Théorème de Hasse-Minkowski

Tom Burel, Nicolas Doineau, Julien Soumier

April 2021

Projet de Master 1

Motivations

Depuis les Babyloniens qui s'essayèrent à la recherche de solutions d'équations du premier et second degré, l'homme s'interroge sur les possibles résolutions d'équations plus complexes. En particulier dans ce projet nous allons voir comment déterminer si une forme quadratique a des racines rationnelles ou non. L'outil principal mis à disposition est le théorème de Hasse-Minkowski, dont la démonstration est l'objectif de ce travail. Nous détaillerons la construction des notions dont nous aurons besoin afin d'atteindre ce résultat, dans le but de comprendre en profondeur les mathématiques mises en jeu. Une fois la démonstration achevée, il est naturel de se demander dans quelle mesure ce "principe local-global" se généralise-t-il. Nous verrons alors un contre exemple, découvert par Selmer, montrant que le théorème de Hasse-Minkoski ne se généralise pas au degré 3.

Table des matières

Nous avons abondamment utilisé les ressources suivantes : [Ser95] *Cours d'arithmétique*, de J.P Serre, [Con] *Selmer's example* de K. Conrad, et [Col] *Les nombres p-adiques, notes de cours de M2* par P. Colmez. Ce dernier nous a aidé à appréhender les nombres p-adiques dans leur structure. Notre guide pour démontrer le théorème de Hasse-Minkowski fut le livre de Serre, dont nous avons suivi la démarche, tout en développant ce qui nous semblait nécessaire. L'article de Conrad nous a permis de démontrer que l'équation de Selmer est bien un contre-exemple au principe local-global, en passant par des méthodes de théorie algébrique des nombres. Nous nous sommes sérieusement plongés dans l'étude de ces ouvrages, et nous espérons avoir su en restituer les idées principales avec clarté. Nous avons également utilisé diverses feuilles de travaux dirigés pour démontrer des résultats en annexe. Pour finir nous avons utilisé certaines définitions issues de [Bou70] *Éléments de mathématiques, Théorie des ensembles* de Bourbaki, et nous renvoyons à [Sam71] *Théorie algébrique des nombres* de Pierre Samuel pour les résultats de théorie algébrique des nombres non démontrés en annexe.

1 Nombres p-adiques

Dans le cadre de ce projet nous allons voir un exemple de réalisation du principe local-global, le théorème de Hasse-Minkowski. Pour ce faire nous allons introduire de nombreux outils mathématiques, et ici le plus important : les nombres p-adiques.

1.1 Constructions équivalentes

1.1.1 Approche topologique : comme complété de $\mathbb{Q}$

Le théorème de Hasse-Minkowski est un énoncé qui porte notamment sur les *corps p-adiques* $\mathbb{Q}_p$ pour p premier, qu'il faut donc commencer par étudier. Nous en donnerons deux constructions, chacune intéressante et apportant des propriétés fondamentales pour la suite. La première consiste à compléter $\mathbb{Q}$ pour une norme différente de la valeur absolue usuelle.

Dans un premier temps on fixe un corps $\mathbb{K}$.

Définition 1.1. *Une norme de corps sur $\mathbb{K}$ est une application $|\cdot| : \mathbb{K} \to \mathbb{R}_+$ vérifiant les trois propriétés suivantes, où x et y sont dans $\mathbb{K}$:*

(i) *séparation :* $|x| = 0 \Leftrightarrow x = 0$

(ii) *multiplicativité :* $|xy| = |x||y|$

(iii) *inégalité triangulaire :* $|x + y| \leq |x| + |y|$.

Une telle norme de corps $|\cdot|$ munit $\mathbb{K}$ d'une structure de $\mathbb{K}$-espace vectoriel normé. On peut ainsi parler de l'anneau des suites de Cauchy sur $\mathbb{K}$, que l'on note $\mathcal{C}_\mathbb{K}$. L'ensemble $Z_\mathbb{K}$ des suites de Cauchy qui tendent vers 0 en est un idéal.

Définition 1.2. *On appelle complété de $\mathbb{K}$ pour $|\cdot|$ le quotient $\mathbb{K}_c = \mathcal{C}_\mathbb{K}/Z_\mathbb{K}$.*

Cette terminologie est justifiée par le théorème suivant. On ne le montrera pas ici car il s'agit d'un résultat classique de topologie, qui n'est de plus pas central dans notre étude. La preuve peut cependant être retrouvée dans [Col] (pp5-6).

Théorème 1.1. *$\mathbb{K}_c$ est un corps qui est une extension de $\mathbb{K}$ telle que :*

- *$|\cdot|$ se prolonge en une norme de corps sur $\mathbb{K}_c$*
- *$\mathbb{K}$ est dense dans $\mathbb{K}_c$*
- *$\mathbb{K}_c$ est complet pour la norme prolongée $|\cdot|$.*

On peut maintenant passer à notre cas particulier. On note dans la suite $\mathbf{P}$ l'ensemble des nombres premiers. Fixons un $p \in \mathbf{P}$. On note $v_p(a) \in \mathbb{N} \cup \{+\infty\}$ la p-valuation d'un entier $a \in \mathbb{Z}$, en convenant que $v_p(0) = +\infty$.

Définition 1.3. *Si $\frac{a}{b}$ est un rationnel (avec $a \in \mathbb{Z}$ et $b \in \mathbb{Z} \setminus \{0\}$), on définit sa valuation p-adique par $v_p(\frac{a}{b}) = v_p(a) - v_p(b)$.*

La valuation p-adique sur $\mathbb{Q}$ prolonge celle sur $\mathbb{Z}$. Elle est bien définie car pour c, d des entiers on a $v_p(cd) = v_p(c) + v_p(d)$. De plus pour $x \in \mathbb{Q}$, $v_p(x) \in \mathbb{Z} \cup \{+\infty\}$.

Définition 1.4. *On définit la norme p-adique* $|\cdot|_p$ *par* $|x|_p = p^{-v_p(x)}$ *pour* $x \in \mathbb{Q}$.

Proposition 1.1. $|\cdot|_p$ *est une norme de corps sur* $\mathbb{Q}$. *Elle vérifie de plus l'inégalité ultramétrique : pour* $x, y \in \mathbb{Q}$, $|x+y|_p \leq \max(|x|_p, |y|_p)$.

Démonstration. La séparation et la multiplicativité sont évidentes, et l'inégalité triangulaire découle de l'inégalité ultramétrique, que l'on montre. Soit a, b, c, d dans $\mathbb{Z} \setminus \{0\}$. Quitte à échanger on suppose que $\left|\frac{a}{b}\right|_p \geq \left|\frac{c}{d}\right|_p$: montrons que $\left|\frac{a}{b} + \frac{c}{d}\right|_p \leq \left|\frac{a}{b}\right|_p$. On a $\left|\frac{a}{b} + \frac{c}{d}\right|_p = p^{v_p(bd)-v_p(ad+bc)}$, or $\left|\frac{a}{b}\right|_p \geq \left|\frac{c}{d}\right|_p$ se réécrit $p^{v_p(b)-v_p(a)} \geq p^{v_p(d)-v_p(c)}$, puis $v_p(bc) \geq v_p(ad)$. Ainsi $v_p(ad+bc) \geq \min(v_p(ad), v_p(bc)) = v_p(ad)$, et $\left|\frac{a}{b} + \frac{c}{d}\right|_p \leq p^{v_p(bd)-v_p(ad)} = \left|\frac{ad}{bd}\right|_p = \left|\frac{a}{b}\right|_p$. □

Donnons alors une première définition des corps p-adiques.

Définition 1.5. *On appelle corps p-adique et on note* $\mathbb{Q}_p$ *le complété de* $\mathbb{Q}$ *pour la norme* $|\cdot|_p$.

La norme prolongée $|\cdot|_p$ est encore ultramétrique.

Il est connu qu'en choisissant plutôt comme norme de corps sur $\mathbb{Q}$ la valeur absolue classique, le même procédé donne pour complété le corps $\mathbb{R}$. En fait, le théorème suivant montre que les seuls complétés de $\mathbb{Q}$ sont d'une part les $\mathbb{Q}_p$ pour $p \in \mathbf{P}$, et d'autre part $\mathbb{R}$.

Théorème 1.2 (Ostrowski)**.** *Toute norme de corps sur* $\mathbb{Q}$ *est soit équivalente à une* $|\cdot|_p$ *pour un* $p \in \mathbf{P}$, *soit équivalente à la valeur absolue.*

Comme pour le théorème précédent on ne donne pas la démonstration ici, mais elle est faite dans [Col] (p4).

Revenons plus particulièrement à notre complété $\mathbb{Q}_p$. Vu que la norme se prolonge de $\mathbb{Q}$ à $\mathbb{Q}_p$, c'est aussi la cas de la valuation, par la formule naturelle $v_p(x) = -\log_p |x|_p \in \mathbb{R} \cup \{+\infty\}$. Les propriétés suivantes sont toujours vraies pour $x, y \in \mathbb{Q}_p$:

(i) $v_p(x) = +\infty \Leftrightarrow x = 0$

(ii) $v_p(xy) = v_p(x) + v_p(y)$

(iii) $v_p(x+y) \geq \min(v_p(x), v_p(y))$.

Comme la topologie de $\mathbb{Q}$ est définie par $|\cdot|_p$ (et que $-\log_p : \mathbb{R}_+ \to \mathbb{R} \cup \{+\infty\}$ est continue), v_p est une application continue.

Définition 1.6. *On appelle entier de* $\mathbb{Q}_p$ *un élément* x *tel que* $v_p(x) \geq 0$, *autrement dit tel que* $|x|_p \leq 1$. *On note* $\mathbb{Z}_p$ *l'ensemble des entiers de* $\mathbb{Q}_p$ *; c'est un sous-anneau de* $\mathbb{Q}_p$.

Remarquons que $\mathbb{Q}_p$ est le corps des fractions de $\mathbb{Z}_p$ (car si $x \in \mathbb{Q}_p^*$, x ou x^{-1} est dans $\mathbb{Z}_p$), et que $\mathbb{Z}_p$ est fermé dans $\mathbb{Q}_p$.

Proposition 1.2. *Pour* $n \geq 1$ *on a l'isomorphisme d'anneaux suivants :* $\mathbb{Z}_p/p^n\mathbb{Z}_p \simeq \mathbb{Z}/p^n\mathbb{Z}$.

Démonstration. Si $p^n | x$ dans $\mathbb{Z}_p$ avec $x \in \mathbb{Z}$ alors $p^n | x$ dans $\mathbb{Z}$. Cela permet de définir l'injection canonique $\varphi : \mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}_p/p^n\mathbb{Z}_p$. Montrons qu'elle est surjective.

Soit $\overline{y} \in \mathbb{Z}_p/p^n\mathbb{Z}_p$; on en prend un relèvement $y \in \mathbb{Z}_p$. Par densité de $\mathbb{Q}$ dans $\mathbb{Q}_p$, soit $r \in \mathbb{Q}$ tel que $v_p(y-r) \geq n$. Il vient $r = y - (y-r) \in \mathbb{Z}_p$, c'est-à-dire $v_p(r) \geq 0$. Alors, en écrivant $r = \frac{a}{b}$ avec a, b des entiers premiers entre eux, on a $p \nmid b$. Soit $c \in \mathbb{Z}$ tel que dans $\mathbb{Z}_p/p^n\mathbb{Z}_p$, $\overline{bc} = 1$: on va vérifier que $\varphi(\overline{ac}) = \overline{y}$.

$v_p(y-ac) \geq min(v_p(y-r), v_p(r-ac))$: d'une part $v_p(y-r) \geq n$; d'autre part $v_p(r-ac) = v_p(r) + v_p(1-bc) \geq 0 + n = n$. Ainsi $v_p(y-ac) \geq n$, autrement dit $\overline{y} = \overline{ac}$ dans $\mathbb{Z}_p/p^n\mathbb{Z}_p$, et $\overline{y} = \varphi(\overline{ac})$. □

1.1.2 Approche algébrique : comme limite projective

Il existe une autre façon de construire $\mathbb{Z}_p$ et donc $\mathbb{Q}_p$, qui est tout à fait différente : elle est entièrement algébrique et mobilise la notion de *limite projective*. Nombre de propriétés algébriques vont découler de cette seconde construction, et nous servir par la suite.

Définition 1.7. *Considérons $(I, \leq)$ est un ensemble ordonné et $(E_i)_{i\in I}$ une famille d'ensembles indexée par I. On suppose aussi que pour $i \leq j$ dans I il existe une application $f_i^j : E_j \to E_i$, de sorte que :*

- *pour tout $i \in I$, $f_i^i = \mathrm{Id}_{E_i}$*
- *pour $i \leq j \leq k$ dans I, $f_i^k = f_i^j \circ f_j^k$.*

On dit alors que le couple $\left((E_i)_{i\in I}, (f_i^j)_{i\leq j}\right)$ est un système projectif. De plus, on appelle limite projective du système et on note $\varprojlim E_i$ l'ensemble :

$$\left\{ x \in \prod_{i\in I} E_i \;\middle|\; \forall i \leq j, f_i^j(x_j) = x_i \right\}.$$

Pour un système projectif, le diagramme suivant, avec $i \leq j \leq k$, est donc commutatif.

$$\begin{array}{ccccccc} \cdots & \longleftarrow & E_i & \xleftarrow{f_i^k} & E_k & \longleftarrow & \cdots \\ & & & {\scriptstyle f_i^j}\nwarrow \quad \swarrow{\scriptstyle f_j^k} & & & \\ & & & E_j & & & \end{array}$$

Un certain nombre de structures algébriques passent à la limite projective : les cas des groupes abéliens et des anneaux nous seront utiles. Si $\left((E_i)_{i\in I}, (f_i^j)_{i\leq j}\right)$ est un système projectif tel que tous les E_i sont munis de l'une de ces deux structures (la même évidemment) et tel que pour tout $i \leq j \in I$, f_i^j est un morphisme, alors $\varprojlim E_i$ est naturellement muni de la même structure. Voyons deux propositions liées à cela.

Proposition 1.3. *Soient $\left((E_i)_{i\in I}, (f_i^j)_{i\leq j}\right)$ et $\left((F_i)_{i\in I}, (g_i^j)_{i\leq j}\right)$ deux systèmes projectifs de groupes abéliens ou d'anneaux, indexés par le même I. On suppose que pour tout $i \in I$ il existe un isomorphisme $\phi_i : E_i \to F_i$ qui vérifie pour tout $i \leq j \in I$: $\phi_i \circ f_i^j = g_i^j \circ \phi_j$ (voir diagramme commutatif ci-dessous). Alors $\varprojlim E_i \simeq \varprojlim F_i$.*

$$\begin{array}{ccc} E_i & \xleftarrow{f_i^j} & E_j \\ {\scriptstyle \phi_i}\downarrow & & \downarrow{\scriptstyle \phi_j} \\ F_i & \xleftarrow[g_i^j]{} & F_j \end{array}$$

Démonstration. On définit $\Phi : \left\{ \begin{array}{ccc} \varprojlim E_i & \to & \varprojlim F_i \\ x & \mapsto & (\phi_i(x_i))_{i\in I} \end{array} \right.$. Montrons que Φ est bien définie et surjective en utilisant le diagramme. Soit $i \leq j$. Si $x \in \varprojlim E_i$: $g_i^j(\phi_j(x_j)) = \phi_i(f_i^j(x_j)) = \phi_i(x_i)$, et $\phi(x) \in \varprojlim F_i$. Si $y \in \varprojlim F_i$ on pose $x = (\phi_i^{-1}(y_i))_{i\in I}$: $f_i^j(x_j) = f_i^j(\phi_j^{-1}(y_j)) = \phi_i^{-1}(g_i^j(y_j)) = \phi_i^{-1}(y_i) = x_i$, et $y = \Phi(x)$. On obtient de plus sans difficulté que Φ est un morphisme injectif. □

Proposition 1.4. *Soient $\left((E_i)_{i\in I}, (f_i^j)_{i\leq j}\right)$ et $\left((F_i)_{i\in I}, (g_i^j)_{i\leq j}\right)$ deux systèmes projectifs de groupes abéliens ou d'anneaux, indexés par le même I. Alors $\left((E_i \times F_i)_{i\in I}, \left((f_i^j, g_i^j)\right)_{i\leq j}\right)$ est un système projectif, et on a l'isomorphisme $\varprojlim(E_i \times F_i) \simeq \varprojlim E_i \times \varprojlim F_i$.*

Démonstration. On définit $\Psi : \left\{ \begin{array}{ccc} \varprojlim(E_i \times F_i) & \to & \varprojlim E_i \times \varprojlim F_i \\ \big((x_i, y_i)\big)_{i\in I} & \mapsto & \big((x_i)_{i\in I}, (y_i)_{i\in I}\big) \end{array} \right.$. On voit facilement que Ψ est bien définie, surjective, et un morphisme injectif. □

Définition 1.8. *Pour $n \geq 1$ on note $A_n = \mathbb{Z}/p^n\mathbb{Z}$, et pour $1 \leq m \leq n$ on définit le morphisme d'anneaux :*

$$f_m^n : \left\{ \begin{array}{ccc} A_n & \to & A_m \\ x\ [p^n] & \mapsto & x\ [p^m] \end{array} \right. .$$

$((A_n)_{n\geq 1}, (f_m^n)_{m\leq n})$ est alors un système projectif, dont on note la limite projective $\mathbb{Z}'_p$.

Étant donné que les A_n sont des anneaux et les f_m^n des morphismes d'anneaux, on voit que $\mathbb{Z}'_p$ est naturellement muni d'une structure d'anneau. Le but va bien sûr être d'obtenir un isomorphisme $\mathbb{Z}_p \simeq \mathbb{Z}'_p$, ce qui montrera que $\mathbb{Q}_p$ peut aussi être vu comme le corps des fractions de la limite projective $\mathbb{Z}'_p$ ci-dessus.

Avant cela, intéressons nous quelques instants aux deux morphismes suivants, pour $n \geq 1$:

$$\mu_n : \left\{ \begin{array}{ccc} \mathbb{Z}'_p & \to & \mathbb{Z}'_p \\ x & \mapsto & p^n x \end{array} \right. \quad \text{et} \quad \pi_n : \left\{ \begin{array}{ccc} \mathbb{Z}'_p & \to & A_n \\ x & \mapsto & x_n \end{array} \right. .$$

Proposition 1.5. *Pour $n \geq 1$ la suite $0 \to \mathbb{Z}'_p \xrightarrow{\mu_n} \mathbb{Z}'_p \xrightarrow{\pi_n} A_n \to 0$ est exacte. En particulier, $\mathbb{Z}'_p/p^n\mathbb{Z}'_p \simeq A_n$.*

Démonstration. Cette proposition se décompose en trois affirmations : μ_n est injective ; $\mathrm{Im}(\mu_n) = \mathrm{Ker}(\pi_n)$; π_n est surjective. La dernière est triviale : on montre les deux premières.

Pour le premier point, $\mu_n = \mu_1^n$ donc il suffit de montrer que μ_1 est injective. Soit $x \in \mathrm{Ker}(\mu_1)$: $px = 0$. Soit $m \geq 1$: dans A_{m+1}, $px_{m+1} = 0$, donc $x_{m+1} = p^m y$ avec $y \in A_{m+1}$. Alors dans A_m : $x_m = f_m^{m+1}(x_{m+1}) = p^m f_m^{m+1}(y) = 0$. Ainsi $x = 0$, ce qui montre l'injectivité de μ_1.

Montrons maintenant que $\mathrm{Im}(\mu_n) = \mathrm{Ker}(\pi_n)$. Pour l'inclusion directe, avec $x \in \mathbb{Z}'_p$ on a $\pi_n(p^n x) = p^n \pi_n(x) = 0$ dans A_n.

Pour l'inclusion réciproque, soit $x \in \mathrm{Ker}(\pi_n)$. Soit $m \geq 1$. Dans A_{m+n}, $x_{m+n} \equiv 0\ [p^n]$, et on peut prendre $z_{m+n} \in A_{m+n}$ tel que $x_{m+n} = p^n z_{m+n}$. On pose ensuite $y_m = f_m^{m+n}(z_{m+n}) \in A_m$. Alors $p^n y_m = f_m^{m+n}(p^n z_{m+n}) = f_m^{m+n}(x_{m+n}) = x_m$. On a ainsi $x = p^n y$; il ne reste qu'à vérifier que $y \in \mathbb{Z}'_p$. Soient $1 \leq m \leq m'$: dans A_{m+n}, $f_{m+n}^{m'+n}(x_{m'+n}) = x_{m+n}$. En utilisant la commutativité du diagramme

$$\begin{array}{ccc} A_{m'} & \xleftarrow{f_{m'}^{m'+n}} & A_{m'+n} \\ {\scriptstyle f_m^{m'}}\downarrow & & \downarrow{\scriptstyle f_{m+n}^{m'+n}} \\ A_m & \xleftarrow[f_m^{m+n}]{} & A_{m+n} \end{array}$$

on écrit une suite de congruences :

$$\begin{array}{rll} f_{m+n}^{m'+n}(x_{m'+n}) \equiv x_{m+n}\ [p^{m+n}] & & \text{dans } A_{m+n} \\ p^n f_{m+n}^{m'+n}(z_{m'+n}) \equiv p^n z_{m+n}\ [p^{m+n}] & & \\ f_{m+n}^{m'+n}(z_{m'+n}) \equiv z_{m+n}\ [p^m] & & \\ f_m^{m'+n}(z_{m'+n}) \equiv f_m^{m+n}(z_{m+n})\ [p^m] & & \text{dans } A_m \\ f_m^{m'}(y_{m'}) \equiv y_m\ [p^m]. & & \end{array}$$

On a obtenu $f_m^{m'}(y_{m'}) = y_m$ dans A_m, ce qui montre bien que $y \in \mathbb{Z}'_p$. Donc $x \in \mathrm{Im}(\mu_n)$.

□

L'isomorphisme de cette proposition peut aussi être obtenu en combinant la proposition 1.2 et le théorème suivant, mais il est tout de même intéressant d'avoir fait la preuve directe.

Théorème 1.3. *Les deux constructions sont équivalentes :* $\mathbb{Z}_p \simeq \mathbb{Z}'_p$.

Démonstration. On va montrer que $\mathbb{Z}_p \simeq \varprojlim(\mathbb{Z}_p/p^n\mathbb{Z}_p)$. En effet vu que l'isomorphisme passe à la limite projective, la proposition 1.2 nous donnera $\mathbb{Z}_p \simeq \varprojlim A_n = \mathbb{Z}'_p$. On considère le morphisme d'anneaux

$$\psi : \begin{cases} \mathbb{Z}_p & \to & \varprojlim(\mathbb{Z}_p/p^n\mathbb{Z}_p) \\ x & \mapsto & (x\ [p^n])_{n\geq 1} \end{cases} \text{ : montrons que c'est un isomorphisme.}$$

Injectivité : soit $x \in \mathrm{Ker}(\psi)$. Pour tout $n \geq 1$, $v_p(x) \geq n$. Alors $v_p(x) = +\infty$ et $x = 0$.

Surjectivité : soit $y \in \varprojlim(\mathbb{Z}_p/p^n\mathbb{Z}_p)$. Pour $n \geq 1$ on choisit un relèvement $z_n \in \mathbb{Z}_p$ de y_n. Alors pour $n \geq 1$ et $k \geq 0$: $z_{n+k} - z_n \equiv y_{n+k} - y_n \equiv 0\ [p^n]$. Cela signifie que $v_p(z_{n+k} - z_n) \geq n$, et que z est une suite de Cauchy. Par complétude de $\mathbb{Q}_p$ on peut considérer sa limite x, qui se trouve dans $\mathbb{Z}_p$ par fermeture. Un passage à la limite (en k) donne $v_p(x - z_n) \geq n$, ce qui se réécrit $x \equiv z_n\ [p^n]$. Ceci montre que $\psi(x) = y$. □

À partir de maintenant on identifie $\mathbb{Z}_p$ et $\mathbb{Z}'_p$ (et donc de même pour $\mathbb{Q}_p$ et le corps des fractions $\mathbb{Q}'_p$ de $\mathbb{Z}'_p$).

1.2 Propriétés importantes

1.2.1 Unités p-adiques

Définition 1.9. *On appelle unité p-adique un entier p-adique inversible dans* $\mathbb{Z}_p$. *On note* $\mathbf{U} = \mathbb{Z}_p^*$ *le groupe des unités p-adiques.*

Proposition 1.6. *Pour* $x \in \mathbb{Z}_p$ *:* $x \in \mathbf{U} \Leftrightarrow p \nmid x$.

Démonstration. Si $x \in \mathbf{U}$, dans A_1 on a $x_1(x^{-1})_1 = 1$, d'où $p \nmid x_1$. Alors $p \nmid x$ dans $\mathbb{Z}_p$.

Réciproquement si $p \nmid x$, x_n est inversible dans A_n pour tout $n \geq 1$. On pose $y = (x_n^{-1})_{n\geq 1} \in \prod_{n\geq 1} A_n$, de sorte que $xy = 1$. Il reste à montrer que $y \in \mathbb{Z}_p$. Soient $1 \leq m \leq n$: $x_m f_m^n(x_n^{-1}) = f_m^n(x_n) f_m^n(x_n^{-1}) = f_m^n(1) = 1$. Donc $f_m^n(x_n^{-1}) = x_m^{-1}$: c'est ce que l'on voulait. □

On peut donc écrire : $\mathbf{U} = \{x \in \mathbb{Q}_p \mid v_p(x) = 0\}$. En particulier $\mathbf{U}$ est fermé dans $\mathbb{Q}_p$.

On avait vu que la valuation p-adique se prolongeait à $\mathbb{Q}_p$, avec pour $x \in \mathbb{Q}_p^*$, $v_p(x) \in \mathbb{R}$. En fait on peut déduire de ce qui précède et des propriétés de v_p le théorème suivant.

Théorème 1.4. *Soit* $x \in \mathbb{Q}_p^*$. $v_p(x) \in \mathbb{Z}$, *et on peut écrire* $x = up^{v_p(x)}$ *avec un* $u \in \mathbf{U}$ *(qui est unique).*

Démonstration. Dans un premier temps, prenons $x \in \mathbb{Z}_p \setminus \{0\}$. Soit $m = \min\left\{n \in \mathbb{N} \,\middle|\, x_{n+1} \neq 0\right\}$. Si $m = 0$, $p \nmid x$ donc $x \in \mathbf{U}$. Sinon, $x \in \mathrm{Ker}(\pi_m) \setminus \mathrm{Ker}(\pi_{m+1}) = p^m\mathbb{Z}_p \setminus p^{m+1}\mathbb{Z}_p$. Ainsi $x = p^m y$ avec $p \nmid y$, c'est-à-dire $y \in \mathbf{U}$.

Soit maintenant $u \in \mathbf{U}$: $v_p(u) + v_p(u^{-1}) = v_p(1) = 0$, or les deux sont positives : on en déduit que $v_p(u) = 0$. Alors si on considère $x \in \mathbb{Z}_p \setminus \{0\}$ et que par ce qui précède on l'écrit $x = up^n$ avec $u \in \mathbf{U}$ et $n \in \mathbb{N}$, on obtient $v_p(x) = v_p(p^n) = n$. Enfin soit $x \in \mathbb{Q}_p^*$: $x = \frac{y}{z}$ avec y et z des entiers p-adiques non nuls que l'on peut écrire respectivement $up^{v_p(y)}$ et $vp^{v_p(z)}$. Alors $x = uv^{-1}p^{v_p(y)-v_p(z)} = uv^{-1}p^{v_p(x)}$. □

Ce théorème suggère que la structure du groupe $\mathbb{Q}_p^*$ peut se déduire de celle de $\mathbf{U}$. Avoir une bonne connaissance de $\mathbb{Q}_p^*$ nous sera utile plus tard, notamment pour travailler avec ses carrés. Nous allons donc maintenant étudier finement la structure du groupe des unités $\mathbf{U}$.

Définition 1.10. *Soit $n \geq 1$. On définit $\mathbf{U}_n = 1 + p^n\mathbb{Z}_p$: il s'agit d'un sous-groupe de $\mathbf{U}$.*

La suite $(\mathbf{U}_n)_{n\geq 1}$ est décroissante pour l'inclusion. Le fait qui suit va être utile pour se ramener à des groupes finis dans les preuves.

Proposition 1.7. *Si pour $1 \leq m \leq n$ on pose $g_m^n : \left\{ \begin{array}{ccc} \mathbf{U}/\mathbf{U}_n & \to & \mathbf{U}/\mathbf{U}_m \\ u\mathbf{U}_n & \mapsto & u\mathbf{U}_m \end{array} \right.$, alors $((\mathbf{U}/\mathbf{U}_n)_{n\geq 1}, (g_m^n)_{m\leq n})$ est un système projectif et $\mathbf{U} \simeq \varprojlim \mathbf{U}/\mathbf{U}_n$.*

En fait de la même manière, si l'on fixe $m \geq 1$ on a $\mathbf{U}_m \simeq \varprojlim \mathbf{U}_m/\mathbf{U}_n$ (où les limite projectives sont indexées par $n \geq m+1$).

Démonstration. Le système est projectif car les g_m^n sont simplement les réductions successives modulo les $\mathbf{U}_m$ (multipicativement). Montrons que le morphisme suivant est un isomorphisme :

$$\psi : \left\{ \begin{array}{ccc} \mathbf{U} & \to & \varprojlim \mathbf{U}/\mathbf{U}_n \\ u & \mapsto & (u\mathbf{U}_n)_{n\geq 1} \end{array} \right. .$$

On fait le même raisonnement que dans la preuve du théorème 1.3. Soit $u \in \mathrm{Ker}(\psi)$: pour tout $n \geq 1$, $u \in \mathbf{U}_n$, c'est-à-dire $p^n | u-1$. Alors $u - 1 = 0$ et $u = 1$. Soit $(u_n\mathbf{U}_n)_{n\geq 1} \in \varprojlim \mathbf{U}/\mathbf{U}_n$. Soient $n \geq 1$ et $k \geq 0$: $u_{n+k} \in u_n\mathbf{U}_n$ donc on peut écrire $u_{n+k} = u_n(1+p^n x)$ avec $x \in \mathbb{Z}_p$. Alors $u_{n+k} - u_n = p^n u_n x$ et $v_p(u_{n+k} - u_n) \geq n$: $u \in \mathbf{U}^{\mathbb{N}^*}$ est une suite de Cauchy. Par complétude de $\mathbb{Q}_p$ soit u_∞ sa limite ; elle est dans $\mathbf{U}$ car c'est un fermé de $\mathbb{Q}_p$. Par passage à la limite en k, pour $n \geq 1$ on a $v_p(u_\infty - u_n) \geq n$. Soit alors $y \in \mathbb{Z}_p$ tel que $u_\infty - u_n = p^n y$: $u_\infty = u_n(1 + p^n u_n^{-1} y) \in u_n\mathbf{U}_n$, c'est-à-dire $u_\infty \mathbf{U}_n = u_n\mathbf{U}_n$. Donc $(u_n\mathbf{U}_n)_{n\geq 1} = \psi(u_\infty)$. □

Proposition 1.8. *On a l'isomorphisme $\mathbf{U}/\mathbf{U}_1 \simeq \mathbb{F}_p^*$. De plus pour $n \geq 1$, le quotient $\mathbf{U}_1/\mathbf{U}_n$ est d'ordre p^{n-1}.*

Démonstration. On a parlé plus tôt du morphisme d'anneaux $\pi_1 : \mathbb{Z}_p \to A_1 = \mathbb{F}_p$: en passant au groupe des inversibles on obtient un morphisme de groupes surjectif $\mathbf{U} \to \mathbb{F}_p^*$. On voit alors facilement que le noyau de ce morphisme est $\mathbf{U}_1$. Le théorème de factorisation donne le premier résultat.

Pour le second on définit l'application $\phi : \left\{ \begin{array}{ccc} \mathbf{U}_n & \to & \mathbb{Z}/p\mathbb{Z} \\ 1+p^n x & \mapsto & \overline{x} \end{array} \right.$ où $\bar{\cdot}$ désigne la réduction modulo p. Comme $\mathbb{Z}_p/p^n\mathbb{Z}_p \simeq \mathbb{Z}/p\mathbb{Z}$, ϕ est bien définie et surjective. Soit $x, y \in \mathbb{Z}_p$: $(1+p^n x)(1+p^n y) = 1 + p^n(x + y + p^n xy)$ donc $\phi\left((1+p^n x)(1+p^n y)\right) = \overline{x+y+p^n xy} = \overline{x} + \overline{y} = \phi(1+p^n x) + \phi(1+p^n y)$: ϕ est un morphisme de groupes. De plus il est clair que $\mathrm{Ker}(\phi) = \mathbf{U}_{n+1}$: le théorème de factorisation fournit cette fois l'isomorphisme $\mathbf{U}_n/\mathbf{U}_{n+1} \simeq \mathbb{Z}/p\mathbb{Z}$. En particulier $\mathbf{U}_n/\mathbf{U}_{n+1}$ est d'ordre p ; le résultat s'en déduit par récurrence. □

Lemme 1.1. *Soit $0 \to A \overset{\subseteq}{\to} E \overset{g}{\to} B \to 0$ une suite exacte de groupes abéliens finis (notés additivement). On fait l'hypothèse que les ordres de A et B sont premiers entre eux. Alors : $E \simeq A \times B$.*

Démonstration. On note a et b les ordres respectifs de A et B. Soit $B' = \{x \in E \mid bx = 0\}$. On va montrer que $E = A \oplus B'$, puis que $B' \simeq B$.

Pour le premier point il suffit de montrer que $A \cap B' = 0$ et $A + B' = E$. Par hypothèse soit une relation de Bézout entre a et b : $ar + bs = 1$. Soit $x \in A \cap B'$: $x = (ar+bs)x = arx + bsx = 0$ (car aA et bB' sont nuls). Soit $x \in E$: on réécrit $x = arx + bsx$. D'abord, $g(bE) = bB = 0$ donc $bE \subset \mathrm{Ker}(g) = A$, et $bsx \in A$. Ensuite, E est d'ordre ab, donc $abrx = 0$: $arx \in B'$. D'où $x \in A + B'$.

Comme $\mathrm{Ker}(g) = A$, g induit un isomorphisme de B' sur B. Cela conclut. □

Proposition 1.9. *On peut décomposer* $\mathbf{U}$ *selon l'isomorphisme suivant :* $\mathbf{U} \simeq \mathbf{U}_1 \times \mathbb{F}_p^*$.

Démonstration. Soit $n \geq 1$: $(\mathbf{U}/\mathbf{U}_n)/(\mathbf{U}_1/\mathbf{U}_n) \simeq \mathbf{U}/\mathbf{U}_1 \simeq \mathbb{F}_p^*$ donc on peut considérer la suite exacte $1 \to \mathbf{U}_1/\mathbf{U}_n \to \mathbf{U}/\mathbf{U}_n \to \mathbb{F}_p^* \to 1$. $\mathbf{U}_1/\mathbf{U}_n$ est d'ordre p^{n-1}, $\mathbb{F}_p^*$ est d'ordre $p-1$: on peut appliquer le lemme, qui donne $\mathbf{U}/\mathbf{U}_n \simeq \mathbf{U}_1/\mathbf{U}_n \times \mathbb{F}_p^*$.

On va maintenant passer à la limite projective, en indexant par $n \geq 1$. On a vu (proposition 1.7) que $\mathbf{U} \simeq \varprojlim \mathbf{U}/\mathbf{U}_n$. En incluant $n = 1$ dans la limite projective (plutôt que $n \geq 2$), vu que $\mathbf{U}_1/\mathbf{U}_1$ est trivial on peut encore écrire $\mathbf{U}_1 \simeq \varprojlim \mathbf{U}_1/\mathbf{U}_n$. Ensuite on considère la suite constante $(\mathbb{F}_p^*)_{n\geq 1}$, qui forme un système projectif (que l'on peut qualifier de trivial) quand on la munit de l'identité. On a bien sûr $\varprojlim \mathbb{F}_p^* \simeq \mathbb{F}_p^*$. Il ne reste qu'à appliquer les propositions 1.3 (le diagramme requis est bien commutatif) et 1.4 sur les limites projectives pour obtenir $\mathbf{U} \simeq \mathbf{U}_1 \times \mathbb{F}_p^*$. □

L'enjeu est ensuite de raffiner en explicitant la structure de $\mathbf{U}_1$. Pour cela voici d'abord un lemme.

Lemme 1.2. *Soit* $n \geq 1$ *si* $p \neq 2$, *ou* $n \geq 2$ *si* $p = 2$. *Si* $x \in \mathbf{U}_n \setminus \mathbf{U}_{n+1}$ *alors* $x^p \in \mathbf{U}_{n+1} \setminus \mathbf{U}_{n+2}$.

Démonstration. Par hypothèse on écrit $x = 1 + p^n k$ avec $k \in \mathbb{Z}_p$, $p \nmid k$. Alors $x^p = \sum_{i=0}^{p} \binom{p}{i} p^{in} k^i$. Pour $2 \leq i \leq p-1$, $v_p\left(\binom{p}{i} p^{in}\right) \geq 1 + in \geq 2n + 1 \geq n + 2$. De plus (puisque l'on a pris $n \geq 2$ si $p = 2$) $pn \geq n + 2$. Donc $x^p \equiv 1 + p^{n+1}k \ [p^{n+2}]$: comme $p \nmid k$, cela conclut. □

On note que le lemme distingue les cas p impair et pair. Il s'agit de l'une des raisons pour lesquelles les deux cas devront être distingués dans de nombreux théorèmes à venir, à commencer par le suivant.

Théorème 1.5 (Structure du groupe $\mathbf{U}_1$)**.** *On distingue les cas* p *impair et pair.*

- *Si* $p \neq 2$ *:* $\mathbf{U}_1 \simeq \mathbb{Z}_p$.
- *Si* $p = 2$ *:* $\mathbf{U}_1 \simeq \mathbb{Z}_2 \times \mathbb{Z}/2\mathbb{Z}$.

Démonstration. On traite d'abord le cas $p \neq 2$. Soit $\alpha = 1 + p$: $\alpha \in \mathbf{U}_1 \setminus \mathbf{U}_2$, donc le lemme implique que pour tout $m \in \mathbb{N}$, $\alpha^{p^m} \in \mathbf{U}_{m+1} \setminus \mathbf{U}_{m+2}$. Soit $n \geq 2$: on note $\alpha_n = \alpha \mathbf{U}_n$ l'image de α dans $\mathbf{U}_1/\mathbf{U}_n$. Alors $\alpha_n^{p^{n-2}} \neq 1$ et $\alpha_n^{p^{n-1}} = 1$. Mais $\mathbf{U}_1/\mathbf{U}_n$ est d'ordre p^{n-1} : cela signifie qu'il est cyclique, autrement dit on a l'isomorphisme $\mathbf{U}_1/\mathbf{U}_n \simeq A_{n-1}$. Le résultat s'en déduit en passant à la limite projective (indexée par $n \geq 2$) par la proposition 1.3 (le diagramme de la proposition est ici bien commutatif).

Passons au cas $p = 2$. Cette fois on pose $\alpha = 5$: $\alpha \in \mathbf{U}_2 \setminus \mathbf{U}_3$. De manière analogue au premier cas on obtient pour $n \geq 3$ un isomorphisme $\mathbf{U}_2/\mathbf{U}_n \simeq A_{n-2}$; là aussi on passe à la limite projective (indexée par $n \geq 3$) pour obtenir $\mathbf{U}_2 \simeq \mathbb{Z}_2$. Reste à voir que $\mathbf{U}_1 \simeq \mathbf{U}_2 \times \mathbb{Z}/2\mathbb{Z}$.

D'après la preuve de la proposition 1.8, $\mathbf{U}_1/\mathbf{U}_2 \simeq \mathbb{Z}/2\mathbb{Z}$: on considère la suite exacte $1 \to \mathbf{U}_2 \to \mathbf{U}_1 \to \mathbb{Z}/2\mathbb{Z} \to 0$. Soit $u \in \mathbf{U}_1 \setminus \mathbf{U}_2$: on pose $s(1) = u$; on pose aussi $s(0) = 1$. Alors $s : \mathbb{Z}/2\mathbb{Z} \to \mathbf{U}_1$ est une section de la suite exacte, ce qui entraîne que $\mathbf{U}_1 \simeq \mathbf{U}_2 \times \mathbb{Z}/2\mathbb{Z}$. □

Corollaire 1.1 (Structure du groupe $\mathbb{Q}_p^*$)**.** *On distingue les cas* p *impair et pair.*

- *Si* $p \neq 2$ *:* $\mathbb{Q}_p^* \simeq \mathbb{Z} \times \mathbb{Z}_p \times \mathbb{Z}/(p-1)\mathbb{Z}$.
- *Si* $p = 2$ *:* $\mathbb{Q}_2^* \simeq \mathbb{Z} \times \mathbb{Z}_2 \times \mathbb{Z}/2\mathbb{Z}$.

Démonstration. Le théorème 1.4 montre que $\left\{ \begin{array}{ccc} \mathbb{Z} \times \mathbf{U} & \to & \mathbb{Q}_p^* \\ (n, u) & \mapsto & up^n \end{array} \right.$ est un isomorphisme de groupes. Le résultat vient avec la proposition 1.9 et le théorème 1.5. En effet pour $p \neq 2$, $\mathbb{F}_p^* \simeq \mathbb{Z}/(p-1)\mathbb{Z}$; pour $p = 2$, $\mathbb{F}_2^*$ est trivial. □

1.2.2 Principe d'approximation faible

Dans la suite, on note $\mathbb{Q}_\infty = \mathbb{R}$ et $\mathbf{V} = \mathbf{P} \cup \{\infty\}$. Par construction on sait que pour $v \in \mathbf{V}$, $\mathbb{Q}$ est dense dans $\mathbb{Q}_v$. Maintenant on va voir que l'on peut aller plus loin.

Proposition 1.10 (Principe d'approximation faible)**.** *Soit S une partie finie de $\mathbf{V}$. L'image de $\mathbb{Q}$ dans $\prod_{s\in S} \mathbb{Q}_s$ par l'injection naturelle $x \mapsto (x)_{s\in S}$ est dense pour la topologie produit.*

Démonstration. S étant fini, il existe $p_1, \cdots, p_n \in \mathbf{P}$ distincts tels que $S \subset \{\infty, p_1, \cdots ., p_n\}$. Ainsi si on montre le résultat pour $\{\infty, p_1, \cdots ., p_n\}$, notre proposition en découlera par injection canonique de $\prod_{s\in S} \mathbb{Q}_s$ dans $\prod_{s\in\{\infty,p_1,\cdots .,p_n\}} \mathbb{Q}_s$. On considère alors dans la suite que $S = \{\infty, p_1, \cdots ., p_n\}$.

Soit alors $(x_\infty, x_1, \cdots, x_n) \in \prod_{s\in S} \mathbb{Q}_s$.

Traitons d'abord le cas où $x_i \in \mathbb{Z}_{p_i}$ pour $i \in [\![1, n]\!]$. Il s'agit de montrer que pour tout $\epsilon < 0$ et tout $N \in \mathbb{N}$, il existe $x \in \mathbb{Q}$ tel que :

$$|x_\infty - x| \leq \epsilon \text{ et } v_{p_i}(x_i - x) \geq N \text{ pour } i \in [\![1, n]\!].$$

Soit $\epsilon < 0$ et $N \in \mathbb{N}$. Pour un tel i on note $m_i = p_i^N$. Les m_i sont alors tous premier entre eux et il existe par le théorème des restes chinois un $x_0 \in \mathbb{Z}$ tel que

$$\forall\, i \in [\![1, n]\!], x_0 \equiv x_i\ [m_i].$$

Ainsi pour chaque i, $v_{p_i}(x_0 - x_i) \geq v_{p_i}(m_i) \geq N$. Prenons maintenant $q \in \mathbb{P}$ impair et différent des p_i. Comme $\frac{1}{q^m} \underset{m\to\infty}{\longrightarrow} 0$, on peut approcher n'importe quel réel par un $\frac{a}{q^m}$ pour un $a \in \mathbb{Z}$ premier aux p_i. Ainsi on considère $u = \frac{a}{q^m}$ tel que :

$$\left| \frac{x_\infty - x_0}{p_1^N \cdots p_n^N} - u \right| \leq \frac{\epsilon}{p_1^N \cdots p_n^N}.$$

Alors après multiplication par $p_1^N \cdots p_n^N$ on a

$$|x_\infty - x_0 - up_1^N \cdots p_n^N| \leq \epsilon$$

et donc si on pose $x = x_0 + up_1^N \cdots p_n^N \in \mathbb{Q}$ on a la bonne approximation $|x_\infty - x| \leq \epsilon$. En outre pour $i \in [\![1, n]\!]$ on a :

$$\begin{aligned} v_{p_i}(x_i - x) &= v_{p_i}(x_i - x_0 - up_1^N \cdots p_n^N) \\ &\geq min(N, v_{p_i}(up_1^N \cdots p_n^N)) \\ &\geq N \qquad \text{(car } q \text{ est choisi de sorte que } v_{p_i}(u) = 0 \text{ et } i \neq j \Longrightarrow v_{p_i}(p_j) = 0). \end{aligned}$$

Ainsi x vérifie toutes les conditions voulues, et convient pour approcher $(x_\infty, x_1, \cdots, x_n)$.

Traitons maintenant le cas général, en ce ramenant au cas précédent. Comme si on travaillait dans $\mathbb{Q}$ on peut en multipliant par un $c_i \in \mathbb{Z}$ avoir : $x_i' = x_i c_i \in \mathbb{Z}_{p_i}$ (en prenant $p_i^{-v_{p_i}(x_i)}$ par exemple). Ainsi on peut envoyer, par homothétie de rapport k un entier, $(x_1, \cdots, x_n)$ sur $(x_1', \cdots, x_n') \in \prod_{i=1}^n \mathbb{Z}_{p_i}$. On trouve le x qui convient pour $(x_\infty k, x_1', \cdots x_n')$ par ce qui précède, et alors $\frac{x}{k} \in \mathbb{Q}$ convient pour $(x_\infty, x_1, \cdots, x_n)$. □

1.2.3 Lemme de Hensel

Le principe que nous allons voir est fondamental pour résoudre des équations p-adiques. L'idée est qu'une fois que l'on a une solution polynomiale "approchée" (c'est-à-dire modulo p), on peut la relever en une solution exacte. Nous commençons pas un lemme.

Lemme 1.3. *Soit $f \in \mathbb{Z}_p[X]$, et soit f' sa dérivée. Soient $x \in \mathbb{Z}_p$, $n, k \in \mathbb{Z}$ tels que :*
$0 \leq 2k < n$, $f(x) \equiv 0 \pmod{p^n}$, $v_p(f'(x)) = k$.
Alors il existe $y \in \mathbb{Z}_p$ tel que :

$$\begin{cases} f(y) \equiv 0 \pmod{p^{n+1}} \\ v_p(f'(y)) = k \quad et \quad y \equiv x \pmod{p^{n-k}} \end{cases}.$$

Démonstration. Commençons par prendre y de la forme $x + p^{n-k}z$ avec $z \in \mathbb{Z}_p$. D'après la formule de Taylor appliquée à f en x on a :

$$f(y) = f(x) + p^{n-k}zf'(x) + p^{2n-2k}a \qquad \text{avec a} \in \mathbb{Q}_p$$

Montrons que $a \in \mathbb{Z}_p$. On écrit f sous la forme :

$$f(X) = a_m X^m + \cdots + a_1 X + a0, a_i \in \mathbb{Z}_p, \forall i \in \{1, \cdots, m\},$$

ainsi

$$a = z^2.\frac{f^{(2)}(x)}{2!} + \cdots + (p^{n-k})^{m-2}.z^m.\frac{f^{(m)}(x)}{m!}.$$

Pour voir que a est un entier, il suffit de montrer que, pour tout $l \in \{1, \cdots, m\}$, $\frac{f^{(l)}(x)}{l!} \in \mathbb{Z}_p$; Par linéarité, on se ramène à montrer, pour tout $j \geq l$, que :

$$\frac{(a_j X^j)^{(l)}}{l!}(x) = a_j \frac{j(j-1)\cdots(j-l+1)}{l!} x^{j-l} \in \mathbb{Z}_p,$$

et on conclut en utilisant le fait que

$$\frac{j(j-1)\cdots(j-l+1)}{l!} = \binom{j}{l} \in \mathbb{Z}.$$

D'autre part, prenons $b \in \mathbb{Z}_p$, $c \in \mathbb{Z}_p^\times$ tels que $f(x) = p^n b$ et $f'(x) = p^k c$.
Comme c est inversible, en choisissant $z = -bc^{-1} \in \mathbb{Z}_p$, on a : $b + zc = 0$.
Par hypothèse, $2n - 2k > n$, donc :
$f(y) = p^n(b + zc) + p^{2n-2k}a \equiv 0 \pmod{p^{n+1}}$.
En appliquant la formule de Taylor à f' en y, on obtient :

$$f'(y) = p^k c + p^{n-k} z f''(y) + p^{2n-2k} a' \quad \text{avec } a' \in \mathbb{Z}_p.$$

(On applique ici le même raisonnement que ci-dessus pour voir que $a' \in \mathbb{Z}_p$.) Comme $n - k > k$, on a bien $v_p(f'(y)) = k$, et donc y convient. □

De ce lemme on va tirer un résultat essentiel, le *lemme de Hensel*, qui sera notre outil pour relever une solution d'équation polynomiale modulo p en une solution dans $\mathbb{Z}_p$. Donnons un premier résultat général.

Théorème 1.6 (Lemme de Hensel). *Soient $f \in \mathbb{Z}_p[X_1 \cdots X_m]$, $x \in (\mathbb{Z}_p)^m$, $n, k \in \mathbb{Z}$ et $j \in [\![1, m]\!]$ tels que :*

$$0 \leq 2k < n, \quad f(x) \equiv 0\ [p^n], \quad v_p(\tfrac{\partial f}{\partial X_j}(x)) = k.$$

Alors il existe un zéro y de f dans $(\mathbb{Z}_p)^m$ tel que $x \equiv y\ [p^{n-k}]$.

Démonstration. On va d'abord travailler dans le cas $m = 1$, c'est-à-dire celui d'un polynôme à une indéterminée. L'idée est d'appliquer récursivement le lemme précèdent afin de créer, grâce aux dérivées, une suite dont la limite sera notre solution. On remarque que ce que l'on fait est un analogue p-adique de la méhode de Newton (qui se déroule elle avec des réels).
On note $x_0 = x$ (ce sera le premier terme de notre suite), et le lemme nous donne x_1 tel que :

$$\begin{cases} f(x_1) \equiv 0 \pmod{p^{n+1}} \\ v_p(f'(x_1)) = k \quad \text{et} \quad x_1 \equiv x_0 \pmod{p^{n-k}} \end{cases}.$$

En remplaçant n par $n+1$ on constate que x_1 satisfait à son tour les hypothèses du lemme précédent. On construit alors x_2 de la même manière. Ainsi de proche en proche construit la suite $(x_n)_n$ telle que pour tout $i \in \mathbb{N}$:

$$\begin{cases} f(x_i) \equiv 0 \pmod{p^{n+i}} & (1) \\ x_{i+1} \equiv x_i \pmod{p^{n+i-k}} & (2) \end{cases}.$$

La deuxième assertion nous donne $|x_{i+1} - x_i|_p \leq \frac{1}{n+i-k}$, donc que $(x_n)_n$ est de Cauchy dans $\mathbb{Z}_p$, donc converge vers une limite que l'on note y. Par construction on a bien $y \equiv x \ (mod\ p^{n-k})$ et par passage à la limite dans (1) on a $f(y) = 0$.

Maintenant si $m > 1$ on va se ramener au cas où $m = 1$. Soit un f comme dans l'énoncé, avec $v_p\left(\frac{\partial f}{\partial X_j}(x)\right) = k$ et $x = (x_i)_{1 \leq i \leq m}$. Alors on introduit la fonction polynomiale d'une variable $g : a \mapsto f(x_1, \cdots, x_{j-1}, a, x_{j+1}, \cdots, x_m)$. Appliquer ce que l'on a fait dans le cas m=1 à g et x_j donne $y_j \in \mathbb{Z}_p$ tel que $x_j \equiv y_j\ [p^{n-k}]$ et $g(y_j) = 0$. On construit finalement

$$y = (x_1, \cdots, x_{j-1}, y_j, x_{j+1}, \cdots, x_m) \in (\mathbb{Z}_p)^m.$$

Ce y répond à la question.

□

Ceci est le *Lemme de Hensel* dans toute sa généralité. On peut en donner un corollaire plus parlant dans le cas où $m = 1,\ n = 1\ et\ k = 0$:

Corollaire 1.2. *Soient $f \in \mathbb{Z}_p[X]$, f' sa dérivée, et $x \in \mathbb{Z}_p$ tel que :*

$$f(x) \equiv 0\ [p\mathbb{Z}_p] \qquad et \qquad f'(x) \not\equiv 0\ [p\mathbb{Z}_p].$$

Alors il existe $y \in \mathbb{Z}_p$ tel que $f(y) = 0$ et $x \equiv y\ [p\mathbb{Z}_p]$.

Définition 1.11. *Un point $(x_1, \cdots, x_m) \in \mathbb{Z}_p^m$ est dit primitif si l'un des x_i est inversible.*

Ce qui va être particulièrement utile pour nos futures démonstrations est le corollaire suivant.

Corollaire 1.3. *On suppose $p \neq 2$. On note $f = \sum a_{ij} X_i X_j$ avec $a_{ij} = a_{ji}$ une forme quadratique telle que $a_{ij} \in \mathbb{Z}_p$, et on prend un $a \in \mathbb{Z}_p$. Si $\det(a_{ij})$ est inversible alors toute solution primitive de l'équation $f(x) \equiv a\ [p]$ se relève en une solution exacte.*

Démonstration. Soit $x = (x_1, \cdots, x_m)$ une solution primitive de $f(x) \equiv a\ [p]$. On veut se placer dans le cadre du lemme de Hensel, avec n=1 et k=0. On a que

$$\frac{\partial f}{\partial X_j} = 2 \sum_i a_{ij} X_i.$$

Or $\det(a_{ij})$ est inversible, donc non divisible par p. En outre il existe $i \leq m$ tel que x_i est inversible donc non divisible par p. Ainsi l'équation matricielle à coefficients dans le corps $\mathbb{F}_p$

$$\begin{pmatrix} \frac{\partial f}{\partial X_1}(x) \\ \vdots \\ \frac{\partial f}{\partial X_n}(x) \end{pmatrix} = \begin{pmatrix} 2a_{1,1} & \cdots & 2a_{1,n} \\ \vdots & \ddots & \vdots \\ 2a_{n,1} & \cdots & 2a_{n,n} \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

nous permet de déduire que l'un des $\frac{\partial f}{\partial X_j}(x)$ est non nul dans $\mathbb{F}_p$. On conclut alors par le lemme de Hensel. □

1.2.4 Le groupe $\mathbb{Q}_p^{2*}$ des carrés de $\mathbb{Q}_p^*$

Dans la suite si $\mathbb{K}$ est un corps on notera $\mathbb{K}^{2*} = \{x^2; x \in \mathbb{K}^*\}$ l'ensemble de ses carrés non nuls. Il s'agit d'un sous-groupe de $\mathbb{K}^*$.

Afin de fournir une preuve complète du théorème de Hasse-Minkowski, nous avons besoin de savoir que $\mathbb{Q}_p^{2*}$ est ouvert dans $\mathbb{Q}_p^*$. Ce résultat pourrait se déduire des théorèmes suivants (1.8 et 1.9), mais il est intéressant de voir dans la preuve qui suit comment le lemme de Hensel peut être utilisé.

Théorème 1.7. *$\mathbb{Q}_p^{2*}$ est un ouvert de $\mathbb{Q}_p^*$*

Démonstration. Soit $c \in \mathbb{Q}_p^{2*}$. Il existe alors $a = p^\alpha u$ dans $\mathbb{Q}_p^*$ avec $\alpha \in \mathbb{Z}$ et $u \in \mathbb{U}$ tel que $a^2 = c$.

Si $\alpha \geq 0$ alors $a \in \mathbb{Z}_p$. On considère la boule ouverte $B = B(c, \frac{1}{p^{2\alpha+3}})$. Soit $x \in B$. On prend le polynôme $P = X^2 - x$. On a $|c - x|_p < \frac{1}{p^{2\alpha+3}}$, c'est à dire $a^2 = c \equiv x\,[p^{2\alpha+3}]$. Ainsi $x \in \mathbb{Z}_p$ et $P \in \mathbb{Z}_p[X]$, et on a $P(a) \equiv 0\,[p^{2\alpha+3}]$. En outre

$$v_p(P'(a)) = v_p(2a) \leq 1 + v_p(a) \leq 1 + \alpha.$$

Comme $2v_p(P'(a)) < 2\alpha + 3$ le lemme de Hensel nous permet de relever a en $r \in \mathbb{Z}_p$, racine de P. Ainsi $r^2 = x$ et x est bien un carré. x est non nul (sinon $p^{2\alpha+3}|c$, ce qui est absurde) donc $x \in \mathbb{Q}_p^{2*}$.

Si $\alpha < 0$. On pose $B = B(c, \frac{1}{p^3})$. Soit $x \in B$. On a alors

$$|c - x|_p < \frac{1}{p^3}.$$

On a également :

$$|x|_p \leq \max(|x - c|_p, |c|_p).$$

Or

$$|c|_p = |p^{2\alpha}|_p = p^{-2\alpha} > \frac{1}{p^3}$$

donc $|x|_p \leq p^{-2\alpha}$ et $v_p(x) \geq 2\alpha$. Ainsi le polynôme $X^2 - p^{-2\alpha}x$ est dans $\mathbb{Z}_p[X]$. Comme $x \in B$ on a :

$$\begin{aligned} p^{2\alpha}u^2 = c &\equiv x\,[p^3] \\ u^2 &\equiv p^{-2\alpha}x\,[p^{-2\alpha+3}] \\ P(u) &\equiv 0\,[p^{-2\alpha+3}]. \end{aligned}$$

Et comme $u \in \mathbb{Z}_p$ et $2v_p(P'(u)) = 2v_p(2u) \leq 2 < -2\alpha + 3$ on peut relever u en $r \in \mathbb{Z}_p$ racine de P. Ainsi on a :

$$(rp^\alpha)^2 = x$$

Et x est un carré dans $\mathbb{Q}_p^*$. (Là encore $x \neq 0$, car $p^3 \nmid c$). □

Il est en outre nécessaire pour la suite et intéressant de caractériser les carrés de $\mathbb{Q}_p^*$. Nous allons pour cela utiliser les résultats vus plus tôt sur le groupe des unités p-adiques $\mathbf{U}$. Les cas p impair et pair continuent bien sûr d'être distingués ; commençons avec $p \neq 2$.

On a vu précédemment l'isomorphisme $\mathbf{U}/\mathbf{U}_1 \simeq \mathbb{F}_p^*$; cela permet de définir, pour $u \in \mathbf{U}$, $(\frac{u}{p})$ le symbole de Legendre de l'image de u dans $\mathbb{F}_p^*$. Alors u est un carré modulo (multiplicativement) $\mathbf{U}_1$ si et seulement si $(\frac{u}{p}) = 1$.

Théorème 1.8 (Caractérisation des carrés de $\mathbb{Q}_p^*$, $p \neq 2$)**.** *Soient $p \in \mathbf{P} \setminus \{2\}$ et $x = up^n \in \mathbb{Q}_p^*$ avec $u \in \mathbf{U}$ et $n \in \mathbb{Z}$. On a l'équivalence suivante :*

$$x \in \mathbb{Q}_p^{2*} \iff \begin{cases} n \text{ pair} \\ (\frac{u}{p}) = 1 \end{cases}.$$

Démonstration. Par le théorème 1.4, x est un carré si et seulement si n est pair et u est un carré. D'après la proposition 1.9, $\mathbf{U} \simeq \mathbf{U}_1 \times \mathbb{F}_p^*$: on peut écrire (u_1, a) l'image de u par cet isomorphisme. Donc pour que u soit un carré, il faut et il suffit que u_1 soit un carré dans $\mathbf{U}_1$ et que a soit un carré dans $\mathbb{F}_p^*$. Le second point équivaut à $(\frac{a}{p}) = 1$, c'est-à-dire à $(\frac{u}{p}) = 1$ par définition.

Il reste à prouver que "u_1 *est un carré dans* $\mathbf{U}_1$" est une condition vide. On utilise le théorème 1.5 de structure de $\mathbf{U}_1$: soit ϕ l'isomorphisme de $\mathbf{U}_1$ dans $\mathbb{Z}_p$. Puisque $p \neq 2$, 2 est inversible dans $\mathbb{Z}_p$. On note alors $a = \frac{1}{2}\phi(u_1) \in \mathbb{Z}_p$. Ainsi $\phi^{-1}(a)^2 = \phi^{-1}(a+a) = \phi^{-1}(\phi(u_1)) = u_1$: u_1 est un carré. □

Corollaire 1.4. *Soit $p \in \mathbf{P} \setminus \{2\}$. On a l'isomorphisme de groupes $\mathbb{Q}_p^*/\mathbb{Q}_p^{2*} \simeq (\mathbb{Z}/2\mathbb{Z})^2$. De plus si $u \in \mathbf{U}$ vérifie $(\frac{u}{p}) = -1$, $\{1, u, p, up\}$ est un système de représentants du quotient dans $\mathbb{Q}_p^*$.*

Démonstration. On peut interpréter le théorème qui précède de la façon suivante : l'isomorphisme $\mathbb{Q}_p^* \simeq \mathbb{Z} \times \mathbf{U}_1 \times \mathbb{F}_p^*$ envoie $\mathbb{Q}_p^{2*}$ sur $2\mathbb{Z} \times \mathbf{U}_1 \times \mathbb{F}_p^{2*}$. Alors $\mathbb{Q}_p^*/\mathbb{Q}_p^{2*} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{F}_p^*/\mathbb{F}_p^{2*} \simeq (\mathbb{Z}/2\mathbb{Z})^2$. L'affirmation sur les représentants est évidente. □

Le cas $p = 2$ est donné par le théorème suivant.

Théorème 1.9 (Caractérisation des carrés de $\mathbb{Q}_2^*$)**.** *Soit $x = u2^n \in \mathbb{Q}_2^*$ avec $u \in \mathbf{U}$ et $n \in \mathbb{Z}$. On a l'équivalence suivante :*

$$x \in \mathbb{Q}_2^{2*} \iff \begin{cases} n \text{ pair} \\ u \equiv 1\ [8] \end{cases}.$$

Démonstration. De même que pour le cas $p \neq 2$, x est un carré si et seulement si n est pair et u est un carré. D'après l'isomorphisme $\mathbf{U} \simeq \mathbf{U}_1/\mathbf{U}_2$ où $\mathbf{U}_1/\mathbf{U}_2$ est d'ordre 2, u est un carré dans $\mathbf{U}$ si et seulement si $u \in \mathbf{U}_2$ et u est un carré dans $\mathbf{U}_2$. Notons G le sous-groupe des carrés de $\mathbf{U}_2$: on va montrer que $G = \mathbf{U}_3$. Comme $\mathbf{U}_3$ est l'ensemble des unités v telles que $v \equiv 1\ [8]$, cela terminera la preuve.

Si $1 + 4x \in \mathbf{U}_2$ (avec $x \in \mathbb{Z}_2$), $(1+4x)^2 \equiv 1\ [8]$: on a $G \subset \mathbf{U}_3$. De plus on a construit dans la preuve du théorème 1.5 de structure de $\mathbf{U}_1$ un isomorphisme de $\mathbb{Z}_2$ dans $\mathbf{U}_2$. G est l'image de $2\mathbb{Z}_2$ par cet isomorphisme donc $\mathbf{U}_2/G \simeq \mathbb{Z}_2/2\mathbb{Z}_2 \simeq \mathbb{Z}/2\mathbb{Z}$, et G est d'indice 2 dans $\mathbf{U}_2$. Comme c'est aussi le cas de $\mathbf{U}_3$, l'indice de G dans $\mathbf{U}_3$ est 1 : il y a égalité. □

Corollaire 1.5. *On a l'isomorphisme de groupes $\mathbb{Q}_2^*/\mathbb{Q}_2^{2*} \simeq (\mathbb{Z}/2\mathbb{Z})^3$. De plus $\{\pm 1, \pm 5, \pm 2, \pm 10\}$ est un système de représentants du quotient dans $\mathbb{Q}_2^*$.*

Démonstration. Là encore on réinterprète le théorème : l'isomorphisme $\mathbb{Q}_2^* \simeq \mathbb{Z} \times \mathbf{U}_1/\mathbf{U}_2 \times \mathbf{U}_2$ envoie $\mathbb{Q}_2^{2*}$ sur $2\mathbb{Z} \times 1 \times \mathbf{U}_3$. Alors $\mathbb{Q}_p^*/\mathbb{Q}_p^{2*} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbf{U}_1/\mathbf{U}_2 \times \mathbf{U}_2/\mathbf{U}_3 \simeq (\mathbb{Z}/2\mathbb{Z})^3$. L'affirmation sur les représentants est conséquence des deux faits suivants : $\{\pm 1\}$ est un système de représentants de $\mathbf{U}_1/\mathbf{U}_2$ dans $\mathbf{U}_1$, et $\{1, 5\}$ est un système de représentants de $\mathbf{U}_2/\mathbf{U}_3$ dans $\mathbf{U}_2$. □

2 Formes quadratiques sur $\mathbb{Q}_p$ et théorème de Hasse-Minkowski

Nous en venons maintenant aux formes quadratiques, ce qui va nous mener à la preuve du théorème de Hasse-Minkowski.

2.1 Premières définitions

On considère un corps $\mathbb{K}$ de caractéristique différente de 2, et E un $\mathbb{K}$-espace vectoriel de dimension $n \in \mathbb{N}$ finie. Nous nous intéresserons seulement à des formes quadratiques sur une telle structure E, bien que l'on pourrait généraliser à des modules sur des anneaux (voir [Bou70]).

Définition 2.1 (Forme quadratique)**.** *Une forme quadratique sera une application $q : E \to \mathbb{K}$ vérifiant :*
- $\forall\, k \in \mathbb{K} \quad \forall x \in E,\ q(kx) = k^2 q(x)$
- l'application $B : E \times E \to \mathbb{K}$ définie par $B(x,y) = q(x+y) - q(x) - q(y)$ est bilinéaire.

Dans la suite on fixe une telle forme quadratique q.

Définition 2.2. *En notant, pour $x, y \in V$, $x \cdot y = \frac{1}{2}B(x,y)$, on définit une application bilinéaire symétrique. On la nomme produit scalaire associé à q (attention cependant ce n'est pas nécessairement un produit scalaire au sens usuel).*

Si $x, y \in V$, il vient rapidement que $q(x+y) = q(x) + q(y) + 2(x \cdot y)$ et que $x \cdot x = q(x)$.

Définition 2.3. .

- On dit que q représente un $k \in \mathbb{K}$ quand il existe $x \in E$ tel que $q(x) = k$.

- On dit que $x \in E$ est isotrope pour q quand $q(x) = 0$.

Si maintenant on pose $B = (e_1, \cdots, e_n)$ une base de E. Alors on peut définir M la *matrice de Q par rapport à B* en notant : $\forall\, i, j \in [\![1, n]\!],\ a_{ij} = e_i \cdot e_j$ et $M = (a_{ij})$. Ainsi on retrouve l'idée classique que l'on a d'une forme quadratique :

$$\text{si } x = \sum_{i=1}^{n} x_i e_i \text{ alors } q(x) = \sum_{i,j=1}^{n} a_{ij} x_i x_j.$$

Ainsi en notant $\mathbb{K}^{2*}$ l'ensemble des carrés non nuls de $\mathbb{K}$, on a "unicité" de $det(A)$ dans $\mathbb{K}/\mathbb{K}^{2*}$. En effet notons B' une autre base obtenue à partir de B grâce à une matrice P inversible et A' la matrice de q dans B'. La multiplicativité du déterminant nous donne alors $det(A) = det(A')det(P)^2$, avec $det(P) \in \mathbb{K}^{2*}$.

Dans la suite on notera alors $\mathrm{Disc}(q)$ cet élément de $\mathbb{K}/\mathbb{K}^{2*}$.

On voit que le concept de forme quadratique est intimement lié avec celui de forme bilinéaire symétrique, il convient alors de donner les définition habituelles.

Définition 2.4 (Orthogonalité)**.** *Définitions habituelles :*

- Deux éléments x et y de E sont dits orthogonaux pour q si $x \cdot y = 0$.

- On désigne l'orthogonal pour q de S, une partie de E, par $S^\circ = \{x \in E \mid \forall y \in S\ x \cdot y = 0\}$.

- Si $E^\circ = 0$, q est dit non dégénérée.

- Une base $(f_1, \cdots, f_m)$ d'un sous-espace vectoriel V de E est orthogonale pour q quand $\forall\, i, j \in [\![1, m]\!],\ i \neq j \implies f_i \cdot f_j = 0$.

Si cela n'entraîne pas d'ambiguïté on se permettra de parler d'orthogonalité (ou d'isotropie), et non d'orthogonalité (ou d'isotropie) par rapport à une forme quadratique.

Il est immédiat de voir que :

i) Si V est un sous-espace de E, alors V° est un sous-espace de E et $E = V \widehat{\bigoplus} V^\circ$.

ii) q est non dégénérée revient à dire que $\mathrm{Disc}(q)$ est non nul.

On va maintenant voir un théorème facilitant la démonstration des théorèmes généraux sur les formes quadratiques.

Théorème 2.1. *Soit E un espace vectoriel de dimension finie, et q une forme quadratique sur E.*
Il existe une base orthogonale de E pour q.

Démonstration. On procède par récurrence sur $n = dim(E)$.

Si $n = 0$ c'est évident.

Soit E un espace vectoriel de dimension $n+1$. Si tout élément de E est isotrope, alors toute base est orthogonale. Sinon il existe $x \in E$ tel que $x \cdot x \neq 0$. On peut alors décomposer $E = \mathbb{K}.x \widehat{\bigoplus} H$ avec H le plan orthogonal à $\mathbb{K}x$. Donc par hypothèse de récurrence on a $(e_1, \cdots .e_{n-1})$ une base orthogonale de H, et donc $(e_1, \cdots, e_{n-1}, x)$ est une base orthogonale de E. □

Faisons une remarque avant de passer à la proposition suivante : si q est non dégénérée alors pour tout $x \in E$ il existe $y \in E$ tel que $x \cdot y = 1$. En effet il existe $y' \in E$ tel que $x \cdot y \neq 0$: $y = \frac{1}{x \cdot y} y'$ convient.

Proposition 2.1. *Soit q une forme quadratique non dégénérée. Si q représente 0, alors q représente tout $a \in \mathbb{K}$.*

Démonstration. Soit $a \in \mathbb{K}$. Par hypothèse, soient $x \in E$ non nul tel que $q(x) = 0$, puis $y \in E$ tel que $x \cdot y = 1$. On pose $z = y - \frac{y \cdot y}{2} x$. Calculons : $q(z) = q(y) + q(\frac{y \cdot y}{2} x) - 2(y \cdot \frac{y \cdot y}{2} x) = q(y) + 0 - (y \cdot y)(y \cdot x) = 0$; et $x \cdot z = x \cdot y - x \cdot \frac{y \cdot y}{2} x = 1 - \frac{y \cdot y}{2} q(x) = 1$.

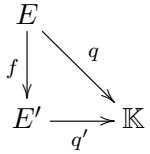
Alors : $q(x + \frac{a}{2} z) = q(x) + q(\frac{a}{2} z) + 2(x \cdot \frac{a}{2} z) = 0 + 0 + a(x \cdot z) = a$. □

Cette proposition nous servira bientôt à prouver deux lemmes importants pour pouvoir démontrer le théorème de Hasse-Minkowski.

2.2 Formes quadratiques équivalentes

On veut maintenant définir des classes d'équivalences sur l'ensemble des formes quadratiques, dans l'optique de simplifier les démonstrations complexes. Comme souvent en mathématiques on va passer par la notion de morphisme.

Définition 2.5. *Soit q et q' deux formes quadratiques sur E et E' deux $\mathbb{K}$-espaces vectoriels de dimension finie. Un morphisme de formes quadratiques entre q et q' est une application linéaire : $f : E \to E'$ tel que le diagramme suivant commute :*



(i.e $q = q' \circ f$)

On peut alors définir la notion d'isomorphisme de forme quadratique qui mènera naturellement à celle de forme quadratiques équivalentes.

Définition 2.6. *Équivalence*

- *On appelle isomorphisme de formes quadratiques, un morphisme de formes quadratiques qui est aussi un isomorphisme d'espace vectoriel.*
- *Deux formes quadratiques sont équivalentes quand il existe un isomorphisme d'espace vectoriel de l'une vers l'autre. On notera $q \sim q'$.*

On remarque que $q \sim q'$ revient à dire que si A et A' sont les matrices de q et q' respectivement (dans une base quelconque) alors il existe X une matrice inversible telle que $A' = XA\,{}^tX$. Il est en outre clair mais néanmoins fondamental de remarquer que q représente 0 si et seulement si q' représente 0. Ainsi le théorème 2.1 nous donne le corollaire suivant.

Théorème 2.2. *Soit E un espace vectoriel de dimension finie n, et q une forme quadratique sur E. Il existe $a_1, \cdots, a_n$ dans $\mathbb{K}$ tels que $q \sim a_1X_1^2 + \cdots + a_nX_n^2$.*

Démonstration. On décompose E en une base orthogonale pour q, c'est à dire $E = \widehat{\bigoplus_{i=1,\cdots,n}} \mathbb{K}e_i$. La base étant orthogonale la matrice $A = (e_i \cdot e_j)_{ij}$ de q dans cette base est diagonale et donc de la forme voulue :

$$A = \begin{pmatrix} a_1 & 0 & \cdots & 0 \\ 0 & \ddots & 0 & \vdots \\ \vdots & 0 & \ddots & 0 \\ 0 & \cdots & 0 & a_n \end{pmatrix} \qquad \text{avec } a_i = e_i \cdot e_i.$$

□

Ceci légitime la définition suivante :

Définition 2.7. *Le rang d'une forme quadratique est le nombre de a_i non nuls dans la décomposition précédente.*

On remarque en outre qu'avec les notations du théorème précédent $d(q) = a_1 \cdots a_n$ dans $\mathbb{K}/\mathbb{K}^{2*}$.

On introduit maintenant une notion qui nous permettra de démontrer un résultat fondamental sur un invariant d'une forme quadratique. On fixe q une forme quadratique non dégénérée sur un $\mathbb{K}$-espace vectoriel E de dimension $n \geq 3$. Gardons en tête que la notion d'*orthogonalité* est alors relatif à q.

Définition 2.8 (Contiguité)**.** *Deux bases orthogonales sont dites contiguës si elles ont un élément en commun. De plus $(B_1, \cdots, B_n)$ est une chaîne de base orthogonale contiguë reliant deux bases orthogonales B et B' si $B = B_1$, $B' = B_n$, et que pour $i \in [\![1, n-1]\!]$ B_i et B_{i+1} sont deux bases orthogonales contiguës.*

Théorème 2.3. *Deux bases orthogonales $\chi = (e_1, \cdots e_n)$ et $\chi' = (e'_1, \cdots e'_n)$ sont toujours reliées par une chaîne de bases orthogonales contiguës.*

Démonstration. On pose q la forme quadratique $x \mapsto x \cdot x$. On distingue 3 cas :

Cas 1 : $(e_1 \cdot e_1)(e'_1 \cdot e'_1) - (e_1 \cdot e'_1)^2 \neq 0$

Ceci signifie que e_1 et e'_1 ne sont pas colinéaires et que le plan $P = ke_1 + ke'_1$ est non dégénéré, car $(e_1 \cdot e_1)(e'_1 \cdot e'_1) - (e_1 \cdot e'_1)^2$ est un représentant du discriminant de q.

De là, e_1 et e'_1 étant des vecteurs d'une base orthogonale d'un module quadratique non dégénéré, on a : $(e_1 \cdot e_1) \neq 0$ et $(e'_1 \cdot e'_1) \neq 0$.

On définit alors $\varepsilon_2 = \begin{cases} e'_1 & \text{si } (e_1 \cdot e'_1) = 0 \\ e_1 + \frac{e_1 \cdot e_1}{e_1 \cdot e'_1} e'_1 & \text{sinon} \end{cases}$ de sorte à avoir : $P = \mathbb{K}e_1 \widehat{\bigoplus} \mathbb{K}\varepsilon_2$.

De même, on définit ε'_2 de telle sorte que $P = \mathbb{K}e'_1 \widehat{\bigoplus} \mathbb{K}\varepsilon'_2$.

Soit H l'orthogonale de P, comme P est non dégénéré, $E = P \widehat{\bigoplus} H$. soit $(e''_3, \cdots, e''_n)$ une base de H, on peut alors passer de χ à χ' par la chaîne suivante :

$$\chi \to (e_1, \varepsilon_2, e_3'', \cdots, e_n'') \to (e_1', \varepsilon_2', e_3'', \cdots, e_n'') \to \chi'.$$

Cas 2 : $(e_1 \cdot e_1)(e_2' \cdot e_2') - (e_1 \cdot e_2')^2 \neq 0$

On raisonne de la même manière en remplaçant e_1' par e_2'.

Cas 3 : $(e_1 \cdot e_1)(e_i' \cdot e_i') - (e_1 \cdot e_i')^2 = 0 \quad$ pour $i = 1, 2$.

Dans ce cas montrons qu'il existe $x \in k, e_x = e_1' + xe_2'$ soit non isotrope et $Vect(e_1, e_x)$ soit un plan non dégénéré.
Dans un premier temps, on a : $(e_x \cdot e_x) = (e_1' \cdot e_1') + x^2(e_2' \cdot e_2')$, donc pour avoir e_x non isotrope, nécessairement $x^2 \neq -\frac{(e_1' \cdot e_1')}{(e_2' \cdot e_2')}$.

D'autre part, pour que e_x engendre avec e_1 un plan non dégénéré il faut et il suffit que

$$Disq(q) \neq 0 \quad \Leftrightarrow \quad (e_1 \cdot e_1)(e_x \cdot e_x) - (e_1 \cdot e_x)^2 \neq 0$$

Or $(e_1 \cdot e_1)(e_i' \cdot e_i') - (e_1 \cdot e_i')^2 = 0 \quad$ Pour $i = 1, 2$ donc

$$\begin{aligned}(e_1 \cdot e_1)(e_x \cdot e_x) &= (e_1 \cdot e_1)((e_1' \cdot e_1') + x^2(e_2' \cdot e_2')) \\ &= (e_1 \cdot e_1')^2 + x^2(e_1 \cdot e_2')^2 \\ &= ((e_1 \cdot e_1') + x(e_1 \cdot e_2'))^2 - 2x(e_1 \cdot e_1')(e_1 \cdot e_2') \\ &= (e_1 \cdot e_x)^2 - 2x(e_1 \cdot e_1')(e_1 \cdot e_2')\end{aligned}$$

Donc $(e_1 \cdot e_1)(e_x \cdot e_x) - (e_1 \cdot e_x)^2 = -2x(e_1 \cdot e_1')(e_1 \cdot e_2')$ et la condition du cas 3 donne $(e_1 \cdot e_i') \neq 0$ pour $i = 1, 2$. Donc

$$\begin{cases} -2x(e_1 \cdot e_1')(e_1 \cdot e_2') \neq 0 \\ x^2 \neq -\frac{(e_1' \cdot e_1')}{(e_2' \cdot e_2')} \end{cases}$$

Ce qui exclu au plus 3 valeurs pour x.
De là, si k possède plus de 3 éléments c'est bon, le dernier cas à traiter est le cas $k = \mathbb{F}_3$.
Dans ce cas, le seul carré non nuls est 1 donc la condition du cas 3 devient : $(e_1 \cdot e_1)(e_i' \cdot e_i') = 1 \quad$ pour $i = 1, 2 \quad$ donc $\quad \frac{(e_1' \cdot e_1')}{(e_2' \cdot e_2')} = 1$.
$x = 1$ convient.

Soit alors e_x comme ci-dessus. Comme e_x n'est pas isotrope, il existe e_2'' tel que (e_x, e_2'') est une base orthogonale de $P = \mathbb{K}e_1' \widehat{\oplus} \mathbb{K}e_2'$.

On pose alors $\chi'' = (e_x, e_2'', e_3', \cdots, e_n') \quad$ et comme $\mathbb{K}e_x + \mathbb{K}e_1$ est non dégénéré, on peut relier χ'' à χ' comme dans le cas 1. □

Terminons par énoncer deux propositions qui seront utiles à la démonstration du théorème de Hasse-Minkowski. Elles utilisent de façon essentielle la proposition 2.1.

Proposition 2.2. *Soient $f = b_1X_1^2 + \cdots + b_mX_m^2$ et $g = c_1Y_1^2 + \cdots + c_mY_m^2$ des formes quadratiques en des variables différentes sur E (de dimension $m + n$). Alors $f - g$ représente 0 si et seulement si il existe $a \in \mathbb{K}^*$ représenté par f et par g.*

Démonstration. Le sens réciproque est trivial. Supposons que $f - g$ représente 0 : soit $x \in E \setminus \{0\}$ tel que $(f - g)(x) = 0$, c'est-à-dire $f(x) = g(x)$. Si $f(x) \neq 0$ c'est bon. Sinon, f et g représentent 0, donc par la proposition 2.1 représentent toutes les deux 1 (par exemple). □

Proposition 2.3. *Soient f une forme quadratique, Z une indéterminée n'apparaissant pas dans f, et $a \in \mathbb{K}$. Alors f représente a si et seulement si $f - aZ^2$ représente 0.*

Démonstration. Cette fois c'est le sens direct qui est trivial, supposons donc que $f - aZ^2$ représente 0. On identifie E et $\mathbb{K}^{n+1}$, avec n le rang de f. Soit $(x_1, \cdots, x_n, z) \in \mathbb{K}^{n+1}$ tel que $f(x_1, \cdots, x_n) - az^2 = 0$. Si $z \neq 0$, $a = f(\frac{x_1}{z}, \cdots, \frac{x_n}{z})$. Si $z = 0$, f représente 0, donc représente a d'après la proposition 2.1. □

2.3 Symbole de Hilbert

On rappelle que l'on a pris les notations $\mathbb{Q}_\infty = \mathbb{R}$ et $\mathbf{V} = \mathbf{P} \cup \{\infty\}$. On considère un complété $\mathbb{K}$ de $\mathbb{Q}$, c'est-à-dire un $\mathbb{Q}_v$ avec $v \in \mathbf{V}$. L'idée est d'avoir un outil arithmétique permettant de savoir si une équation du type suivant, avec $a, b \in \mathbb{K}^*$, a une solution :

$$(E_{a,b}) : \qquad x^2 - ay^2 - bz^2 = 0.$$

On note qu'il s'agit de la même idée qui nous pousse à introduire le symbole de Legendre, dans le cas des équations de la forme $x^2 - a = 0$ avec $a \in \mathbb{F}_p$, où p est premier.

2.3.1 Propriétés locales

Définition 2.9. *Soient $a, b \in \mathbb{K}^*$, on définit le symbole de Hilbert de a et b relativement à $\mathbb{K}$ par :*

$$(a, b) = \begin{cases} 1 & \text{si il existe une solution non triviale de } (E_{a,b}) \text{ sur } \mathbb{K} \\ -1 & \text{sinon} \end{cases}.$$

Nous allons maintenant développer des propriétés qui nous seront utiles pour démontrer des théorèmes plus généraux sur les formes quadratiques. La suivante nous donne une information sur le symbole de Hilbert via une extension quadratique (ou triviale).

Proposition 2.4. *Pour $a, b \in \mathbb{K}^*$, on a l'équivalence :*

$$(a, b) = 1 \text{ si et seulement si } \exists \alpha \in \mathbb{K}(\sqrt{b}),\ a = \mathrm{N}_{\mathbb{K}(\sqrt{b})/\mathbb{K}}(\alpha).$$

Avant la démonstration rappelons le fait suivant, en supposant que b n'est pas un carré dans $\mathbb{K}$. On note dans les lignes qui suivent $\mathrm{N} = \mathrm{N}_{\mathbb{K}(\sqrt{b})/K}$ par souci de lisibilité.

$(1, \sqrt{b})$ est une $\mathbb{K}$-base de $\mathbb{K}(\sqrt{b})$, et pour $x + y\sqrt{b} \in \mathbb{K}(\sqrt{b})$, $\mathrm{N}(x + ry) = x^2 - by^2$. En outre l'ensemble $\{\mathrm{N}(\alpha)\ ;\ \alpha \in \mathbb{K}(\sqrt{b})^*\}$ est un sous-groupe multiplicatif de $\mathbb{K}^*$, que l'on note $\mathrm{N}\mathbb{K}_b^*$.

Démonstration. Distinguons deux cas.

- Si b est un carré dans $\mathbb{K}$, alors $\mathbb{K}(\sqrt{b}) = \mathbb{K}$ et $\mathrm{N} = Id_{\mathbb{K}}$. Tout $a \in \mathbb{K}^*$ est donc la norme d'un élément de $\mathbb{K}(\sqrt{b})$. De plus $(E_{a,b})$ a une solution non triviale, $(\sqrt{b}, 0, 1)$. Donc pour tout $a \in \mathbb{K}^*$ on a $(a, b) = 1$. Les deux assertions sont toujours vraies, d'où l'équivalence.

- Si maintenant b n'est pas un carré dans $\mathbb{K}$, $\mathbb{K}(\sqrt{b})$ est bien une extension quadratique de $\mathbb{K}$. Si $(a, b) = 1$ alors on a $(x, y, z) \in \mathbb{K}^3$ non nul tel que $x^2 - ay^2 - bz^2 = 0$. On remarque que si $y = 0$ alors $x^2 = bz^2$, donc comme la solution est non triviale $z \neq 0$. Dans ce cas $b = (\frac{x}{z})^2$, et b est un carré, ce qui est exclu par hypothèse. Ainsi $y \neq 0$. On constate alors que a est la norme de $\frac{x}{y} + \frac{z}{y}\sqrt{b}$. Réciproquement si on a $x + y\sqrt{b} \in \mathbb{K}(\sqrt{b})^*$ tel que $a = \mathrm{N}(x + y\sqrt{b}) = x^2 - by^2$, alors $(x, 1, y)$ est solution non triviale de $(E_{a,b})$, et donc $(a, b) = 1$. □

Énonçons maintenant une liste de quelques propriétés permettant de manier plus aisément le symbole de Hilbert.

Proposition 2.5. *Soit $a, b, c \in \mathbb{K}^*$.*

i) $(a,b) = (b,a)$ *et* $(a,c^2) = 1$.

ii) $(a,-a) = 1$, *et si* $a \neq 1$ *alors* $(a, 1-a) = 1$.

iii) *Si* $(a,b) = 1$ *alors* $(aa', b) = (a', b)$.

iv) $(a,b) = (a,-ab) = (a,(1-a)b)$ *(avec* $a \neq 1$ *pour la dernière égalité).*

Démonstration.

i) La première égalité vient du fait que (x,y,z) est solution de $(E_{a,b})$ si et seulement si (x,z,y) est solution de $(E_{b,a})$. La seconde est vraie car $(c,0,1)$ est solution non triviale de (E_{a,c^2}).

ii) $(a,-a) = 1$ car $(0,1,1)$ est solution non triviale de $(E_{a,-a})$. Si on suppose que $a \neq 1$, alors $(1,1,1)$ est solution non triviale de $(E_{a,1-a})$.

iii) Supposons que $(a,b) = 1$. D'après la proposition 2.4, $a \in \mathrm{N}\mathbb{K}_b^*$. Puisque $\mathrm{N}\mathbb{K}_b^*$ est un groupe, $a' \in \mathrm{N}\mathbb{K}_b^*$ si et seulement si $a'a \in \mathrm{N}\mathbb{K}_b^*$. La même proposition permet de conclure.

iv) Comme $(a,-a) = 1$, d'après **iii)** $(a,b) = (a,-ab)$. De même pour l'autre égalité si on suppose que $a \neq 1$. □

On va maintenant démontrer un résultat important exprimant le symbole de Hilbert au moyen du symbole de Legendre bien connu $(\frac{\cdot}{\cdot})$. Introduisons auparavant deux notations héritées de l'étude de ce dernier.

Définition 2.10. *On pose pour* $n \in \mathbb{N}$ *:*

- $\epsilon(n)$ *le résidu de* $\frac{n-1}{2}$ *modulo* 2, *c'est-à-dire* $\begin{cases} 0 & \text{si } n \equiv 1\ [4] \\ 1 & \text{si } n \equiv 3\ [4] \end{cases}$.
- $\omega(n)$ *le résidu de* $\frac{n^2-1}{8}$ *modulo* 2, *c'est-à-dire* $\begin{cases} 0 & \text{si } n \equiv \pm 1\ [8] \\ 1 & \text{si } n \equiv \pm 3\ [8] \end{cases}$.

Ces deux notations permettent d'exprimer les résultats classiques suivants, pour p premier : $(\frac{-1}{p}) = (-1)^{\epsilon(p)}$ et $(\frac{2}{p}) = (-1)^{\omega(p)}$.

Théorème 2.4. *Soit* $a, b \in \mathbb{K}^*$.

(i) *Si* $\mathbb{K} = \mathbb{R}$ *:* $(a,b) = 1$ *si et seulement si* $a > 0$ *ou* $b > 0$.

(ii) *Si* $\mathbb{K} = \mathbb{Q}_p$ *avec* $p \neq 2$ *premier, en écrivant* $a = up^\alpha$ *et* $b = vp^\beta$ *avec* $u, v \in \mathbf{U}$ *:*

$$(a,b) = (-1)^{\alpha\beta\epsilon(p)} \left(\frac{u}{p}\right)^\beta \left(\frac{v}{p}\right)^\alpha.$$

(iii) *Si* $\mathbb{K} = \mathbb{Q}_2$, *en écrivant* $a = u2^\alpha$ *et* $b = v2^\beta$ *avec* $u, v \in \mathbf{U}$ *:*

$$(a,b) = (-1)^{\epsilon(u)\epsilon(v) + \beta\omega(u) + \alpha\omega(v)}.$$

Un lemme est nécessaire pour prouver ce théorème dans les deuxième et troisième cas.

Lemme 2.1. *On se place dans $\mathbb{Q}_p$ avec p premier. Soit $u \in \mathbf{U}$. Si $(u,p)=1$, alors $(E_{u,p})$ possède une solution (x,y,z) dans $\mathbb{Z}_p$ vérifiant $x,y \in \mathbf{U}$.*

Démonstration. Par définition du symbole de Hilbert, $(E_{u,p})$ admet une solution non triviale (x,y,z). Quitte à la multiplier par p^{-n} où $n=\min(v_p(x),v_p(y),v_p(z))$, on peut la supposer dans $\mathbb{Z}_p$ et primitive. Montrons alors que x et y sont des unités p-adiques.

Si ce n'est pas le cas, on a $p|x$ ou $p|y$. Or $x^2-uy^2-pz^2=0$, donc $x^2 \equiv uy^2\ [p]$, et on a à la fois $p|x$ et $p|y$. Mais ceci implique $p^2|pz^2$, c'est-à-dire $p|z$: c'est absurde car (x,y,z) est une solution primitive.

□

Passons à la preuve du théorème.

Démonstration.

(i) Ce cas est trivial puisque $\mathbb{R}^{2*}=\mathbb{R}_+^*$.

(ii) Il est clair que l'on n'a besoin de considérer que les résidus de α et β modulo 2, et $(\cdot,\cdot)$ étant symétrique, il reste trois sous-cas à traiter : $\alpha=\beta=0$; $\alpha=0$ et $\beta=1$; $\alpha=\beta=1$.

- Sous-cas $\alpha=\beta=0$. Il s'agit de montrer que $(u,v)=1$. On considère la forme $f=X^2-uY^2-vZ^2$. Vue dans $\mathbb{Z}_p/p\mathbb{Z}_p \simeq \mathbb{F}_p$, f étant de rang 3 elle admet un zéro non trivial par le corollaire du théorème de Chevalley sur les formes quadratiques. Mais le discriminant de f est $uv \in \mathbf{U}$: en appliquant le corollaire 1.3 du lemme de Hensel, la solution modulo p se relève en solution non triviale dans $\mathbb{Z}_p$. Ceci montre que $(u,v)=1$.

- Sous-cas $\alpha=0$, $\beta=1$. Cette fois on souhaite obtenir $(u,pv)=(\frac{u}{p})$. On vient de voir que $(u,v)=1$, d'après la proposition 2.5 il reste à montrer $(u,p)=(\frac{u}{p})$. Si $(\frac{u}{p})=1$, u est un carré et $(u,p)=1$. Si réciproquement $(u,p)=1$, on peut utiliser le lemme : soit (x,y,z) une solution à $(E_{u,p})$ dans $\mathbb{Z}_p$ telle que $x,y \in \mathbf{U}$. On a alors $x^2 \equiv uy^2\ [p]$, et u est un carré : $(\frac{u}{p})=1$.

- Sous-cas $\alpha=\beta=1$. Ici la formule voulue est $(up,vp)=(-1)^{\frac{p-1}{2}}(\frac{uv}{p})$. Calculons :

$$\begin{aligned}(up,vp) &= (up,-uvp^2)\\ &= (up,-uv)\\ &= \left(\frac{-uv}{p}\right) && \text{par le cas précédent}\\ &= (-1)^{\frac{p-1}{2}}\left(\frac{uv}{p}\right).\end{aligned}$$

(iii) La remarque sur les trois cas à traiter demeure.

- Sous-cas $\alpha=\beta=0$. On veut prouver que $(u,v)=\begin{cases}-1 & \text{si } u\equiv v\equiv 3\ [4]\\ 1 & \text{sinon}\end{cases}$. Par symétrie on distingue deux cas : $u\equiv 1\ [4]$ et $u\equiv v\equiv 3\ [4]$.

Si d'abord $u\equiv 1\ [4]$, ou bien $u\equiv 1\ [8]$ et u est un carré d'après le théorème 1.9, et alors $(u,v)=1$; ou bien $u\equiv 5\ [8]$. Dans ce second cas, vu que $4v\equiv 4\ [8]$, $u+4v\equiv 1\ [8]$. Le même théorème permet d'écrire $u+4v=w^2$ avec $w\in\mathbf{U}$, c'est-à-dire que $x^2-uy^2-vz^2$ s'annule en $(w,1,2)$: $(u,v)=1$.

Maintenant, si $u\equiv v\equiv 3\ [4]$, on suppose par l'absurde que l'on dispose d'une solution primitive (x,y,z) à $(E_{u,v})$: alors $x^2+y^2+z^2\equiv 0\ [4]$. Mais x^2 est nécessairement congru à 0 ou à 1 modulo 4, de même pour y^2 et z^2. On en déduit que chacun est congru à 0. Cela signifie que $x\equiv y\equiv z\equiv 0\ [2]$: c'est absurde car notre solution est supposée primitive ! Finalement ici $(u,v)=-1$.

- Sous-cas $\alpha = 0$, $\beta = 1$. Il s'agit de démontrer que $(u, 2v) = (-1)^{\epsilon(u)\epsilon(v)+\omega(u)}$. Commençons par montrer que $(u, 2) = (-1)^{\omega(u)}$, ce qui se reformule $(u, 2) = \begin{cases} 1 & \text{si } u \equiv \pm 1 \ [8] \\ -1 & \text{sinon} \end{cases}$.

Si $u \equiv \pm 1$ [8] : soit $u \equiv 1$ [8], u est un carré et donc $(u, 2) = 1$; soit $u \equiv -1$ [8]. Dans ce cas $(E_{u,v})$ admet $(1, 1, 1)$ comme solution modulo 8. Le corollaire 1.3 du lemme de Hensel permet de conclure que $(u, 2) = 1$.

Réciproquement si $(u, 2) = 1$, le lemme précédant la démonstration donne l'existence de $(x, y, z) \in \mathbb{Z}_p$ avec $x, y \in \mathbf{U}$ tel que $x^2 - uy^2 - 2z^2 = 0$. Ainsi $x^2 \equiv y^2 \equiv 1$ [8], et $1 - u - 2z^2 \equiv 0$ [8]. Or z^2 est congru à 0, 1 ou 4 modulo 8 : en insérant ceci dans la congruence qui précède, on obtient dans les trois cas $u \equiv \pm 1$ [8].

Il reste maintenant à prouver que $(u, 2v) = (u, 2)(u, v)$. La proposition 2.5 permet d'affirmer que c'est vrai quand l'un des deux symboles de droite vaut 1 ; il reste le cas $(u, 2) = (u, v) = -1$. Vu que $(u, 2) = -1$, $u \equiv \pm 3$ [8] ; de plus $(u, v) = -1$ donc $u \equiv v \equiv 3$ [4]. On en déduit que $u \equiv 3$ [8] et que $v \equiv 3$ [8] ou $v \equiv -1$ [8].

Si $v \equiv 3$ [8] on écrit, avec $k \in \mathbb{Z}_p$: $v = 3 + 8k = 3\left(1 + 8\frac{k}{3}\right)$; or $1 + 8\frac{k}{3} \equiv 1$ [8] donc le facteur de gauche est un carré : on peut supposer $v = 3$. Alors on écrit de même, avec $l \in \mathbb{Z}_p$, $u = -5 + 8l = -5\left(1 - 8\frac{l}{5}\right)$: pour la même raison on peut supposer $u = -5$. Mais $(-5, 6) = 1$: en effet, $(1, 1, 1)$ est solution de $(E_{-5,6})$: $x^2 + 5y^2 - 6z^2$.

Si $v \equiv -1$ [8] le même raisonnement montre que l'on peut remplacer v par -1. Cette fois on choisit de remplacer u par 3. Là encore $(3, -2) = 1$, car $(1, 1, 1)$ est solution de $(E_{3,-2})$: $x^2 - 3y^2 + 2z^2$.

- Sous-cas $\alpha = \beta = 1$. Dans cette dernière situation, il s'agit de montrer que $(2u, 2v) = (-1)^{\epsilon(u)\epsilon(v)+\omega(u)+\omega(v)}$. On a $(2u, 2v) = (2u, -4uv) = (2u, -uv) = (-1)^{\epsilon(u)\epsilon(-uv)+\omega(-uv)}$ (la dernière égalité provient du cas précédent). D'une part $\epsilon(u)\epsilon(-uv) = \epsilon(u)(\epsilon(-1) + \epsilon(u) + \epsilon(v)) = \epsilon(u) + \epsilon(u)^2 + \epsilon(u)\epsilon(v) \equiv \epsilon(u)\epsilon(v)$ [2] ; d'autre part $\omega(-uv) = \omega(-1) + \omega(u) + \omega(v) = \omega(u) + \omega(v)$. Ceci conclut ce sous-cas, et du même coup la preuve de ce théorème.

□

On rappelle désormais que tout groupe abélien dont les éléments sont tous d'ordre 1 ou 2 peut être muni d'une structure de $\mathbb{F}_2$-espace vectoriel (la loi interne étant la loi de groupe, et la loi externe étant l'exponentiation). Le groupe $\mathbb{K}^*/\mathbb{K}^{2*}$ vérifie la condition : on le munit d'une telle structure.

Théorème 2.5. *Le symbole de Hilbert $(\cdot, \cdot)$ est une forme bilinéaire non dégénérée sur le $\mathbb{F}_2$-espace vectoriel $\mathbb{K}^*/\mathbb{K}^{2*}$.*

Voir $\mathbb{K}^*/\mathbb{K}^{2*}$ comme un espace vectoriel permet une écriture simple de ce théorème, mais on peut aussi le reformuler comme ceci : $(aa', b) = (a, b)(a', b)$ pour tous $a, a', b \in \mathbb{K}^*$; et si $a \in \mathbb{K}^*$ vérifie $\forall b \in \mathbb{K}^*, (a, b) = 1$, alors a est un carré dans $\mathbb{K}$.

Démonstration. - Cas $\mathbb{K} = \mathbb{R}$. Une suite d'équivalences démontre la bilinéarité :

$$\begin{aligned}(a, b)(a', b) = 1 &\Leftrightarrow (a, b) = (a', b) = 1 \text{ ou } (a, b) = (a', b) = -1 \\ &\Leftrightarrow (a, a' > 0 \text{ ou } b > 0) \text{ ou } (a, a', b < 0) \\ &\Leftrightarrow a, a' > 0 \text{ ou } b > 0 \text{ ou } a, a' < 0 \\ &\Leftrightarrow aa' > 0 \text{ ou } b > 0 \\ &\Leftrightarrow (aa', b) = 1.\end{aligned}$$

De plus si $a \in \mathbb{R}^*$ est tel que pour tout $b \in \mathbb{R}^*$, $(a, b) = 1$, alors $(a, -1) = 1$ et $a > 0$, ce qui signifie bien que $a \in \mathbb{K}^{2*}$.

- Cas $\mathbb{K} = \mathbb{Q}_p$ avec $p \neq 2$ premier. La bilinéarité découle de la formule du théorème précédent. Soit $a \in \mathbb{K}^*$ non carré : trouvons $b \in \mathbb{K}^*$ tel que $(a, b) = -1$. On a vu dans le corollaire 1.4 (au théorème 1.8) que $\mathbb{Q}_p^*/\mathbb{Q}_p^{2*} \simeq \mathbb{F}_2^2$, et que l'on peut prendre comme représentants dans $\mathbb{Q}_p^*$ $\{1, u, p, up\}$ avec $u \in \mathbf{U}$

vérifiant $(\frac{u}{p}) = -1$. a est donc, à multiplication par un carré près, u, p ou up. On peut alors prendre pour b respectivement p, u et u (en effet on voit facilement que (u,p), (p,u) et (up,u) valent -1).

- Cas $\mathbb{K} = \mathbb{Q}_2$. Là encore la bilinéarité s'obtient par le théorème précédent, et il s'agit de prendre $a \in \mathbb{K}^*$ non carré et de trouver $b \in \mathbb{K}^*$ tel que $(a,b) = -1$. Cette fois d'après le corollaire 1.5 (au théorème 1.9) $\mathbb{Q}_2^*/\mathbb{Q}_2^{2*} \simeq \mathbb{F}_2^3$, avec les représentants $\{\pm 1, \pm 5, \pm 2, \pm 10\}$. Pour $a = 2u$ avec $u \in \{\pm 1, \pm 5\}$, $b = 5$ convient car $(2u,5) = (-1)^{\epsilon(u)\epsilon(5)+\omega(5)} = (-1)^{0+1} = -1$. Ceci montre aussi que pour $a = 5$, $b = 2$ convient. Enfin si $a \in \{-1,-5\}$, $\epsilon(a) = 1$ et $b = -1$ convient : $(a,-1) = (-1)^{\epsilon(u)\epsilon(-1)} = -1$.

□

Corollaire 2.1. *Si $b \in \mathbb{K}^*$ n'est pas un carré, le sous-groupe $\mathrm{N}\mathbb{K}_b^*$ de $\mathbb{K}^*$ est d'indice 2.*

Démonstration. Posons $\varphi_b : \left\{ \begin{array}{ccc} \mathbb{K}^* & \to & \{-1,1\} \\ a & \mapsto & (a,b) \end{array} \right.$. C'est un morphisme de groupes, qui est surjectif vu que $(\cdot,\cdot)$ est non dégénéré. De plus d'après la proposition 2.4, $\mathrm{Ker}\varphi_b = \mathrm{N}\mathbb{K}_b^*$. Le théorème de factorisation donne $\mathbb{K}^*/\mathrm{N}\mathbb{K}_b^* \simeq \{-1,1\}$.

□

2.3.2 Propriétés globales

Soit $v \in \mathbf{V}$. Si $a,b \in \mathbb{Q}^*$, on peut les considérer dans $\mathbb{Q}_v$, et donc considérer leur symbole de Hilbert relativement à $\mathbb{Q}_v$. Pour pouvoir se placer dans plusieurs $v \in \mathbf{V}$ à la fois, on note ce symbole $(a,b)_v$.

Dans la suite, si E est un ensemble dénombrable, par "pour presque tout $e \in E$", on entend "pour tout $e \in E$ sauf un nombre fini".

Théorème 2.6 (Formule du produit de Hilbert)**.** *Soient $a,b \in \mathbb{Q}^*$. Pour presque tout $v \in \mathbf{V}$, $(a,b)_v = 1$. De plus :*

$$\prod_{v \in \mathbf{V}} (a,b)_v = 1.$$

Démonstration. Par bilinéarité il suffit de montrer le théorème pour $a,b \in \{-1\} \cup \mathbf{P}$. On utilise systématiquement les formules du théorème 2.4.

Si $a = b = -1$: pour $v \neq 2$ premier, $(-1,-1)_v = 1$, et $(-1,-1)_2 = (-1,-1)_\infty = -1$.

Si $a = -1$ et $b = 2$: $(-1,2)_v = 1$ pour tout $v \in \mathbf{V}$.

Si $a = -1$ et $b \neq 2$ premier : pour $v \notin \{2,b\}$, $(-1,b)_v = 1$; de plus $(-1,-1)_2 = (-1,-1)_b = (-1)^{\epsilon(b)}$.

Si $a = b$ premier : pour tout $v \in \mathbf{V}$, $(a,a)_v = (-1,a)_v$; on se ramène aux cas précédents.

Si $a = 2$ et $b \neq 2$ premier : pour $v \notin \{2,b\}$, $(2,b)_v = 1$; en outre $(2,b)_2 = (-1)^{\omega(b)}$ et $(2,b)_b = (\frac{2}{b}) = (-1)^{\omega(b)}$.

Si $a \neq b$ premiers différents de 2 : pour $v \notin \{2,a,b\}$, $(a,b)_v = 1$. Les autres symboles sont $(a,b)_2 = (-1)^{\epsilon(a)\epsilon(b)}$, $(a,b)_a = (\frac{b}{a})$, $(a,b)_b = (\frac{a}{b})$. La loi de réciprocité quadratique permet de conclure.

□

Concluons cette discussion sur le symbole de Hilbert par le théorème suivant, qui donne une condition nécessaire et suffisante quant à l'existence d'un $x \in \mathbb{Q}$ de symboles de Hilbert fixés. Il sera utile pour montrer le théorème de Hasse-Minkowski.

Théorème 2.7. *Soient I un ensemble fini, $(a_i)_{i\in I} \in (\mathbb{Q}^*)^I$, $(\varepsilon_{i,v})_{(i,v)\in I\times\mathbf{V}} \in \{-1,1\}^{I\times\mathbf{V}}$. Il existe $x \in \mathbb{Q}^*$ vérifiant $\forall (i,v) \in I\times\mathbf{V}, (a_i,x)_v = \varepsilon_{i,v}$ si et seulement si les trois conditions suivantes sont satisfaites :*

(i) *pour presque tout $(i,v) \in I\times\mathbf{V}$, $\varepsilon_{i,v} = 1$*

(ii) *pour tout $i \in I$, $\prod_{v\in\mathbf{V}} \varepsilon_{i,v} = 1$*

(iii) *pour tout $v \in \mathbf{V}$ il existe $x_v \in \mathbb{Q}_v^*$ tel que $\forall i \in I, (a_i,x_v)_v = \varepsilon_{i,v}$.*

Démonstration. Le sens direct se déduit du théorème précédent pour (i) et (ii), et est trivial pour (iii). Montrons la réciproque. On suppose que l'on dispose de $(a_i)_{i\in I} \in (\mathbb{Q}^*)^I$, $(\varepsilon_{i,v})_{(i,v)\in I\times\mathbf{V}} \in \{-1,1\}^{I\times\mathbf{V}}$ et $(x_v)_{v\in\mathbf{V}} \in \prod_{v\in\mathbf{V}} \mathbb{Q}_v^*$ satisfaisant les trois conditions ; quitte à multiplier les a_i par des carrés d'entiers on peut supposer qu'ils sont eux-mêmes entiers non nuls. On définit les deux parties de $\mathbf{V}$ suivantes (elles sont finies par hypothèse) :

$$S = \{2,\infty\} \cup \left\{p \in \mathbf{P} \middle| \exists i \in I,\ p|a_i\right\}$$
$$T = \{v \in \mathbf{V} | \exists i \in I,\ \varepsilon_{i,v} = -1\}.$$

- Cas $S\cap T = \varnothing$. On traite en premier lieu ce cas particulier, qui nous permettra ensuite de démontrer le cas général. Définissons deux entiers positifs :

$$\sigma = 8 \prod_{\substack{s\in S\\ s\neq 2\\ s\neq\infty}} s \quad \text{et} \quad \tau = \prod_{\substack{t\in T\\ t\neq\infty}} t\,.$$

Puisque l'on suppose S et T disjoints, σ et τ sont premiers entre eux. Le théorème de progression arithmétique de Dirichlet indique alors que l'ensemble $\left\{p \in \mathbf{P} \;\middle|\; p \equiv \tau\ [\sigma]\right\}$ est infini. $S\cup T$ étant au contraire fini, on peut choisir $q \in \mathbf{P}\setminus(S\cup T)$ tel que $q \equiv \tau\ [\sigma]$. Posons maintenant $x = \tau q$: nous allons prouver que ce x convient. Soient $i \in I$ et $v \in \mathbf{V}$.

Si $v \in S$, $v \notin T$ donc $\varepsilon_{i,v} = 1$. Montrons que $(a_i,x)_v = 1$; il suffit d'obtenir que x est un carré dans $\mathbb{Q}_v^*$. Si $v = \infty$ c'est vrai car $x > 0$. Sinon, notons d'abord que $x \in \mathbf{U}$ et que $x \equiv \tau^2\ [\sigma]$. Pour $v = 2$, $x \equiv \tau^2\ [8]$. Comme $2 \in S$, $2 \notin T$ et $2 \nmid \tau$. Ceci implique $x \equiv 1\ [8]$, et le théorème 1.9 de caractérisation des carrés de $\mathbb{Q}_2^*$ permet de conclure. Pour $v \neq 2$, $x \equiv \tau^2\ [v]$, ce qui se réécrit $x = \tau^2(1 + v\frac{k}{\tau^2})$ avec $k \in \mathbb{Z}_v$. $v \in S$ donc $v \notin T$ et $v \nmid \tau$, d'où $\frac{k}{\tau^2} \in \mathbb{Z}_v$: le théorème 1.8 de caractérisation des carrés de $\mathbb{Q}_p^*$ pour $p \neq 2$ entraîne que x est un carré dans $\mathbb{Q}_v^*$.

Si $v \notin S$, on a $v \nmid a_i$ donc $a_i \in \mathbf{U}$; de plus $v \neq 2$ donc $(a_i,b)_v = (\frac{a_i}{v})^{v_v(b)}$ pour $b \in \mathbb{Q}_v^*$. Si $v \notin T\cup\{q\}$, d'une part $\varepsilon_{i,v} = 1$, et d'autre part $v_v(x) = 0$ donc $(a_i,x)_v = 1$. Si $v \in T$, $v_v(x) = 1$ et on peut prendre $j \in I$ tel que $\varepsilon_{j,v} = -1$. Mais alors $(\frac{a_j}{v})^{v_v(x_v)} = -1$, ce qui impose $v_v(x_v) \equiv 1\ [2]$. On en déduit que $(a_i,x)_v = (\frac{a_i}{v}) = (a_i,x_v)_v = \varepsilon_{i,v}$. Si enfin $v = q$, la formule du produit, les cas précédents et l'hypothèse (ii) donnent le résultat :

$$(a_i,x)_q = \prod_{v\neq q} (a_i,x)_v = \prod_{v\neq q} \varepsilon_{i,v} = \varepsilon_{i,q}.$$

- Cas général. Comme $\mathbb{Q}_s^{2*}$ est un ouvert de $\mathbb{Q}_s^*$ pour $s \in S$, $\prod_{s\in S} x_s\mathbb{Q}_s^{2*}$ est ouvert dans $\prod_{s\in S}\mathbb{Q}_s^*$. Or le principe d'approximation faible indique que l'image du plongement naturel de $\mathbb{Q}^*$ dans ce dernier produit est dense : elle intersecte donc le premier produit. Ainsi on prend $y \in \mathbb{Q}^*$ tel que pour tout $s \in S$, $y \in x_s\mathbb{Q}_s^{2*}$; alors $(a_i,y)_s = (a_i,x_s)_s = \varepsilon_{i,s}$ pour $i \in I$.

On pose maintenant, pour $(i,v) \in I\times\mathbf{V}$, $\eta_{i,v} = \varepsilon_{i,v}(a_i,y)_v$. Cette famille, jointe à $(a_i)_{i\in I}$, vérifie les hypothèses (i), (ii) et (iii) ; de plus si $i \in I$ et $s \in S$ alors $\eta_{i,s} = 1$. On peut donc lui appliquer le cas particulier précédent : soit $y' \in \mathbb{Q}^*$ vérifiant $(a_i,y')_v = \eta_{i,v}$ pour tout $(i,v) \in I\times\mathbf{V}$. Pour finir on pose $x = yy'$: il convient pour notre famille $(\varepsilon_{i,v})_{(i,v)\in I\times\mathbf{V}}$ (en effet pour $(i,v) \in I\times\mathbf{V}$: $(a_i,x)_v = (a_i,y)_v\eta_{i,v} = \varepsilon_{i,v}$). □

2.4 Représentation sur $\mathbb{Q}_p$

On fixe un $p \in \mathbf{P}$. On veut trouver une condition nécessaire et suffisante sur une forme quadratique f pour dire si elle représente 0 sur $\mathbb{Q}_p$ ou non. Pour y arriver nous allons introduire deux objets qui nous donnerons les conditions voulues sur f pour qu'elle représente 0. Le travail qui suit va d'abord être de constater que ces deux objets sont des *invariants* de la classe d'équivalence de f. Ainsi on pourra se ramener à $f \sim a_1X_1^2 + \cdots + a_nX_n^2$ pour démontrer le théorème voulu. On note $\mathbb{K} = \mathbb{Q}_p$.

On considérons une forme quadratique f non dégénérée sur E de dimension n. Le premier invariant est le discriminant $d(f)$ que l'on voit comme élément de $\mathbb{K}/\mathbb{K}^{2*}$. On a déjà vu (à la suite du théorème 2.2) que $d(f)$ ne dépend pas de la classe de f si on le voit dans $\mathbb{K}/\mathbb{K}^{2*}$ (c'est-à-dire de la base dans laquelle on regarde la matrice de f), et qu'on peut l'obtenir par $d(f) = e_1.e_1 \cdots e_n.e_n$ pour $(e_i)_i$ une base orthogonale de E.

Tout le travail va alors être de construire le second invariant, nous suivrons alors le cheminement exposé dans le *Cours d'arithmétique* de Jean-Pierre Serre.On construit cet invariant d'abord à partir des base orthogonales (relativement à f) :

Définition 2.11. *On pose* $\mathbf{e}(B) = \prod_{i<j}(a_i, a_j)$ *si* $B = (e_1, \cdots, e_n)$ *est une base orthogonale de* E *et* $a_i = e_i.e_i$.

On constate que c'est un élément de $\{-1, +1\}$. Le fait que cet objet ne dépende pas de la classe d'équivalence de f découle directement du théorème suivant :

Théorème 2.8. $\mathbf{e}(B)$ *ne dépend pas de la base orthogonale* B.

Démonstration. Distinguons deux cas :

Cas n=1 : Si $n = 1$ le produit est vide donc pour toute base $\mathbf{e}(B) = 1$.

Cas n≥2 : On procède par récurrence sur n. Montrons le résultat pour $n = 2$. On note $B = (e_1, e_2)$ et $a_i = e_i.e_i$. Ainsi $\mathbf{e}(B) = (a_1, a_2)$. Donc si $\mathbf{e}(B) = 1$, on a $(x, y, z) \in \mathbb{K}$ non nul, tel que $x^2 - a_1y^2 - a_2z^2 = 0$, c'est à dire $x^2 = a_1y^2 + a_2z^2$. Si $x^2 = 0$ la forme quadratique $q = a_1X_1^2 + a_2X_2^2$ représente 0. Et sinon, $x^2 \neq 0$ donc $1 = a_1\frac{y^2}{x^2} + a_2\frac{z^2}{x^2}$ et q représente 1. On a alors que $\mathbf{e}(B) = 1$ si et seulement si q représente 1 ou 0 (la réciproque étant évidente). Or cette condition nécessaire et suffisante ne dépend pas de la base choisi. D'où le cas $n = 2$.

Maintenant on peut supposer $n \geq 3$. Soit $B = (e_1, \cdots, e_n)$ et $B' = (e'_1, \cdots, e'_n)$ deux bases orthogonales. Supposons dans un premier temps que B et B' soient contiguë. Quitte à permuter l'ordre des éléments des bases on peut supposer que $e_1 = e'_1$ car le symbole de Hilbert est symétrique. Notons $a_i = e_i.e_i$ et $a'_i = e'_i.e'_i$. On a alors

$$\begin{aligned}\mathbf{e}(B) &= (a_1, a_2 \cdots a_n) \prod_{2\leq i<j} (a_i, a_j) && \text{par multiplicativité du symbole de Hilbert}\\ &= (a_1, a_1 d(f)) \prod_{2\leq i<j} (a_i, a_j) && \text{car dans } \mathbb{K}/\mathbb{K}^{2*},\ a_2 \cdots a_n = a_1^{-1}a_1a_2 \cdots a_n = a_1^{-1}d(f) = a_1^2a_1^{-1}d(f) = a_1d(f)\end{aligned}$$

De même on a $\mathbf{e}(B') = (a'_1, a'_1d(f)) \prod_{2\leq i<j} (a'_i, a'_j) = (a_1, a_1d(f)) \prod_{2\leq i<j} (a'_i, a'_j)$. On applique alors l'hypothèse de récurrence à $(e_2, \cdots e_n)$ et $(e'_2, \cdots, e'_n)$ et on a $\prod_{2\leq i<j} (a_i, a_j) = \prod_{2\leq i<j} (a'_i, a'_j)$ d'où l'égalité $\mathbf{e}(B) = \mathbf{e}(B')$.

Si maintenant B et B' ne sont pas contiguë, on sait néanmoins qu'il existe une chaîne de base orthogonale contiguë reliant les deux. Ainsi par ce qu'on vient de démontrer B et B' satisfont le théorème. □

De ceci on peut tirer la conclusion voulue. Si $f \sim a_1X_1^2 + \cdots + a_nX_n^2$ non dégénérée, alors les objets $d(f) = a_1 \cdots a_n$ (vu dans le quotient) et $\mathbf{e}(f) = \prod_{i<j}(a_i, a_j)$ sont bien définis et ne dépendent pas de la classe d'équivalence de f.

2.5 Théorème de Hasse Minkowski

Dans cette partie, on démontre le théorème de Hasse Minkowski. Si f est une forme quadratique sur $\mathbb{Q}$, pour $v \in \mathbf{V}$ on note f_v la forme quadratique sur $\mathbb{Q}_v$ dont les coefficients sont les images de ceux de f par l'injection de $\mathbb{Q}$ dans $\mathbb{Q}_v$.

Avant d'énoncer le théorème, nous allons donner deux petits lemmes qui nous serviront lors de la preuve. Le premier est un calcul de symbole de Hilbert.

Lemme 2.2. *Soit $v \in \mathbf{V}$, soient a, b et x dans $\mathbb{Q}_v^*$. La forme $aX^2 + bY^2 - xZ^2$ représente 0 si et seulement si $(x, -ab)_v = (a, b)_v$.*

Démonstration. $aX^2 + bY^2 - xZ^2$ représente 0 si et seulement si $Z^2 - \frac{a}{x}X^2 - \frac{b}{x}Y^2$ représente 0, c'est-à-dire par définition du symbole de Hilbert si et seulement si $\left(\frac{a}{x}, \frac{b}{x}\right)_v = 1$. Or : $\left(\frac{a}{x}, \frac{b}{x}\right)_v = (ax, bx)_v = (a, b)_v(x, b)_v(ax, x)_v = (a, b)_v(x, b)_v(x, -a)_v = (a, b)_v(x, -ab)_v$. □

Le second est purement calculatoire.

Lemme 2.3. *Si $|.|$ est une norme et que l'on a $|b - a| < \epsilon$, Alors $|b^2 - a^2| < \epsilon(2|a| + \epsilon)$*

Démonstration. On écrit $b = a + c$ avec par hypothèse $|c| < \epsilon$. Alors

$$|b^2 - a^2| = |a^2 + 2ac + c^2 - a^2| = |2ac + c^2| = |c||2a + c| < \epsilon\,(2|a| + |c|) < \epsilon\,(2|a| + \epsilon)\,.$$

□

Théorème 2.9 (de Hasse-Minkowski)**.** *Pour que f représente 0 sur $\mathbb{Q}$, il faut et il suffit que, pour tout $v \in V$, la forme f_v représente 0 sur $\mathbb{Q}_v$.*

Démonstration. le sens direct est immédiat via l'injection de $\mathbb{Q}$ dans chaque $\mathbb{Q}_v$.

Pour le sens indirect, on pose n le nombre de variables prises par f et on distingue les cas $n = 2, 3, 4$ et $n \geq 5$.

Cas n=2.
On peut supposer grâce au théorème 2.2 que $f = X_1^2 - aX_2^2$. Comme f représente 0 sur $\mathbb{R}$, $a > 0$. On peut alors écrire $a = \prod_{p \in \mathbf{P}} p^{v_p(a)}$.

Soit $p \in \mathbb{P}$. Par hypothèse il existe un couple $(x_1^p, x_2^p) \in {\mathbb{Q}_p}^2$ non nul tel que $(x_1^p)^2 = a(x_2^p)^2$. Comme $a > 0$ on a même x_1^p et x_2^p tous deux non nuls, et alors $a = (\frac{x_1^p}{x_2^p})^2$ est un carré dans $\mathbb{Q}_p$. Or si on écrit $\frac{x_1^p}{x_2^p} = p^\beta v$ avec $\beta = v_p(\frac{x_1^p}{x_2^p})$ et $v \in \mathbf{U}$, on a $a = p^{2\beta}v^2$. Or v^2 est encore une unité p-adique donc $v_p(a) = 2\beta$ est pair.

Ainsi pour tout $p \in \mathbf{P}$, $v_p(a)$ est pair : a est bien un carré dans $\mathbb{Q}$. $(\sqrt{a}, 1) \in \mathbb{Q}^2$ est alors une solution non triviale à l'équation $f = 0$, et f représente 0 sur $\mathbb{Q}$.

Cas n=3.
Toujours par le théorème 2.2, on peut supposer que $f = cX_1^2 - aX_2^2 - bX_3^2$, et on peut supposer que $c = 1$ quitte à remplacer f par $c^{-1}f$.

On peut aussi supposer quitte à multiplier a et b par des carrés de rationnels que a et b sont des entiers sans facteurs carrés et on suppose enfin que $|a| < |b|$.
On raisonne alors par récurrence sur l'entier $m = |a| + |b|$. Dans le cas $m = 2$, on a $f = X_1^2 \pm X_2^2 \pm X_3^2$. le cas $f = X_1^2 + X_2^2 + X_3^2$ est impossible car f_∞ doit représenter 0, dans les autres cas f représente 0 dans $\mathbb{Q}$. Si $m > 2$, on a $|b| \geq 2$, on écrit $b = \pm p_1 \cdots p_r$, où les p_i sont deux-à-deux distincts. Soit p l'un des p_i.
Montrons alors que a est un carré modulo p.
Si $a \equiv 0\ [p]$ alors c'est bon. Sinon par hypothèse, il existe $(x, y, z) \in {\mathbb{Q}_p}^3$ tels que $z^2 - ax^2 - by^2 = 0$.
On peut de plus supposer que (x, y, z) est un élément primitif de $\mathbb{Z}_p$ (en effet en notant $h = \inf(v_p(x), v_p(y), v_p(z))$ et en prenant $p^{-h}(x, y, z)$, c'est toujours une solution, mais primitive et dans $\mathbb{Z}_p$).
On a $z^2 - ax^2 \equiv 0\ [p]$. Si $x \equiv 0\ [p]$, alors $z^2 \equiv 0 \mod p$. De là, $z^2 - ax^2 = by^2$ donc by^2 est divisible par p^2, or $v_p(b) = 1$ donc nécessairement $y^2 \equiv 0\ [p]$, ce qui contredit le fait que (x, y, z) est primitif.
Donc $x \not\equiv 0\ [0]$ et $a \equiv (zx^{-1})^2 \mod p$: a est un carré modulo p pour tout p divisant b.
Par le théorème des restes chinois, $\mathbb{Z}/b\mathbb{Z} = \prod_{i=1}^{r} \mathbb{Z}/p_i\mathbb{Z}$ donc a est un carré modulo b. Donc il existe t et b' des entiers tels que : $t^2 = a + bb'$, et on peut choisir t de sorte que $|t| \leq |b|/2$.
L'expression $bb' = t^2 - a$ montre que bb' est la norme d'un élément de $k(\sqrt{a})$ où $k = \mathbb{Q}$ ou $\mathbb{Q}_v$. Donc, par la proposition 2.4, on a $(a, bb') = 1$. Or $(a, bb') = (a, b)(a, b')$, donc $(a, b) = (a, b')$. Ce qui signifie que f représente 0 dans k si et seulement si $f' = X_1^2 - aX_2^2 - b'X_3^2$ représente 0 dans k.
En particulier, f' représente 0 dans chacun des $\mathbb{Q}_v$. De plus :

$$|b'| = \left|\frac{t^2-a}{b}\right| \leq \left|\frac{t^2}{b}\right| + \left|\frac{a}{b}\right| \leq \frac{|b|}{4} + 1 < |b| \quad \text{car } |b| \geq 2.$$

En écrivant $b' = b''u^2$ où b'', u sont des entiers et b'' est sans facteurs carrés et $|b''| < |b|$, enfin la forme f' est équivalente à la forme $f'' = X_1^2 - aX_2^2 - b''X_3^2$ à laquelle on peut appliquer l'hypothèse de récurrence pour établir que f'' représente 0 et donc que f représente 0 aussi.

Cas n=4.

On écrit $f = aX_1^2 + bX_2^2 - (cX_3^2 + dX_4^2)$. Soit $v \in \mathbf{V}$. f_v représente 0 donc la proposition 2.2 donne $x_v \in \mathbb{Q}_v^*$ représenté à la fois par $aX_1^2 + bX_2^2$ et $cX_3^2 + dX_4^2$. Alors $aX_1^2 + bX_2^2 - x_vZ^2$ et $cX_3^2 + dX_4^2 - x_vZ^2$ représentent 0 sur $\mathbb{Q}_v^*$ et on applique le premier lemme : $(x_v, -ab)_v = (a, b)_v$ et $(x_v, -cd)_v = (c, d)_v$.

Les conditions sont réunies pour appliquer le théorème 2.7 avec $a_1 = -ab$, $a_2 = -cd$, $\varepsilon_{1,v} = (a, b)_v$, $\varepsilon_{2,v} = (c, d)_v$ pour $v \in \mathbf{V}$. Soit $x \in \mathbb{Q}^*$ tel que pour tout $v \in \mathbf{V}$, $(x, -ab)_v = (a, b)_v$ et $(x, -cd)_v = (c, d)_v$. On utilise à nouveau le premier lemme, mais dans l'autre sens : pour tout $v \in \mathbf{V}$, $aX_1^2 + bX_2^2 - xZ^2$ et $cX_3^2 + dX_4^2 - xZ^2$ représentent 0 sur $\mathbb{Q}_v$. En appliquant le cas $n = 3$ qui précède on voit que les deux formes représentent 0 sur $\mathbb{Q}$, c'est-à-dire d'après la proposition 2.3 que $aX_1^2 + bX_2^2$ et $cX_3^2 + dX_4^2$ représentent x sur $\mathbb{Q}$: finalement f représente 0 sur $\mathbb{Q}$.

Cas n $\geq$ 5. On procède maintenant par récurrence sur n, l'initialisation étant le cas précédent. On peut supposer $f = \sum a_iX_i^2$, et on la met sous la forme

$$f(X_1, \cdots, X_n) = h(X_1, X_2) - g(X_3, \cdots, X_n)$$

avec $h = a_1X_1^2 + a_2X_2^2$ et $g = -(a_3X_3^2 + \cdots + a_nX_n^2)$. On note $S = \{2, \infty\} \cup \{p \in \mathbf{P} \mid \exists\, i \geq 3,\ v_p(a_i) \neq 0\}$, qui est fini car on a un nombre fini de a_i. Soit $v \in S$, on sait par hypothèse que f_v représente 0, donc que g et h représentent un même élément non nul par la proposition 2.2. Donc il existe $a_v \in \mathbb{Q}_v^*$ et $x_1^v, \cdots, x_n^v \in \mathbb{Q}_v$ tels que

$$h(x_1^v, x_2^v) = a_v = g(x_3^v, \cdots, x_n^v).$$

Nous allons montrer qu'il existe $x_1, x_2 \in \mathbb{Q}$ tels que $\frac{h(x_1,x_2)}{a_v} \in \mathbb{Q}_p^{2*}$. D'une part on remarque que $\frac{h(x_1^v,x_2^v)}{a_v} = 1$ et donc que $\frac{h(x_1^v,x_2^v)}{a_v} \in \mathbb{Q}_p^{2*}$. Or le sous-groupe des carrés est un ouvert de $\mathbb{Q}_p^*$, il existe donc un $\epsilon > 0$ tel que pour tout $x \in \mathbb{Q}_p^*$ tel que si $\left|x - \frac{h(x_1^v,x_2^v)}{a_v}\right|_p < \epsilon$ alors $x \in \mathbb{Q}_p^{2*}$. D'autre part grâce au

principe d'approximation faible, on peut trouver $x_1, x_2 \in \mathbb{Q}$ tels que $|x_i - x_i^v|_v < \mu$ pour chaque $v \in S$ et $i = 1, 2$ et $\mu > 0$ une constante assez petite bien choisie. Le calcul suivant nous éclairera sur la valeur à prendre pour μ. On a :

$$\begin{aligned}
\left|\frac{h(x_1^v, x_2^v)}{a_v} - \frac{h(x_1, x_2)}{a_v}\right|_v &= \left|\frac{a_1}{a_v}((x_1^v)^2 - x_1^2) + \frac{a_2}{a_v}((x_2^v)^2 - x_2^2)\right|_v \\
&\leq k\ \left(|(x_1^v)^2 - x_1^2|_v + |(x_2^v)^2 - x_2^2|_v\right) && \text{avec } k = \max\left(\left|\frac{a_1}{a_v}\right|_v, \left|\frac{a_2}{a_v}\right|_v\right) \\
&\leq k\, 2\mu\, (2|x_1^v|_v + 2|x_2^v|_v + 2\mu) && \text{par application du second lemme} \\
&\leq 4k\mu(N_v + \mu) && \text{avec } N_v = |x_1^v| + |x_2^v|.
\end{aligned}$$

On veut alors choisir $\mu > 0$ racine de $P = 4kX(N_v + X) - \epsilon$. C'est possible car il s'agit d'un trinôme du second degré de discriminant $\Delta = 16k^2N_v^2 + 16k\epsilon$ positif, et tel que $-4kN_v + \sqrt{\Delta} > 0$ car $16k\epsilon > 0$. Ainsi le trinôme P admet une racine positive, que l'on notera μ. En reportant dans notre calcul plus haut on trouve :

$$\left|\frac{h(x_1^v, x_2^v)}{a_v} - \frac{h(x_1, x_2)}{a_v}\right|_v \leq 4k\mu(N_v + \mu) \leq \epsilon \quad \text{par définition de } \mu.$$

D'après notre première remarque on a trouvé $x_1, x_2 \in \mathbb{Q}$ tels que $\frac{h(x_1,x_2)}{a_v} \in \mathbb{Q}_p^{2*}$. On notera $a = h(x_1, x_2)$ dans la suite. Considérons la forme quadratique :

$$f_1(Z, X_3, \cdots X_n) = aZ^2 - g(X_3, \cdots, X_n).$$

L'objectif est maintenant de montrer que f_1 représente 0 dans $\mathbb{Q}_v$ pour tout $v \in \mathbf{V}$, pour pouvoir appliquer l'hypothèse de récurrence.

Cas $v \in S$. On sait que g représente a_v, donc comme $\frac{a}{a_v} \in \mathbb{Q}_p^{2*}$, g représente aussi a. Donc il est clair que f_1 représente 0 dans $\mathbb{Q}_v$.

Cas $v \notin S$. En particulier $v \neq \infty$, alors par application du corollaire au théorème de Chevalley (décrit dans l'annexe) on obtient une solution approchée non triviale x' de g dans $\mathbb{Z}/v\mathbb{Z}$. De plus par définition de S on a $v_v(a_i) = 0$ pour $i \geq 3$, donc ces derniers sont dans $\mathbb{Z}_v \setminus \{0\}$, et on sait que $d_v(g) = a_1 \cdots a_n$ est non nul donc inversible (si on écrit $g = \sum c_{ij}X_iX_j$ et $c_{ij} = c_{ji}$ alors $\det(c_{ij}) = a_1 \cdots a_n$). Ainsi par le corollaire au lemme de Hensel on peut relever cette solution approchée x' en une solution exacte de g dans $\mathbb{Z}_v$, donc dans $\mathbb{Q}_v$. g représente 0 dans $\mathbb{Q}_p$, et f_1 aussi.

Finalement dans tous les cas f_1 représente 0 dans $\mathbb{Q}_v$, et par hypothèse de récurrence (f_1 est de rang $n - 1$) on sait que f_1 représente 0 dans $\mathbb{Q}$. Ainsi g représente a dans $\mathbb{Q}$, et comme $a = h(x_1, x_2)$ avec $x_1, x_2 \in \mathbb{Q}$, f représente bien 0 dans $\mathbb{Q}$.

□

3 Contre exemple en degré supérieur

3.1 Contre-exemple de Selmer

Nous avons vu que le théorème de Hasse-Minkowski nous permet de passer de l'existence de solutions sur les complétés de $\mathbb{Q}$ à une solution sur $\mathbb{Q}$ directement. Cela s'appelle un passage du local au global, les $\mathbb{Q}_v$ étant les corps locaux, et $\mathbb{Q}$ le corps global. Il est légitime de se demander jusqu'où nous pouvons pousser ce principe : toutes les équations polynomiales vérifient-elles le principe local global ?

Malheureusement on connaît des contre-exemples, ce qui confirme que le principe local-global est relativement fin. L'un des plus connus est dû à Ernst Sejersted Selmer, il s'agit de l'équation :

$$3x^3 + 4y^3 + 5z^3 = 0. \tag{1}$$

Pour étudier cette équation, nous allons voir dans un premier temps qu'elle admet des solutions non triviales dans chaque $\mathbb{Q}_v$, c'est à dire toutes les solutions locales. Mais dans un second temps nous verrons qu'elle n'admet pas de solution dans $\mathbb{Q}$ autre que 0.

3.1.1 Existence de solutions locales

Premièrement on remarque que $(-1, \sqrt[3]{\frac{3}{4}}, 0)$ convient comme solution réelle. Pour trouver des solutions sur les autres $\mathbb{Q}_p$ nous allons dans un premier temps trouver des solutions modulo p, puis les relever par le lemme de Hensel. Séparons trois cas : $p = 3, 5$ et le reste.

Plaçons nous dans $\mathbb{Q}_3$. On démarre comme dans le cas réel par fixer deux coefficients assez simples. Ici on prend $x = 0$ et $z = -1$. L'équation (1) devient donc $4y^3 - 5 = 0$. On note $P = 4Y^3 - 5$ le polynôme correspondant, à coefficients dans $\mathbb{Z}_3$. Ainsi $P' = 12Y^2$. L'idée est de se ramener au lemme de Hensel. Pour tout $y \in \mathbb{Z}_p,\ v_p(P'(y)) \geq 1$ car $3|12$. En reprenant les notations du lemme, cela nous dit que $k \geq 1$, on essaye alors avec $k = 1$, et donc $n = 3$, le plus petit entier tel que $0 \leq 2k < n$. On cherche alors $y \in \mathbb{Z}_3$ tel que $P(y) \equiv 0\,[3^3]$ et $v_3(P'(y)) = 1$. On va donc travailler modulo 27. La condition sur $P'(y)$ nous dit que le y que l'on cherche ne doit pas être divisible par 3. En outre un tel y vérifie :

$$P(y) \equiv 0\,[27]$$
$$i.e\ \ 4y^3 \equiv 5\,[27].$$

Or $\frac{5}{4} \equiv 8\,[27]$ dans le sens où $4 \cdot 8 \equiv 5\,[27]$; mais 8 est un cube non divisible par 3. Ainsi le 2 convient pour le y cherché et donc on peut relever cette solution approché de P en $\alpha \in \mathbb{Z}_3$ annulant P. Enfin $(0, \alpha, -1)$ est solution 3-adique de (1).

Nous allons suivre le même schéma de preuve, cette fois-ci dans $\mathbb{Q}_5$. On pose cette fois $x = 1$ et $z = 0$, et donc $P = 4Y^3 + 3$, $P' = 12Y^2$. Comme 5 ne divise pas 12 on peut commencer par chercher avec $k = 0$ et $n = 1$. On cherche donc $y \in \mathbb{Z}_5$ tel que $P(y) \equiv 0\,[5]$ et $v_3(P'(y)) = 0$. Cette fois si un tel y vérifie :

$$4y^3 \equiv -3\,[5].$$

Or $\frac{-3}{4} \equiv 3$. En constant que $3 \equiv 2^3\,[5]$ et que 5 ne divise pas 3, on sait que 2 convient. On relève alors ce dernier en $\alpha \in \mathbb{Z}_p$ et donc $(1, \alpha, 0)$ est une solution 5-adique de (1).

On considère maintenant p premier différent de 3 et 5. Si on suppose que $3 = a^3$ dans $\mathbb{F}_p^*$, alors on peut appliqué le lemme de Hensel à $X^3 - 3$ pour relever a en un $\alpha \in \mathbb{Z}_p$, et alors $(\alpha, -1, -1)$ est une solution p-adique de (1).

Sinon 3 n'est pas un cube dans $\mathbb{F}_p^*$, alors grâce au théorème 4.2 de l'annexe on sait que $3k = p-1$ pour u $k \in \mathbb{N}$ et que les cubes de $\mathbb{F}_p^*$ forment un sous-groupe d'indice 3. Or en particulier $1, 3\ et\ 3^2$ ne sont pas dans la même classe (en effet par hypothèse 3 n'est pas un cube donc n'est pas dans la même classe que 1). De plus si 3 et 9 étaient dans la même classe on aurait $3x^3 = 9$ dans $\mathbb{F}_p^*$ pour un certain x. Alors on aurait $x^3 = 3$ ce qui est absurde. Si maintenant 9 est dans la classe de 1 on aurait pour un $x \in \mathbb{F}_p^*$:

$$1 \equiv 9x^3 \equiv 3^2x^3\ [p]$$

Donc en passant à l'exposant k

$$1 \equiv 3^{2k}x^{3k} \equiv 3^{2k}\ [p]$$

Or c'est absurde car 3 est d'ordre $3k = p-1$ dans $\mathbb{F}_p^*$. Ainsi $1, 3$ et 9 sont dans des classes différentes. Comme il y a trois classes, on a un système de représentant. Grâce à ça on sait que comme $p \neq 5$, $5 \neq 0$ dans $\mathbb{F}_p$. Donc il existe un $b \in \mathbb{F}_p^*$ tel que $5 \equiv b^3, 3b^3$ ou $9b^3$ modulo p.

Si $5 \equiv b^3\ [p]$, alors on peut relever b en $\beta \in \mathbb{Z}_p$ solution de $x^3 - 5 = 0$, car $v_p(3\beta^2) = 2v_p(\beta) = 2v_p(b) = 0$ comme $b \neq 0$ dans $\mathbb{F}_p$. Dans ce cas $(\beta, -\beta, 1)$ est une solution p-adique de (1).

Si $5 \equiv 3b^3\ [p]$, on relève par le lemme de Hensel b en $\beta \in \mathbb{Z}_p$ car $pgcd(3^2, p) = 1$. Ainsi $(\beta, 0, -1)$ est une solution p-adique de (1).

Si $5 \equiv 9b^3\ [p]$, donc dans $\mathbb{F}_p^*$ on a $15 = (3b)^3$. On relève alors $3b$ en $\beta \in \mathbb{Z}_p$ toujours car $pgcd(3^3, p) = 1$. Ainsi $(3\beta, 5, -7)$ est une solution p-adique de (1).

On a bien montré que dans chaque cas et chaque $\mathbb{Q}_v$, (1) admet une solution.

3.1.2 Absence de solution globale

Il s'agit maintenant de montrer que l'équation $3x^3 + 4y^3 + 5z^3 = 0$ n'admet pas de solution rationnelle autre que $(0, 0, 0)$. Pour ce faire nous allons voir que

$$X^3 + 6Y^3 = 10Z^3 \tag{2}$$

ne possède pas de solution rationnelle non triviale. En effet si (1) en avait une notée (x, y, z), alors $(2y, x, -z)$ serait solution non nulle de (2).

Supposons que (2) admet une solution non triviale (X, Y, Z). Quitte à multiplier par le cube du $ppcm$ des dénominateurs. On remarque que si l'une des coordonnées de la solution est nulle, alors la solution est $(0, 0, 0)$ car $6, 10$ et $\frac{6}{10}$ne sont pas des cubes de rationnels. On peut alors supposer qu'aucune des coordonnées n'est nulle.

Si maintenant on a un $p \in \mathbf{P}$ divisant deux des trois coordonnées. Alors p divise également la troisième, en effet prenons l'exemple où p divise X et Y, les deux autres cas étant similaire. On a alors :

$$\begin{aligned} & (pk_x)^3 + 6(pk_y)^3 = 10Z^3 \\ \text{donc} \quad & p^3(k_x^3 + 6k_y^3) = 10Z^3. \end{aligned}$$

Or $10 = 2 \times 5$ est premier avec p^3. Ainsi $p^3 | Z^3$ et donc p divise Z. Finalement on peut alors supposer que X, Y et Z sont premiers deux à deux, quitte à diviser par un p^3.

Maintenant comme 2 divise 6 et 10, 2 divise X^3, donc X est pair. X, Y et Z étant premiers deux à deux Y et Z sont alors impairs. En outre si X (respectivement Z) était divisible par 3, alors comme $6 = 2 \times 3$, Z (respectivement X) le serait également ce qui est absurde car $\mathrm{pgcd}(X, Y, Z) = 1$. De même si X ou Y était divisible par 5, on aurait une contradiction.

Résumons ce que l'on sait maintenant sur X, Y et Z, en sachant qu'ils sont premiers deux à deux.

X	non nul, pair, non divisble par 3, non divisible par 5
Y	non nul, impair, non divisible par 5
Z	non nul, impair, non divisible par 3

Nous allons maintenant travailler dans $\mathbb{Z}[\sqrt[3]{6}]$ pour pouvoir factoriser plus aisément. Posons $\alpha = \sqrt[3]{6}$. On factorise alors :

$$X^3 + 6Y^3 = (X + Y\alpha)(X^2 - XY\alpha + Y^2\alpha^2).$$

(2) devient donc :

$$(X + Y\alpha)(X^2 - XY\alpha + Y^2\alpha^2) = 10Z^3. \tag{3}$$

Pour arriver à une contradiction nous allons passer par la théorie algébrique des nombres, en commençant par la proposition suivante :

Proposition 3.1. *Le discriminant de $\mathbb{Q}(\alpha)$ est $\Delta_{\mathbb{Q}(\alpha)} = -2^2 \cdot 3^5$, et son anneau des entiers est $\mathbb{Z}[\alpha]$.*

Démonstration. En toute généralité prenons $d \in \mathbb{N}^*$ sans facteur cubique. Alors $(1, \sqrt[3]{d}, \sqrt[3]{d}^2)$ est une base du $\mathbb{Z}$-module $\mathbb{Z}[\sqrt[3]{d}]$. Prenons $x = a + b\sqrt[3]{d} + c\sqrt[3]{d}^2$ avec $a, b, c \in \mathbb{Z}$, et notons m_x l'endomorphisme $\mathbb{Q}$-linéaire de $\mathbb{Q}(\sqrt[3]{d})$ de multiplication par x. On note Tr et N la trace et la norme relatives à l'extension $\mathbb{Q}(\sqrt[3]{d})/\mathbb{Q}$. On a alors :

$$\mathrm{Tr}(x) = \mathrm{Tr}\begin{pmatrix} a & dc & db \\ b & a & dc \\ c & b & a \end{pmatrix} = 3a.$$

On déduit de ceci $\Delta_{\mathbb{Q}(\alpha)}$, qui est le discriminant de la $\mathbb{Z}$-base $(1, \sqrt[3]{d}, \sqrt[3]{d^2})$ de $\mathbb{Z}[\sqrt[3]{d}]$:

$$\begin{aligned} \Delta_{\mathbb{Q}(\alpha)} &= \det\left(\mathrm{Tr}\left(d^{\frac{i+j}{3}}\right)_{i,j\in\{0,1,2\}}\right) \\ &= \begin{vmatrix} 3 & 0 & 0 \\ 0 & 0 & 3d \\ 0 & 3d & 0 \end{vmatrix} \\ &= -27d^2. \end{aligned}$$

On remarque en outre que $\mathbb{Z}[\sqrt[3]{d}]$ est un sous module de $\mathscr{O}_{\mathbb{Q}(\sqrt[3]{d})}$ de même rang. Prenons alors une $\mathbb{Z}$-base $\mathfrak{B} = (e_1, e_2, e_3)$ de $\mathscr{O}_{\mathbb{Q}(\sqrt[3]{d})}$. Le théorème de structure nous donne l'existence de (a_1, a_2, a_3) dans $\mathbb{Z}[\sqrt[3]{d}]$ tels que $\mathfrak{B}' = (a_1e_1, a_2e_2, a_3e_3)$ soit une base de $\mathbb{Z}[\sqrt[3]{d}]$.

On sait donc que la matrice de passage de $\mathfrak{B}$ à $\mathfrak{B}'$ est : $P = \begin{pmatrix} a_1 & 0 & 0 \\ 0 & a_2 & 0 \\ 0 & 0 & a_3 \end{pmatrix}$. En écrivant M (respectivement M') la matrice de l'application $(x, y) \mapsto Tr(xy)$ dans la base $\mathfrak{B}$ (respectivement $\mathfrak{B}'$) on a donc

$$\begin{aligned} M' &= P^t M P \\ \text{et donc} \quad \Delta(\mathbb{Z}[\sqrt[3]{d}]) &= (\det P)^2 \Delta_{\mathbb{Q}(\sqrt[3]{d})} \qquad \text{en passant au déterminant.} \end{aligned}$$

Or ici on remarque que $a_1a_2a_3$ est l'indice de $\mathbb{Z}[\sqrt[3]{d}]$ en plus d'être le déterminant de P. En effet :

$$\begin{aligned} \left[\mathscr{O}_{\mathbb{Q}(\sqrt[3]{d})} : \mathbb{Z}[\sqrt[3]{d}]\right] &= \left|\mathscr{O}_{\mathbb{Q}(\sqrt[3]{d})} / \mathbb{Z}[\sqrt[3]{d}]\right| \\ &= \left|\bigoplus_{i=1}^{3} \mathbb{Z}e_i \Big/ \bigoplus_{i=1}^{3} \mathbb{Z}a_ie_i\right| \\ &= a_1a_2a_3. \end{aligned}$$

De tout cela on tire :

$$\left[\mathscr{O}_{\mathbb{Q}(\sqrt[3]{d})} : \mathbb{Z}[\sqrt[3]{d}]\right]^2 \Delta_{\mathbb{Q}(\sqrt[3]{d})} = \Delta(\mathbb{Z}[\sqrt[3]{d}]) = -27d^2$$

et dans notre cas :

$$\left[\mathscr{O}_{\mathbb{Q}(\alpha)} : \mathbb{Z}[\alpha]\right]^2 = \Delta_{\mathbb{Q}(\alpha)} = \Delta(\mathbb{Z}[\alpha]) = -27 \cdot 6^2 = -2^2 \cdot 3^5.$$

Ainsi on sait que $\left[\mathscr{O}_{\mathbb{Q}(\alpha)} : \mathbb{Z}[\alpha]\right]$ divise 18. Or comme $T^3 - 6$ est d'Eisenstein en $p = 2$ et $p = 3$, la proposition 4.1 de l'annexe nous dis que $\left[\mathscr{O}_{\mathbb{Q}(\alpha)} : \mathbb{Z}[\alpha]\right]$ n'est divisible ni par 2 ni par 3. Ainsi l'indice de $\mathbb{Z}[\alpha]$ dans les entiers de $\mathbb{Q}(\alpha)$ est 1. D'où $\mathbb{Z}[\alpha]$ est l'anneau des entiers de $\mathbb{Q}(\alpha)$. □

L'anneau des entiers d'un corps de nombre étant un anneau de Dedekind, il va être judicieux de raisonner sur ses idéaux. L'équation (3) nous donne une égalité entre idéaux :

$$(X + Y\alpha)(X^2 - XY\alpha + Y^2\alpha^2) = (10)(Z)^3. \tag{4}$$

On veut factoriser (10), qui est le produit de (2) et (5). On va utiliser le théorème 4.3, énoncé et démontré dans l'annexe, qui a pour objet la factorisation des idéaux de la forme (p) avec $p \in \mathbf{P}$. Le polynôme minimal de $\alpha = \sqrt[3]{6}$ sur $\mathbb{Z}$ est bien sûr $P = T^3 - 6$. On a aussi recourt à un autre résultat, lui aussi démontré en annexe, qui dit que pour tout idéal premier non nul $\mathfrak{p}$ de $\mathbb{Z}[\alpha]$, il existe un unique $p \in \mathbf{P}$ vérifiant $\mathfrak{p}|(p)$, et qu'alors la norme de $\mathfrak{p}$ est une puissance de p.

Modulo 2 on a $\bar{P} = T^3$, ce dont on déduit la factorisation $(2) = \mathfrak{p}_2^3$ avec $\mathfrak{p}_2$ premier de norme une puissance de 2. $\mathrm{N}(2) = 2^3$ donc $\mathrm{N}(\mathfrak{p}_2) = 2$.

Modulo 5, $\bar{P} = T^3 - 1 = (T - 1)(T^2 + T + 1)$. On voit facilement que $T^2 + T + 1$ n'a aucune racine sur $\mathbb{F}_5$: il est irréductible. Ainsi (5) est le produit de deux idéaux premiers distincts de normes des puissances de 5. Vu que $\mathrm{N}(5) = 5^3$, l'une de ces normes est 5 et l'autre est 5^2. On note respectivement $\mathfrak{p}_5$ et $\mathfrak{p}_{25}$ les idéaux considérés : $(5) = \mathfrak{p}_5\mathfrak{p}_{25}$.

En outre si $\mathfrak{q}$ est un idéal premier de norme 2, alors $2 \in \mathfrak{q}$ et $\mathfrak{q}|(2)$, d'où $\mathfrak{q} = \mathfrak{p}_2$. $\mathfrak{p}_2$ est donc l'unique idéal premier de $\mathbb{Z}[\alpha]$ de norme 2. De même $\mathfrak{p}_5$ est l'unique idéal premier de $\mathbb{Z}[\alpha]$ de norme 5. Or en tâtonnant on peut trouver des éléments de $\mathbb{Z}[\alpha]$ de normes ± 2 et ± 5. En effet si on prend a, b dans $\mathbb{Z}$, $\mathrm{N}(a + \alpha b) = a^3 + 6b^3$. On trouve ainsi $\mathrm{N}(\alpha - 2) = -2$ et $\mathrm{N}(\alpha - 1) = 5$, ce qui donne $\mathfrak{p}_2 = (\alpha - 2)$ et $\mathfrak{p}_5 = (\alpha - 1)$.

En continuant à utiliser ce raisonnement, on peut prouver le fait suivant.

Proposition 3.2. *Le nombre de classes du corps $\mathbb{Q}(\alpha)$ est 1 ; autrement dit son anneau des entiers $\mathbb{Z}[\alpha]$ est principal.*

Démonstration. On utilise la borne de Minkowski, rappelée en annexe sans preuve. $\mathbb{Q}(\alpha)$ a deux plongements complexes, qui envoient α respectivement sur $\mathrm{j}\alpha$ et $\mathrm{j}^2\alpha$, où $\mathrm{j} = \mathrm{e}^{\frac{2i\pi}{3}}$. On a donc $r_2 = 1$. Ainsi on calcule :

$$\left(\frac{4}{\pi}\right)^1 \frac{3!}{3^3}\sqrt{|-2^2 \cdot 3^5|} = \frac{16\sqrt{3}}{\pi} < 9.$$

Donc toute classe d'idéaux contient un idéal de norme au plus 8. Nous allons alors passer en revue tout les idéaux premiers de norme dans $[\![2, 8]\!]$. On a vu qu'il y avait un unique idéal de norme 2, $\mathfrak{p}_2$ qui est principal. Si on avait I un idéal de norme 4, alors on a $(4) \subset I$. Or $(4) = (2)(2) = \mathfrak{p}_2^6$, donc I n'est pas premier. Par le même raisonnement pour 8, on sait qu'il n'existe pas d'idéal premier de norme 4 ou 8. En utilisant le théorème 4.3 de l'annexe, on factorise l'idéal $(3) = \mathfrak{p}_3^3$ car $T^3 - 6 \equiv T^3\,[3]$. $\mathfrak{p}_3$ est alors premier et est l'unique idéal de norme 3, par le même raisonnement que pour $\mathfrak{p}_2$. Or comme $\mathrm{N}(\alpha) = 6$, $(\alpha) = \mathfrak{p}_2\mathfrak{p}_3$. Or on a vu que $\mathfrak{p}_2$ est principal, donc finalement $\mathfrak{p}_3$ est principal. On a vu que l'unique idéal de norme 5 est $\mathfrak{p}_5$ qui est principal. Il ne peut y avoir d'idéal de norme 6, car 6 n'est pas puissance de nombre premier. Il reste le cas de la norme égale à 7. On factorise dans $\mathbb{F}_p[X]$:

$$T^3 - 6 \equiv T^3 + 1 \equiv (T + 1)(T^2 - T + 1) \equiv (T + 1)(T^2 + 6T + 8) \equiv (T + 1)(T + 2)(T + 4)\,[7].$$

Ainsi on peut factoriser $(7) = \mathfrak{p}_7\mathfrak{p}_7'\mathfrak{p}_7''$, en trois idéaux premiers de norme 7, tels que $\mathfrak{p}_7|(\alpha+1)$, $\mathfrak{p}_7'|(\alpha+2)$ et $\mathfrak{p}_7''|(\alpha+4)$. Or on a vu que $\mathrm{N}(b\alpha+a) = a^3+6b^3$, et donc :

$$\begin{aligned}
&\mathrm{N}(\alpha+1) = 7, && \text{qui nous donne } (\alpha+1) = \mathfrak{p}_7\\
&\mathrm{N}(\alpha+2) = 14, && \text{qui nous donne } (\alpha+2) = \mathfrak{p}_2\mathfrak{p}_7'\\
&\mathrm{N}(\alpha+4) = 70, && \text{qui nous donne } (\alpha+4) = \mathfrak{p}_2\mathfrak{p}_5\mathfrak{p}_7''.
\end{aligned}$$

Or sachant que $\mathfrak{p}_2$ et $\mathfrak{p}_5$ sont principaux, on en déduit que tous les idéaux premiers de norme (7) sont principaux. On peut alors conclure que le groupe des classes de $\mathbb{Q}(\alpha)$ est engendré par l'image d'idéaux principaux, donc engendré par la classe du neutre. Ainsi le nombre de classe de $\mathbb{Q}_p$ est 1.

□

Poursuivons la preuve de l'absence de solution globale, en nous attardant sur un lemme technique.

Lemme 3.1. *Il existe un idéal* $\mathfrak{a}$ *de* $\mathbb{Z}[\alpha]$ *tel que :*

$$(X+Y\alpha) = \mathfrak{p}_2\mathfrak{p}_5\mathfrak{a}^3.$$

Démonstration. Dans un premier temps montrons que $\mathfrak{p}_2$ est l'unique facteur premier commun à $(X+Y\alpha)$ et $(X^2-XY\alpha+Y^2\alpha^2)$. D'abord, $(\alpha-2) = \mathfrak{p}_2$ est premier donc $\alpha-2$ est un élément premier de l'anneau $\mathbb{Z}[\alpha]$, et $\alpha-2|2$. Mais X est pair donc $\alpha-2|X$; et $\alpha^3 = 6$ donc $\alpha-2|\alpha^3$ et $\alpha-2|\alpha$. Ainsi $\mathfrak{p}_2 = (\alpha-2)$ divise bien les idéaux $(X+Y\alpha)$ et $(X^2-XY\alpha+Y^2\alpha^2)$.

Réciproquement soit $\mathfrak{q}$ premier divisant les deux idéaux ci-dessus. $X^2-XY\alpha+Y^2\alpha^2 = (X+Y\alpha)^2 - 3XY\alpha$ donc $\mathfrak{q}$ divise $(3XY\alpha) = (3)(X)(Y)(\alpha)$: il en divise un des quatre.

- Si $\mathfrak{q}|(3)$, $\mathfrak{q} \nmid (10)$ et on déduit de l'égalité (4) que $\mathfrak{q}|(Z)$. Mais $\mathrm{N}(\mathfrak{q})$ est une puissance de 3, et en passant à la norme on obtient que $3|Z$, ce qui est faux. Donc $\mathfrak{q} \nmid (3)$.
- Si $\mathfrak{q}|(X)$, $\mathfrak{q}|(Y\alpha)$. X et Y sont premiers entre eux donc $\mathfrak{q}|(\alpha)$.
- Si $\mathfrak{q}|(Y)$, $\mathfrak{q}|(X)$. Comme X et Y sont premiers entre eux c'est absurde.

On trouve donc que $\mathfrak{q} \nmid (3)$ et $\mathfrak{q}|(\alpha)$. Mais $(\alpha)^3 = (6) = \mathfrak{p}_2^3(3)$: ceci impose $\mathfrak{q} = \mathfrak{p}_2$.

Il est ensuite possible de raffiner ceci. D'une part on a non seulement $\alpha-2|X$ mais même $(\alpha-2)^3|X$. D'autre part $v_{\mathfrak{p}_2}((Y\alpha)) = v_{\mathfrak{p}_2}((Y)) + v_{\mathfrak{p}_2}((\alpha)) = 0+1 = 1$, donc $\alpha-2$ divise $Y\alpha$ exactement une fois. D'où $\mathfrak{p}_2 = (\alpha-2)$ divise $(X+Y\alpha)$ exactement une fois. On peut ainsi prendre des idéaux $\mathfrak{b}$ et $\mathfrak{c}$ premiers entre eux et tels que $\mathfrak{p}_2 \nmid \mathfrak{b}$ de sorte que :

$$(X+Y\alpha) = \mathfrak{p}_2\mathfrak{b} \quad \text{et} \quad (X^2-XY\alpha+Y^2\alpha^2) = \mathfrak{p}_2\mathfrak{c}.$$

Insérer ceci dans l'égalité (4) donne $\mathfrak{p}_2^2\mathfrak{b}\mathfrak{c} = (10)(Z)^3$, c'est-à-dire $\mathfrak{b}\mathfrak{c} = \mathfrak{p}_2\mathfrak{p}_5\mathfrak{p}_{25}(Z)^3$. Voyons quel idéal premier divise $\mathfrak{b}$, $\mathfrak{c}$.

- $\mathfrak{p}_2 \nmid \mathfrak{b}$ donc $\mathfrak{p}_2|\mathfrak{c}$.
- Puisque $X^3+6Y^3 = 10Z^3$, $X^3 \equiv (-Y)^3$ [5]. Or $5 \not\equiv 1$ [3] donc $(x \mapsto x^3)$ est une permutation de $\mathbb{F}_5$ (ce résultat a déjà été évoqué plus tôt et est prouvé dans l'annexe). Ainsi $X \equiv -Y$ [5] ; en particulier $X \equiv -Y$ [$\mathfrak{p}_5$]. En gardant en tête que $\mathfrak{p}_5 = (\alpha-1)$, on calcule : $X+Y\alpha \equiv X+Y \equiv 0$ [$\mathfrak{p}_5$]. Alors $\mathfrak{p}_5|(X+Y\alpha)$, et $\mathfrak{p}_5|\mathfrak{b}$.
- Si $\mathfrak{p}_{25}|\mathfrak{b}$, $(5) = \mathfrak{p}_5\mathfrak{p}_{25}$ divise $(X+Y\alpha)$, et 5 divise X et Y dans $\mathbb{Z}$: c'est absurde. Donc $\mathfrak{p}_{25}|\mathfrak{c}$.

On écrit $\mathfrak{b} = \mathfrak{p}_5\mathfrak{b}'$ et $\mathfrak{c} = \mathfrak{p}_2\mathfrak{p}_{25}\mathfrak{c}'$ avec $\mathfrak{b}'$ et $\mathfrak{c}'$ des idéaux. L'égalité précédente $\mathfrak{b}\mathfrak{c} = \mathfrak{p}_2\mathfrak{p}_5\mathfrak{p}_{25}(Z)^3$ se simplifie en $\mathfrak{b}'\mathfrak{c}' = (Z)^3$. Ceci impose que $\mathfrak{b}'$ et $\mathfrak{c}'$ soient des cubes ; si on écrit $\mathfrak{b}' = \mathfrak{a}^3$ on a enfin $(X+Y\alpha) = \mathfrak{p}_2\mathfrak{p}_5\mathfrak{a}^3$.

□

On a vu plus tôt que $\mathbb{Z}[\alpha]$ était un anneau principal : en prenant $\beta \in \mathbb{Z}[\alpha]$ tel que $\mathfrak{a} = (\beta)$, le lemme se réécrit :

$$X + Y\alpha = (\alpha - 2)(\alpha - 1)u\beta^3$$

avec un $u \in \mathbb{Z}[\alpha]^*$.

Le dernier lemme à montrer est le suivant :

Lemme 3.2. *Le groupe $\mathbb{Z}[\alpha]^*/(\mathbb{Z}[\alpha]^*)^3$ est cyclique d'ordre 3 et admet comme générateur $\overline{1 - 6\alpha + 3\alpha^2}$.*

Démonstration. On va utiliser le théorème des unités de Dirichlet pour décrire $\mathbb{Z}[\alpha]^*$.
Premièrement, $\mathbb{Q}(\alpha) \subset \mathbb{R}$ donc $r_1 = 1$ et le groupe des racines de l'unité de $\mathbb{Q}(\alpha)$ est $\{\pm 1\}$, de plus on a déjà vu que le nombre de paires de plongements complexes de $\mathbb{Q}(\alpha)$ vaut 1. Par le théorème des unités de Dirichlet, $\mathbb{Z}[\alpha]^* \simeq \{\pm 1\} \times \mathbb{Z}$ d'où $(\mathbb{Z}[\alpha]^*)^3 \simeq \{\pm 1\} \times 3\mathbb{Z}$ et donc $\mathbb{Z}[\alpha]^*/(\mathbb{Z}[\alpha]^*)^3$ est d'ordre 3 donc cyclique, et il suffit de montrer que $1 - 6\alpha + 3\alpha^2$ est une unité qui n'est pas un cube.
On avait montré que $(2) = \mathfrak{p}_2^3 = (\alpha - 2)^3$ donc

$$\begin{aligned}\mathbb{Z}[\alpha] &= (\alpha - 2)^3(2)^{-1} \\ &= (\alpha - 2)^3(2^{-1}) \\ &= ((\alpha - 2)^3 2^{-1}).\end{aligned}$$

Donc $\frac{(\alpha-2)^3}{2}$ est inversible, or

$$\begin{aligned}\frac{(\alpha - 2)^3}{2} &= \frac{\alpha^3 - 6\alpha^2 + 12\alpha - 8}{2} \\ &= \frac{6 - 6\alpha^2 + 12\alpha - 8}{2} \\ &= -1 + 6\alpha - 3\alpha^2\end{aligned}$$

donc $1 - 6\alpha + 3\alpha^2$ est inversible. Reste à voir que ce n'est pas un cube.
On a vu que $(\alpha + 1)$ est de norme 7, si $1 - 6\alpha + 3\alpha^2$ est un cube dans $\mathbb{Z}[\alpha]^*$ alors son image dans $\mathbb{Z}[\alpha]^*/(\alpha + 1) \simeq \mathbb{F}_7$ est aussi un cube. Calculons les images de α et α^2 :

$$\alpha = \alpha + 1 - 1 \equiv -1 \mod (\alpha + 1) \quad \text{et} \quad \alpha^2 = (\alpha + 1)^2 - 2\alpha - 1 \equiv 2 - 1 \equiv 1 \mod (\alpha + 1).$$

Donc $1 - 6\alpha + 3\alpha^2 \equiv 10 \equiv 3 \mod (\alpha + 1)$; or 3 n'est pas un cube dans $\mathbb{F}_7$. Cela achève la preuve. □

A partir de là, $1 - 6\alpha + 3\alpha^2 = \frac{(2-\alpha)^3}{2}$ et il existe $k \in \{0, 1, 2\}$ et $v \in \mathbb{Z}[\alpha]^*$ tel que :

$$\begin{aligned}X + Y\alpha &= (\alpha - 2)(\alpha - 1)u\beta^3 \\ &= (\alpha - 2)(\alpha - 1)\left(\frac{(2 - \alpha)^3}{2}\right)^k v^3\beta^3 \\ &= (\alpha - 2)(\alpha - 1)\left(\frac{1}{2^k}\right)((2 - \alpha)^k v\beta)^3.\end{aligned}$$

On pose $\gamma = (2 - \alpha)^k v\beta$ et on multiplie à gauche et à droite par 2^k, ce qui donne :

$$2^k X + 2^k Y\alpha = (\alpha - 2)(\alpha - 1)\gamma^3$$

Or $\gamma \in \mathbb{Z}[\alpha]$ donc il existe $A, B, C \in \mathbb{Z}$ tels que $\gamma = A + B\alpha + C\alpha^2$, on remplace γ dans le membre de droite et on isole les coefficients devant α^2 :

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

De là, on voit que A est divisible par 3 en passant à gauche le premier terme du membre de droite ; ensuite sachant que $3|A$ tous les termes à part le second sont divisibles par 9, donc nécessairement $3|B$; puis tous les termes sont alors divisibles par 27 à part le troisième, ce qui implique que $3|C$. On peut alors diviser A, B, C par 3, et en notant A', B', C' les quotients, on remarque que A', B', C' vérifient la même équation que A, B, C (car l'équation vérifiée par A, B, C est polynomiale homogène de degré 3). Donc A, B, C sont "indéfiniment" divisibles par 3, ce qui implique qu'ils sont tous nuls, d'où la contradiction. Ainsi il n'existe pas de solution rationnelle non triviale à l'équation de Selmer.

Nous venons ainsi de démontrer que l'équation $3x^3 + 4y^3 + 5z^3 = 0$ possède des solutions sur chaque $\mathbb{Q}_v$, mais n'a pas de solution rationnelle. On comprend alors qu'un problème sur $\mathbb{Q}$ ne se résume pas simplement à un problème sur chacun de ses complétés. C'est l'indice que des mathématiques plus fines sont derrière le principe local-global. En effet il s'agit encore aujourd'hui d'un domaine de recherche actif, et les travaux de mathématiciens, comme Jean-Marc Fontaine par exemple, font appel à des théories plus profondes.

4 Annexe

4.1 Théorème de Chevalley

Soit p un nombre premier.

Théorème 4.1. *On considère $f_i \in \mathbb{F}_p[X_1, \cdots, X_n]$ pour $i \in [\![1; M]\!]$. Notons V l'ensemble de leurs zéros commun dans $\mathbb{F}_p^n$. Si $\sum_{i=1}^{M} \deg(f_i) < n$, alors $\mathrm{Card}(V) \equiv 0\,[p]$.*

Du théorème on s'empresse de donner le corollaire suivant.

Corollaire 4.1. *Toute forme quadratique de rang supérieur à 3 admet un zéro dans $\mathbb{F}_p$.*

Démonstration. On écrit $f = \sum a_i X_i^2$, qui satisfait les hypothèses du théorème de Chevalley. Alors $\mathrm{Card}(V) \equiv 0[p]$. Or si on avait $V = \{0\}$ alors $\mathrm{Card}(V) = 1$. Ce qui est absurde. □

Nous allons maintenant montrer le théorème de Chevalley. On commence par montrer le lemme suivant.

Lemme 4.1. *Soit $m \geq 0$ un entier. Alors*

$$\sum_{x \in \mathbb{F}_p} x^m = \begin{cases} -1 & \text{si } m \geq 1 \text{ et } p-1 | m \\ 0 & \text{sinon} \end{cases}.$$

Démonstration. Le cas $m = 0$ est trivial, on suppose que $m \geq 1$. Alors $\mathbb{F}_p^*$ est cyclique, et on en note w un générateur. Ainsi on a l'égalité

$$\sum_{x \in \mathbb{F}_p} x^m = \sum_{i=1}^{p-1} (w^i)^m = \sum_{i=1}^{p-1} (w^m)^i.$$

On reconnaît une somme géométrique, et par la formule bien connue :

$$\sum_{i=1}^{p-1} (w^m)^i = \begin{cases} p-1 = -1 \text{ dans } \mathbb{F}_p & \text{si } w^m \equiv 1[p] \text{ i.e } p-1|m \\ \frac{1-w^{m(p-1)}}{1-w^m} \equiv 0 & \text{sinon} \end{cases}.$$

□

Passons à la preuve du théorème.

Démonstration. Avec les mêmes notations que dans le théorème, on remarque que si on note $P = \prod_{i=1}^{n} (1 - f_i^{p-1})$ alors $\mathbf{1}_V$ coïncide avec P sur $\mathbb{F}_p^n$. En effet si $x = (x_1, \cdots, x_n) \in V$ alors $P(x) = \prod_{i=1}^{n} (1-0) = 1$. Si $x = (x_1, \cdots, x_n) \notin V$ alors on a un $j \in [\![1; n]\!]$ tel que $f_i(x) \in \mathbb{F}_p^*$. Donc $f_i(x)^{p-1} = 1$ ce qui annule P. On a alors dans $\mathbb{F}_p$:

$$\sum_{x \in \mathbb{F}_p^n} P(x) \equiv \sum_{x \in \mathbb{F}_p^n} \mathbf{1}_V(x) \equiv \mathrm{Card}(V).$$

D'autre part si on écrit $P = \sum_{i_1, \cdots, i_n \in \mathbb{N}} \lambda_{i_1, \cdots, i_n} X^{i_1} \cdots X^{i_n}$, il vient :

$$\sum_{x \in \mathbb{F}_p^n} P(x) \equiv \sum_{i_1, \cdots, i_n \in \mathbb{N}} \lambda_{i_1, \cdots, i_n} \left(\sum_{x_1 \in \mathbb{F}_p} x_1^{i_1} \right) \cdots \left(\sum_{x_n \in \mathbb{F}_p} x_n^{i_n} \right).$$

Soit un $\lambda_{i_1,\cdots,i_n} \neq 0$. On voit que $\deg(P) = (p-1)\sum_{i=1}^{M} \deg(f_i) < n(p-1)$. Donc $i_1 + \cdots + i_n < n(p-1)$. Donc il existe un i_j tel que $i_j < p-1$. Donc par application du lemme précédent, $\sum_{x_j \in \mathbb{F}_p} x_j^{i_j} = 0$. Ainsi

$$\sum_{x \in \mathbb{F}_p^n} P(x) \equiv 0 \equiv \mathrm{Card}(V)\ [p].$$

□

4.2 Cubes de $\mathbb{F}_p^*$

Dans la partie 3.1.1 pour la recherche de solutions globales à $3x^3 + 4y^3 + 5y^3 = 0$ on utilise le fait suivant :

Si il existe un élément qui n'est pas un cube dans $\mathbb{F}_p^*$, alors $p-1 \mid 3$ et les cubes de $\mathbb{F}_p^*$ forment un sous-groupe d'indice 3.

Ceci découle en fait directement de la dichotomie donnée par le théorème suivant.

Théorème 4.2.

- *Si* $3|p-1$ *les cubes de* $\mathbb{F}_p^*$ *forment un sous-groupe d'indice* 3.
- *Sinon tous les éléments de* $\mathbb{F}_p^*$ *sont des cubes.*

Démonstration. Il est clair que les cubes de $\mathbb{F}_p^*$ forment un sous-groupe.

Si $3|p-1$, on note $p-1 = 3k$ pour $k \in \mathbb{N}$. Prenons ensuite x un générateur de $\mathbb{F}_p^*$. On note $c = x^3$, ce dernier est alors un générateur du groupe des cubes de $\mathbb{F}_p^*$ qui est de cardinal k, et donc d'indice 3. En effet on remarque que

$$\begin{aligned}
c^0 &= x^0 = 1 \\
c^1 &= x^3 \neq 1 \\
c^2 &= x^{3\cdot 2} \neq 1 \quad \textit{(x est d'ordre p-1>i3 pour tout i<k)} \\
&\vdots \\
c^{k-1} &= x^{3(k-1)} \neq 1 \\
c^k &= x^{3k} = x^{p-1} = 1.
\end{aligned}$$

Donc c est bien d'ordre k. Et si maintenant a est un cube de $\mathbb{F}_p^*$, alors $a = g^3$ pour un certain $g \in \mathbb{F}_p^*$. Or $g = x^l$ pour un $l \leq p-1$ entier. Donc $a = x^{l3}$ donc $a = c^l$. Ainsi g engendre bien les cubes de $\mathbb{F}_p^*$.

Sinon on a $pgcd(3, p-1) = 1$, donc il existe $u, v \in \mathbb{Z}$ tels que $3u + (p-1)v = 1$. Soit $x \in \mathbb{F}_p^*$. Alors dans $\mathbb{F}_p^*$ on a

$$x = x^{3u+(p-1)v} = (x^u)^3 \cdot (x^v)^{p-1}.$$

Or comme $x \in \mathbb{F}_p^*$ on a par le petit théorème de Fermat que $(x^v)^{p-1} \equiv 1\ [p]$. Alors on a dans $\mathbb{F}_p^*$, $x = (x^u)^3$: x est un cube. □

4.3 Résultats de théorie algébrique des nombres

Dans ce paragraphe nous allons démontrer des résultats que nous utilisons dans la partie **3.1.2** sur l'absence de solution globale à l'exemple de Selmer. On notera K un corps de nombre de degré n sur $\mathbb{Q}$, et $\mathscr{O}_K$ son anneau des entiers. On notera aussi les applications $\mathrm{Tr}_{K/\mathbb{Q}}$ et $\mathrm{N}_{K/\mathbb{Q}}$ respectivement Tr et N.

Proposition 4.1. *Soit $p \in \mathbf{P}$. Soit $u \in \mathscr{O}_K$ tel que son polynôme minimal soit de degré n et de Eisenstein en p. On a alors que $p \nmid \big[\mathscr{O}_K : \mathbb{Z}[u]\big]$.*

Démonstration. Supposons que $p \,|\, \big[\mathscr{O}_K : \mathbb{Z}[u]\big]$. On sait que $\mathscr{O}_K/\mathbb{Z}[u]$ est un groupe abélien fini pour la loi $+$ de cardinal $\big[\mathscr{O}_K : \mathbb{Z}[u]\big]$. Ainsi grâce au lemme de Cauchy, il existe un $x' \in \mathscr{O}_K/\mathbb{Z}[u]$ d'ordre p, c'est à dire tel que $px' = 0$ dans le quotient. Ainsi en notant x un relevé de x', on a $x \in \mathscr{O}_K \setminus \mathbb{Z}[u]$ tel que $px \in \mathbb{Z}[u]$. Ainsi il existe $b_0, \cdots, b_{n-1}$ dans $\mathbb{Z}$ tels que

$$xp = b_0 u + \cdots + b_{n-1}u^{n-1}. \tag{5}$$

On remarque en outre que si tous les b_i étaient divisible par p, alors on pourrait simplifier l'équation précédente et avoir $x \in \mathbb{Z}[u]$, ce qui est exclu. Ainsi on peut considérer $r \in [\![0, n-1]\!]$ minimal pour la propriété "p ne divise pas b_i". On sait alors par minimalité de r que :

$$\begin{aligned} b_0 \equiv \cdots \equiv b_{r-1} &\equiv 0 \mod p\mathscr{O}_K \\ b_0 + b_1 u + \cdots + b_{r-1}u^{r-1} &\equiv 0 \mod p\mathscr{O}_K. \end{aligned}$$

Avec ceci et l'équation (5) on a :

$$b_r u^r + \cdots + b_{n-1}u^{n-1} \equiv 0 \mod p\mathscr{O}_K.$$

En multipliant l'équation précédente par u^{n-1-r} et en remarquant que $u^n \equiv 0 \mod p\mathscr{O}_K$ car son polynôme minimal est d'Eisenstein en p :

$$b_r u^{n-1} \equiv 0 \mod p\mathscr{O}_K$$

Ainsi il existe $z \in \mathscr{O}_K$ tel que $pz = b_r u^{n-1}$. En prenant la norme on trouve directement

$$\begin{aligned} \mathrm{N}(pz) &= \mathrm{N}(b_r u^{n-1}) \\ p^n \mathrm{N}(z) &= b_r^n \mathrm{N}(u)^{n-1}. \end{aligned}$$

On tire de cela que $p^n \,|\, b_r^n \mathrm{N}(u)^{n-1}$, or p ne divise pas b_r, donc $p^n \,|\, \mathrm{N}(u)^{n-1}$. Ce qui nous donne $p^2 \,|\, \mathrm{N}(u)$. Mais $\mathrm{N}(u)$ est au signe près le coefficient constant du polynôme minimal de u, qui est de Eisenstein en p. D'où la contradiction. □

Donnons maintenant deux résultats en lien avec la factorisation des idéaux (p) de $\mathscr{O}_K$ pour p premier.

Proposition 4.2. *Soit $\mathfrak{p}$ un idéal premier non nul de $\mathscr{O}_K$. Il existe un unique nombre premier p tel que $\mathfrak{p}|(p)$. De plus, $\mathrm{N}(\mathfrak{p})$ est une puissance de p.*

Démonstration. $\mathfrak{p} \cap \mathbb{Z}$ est un idéal non nul de $\mathbb{Z}$, qui est premier puisque $\mathfrak{p}$ l'est. Ainsi on peut l'écrire $p\mathbb{Z}$ avec $p \in \mathbf{P}$. Il suit que $p \in \mathfrak{p}$, c'est-à-dire $\mathfrak{p}|(p)$. Si $q \in \mathbf{P}$ est aussi tel que $\mathfrak{p}|(q)$, alors $q \in \mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$, et $q = p$.

Pour ce qui est de la norme, $\mathscr{O}_K/\mathfrak{p}$ est un corps fini de caractéristique p, donc de cardinal une puissance de p. Par définition, ce cardinal est $\mathrm{N}(\mathfrak{p})$. □

Théorème 4.3. *Soit α un entier algébrique dont on note $P \in \mathbb{Z}[T]$ le polynôme minimal. Soit $p \in \mathbf{P}$. On écrit la décomposition en facteurs premiers de $\bar{P}$ sur $\mathbb{F}_p[T]$: $\bar{Q_1}^{k_1} \cdots \bar{Q_r}^{k_r}$, où les $\bar{Q_i}$ sont irréductibles deux à deux premiers entre eux. Alors l'idéal (p) de $\mathbb{Z}[\alpha]$ s'écrit $(p) = \mathfrak{q}_1^{k_1} \cdots \mathfrak{q}_r^{k_r}$, où les $\mathfrak{q}_i$ sont des idéaux premiers non nuls distincts.*

Démonstration. Puisque la réduction modulo p est un morphisme d'anneaux surjectif de $\mathbb{Z}[T]$ dans $\mathbb{F}_p[T]$, l'application

$$\psi : \left\{ \begin{array}{ccc} \mathbb{Z}[\alpha] & \to & \mathbb{F}_p[T]/(\bar{P}) \\ R(\alpha) & \mapsto & \bar{R} \bmod \bar{P} \end{array} \right.$$

est un morphisme d'anneaux surjectif. On vérifie que $\mathrm{Ker}(\psi) = (p)$: soit $R \in \mathbb{Z}[T]$ tel que $\deg R < \deg P$:

$$\begin{aligned} \psi(R(\alpha)) = 0 &\Leftrightarrow \bar{P} | \bar{R} \text{ dans } \mathbb{F}_p[T] \\ &\Leftrightarrow \bar{R} = 0 \qquad\qquad \text{car } \deg \bar{R} < \deg P = \deg \bar{P} \\ &\Leftrightarrow p | R \text{ dans } \mathbb{Z}[T] \\ &\Leftrightarrow p | R(\alpha) \text{ dans } \mathbb{Z}[\alpha]. \end{aligned}$$

Soit $1 \leq i \leq r$. $\bar{Q}_i$ étant irréductible, $(\bar{Q}_i)$ est un idéal premier non nul de $\mathbb{F}_p[T]$. Puisque $\bar{Q}_i | \bar{P}$, on peut passer au quotient : $(\bar{Q}_i \bmod \bar{P}) = (\bar{Q}_i)/(\bar{P})$ est un idéal premier non nul de $\mathbb{F}_p[T]/(\bar{P})$. On note $\mathfrak{q}_i = \psi^{-1}\left((\bar{Q}_i \bmod \bar{P})\right)$ son image réciproque par le morphisme ψ, qui est donc un idéal premier non nul de $\mathbb{Z}[\alpha]$.

Si $i \neq j$, $\bar{Q}_i$ et $\bar{Q}_j$ sont premiers entre eux, donc $\mathfrak{q}_i \neq \mathfrak{q}_j$. Finalement :

$$\begin{aligned} (p) &= \mathrm{Ker}(\psi) \\ &= \psi^{-1}((0)) \\ &= \psi^{-1}\left(\left(\bar{Q}_1{}^{k_1} \cdots \bar{Q}_r{}^{k_r} \bmod \bar{P}\right)\right) \\ &= \psi^{-1}\left((\bar{Q}_1 \bmod \bar{P})^{k_1} \cdots (\bar{Q}_r \bmod \bar{P})^{k_r}\right) \\ &= \psi^{-1}\left((\bar{Q}_1 \bmod \bar{P})\right)^{k_1} \cdots \psi^{-1}\left((\bar{Q}_r \bmod \bar{P})\right)^{k_r} \\ &= \mathfrak{q}_1^{k_1} \cdots \mathfrak{q}_r^{k_r}. \end{aligned}$$

□

On peut ajouter que si Q_i est un relèvement de $\bar{Q}_i$ dans $\mathbb{Z}[T]$, alors $\psi(Q_i(\alpha)) = \bar{Q}_i \bmod \bar{P}$, et par définition de $\mathfrak{q}_i$ on a $Q_i(\alpha) \in \mathfrak{q}_i$.

Remarque : cela ne nous sert pas ici, mais puisque $(p) = \mathrm{Ker}(\psi)$, en appliquant successivement le théorème de factorisation et le théorème des restes chinois on obtient un isomorphisme d'anneaux

$$\mathbb{Z}[\alpha]/(p) \simeq \prod_{i=1}^{r} \mathbb{F}_p[T]/\left(\bar{Q}_i{}^{k_i}\right).$$

Lors de l'étude du contre-exemple de Selmer, pour montrer que $\mathbb{Z}[\sqrt[3]{6}]$ est un anneau principal on a recourt au résultat classique de la borne de Minkowski. Nous rappelons son énoncé ici, sans démonstration. Cette dernière peut cependant être trouvée dans [Sam71](pp67-70).

Théorème 4.4 (Borne de Minkowski)**.** *Soit K un corps de nombres de degré n sur $\mathbb{Q}$. On note $2r_2$ son nombre de plongements complexes et Δ_K son discriminant. Toute classe d'idéaux de K possède un idéal $\mathfrak{a}$ dont la norme vérifie :*

$$\mathrm{N}(\mathfrak{a}) \leq \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^{r_2} \sqrt{|\Delta_K|}.$$

Enfin le théorème suivant est lui aussi utilisé dans le contre-exemple de Selmer, et sa preuve se trouve également dans [Sam71] (p72)

Théorème 4.5 (des unités de Dirichlet)**.** *: Soit K un corps de nombres. On note r_1 son nombre de plongements réels et $2r_2$ son nombre de plongements complexes. Le groupe des unités de $\mathcal{O}_K$ est isomorphe au produit du groupe des racines de l'unité de K et d'un groupe abélien libre de rang $r_1 + r_2 - 1$, c'est-à-dire (en notant R le groupe des racines de l'unité) :*

$$\mathbb{Z}[\alpha]^* \simeq R \times \mathbb{Z}^{r_1+r_2-1}.$$

Références

[Bou70] Nicolas Bourbaki. *Éléments de mathématiques, Théorie des ensembles*. Springer, 1970.

[Col] Pierre Colmez. *les nombres p-adique, notes du cours de M2*.

[Con] Keith Conrad. *Selmer's example*.

[Sam71] Pierre Samuel. *Théorie algébrique des nombres*. Hermann, 1971.

[Ser95] Jean-Pierre Serre. *Cours d'arithmétique*. PUF, 1995.