo q. Si $\mathfrak{q}$ est un idéal premier au-dessus de q, dans le corps fini $\mathbb{Z}_K/\mathfrak{q} = \mathbb{Z}[\zeta_p]/\mathfrak{q}$ on a $\overline{F}(\overline{\zeta}) = 0$, où $\overline{\zeta}$ est l'image de ζ dans $\mathbb{Z}_K/\mathfrak{q}$. Puisque ceci est vrai pour les $p-1$ racines primitives p-ièmes de l'unité ζ et que ces racines ne sont pas congrues modulo $\mathfrak{q}$ puisque la norme de leur différence est égal à p, il en résulte que $\overline{F}$ a

au moins $p-1$ racines distinctes dans $\mathbb{Z}_K/\mathfrak{q}$. Puisque $\deg(F) = q-2$ on doit donc avoir $p-1 \leqslant q-2$, donc $p < q$. □

Nous énonçons maintenant sans démonstration le théorème remarquable et très important de F. Thaine (voir [**3**] ou la deuxième édition de [**4**] pour la démonstration). Nous ne donnons que le cas particulier dont nous aurons besoin.

***Théorème 8.13* (Thaine).** — *Rappelons que C est le groupe des p-unités cyclotomiques de K. On a*

$$\mathrm{Ann}_{\mathbb{F}_q[G^+]}(E/CE^q) \subset \mathrm{Cl}(K^+)[q].$$

Le théorème principal de cette partie que nous utiliserons pour démontrer le quatrième et dernier théorème de Mihăilescu est le suivant.

Théorème 8.14. — *Soient p et q des nombres premiers impairs tels que $p > q$ et $p \not\equiv 1 \pmod q$. On a alors* $\mathrm{Ann}_{\mathbb{F}_q[G^+]}(S^+ \cap S_q) \neq 0$.

Démonstration. — Posons $R = \mathbb{F}_q[G^+]$, qui est semi-simple d'après le lemme 8.5. D'après le lemme 8.8 (5), E/E^q est un R-module cyclique R, donc d'après la proposition 8.6 (5) et (4) tout sous-module M de E/E^q est aussi cyclique, donc isomorphe à $R/\operatorname{Ann}_R(M)$. Puisque $R \simeq \mathbb{F}_q[X]/((X^{(p-1)/2}-1)\mathbb{F}_q[X])$, tout idéal de R est isomorphe à $f(X)\mathbb{F}_q[X]/((X^{(p-1)/2}-1)\mathbb{F}_q[X])$ pour un $f(X) \in \mathbb{F}_q[X]$ divisant $X^{(p-1)/2}-1$, que l'on peut supposer unitaire, et donc en particulier $M \simeq R/\operatorname{Ann}_R(M) \simeq \mathbb{F}_q[X]/(f(X)\mathbb{F}_q[X])$. En particulier on a $\dim_{\mathbb{F}_q}(M) = \deg(f)$.

Rappelons maintenant que d'après le lemme 6.9 (3) on a une suite exacte de R-modules $0 \to E/E^q \to S^+ \to \mathrm{Cl}(K)[q]^+ \to 0$. Par définition on a $E_q = \{u \in E,\ [u] \in S_q\}$, donc par restriction cette suite exacte donne la suite exacte $0 \to E_q/E^q \to S^+ \cap S_q \to \mathrm{Cl}(K)[q]^+$, où le dernier homomorphisme n'est pas nécessairement surjectif. Puisque R est semi-simple, d'après la proposition 8.6 (2) toute suite exacte est scindée, donc en particulier $S^+ \cap S_q$ est isomorphe à un sous-module de $E_q/E^q \oplus \mathrm{Cl}(K)[q]^+$, ce que nous noterons $S^+ \cap S_q \hookrightarrow E_q/E^q \oplus \mathrm{Cl}(K)[q]^+$.

Rappelons aussi que C est le groupe des p-unités cyclotomiques et que $C_q = C \cap E_q$. Considérons la suite d'inclusions $0 \subset C_qE^q/E^q \subset$

$CE^q/E^q \subset E/E^q$, et appelons E_1, E_2 et E_3 les quotients successifs, c'est à dire $E_1 = C_qE^q/E^q$, $E_2 = CE^q/C_qE^q$ et $E_3 = E/CE^q$. Puisque R est semi-simple, d'après la proposition 8.6 (1) et (2) tout R-module est semi-simple et toute suite exacte est scindée. En particulier si $0 \subset A \subset B \subset C$ est une suite d'inclusions on a $C \simeq B \oplus (C/B) \oplus \simeq A \oplus (B/A) \oplus (C/B)$. Comme d'après le lemme 8.8 E/E^q est un R-module libre de dimension 1 on a donc un isomorphisme

$$E_1 \oplus E_2 \oplus E_3 \simeq R \simeq \mathbb{F}_q[X]/((X^{(p-1)/2} - 1)\mathbb{F}_q[X]).$$

Il en résulte que les E_i sont isomorphes à des sous-modules de R, qui comme ci-dessus sont isomorphes à $\mathbb{F}_q[X]/(e_i(X)\mathbb{F}_q[X])$ pour des facteurs unitaires $e_i(X)$ de $X^{(p-1)/2} - 1$ tels que $\dim_{\mathbb{F}_q}(E_i) = \deg(e_i)$. D'après l'isomorphisme ci-dessus on a $e_1e_2e_3 = X^{(p-1)/2} - 1$.

Par définition de S on a $E^q \subset E_q$ et donc $C_qE^q \subset E_q$. Nous avons donc une suite exacte

$$1 \longrightarrow C_qE^q/E^q \longrightarrow E_q/E^q \longrightarrow E_q/C_qE^q \longrightarrow 1.$$

Puisque les suites exactes sont scindées il en résulte que $E_q/E^q \simeq E_1 \oplus E_q/C_qE^q$. D'autre part il est clair que le noyau de l'application naturelle de E_q dans E/CE^q est égal à $E_q \cap C_qE^q$: une inclusion est triviale. Réciproquement, si $x \in E_q$ est de la forme $x = ce^q$ avec $c \in C$ et $e \in E$ alors, puisque $e^q \in E_q$, on a $c \in E_q \cap C = C_q$, et donc $x \in C_qE^q$. Il en résulte que E_q/C_qE^q est isomorphe à un sous-groupe de $E_3 = E/CE^q$. Rassemblant tous les résultats ci-dessus on obtient

$$S^+ \cap S_q \hookrightarrow E_q/E^q \oplus \mathrm{Cl}(K)[q]^+ \simeq E_1 \oplus E_q/C_qE^q \oplus \mathrm{Cl}(K)[q]^+ \hookrightarrow E_1 \oplus E_3 \oplus \mathrm{Cl}(K)[q]^+.$$

C'est maintenant que nous appliquons le théorème de Thaine. D'après ce théorème, tout annulateur de $E_3 = E/CE^q$ est aussi un annulateur de $\mathrm{Cl}(K^+)[q]$, qui est égal à $\mathrm{Cl}(K)[q]^+$ d'après le lemme 8.7. Puisque par définition e_i annule E_i, il en résulte que e_1e_3 annule $E_1 \oplus E_3$, et le théorème de Thaine implique que e_3 annule $\mathrm{Cl}(K)[q]^+$, et donc que e_1e_3 annule $S^+ \cap S_q$.

Supposons donc maintenant par l'absurde que $\mathrm{Ann}_R(S^+ \cap S_q) = 0$. On a donc $e_1e_3 = 0$ dans $\mathbb{F}_q[X]/((X^{(p-1)/2} - 1)\mathbb{F}_q[X])$, en d'autres termes $X^{(p-1)/2} - 1 = e_1e_2e_3 \mid e_1e_3$, donc $e_2 = 1$, et donc $E_2 = 0$. Par

définition ceci signifie que $C_qE^q = CE^q$. Comme $E^q \subset E_q$ on a donc $C_q \cap E^q = C \cap E^q$. J'affirme que $C = C_q$: en effet, soit $c \in C$. Puisque $c = c \cdot 1 \in CE^q = C_qE^q$ nous pouvons écrire $c = c_qe^q$ avec $c_q \in C_q$ et $e \in E$. Ainsi $e^q = c/c_q \in C \cap E^q = C_q \cap E^q \subset C_q$, donc $c = c_qe^q \in C_q$, ce qui démontre mon assertion. Appliquant maintenant le lemme 8.12 on en déduit que $p < q$, en contradiction avec les hypothèses de la proposition. □

8.4. Préliminaires sur les séries entières. — Nous touchons presque au but, en tous cas nous avons surmonté les étapes les plus difficiles. Pour aborder la démonstration du dernier théorème, nous avons besoin de résultats de nature un peu particulière sur les séries formelles et les séries entières, à nouveau indépendants de Catalan. Rappelons que si R est un anneau commutatif on désigne par $R[[T]]$ l'anneau des séries formelles en une variable à coefficients dans R.

Lemme 8.15. — *Soit R un anneau commutatif de caractéristique 0, soient $f(T) = \sum_{k\geqslant 0}(a_k/k!)T^k$ et $g(T) = \sum_{k\geqslant 0}(b_k/k!)T^k$, et soit $q \in R$. Supposons qu'il existe a et b dans R tels que $a_k \equiv a^k \pmod{qR}$ et $b_k \equiv b^k \pmod{qR}$. On a alors $fg(T) = \sum_{k\geqslant 0}(c_k/k!)T^k$ avec $c_k \equiv (a+b)^k \pmod{qR}$.*

Démonstration. — Évident et laissé au lecteur. □

Comme toujours, dans la suite on suppose que p et q sont des nombres premiers impairs distincts.

Définition 8.16

(1) Si $F(T) = \sum_{k\geqslant 0} a_kT^k \in K[[T]]$ est une série formelle en T à coefficients dans K, pour tout $\sigma \in G$ nous poserons $F^\sigma(T) = \sum_{k\geqslant 0} \sigma(a_k)T^k$.

(2) Si $F(T) = \sum_{k\geqslant 0} a_kT^k \in K[[T]]$ est une série formelle, pour tout entier $k \geqslant 0$ on appelle $F_k(T)$ la somme des termes de degré au plus égaux à k, en d'autres termes $F_k(T) = \sum_{0\leqslant j\leqslant k} a_jT^j$.

(3) Soit $\theta = \sum_{\sigma\in G} n_\sigma\sigma \in \mathbb{Z}[G]$. On définit $F_\theta(T) \in K[[T]]$ comme la série formelle définie par le produit suivant

$$F_\theta(T) = \prod_{\sigma\in G}(1 - \sigma(\zeta_p)T)^{n_\sigma/q},$$

où la puissance est calculée en utilisant le développement du binôme généralisé.

Notons que, puisque $|\sigma(\zeta_p)| = 1$, si $z \in \mathbb{C}$ est tel que $|z| < 1$, la série *entière* obtenue en remplaçant T par z dans $F_\theta(T)$ converge absolument, et sa somme sera évidemment notée $F_\theta(z)$.

Définition 8.17. — Soit $F(T) = \sum_{k\geqslant 0} a_k T^k \in \mathbb{C}[[T]]$ et $G(T) = \sum_{k\geqslant 0} b_k T^k \in \mathbb{R}[[T]]$. Nous dirons que G *domine* F si pour tout k on a $|a_k| \leqslant b_k$.

Proposition 8.18. — *Pour simplifier, écrivons F à la place de F_θ.*

(1) *Les coefficients de $F(T)$ sont entiers en dehors de q, en d'autres termes sont de la forme a/q^k pour un $a \in \mathbb{Z}_K$ et $k \in \mathbb{Z}_{\geqslant 0}$.*

(2) *Plus précisément, si $\theta = \sum_{\sigma\in G} n_\sigma \sigma$, alors on a $F(T) = \sum_{k\geqslant 0}(a_k/(q^k k!))T^k$, où $a_k \in \mathbb{Z}_K$ vérifie*

$$a_k \equiv \Big(-\sum_{\sigma\in G} n_\sigma \sigma(\zeta_p)\Big)^k \pmod{q\mathbb{Z}_K}.$$

(3) *Si $\tau \in G$ et $|t| < 1$ la série $F^\tau(t)$ converge. Si de plus $0 \leqslant n_\sigma \leqslant q$ pour tout $\sigma \in G$, alors si on pose $m = (\sum_{\sigma\in G} n_\sigma)/q$ on a*

$$|F^\tau(t) - F_k^\tau(t)| \leqslant \binom{m+k}{k+1} \frac{|t|^{k+1}}{(1-|t|)^{m+k+1}}.$$

Démonstration. — On a

$$(1-\sigma(\zeta_p)T)^{n_\sigma/q} = \sum_{k\geqslant 0} \binom{n_\sigma/q}{k} (-\sigma(\zeta_p))^k T^k,$$

donc (1) résulte du lemme 3.6. Plus précisément on a

$$\binom{n/q}{k} = \frac{n(n-q)\cdots(n-q(k-1))}{q^k k!},$$

donc $(1-q\sigma(\zeta_p)T)^{n/q} = \sum_{k\geqslant 0} b_k/k!$ où $b_k \equiv \sum_{k\geqslant 0}(-n\sigma(\zeta_p))^k \pmod{q\mathbb{Z}_K}$. Il résulte donc du lemme 8.15 que

$$F(qT) = \prod_{\sigma\in G}(1-\sigma(\zeta_p)T)^{n_\sigma/q} = \sum_{k\geqslant 0}(a_k/k!)T^k,$$

où

$$a_k \equiv \Big(\sum_{\sigma\in G}(-n_\sigma\sigma(\zeta_p))\Big)^k \pmod{q\mathbb{Z}_K},$$

ce qui démontre (2). Pour (3) on remarque que pour $0 \leqslant n \leqslant q$ on a

$$\begin{aligned}\left|\binom{n/q}{k}\right| &= \left|\frac{n(n-q)\cdots(n-q(k-1))}{k!}\right| \\ &= \frac{n(q-n)(2q-n)\cdots(q(k-1)-n)}{k!} \\ &\leqslant \frac{n(n+q)\cdots(n+q(k-1))}{k!} = \binom{-n/q}{k}.\end{aligned}$$

Il en résulte que la série $(1-\sigma(\zeta_p)T)^{n/q}$ est dominée par la série $(1-T)^{-n/q}$, donc $F(T)$ est dominée par $\prod_{\sigma\in G}(1-T)^{-n_\sigma/q} = (1-T)^{-m}$, et il en va de même pour $F^\tau(T)$. Il en résulte que pour $|t|<1$ on a

$$|F^\tau(t)-F_k^\tau(t)| \leqslant \left|(1-|t|)^{-m} - \sum_{0\leqslant j\leqslant k}\binom{-m}{j}(-|t|)^j\right| = |S(|t|)-S_k(|t|)|,$$

disons, où on a posé $S(T) = (1-T)^{-m}$. D'après le théorème de Taylor–Lagrange il existe $c \in [0,|t|]$ tel que $S(|t|) - S_k(|t|) = (|t|^{k+1}/(k+1)!)S^{(k+1)}(c)$. Puisque toutes les dérivées de S sont évidemment positives sur $[0,1[$, elles sont croissantes, et donc

$$\begin{aligned}S^{(k+1)}(c) &\leqslant S^{(k+1)}(|t|) = m(m+1)\cdots(m+k)(1-|t|)^{-m-k-1} \\ &= (m+k)!/((m-1)!(1-|t|)^{m+k+1}),\end{aligned}$$

ce qui démontre (3). □

Proposition 8.19. — *Gardons les mêmes notations et les mêmes hypothèses, mais supposons de plus que $\theta \in (1+\iota)\mathbb{Z}[G]$. Alors*

(1) *$F_\theta = F \in K^+[[T]]$.*

(2) *Supposons que $t \in \mathbb{Q}$ vérifie $|t|<1$ et soit tel qu'il existe $\alpha \in K$ tel que $(1-t\zeta_p)^\theta = \alpha^q$. Alors $\alpha \in K^+$, et pour tout $\sigma \in G$ on a $F^\sigma(t) = \sigma(\alpha)$.*

Démonstration. — Puisque $\theta = \sum_{\sigma\in G} n_\sigma\sigma \in (1+\iota)\mathbb{Z}[G]$ on a $\iota\theta = \theta$ donc $n_{\iota\sigma} = n_\sigma$ pour tout $\sigma \in G$. Si on choisit un ensemble P de représentants de G modulo $\langle\iota\rangle$ on peut donc écrire $F = F_1\overline{F_1}$, où F_1 est le même produit que F mais seulement pour les $\sigma \in P$. Il en résulte que les coefficients de F sont réels, donc dans K^+, ce qui montre (1). Pour (2) le même raisonnement montre que $(1-t\zeta_p)^\theta \in \mathbb{R}$. Il en résulte que $\overline{\alpha}^q = \overline{\alpha^q} = \overline{\beta} = \beta = \alpha^q$, et donc que $\overline{\alpha} = \alpha$ puisque les racines q-ièmes sont uniques dans K. Il en résulte bien que $\alpha \in K^+$. Puisque

G est abélien il en résulte aussi que $\sigma(\alpha) \in K^+$ pour tout $\sigma \in G$. De plus $\sigma(\alpha)^q = (1 - t\sigma(\zeta_p))^\theta = F^\sigma(t)^q$. Toutefois nous avons vu que $F^\sigma(t) \in \mathbb{R}$, donc $F^\sigma(t)/\sigma(\alpha)$ est une racine q-ième de l'unité réelle dans $\mathbb{C}$. Puisque q est impair elle doit être égale à 1, ce qui démontre la proposition. □

Remarque. — Bien qu'assez simple, ce dernier raisonnement est l'un des plus subtils de la démonstration, et a été initialement oublié, rendant la démonstration initiale incomplète.

8.5. Démonstration du quatrième théorème de Mihăilescu

Nous avons étudié ci-dessus des propriétés des unités cyclotomiques, de la partie plus des corps cyclotomiques et des séries entières, sans référence explicite à la conjecture de Catalan, en dehors de l'omniprésence des nombres premiers impairs distincts p et q. Nous commençons maintenant la démonstration proprement dite. Nous conservons bien sûr toutes les notations ci-dessus, et en particulier nous rappelons que $R = \mathbb{F}_q[G^+]$.

Théorème 8.20. — *Soient p et q deux nombres premiers impairs distincts tels que* $\min(p, q) \geqslant 11$*, et soient x et y deux entiers non nuls tels que $x^p - y^q = 1$. Le sous-module de S^+ engendré par la classe $[x - \zeta_p]^{1+\iota}$ est libre, en d'autres termes* $\mathrm{Ann}_R([x - \zeta_p]^{1+\iota}) = 0$.

Démonstration. — Rappelons que puisque $[x-\zeta_p] \in S$ on a effectivement $[x-\zeta_p]^{1+\iota} \in S^+$. Donc, soit $\overline{\psi} = \sum_{\sigma \in G^+} \nu_\sigma \sigma \in \mathrm{Ann}_R([x-\zeta_p]^{1+\iota})$ avec $\nu_\sigma \in \mathbb{F}_q$, donc tel que $[x - \zeta_p]^{(1+\iota)\overline{\psi}} = 1$. Comme ci-dessus, soit P un système de représentants dans G de $G^+ = G/\langle\iota\rangle$, et par abus de notation, si $\sigma \in G^+$ nous écrirons encore σ pour l'élément de P dont la classe est égale à σ. Si on pose $\psi = \sum_{\sigma \in P} \nu_\sigma \sigma$ on a donc $[x - \zeta_p]^{(1+\iota)\psi} = 1$. Par définition de S il en résulte que pour tout $\theta \in \mathbb{Z}[G]$ dont la réduction modulo q est égale à $\pm(1 + \iota)\psi$ on a $(x - \zeta_p)^\theta \in K^{*q}$. Si pour $\sigma \in P$ on pose $\nu_{\iota\sigma} = \nu_\sigma$, nous avons $(1 + \iota)\psi = \sum_{\sigma \in G} \nu_\sigma \sigma \in \mathbb{F}_q[G]$. Soit $\theta_1 = \sum_{\sigma \in G} n_\sigma \sigma \in \mathbb{Z}[G]$ le relèvement de $(1+\iota)\psi$ tel que $0 \leqslant n_\sigma < q$, et donc tel que $\|\theta_1\| < (p-1)q$. Si pour tout entier n tel que $0 \leqslant n < q$ on pose $c(n) = q - n$ pour $n \neq 0$ et $c(0) = 0$, on a encore $0 \leqslant c(n) < q$, et évidemment $n + c(n) \leqslant q$. Il en résulte que $\theta_2 = \sum_{\sigma \in G} c(n_\sigma)\sigma$ est un relèvement de $-(1 + \iota)\psi$, que $0 \leqslant c(n_\sigma) < q$, et donc que $\|\theta_2\| + \|\theta_1\| \leqslant q(p - 1)$. Il en résulte

que pour $i = 1$ ou pour $i = 2$ on doit avoir $\|\theta_i\| \leqslant q(p-1)/2$, et nous appellerons θ celui des deux θ_i (ou l'un des deux) qui satisfait à cette inégalité.

Soit $\alpha \in K^*$ tel que $(x-\zeta_p)^\theta = \alpha^q$. D'après le lemme 3.8 nous savons que $\beta = (x-\zeta_p)/(1-\zeta_p) \in \mathbb{Z}_K$, que $v_{\mathfrak{p}}(\beta) = 0$, et que les idéaux engendrés par les conjugués de β sont premiers entre eux deux à deux. Il en résulte que pour tout $\sigma \in G$ on a $v_{\mathfrak{p}}(x-\sigma(\zeta_p)) = 1$. Ainsi

$$\begin{aligned}\|\theta\| &= \sum_{\sigma\in G} n_\sigma v_{\mathfrak{p}}(x-\sigma(\zeta_p)) = v_{\mathfrak{p}}\Big(\prod_{\sigma\in G}(x-\sigma(\zeta_p))^{n_\sigma}\Big)\\ &= v_{\mathfrak{p}}\left((x-\zeta_p)^\theta\right) = qv_{\mathfrak{p}}(\alpha) \equiv 0 \pmod q.\end{aligned}$$

Puisque $0 \leqslant \|\theta\| \leqslant q(p-1)/2$ il en résulte qu'il existe $m \in [0,(p-1)/2]$ tel que $\|\theta\| = mq$. De plus, puisque n_σ et $n_{\iota\sigma}$ modulo q sont tous deux égaux à ν_σ et qu'ils sont dans l'intervalle $[0, q-1]$ ils sont en fait égaux. Il en résulte que $\theta = (1+\iota)\phi$, où $\phi = \sum_{\sigma\in P} n_\sigma\sigma$ est un relèvement de ψ. En particulier, pour tout $\sigma \in G$, $(x-\sigma(\zeta_p))^\theta = ((x-\sigma(\zeta_p))(z-\iota(\sigma(\zeta_p))))^\phi$ est un nombre réel. Comme les racines q-ièmes sont uniques dans K, quand elles existent, il en résulte que tous les conjugués de α sont réels. Puisque pour $x \in \mathbb{Q}$ on a $x^\theta = x^{\|\theta\|}$, on voit que pour tout $\sigma \in G$ on a $(1-\sigma(\zeta_p)/x)^\theta = (\sigma(\alpha)/x^m)^q$. Comme $1/x \in \mathbb{Q}$ et que $|1/x| < 1$ nous pouvons appliquer la proposition 8.19 et en déduire que pour tout $\sigma \in G$ on a $\sigma(\alpha) = x^m F^\sigma(1/x)$, où $F = F_\theta$. Posons

$$I_\sigma = q^{m+v_q(m!)}|\sigma(\alpha) - x^m F_m^\sigma(1/x)|.$$

Nous allons maintenant utiliser un argument voisin de celui utilisé dans la preuve du théorème de Cassels, et montrer que $|I_\sigma| < 1$ et que $\prod_{\sigma\in G} I_\sigma \in \mathbb{Z}$. Tout d'abord, d'après la proposition 8.18 (3) on a

$$\begin{aligned}I_\sigma &= q^{m+v_q(m!)}|x|^m|F^\sigma(1/x) - F_m^\sigma(1/x)|\\ &\leqslant q^{m+v_q(m!)}\binom{2m}{m+1}|x|^{-1}(1-1/|x|)^{-(2m+1)}\\ &\leqslant q^{m+m/(q-1)+m(\log(4)/\log(q))}|x|^{-1}(1-1/|x|)^{-(2m+1)},\end{aligned}$$

où nous avons utilisé le fait que $v_q(m!) \leqslant m/(q-1)$ et que $\binom{2m}{k} \leqslant 2^{2m}$. Puisque $m \leqslant (p-1)/2$ et que d'après le théorème de Hyrrö on a

$|x| \geqslant q^{p-1}$, il en résulte que

$$\begin{aligned} I_\sigma &\leqslant q^{((p-1)/2)(1+1/(q-1)+\log(4)/\log(q))}|x|^{-1}(1-1/|x|)^{-p} \\ &\leqslant q^{((p-1)/2)(-1+1/(q-1)+\log(4)/\log(q))}(1-1/q^{p-1})^{-p}. \end{aligned}$$

Or $I_\sigma < 1$ équivaut à $\log(I_\sigma)/\log(q) < 0$, et on a

$$\frac{\log(I_\sigma)}{\log(q)} = \frac{p-1}{2}\left(-1+\frac{1}{q-1}+\frac{\log(4)}{\log(q)}\right) - \frac{p}{\log(q)}\log(1-1/q^{p-1}).$$

D'après le théorème des accroissements finis il existe $c \in [0,1]$ tel que

$$\begin{aligned} -\log(1-1/q^{p-1}) &= \log(q^{p-1}) - \log(q^{p-1}-1) \\ &= \frac{1}{q^{p-1}-c} \leqslant \frac{1}{q^{p-1}-1} \leqslant \frac{1}{q^2-1}, \end{aligned}$$

puisque $p \geqslant 3$. Puisque nous avons supposé que $q \geqslant 7$ on en déduit immédiatement que

$$\frac{\log(I_\sigma)}{\log(q)} \leqslant \frac{p-1}{2}\left(-1+\frac{1}{6}+\frac{\log(4)}{\log(7)}\right) + \frac{p}{48\log(7)} \leqslant -0.0497p + 0.061,$$

ce qui est strictement négatif dès que $p \geqslant 2$, ce qui montre qu'on a bien $I_\sigma < 1$.

Étudions maintenant les propriétés arithmétiques de I_σ. D'après la proposition 8.18 on a $F_m^\sigma(T) = \sum_{0\leqslant k\leqslant m} a_k/(q^k k!)T^k$ avec $a_k \in \mathbb{Z}_K$. Il en résulte que $q^{m+v_q(m!)}a_k/(q^k k!) \in \mathbb{Z}_K$, et donc que $q^{m+v_q(m!)}x^m F_m^\sigma(1/x) \in \mathbb{Z}_K$ (notons qu'il n'y a ici aucun problème de convergence puisque nous ne considérons que des *polynômes*). De plus puisque $(x-\zeta_p)^\theta = \alpha^q$ *et que tous les coefficients de* θ *sont positifs ou nuls* α^q est un *entier* algébrique, et il en va donc de même de α, donc $\alpha \in \mathbb{Z}_K = \mathbb{Z}[\zeta_p]$. Il en résulte que $\gamma = q^{m+v_q(m!)}(\alpha - x^m F_m(1/x)) \in \mathbb{Z}_K$, donc que $\mathcal{N}_{K/\mathbb{Q}}(\gamma) \in \mathbb{Z}$. Or $|\mathcal{N}_{K/\mathbb{Q}}(\gamma)| = \prod_{\sigma\in G} I_\sigma < 1$ d'après ce que nous avons démontré ci-dessus. Il en résulte que $\mathcal{N}_{K/\mathbb{Q}}(\gamma) = 0$, et donc que $\gamma = 0$, en d'autres termes que

$$q^{m+v_q(m!)}\alpha = \sum_{0\leqslant k\leqslant m} q^{m+v_q(m!)}\frac{a_k}{q^k k!}x^{m-k}.$$

Nous sommes maintenant proches de la conclusion voulue : tous les termes de la somme ci-dessus sont divisibles par q sauf le terme avec $k = m$. On a donc $0 \equiv (q^{v_q(m!)}/m!)a_m \pmod{q\mathbb{Z}_K}$, donc $a_m \equiv 0 \pmod{q\mathbb{Z}_K}$. D'autre part d'après la proposition 8.18 on a $a_m \equiv s^m$

(mod $q\mathbb{Z}_K$), où $s = -\sum_{\sigma\in G} n_\sigma\sigma(\zeta_p)$. Ainsi $s^m \equiv 0 \pmod{q\mathbb{Z}_K}$, et donc pour tout idéal premier $\mathfrak{q}$ de K au-dessus de q on a $s^m \in \mathfrak{q}$, donc $s \in \mathfrak{q}$, et puisque q est non ramifié, d'après le théorème chinois on en déduit que $s \equiv 0 \pmod{q\mathbb{Z}_K}$, en d'autres termes que $\sum_{\sigma\in G}(n_\sigma/q)\sigma(\zeta_p) \in \mathbb{Z}_K$. Puisque les $\sigma(\zeta_p)$ sont à permutation près les ζ_p^j pour $1 \leqslant j \leqslant p-1$ qui forment une $\mathbb{Z}$-base de $\mathbb{Z}_K$ il en résulte que $n_\sigma/q \in \mathbb{Z}$ pour tout σ, et puisque $0 \leqslant n_\sigma < q$ on en déduit que $n_\sigma = 0$ pour tout σ. Donc $\theta = 0$, et donc $\psi = 0$ et donc $\overline{\psi} = 0$, ce qui démontre le théorème. □

Le quatrième théorème de Mihăilescu est maintenant évident :

Théorème 8.21. — *Soient p et q deux nombres premiers impairs distincts tels que* $\min(p,q) \geqslant 11$*, et soient x et y des entiers non nuls tels que $x^p - y^q = 1$. Alors $p \equiv 1 \pmod q$* ou bien *$q \equiv 1 \pmod p$.*

Démonstration. — D'après le théorème 8.20 ci-dessus, on a

$$\mathrm{Ann}_R([x-\zeta_p]^{1+\iota}) = 0.$$

D'après le premier théorème de Mihăilescu (théorème 5.4), nous savons que $q^2 \mid x$, et comme d'habitude $(-\zeta_p)$ est une puissance q-ième. Il en résulte que $x-\zeta_p \equiv \beta^q \pmod{q^2R_p}$, donc que $[x-\zeta_p] \in S_q$, donc que $[x-\zeta_p]^{1+\iota} \in S_q \cap S^+$. Par symétrie, supposons par exemple que $p > q$, ce qui implique évidemment que $q \not\equiv 1 \pmod p$. Si nous supposons par l'absurde que $p \not\equiv 1 \pmod q$ le théorème 8.14 nous dit que $\mathrm{Ann}_{\mathbb{F}_q[G^+]}(S^+ \cap S_q) \neq 0$, et donc en particulier $\mathrm{Ann}_R([x-\zeta_p]^{1+\iota}) \neq 0$, contradiction. □

8.6. Conclusion : Démonstration de la conjecture de Catalan. — Nous allons maintenant résumer tout le travail que nous avons fait et voir que nous avons en fait démontré la conjecture. Soient x et y deux entiers non nuls et m et $n \geqslant 2$ tels que $x^m - y^n = 1$. D'après le résultat de V. Lebesgue nous savons que le cas $n = 2$ est impossible, et donc *a fortiori* le cas n pair. De même le résultat de Ko Chao nous dit que le cas m pair est impossible, en dehors de l'égalité $3^2 - 2^3 = 1$. On peut donc supposer que m et n sont impairs, et il suffit de démontrer l'impossibilité de l'équation quand $m = p$ et $n = q$ sont des nombres premiers impairs. En particulier l'équation devient symétrique puisque nous pouvons changer (p,q,x,y) en $(q,p,-y,-x)$.

D'après le deuxième théorème de Mihăilescu (plus précisément d'après son corollaire 6.13) nous pouvons supposer que $\min(p,q) \geqslant 11$ (en fait 43, mais 11 nous suffit). D'après le quatrième théorème de Mihăilescu (théorème 8.21), en échangeant p et q si nécessaire grâce à la symétrie, nous pouvons supposer que $p \equiv 1 \pmod{q}$. D'après la formule du binôme on a

$$p^q = (1+(p-1))^q = 1 + q(p-1) + \sum_{2 \leqslant i \leqslant q-1} \binom{q}{i} (p-1)^i + (p-1)^q \equiv 1 \pmod{q^2}.$$

D'autre part d'après le premier théorème de Mihăilescu (théorème 5.4) nous savons que $p^{q-1} \equiv 1 \pmod{q^2}$, et donc $p^q \equiv p \pmod{q^2}$, ce qui combiné avec la congruence ci-dessus montre que $p \equiv 1 \pmod{q^2}$. Enfin d'après le troisième théorème de Mihăilescu (théorème 7.7) nous savons que $p < 4q^2$. Il en résulte que $p = 1 + kq^2$ avec $k = 1$, 2 ou 3. Les cas $k = 1$ et $k = 3$ sont exclus puisque sinon p serait pair, et le cas $k = 2$ est également exclu puisque $q^2 \equiv 1 \pmod{3}$ donc que p serait divisible par 3, ce qui termine la démonstration de la conjecture de Catalan !!!. □

Références

[1] Y. Bilu – « Catalan's conjecture (after Mihailescu) », in *Séminaire Bourbaki 2002/2003*, Astérisque, vol. 294, Société Mathématique de France, 2004, Exp. n° 909, p. 1–25.

[2] W. Keller & J. Richstein – « Solutions de the congruence $a^{p-1} \equiv 1 \pmod{p^r}$ », *Math. Comp.* **74** (2005), p. 927–936.

[3] M. Mischler – « La conjecture de Catalan racontée à un ami qui a le temps », preprint disponible à l'adresse `http://arxiv.org/pdf/math.NT/0502350`, 2005.

[4] L. Washington – *Introduction to cyclotomic fields*, 2e éd., Graduate Texts in Math., vol. 83, Springer-Verlag, 1997.

H. Cohen, Laboratoire A2X, U.M.R. 5465 du C.N.R.S., Université Bordeaux I, 351 Cours de la Libération, 33405 Talence Cedex (France)
E-mail : `Henri.Cohen@math.u-bordeaux1.fr`