Le théorème de Hasse-Minkowski

Yichang CAI et Nicolas MOUTAL,

sous la supervision de Diego IZQUIERDO

Introduction

Notre exposé porte sur le théorème de Hasse-Minkowski, qui est originellement un théorème de classification des formes quadratiques sur $\mathbf{Q}$, prouvé par Hasse en 1923. Il répond à des questions comme « quels sont les entiers qui s'écrivent comme somme de trois carrés d'entiers ? », ou encore « quels sont les points rationnels d'une conique donnée ? ». Le principe de base qu'incarne ce théorème est le « principe local-global ». Ce principe exprime que pour étudier une équation sur $\mathbf{Q}$ (aspect global), il est suffisant d'étudier ses propriétés dans $\mathbf{R}$, et dans $\mathbf{Z}$ modulo $p, p^2, p^3, \ldots$, pour tout nombre premier p (aspect local)[1]. Ce principe n'est pas propre à $\mathbf{Q}$, et Hasse prouva notamment en 1924 qu'il restait vérifié pour les extensions finies de $\mathbf{Q}$.

Dans cet exposé, nous avons étudié le théorème de Hasse-Minkowski sur les corps $\mathbf{F}_q(t)$, où q est une puissance d'un nombre premier impair. Bien qu'à première vue $\mathbf{F}_q(t)$ et $\mathbf{Q}$ paraissent assez différents (en particulier, l'un est de caractéristique nulle et pas l'autre), les anneaux associés $\mathbf{F}_q[t]$ et $\mathbf{Z}$ partagent de nombreuses similarités : ils sont tous deux principaux, ont une infinité d'idéaux premiers, et tous leurs corps résiduels (c'est-à-dire leur quotient par un idéal premier) sont finis. La démonstration sur $\mathbf{F}_q(t)$ suit essentiellement la même démarche que celle sur $\mathbf{Q}$, et nous mettrons en valeur leurs ressemblances et divergences au cours de l'exposé.

La démonstration du théorème de Hasse-Minkowski est mathématiquement riche : de nature essentiellement algébrique, elle repose néanmoins sur des propriétés topologiques (en particulier en ce qui concerne les corps v-adiques), et analytiques (on aura à démontrer le fameux « théorème de la progression arithmétique de Dirichlet », qui nécessite de l'analyse complexe).

Une question naturelle se pose une fois le théorème démontré : peut-on le généraliser ? On a déjà mentionné que le « principe local-global » reste vrai pour une plus grande classe de corps (au moins pour les extensions finies de $\mathbf{Q}$ et $\mathbf{F}_q(t)$). Une autre direction de généralisation est de passer des formes quadratiques aux polynômes de degré supérieur. Bien que le principe reste vrai pour certaines classes d'équations, il est manifestement faux lorsqu'on augmente le degré. Il est assez facile de construire des contre-exemples de degré élevé, comme nous le verrons ; mais un contre-exemple emblématique est celui de Selmer, qui a donné une équation cubique de trois variables ne vérifiant pas le principe. Nous présenterons ce contre-exemple dans une deuxième partie.

1. Ceci peut apparaître à première vue comme une complication, car il y a une infinité de nombres premiers et de puissances de nombres premiers à étudier, mais nous verrons que d'une part, seul un nombre fini de nombres premiers est à étudier à chaque fois, et d'autre part que ceux-ci s'étudient très simplement à l'aide de quelques invariants.

Notre responsable d'exposé, Diego Izquierdo, a été d'une grande aide tant par ses nombreuses explications que par ses relectures attentives. Il nous a proposés de nous attaquer au théorème sur $\mathbf{F}_q(t)$ plutôt que sur $\mathbf{Q}$, ce qui nous a permis de fournir un vrai travail personnel : nous lui en sommes très reconnaissants. Merci !

Table des matières

Chapitre 1

Le théorème de Hasse-Minkowski

Le théorème de Hasse-Minkowski affirme que le « principe local-global » (aussi appelé « principe de Hasse ») est vrai pour les formes quadratiques sur $\mathbf{F}_q(t)$. Cela signifie qu'une forme quadratique à coefficients dans $\mathbf{F}_q[t]$ s'annule non trivialement dans $\mathbf{F}_q(t)$ si et seulement si elle s'annule non-trivalement dans $\mathbf{F}_q[t]/X\mathbf{F}_q[t]$, pour tout $X \in \mathbf{F}_q[t] - \{0\}$, ainsi que dans $\mathbf{F}_q[1/t]/(1/t)^n\mathbf{F}_q[1/t]$, pour tout $n \geq 1$ [1]. Cet ensemble de conditions s'exprime de façon plus naturelle dans le langage des « corps v-adiques », que nous allons présenter maintenant.

1.1 Corps v-adiques

Dans cette partie, nous allons introduire les corps « v-adiques » $\mathbf{F}_q(t)_v$, un ingrédient essentiel du théorème.

Nous commençons par des choses assez générales.

Définition 1.1. Soit k un corps quelconque.

– Une *valeur absolue* sur le corps k est une fonction $|\cdot| : k \to \mathbf{R}$ possédant les propriétés suivantes :

1. Pour tout $x \in k$, $|x| \geq 0$, et $|x| = 0 \iff x = 0$.
2. Pour tous x, $y \in k$, $|xy| = |x| \cdot |y|$.
3. Pour tous x, $y \in k$, $|x + y| \leq |x| + |y|$.

1. En notant f la forme quadratique, on entend par là que pour tout $X \in \mathbf{F}_q[t] - \{0\}$, il existe $Y \in \mathbf{F}_q[t] - \{0\}$ tel que $f(Y) \equiv 0 \pmod{X}$, et : pour tout $n \geq 1$, il existe $Y \in \mathbf{F}_q[1/t]$ tel que $f(Y) \in \mathbf{F}_q[1/t]$ et $f(Y) \equiv 0 \pmod{(1/t)^n}$ dans $\mathbf{F}_q[1/t]$.

– La valeur absolue qui vérifie : pour tout $x \neq 0$, $|x| = 1$ est appelée *valeur absolue triviale*.
– Deux valeurs absolues $|\cdot|_1$, $|\cdot|_2$ sont *équivalentes* si il existe $\alpha > 0$ tel que $|\cdot|_1 = |\cdot|_2^{\alpha}$.

Remarque 1.1. La définition implique notamment que $|1| = 1$ et que $|\zeta| = 1$ pour toute racine de l'unité ζ.

La définition ci-dessus n'est pas sans rappeler celle d'une *norme* sur un espace vectoriel. De la même façon, il est possible de définir une topologie à partir d'une valeurs absolue. Celle-ci sera alors métrique et séparée, en vertu de l'inégalité triangulaire (condition 3). De plus, l'équivalence de deux valeurs absolues correspond à l'égalité des topologies associées.

On peut distinguer deux grandes classes de valeurs absolues, qui sont compatibles avec la relation d'équivalence de la définition ci-haut.

Définition 1.2. Une valeur absolue $|\cdot|$ est dite *archimédienne* si elle vérifie :

$$\forall x,\, y \in k^*,\, \exists n \in \mathbf{N},\, |nx| > |y| \ .$$

Autrement, elle est dite *non-archimédienne*.

On a alors la caractérisation simple suivante :

Théorème 1.1. *Une valeur absolue $|\cdot|$ est non-archimédienne si et seulement si elle satisfait l'inégalité triangulaire forte : pour tous x, $y \in k$, $|x + y| \leq \max(|x|, |y|)$.*

Démonstration. Supposons d'abord que l'inégalité triangulaire forte est vérifiée : cela implique par récurrence que pour tout $n \in \mathbf{N}$, $|n| \leq |1|$, ce qui montre clairement que $|\cdot|$ est non-archimédienne.

Réciproquement, supposons que la valeur absolue $|\cdot|$ est non-archimédienne. Alors il existe x_0,$y_0 \in k^*$ tels que : pour tout $n \in \mathbf{N}$, $|nx_0| \leq |y_0|$. Posons $C = \frac{|y_0|}{|x_0|}$: on a, pour tout $n \in \mathbf{N}$, $|n| \leq C$. Soient maintenant x, $y \in k$ quelconques. On calcule :

$$|(x+y)^n| \leq \sum_{k=0}^{n} \left|\binom{n}{k}\right| \cdot |x|^k |y|^{n-k} \leq C(n+1)\max(|x|,|y|)^n \ ,$$

et en passant à la puissance $1/n$ et en faisant $n \to \infty$, on obtient l'inégalité triangulaire forte. □

Corollaire 1.1.1. *Soit $|\cdot|$ une valeur absolue non-archimédienne ; si $|x| < |y|$, alors $|x + y| = |y|$.*

Démonstration. Il suffit d'appliquer l'inégalité triangulaire forte à $(x+y) = x+y$ et à $y = (x+y)+(-x)$: on obtient successivement $|x+y| \leq \max(|x|,|y|) = |y|$ et $|y| \leq \max(|x+y|,|-x|)$. Or $|y| > |x|$, donc on a nécessairement, vue la deuxième inégalité, $|x+y| > |x|$, puis $|y| \leq |x+y| \leq |y|$, d'où les inégalités sont en fait des égalités. □

Une conséquence simple, mais utile :

Corollaire 1.1.2. *Soient $a_1, \ldots, a_n \in k$ qui vérifient $\forall i \geq 1, |a_i| \leq |a_1|$. Si $|a_1 + \cdots + a_n| < |a_1|$, alors il existe $i_0 \in \{2, \ldots, n\}$ tel que $|a_{i_0}| = |a_1|$.*

Nous allons maintenant étudier les valeurs absolues sur $\mathbf{F}_q(t)$. Remarquons que comme $\mathbf{F}_q$ est un corps fini, tous ses éléments sont des racines de l'unité, et donc toute restriction d'une valeur absolue sur $\mathbf{F}_q(t)$ à $\mathbf{F}_q$ est triviale. En particulier, toute valeur absolue est non-archimédienne. On considère deux cas :

1. $|t| > 1$. Notons C cette valeur. Alors tout polynôme $F(t) = a_0 + \cdots + a_n t^n$ a pour valeur absolue $|F| = C^n$, et par extension, toute fraction rationnelle R a pour valeur absolue $|R| = C^{\deg(R)}$. Réciproquement, si on choisit un nombre réel $C_0 > 1$, la formule $|R|_0 = C_0^{\deg(R)}$ définit une valeur absolue qui lui est équivalente.
2. $|t| \leq 1$. Alors tout polynôme F vérifie $|F| \leq 1$. Considérons l'ensemble des polynômes vérifiant $|F| < 1$: c'est clairement un idéal de $\mathbf{F}_q[t]$ et il est non vide si et seulement si la valeur absolue est non triviale. Excluons le cas trivial, et considérons un générateur unitaire P de l'idéal. Le polynôme P est nécessairement irréductible : car si $P = AB$, alors $|AB| = |A||B| < 1$ par définition, donc $|A| < 1$ ou $|B| < 1$ et P divise A ou B. Notons $C = |P|$. Alors pour tout polynôme F, $|F| = C^{v_P(F)}$, où on a dénoté par $v_P(F)$ la puissance de P dans la décomposition en produit de facteurs premiers de F ; et ce calcul s'étend sans problèmes aux fractions rationnelles. Réciproquement, fixant P un polynôme irréductible unitaire et $C < 1$, une telle formule définit une valeur absolue sur $\mathbf{F}_q(t)$.

En prenant quelques conventions, on a démontré le résultat suivant.

Théorème 1.2. *Notons $\mathscr{V}$ la réunion de l'ensemble des polynômes irréductibles unitaires de $\mathbf{F}_q(t)^*$ et du symbole ∞. Les seules valeurs absolues sur $\mathbf{F}_q(t)$ sont, à équivalence près, les $|\cdot|_v$, pour $v \in \mathscr{V}$, définies de la manière suivante :*

- *Si $v = P$, $|F|_P = \left(\frac{1}{q}\right)^{\deg(P)\cdot v_P(F)}$.*
- *Si $v = \infty$, $|F|_\infty = q^{\deg(F)}$.*

Remarque 1.2.
- La valeur absolue « infinie » n'a rien de spécial par rapport aux autres valeurs absolues : tout se passe comme si elle provenait du « polynôme irréductible $1/t$ » ; une autre façon de le dire est de remarquer que la valeur absolue infinie de $\mathbf{F}_q(t)$ correspond à la valeur absolue issue du polynôme $1/t$ dans $\mathbf{F}_q(1/t)$. Géométriquement, les valeurs absolues correspondent aux points fermés de la droite projective $\mathbf{P}^1_{\mathbf{F}_q}$, et la valeur absolue infinie correspond justement au point à l'infini sur celle-ci. C'est très différent du cas du corps $\mathbf{Q}$, dont les valeurs absolues sont les valeurs absolues non-archimédiennes attachés aux nombres premiers, ainsi qu'une valeur absolue « infinie », *archimédienne*, qui est la valeur absolue usuelle sur $\mathbf{R}$ (voir par exemple [2], page 119).
- Ces conventions sont faites de sorte que pour tout polynôme irréductible unitaire P, on ait : $|P|_P|P|_\infty = 1$. Par multiplicativité, on obtient notamment : pour tout $F \in \mathbf{F}_q(t)$, presque tous les $|F|_v$ sont égaux à 1, et :
$$\prod_{v \in \mathscr{V}} |F|_v = 1 \, .$$

On a déjà remarqué qu'à toute valeur absolue on pouvait associer une topologie, de la même façon que la valeur absolue induit une topologie sur $\mathbf{Q}$ par exemple. Par le même procédé que la complétion de $\mathbf{Q}$ en $\mathbf{R}$, c'est-à-dire avec des suites de Cauchy, il est possible de *compléter* la topologie associée à une valeurs absolue. On obtient alors pour chaque valeur absolue $|\cdot|_v$ un corps complet $\mathbf{F}_q(t)_v$ associé, qu'on appelle *corps v-adique*. La valeur absolue $|\cdot|_v$ s'étend naturellement à $\mathbf{F}_q(t)_v$.

Remarque 1.3. Par exemple, dans le cas de la valeur absolue « infinie » $|\cdot|_\infty$, le corps $\mathbf{F}_q(t)_\infty$ associé est le corps des séries formelles en $1/t$: $\mathbf{F}_q\left(\left(\frac{1}{t}\right)\right)$. En effet, d'une part ce corps est complet et contient $\mathbf{F}_q(t)$, d'autre part toute série $\sum_{n=k}^{\infty} a_n(1/t)^n$, où $k \in \mathbf{Z}$, $a_n \in \mathbf{F}_q$, converge dans $\mathbf{F}_q(t)_\infty$.

En fait, le cas des autres valeurs absolues est parfaitement identique, et on peut voir toute complétion $\mathbf{F}_q(t)_P$ comme le corps des séries formelles en P, où P est irréductible unitaire. Ainsi, si $\deg(P) = d$, on a que $\mathbf{F}_q(t)_P$ est isomorphe à $\mathbf{F}_{q^d}((t))$.

Enfin on voit, comme on l'a laissé entendre au début de ce chapitre, qu'une équation polynômiale est vérifiée dans $\mathbf{F}_q(t)_P$ si et seulement si elle est vérifiée modulo P^n, pour tout $n \geq 1$.

Étudions maintenant la structure des corps obtenus.

Définition 1.3. Pour tout $v \in \mathscr{V}$, on note $\mathcal{O}_v = \{F \in \mathbf{F}_q(t)_v \mid |F|_v \leq 1\}$, et $\mathcal{U}_v = \{F \in \mathbf{F}_q(t)_v \mid |F|_v = 1\}$. Soit enfin $\mathfrak{m}_v = \mathcal{O}_v - \mathcal{U}_v = \{F \in \mathbf{F}_q(t)_v \mid |F|_v < 1\}$.

On a alors la proposition facile suivante.

Proposition 1.1. *Soit $v \in \mathscr{V}$, et $|\cdot|_v$ la valeur absolue associée. Alors $\mathcal{O}_v$ est un anneau intègre, complet, $\mathcal{U}_v$ est son groupe des inversibles et $\mathbf{F}_q(t)_v$ son corps des fractions. De plus, $\mathfrak{m}_v$ est l'unique idéal maximal de $\mathcal{O}_v$. Enfin, tout élément de $\mathbf{F}_q(t)_v^*$ s'écrit de façon unique sous la forme $\pi^n u$, où $u \in U$, $n \in \mathbf{Z}$, et $\pi = v$ si v est un polynôme premier ou $\pi = 1/t$ si $v = \infty$.*

On dit que $\mathcal{O}_v$ est un *anneau de valuation discrète*.

Remarque 1.4. Attention, $\mathbf{F}_q[t]$ n'est *pas* contenu dans $\mathcal{O}_\infty$, ce qui est un peu trompeur. Pour les autres valeurs absolues, ce problème ne se pose pas, et on a même que $\mathcal{O}_v$ est la complétion pour $|\cdot|_v$ de $\mathbf{F}_q[t]$, si $v \neq \infty$.

Voici maintenant le lemme de Hensel, qui permet d'améliorer des solutions approchées.

Lemme 1.1. *Soit $v \in \mathscr{V}$, et $\mathcal{O}_v$ l'anneau associé. Soit f un polynôme à coefficients dans $\mathcal{O}_v$ et f' sa dérivée formelle. Supposons qu'il existe $x \in \mathcal{O}_v$ tel que $|f(x)|_v < |f'(x)|_v^2$. Alors il existe $x_0 \in \mathcal{O}_v$ tel que $x_0 \equiv x \pmod{\mathfrak{m}_v}$ et $f(x_0) = 0$.*

Démonstration. Supposons pour simplifier l'écriture que $v = P$ est un polynôme irréductible unitaire ; notons $\alpha = q^{-\deg(P)} < 1$. Il existe alors des entiers naturels n, k tels que $2k < n$, $|f(x)|_P \leq \alpha^n$, $|f'(x)|_P = \alpha^k$. On va améliorer progressivement la solution : soit x_1 de la forme $x + P^{n-k}y$, où $y \in \mathcal{O}_P$ est à déterminer. Alors :

$$f(x_1) = f(x) + P^{n-k} y f'(x) + P^{2n-2k} r(x) \ ,$$

où $r(x)$ est la suite du développement de Taylor, et est donc un élément de $\mathcal{O}_P$. Mais par hypothèse, $2n - 2k > n$, donc on a

$$\Big| f(x + P^{n-k}y) - \Big(f(x) + P^{n-k} y f'(x) \Big) \Big|_P \leq \alpha^{n+1} \ .$$

Écrivons enfin $f'(x) = P^k u$, où $u \in \mathcal{U}_P$. Alors, en posant $y = -P^{-n} u^{-1} f(x)$, on a d'une part $y \in \mathcal{O}_P$, et d'autre part $|f(x + P^{n-k}y)|_P \leq \alpha^{n+1}$. Enfin,

$$\Big| f'(x + P^{n-k}y) \Big|_P = \Big| f'(x) + P^{n-k} y f''(x) + P^{2n-2k} r'(x) \Big|_P = |f'(x)|_P \ ,$$

car $n - k > k$. Ainsi, on est passé de $|f(x)|_P \leq \alpha^n$ à $|f(x_1)|_P \leq \alpha^{n+1}$, avec $|x - x_1|_P \leq \alpha^{n-k}$ et tout en gardant $|f'(x_1)|_P = \alpha^k$. Recommençons la même procédure : on obtient $x_2 \in \mathcal{O}_P$ tel que $|f(x_2)|_P \leq \alpha^{n+2}$, avec $|x_1 - x_2|_P \leq \alpha^{n+1-k}$, et toujours $|f'(x_2)|_P \leq \alpha^k$; puis en itérant on obtient

une suite $(x_j)_{j\geq 1}$ qui vérifie : $|f(x_j)|_P \leq \alpha^{n+j}$ et $|x_j - x_{j+1}|_P \leq \alpha^{n+j-k}$, pour tout $j \geq 1$.

Comme la valeur absolue $|\cdot|_P$ est non-archimédienne, la dernière inégalité fait de $(x_j)_{j\geq 1}$ une suite de Cauchy : elle converge donc vers un $x_0 \in \mathcal{O}_v$; on a bien sûr $f(x_0) = 0$ et $|x - x_0| \leq \alpha^{n-k}$; *a fortiori* $x \equiv x_0 \pmod{\mathfrak{m}_v}$. □

On en déduit une version multi-variables, qui nous sera très utile.

Théorème 1.3 (Hensel)**.** *Soit $v \in \mathcal{V}$, et f un polynôme de m variables à coefficients dans $\mathcal{O}_v$. Supposons qu'il existe $x \in \mathcal{O}_v^m$ et $j \in \{1, \ldots, m\}$ tels que $|f(x)|_v < |\frac{\partial f}{\partial X_j}(x)|_v^2$. Alors il existe $x_0 \in \mathcal{O}_v^m$ tel que $f(x_0) = 0$ et $x_0 \equiv x \pmod{\mathfrak{m}_v}$ (composante par composante).*

Démonstration. Cela découle directement du lemme, appliqué au polynôme en une variable $\tilde{f}(X) = f(x_1, \ldots, x_{j-1}, X, x_{j+1}, \ldots, x_m)$, où on a noté $x = (x_1, \ldots, x_m)$. □

Remarque 1.5. Le lemme de Hensel est en fait une « implémentation v-adique » de la méthode de Newton. C'est un résultat très général qui est vrai sur tout anneau de valuation discrète, par exemple sur les complétions de $\mathbf{Q}$ par rapport à ses valeurs absolues non-archimédiennes.

Le cas particulier des formes quadratiques nous intéresse. On suppose dans la suite que q est *impair*. On rappelle de plus la définition du *discriminant* d'une forme quadratique sur un corps k : en écrivant la forme quadratique sous forme matricielle, $f(X) = {}^tXM_fX$, le discriminant de f est la classe du déterminant de M_f dans k^*/k^{*2}. Il est notamment invariant par changement de base.

Corollaire 1.3.1. *Soit $v \in \mathcal{V}$, et f une forme quadratique à coefficients dans $\mathcal{O}_v$. Supposons que le discriminant de f soit inversible. Alors, si $a \in \mathcal{O}_v$, toute solution primitive de l'équation $f(x) \equiv a \pmod{\mathfrak{m}_v}$ se relève en une solution de $f(x) = a$ dans $\mathcal{O}_v$.*

Démonstration. Écrivons $f(X)$ sous la forme matricielle ${}^tXM_fX$; par hypothèse M_f est une matrice inversible dans $\mathcal{O}_v$. Soit $x = (x_1, \ldots, x_m)$ une solution primitive de l'équation ; calculons le gradient de f en x :

$$\nabla f(x) = 2M_f \cdot x \ .$$

Comme x est primitif et M_f est inversible, et q est impair, le vecteur $\nabla f(x)$ est également primitif, et on peut appliquer le théorème. □

On en déduit le résultat simple suivant, en considérant la forme $f(X) = X^2 - u$.

Corollaire 1.3.2. *Soit $v \in \mathscr{V}$. Un élément de $\mathcal{U}_v$ est un carré dans $\mathcal{U}_v$ si et seulement si c'est un carré modulo $\mathfrak{m}_v$.*

Et en considérant la forme $f(X) = X^{n-1} - 1$, où $n = |\mathcal{O}_v/\mathfrak{m}_v|$:

Corollaire 1.3.3. *Soit $v \in \mathscr{V}$, soit $n = |\mathcal{O}_v/\mathfrak{m}_v|$. Alors $\mathcal{O}_v$ contient toutes les racines $(n-1)$-ièmes de l'unité.*

Démonstration. Soit $x \in \mathcal{O}_v^*$. Alors $|f(x)|_v < 1$ car $x^{n-1} = 1 \pmod{\mathfrak{m}_v}$. Mais de plus, $|f'(x)|_v = 1$ car x est une unité. On peut appliquer le lemme de Hensel et on trouve donc, pour tout $\bar{x} \in (\mathcal{O}_v/\mathfrak{m}_v)^*$, une racine $(n-1)$-ième de l'unité ζ telle que $\zeta \equiv x \pmod{\mathfrak{m}_v}$. Or il y a précisément $n-1$ tels éléments $\bar{x}$, donc on obtient en fait *toutes* les racines $(n-1)$-ièmes de l'unité. □

Remarque 1.6. Il est facile de voir que $n = q^{\deg(P)}$ si $v = P$, et que $n = q$ si $v = \infty$. En particulier, n est *impair*.

Notons $\mathcal{U}_v^1 = 1 + \mathfrak{m}_v \subset \mathcal{U}_v$; et $\mathbf{U}_{n-1} \subset \mathcal{U}_v$ le groupe des racines $(n-1)$-ièmes de l'unité (toujours avec $n = |\mathcal{O}_v/\mathfrak{m}_v|$). On a le théorème de structure suivant.

Théorème 1.4. *Soit $v \in \mathscr{V}$. Alors le groupe des unités $\mathcal{U}_v$ est isomorphe à $\mathcal{U}_v^1 \times \mathbf{U}_{n-1}$,* via *l'isomorphisme suivant :*

$$\begin{array}{ccc} \mathcal{U}_v^1 \times \mathbf{U}_{n-1} & \xrightarrow{\sim} & \mathcal{U}_v \\ (u, \zeta) & \longmapsto & u\zeta \end{array} .$$

Démonstration. C'est une conséquence de la démonstration du corollaire 1.3.3 ci-dessus. Soit en effet $x \in \mathcal{U}_v$. Il existe alors $\zeta \in \mathbf{U}_{n-1}$ tel que $\zeta \equiv x \pmod{\mathfrak{m}_v}$. Alors $x/\zeta \in \mathcal{U}_v^1$, donc l'application est bien surjective. Elle est de plus injective car $\mathcal{U}_v^1$ et $\mathbf{U}_{n-1}$ ont une intersection réduite à $\{1\}$. □

Comme conséquence du corollaire 1.3.2, on a également un résultat concernant la structure des carrés.

Théorème 1.5. *Soit $v \in \mathscr{V}$, et $x \in \mathbf{F}_q(t)_v^*$. Écrivons $x = \pi^n u$ comme dans la proposition 1.1. Alors x est un carré dans $\mathbf{F}_q(t)_v^*$ si et seulement si n est pair et u est un carré modulo $\mathfrak{m}_v$.*

Démonstration. Supposons que x est un carré : il existe $y \in \mathbf{F}_q(t)_v^*$ tel que $y^2 = x$. En écrivant $y = \pi^k v$, on obtient $x = \pi^n u = y^2 = \pi^{2k} v^2$, et par unicité de cette écriture (proposition 1.1), on identifie $n = 2k$ et $u = v^2$.

Réciproquement, si n est pair, et u est un carré modulo $\mathfrak{m}_v$, on sait par le corollaire 1.3.2 que u est un carré, et comme $\pi^n = (\pi^{n/2})^2$, x est un carré dans $\mathbf{F}_q(t)_v^*$. □

Remarque 1.7. Si par exemple $v = P$ est un polynôme irréductible unitaire, et si on écrit $u \in \mathcal{U}_v$ sous la forme $a_0 + a_1 P + a_2 P^2 + \cdots$, alors la réduction modulo $\mathfrak{m}_v$ de u, qu'on note $\bar{u}$, consiste seulement en le « coefficient d'ordre 0 » a_0, donc u est un carré si et seulement si $a_0 \in (\mathbf{F}_q[t]/(P))^*$ est un carré. On notera au passage le symbole de Legendre :

$$\left(\frac{u}{P}\right) := \left(\frac{\bar{u}}{P}\right) = \begin{cases} 1 & \text{si } \bar{u} \text{ est un carré mod } P \\ -1 & \text{sinon.} \end{cases}.$$

Corollaire 1.5.1. *Pour tout $v \in \mathscr{V}$, on a $[\mathbf{F}_q(t)_v^* : \mathbf{F}_q(t)_v^{*2}] = 4$.*

Démonstration. D'après le théorème 1.5 sur la structure des carrés, il nous suffit de montrer que $[\mathcal{U}_v : \mathcal{U}_v^2] = 2$. D'après le théorème 1.4 sur la structure des unités, on peut étudier séparément $\mathcal{U}_v^1$ et $\mathbf{U}_{n-1}$. Or justement, tous les éléments de $\mathcal{U}_v^1$ sont des carrés car sont congrus à 1 modulo $\mathfrak{m}_v$. Le résultat provient donc de l'imparité de n : $(\mathbf{U}_{n-1})^2/\mathbf{U}_{n-1} \simeq \mathbf{Z}/2\mathbf{Z}$. □

Remarque 1.8. On a en fait montré que le groupe $\mathbf{F}_q(t)_v^*/\mathbf{F}_q(t)_v^{*2}$ est isomorphe à $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$, avec pour générateurs :
- si $v = P$, P et ζ_{n-1} un générateur de $\mathbf{U}_{n-1}$, modulo les carrés ;
- si $v = \infty$, $1/t$ et ζ_{n-1} un générateur de $\mathbf{U}_{n-1}$, modulo les carrés.

Corollaire 1.5.2. *Pour tout $v \in \mathscr{V}$, l'ensemble des carrés est un ouvert de $\mathbf{F}_q(t)_v^*$.*

Démonstration. Soit x un carré dans $\mathbf{F}_q(t)_v^*$. D'après le théorème 1.5, la boule $\{y \in \mathbf{F}_q(t)_v \mid |x - y|_v < |x|_v\}$ ne contient que des carrés. □

Terminons par un résultat d'approximation très utile. Tout d'abord, une remarque : par définition, le corps $\mathbf{F}_q(t)$ est dense dans chacun des $\mathbf{F}_q(t)_v$ (où $v \in \mathscr{V}$) *individuellement*. Mais d'autre part, nous avons déjà remarqué que, pour tout $F \in \mathbf{F}_q(t)$, presque tous les $|F|_v$ sont égaux à 1 et surtout que : $\prod_{v \in \mathscr{V}} |F|_v = 1$. Ceci assure déjà qu'on ne peut pas approcher uniformément arbitrairement près n'importe quel $(F_v)_{v \in \mathscr{V}}$, où $F_v \in \mathbf{F}_q(t)_v$ pour tout v, par une suite d'éléments de $\mathbf{F}_q(t)$.

Nous allons montrer en fait un résultat intermédiaire, mais très général. Pour cela, nous revenons au cas général d'un corps k et de valeurs absolues quelconques.

Théorème 1.6 (Théorème d'approximation faible)**.** *Soit k un corps, et soient n valeurs absolues $|\cdot|_1, \ldots, |\cdot|_n$ non triviales sur k, deux à deux non-équivalentes. Notons $k_1, \ldots, k_n$ les complétions associées aux topologies induites sur k. Alors l'image de k est dense dans le produit $\prod_{i=1}^n k_i$.*

Remarque 1.9. On peut reformuler ce résultat en disant que k est dense dans $\prod_{v\in\mathscr{V}} k_v$ pour la topologie produit.

Nous commençons par un résultat de « liberté » des valeurs absolues non-équivalentes.

Lemme 1.2. *Soient n valeurs absolues $|\cdot|_1, \dots, |\cdot|_n$ non triviales sur k, deux à deux non-équivalentes. Alors il existe $x \in k$ tel que $|x|_1 > 1$ et $|x|_2, \dots, |x|_n < 1$.*

Démonstration. Nous allons le montrer par récurrence sur n.

- $n = 2$: Soient deux valeurs absolues non triviales $|\cdot|_1$ et $|\cdot|_2$ telles que pour tout $x \in k$, $|x|_1 > 1$ implique $|x|_2 > 1$. Nous allons montrer qu'elles sont équivalentes.
  Soit $c \in k$ tel que $|c|_1 > 1$. Pour tout $x \in k$, notons $\gamma(x) = \log|x|_1/\log|c|_1$. Approchons $\gamma(x)$ par des rationnels m/n. Si $\gamma(x) < m/n$, alors $|x|_1 < |c|_1^{m/n}$, donc $|x^n/c^m|_1 < 1$, puis $|x^n/c^m|_2 < 1$, et enfin $|x|_2 < |c|_2^{m/n}$. De même, si $\gamma(x) > m/n$, alors $|x|_1 > |c|_1^{m/n}$ puis $|x|_2 > |c|_2^{m/n}$. Cette propriété de monotonie permet de passer à la limite, et donc $|x|_2 = |c|_2^{\gamma(x)}$. Alors, en posant $\alpha = \log|c|_2/\log|c|_1$, on a bien $|x|_2 = |x|_1^{\alpha}$ pour tout $x \in k$.
  On peut maintenant conclure : si les valeurs absolues $|\cdot|_1$, $|\cdot|_2$ sont non triviales et non-équivalentes, il existe x, $y \in k$ tels que $|x|_1 < 1$ et $|x|_2 \geq 1$, et $|y|_2 < 1$ et $|y|_1 \geq 1$; alors $|x/y|_1 < 1$ et $|x/y|_2 > 1$.
- Hérédité : supposons le résultat vrai au rang n. Soit, par hypothèse de récurrence, un élément $y \in k$ tel que $|y|_1 > 1$, et $|y|_2, \dots, |y|_n < 1$. Soit de plus $z \in k$ tel que $|z|_1 > 1$ et $|z|_{n+1} < 1$. Si $|y|_{n+1} \leq 1$, alors $x = y^r z$, pour r assez grand, convient. Sinon, alors $x = \frac{y^r}{1+y^r} z$, pour r assez grand, convient.

□

Démonstration du théorème. Considérons un n-uplet $(x_1, \dots, x_n) \in \prod_{i=1}^n k_i$, et $\varepsilon > 0$. Alors, par densité de k dans chacun des k_i, pour $i \in \{1, \dots, n\}$, il existe $(\tilde{x}_1, \dots, \tilde{x}_n) \in k^n$ tels que pour tout i, $|\tilde{x}_i - x_i|_i < \varepsilon$. Posons $M = \max_{1\leq i,j\leq n} |\tilde{x}_i|_j$. Par le lemme précédent, il existe $(y_1, \dots, y_n) \in k^n$ tels que pour tout i, $|y_i|_i > 1$ et $|y_i|_j < 1$ si $j \neq i$. Alors, pour r assez grand, $\eta_i = \frac{y_i^r}{1+y_i^r}$ vérifie, pour tout i, $|\eta_i - 1|_i < \varepsilon/M$ et $|\eta_i|_j < \varepsilon/M$ si $j \neq i$. Posons enfin $x = \eta_1\tilde{x}_1 + \cdots + \eta_n\tilde{x}_n$: on a $|x - x_i|_i \leq |x - \tilde{x}_i|_i + |\tilde{x}_i - x_i|_i < n\varepsilon + \varepsilon$ pour tout i. □

Voici un exemple d'application typique de ce résultat, en conjonction avec le corollaire 1.5.2 ci-dessus, que nous aurons l'occasion de rencontrer à nouveau :

Corollaire 1.6.1. *Soit $\mathscr{S}$ une partie finie de $\mathscr{V}$, et soit, pour tout $v \in \mathscr{S}$, $x_v \in \mathbf{F}_q(t)_v$. Alors il existe $x \in \mathbf{F}_q(t)$ tel que, pour tout $v \in \mathscr{S}$, x/x_v soit un carré dans $\mathbf{F}_q(t)_v$.*

Énoncé du théorème de Hasse-Minkowski et plan de la démonstration. Dans le langage des corps v-adiques, le théorème de Hasse-Minkowski affirme qu'une forme quadratique sur $\mathbf{F}_q(t)$ s'annule non trivialement sur $\mathbf{F}_q(t)$ si et seulement si elle s'annule non trivialement sur tout $\mathbf{F}_q(t)_v$, où $v \in \mathscr{V}$.

Pour démontrer ce résultat, nous allons suivre une démarche double : d'une part, nous allons améliorer notre connaissance des formes quadratiques sur les corps v-adiques, et d'autre part nous allons obtenir des résultats de « passage du local au global » (le théorème d'approximation faible 1.6 en constitue déjà un) :

- tout d'abord, nous poursuivrons l'étude des carrés, au moyen du « symbole de Legendre », ce qui constitue le cas des formes quadratiques à deux variables : $aX^2 = bY^2$;
- augmentant le nombre de variables, nous nous intéresserons ensuite aux équations de la forme $aX^2 + bY^2 = Z^2$, qui sont caractérisées par le « symbole de Hilbert » (a, b) : nous étudierons ses propriétés et établirons en particulier un important résultat de « passage du local au global » ;
- le symbole de Hilbert nous permettra ensuite de classifier entièrement les formes quadratiques sur les corps v-adiques, et ce sera aussi l'occasion de rappeler quelques faits généraux sur les formes quadratiques ;
- nous pourrons enfin démontrer le théorème proprement dit.

1.2 Le symbole de Legendre et le symbole de Hilbert

1.2.1 Le symbole de Legendre et la réciprocité quadratique

Rappelons pour commencer que dans toute la suite, q sera supposé *impair*. Nous allons étudier dans cette section les propriétés du symbole de Legendre, qui caractérise les carrés modulo P (où P est irréductible), et en particulier le théorème de la réciprocité quadratique.

Définition 1.4 (Symbole de Legendre)**.** Soit $P \in \mathbf{F}_q[t]$ un polynôme irréductible unitaire, et $A \in \mathbf{F}_q[t]$ non divisible par P. On définit le symbole de

Legendre par :

$$\left(\frac{A}{P}\right) = \begin{cases} 1 & \text{si } A \text{ est un carré mod } P \\ -1 & \text{sinon.} \end{cases}$$

De façon équivalente :

$$\left(\frac{A}{P}\right) = A^{(q^{\deg(P)}-1)/2} \bmod P \, .$$

Si $P \mid A$, on pose $\left(\frac{A}{P}\right) = 0$.

Remarque 1.10. La deuxième définition fait apparaître clairement le caractère *multiplicatif* du symbole de Legendre.

Nous allons démontrer le théorème suivant :

Théorème 1.7 (Réciprocité quadratique)**.** *Soient P, $Q \in \mathbf{F}_q[t]$ deux polynômes unitaires irréductibles distincts. Alors :*

$$\left(\frac{Q}{P}\right) = (-1)^{\deg(P)\deg(Q)\cdot(q-1)/2} \cdot \left(\frac{P}{Q}\right) \, .$$

Démonstration. Vue la formule qu'on doit montrer, une bonne simplification est de tout passer à la puissance $\frac{2}{q-1}$; on va donc calculer :

$$\widetilde{Q}(t) := Q^{1+q+\cdots+q^{\deg(P)-1}} \quad \text{et} \quad \widetilde{P}(t) := P^{1+q+\cdots+q^{\deg(Q)-1}} \, .$$

Alors $\widetilde{Q} \pmod P \in (\mathbf{F}_q[t]/P \cdot \mathbf{F}_q[t])^*$ vérifie $\widetilde{Q}^{q-1} \pmod P = 1$. Par conséquent, il existe un unique $\widetilde{Q}_P \in \mathbf{F}_q$ tel que $\widetilde{Q}_P \equiv \widetilde{Q} \pmod P$ (*via* l'injection $\mathbf{F}_q \hookrightarrow (\mathbf{F}_q[t]/P \cdot \mathbf{F}_q[t])^*$). On a de même $\mathbf{F}_q \ni \widetilde{P}_Q \equiv \widetilde{P} \pmod Q$.

On a maintenant à montrer que :

$$\widetilde{Q}_P \stackrel{?}{=} (-1)^{\deg(P)\deg(Q)} \cdot \widetilde{P}_Q \, . \tag{1.1}$$

Comme le corps de base $\mathbf{F}_q$ est fini, toute extension finie est engendrée par le morphisme de Frobenius ; concrètement, si on se place dans un corps de décomposition L de P et Q, on obtient les factorisations suivantes :

$$Q(t) = (t-\alpha)\cdots(t-\alpha^{q^{\deg(Q)-1}}) \quad \text{et} \quad P(t) = (t-\beta)\cdots(t-\beta^{q^{\deg(P)-1}}) \, .$$

On calcule donc facilement :

$$\widetilde{Q}(t) = Q^{1+q+\cdots+q^{\deg(P)-1}} = \prod_{\substack{1\le i\le \deg(P) \\ 1\le j\le \deg(Q)}} (t^{q^i} - \alpha^{q^j}) \, ,$$

donc :

$$\widetilde{Q}(t) \equiv \prod_{\substack{1\leq i\leq \deg(P)\\ 1\leq j\leq \deg(Q)}} (\beta^{q^{i+k}} - \alpha^{q^j}) \pmod{(t-\beta^{q^k})} .$$

Mais bien sûr, comme $\beta^{q^{\deg(P)}} = \beta$, le résultat précédent est en fait indépendant de k. On en déduit donc :

$$\widetilde{Q}_P \equiv \prod_{\substack{1\leq i\leq \deg(P)\\ 1\leq j\leq \deg(Q)}} (\beta^{q^i} - \alpha^{q^j}) \pmod{P} ,$$

et comme les deux membres de cette congruence sont dans L, il y a en fait égalité. De même, avec des notations similaires :

$$\widetilde{P}_Q = \prod_{\substack{1\leq i\leq \deg(P)\\ 1\leq j\leq \deg(Q)}} (\alpha^{q^j} - \beta^{q^i}) .$$

Ceci montre l'égalité (1.1), et conclut la démonstration du théorème. □

1.2.2 Le symbole de Hilbert

Nous allons maintenant étudier le symbole de Hilbert, qui constitue une généralisation du symbole de Legendre au sens où on n'étudie plus l'équation $X^2 = a$, mais l'équation $aX^2 + bY^2 = 1$ (on a donc augmenté le nombre de variables). Néanmoins, on verra que, dans les corps v-adiques, le symbole de Hilbert s'exprime en fonction du symbole de Legendre (c'est là une propriété arithmétique très agréable des corps v-adiques).

Nous commençons par la définition.

Définition 1.5 (Symbole de Hilbert)**.** Soient k une complétion de $\mathbf{F}_q(t)$ par rapport à une valeur absolue (non-archimédienne), $a, b \in k^*$. Considérons l'équation $(E) : Z^2 - aX^2 - bY^2 = 0$. On définit alors le symbole de Hilbert par :

$$(a,b) = \begin{cases} 1 & \text{si } (E) \text{ admet un triplet solution non trivial,} \\ -1 & \text{sinon.} \end{cases}$$

Lemme 1.3. *On a l'équivalence suivante :* $(a,b) = 1 \iff a$ *est une norme dans* $k(\sqrt{b})^*$.

Démonstration. Supposons $(a,b) = 1$, et soit (x,y,z) un triplet solution non trivial de (E). Si $x = 0$, alors $y \neq 0$, $z \neq 0$ et on obtient que b est un carré, donc $k(\sqrt{b})^* = k^*$, et a y est bien sûr une norme. Si $x \neq 0$, alors $a = \left(\frac{z}{x}\right)^2 - \left(\frac{y}{x}\right)^2 b = \left(\left(\frac{z}{x}\right) + \left(\frac{y}{x}\right)\sqrt{b}\right) \cdot \left(\left(\frac{z}{x}\right) - \left(\frac{y}{x}\right)\sqrt{b}\right)$ est une norme dans $k(\sqrt{b})^*$. □

Comme la norme est multiplicative, on a notamment que si $(a,b)=1$, alors $(a\cdot c,b)=(c,b)$. On a en fait la propriété plus forte suivante : le symbole de Hilbert est *bilinéaire*, c'est-à-dire que le groupe des normes de $k(\sqrt{b})^*$ est d'indice 1 ou 2 dans $k(b)^*$. Ceci résulte des formules suivantes.

Théorème 1.8. *Le symbole de Hilbert se calcule à partir du symbole de Legendre de la façon suivante :*

1. *Si $k=(\mathbf{F}_q(t))_P$, si $U,V\in\mathcal{U}_P$, alors :*

$$(P^\alpha U,P^\beta V)=(-1)^{\alpha\beta\cdot(q^{\deg(P)}-1)/2}\left(\frac{U}{P}\right)^\beta\left(\frac{V}{P}\right)^\alpha . \tag{1.2}$$

2. *Si $k=\mathbf{F}_q(t)_\infty$, si $U,V\in\mathcal{U}_\infty$, alors :*

$$\left(\left(\frac{1}{t}\right)^\alpha U,\left(\frac{1}{t}\right)^\beta V\right)=(-1)^{\alpha\beta\cdot(q-1)/2}\left(\frac{U}{\infty}\right)^\beta\left(\frac{V}{\infty}\right)^\alpha , \tag{1.3}$$

où on a dénoté par $\left(\frac{\cdot}{\infty}\right)$ le « caractère quadratique » $\pmod{\frac{1}{t}}$: $\left(\frac{U}{\infty}\right)=1 \iff U$ est un carré $\pmod{\frac{1}{t}}$.

Démonstration. La démonstration est très générale, et repose sur le Lemme de Hensel (théorème 1.3, page 9) pour les formes quadratiques. Le cas $\mathbf{F}_q(t)_\infty$ est bien sûr complètement similaire aux autres et nous ne le différencions pas. Nous allons en fait démontrer ces formules au cas par cas. Heureusement il y en peu, car on voit que seule la *parité* des puissances α,β importe ici, et de plus, ceux-ci jouent un rôle symétrique. On a donc trois cas.

a) α et β sont pairs. Dans ce cas, on doit étudier l'équation (E) : $Z^2-UX^2-VY^2$. Il est classique[2] que celle-ci admet une solution modulo P ; et comme le discriminant de la forme est inversible modulo P, on peut relever la solution en une solution P-adique. D'où $(U,V)=1$, comme prévu.

b) α est impair, β est pair. Comme $(U,V)=1$, on peut simplement étudier (P,V). Si V est un carré modulo P, alors par le théorème de structure des carrés de $\mathbf{F}_q(t)_P$ (théorème 1.5, page 10), V est un carré dans $\mathbf{F}_q(t)_P$, et on a bien $(P,V)=1=\left(\frac{V}{P}\right)$ (en effet, si $V=W^2$, le triplet $(0,1,W)$ est solution de (E)).

Réciproquement, supposons qu'on ait une solution (x,y,z) à $Z^2-PX^2-VY^2$. Quitte à gérer les dénominateurs, on peut supposer que

2. Dans un corps fini k de caractéristique impaire : si u et v sont non nuls, les ensembles $\{ux^2,x\in k\}$ et $\{1-vy^2,y\in k\}$ possèdent tous deux $(|k|+1)/2$ éléments, donc s'intersectent.

le triplet (x, y, z) est dans $\mathcal{O}_P$ et non divisible dans son ensemble par P. Mais alors y et z ne peuvent être divisibles par P, donc V est un carré modulo P.

c) α et β sont impairs. On va utiliser la formule : $(a, b) = (a, -ab)$, qui provient de ce que $(a, -a) = 1$. On en déduit $(PU, PV) = (PU, -P^2UV) = (PU, -UV) = \left(\frac{-UV}{P}\right) = (-1)^{(q^{\deg(P)}-1)/2} \left(\frac{U}{P}\right) \left(\frac{V}{P}\right)$, comme annoncé.

□

Corollaire 1.8.1. *Le symbole de Hilbert est une forme bilinéaire non dégénérée sur le $\mathbf{F}_2$-espace vectoriel k^*/k^{*2}. En particulier, si $a \neq 1$, les ensembles $H^a_\pm = \{x \in k^*/k^{*2} \mid (a, x) = \pm 1\}$ contiennent chacun 2 éléments. De plus, si a, $a' \in k^*/k^{*2}$, on a $H^a_\epsilon = H^{a'}_{\epsilon'} \iff a = a'$ et $\epsilon = \epsilon'$.*

Démonstration. La bilinéarité et la non-dégénérescence se lisent sur les formules, nous ne détaillons pas. Rappelons également qu'on a montré précédemment (corollaire 1.5.1, page 11) que $|k^*/k^{*2}| = 4$, donc tout hyperplan affine est de cardinal 2. La dernière assertion est également facile : si les deux ensembles H^a_ϵ et $H^{a'}_{\epsilon'}$ sont égaux, ils contiennent simultanément 1 ou non, donc $\epsilon = \epsilon'$. Le fait que $a = a'$ découle alors de la non-dégénérescence du symbole. □

Définition 1.6. On note $\mathcal{V}$ la réunion de l'ensemble des polynômes irréductibles unitaires de $\mathbf{F}_q[t]$ et du symbole ∞. Soit $v \in \mathcal{V}$; si A, $B \in \mathbf{F}_q(t)^*$, on note $(A, B)_v$ le symbole de Hilbert de leurs images dans $\mathbf{F}_q(t)_v$.

On a alors la proposition suivante.

Proposition 1.2 (Loi de réciprocité de Hilbert)**.** *Soient $A, B \in \mathbf{F}_q(t)^*$. Alors $(A, B)_v = 1$ pour presque tout $v \in \mathcal{V}$ et :*

$$\prod_{v \in \mathcal{V}} (A, B)_v = 1 \, . \tag{1.4}$$

Démonstration. Concernant la première assertion, les formules de la proposition 1.8 ci-dessus montrent que si P est un polynôme irréductible unitaire qui ne divise ni A ni B, alors $(A, B)_P = 1$. Comme il n'y a qu'un nombre fini de polynômes irréductibles unitaires qui divisent A ou B, presque tous les $(A, B)_v$ sont égaux à 1.

Puis, par bilinéarité, il suffit de vérifier la formule pour A, B égaux à une constante ou à un polynôme premier. Celle-ci est alors en fait équivalente à la réciprocité quadratique (théorème 1.7, page 14), par un calcul immédiat. □

On en vient au théorème principal sur le symbole de Hilbert.

Théorème 1.9. *Soient $(A_i)_{i\in I}$ des éléments en nombre fini de $\mathbf{F}_q(t)^*$, soient $\epsilon_{i,v} = \pm 1, i \in I, v \in \mathscr{V}$. Il existe $X \in \mathbf{F}_q(t)^*$ tel que $(X, A_i)_v = \epsilon_{i,v}$ pour tout i, v si et seulement si :*

1. *Pour tout $i \in I$, $\epsilon_{i,v} = 1$ pour presque tout $v \in \mathscr{V}$.*
2. *Pour tout $i \in I$, $\prod_{v\in\mathscr{V}} \epsilon_{i,v} = 1$.*
3. *Pour tout $v \in \mathscr{V}$, il existe $X_v \in \mathbf{F}_q(t)_v^*$ tel que pour tout $i \in I$, $(A_i, X_v)_v = \epsilon_{i,v}$.*

La démonstration de ce théorème nécessite deux « lemmes » :

Lemme 1.4 (Théorème d'approximation faible)**.** *Soit $\mathscr{S}$ une partie finie de $\mathscr{V}$. Alors l'image de $\mathbf{F}_q(t)$ est dense dans $\prod_{v\in\mathscr{S}} \mathbf{F}_q(t)_v$.*

C'est le théorème 1.6, démontré à la page 11.

Lemme 1.5 (Progression arithmétique de Dirichlet)**.** *Soient A, B des polynômes unitaires non nuls de $\mathbf{F}_q[t]$; supposons que A et B sont premiers entre eux. Alors, pour n assez grand, il existe P irréductible unitaire et de degré n tel que $P \equiv A \pmod{B}$.*

Ce résultat est démontré en annexe, page 38.

Démonstration du théorème. Les conditions données sont évidemment nécessaires. Nous allons montrer qu'elles sont suffisantes.

On suppose pour commencer, quitte à les multiplier par des carrés, que les A_i sont des polynômes. Définissons les sous-ensembles *finis* de $\mathscr{V}$ suivants :

$$\mathscr{S} = \Big\{\infty\Big\} \cup \Big\{\text{facteurs premiers des } A_i\Big\} \quad \text{et} \quad \mathscr{T} = \Big\{v \;\Big|\; \exists i, \epsilon_{i,v} = -1\Big\}.$$

On va d'abord se ramener au cas où $\mathscr{S}$ et $\mathscr{T}$ sont disjoints, par la technique suivante. Par le lemme d'approximation 1.4, il existe $X' \in \mathbf{F}_q(t)^*$ tel que $\frac{X'}{X_v}$ soit un carré dans $\mathbf{F}_q(t)_v^*$, pour tout $v \in \mathscr{S}$ (rappelons que les carrés des corps v-adiques forment un *ouvert*). Alors : $(A_i, X')_v = (A_i, X_v) = \epsilon_{i,v}$, pour tout $v \in \mathscr{S}$, $i \in I$. Ainsi, quitte à multiplier X par X', on peut effectivement supposer que $\mathscr{S} \cap \mathscr{T} = \emptyset$.

Posons alors :

$$A = \prod_{L\in\mathscr{T}} L \quad \text{et} \quad M = \prod_{L\in\mathscr{S}, L\neq\infty} L\,.$$

Les polynômes A et M sont unitaires et premiers entre eux. Par le lemme de la progression arithmétique 1.5, il existe un polynôme P irréductible unitaire tel que $P \equiv A \pmod{M}$, $P \notin \mathscr{S} \cup \mathscr{T}$, et $\deg(P) \equiv \deg(A) \pmod 2$. Le polynôme $X = A \cdot P$ répond alors au problème :

– Le polynôme X est unitaire et de degré pair ; c'est donc un carré dans $\mathbf{F}_q(t)_\infty$ (voir le théorème de structure des carrés 1.5, page 10). Par conséquent, $(A_i, X)_\infty = 1$, pour tout $i \in I$.
– Si $v \in \mathscr{S} - \{\infty\}$, alors $X \equiv A^2 \pmod{\mathfrak{m}_v}$; et comme A est une unité v-adique le théorème de structure des carrés 1.5, page 10, implique de nouveau que X est un carré dans $\mathbf{F}_q(t)_v$, donc $(A_i, X)_v = 1$, pour tout $i \in I$.
– Si $v \in \mathscr{T}$, alors il existe $X_v \in \mathbf{F}_q(t)_v$, $i_0 \in I$ tels que $(A_{i_0}, X_v)_v = -1$. Or, $A_{i_0} \in \mathcal{U}_v$ par définition, donc on a : $(A_{i_0}, X_v) = \left(\frac{A_{i_0}}{v}\right)^{\mathrm{ord}_v(X_v)}$ d'après les formules de la proposition 1.8. On en déduit que $\mathrm{ord}_v(X_v) \equiv 1 \pmod 2$. Or, comme v apparaît une fois dans la décomposition en facteurs premiers de X (c'est-à-dire $\mathrm{ord}_v(X) = 1$), $(A_i, X)_v = \left(\frac{A_i}{v}\right) = (A_i, X_v)_v = \epsilon_{i,v}$ pour tout $i \in I$.
– Si $v \notin \mathscr{S} \cup \mathscr{T} \cup \{P\}$: X est une unité v-adique, donc on a automatiquement $(A_i, X)_v = 1$ pour tout $i \in I$.
– Le cas restant $v = P$ se déduit finalement de la formule du produit (1.4) : comme les suites $(\epsilon_{i,v})_{v\in\mathscr{V}}$ et les $((A_i, X)_v)_{v\in\mathscr{V}}$ contiennent, pour tout $i \in I$, un nombre pair de -1, et que d'après les points précédents elles diffèrent d'au plus un élément, elles sont en fait identiques.

□

1.3 Classification des formes quadratiques sur les corps v-adiques

Dans cette partie, nous allons étudier les formes quadratiques sur les complétions $\mathbf{F}_q(t)_v$, notre objectif étant leur classification à l'aide de quelques invariants. Nous nous sommes beaucoup inspirés du chapitre IV du livre de Serre [4].

Commençons par quelques généralités : nous fixons k un complété de $\mathbf{F}_q(t)$ par rapport à une valeur absolue (non-archimédienne), où q est une puissance d'un nombre premier *impair*.

Définition 1.7. Soit V un k-espace vectoriel de dimension finie. Une forme bilinéaire symétrique sur V est une application $B : V \times V \to k$ telle que :
– pour tous x, x', $y \in V$, $\lambda \in k$, $B(\lambda x + x', y) = \lambda B(x, y) + B(x', y)$;
– pour tous x, $y \in V$, $B(x, y) = B(y, x)$.

L'application $f : \begin{array}{l} V \longrightarrow k \\ x \longmapsto f(x) = B(x, x) \end{array}$ est une *forme quadratique*.

Soit donc B une forme quadratique sur un espace V. Si $(e_1, \ldots, e_n)$ est

une base de V, alors on calcule :

$$B(x_1e_1 + \cdots + x_ne_n, y_1e_1 + \cdots + y_ne_n) = \sum_{1\leq i,j\leq n} x_iy_jB(e_i, e_j) \ .$$

Posons $M_B = (B(e_i, e_j))_{1\leq i,j\leq n}$. Alors on peut écrire B sous forme matricielle : $B(X, Y) = {}^tXM_BY$. Sous un changement de base de matrice P, la matrice se transforme en : $M'_B = {}^tPM_BP$. Deux formes bilinéaires symétriques dont les matrices vérifient une telle relation sont dites *équivalentes*, et on notera $\sim$ cette relation d'équivalence. De plus dans la suite, quitte à effectuer un changement de base, on considèrera toujours que $V = k^n$, avec $n \geq 1$. Ainsi, les formes quadratiques seront vues comme des polynômes homogènes de degré 2 à n variables $f(X_1, \ldots, X_n)$.

Un invariant notable des classes d'équivalence de formes quadratiques est le *discriminant* $disc(B)$ de B, défini comme étant la classe de $\det(M_B)$ dans k^*/k^{*2}. Il y en a un autre : le rang de la matrice M_B, appelé *rang de* B et noté $rg(B)$. Dans la suite, on supposera la forme bilinéaire B *non dégénérée*, c'est-à-dire que M_B est inversible.

Remarque 1.11. On écrira aussi $disc(f)$ et $rg(f)$ au lieu de $disc(B)$ et $rg(B)$.

Définition 1.8. Soient B une forme bilinéaire symétrique, x, $y \in V$. On dit que x et y sont *orthogonaux* (pour B) si $B(x, y) = 0$. Si $S \subset V$, on note $S^\perp$ *l'orthogonal de* S, défini par : $S^\perp = \{x \in V \mid \forall s \in S, B(x, s) = 0\}$.

Lemme 1.6. *Si B est une forme bilinéaire symétrique non dégénérée, tout sous-espace W de V vérifie :* $\dim(W) + \dim(W^\perp) = \dim(V)$. *De plus,* $W \cap W^\perp = \{0\} \iff B_{|W}$ *est non dégénérée.*

Démonstration. On considère l'application $\widehat{B} : \begin{array}{c} V \longrightarrow V^* \\ x \longmapsto (y \mapsto B(x, y)) \end{array}$. C'est un isomorphisme car B est non dégénérée. Notons maintenant $r_{|W}$ l'application de $V^* \to W^*$ de restriction à W. Alors $r_{|W} \circ \widehat{B}$ est surjective de V dans W^* et a pour noyau $W^\perp$: le théorème du rang permet de conclure.

Le deuxième point découle de la remarque que $W \cap W^\perp = \ker \widehat{B_{|W}}$. □

Théorème 1.10. *Soit $f(X_1, \ldots, X_n)$ une forme quadratique. Il existe alors $a_1, \ldots, a_n \in k$ tels que $f \sim a_1{X_1}^2 + \cdots + a_n{X_n}^2$.*

Démonstration. Pour prouver le théorème, on doit en fait trouver une base dans laquelle f prend cette forme. On va raisonner par récurrence sur n, la dimension de l'espace V. Le résultat est automatique si $n = 1$, montrons donc l'hérédité $n \to n+1$. Si $f(X_1, \ldots, X_{n+1})$ est une forme quadratique non nulle, il existe $x_1 \in V$ tel que $f(x_1) \neq 0$. On peut alors, d'après le lemme 1.6

ci-dessus, décomposer V en $kx \oplus (kx)^\perp$. On applique alors l'hypothèse de récurrence à $(kx)^\perp$ et $f_{|(kx)^\perp}$ puis on complète la base obtenue avec le vecteur x, ce qui conclut. □

Remarque 1.12.
- Les coefficients a_i ne sont pas uniques.
- Une base dans laquelle f prend cette forme « diagonalisée » est appelée *base orthogonale* de V.
- Dans une telle base, la matrice M_B s'écrit $\begin{pmatrix} a_1 & & 0 \\ & \ddots & \\ 0 & & a_n \end{pmatrix}$. En particulier, $disc(B) \equiv a_1 \cdots a_n \pmod{k^{*2}}$.

Nous allons maintenant nous intéresser aux valeurs prises par une forme quadratique : on dira que f *représente* $a \in k$ s'il existe $x_a \in V - \{0\}$ tel que $f(x_a) = a$. Remarquons que si f représente $a \neq 0$, alors f représente toute la classe de a dans k^*/k^{*2} : si $b = c^2 a$, et $f(x_a) = a$, alors $f(cx_a) = b$. Par conséquent, dans la suite on sera parfois amené à parler des classes de k^*/k^{*2} qui sont représentées par f. Le théorème suivant montre d'ailleurs que 0 joue un rôle à part dans k parmi les images possibles de f.

Définition 1.9. Soit $f(X_1, X_2)$ une forme quadratique non dégénérée à deux variables ; elle est dite *hyperbolique* si $f \sim X_1X_2 \sim {X_1}^2 - {X_2}^2$.

Théorème 1.11. *Si $f(X_1, \ldots, X_n)$ est une forme quadratique non dégénérée qui représente 0, alors on peut décomposer $f \sim f_H(X_1, X_2) + g(X_3, \ldots, X_n)$ avec f_H hyperbolique ; et f représente tout élément de k.*

Démonstration. Soit $x_0 \in V - \{0\}$ tel que $f(x_0) = 0$. Comme f est non dégénérée, il existe $x \in V$ tel que $B(x_0, x) \neq 0$. Quitte à renormaliser, supposons que $B(x_0, x) = 1$. Alors $x_1 = x - \frac{1}{2}B(x, x) \cdot x_0$ vérifie $B(x_0, x_1) = 1$ et $B(x_1, x_1) = 0$. Donc, dans le plan $\mathcal{P}$ engendré par (x_0, x_1), la matrice de f est $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Ainsi, $B_{|\mathcal{P}}$ est non dégénérée, donc $V = \mathcal{P} \oplus \mathcal{P}^\perp$ d'après le lemme 1.6, et en posant $f_H = f_{|\mathcal{P}}$, $g = f_{|\mathcal{P}^\perp}$, on a le résultat.

De plus, f_H représente tout élément a de k, en effet en conservant les notations ci-dessus, $f_H(x_0 + \frac{1}{2}ax_1) = a$. Donc il en est de même pour f. □

Corollaire 1.11.1. *Soient $f(X_1, \ldots, X_n)$ une forme quadratique non dégénérée, $a \in k^*$. Il y a équivalence entre les assertions suivantes :*

a) Il existe une forme quadratique g telle que $f \sim g(X_1, \ldots, X_{n-1}) + a{X_n}^2$.

b) La forme $f(X_1, \ldots, X_n)$ représente a.

c) La forme $f(X_1, \ldots, X_n) - a{X_{n+1}}^2$ représente 0.

Démonstration. Les implications a) ⇒ b) ⇒ c) sont immédiates. Nous allons remonter les implications à l'envers. Supposons donc c). Si f représente 0, elle représente aussi a par le théorème 1.11 ci-dessus. Sinon, il existe $(x_1, \ldots, x_n, x_{n+1}) \in k^{n+1}$, avec $x_{n+1} \neq 0$, tel que $f(x_1, \ldots, x_n) - a{x_{n+1}}^2 = 0$; alors $f(x_1/x_{n+1}, \ldots, x_n/x_{n+1}) = a$.

Supposons maintenant b). Soit donc $x_a \in V$ tel que $f(x_a) = B(x_a, x_a) = a$. Comme $a \neq 0$, on a $V = kx_a \oplus (kx_a)^\perp$ par le lemme 1.6. Ainsi, en décomposant f selon cette somme, on obtient a). □

Corollaire 1.11.2. *Soient $g(X_1, \ldots, X_{n_g})$ et $h(X_1, \ldots, X_{n_h})$ deux formes quadratiques non dégénérées, avec n_g, $n_h \geq 1$, et soit $f = g(X_1, \ldots, X_{n_g}) - h(X_{n_g+1}, \ldots, X_{n_g+n_h})$. Alors f représente 0 si et seulement si il existe $a \neq 0$ qui est représenté simultanément par g et h.*

Démonstration. Le sens réciproque étant évident, nous ne montrons que le sens direct. Soit donc (x_g, x_h) un zéro non nul de f, où x_g est un vecteur correspondant aux n_g premières composantes, et x_h aux n_h suivantes. Nécéssairement, x_g ou x_h est non nul. Supposons que ce soit x_g (quitte à intervertir g et h). Alors :

- si $g(x_g) \neq 0$: $a = g(x_g) = h(x_h)$ convient ;
- si $g(x_g) = 0$: par le théorème 1.11, g représente tout élément de k. Comme h est non dégénérée, elle prend au moins une valeur $h(y)$ non nulle, qui est représentée par g, et $a = h(y)$ convient.

□

Remarque 1.13. Ce corollaire est très utile car il permet de diminuer le nombre de variables de la forme à étudier. En particulier, en conjonction avec le corollaire précédent, on l'utilisera pour passer de l'étude de la représentation de 0 par une forme à 4 variables à celle de deux formes à 3 variables.

Nous allons maintenant classifier les formes quadratiques sur k (nous rappelons que k est de la forme $\mathbf{F}_q(t)_v$, où $v \in \mathscr{V}$). Nous avons déjà rencontré deux invariants : le rang $rg(f)$ et le discriminant $disc(f)$. Nous allons à présent en introduire un troisième. Soit f une forme quadratique sur V, soit $\mathscr{B} = (e_1, \ldots, e_n)$ une base orthogonale de V pour f, et posons $a_i = f(e_i)$. On définit alors :

$$\varepsilon(f, \mathscr{B}) = \prod_{i<j} (a_i, a_j) \ ,$$

où $(\cdot, \cdot)$ désigne le symbole de Hilbert sur k. Nous allons démontrer que c'est bien un invariant de la classe d'équivalence de la forme f. Pour cela, il suffit de montrer qu'il est indépendant de la base orthogonale $\mathscr{B}$. C'est facile si $n = 1$ ou 2 :

– si $n = 1$, $\varepsilon(f, \mathscr{B}) = 1$ indépendamment de la base $\mathscr{B}$;
– si $n = 2$, $\varepsilon(f, \mathscr{B}) = (a_1, a_2) = 1$ si et seulement si la forme $Z^2 - a_1X^2 - a_2Y^2$ réprésente 0, c'est-à-dire, vu le corollaire 1.11.1, si et seulement si la forme f représente 1 : c'est bien indépendant de la base $\mathscr{B}$.

Le résultat pour $n \geq 3$ se montre ensuite par récurrence. Le lemme suivant montre tout d'abord qu'on peut s'intéresser uniquement aux bases orthogonales ayant au moins un vecteur en commun.

Lemme 1.7. *Soit f une forme quadratique non dégénérée, de rang supérieur ou égal à 3 et soient $\mathscr{B} = (e_1, \ldots, e_n)$ et $\mathscr{B}' = (e'_1, \ldots, e'_n)$ deux bases orthogonales. Alors il existe une suite finie $\mathscr{B}^{(0)} = \mathscr{B}, \ldots, \mathscr{B}^{(m)} = \mathscr{B}'$ de bases orthogonales telle que pour tout $i \in \{0, \ldots, m-1\}$, les bases $\mathscr{B}^{(i)}$ et $\mathscr{B}^{(i+1)}$ ont un vecteur en commun.*

Démonstration. Nous allons former un élément $e'_x = e'_1 + xe'_2$ qui engendre avec e_1 un plan non dégénéré, et tel que $f(e'_x) \neq 0$. Pour cela, il suffit de choisir $x \in k$ tel que :

$$f(e_1)f(e'_x) - B(e_1, e'_x)^2 \neq 0 \quad \text{et} \quad f(e'_x) \neq 0 \,,$$

c'est-à-dire :

$$\alpha x^2 + \beta x + \gamma \neq 0 \quad \text{et} \quad f(e'_1) + x^2 f(e'_2) \neq 0 \,, \qquad (*)$$

où :

$$\begin{cases} \alpha = (f(e_1)f(e'_2) - B(e_1, e'_2)^2) \\ \beta = -2B(e_1, e'_1)B(e_1, e'_2) \\ \gamma = (f(e_1)f(e'_1) - B(e_1, e'_1)^2) \end{cases} .$$

Rappelons que comme f est non dégénérée, les trois valeurs $f(e_1)$, $f(e'_1)$, $f(e'_2)$ sont non nulles. On en déduit que α, β, γ ne peuvent être nuls simultanément. Ainsi les conditions polynômiales $(*)$ éliminent au plus 4 valeurs de x, mais le corps k est infini : l'existence de e_x est assurée.

Considérons maintenant les deux *plans* $\mathcal{P}_x$ et $\mathcal{P}'$, engendrés respectivement par (e_1, e'_x) et (e'_1, e'_2). Ils sont tous deux non dégénérés, et comme $f(e_1)$, $f(e'_x) \neq 0$, il existe $e_2^{(1)}$, $e_2^{(2)}$, $e_2^{(3)}$ tels que :
– $(e_1, e_2^{(1)})$ forme une base orthogonale de $\mathcal{P}_x$.
– $(e'_x, e_2^{(2)})$ forme une base orthogonale de $\mathcal{P}_x$.
– $(e'_x, e_2^{(3)})$ forme une base orthogonale de $\mathcal{P}'$.

Comme le plan $\mathcal{P}_x$ est non dégénéré, il est en somme directe avec son orthogonal $\mathcal{H}_x$, et en notant $(e''_3, \ldots, e''_n)$ une base orthogonale de $\mathcal{H}_x$, on obtient le résultat annoncé avec la chaîne : $\mathscr{B} \to (e_1, e_2^{(1)}, e''_3, \ldots, e''_n) \to (e'_x, e_2^{(2)}, e''_3, \ldots, e''_n) \to (e'_x, e_2^{(3)}, e'_3, \ldots, e'_n) \to \mathscr{B}'$.

□

En remarquant que ε est invariant par permutation des vecteurs de la base, on peut maintenant conclure grâce au lemme suivant.

Lemme 1.8. *Soit f une forme quadratique non dégénérée sur k^n, et soient $\mathscr{B} = (e_1, \ldots, e_n)$ et $\mathscr{B}' = (e_1, e'_2 \ldots, e'_n)$ deux bases orthogonales pour f qui ont un élément en commun. Alors $\varepsilon(f, \mathscr{B}) = \varepsilon(f, \mathscr{B}')$.*

Démonstration. On le montre par récurrence sur n. Supposons le résultat vrai au rang $n-1$. D'après le lemme 1.7 ci-dessus, cela implique que pour toute forme quadratique de $n-1$ variables, ε est indépendant de la base orthogonale choisie.

Posons $a'_i = f(e'_i)$, et $a'_1 = a_1$. Alors on a :

$$\varepsilon(f, \mathscr{B}) = (a_1, a_2 \cdots a_n) \prod_{2 \leq i < j \leq n} (a_i, a_j) = (a_1, disc(f) \cdot a_1) \prod_{2 \leq i < j \leq n} (a_i, a_j) \ ,$$

et :

$$\varepsilon(f, \mathscr{B}') = (a_1, disc(f) \cdot a_1) \prod_{2 \leq i < j \leq n} (a'_i, a'_j) \ .$$

Considérons maintenant la forme quadratique $f_1 = f_{|(ke_1)^\perp}$. Les familles $(e_2, \ldots, e_n)$ et $(e'_2, \ldots, e'_n)$ sont des bases orthogonales pour f_1 ; donc par hypothèse de récurrence, $\varepsilon\left(f_1, (e_2, \ldots, e_n)\right) = \varepsilon\left(f_1, (e'_2, \ldots, e'_n)\right)$. Or,

$$\varepsilon\left(f_1, (e_2, \ldots, e_n)\right) = \prod_{2 \leq i < j \leq n} (a_i, a_j) \quad \text{et} \quad \varepsilon\left(f_1, (e'_2, \ldots, e'_n)\right) = \prod_{2 \leq i < j \leq n} (a'_i, a'_j) \ ,$$

d'où le résultat.

□

On en déduit le résultat annoncé : $\varepsilon(f, \mathscr{B})$ ne dépend en fait que de f ; et il est évident que c'est un invariant de la classe d'équivalence de f. On le notera plus simplement $\varepsilon(f)$.

Nous allons maintenant montrer que les trois invariants que sont $rg(f)$, $disc(f)$, $\varepsilon(f)$ caractérisent complètement l'ensemble des valeurs prises par f. Nous commençons par un lemme de rappel (voir le corollaire 1.5.1, page 11).

Lemme 1.9 (Rappel)**.** *Le $\mathbf{F}_2$-espace vectoriel k^*/k^{*2} est de dimension 2. Si $a \neq 1$, les hyperplans affines $H^a_\pm = \{x \in k^*/k^{*2} \mid (a, x) = \pm 1\}$ contiennent chacun 2 éléments. Enfin, si a, $a' \in k^*/k^{*2}$, on a $H^a_\epsilon = H^{a'}_{\epsilon'} \iff a = a'$ et $\epsilon = \epsilon'$.*

On peut maintenant énoncer le théorème principal.

Théorème 1.12. *Soit f une forme quadratique, soit $n = rg(f) \geq 1$, $d = disc(f) \in k^*/k^{*2}$, $\varepsilon = \varepsilon(f) = \pm 1$. Alors f réprésente 0 si et seulement si :*

$n = 2$: $d = -1$;
$n = 3$: $(-1, -d) = \varepsilon$;
$n = 4$: *soit* $d \neq 1$, *soit* $d = 1$ *et* $\varepsilon = (-1, -1)$;
$n \geq 5$: *toujours.*

De chaque point on déduit les points correspondants du corollaire suivant.

Corollaire 1.12.1. *Soit* $a \in k^*/k^{*2}$. *Alors* f *représente* a *si et seulement si :*
$n = 1$: $d = a$;
$n = 2$: $(a, -d) = \varepsilon$;
$n = 3$: *soit* $d \neq -a$, *soit* $d = -a$ *et* $\varepsilon = (-1, -d)$;
$n \geq 4$: *toujours.*

Remarque 1.14. Cela implique que si f est de rang n et ne représente pas 0, elle représente exactement $\min(n, 4)$ éléments de k^*/k^{*2}.

Démonstration. Tous les résultats proviennent de ce que les invariants de la forme $f_a = f(X_1, \ldots, X_n) - a{X_{n+1}}^2$ s'expriment en fonction de ceux de f comme : $disc(f_a) = -ad$, $\varepsilon(f_a) = (-a, d) \cdot \varepsilon$, et que f représente a si et seulement si f_a représente 0 (par le corollaire 1.11.1). □

Démonstration du théorème. On diagonalise la forme f par le théorème 1.10 : $f \sim a_1{X_1}^2 + \cdots a_n{X_n}^2$, et on traite tous les cas un par un.

$n = 2$: La forme représente 0 si et seulement si $-a_1/a_2$ est un carré, or en multipliant par ${a_2}^2$, on voit que $-a_1/a_2 = -d$ dans k^*/k^{*2}, ce qui conclut.

$n = 3$: En multipliant par a_3, on voit que f représente 0 si et seulement si ${X_3}^2 - (-a_1a_3){X_1}^2 - (-a_2a_3){X_2}^2$ représente 0, c'est-à-dire si et seulement si $(-a_1a_3, -a_2a_3) = 1$. Nous allons développer succesivement ce symbole par bilinéarité.

D'une part : $(-a_1a_3, -a_2a_3) = (-a_1a_3, -1)(-a_1a_3, a_2a_3)$;
de plus, $(-a_1a_3, a_2a_3) = (-1, a_2a_3)(a_1, a_2a_3)(a_3, a_2a_3)$.
Comme $(-a_1a_3, -1)(-1, a_2a_3) = (-1, -a_1a_2)$
et $(a_1, a_2a_3)(a_3, a_2a_3) = (a_1, a_2)(a_1, a_3)(a_2, a_3)(a_3, a_3)$,
on obtient au total $(-1, -a_1a_2)\varepsilon(a_3, a_3)$.
C'est bientôt fini : comme $(-a_3, a_3) = 1$, on a $(a_3, a_3) = (-1, a_3)$,
donc on obtient en fait $(-1, -a_1a_2a_3)\varepsilon$, c'est-à-dire $(-1, -d)\varepsilon$.

D'où le résultat : f représente 0 si et seulement si $(-1, -d) = \varepsilon$.

$n = 4$: On va appliquer le corollaire 1.11.2 à la décomposition suivante :

$$f = \left(a_1 {X_1}^2 + a_2 {X_2}^2\right) - \left(-a_3 {X_3}^3 - a_4 {X_4}^2\right) .$$

D'après ce corollaire, f représente 0 si et seulement si il existe $a \in k^*/k^{*2}$ représenté par les deux termes de la décomposition. Comme on a montré le cas $n = 3$ du théorème, on peut utiliser le cas $n = 2$ du corollaire 1.12.1 : l'existence de a équivaut alors à ce que l'intersection des deux espaces affines $H_1 = \{x \in k^*/k^{*2} \mid (x, -a_1a_2) = (a_1, a_2)\}$ et $H_2 = \{x \in k^*/k^{*2} \mid (x, -a_3a_4) = (-a_3, -a_4)\}$ soit non vide. Ces deux espaces sont en fait des hyperplans affines (ils sont non vides car $a_1 \in H_1$, $-a_3 \in H_3$) ; par le lemme 1.9 ci-dessus, ils sont disjoints si et seulement si ils sont complémentaires, ce qui équivaut à $a_1a_2 \equiv a_3a_4$ dans k^*/k^{*2} et $(a_1, a_2) = -(-a_3, -a_4)$. Or $(a_1, a_2)(-a_3, -a_4)(-1, -1) = (a_1, a_2)(a_3, a_4)(-1, a_3a_4)$, et comme $(-1, a_3a_4) = (a_3a_4, a_3a_4)$, on obtient comme condition équivalente : $d = 1$ et $(a_1, a_2)(a_3, a_4)(da_1a_2, a_3a_4) = -(-1, -1)$, c'est-à-dire $d = 1$ et $\varepsilon = -(-1, -1)$.

$n \geq 5$: Quitte à mettre les variables supplémentaires à 0, il suffit de traiter le cas $n = 5$. On va à nouveau utiliser la partie $n = 2$ du corollaire 1.12.1. D'après ce corollaire, et d'après le lemme 1.9, toute forme de rang 2 représente au moins 2 valeurs de k^*/k^{*2}. En effet, la condition $(a, -d) = \varepsilon$ peut éventuellement être irréalisable si $d = -1$, mais dans ce cas on a déjà vu que f représentait 0 et donc toute valeur de k (et on peut en effet vérifier par un calcul direct que $\varepsilon = 1$). Ainsi, il existe $a \in k^*/k^{*2}$ représenté par f *et qui est différent de* d. En vertu du corollaire 1.11.1, on peut alors écrire $f(X_1, \ldots, X_5) \sim aX_1^2 + g(X_2, \ldots, X_5)$, avec $rg(g) = 4$. Or $disc(g) = d/a \neq 1$, donc par le cas $n = 4$ prouvé ci-haut, g représente 0, donc f aussi, ce qui achève la démonstration.

□

On en déduit le théorème de classification suivant.

Théorème 1.13. *Les trois invariants : $rg(f)$, $disc(f)$, et $\varepsilon(f)$ caractérisent complètement la classe d'équivalence de f.*

Démonstration. On a vu précédemment que deux formes équivalentes ont nécessairement même rang, discriminant, et ε. Réciproquement, si deux formes f et g ont les mêmes invariants, alors d'après le corollaire 1.12.1, elles représentent les mêmes éléments de k^*/k^{*2}. Soit donc $a \in k^*$ représenté à la fois par f et par g. Par le corollaire 1.11.1, on peut écrire $f \sim aX_1^2 + f_1(X_2, \ldots)$,

$g \sim aX_1{}^2 + g_1(X_2, \ldots)$, avec f_1 et g_1 des formes de rang $rg(f)-1 = rg(g)-1$. Mais alors on a :

$$\begin{array}{ll} disc(f_1) = adisc(f) & \varepsilon(f_1) = \varepsilon(f)(a, disc(f_1)) \\ = adisc(g) = disc(g_1) \quad \text{et} & = \varepsilon(g)(a, disc(g_1)) = \varepsilon(g_1) \end{array} .$$

En diminuant le rang par récurrence, on se ramène au cas $rg(f) = rg(g) = 0$, qui est trivial. □

1.4 Démonstration du théorème de Hasse-Minkowski

Considérons une forme quadratique f de rang n sur $\mathbf{F}_q(t)$, que nous supposons non dégénérée. Nous allons montrer le théorème suivant :

Théorème 1.14 (Hasse-Minkowski)**.** *Pour que f représente 0 dans $\mathbf{F}_q(t)$, il faut et il suffit que, pour tout $v \in \mathscr{V}$, la forme f représente 0 dans $\mathbf{F}_q(t)_v$.*

Démonstration. La nécessité est triviale. Pour la suffisance, on écrit f sous la forme

$$f = A_1 X_1{}^2 + \cdots + A_n X_n^2 , \quad \text{où } A_i \in \mathbf{F}_q(t)^* .$$

Quitte à remplacer f par $A_1 f$ et multiplier chaque A_i par un carré dans $\mathbf{F}_q(t)^*$, on peut en outre que supposer que $A_1 = 1$ et $A_i \in \mathbf{F}_q[t]$.
On considère séparément les cas $n = 2$, 3, 4 et $n \geq 5$.

i) Le cas $n = 2$.
On a $f = X_1{}^2 - AX_2{}^2$ avec $A \in \mathbf{F}_q[t]$. On écrit A sous la forme :

$$A = c \prod_P P^{\mathrm{ord}_P(A)} ,$$

où $c \in \mathbf{F}_q^*$ et P sont des polynômes irréductibles unitaires. Comme f_∞ représente 0, il existe une série $\sum_{n=k}^{\infty} a_n (1/t)^n$ avec $a_k \neq 0$ telle que $(\sum_{n=k}^{\infty} a_n (1/t)^n)^2 = A$ dans $\mathbf{F}_q(t)_\infty$. En comparant les coefficients devant t^{-2k} dans ces deux expressions, on obtient que c est un carré dans $\mathbf{F}_q$. De plus, pour chaque polynôme irréductible unitaire P, le fait que f_P représente 0 montre que A est un carré dans $\mathbf{F}_q(t)_P^*$, et donc que $\mathrm{ord}_P(A)$ est pair. Il en résulte que A est un carré dans $\mathbf{F}_q(t)$ et que f représente 0.

ii) Le cas $n = 3$.
On a $f = X_1{}^2 - AX_2{}^2 - BX_3{}^2$. Quitte à multiplier A, B par des carrés dans $\mathbf{F}_q(t)^*$, on peut supposer que pour tout polynôme irréductible P, $\mathrm{ord}_P(A)$ et $\mathrm{ord}_P(B)$ sont égaux à 0 ou 1. On peut aussi supposer

que $\deg(A) \leq \deg(B)$. On raisonne alors par récurrence sur l'entier $m = \deg(A) + \deg(B)$.

Si $m = 0$, alors $A, B \in \mathbf{F}_q^*$. On a déjà vu que comme $\mathbf{F}_q^2$ a $(q+1)/2$ éléments, les ensembles $\{Ax^2, x \in \mathbf{F}_q\}$ et $\{1 - By^2, y \in \mathbf{F}_q\}$ doivent nécessairement s'intersecter, donc il existe x, $y \in \mathbf{F}_q$ tels que $Ax^2 + By^2 = 1$: f représente 0.

Supposons $m \geq 1$, et que le cas $\deg(A) + \deg(B) < m$ est démontré. Alors $\deg(B) \geq 1$; nous écrivons B sous la forme $B = c \cdot P_1 \cdots P_k$, où $c \in \mathbf{F}_q^*$ et chaque P_i est un polynôme irréductible unitaire. Soit P l'un des P_i. Nous allons voir que A est un carré modulo P. C'est évident si $A \equiv 0 \pmod{P}$. Sinon, A est une unité dans $\mathbf{F}_q(t)_P^*$. Par hypothèse, il existe un triplet (x, y, z) non nul dans $\mathbf{F}_q(t)_P$ tel que $z^2 - Ax^2 - By^2 = 0$, et l'on peut supposer que (x, y, z) n'est pas divisible dans son ensemble par P. On vérifie alors que $P \nmid x$, et donc A est un carré modulo P. Par le théorème des restes chinois, il s'ensuit que A est un carré modulo B.

Il existe donc T, $B' \in \mathbf{F}_q[t]$ tels que $T^2 - A = BB'$, et on peut chosir T tel que $\deg(T) \leq \deg(B) - 1$; on a alors : $\deg(B') = \deg(T^2 - A) - \deg(B) \leq \deg(B) - 1$. Écrivons B' sous la forme $B''U^2$ avec B'' sans facteurs carrés, on a toujours $\deg(B'') \leq \deg(B) - 1$. Par bilinéarité du symbole de Hilbert (Corollaire 1.8.1, page 17), on voit que, quel que soit le corps dans lequel on se place, $(A, B'') = 1 \iff (A, B) = 1$ (car la formule $T^2 - A = BB''U^2$ montre justement que $(A, BB'') = 1$). Notons $f'' = {X_1}^2 - A{X_2}^2 - B''{X_3}^2$: alors, comme f, elle représente 0 dans tout corps v-adique ; de plus on a déjà remarqué que $\deg(B'') < \deg(B)$: l'hypothèse de récurrence s'applique donc à f''. On en déduit que f'' représente 0, donc f aussi.

iii) Le cas $n = 4$.
On a $f = A{X_1}^2 + B{X_2}^2 - (C{X_3}^2 + D{X_4}^2)$. Soit $v \in \mathscr{V}$. Puisque f_v représente 0, on déduit du Corollaire 1.11.2, page 22, qu'il existe $X_v \in \mathbf{F}_q(t)_v^*$ qui est représenté à la fois par $A{X_1}^2 + B{X_2}^2$ et $C{X_3}^2 + D{X_4}^2$, donc d'après le théorème de classification 1.12.1, page 25, on a

$$(X_v, -AB)_v = (A, B)_v \quad \text{et} \quad (X_v, -CD)_v = (C, D)_v.$$

D'après la loi de réciprocité de Hilbert (proposition 1.2, page 17), $(A, B)_v$ et $(C, D)_v$ valent 1 pour presque tout $v \in \mathscr{V}$ et vérifient la formule du produit $\prod_{v \in \mathscr{V}} (A, B)_v = \prod_{v \in \mathscr{V}} (C, D)_v = 1$, on peut donc appliquer le théorème 1.9, page 18 : cela montre qu'il existe $X \in \mathbf{F}_q(t)^*$ tel que :

$$(X, -AB)_v = (A, B)_v \quad \text{et} \quad (X, -CD)_v = (C, D)_v$$

pour tout $v \in \mathscr{V}$. Ainsi, la forme $AX_1{}^2 + BX_2{}^2 - XZ^2$ représente 0 dans chacun des $\mathbf{F}_q(t)_v$, donc dans $\mathbf{F}_q(t)$ d'après le cas $n = 3$ qu'on a prouvé ci-dessus. On en conclut que X est représenté dans $\mathbf{F}_q(t)$ par $AX_1{}^2 + BX_2{}^2$, et le même argument s'applique à $CX_3{}^2 + DX_4{}^2$, d'où le fait que f représente 0.

iv) Le cas $n \geq 5$.
On montre que f représente toujours 0 dans ce cas. Il suffit bien sûr d'établir seulement le cas $n = 5$, quitte à mettre les variables supplémentaires à 0.
Écrivons $f = h \dotplus (-g)$ avec $h = A_1X_1{}^2 + A_2X_2{}^2$ et $g = A_3X_3{}^2 + A_4X_4{}^2 + A_5X_5{}^2$. Soit $\mathscr{S}$ la partie de $\mathscr{V}$ formée de ∞ et des polynomes irréductibles P tels qu'il existe i vérifiant $P \mid A_i$. C'est un ensemble *fini*.
Comme conséquence du Corollaire 1.11.2, page 22, pour chaque $v \in \mathscr{S}$ il existe $A_v \in \mathbf{F}_q(t)_v^*$ qui est représenté à la fois par $A_1X_1{}^2 + A_2X_2{}^2$ et $A_3X_3{}^2+A_4X_4{}^2+A_5X_5{}^2$: on écrit $A_v = A_1B_{1,v}{}^2+A_2B_{2,v}{}^2$, où $B_{1,v}, B_{2,v} \in \mathbf{F}_q(t)_v$. Mais les carrés de $\mathbf{F}_q(t)_v^*$ forment un ensemble *ouvert* (Corollaire 1.5.2, page 11), et $A_1B_1{}^2+A_2B_2{}^2$ est une fonction continue de B_1 et B_2. Par le théorème d'approximation faible (Théorème 1.6, page 11), il existe B_1,$B_2 \in \mathbf{F}_q(t)$ tels que $A = A_1B_1{}^2+A_2B_2{}^2$ satisfait $\frac{A}{A_v} \in \mathbf{F}_q(t)_v^{*2}$ pour tout $v \in \mathscr{S}$. Cela implique que $A_3X_3{}^2 + A_4X_4{}^2 + A_5X_5{}^2 - AZ^2$ représente 0 dans $\mathbf{F}_q(t)_v$ pour tout $v \in \mathscr{S}$. Et pour $v \notin \mathscr{S}$, la forme précédente représente aussi 0, parce que $A_i \in \mathcal{U}_v$ pour $i = 3$, 4, 5, et $A_3X_3{}^2 + A_4X_4{}^2 + A_5X_5{}^2$ représente 0 dans ce cas (cela découle des formules pour le symbole de Hilbert, données au théorème 1.8, page 16) . Donc par le cas $n = 4$ prouvé ci-dessus, $A_3X_3{}^2 + A_4X_4{}^2 + A_5X_5{}^2 - AZ^2$ représente 0 dans $\mathbf{F}_q(t)$: A est représenté à la fois par g et h, donc f représente 0.

□

Chapitre 2

Contre-exemples

Comme nous l'avons expliqué en introduction, le « principe local-global » ne se généralise pas aux équations de degré supérieur. Nous allons tout d'abord présenter des contre-exemples très simples, avant de présenter le contre-exemple le plus célèbre sur $\mathbf{Q}$: le contre-exemple de Selmer. Celui-ci consiste en l'équation $3X^3 + 4Y^3 + 5Z^3 = 0$.

2.1 Quelques contre-exemples simples

Nous allons tout d'abord fabriquer quelques contre-exemples très simples au « principe local-global », c'est-à-dire que nous allons trouver des equations polynômiales admettant des solutions dans tout corps v-adique $\mathbf{F}_q(t)_v$, pour $v \in \mathscr{V}$, mais pas dans le corps global $\mathbf{F}_q(t)$. Rappelons le résultat du théorème 1.5, démontré page 10.

Théorème 2.1 (Rappel)**.** *Soit $v \in \mathscr{V}$, et $x \in \mathbf{F}_q(t)_v^*$. Écrivons $x = \pi^n u$ comme dans la proposition 1.1. Alors x est un carré dans $\mathbf{F}_q(t)_v^*$ si et seulement si n est pair et u est un carré modulo $\mathfrak{m}_v$.*

Corollaire 2.1.1 (Rappel)**.** *Pour tout $v \in \mathscr{V}$, on a $[\mathbf{F}_q(t)_v^* : \mathbf{F}_q(t)_v^{*2}] = 4$. En particulier, les carrés forment un sous-groupe d'indice 2 parmi les unités.*

Premier exemple Considérons l'équation :

$$\big(X^2 - t\big)\big(X^2 - (t+1)\big)\big(X^2 - t(t+1)\big)\big(X^2 - (t+2)\big) = 0\,. \qquad (*)$$

Pour tout polynôme irréductible $P \neq t$, $t+1$, cette équation admet une solution dans $\mathbf{F}_q(t)_P$: en effet t et $t+1$ y sont des unités, et comme les carrés forment un sous-groupe d'ordre 2 parmi les unités, t, $t+1$, ou $t(t+1)$ est

un carré modulo P. De plus, $t(t+1) = (1/t)^{-2}(1+1/t)$ est un carré dans $\mathbf{F}_q(t)_\infty = \mathbf{F}_q((1/t))$, et $t+1$ est un carré dans $\mathbf{F}_q(t)_t = \mathbf{F}_q((t))$ pour la même raison. Enfin, $t+2$ est un carré dans $\mathbf{F}_q(t)_{t+1}$.

Néanmoins, aucun des polynômes t, $t+1$, $t+2$, $t(t+1)$ n'est un un carré dans $\mathbf{F}_q(t)$: les trois premiers sont irréductibles, et le dernier est le produit de deux polynômes irréductibles distincts. Ainsi, l'équation $(*)$ ne vérifie pas le « principe local-global ».

Deuxième exemple Il est facile de construire un deuxième exemple avec plus de variables à partir du premier. Par exemple, l'équation :

$$Z^3 - tY^3 + t^2\left[(X^2-t)(X^2-(t+1))(X^2-t(t+1))(X^2-(t+2))\right]^3 = 0$$

admet des solutions dans toute complétion, d'après ce qu'on a fait ci-dessus, mais par des considérations de degré évidentes, n'admet aucune solution sur $\mathbf{F}_q(t)$ (à nouveau par ce qu'on a fait précédemment).

2.2 Le contre-exemple de Selmer

Finalement, voici le contre-exemple de Selmer [3] : nous allons montrer que l'équation

$$3x^3 + 4y^3 + 5z^3 = 0 \tag{2.1}$$

a une solution non nulle dans chaque complété de $\mathbf{Q}$ [1], mais n'a que la solution nulle dans $\mathbf{Q}$. Cela signifie que l'équation (2.1) ne satisfait pas le principe de Hasse. Le premier point est relativement facile à prouver : il s'agit d'une application du lemme de Hensel. Par contre, le deuxième point est plus difficile, et nous aurons besoin d'introduire certains outils de la théorie algébrique des nombres. Cette partie est inspirée de [1].

Nous commençons par prouver que l'équation (2.1) a des solutions locales.

Rappelons déjà le lemme de Hensel, dans le cas de $\mathbf{Q}$ (la démonstration est identique à celle donnée au Lemme 1.1, page 8, qui est énoncé dans le cas de $\mathbf{F}_q(t)$).

Lemme 2.1 (Lemme de Hensel)**.** *Soit P un polynôme à coefficients dans $\mathbf{Z}_p$. S'il existe $\alpha_0 \in \mathbf{Z}_p$ tel que, pour un certain entier N, on ait*

$$P'(\alpha_0) \equiv 0 \pmod{p^N}, \quad P'(\alpha_0) \not\equiv 0 \pmod{p^{N+1}}, \quad P(\alpha_0) \equiv 0 \pmod{p^{2N+1}},$$

1. On peut montrer (voir [2], page 119) que les seules valeurs absolues sur $\mathbf{Q}$ sont :
   - la valeur absolue usuelle, notée $|\cdot|_\infty$;
   - les valeurs absolues non-archimédiennes associées aux nombres premiers.

Les complétions associées sont $\mathbf{Q}_\infty = \mathbf{R}$ et $\mathbf{Q}_p$, pour tout p premier. On note de plus $\mathbf{Z}_p$ l'anneau $\{x \in \mathbf{Q}_p \mid |x|_p \leq 1\}$.

alors il existe $\alpha \in \mathbf{Z}_p$ *tel que*

$$P(\alpha) = 0, \quad et \quad \alpha \equiv \alpha_0 \pmod{p^{N+1}}.$$

Théorème 2.2. *L'équation* (2.1) *a une solution non nulle dans chaque complété de* $\mathbf{Q}$.

Démonstration. Dans $\mathbf{Q}_\infty = \mathbf{R}$, il est évident qu'il existe une solution non nulle.

Soit p un nombre premier. Nous allons prouver que l'équation (2.1) possède une solution non nulle sur $\mathbf{Z}_p$. Nous distinguons 3 cas :

- Si $p = 3$, l'équation $4y^3 - 5 = 0$ a une solution modulo 27, donc par le lemme de Hensel il existe $y_0 \in \mathbf{Z}_3$ tel que $4y_0^3 - 5 = 0$ et $(0, y_0, -1)$ est une solution de l'équation (2.1) dans $\mathbf{Z}_3$.
- Si $p = 5$, l'équation $4y^3 + 3 = 0$ a une solution modulo 5, donc par le lemme de Hensel il existe $y_0 \in \mathbf{Z}_5$ tel que $4y_0^3 + 3 = 0$ et $(1, y_0, 0)$ est une solution de l'équation (2.1) dans $\mathbf{Z}_5$.
- Maintenant, supposons que p soit un nombre premier autre que 3 et 5. Si 3 est un cube dans $(\mathbf{Z}/p\mathbf{Z})^\times$, alors $3x^3 - 1 = 0$ a une solution modulo p. Donc il existe $x_0 \in \mathbf{Z}_p$ tel que $3x_0^3 - 1 = 0$, et $(x_0, 1, -1)$ est une solution de l'équation (2.1) dans $\mathbf{Z}_p$. Si 3 n'est pas un cube dans $(\mathbf{Z}/p\mathbf{Z})^\times$, alors le sous-groupe des cubes dans $(\mathbf{Z}/p\mathbf{Z})^\times$ est d'indice 3, et {1,3,9} est un système de représentants de $(\mathbf{Z}/p\mathbf{Z})^\times/(\mathbf{Z}/p\mathbf{Z})^{\times 3}$. Considérons les trois cas suivants :

  1. Si 5 est un cube, alors $5z^3 - 1 = 0$ a une solution modulo p, donc il existe $z_0 \in \mathbf{Z}_p$ tel que $5z_0^3 - 1 = 0$, et $(-1, 1, z_0)$ est une solution de l'équation (2.1) dans $\mathbf{Z}_p$.
  2. Si 5/3 est un cube, alors $5z^3 - 3 = 0$ a une solution modulo p, donc il existe $z_0 \in \mathbf{Z}_p$ tel que $5z_0^3 - 3 = 0$, et $(-1, 0, z_0)$ est une solution de l'équation (2.1) dans $\mathbf{Z}_p$.
  3. Si 5/9 est un cube, alors $t^3 - 15 = 0$ a une solution modulo p, donc il existe $t_0 \in \mathbf{Z}_p$ tel que $t_0^3 - 15 = 0$, donc $(3t_0, 5, -7)$ est une solution de l'équation (2.1) dans $\mathbf{Z}_p$.

□

Montrons maintenant que l'équation (2.1) n'a pas de solution non nulle dans $\mathbf{Q}$. En ecrivant l'équation (2.1) sous la forme $(2y)^3 + 6x^3 = 10(-z)^3$, on remarque qu'il suffit de montrer que l'équation $x^3 + 6y^3 = 10z^3$ n'a pas de solution non nulle dans $\mathbf{Q}$. Supposons que (a, b, c) soit une telle solution, quitte à eliminer des dénominateurs, on peut supposer que a, b et c sont

entiers et que $\text{pgcd}(a,b,c) = 1$. On remarque qu'aucun des entiers a, b, c n'est nul.

Dans $\mathbf{Z}\left[\sqrt[3]{6}\right]$, on a la relation :

$$(a + b\sqrt[3]{6})(a^2 - ab\sqrt[3]{6} + b^2\sqrt[3]{36}) = 10c^3 \ . \tag{2.2}$$

Il convient donc d'étudier la structure de $\mathbf{Z}\left[\sqrt[3]{6}\right]$. Pour ce faire, nous allons d'abord introduire la théorie des entiers algébriques, la théorie de Minkowski, et le théorème des unités de Dirichlet. Nous ne donnerons pas les preuves, qui peuvent être trouvées dans les sections $1-7$ du chapitre 1 du livre *Algebraic Number Theory* de Jürgen Neukirch [2].

Nous rappelons d'abord la théorie des entier algébriques.

Définition 2.1. Soit K un corps et A un sous-anneau de K. Un élément de K est dit *entier* sur A s'il est annulé par un polynôme unitaire à coefficients dans A.

Les éléments entiers sur A forment un sous-anneau de K.

Définition 2.2. Soit A un anneau intègre, il se plonge alors dans son corps des fractions. L'anneau A est dit intégralement clos si l'ensemble des éléments entiers sur A dans son corps des fractions est réduit à A.

On rappelle qu'un *corps de nombres* est une extension finie du corps $\mathbf{Q}$, et si K est un corps de nombres, O_K est l'anneau des entiers du corps K. Si $\alpha_1, \ldots, \alpha_n$ est une base de l'extension de corps $K/\mathbf{Q}$, on définit le *discriminant* $d(\alpha_1, \ldots, \alpha_n) = \det\left(\text{Tr}_{K/\mathbf{Q}}(\alpha_i\alpha_j)\right)$. Nous avons la proposition suivante :

Proposition 2.1. *Soit $\mathfrak{a} \neq 0$ un O_K-sous-module de type fini dans K. Alors $\mathfrak{a}$ est un $\mathbf{Z}$-module libre de rang $[K : \mathbf{Q}]$.*

Par conséquent, pour un idéal $\mathfrak{a}$, nous pouvons définir $d(\mathfrak{a}) = d(\alpha_1, \ldots, \alpha_n)$ où $\alpha_1, \ldots, \alpha_n$ est une $\mathbf{Z}$-base de $\mathfrak{a}$. Cette quantité est indépendante de la base choisie.

Nous montrons à présent que l'anneau des entiers de $K = \mathbf{Q}(\sqrt[3]{6})$ est $O_K = \mathbf{Z}\left[\sqrt[3]{6}\right]$.

Proposition 2.2. *Si $\mathfrak{a}_1 \subseteq \mathfrak{a}_2$ sont deux O_K-sous-modules de type fini dans K, alors $[\mathfrak{a}_2 : \mathfrak{a}_1]$ est fini, et nous avons la fomule $d(\mathfrak{a}_1) = [\mathfrak{a}_2 : \mathfrak{a}_1]^2 \cdot d(\mathfrak{a}_2)$.*

Proposition 2.3. *Soient K un corps de nombres, $u \in O_K$ tel que $K = \mathbf{Q}(u)$, et p un nombre premier tel que le polynôme minimal de u sur $\mathbf{Q}$ soit d'Eisenstein en p. Alors $p \nmid [O_K : \mathbf{Z}[u]]$.*

Corollaire 2.2.1. *L'anneau des entiers de corps* $K = \mathbf{Q}(\sqrt[3]{6})$ *est* $\mathbf{Z}\left[\sqrt[3]{6}\right]$.

Démonstration. Nous avons $\mathbf{Z}\left[\sqrt[3]{6}\right] \subseteq O_K$, et $d(\mathbf{Z}\left[\sqrt[3]{6}\right]) = -2^2 \cdot 3^5$, donc d'après la propositon 2, les seuls diviseurs premiers possibles de $[O_K : \mathbf{Z}\left[\sqrt[3]{6}\right]]$ sont $2, 3$. Le polynôme minimal de $\sqrt[3]{6}$ est $x^3 - 6$. Il est d'Eisenstein en 2 et 3, et donc d'après la propositon 3, on a $[O_K : \mathbf{Z}\left[\sqrt[3]{6}\right]] = 1$. □

L'anneau O_K a une propriété importante :

Théorème 2.3. *Soit K un corps de nombres. Alors O_K est noethérien, intégralement clos et tous ses idéaux premiers non nuls sont maximaux.*

Un anneau intègre satisfaisant la propriété ci-dessus est appelé *anneau de Dedekind*. Un tel anneau vérifie que tout idéal non nul se décompose de manière unique en un produit d'idéaux premiers non nuls ; en ce sens un anneau de Dedekind est similaire à un anneau factoriel.

Dans cette situation, il est intéressant d'introduire la notion d'idéal fractionnaire. Soient A un anneau de Dedekind et K son corps des fractions.

Définition 2.3. Un idéal fractionnaire de A est une partie de K de la forme $d^{-1}J$ où d est un élément non nul de A et J un idéal non nul de A. C'est un sous-A-module de K de type fini.

Proposition 2.4. *Les idéaux fractionnaires forment un groupe abélien J_K, et tout idéal fractionnaire se décompose de manière unique en un produit fini de puissances positives ou négatives d'idéaux premiers non nuls. Cela signifie que J_K est un groupe abelien* libre.

Définition 2.4. Les idéaux fractionnaires principaux non nuls (a), $a \in K^*$, forment un sous-groupe du groupe des idéaux fractionnaires non nuls, noté P_K. Nous appelons le groupe quotient $Cl_K = J_K/P_K$ le groupe des classes d'idéaux.

Nous avons une suite exacte :

$$1 \longrightarrow A^* \longrightarrow K^* \longrightarrow J_K \longrightarrow Cl_K \longrightarrow 1 \ ,$$

où le morphisme central est $a \to (a)$. Ainsi Cl_K et A^* mesurent la différence entre K^* et J_K. Etudions maintenant les structures de Cl_K et A^*. Pour un corps de nombres K, ces structures sont déterminées par la théorie de Minkowski et le théorème des unités de Dirichlet respectivement.

À partir de maintenant, soit K un corps de nombres de degré n. Il y a alors n plongements $K \hookrightarrow \mathbf{C}$; supposons qu'il y ait r plongements réels et s paires de plongements complexes.

La théorie de Minkowski nous permet de déterminer le groupe Cl_K : nous allons voir que le groupe Cl_K est toujours fini, et que pour $K = \mathbf{Q}\left[\sqrt[3]{6}\right]$, Cl_K est le groupe trival, c'est-à-dire que $\mathbf{Z}\left[\sqrt[3]{6}\right]$ est un anneau principal.

Nous définissons la norme d'un idéal non nul $\mathfrak{a}$ de O_K par $\mathfrak{N}(\mathfrak{a}) = [O_K : \mathfrak{a}]$. La norme est multiplicative : pour deux idéaux non nuls $\mathfrak{a}$ et $\mathfrak{b}$, nous avons $\mathfrak{N}(\mathfrak{ab}) = \mathfrak{N}(\mathfrak{a})\mathfrak{N}(\mathfrak{b})$.

Nous avons alors le résultat suivant :

Théorème 2.4. *Dans chaque classe d'idéaux d'un corps de nombres K, il y a un idéal $\mathfrak{a}$ tel que $\mathfrak{N}(\mathfrak{a}) \leq \frac{n!}{n^n}(\frac{4}{\pi})^s\sqrt{|d(O_K)|}$. Le nombre $\frac{n!}{n^n}(\frac{4}{\pi})^s\sqrt{|d(O_K)|}$ est appelé* la borne de Minkowski.

Ainsi, comme tout idéal non nul de O_K se décompose de manière unique en un produit d'idéaux premiers, pour prouver que O_K est un anneau principal il suffit de vérifier que tous les idéaux premiers de norme inférieure à $\frac{n!}{n^n}(\frac{4}{\pi})^s\sqrt{|d(O_K)|}$ sont principaux.

Nous donnons à présent le théorème des unités de Dirichlet, qui détermine la structure du groupe des unités de O_K pour un corps de nombres K.

Théorème 2.5. *Soit K un corps de nombres. Le groupe O_K^* est isomorphe au produit du groupe des racines de l'unité de K et d'un groupe abélien libre de rang $r + s - 1$.*

Maintenant nous pouvons prouver :

Théorème 2.6. *L'équation (2.1) n'a pas de solution non nulle dans* $\mathbf{Q}$.

Démonstration. Nous avons vu qu'il est suffisant de montrer que l'équation (2.2) n'a pas de solutions non nulles dans $\mathbf{Z}$. Soit donc (a, b, c) une telle solution, avec $\text{pgcd}(a, b, c) = 1$. On voit immédiatement que a est pair, b et c sont impairs, et 3 et 5 ne divisent pas a.

Soit $K = \mathbf{Q}\left[\sqrt[3]{6}\right]$. Nous avons $O_K = \mathbf{Z}\left[\sqrt[3]{6}\right]$ par le corollaire 2.2.1. De plus, il y a un plongement réel et une paire de plongements complexes pour K, donc $r = s = 1$. Nous démontrons maintenant le théorème étape par étape.

Etape 1 : Nous allons montrer que O_K est un anneau principal. Nous calculons que $d(O_K) = -2^2 \cdot 3^5$, donc la borne de Minkowski est

$$\frac{3!}{3^3}\left(\frac{4}{\pi}\right)^1\sqrt{|d(O_K)|} = \frac{16\sqrt{3}}{\pi} \approx 8.8\ .$$

Il est donc suffisant de prouver que chaque idéal premier $\mathfrak{p}$ avec $\mathfrak{N}(\mathfrak{p}) \leq 8.8$ est principal. Un tel idéal doit diviser (p) pour certains $p \in \{2, 3, 5, 7\}$.

Nous vérifions la factorisation de (p) pour $p \in \{2, 3, 5, 7\}$. Noter que (p) se factorise dans O_K de la même manière que $(x^3 - 6)$ se factorise dans $\mathbf{F}_p[x]$, ainsi : $(2) = \mathfrak{p}_2^3$, $(3) = \mathfrak{p}_3^3$, $(5) = \mathfrak{p}_5\mathfrak{p}_{25}$ et $(7) = \mathfrak{p}_7\mathfrak{p}_7'\mathfrak{p}_7''$. Comme $N_{K/\mathbf{Q}}(2 - \sqrt[3]{6}) = 2$ et $N_{K/\mathbf{Q}}(1 - \sqrt[3]{6}) = -5$, nous devons avoir $\mathfrak{p}_2 = (2 - \sqrt[3]{6})$ et $\mathfrak{p}_5 = (1 - \sqrt[3]{6})$. Comme $N_{K/\mathbf{Q}}(\sqrt[3]{6}) = 6$, on a $(\sqrt[3]{6}) = \mathfrak{p}_2\mathfrak{p}_3$, et on en déduit que $\mathfrak{p}_2$, $\mathfrak{p}_3$ et $\mathfrak{p}_5$ sont principaux. Comme $N_{K/\mathbf{Q}}(1+\sqrt[3]{6}) = 7$, $N_{K/\mathbf{Q}}(2+\sqrt[3]{6}) = 14$, $N_{K/\mathbf{Q}}(4 + \sqrt[3]{6}) = 70$, et vu que 1, 2 et 4 ne sont pas congrus deux-à-deux modulo 7, nous pouvons supposer $(1 + \sqrt[3]{6}) = \mathfrak{p}_7$, $(2 + \sqrt[3]{6}) = \mathfrak{p}_7'\mathfrak{p}_2$ et $(4 + \sqrt[3]{6}) = \mathfrak{p}_7''\mathfrak{p}_2\mathfrak{p}_5$, donc $\mathfrak{p}_7$, $\mathfrak{p}_7'$, $\mathfrak{p}_7''$ sont tous principaux. Nous avons prouvé que O_K est un anneau principal.

Etape 2 : Nous allons montrer que $(a + b\sqrt[3]{6}, a^2 - ab\sqrt[3]{6} + b^2\sqrt[3]{36}) = \mathfrak{p}_2$.

D'une part, $\mathfrak{p}_2 \mid (a + b\sqrt[3]{6}, a^2 - ab\sqrt[3]{6} + b^2\sqrt[3]{36})$ car $\mathfrak{p}_2 \mid a$ et $\mathfrak{p}_2 \mid \sqrt[3]{6}$. De plus, $\mathfrak{p}_2^2 \nmid a + b\sqrt[3]{6}$ car sinon, en prenant la norme des deux côtés, on obtiendrait $4 \mid 10c^3$, ce qui contredit le fait que c est impair.

D'autre part, soit $\mathfrak{p}$ un idéal premier tel que $\mathfrak{p} \mid (a + b\sqrt[3]{6}, a^2 - ab\sqrt[3]{6} + b^2\sqrt[3]{36})$, alors $\mathfrak{p} \mid (3)(a^2)$ et $\mathfrak{p} \mid (3)(b^2)(\sqrt[3]{36})$. Supposons que $\mathfrak{p} \mid 3$. Alors $\mathfrak{p} = \mathfrak{p}_3$, donc $\mathfrak{p}_3 \mid (a)$, puis $3 \mid a$, contradiction. Ainsi, $\mathfrak{p} \mid (a)$ et $\mathfrak{p} \mid (b)^2\mathfrak{p}_2^2$. Or, (a) et (b) sont premiers entre eux, d'où $\mathfrak{p} = \mathfrak{p}_2$. Nous avons ainsi prouvé que $(a + b\sqrt[3]{6}, a^2 - ab\sqrt[3]{6} + b^2\sqrt[3]{36}) = \mathfrak{p}_2$.

Etape 3 : Nous allons montrer que $\mathfrak{p}_5 \mid a + b\sqrt[3]{6}$ et $(5) \nmid a + b\sqrt[3]{6}$.

Comme $a^3 + b^3 \equiv 10c^3 \equiv 0 \pmod{\mathfrak{p}_5}$, nous avons $a + b \equiv 0 \pmod{\mathfrak{p}_5}$, donc $a + b\sqrt[3]{6} \equiv a + b \equiv 0 \pmod{\mathfrak{p}_5}$ car $\mathfrak{p}_5 = (1 - \sqrt[3]{6})$. De plus, $(5) \nmid a + b\sqrt[3]{6}$ parce que $5 \nmid a$.

Etape 4 : L'équation (2.2) implique que :

$$(a + b\sqrt[3]{6})(a^2 - ab\sqrt[3]{6} + b^2\sqrt[3]{36}) = \mathfrak{p}_2^3\mathfrak{p}_5\mathfrak{p}_{25}c^3 \ ,$$

donc en utilisant les étapes 2 et 3, on voit que $(a + b\sqrt[3]{6}) = \mathfrak{p}_2\mathfrak{p}_5(\alpha)^3 = (2 - \sqrt[3]{6})(1 - \sqrt[3]{6})(\alpha)^3$, où $\alpha \in \mathbf{Z}\left[\sqrt[3]{6}\right]$, on en déduit qu'il existe $u \in \mathbf{Z}\left[\sqrt[3]{6}\right]^*$ tel que

$$a + b\sqrt[3]{6} = (2 - \sqrt[3]{6})(1 - \sqrt[3]{6})\alpha^3 u. \tag{2.3}$$

Etape 5 : Pour $K = \mathbf{Q}\left[\sqrt[3]{6}\right]$, il y a un plongement réel et une paire de plongements complexes. En appliquant le théorème des unités de Dirichlet (Théorème 2.5), nous avons $\mathbf{Z}\left[\sqrt[3]{6}\right]^* = \{\pm 1\} \times \mathbf{Z}$, donc $\mathbf{Z}\left[\sqrt[3]{6}\right]^* / \mathbf{Z}\left[\sqrt[3]{6}\right]^{*3}$ est un groupe cyclique d'ordre 3. On rappelle que $(2) = (2 - \sqrt[3]{6})^3$, et donc que $\frac{(2-\sqrt[3]{6})^3}{2} = 1 - 6\sqrt[3]{6} + 3\sqrt[3]{36}$ est une unité. De plus, nous avons $\frac{(2-\sqrt[3]{6})^3}{2} \equiv 3 \pmod{\mathfrak{p}_7}$. Ce n'est pas un cube dans $\mathbf{Z}/7\mathbf{Z}$ et donc $\frac{(2-\sqrt[3]{6})^3}{2}$ en-

gendre $\mathbf{Z}\left[\sqrt[3]{6}\right]^*/\mathbf{Z}\left[\sqrt[3]{6}\right]^{*3}$. Nous pouvons ainsi supposer que $u = (\frac{(2-\sqrt[3]{6})^3}{2})^k$, avec $k \in \{0, 1, 2\}$.

Etape 6 : On multiplie l'équation (2.3) par 2^k, ce qui donne :

$$2^k(a + b\sqrt[3]{6}) = (2 - \sqrt[3]{6})(1 - \sqrt[3]{6})\beta^3 ,$$

où $\beta = (2 - \sqrt[3]{6})^k\alpha$. Écrivons β sous la forme $A + B\sqrt[3]{6} + C\sqrt[3]{36}$, avec A, B, $C \in \mathbf{Z}$. En comparant les coefficients devant $\sqrt[3]{36}$, on obtient :

$$0 = A^3+6B^3+36C^3+36ABC-9(A^2B+6B^2C+6C^2A)+6(AB^2+6BC^2+CA^2) .$$

Montrons que $(A, B, C) = (0, 0, 0)$. Dans le cas contraire, on peut supposer que $\text{pgcd}(A, B, C) = 1$. En reduisant successivement modulo $3, 6, 9$, nous obtenons $3 \mid A$, $3 \mid B$ et $3 \mid C$, contradiction. Donc $\beta = 0$ et $a = b = 0$, ce qui est absurde. □

Annexe A

Le théorème de la progression arithmétique de Dirichlet

Dans cette annexe, nous allons démontrer le théorème suivant, utilisé pour démontrer le théorème 1.9, page 18.

Théorème A.1. *Soient A, B des polynômes unitaires non nuls de $\mathbf{F}_q[t]$; supposons que A et B sont premiers entre eux.*
Alors, pour n assez grand, il existe P irréductible unitaire et de degré n tel que $P \equiv A \pmod{B}$.

Pour cela, nous allons suivre la même démarche que pour la démonstration sur $\mathbf{Z}$, c'est-à-dire en utilisant les *séries L*.

Définition A.1. Soit G un groupe abélien fini. Un *caractère* de G est un morphisme de $G \to \mathbf{C}^*$. L'ensemble des caractère forme un groupe, appelé le *dual* de G, et noté $\widehat{G}$.

En particulier : si $B \in \mathbf{F}_q[t] - \{0\}$ et $G_B = (\mathbf{F}_q[t]/B \cdot \mathbf{F}_q[t])^*$, on parlera de *caractères modulo B* pour désigner les éléments de $\widehat{G_B}$. Ces caractères peuvent être étendus à $\mathbf{F}_q[t]$ tout entier de la manière suivante : si $\chi \in \widehat{G_B}$, on pose, pour $f \in \mathbf{F}_q[t]$:

$$\chi(f) = \begin{cases} \chi(f \bmod B) & \text{si } B \wedge f = 1 \\ 0 & \text{sinon} \end{cases},$$

où « $f \bmod B$ » désigne bien sûr la projection naturelle de f dans G_B.

Proposition A.1. *Soit G un groupe abélien fini. Alors le groupe $\widehat{G}$ est abélien fini et est isomorphe à G. En particulier, ces deux groupes ont le même cardinal.*

Démonstration. Que $\widehat{G}$ est un groupe abélien est évident. Quant à l'isomorphisme, on le construit en décomposant G en produit de groupes cycliques : il suffit alors de montrer le résultat pour ces derniers.
Soit H un groupe cyclique, de générateur h_0 et de cardinal n ; soit $\chi \in \widehat{H}$. On note $z_0 = \chi(h_0)$. Comme $h_0^n = 1$, on a nécessairement $z_0^n = 1$, donc z_0 est une racine n-ième de l'unité. Réciproquement, si on choisit z_0 parmi les racines n-ièmes de l'unité, cela détermine de manière unique un caractère de H. Il y a donc un isomorphisme entre $\widehat{H}$ et le groupe des racines n-ièmes de l'unité $\mathbf{U}_n$, lui-même isomorphe à $\mathbf{Z}/n\mathbf{Z}$, donné par : $\widehat{H} \ni \chi \mapsto \chi(h_0) \in \mathbf{U}_n$. □

Remarque A.1. On remarque les choses suivantes :

1. L'isomorphisme exhibé dépend du choix du générateur h_0 .
2. Cela implique que G et $\widehat{\widehat{G}}$ sont isomorphes ; mais à la différence de G et $\widehat{G}$, il y a un isomorphisme *canonique* donné par : $g \mapsto \Big(\chi \mapsto \chi(g)\Big)$ (en effet, on montre que ce morphisme est injectif et on conclut par cardinalité).

On a les « relations d'orthogonalité » importantes suivantes :

Proposition A.2. *Soit $n = |G| = |\widehat{G}|$.*

1. Si $g \in G$:

$$\sum_{\chi \in \widehat{G}} \chi(g) = \begin{cases} n & \text{si } g = 1 \\ 0 & \text{sinon} \end{cases} . \tag{A.1}$$

2. Si $\chi \in \widehat{G}$:

$$\sum_{g \in G} \chi(g) = \begin{cases} n & \text{si } \chi = 1 \\ 0 & \text{sinon} \end{cases} . \tag{A.2}$$

Démonstration. Ces deux relations sont bien sûr duales l'une de l'autre, à travers l'isomorphisme mentionné dans la remarque précédente. Il suffit de montrer par exemple la formule (A.2). C'est classique :

- si $\chi = 1$, la formule est évidente ;
- sinon, soit $g_0 \in G$ tel que $\chi(g_0) \neq 1$. Alors, en réordonnant la somme par la bijection sur G : $g \mapsto g_0^{-1} \cdot g$, on a :

$$\sum_{g \in G} \chi(g) = \sum_{g_0^{-1} g \in G} \chi(g) = \sum_{g \in G} \chi(g_0 \cdot g) = \chi(g_0) \cdot \sum_{g \in G} \chi(g) .$$

D'où le résultat. □

Remarque A.2. Si on pose $\langle \chi, \chi' \rangle = \frac{1}{\sqrt{n}} \sum_{g \in G} \chi(g) \cdot \overline{\chi'(g)}$, les formules ci-haut expriment que l'ensemble des caractères d'un groupe forme une famille orthonormée pour $\langle \cdot, \cdot \rangle$. En particulier, si $G = G_B = (\mathbf{F}_q[t]/B \cdot \mathbf{F}_q[t])^*$, on peut définir ainsi une sorte de « transformée de Fourier » sur les fonctions de $\mathbf{F}_q[t] \to \mathbf{C}^*$.

Dans la suite, on fixe $B \in \mathbf{F}_q[t] - \{0\}$. La remarque précédente conduit alors aux définitions suivantes :

Définition A.2. On rappelle que $|\cdot|_\infty = q^{\deg(\cdot)}$.

1. On définit la *fonction zêta* par :

$$\zeta(s) = \sum_{\substack{f \in \mathbf{F}_q[t] \\ \text{unitaire}}} \frac{1}{|f|_\infty^s} \,. \tag{A.3}$$

2. Soit $\chi \in \widehat{G_B}$. On définit la *série* L associée par :

$$L_\chi(s) = \sum_{\substack{f \in \mathbf{F}_q[t] \\ \text{unitaire}}} \frac{\chi(f)}{|f|_\infty^s} \,. \tag{A.4}$$

Remarque A.3. Ces fonctions s'expriment en fonction de s au travers de l'expression q^{-s} ; elles sont donc périodiques de période $2\pi i / \log q$. Dans la suite, nous sous-entendons cette périodicité : lorsqu'on parlera « du » pôle de ζ en 1, il sera implicite que ce pôle est en fait répété par périodicité. Plus précisément, on fera comme si on travaille dans la bande $\{-\pi i/\log(q) < \Im(s) \leq \pi i/\log(q)\}$.

Théorème A.2. *Soit $\mathscr{P} = \{P \in \mathbf{F}_q[t]$ irréductible unitaire$\}$*

1. *La fonction ζ est holomorphe sur le demi-plan $\{\Re(z) > 1\}$, a un pôle simple en $s = 1$, et on a les formules :*

$$\zeta(s) \overset{(a)}{=} \prod_{P \in \mathscr{P}} \frac{1}{1 - \frac{1}{|P|_\infty^s}} \overset{(b)}{=} \frac{1}{1 - q^{1-s}} \,. \tag{A.5}$$

2. *Si $\chi = 1$: L_1 est holomorphe sur le demi-plan $\{\Re(z) > 1\}$, a un pôle simple en $s = 1$, et on a les formules :*

$$L_1(s) = \prod_{\substack{P \in \mathscr{P} \\ P \nmid B}} \frac{1}{1 - \frac{1}{|P|_\infty^s}} = \zeta(s) \cdot \prod_{\substack{P \in \mathscr{P} \\ P \mid B}} \left(1 - \frac{1}{|P|_\infty^s}\right) \,. \tag{A.6}$$

3. *Si $\chi \neq 1$: L_χ est un polynôme en q^{-s}, et on a de plus la formule, pour $\Re(s) > 1$:*

$$L_\chi(s) = \prod_{\substack{P \in \mathscr{P} \\ P \nmid B}} \frac{1}{1 - \frac{\chi(P)}{|P|_\infty^s}} \,. \tag{A.7}$$

Démonstration. 1. Commençons par un peu de dénombrement : le nombre de polynômes unitaires de degré n vaut exactement q^n (car il y a n coefficients à choisir dans $\mathbf{F}_q$). Ainsi, en réordonnant les termes, on voit qu'on a à considérer la convergence de séries de terme général : $\left|\frac{q^n}{q^{n\cdot s}}\right| = (q^{1-\Re(s)})^n$, qui est assurée dès que $\Re(s) > 1$. D'ailleurs, la somme de la série $\sum_{n=0}^{\infty}(q^{1-s})^n$ vaut précisément $\frac{1}{1-q^{1-s}}$, ce qui donne la formule (b) pour ζ.
Puis la formule du produit provient classiquement de la décomposition en produit de facteurs premiers. Plus précisément, si $\mathscr{A} \subset \mathscr{P}$ est un sous-ensemble *fini* de polynômes irréductibles unitaires, on a :

$$\prod_{P \in \mathscr{A}} \frac{1}{1 - |P|_\infty^{-s}} = \prod_{P \in \mathscr{A}} \left(\sum_{k=0}^{\infty} |P|_\infty^{-sk} \right) = \sum_{f \in \mathbf{P}(\mathscr{A})} \frac{1}{|f|_\infty^s} \,,$$

où $\mathbf{P}(\mathscr{A})$ est l'ensemble des polynômes unitaires qui se décomposent en facteurs premiers tous dans $\mathscr{A}$. En prenant une suite croissante (pour l'inclusion) de $\mathscr{A}_i \subset \mathscr{P}, i \in \mathbf{N}$ finis tels que $\bigcup_{i \in \mathbf{N}} \mathscr{A}_i = \mathscr{P}$, on obtient l'égalité (a) pour ζ.

2. La démonstration est tout à fait analogue au cas de ζ.
3. À nouveau, la formule du produit se démontre de façon analogue, et repose sur la propriété de multiplicativité des caractères. Il reste donc à démontrer que la série (A.4) définissant L_χ est constituée d'un nombre fini de termes non nuls. Écrivons :

$$L_\chi(s) = \sum_{n=1}^{\infty} \frac{1}{q^{ns}} \overbrace{\sum_{\substack{f \in \mathbf{F}_q[t] \\ \text{unitaire} \\ \deg(f)=n}} \chi(f)}^{a_n} \,.$$

Nous allons montrer que : si $n \geq \deg(B)$, alors $a_n = 0$. Cela découle du lemme suivant.

Lemme A.1. *Soit, pour tout entier r, $\mathscr{D}_r = \{f \in \mathbf{F}_q[t] \text{ unitaire}, \deg(f) = r\}$. Soit $n \geq \deg(B)$. Il y a une bijection entre $\mathscr{D}_{n-\deg(B)} \times \mathbf{F}_q[t]_{\deg(B)-1}$ et $\mathscr{D}_n$, donnée par : $(h, g) \mapsto B \cdot h + g$.*

Démonstration. L'injectivité de l'application est claire ; et on conclut par cardinalité. □

Avec le lemme, on termine facilement l'argument : comme $\chi(B\cdot h+g) = \chi(g)$, cela découle de la relation d'orthogonalité (A.2).

□

Corollaire A.2.1. *La fonction ζ se prolonge en une fonction méromorphe sur $\mathbf{C}$, avec un pôle simple en 1 ; il en est de même de L_1. Pour tout caractère $\chi \neq 1$, la série L_χ est holomorphe sur $\mathbf{C}$.*

Remarque A.4. On voit ici que le fait de travailler dans $\mathbf{F}_q[t]$ simplifie considérablement les séries ζ et L_χ par rapport à dans $\mathbf{Z}$, on obtient ainsi des propriétés de prolongement analytique beaucoup plus facilement.

Corollaire A.2.2. *On a : $\sum_{P\in\mathscr{P}} \frac{1}{|P|_\infty} = \infty$.*
En particulier, il y a une infinité de polynômes irréductibles.

Démonstration. Supposons par l'absurde que cette somme converge ; alors ceci impliquerait la convergence du produit infini $\prod_{P\in\mathscr{P}}(1 - \frac{1}{|P|_\infty})^{-1}$, ce qui est absurde, car justement ζ a un pôle en $s = 1$. □

L'idée de la démonstration est maintenant de répéter le même argument que dans le corollaire, mais avec les séries L. Plus précisément, si on parvient à montrer que les produits convergent (c'est-à-dire ne sont ni nuls ni infinis) en $s = 1$ sauf pour le caractère trivial $\chi = 1$, on aura un contrôle précis de la divergence de la « transformée de Fourier » de la fonction $\frac{1}{|P|_\infty^s}$ (à savoir que seule la composante $\chi = 1$ diverge en $s = 1$), et en exprimant $\sum_{\substack{P\in\mathscr{P} \\ P\equiv A \pmod B}} \frac{1}{|P|_\infty^s}$ en fonction de ces transformées, on pourra montrer que cette série diverge en $s = 1$, ce qui conclura la démonstration.
En réalité, comme on a besoin d'un contrôle sur le degré des polynômes P satisfaisant à la condition précédente, il nous faut étudier la convergence et la non-annulation des séries L non pas en $s = 1$ seulement, mais sur toute la droite $\Re(s) = 1$. Nous allons donc maintenant étudier les zéros des séries L.

Introduisons la fonction :

$$f(s) = \prod_{\chi\in\widehat{G_B}} L_\chi(s) \,. \tag{A.8}$$

C'est une fonction méromorphe sur $\mathbf{C}$; elle a éventuellement un pole simple en $s = 1$.

Remarque A.5 (Rappel). Dans le passage qui va suivre, la remarque plus haut sur la périodicité des fonctions considérées va jouer un rôle important. Nous rappelons donc que toutes les fonctions introduites jusqu'à présent sont périodiques en la variable s, de période $\frac{2\pi i}{\log(q)}$. De plus, sauf mention explicite, cette périodicité est sous-entendue : on fait comme si on travaillait seulement sur la bande $\{-\pi i/\log(q) < \Im(s) \leq \pi i/\log(q)\}$.

Théorème A.3. *Pour tout s tel que $\Re(s) = 1$, sauf peut-être pour $s = 1 + \frac{\pi i}{\log(q)}$, $f(s) \neq 0$.*

Cela donne déjà une bonne partie du travail :

Corollaire A.3.1. *Pour tout s tel que $\Re(s) = 1$ et $s \notin \{1, 1+\frac{\pi i}{\log(q)}\}$, $L_\chi(s) \neq 0$ pour tout caractère χ.*

Démonstration du corollaire. C'est clair : sauf en $s = 1$, toutes les séries L_χ sont holomorphes sur la droite $\Re(s) = 1$, donc si l'une s'annule, elle annule tout le produit, ce qui est absurde. □

Démonstration du théorème. Considérons le logarithme de f :

$$\log f(s) = \sum_{\chi \in \widehat{G_B}} \log L_\chi(s) = \sum_{P \in \mathscr{P}} \sum_{n=1}^{\infty} \left(\sum_{\chi \in \widehat{G_B}} \chi(P^n) \right) \frac{|P|_\infty^{-ns}}{n} .$$

Or, $\sum_{\chi \in \widehat{G_B}} \chi(P^n) = 0$ ou $|G_B|$, c'est en particulier *réel et positif.*
Astuce : on remarque que, pour tout $x \in \mathbf{R}$, $3 + 4\cos(x) + \cos(2x) = 3 + 4\cos(x) + 2\cos^2(x) - 1 = 2(1 + \cos(x))^2 \geq 0$.
Considérons donc, à $t \in \mathbf{R}$ fixé la fonction $g_t(s) = f(s)^3 \cdot f(s+it)^4 \cdot f(s+2it)$, où $s \in \mathbf{R}$. Alors, on a :

$$\begin{aligned} \log |g_t(s)| &= \Re(\log g_t(s)) \\ &= \sum_{\substack{P \in \mathscr{P} \\ n \geq 1 \\ \chi \in \widehat{G_B}}} \chi(P^n) \frac{|P|_\infty^{-ns}}{n} \begin{pmatrix} 3 + 4\cos(n \deg(P) \log(q) t) \\ + \cos(2n \deg(P) \log(q) t) \end{pmatrix} \\ &\geq 0 , \qquad \text{d'où } |g_t(s)| \geq 1. \end{aligned}$$

Maintenant, on sait que f a éventuellement un pôle d'ordre au plus 1 en $s = 1$. Si $f(1 + it) = 0$, alors à cause du jeu des puissances, $g_t(1) = 0$, ce qui est contradictoire. Mais attention : cet argument ne marche pas si $t = \frac{\pi}{\log(q)}$, car alors $f(s + 2it) = f(s)$ et donc le pôle éventuel en $s = 1$ est répété et peut compenser l'annulation en $1 + it$. La seule chose qu'on peut dire est que f a un zéro d'ordre *au plus 1* en $s = 1 + \frac{\pi i}{\log(q)}$.

Pour toutes les autres valeurs de t, l'argument fonctionne, et on en déduit que f ne s'annule pas en $1 + it$, pour $t \notin \{0, \frac{\pi i}{\log(q)}\}$. □

On voit qu'à cause de la singularité en $s = 1$, il nous faut un résultat plus fin pour conclure dans les deux cas restants. On va d'avord traiter le cas $s = 1$, et le cas $s = 1 + \frac{\pi i}{\log(q)}$ en découlera simplement.

Lemme A.2. *Soient, pour tout $P \in \mathscr{P}$, f_P et g_P respectivement l'ordre de P dans le groupe G_B et l'indice du sous-groupe qu'il engendre. Alors, pour $\Re(s) > 1$:*

$$f(s) = \prod_{\substack{P \in \mathscr{P} \\ P \nmid B}} \frac{1}{\left(1 - \frac{1}{|P|_\infty^{f_P s}}\right)^{g_P}} \cdot \tag{A.9}$$

Démonstration. Considérons l'application $\varphi : \begin{array}{c} \widehat{G} \longrightarrow \mathbf{C}* \\ \chi \longmapsto \chi(P) \end{array}$. Comme P est d'ordre f_P, on a automatiquement que l'image de φ est exactement le groupe des racines f_P-ièmes de l'unité ; par conséquent son noyau a pour cardinal g_P. On en déduit que dans l'image de φ, chaque racine f_P-ième de l'unité apparait g_P fois, donc :

$$\prod_{\chi \in \widehat{G_P}} (1 - \chi(P)T) = \prod_{\omega \in U_{f_P}} (1 - \omega T)^{g_P} = (1 - T^{f_P})^{g_P} \cdot$$

Or, d'après les formules (A.6) et (A.7) du théorème A.2, pour $\Re(s) > 1$:

$$f(s) = \prod_{\chi \in \widehat{G_B}} \prod_{\substack{P \in \mathscr{P} \\ P \nmid B}} \frac{1}{1 - \frac{\chi(P)}{|P|_\infty}} \cdot$$

En intervertissant les produits, on voit que la formule annoncée découle du calcul ci-dessus, où $T = \frac{1}{|P|_\infty}$.

□

Lemme A.3. *Soit $F(s) = \sum_{n=1}^{\infty} a_n q^{-ns}$, où tous les a_n sont* réels et positifs. *Alors il existe $\rho \in \mathbf{R} \cup \{-\infty, +\infty\}$ tel que l'ensemble de convergence absolue de la série F soit le demi-plan ouvert $\{\Re(s) > \rho\}$. De plus, F ne peut se prolonger holomorphiquement au voisinage de $s = \rho$.*

Démonstration. La transformation $t = q^{-s}$ transforme la série $F(s)$ en une série entière $G(t) = \sum_{n=1}^{\infty} a_n t^n$. Il est connu qu'une telle série admet un disque de convergence, disons de rayon R. L'image inverse de ce disque par l'inverse de la fonction exponentielle donne alors bien un demi-plan ouvert $\{\Re(s) > \rho\}$, où $\rho = -\log R / \log q$ (avec des conventions évidentes si $R = 0$ ou ∞).

Supposons que F s'étende holomorphiquement au voisinage de ρ. Quitte à se translater, on peut supposer que $\rho = 0$ et que F est holomorphe dans un disque $D(1, 1 + \epsilon)$. Écrivons alors sa série de Taylor en 1 :

$$F(s) = \sum_{k=0}^{\infty} \frac{1}{k!} F^{(k)}(1)(s-1)^k = \sum_{k=0}^{\infty} \frac{1}{k!} \sum_{n=1}^{\infty} a_n \log(n)^k n^{-1} (1-s)^k \cdot$$

Notamment, si on évalue ceci en $-\epsilon/2$, on obtient une série double convergente à termes positifs : on intervertit sans se poser de questions, et on obtient que la série suivante converge :

$$F(-\epsilon/2) = \sum_{n=1}^{\infty} a_n n^{-1} \sum_{k=0}^{\infty} \frac{(1+\epsilon/2)^k \log(n)^k}{k!} = \sum_{n=1}^{\infty} a_n n^{\epsilon/2} \ .$$

Comme les coefficients sont positifs, cela prouve la convergence absolue de la série F pour $s = -\epsilon/2$, ce qui contredit la valeur $\rho = 0$. □

Remarque A.6. La première partie du lemme est également valide même si les coefficients sont des complexes quelconques. Néanmoins, la positivité est nécessaire dans la deuxième partie : les séries L en sont un bon exemple !

Avec ces deux lemmes en poche, on peut énoncer le résultat tant attendu :

Théorème A.4. *Pour tout caractère $\chi \neq 1$, $L_\chi(1) \neq 0$.*

Démonstration. Supposons par l'absurde qu'un des L_χ s'annule en $s = 1$. Alors cette annulation compense le pôle simple de L_1, donc f est holomorphe en $s = 1$, puis sur $\mathbf{C}$ tout entier. Par le Lemme A.2, on sait que f est une série satisfaisant aux hypothèses du Lemme A.3. Par conséquent, on a que la série définissant f converge sur ce même domaine.
Or, en examinant la formule du Lemme A.2, on voit bien que ceci est impossible : en notant $n = |G_B|$, on a que $1 - \frac{1}{|P|_\infty^{ns}} \geq \left(1 - \frac{1}{|P|_\infty^{f_P s}}\right)^{g_P}$ pour s réel positif, donc le produit définissant f a ses coefficients supérieurs à ceux de $L_1(ns)$, qui diverge en $s = 1/n$. D'où la contradiction. □

Remarque A.7. On aurait pu se passer de ceci si on voulait simplement traiter le cas des caractères non réels ; en effet ceux-ci apparaissent toujours par paires, avec leur conjugué. Comme $L_{\overline{\chi}}(1) = \overline{L_\chi(1)}$, les annulations vont par paires également, ce qui *annule* la fonction f en $s = 1$, d'où une contradiction. Le cas des caractères réels ne peut néanmoins être évité, mais il est plus simple que le cas général, vu qu'ils ne prennent comme valeur que 1 ou -1...

On en déduit, comme annoncé plus haut :

Corollaire A.4.1. *Pour tout caractère $\chi \neq 1$, $L_\chi(1 + \frac{\pi i}{\log(q)}) \neq 0$.*

Démonstration. Cela résulte du calcul suivant.

$$\begin{aligned} L_\chi(s)L_\chi(s+\frac{\pi i}{\log(q)}) &= \prod_{\substack{P\in\mathscr{P}\\ P\nmid B}} \frac{1}{1-\frac{\chi(P)}{(q^s)^{\deg(P)}}}\frac{1}{1-\frac{\chi(P)}{(-q^s)^{\deg(P)}}} \\ &= \prod_{\substack{P\in\mathscr{P}\\ P\nmid B\\ \deg(P)\text{ pair}}} \left(\frac{1}{1-\frac{\chi(P)}{(q^s)^{\deg(P)}}}\right)^2 \prod_{\substack{P\in\mathscr{P}\\ P\nmid B\\ \deg(P)\text{ impair}}} \frac{1}{1-\frac{\chi(P)^2}{(q^{2s})^{\deg(P)}}} \\ &= L_\chi^{(\text{pair})}(s)^2 \cdot L_{\chi^2}^{(\text{impair})}(2s)\ , \end{aligned} \tag{A.10}$$

avec des notations aisément compréhensibles. Supposons que le membre de gauche de cette égalité s'annule en $s=1$. D'une part, par le théorème A.4, $L_\chi(1)\neq 0$, et d'autre part, on a vu que L_χ a un zéro d'ordre *au plus* 1 en $1+\frac{\pi i}{\log(q)}$. On en déduit donc que l'annulation du terme de gauche est d'ordre au plus 1 en $s=1$.

Alors il en est de même du membre de droite ; donc un des deux facteurs du produit a un *zéro simple* en $s=1$. Mais il est clair (d'après la formule (A.10) ci-dessus) que $L_\chi^{(\text{impair})}(2)\neq 0$, quel que soit χ. D'où la contradiction, et $L_\chi(1+\frac{\pi i}{\log(q)})\neq 0$. □

On a donc montré que pour tout caractère $\chi\neq 1$, L_χ ne s'annule pas sur la droite $\Re(s)=1$. En particulier, par continuité / compacité, il existe $0<\alpha_\chi<1$ tel que pour tout s dans le domaine $\{Re(s)>\alpha_\chi, -\pi i/\log(q)\leq \Im(s)\leq \pi i/\log(q)\}$, $L_\chi(s)\neq 0$. Mais par périodicité, cela implique que L_χ ne s'annule pas sur tout le demi-plan $\{\Re(s)>\alpha_\chi\}$. En posant $\alpha=\max_{\chi\neq 1}\alpha_\chi$, on obtient donc le résultat suivant.

Théorème A.5. *Il existe une constante $0<\alpha<1$ telle que pour tout caractère $\chi\neq 1$, pour tout s tel que $\Re(s)>\alpha$, $L_\chi(s)\neq 0$.*

Remarque A.8. Autant la périodicité en s s'est montrée « embêtante » pour étudier les zéros sur la droite $\Re(s)=1$, autant celle-ci joue maintenant en notre faveur, car on peut établir un résultat de localisation des zéros des séries L très fort. Il faut en particulier comparer ceci avec le cas de $\mathbf{Z}$, où on est loin d'avoir un tel résultat. En fait, dans $\mathbf{F}_q[t]$, il y a un résultat encore plus fort, puisque *l'Hypothèse de Riemann généralisée est démontrée* ; cela implique notamment qu'on peut prendre $\alpha=1/2$ dans le théorème précédent (voir par exemple [5], page 169).

Dans la suite, on va exploiter la structure polynômiale des L_χ en la variable $z=q^{-s}$: on va donc noter $L_\chi(s)=P_\chi(q^{-s})$, où les P_χ sont

des pôlynômes (bien sûr, $\chi \neq 1$). On notera également $n_\chi = \deg(P_\chi)$, et $w_\chi^{(1)}, \ldots, w_\chi^{(n_\chi)}$ ses racines.

On a alors l'égalité simple :

$$\prod_{i=1}^{n_\chi}(z - w_\chi^{(i)}) = \prod_{n=1}^{\infty} \prod_{\substack{P \in \mathscr{P} \\ P \nmid B \\ \deg(P)=n}} (1 - \chi(P) z^n)^{-1} ,$$

pour tout z tel que $\Re(z) > 1$. Passant à la dérivée logarithmique pour transformer le produit en somme, on est ramené à :

$$\sum_{i=1}^{n_\chi} \sum_{n=0}^{\infty} -\frac{1}{w_\chi^{(i)}} \left(\frac{z}{w_\chi^{(i)}}\right)^n = \sum_{n=1}^{\infty} \sum_{\substack{P \in \mathscr{P} \\ P \nmid B \\ \deg(P)=n}} \sum_{k=1}^{\infty} n \chi(P)^k z^{nk-1} .$$

Réordonnons la somme de droite : on obtient une identité entre deux séries. En identifiant les coefficients, on déduit :

$$-\sum_{i=1}^{n_\chi} \left(\frac{1}{w_\chi^{(i)}}\right)^{n+1} = \sum_{\substack{P \in \mathscr{P}, k \geq 1 \\ k \deg(P) - 1 = n \\ P \nmid B}} \deg(P) \cdot \chi(P)^k . \tag{A.11}$$

Notons $a_\chi(n+1)$ ce coefficient. Posons de plus :

$$a_1(n) = \sum_{\substack{P \in \mathscr{P}, k \geq 1 \\ k \deg(P) = n \\ P \nmid B}} \deg(P) , \tag{A.12}$$

de sorte que pour tout caractère χ, $a_\chi(n)$ soit le coefficient d'ordre n dans la dérivée logarithmique de L_χ.

Lemme A.4. *Si $\chi \neq 1$, alors $a_\chi(n) = O(q^{n\alpha})$. De plus, $a_1(n) = q^n + O(1)$*

Démonstration. D'une part, nous savons par le théorème A.5 que les racines de P_χ (pour $\chi \neq 1$) sont toutes de module supérieur à $\frac{1}{q^\alpha}$. Il en résulte que $a_\chi(n) = O(q^{\alpha n})$ pour $\chi \neq 1$.
D'autre part, si nous revenons à la formule (A.6), on voit que :

$$L_1(s) = \prod_{\substack{P \in \mathscr{P} \\ P \mid B}} (1 - q^{-s \deg(P)}) \cdot \frac{1}{1 - q \cdot q^{-s}} .$$

En prenant la dérivée logarithmique par rapport à la variable $z = q^{-s}$, on obtient, par identification, que :

$$a_1(n) = q^n - \sum_{\substack{P \in \mathscr{P} \\ P|B \\ \deg(P)|n}} \deg(P) = q^n + O(1) \ ,$$

comme annoncé. □

Lemme A.5. *Pour tout caractère χ, on a :*

$$a_\chi(n) = n \sum_{\substack{P \in \mathscr{P} \\ \deg(P)=n \\ P \nmid B}} \chi(P) + O(nq^{n/2}) \ .$$

Démonstration. Séparons le cas $k = 1$ du reste dans la somme de la formule (A.11).
On obtient :

$$\left| \sum_{\substack{P \in \mathscr{P}, k \geq 2 \\ k \deg(P)=n \\ P \nmid B}} \deg(P) \cdot \chi(P)^k \right| \leq \sum_{\substack{P \in \mathscr{P}, deg(P) \leq n/2 \\ P \nmid B}} \deg(P) = O(nq^{n/2}) \ ,$$

et :

$$\sum_{\substack{P \in \mathscr{P}, k=1 \\ k \deg(P)=n \\ P \nmid B}} \deg(P) \cdot \chi(P)^k = n \sum_{\substack{P \in \mathscr{P} \\ \deg(P)=n \\ P \nmid B}} \chi(P) \ .$$

D'où le résultat. □

Appliquons finalement la technique mentionnée dans une remarque précédente : on va isoler la congruence à A modulo B grâce à une sorte de « transformée de Fourier » ; plus précisément, on calcule, grace au lemme précédent :

$$\sum_{\chi \in \widehat{G_B}} \chi(A^{-1}) \cdot a_\chi(n) = \sum_{\chi \in \widehat{G_B}} \sum_{\substack{P \in \mathscr{P} \\ \deg(P)=n \\ P \nmid B}} n\chi(A^{-1}P) + O(nq^{n/2}) \ .$$

Par les relations d'orthogonalité, on obtient simplement :

$$\sum_{\chi \in \widehat{G_B}} \chi(A^{-1}) \cdot a_\chi(n) = n|G_B| \cdot \#\left\{P \in \mathscr{P} \,|\, \deg(P) = n, P \equiv A \pmod{B}\right\} \ .$$

En appliquant le lemme A.4, on obtient le théorème suivant, qui implique à son tour le théorème A.1.

Théorème A.6. *On a l'équivalent suivant, pour $n \to \infty$:*

$$\#\left\{P \in \mathscr{P} \,|\, \deg(P) = n, P \equiv A \pmod{B}\right\} \sim \frac{1}{|G_B|}\frac{q^n}{n}\,. \tag{A.13}$$

Remarque A.9. Pour conclure, on peut remarquer que le théorème A.6 admet les interprétations suivantes :

1. L'équivalent obtenu ne dépend pas de A : les pôlynômes premiers se répartissent donc « uniformément » parmi les progressions arithmétiques admissibles de pas B.
2. En sommant sur les progressions arithmétiques admissibles, on obtient que le nombre de pôlynômes premiers de degré n est équivalent à q^n/n : cela constitue une sorte de « théorème des nombres premiers », mais pour les polynômes.

Bibliographie

[1] Keith Conrad. Selmer's example. *(webpage)*.

[2] Jürgen Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999.

[3] Ernst S. Selmer. The Diophantine equation $ax^3 + by^3 + cz^3 = 0$. *Acta Math.*, 85 :203–362 (1 plate), 1951.

[4] Jean-Pierre Serre. *Cours d'arithmétique*. Presses Universitaires de France, Paris, 1977. Le Mathématicien, No. 2.

[5] Henning Stichtenoth. *Algebraic function fields and codes*, volume 254 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, second edition, 2009.