Cours d'arithmétique

Alban PIROUTET, Léo FILMONT

Janvier-Avril 2024

Table des matières

1 Introduction

2 Chapitre 1 : Corps finis

§1. Généralités .

2.1 Corps finis

Soit K un corps. L'image de Z dans K est un anneau intègre, donc isomorphe à Z ou à Z/pZ avec p un entier naturel.

Lemme 1. *Soit K un corps de caractéristique $p > 0$ alors p est un entier naturel premier. De plus l'application $\sigma : x \to x^p$ est un isomorphisme de K sur un de sous-corps K^p.*

Définition 1. *Supposons par l'absurde que p n'est pas premier alors $p = ab$ avec $1 < a < p$ quitte à échanger. On note Ψ le morphisme de Z dans K. Par définition $Ker(\psi)$=Z/pZ. Or $\psi(p) = \psi(ab) = \psi(a)\psi(b) = 0$ or K est intègre donc quitte à échanger a et b on a $\psi(a) = 0$ donc $p|a$: absurde. Ainsi a=1 donc p est premier.*
On a $\sigma(xy) = (xy)^p = x^p \times y^p = \sigma(x) \times \sigma(y)$ car K est supposé commutatif. De plus comme p est premier on a $\forall\ 1 < k < p$,$p|\binom{p}{k}$ donc en utilisant la formule du binôme de Newton on a: $\sigma(x+y) = (x+y)^p = \sum_{k=0}^{p} \binom{p}{k} x^k \times y^{p-k} = \sum_{k=1}^{p-1} \binom{p}{k} x^k \times y^{p-k} + x^p + y^p = x^p + y^p = \sigma(x) + \sigma(y)$.
De plus il est clair que σ est injectif car K est intègre.

Théorème 1. *i) Si K est un corps fini de caractéristique $p > 0$ qui est un nombre premier, en notant $f = [K : Z/pZ]$ on a $card(K) = p^f$.*

ii) Soit p un nombre premier et soit $q = p^f$ avec $f >= 1$ une puissance de p. Soit Ω un corps algébriquement clos de caractéristique p. Il existe un sous-corps de Z/qZ de Ω et un seul à q éléments; c'est l'ensemble des racines du polynôme $X^q - X$.

iii) Tout corps fini à $q = p^f$ éléments est isomorphe à $F_q = Z/qZ$.

2.2 Groupe multiplicatif d'un corps fini

Soit p un nombre premier, $f \geq 1$ un entier et $q = p^f$.

Théorème 2. *Le groupe multiplicatif F_q^* du corps fini F_q est cyclique d'ordre $q - 1$.*

Lemme 2. *Si n est un entier ≥ 1, on a $n = \sum_{d|n} \psi(d)$*

Lemme 3. *Soit H un groupe fini d'ordre n. On suppose que, pour tout diviseur d de n, l'ensemble des $x \in H$ tels que $x^d = 1$ a au plus d éléments. Alors H est cyclique.*

§2. Equations sur un corps fini Soit q une puissance d'un nombre premier p, et on considère K un corps de cardinal q.

2.3 Sommes de puissances

Lemme 4. *Soit u un entier ≥ 0. La somme $S(X^u) = \sum_{x \in K} x^u$ est égale à -1 si $u \geq 1$ et divisible par $q-1$; elle est égale à 0 sinon.*

2.4 Le théorème de Chevalley

Théorème 3. *(Chevalley-Warning). Soient $f_\alpha \in K[X_1, ..., X_n]$ des polynômes à n variables tels que $\sum deg(f_\alpha) < n$, et soit V l'ensemble de leur zéros communs dans K^n. On a $Card(V) \equiv 0 \pmod p$.*

Corollaire 1. *Si $\sum deg(f_\alpha) < n$ et si les f_α sont sans terme constant, les f_α ont un zéros non trivial.*

Corollaire 2. *Toute forme quadratique d'au moins 3 variables sur K a un zéro non trivial.*

§3. Loi de réciprocité quadratique

2.5 Carrés de $\mathbb{F}_q$

Soit q une puissance d'un nombre premier p.

Théorème 4. *a) Si $p = 2$, tout élément de $\mathbb{F}_q$ est un carré.*
b) Si $p \neq 2$, les carrés de $\mathbb{F}_q^*$ forment un sous-groupe d'indice 2 de $\mathbb{F}_q^*$; ce sous-groupe est le noyau de l'homomorphisme $x \mapsto x^{\frac{q-1}{2}}$, à valeurs dans $\{\pm 1\}$.

Démonstration. Le cas a) résulte du fait que $x \mapsto x^2$ est un automorphisme de $\mathbb{F}_q$. Dans le cas b), on considère Ω une clôture algébrique de $\mathbb{F}_q$; si $x \in \mathbb{F}_q$, soit $y \in \Omega$ tel que $y^2 = x$. On a $y^{q-1} = x^{\frac{q-1}{2}} = \pm 1$ car $x^{q-1} = 1$. Pour que x soit un carré dans $\mathbb{F}_q$, il faut et il suffit que y appartienne à $\mathbb{F}_q$, c'est à dire que $y^{q-1} = 1$. On remarque donc que $\mathbb{F}_q^{*2}$ est le noyau de $x \mapsto x^{\frac{q-1}{2}}$. De plus $\mathbb{F}_q^*$ est cyclique d'ordre $q-1$, l'indice de $\mathbb{F}_q^{*2}$ est donc 2.

2.6 Symbole de Legendre (cas élémentaire)

Définition 2. *Soit p un nombre premier différent de 2, et soit $x \in \mathbb{F}_p^*$. On appelle symbole de Legendre de x, et on note $(\frac{x}{p})$, l'entier $x^{\frac{q-1}{2}} = \pm 1$. On étend ce symbole à $\mathbb{F}_p$ à tout entier en posant $(\frac{0}{p}) = 0$. De plus si $x \in \mathbb{Z}$ a pour image $x' \in \mathbb{F}_p$ on pose $(\frac{x}{p}) = (\frac{x'}{p})$. D'après le théorème précédent on $(\frac{x}{p}) = 1 \equiv$*

Calcul de $(\frac{x}{p})$ pour $x = 1, -1, 2$. On considère le cas où n est un entier impair. On définit $\epsilon(n)$ et $\omega(n)$ par:

$$\epsilon(n) \equiv \frac{n-1}{2} \mod 2 = \begin{cases} 0 & \text{si } n \equiv 1 \mod 4 \\ 1 & \text{si } n \equiv -1 \mod 4 \end{cases}$$

$$\omega(n) \equiv \frac{n^2-1}{8} \mod 2 = \begin{cases} 0 & \text{si } n \equiv \pm 1 \mod 8 \\ 1 & \text{si } n \equiv \pm 5 \mod 8 \end{cases}$$

Théorème 5. *On a les formules suivantes :*
i) $(\frac{1}{p}) = 1$

ii) $(\frac{-1}{p}) = (-1)^{\epsilon(p)}$

iii) $(\frac{2}{p}) = (-1)^{\omega(p)}$

2.7 Loi de réciprocité quadratique

Soient l et p deux nombres premiers distincts, différents de 2.

Théorème 6. *On a* $(\frac{l}{p}) = (\frac{p}{l})(-1)^{\epsilon(l)\epsilon(p)}$

Démonstration. On se place dans une clôture algébrique Ω de $\mathbb{F}_p$, et l'on fixe $\zeta \in \Omega$ racine primitive l-ième de l'unité. L'objet central de la preuve est la somme de Gauss $S := \sum_{x \in \mathbb{F}_l} (\frac{x}{l}) \zeta^x$. On vérifie par calcul que celle ci vérifie $S^2 = (\frac{-1}{l})l$, et $S^p = (\frac{p}{l})S$ d'où $S^{p-1} = (\frac{p}{l})$, ce qui offre l'expression souhaitée pour $l^{\frac{p-1}{2}} = (\frac{l}{p})$.

3 Chapitre II: Corps p-adiques

Pour l'ensemble du chapitre p désigne un nombre premier.

§1. L'anneau Z_p et le corps Q_p
Pour tout $n \geq 1$, on pose $A_n = Z/p^n Z$. On peut observer qu'un élément de A_n définit entièrement un élément de A_{n-1}. On a donc un morphisme $\Phi_n : A_n \to A_{n-1}$ qui est surjectif, et de noyau $p^{n-1}A_n$.
La suite $...\to A_n \to A_{n-1} \to ... \to A_1$ constitue un "système projectif".

Définition 3. *On désigne par anneau des entiers p-adiques noté Z_p, la limite du système projectif (A_n, Φ_n). Par définition un élement de Z_p est une suite $x = (..., x_n, ..., x_1)$ avec $x_n \in A_n$ et $\Phi_n(x_n) = x_{n-1}$ si $n \geq 2$. On définit naturellement l'addition et la multiplication dans Z_p par l'addition et la multiplication coordonnées par coordonnées.*

3.1 Propriétés de Z_p

Soit ϵ_n l'application n-ième composante.

Proposition 1.
La suite $0 \to Z_p \xrightarrow{p^n} Z_p \xrightarrow{\epsilon_n} A_n \to 0$ *est exacte.*

Proposition 2. *i) Un élément de Z_p (resp. de A_n) soit inversible, il faut et il suffit qu'il ne soit pas divisible par p.*
ii) Si U désigne le groupe des éléments inversibles de Z_p, tout élément de Z_p différent de 0 s'écrit de façon unique sous la forme $p^n u$, avec $u \in U$ et $n \geq 0$.

Proposition 3. *[L'anneau $\mathbb{Z}_p$] L'aneau $\mathbb{Z}_p$ est un anneau de valuation, de manière équivalente, c'est un anneau principal possédant pour unique idéal maximal $\mathfrak{m} := p\mathbb{Z}_p$. C'est donc un anneau local, dont les idéaux sont donnés par la chaîne $A \supsetneq \mathfrak{m} \supsetneq \mathfrak{m}^2 \supsetneq \mathfrak{m}^3 \supsetneq ....$ Les éléments irréductibles (/ premiers /extrémaux) sont les pu où $u \in U$.*

Démonstration. La valuation v sur $\mathbb{Z}_p$ (qui à tout $p^n u \in \mathbb{Z}_p$, avec $n \in \mathbb{N}$ et $u \in U$ associe n) s'étend à $\mathbb{Q}_p = Frac(\mathbb{Z}_p)$ (voir paragraphe suivant) et l'on a clairement $\mathbb{Z}_p = \{x \in \mathbb{Q}_p \mid v(x) \geq 0\}$. Le reste découle des propriétés des anneaux à valuation discrète.

3.2 Le corps Q_p

Définition 4. *On appelle corps des fractions des nombres p-adiques, et on note Q_p, le corps des fractions de l'anneau Z_p.*

On peut observer que $Q_p = Z_p[p^{-1}]$.

§2. Equations p-adiques

3.3 Solutions

Lemme 5. *Soit $... \to X_n \to X_{n-1} \to ... \to X_1$ un système projectif et X sa limite projective. Si les X_n sont finis et non vides, X est non-vide.*

Notation : Si $f \in Z_p[X_1, ..., X_m]$ est un polynôme à coefficients dans Z_p, et si $n \geq 1$, on note f_n le polynôme à coefficients dans A_n déduit de f par réduction modulo p^n.

Proposition 4. *Soient $f^{(i)} \in Z_p[X_1, ..., X_m]$ des polynômes à coefficients entiers p-adiques. Les propositions suivantes sont équivalentes :*

i) Les $f^{(i)}$ ont un zéro commun dans ${Z_p}^m$.

ii) Pour tout $n \geq 1$, les polynômes $(f_n)^{(i)}$ ont un zéro commun dans $(A_n)^m$.

Notation : Un point $x = (x_1, ..., x_m)$ de $(Z_p)^m$ est dit "primitif" si l'un des x_i est inversible, c'est à dire si les x_i ne sont pas tous divisibles par p; on définit de manière analogue les éléments primitifs de $(A_n)^m$.

Proposition 5. *Soient $f^{(i)} \in Z_p[X_1, ..., X_m]$ des polynômes homogènes à coefficientss entiers p-adiques. Il y a équivalence entre :*

a) Les $f^{(i)}$ ont un zéro commun non trivial dans $(Q_p)^m$.

b) Les $f^{(i)}$ ont un zéro commun primitif dans $(Z_p)^m$.

c) Pour tout $n \geq 1$, les $f_n^{(i)}$ ont un zéro commun primitif dans $(A_n)^m$.

3.4 Amélioration des solutions approchées

Lemme 6. *Soit $f \in Z_p[X]$, et f' sa dérivée. Soient $x \in Z_p$,$n, k \in Z$ tels que $0 \leq 2k < n$, $f(x) \equiv 0 \pmod p$,$v_p(f'(x)) = k$. Il existe alors $y \in Z_p$ tel que : $f(y) \equiv 0 \pmod{p^{n+1}}$, $v_p(f'(y)) = k$ et $y \equiv x \pmod{p^{n-k}}$.*

Démonstration. On considère y de la forme $x + p^{n-k}z$ avec $z \in \mathbb{Z}_p$. La formule de Taylor assure que :

$f(y) = f(x) + p^{n-k}zf'(x) + p^{2n-2k}a$ avec $a \in \mathbb{Z}_p$. D'après les hypothèses on a $f(x) = p^n b$ et $f'(x) = p^k c$, avec $b \in \mathbb{Z}_p$ et $c \in \mathbb{U}$; il est donc possible de prendre z tel que $b + cz \equiv 0 \pmod p$. La formule précédente permet donc d'avoir :
$f(y) = p^n(b + cz) + p^{2n-2k} \equiv 0 \pmod{p^{n+1}}$ car $2n - 2k > n$.
On réapplique la formule de Taylor cette fois-ci à f', on $f'(y) \equiv p^k c \pmod p$ or $n - k > k$ donc on a bien $v_p(f'(y)) = k$.

Théorème 7. *Soient $f \in Z_p[X_1, ..., X_m]$, $x = (x_i) \in (Z_p)^m$,$n, k \in Z$, et $j \in [\![1 \ ; \ n]\!]$. On suppose que $0 \leq 2k < n$, et que $f(x) \equiv 0 \pmod{p^n}$ et $v_p(\frac{\partial f}{\partial X_j}(x)) = k$.*
Il existe un zéro y de f dans $(Z_p)^m$ qui est congru à x modulo p^{n-k}.

Démonstration. On prouve d'abord le théorème pour $m = 1$. On applique le lemme précédent à $x^{(0)} = x$, on obtient $x^{(1)} \in \mathbb{Z}_p$, avec $x^{(1)} \equiv x^{(0)} \pmod{p^{n-k}}$ et tel que : $f(x^{(1)}) \equiv 0 \pmod{p^{n+1}}$, et $v_p(f'(x^{(1)})) = k$ On réapplique le lemme à $x^{(1)}$. Ainsi on construit une suite $x^{(0)}, x^{(1)}, \ldots, x^{(q)}, \ldots$ avec :
$x^{(q+1)} \equiv x^{(q)} \pmod{p^{n+q-k}}$ et $f(x^{(q)}) \equiv 0 \pmod{p^{n+q}}$. On peut remarquer que c'est une suite de Cauchy donc converge vers un certain y. On peut affirmer qu'alors : $f(y) = 0$ et $y \equiv x \pmod{p^{n-k}}$, ce qui conclut la preuve pour le cas $m = 1$.
Si $m > 1$ on peut se ramener au cas précédent en construisant le polynôme à une variable $\tilde{f} \in \mathbb{Z}_p[X_j]$ obtenu en remplaçant les X_i par x_i pour $i \neq j$.On applique le résultat précédent à $\tilde{f}$ et à x_j. On prouve ainsi l'existence de $y_j \equiv x_j \pmod{p^{n-k}}$ avec $\tilde{f}(y_j) = 0$. On pose $y_i = x_i$ pour $i \neq j$ et $y = (y_i)$ est solution.

Corollaire 3. *1. Tout zéro simple de la réduction modulo p d'un polynôme f se relève en un zéro de f à coefficients dans Z_p. (On rappelle que si Q est un polynôme sur un corps, un zéro de Q est dit simple si au moins l'une des dérivées partielles $\frac{\partial Q}{\partial X_j}$ est nul en x.)*

Corollaire 4. *Supposons que $p \neq 2$. Soit $f(X) = \sum a_{ij}X_iX_j$ avec $a_{ij} = a_{ji}$, une forme quadratique à coefficients dans Z_p dont le discriminant $det(a_{ij})$ est inversible. Soit $a \in Z_p$. Toute solution primitive de l'équation $f(x) \equiv a \pmod p$ se relève en une solution exacte.*

§3. Le groupe multiplicatif Q_p

3.5 La filtration du groupe des unités.

ds
On note U le groupe des inversibles de Z_p, $\pi_n : Z_p \to Z/p^nZ$ pour tout $n \in \mathbb{N}^*$ les surjections canoniques, qui induisent les morphismes surjectifs $\epsilon_n : U \to (Z/p^nZ)^*$. On pose $U_n := 1 + p^nZ_p$. La suite $1 \to U_n \to U \to (Z/p^nZ)^* \to 1$ est exacte.

Par ailleurs $\lambda : U_n \to Z/pZ;\ 1 + p^nx \mapsto x$ est un morphisme de groupe de noyau U_{n+1}, ce qui donne un isomorphisme $U_n/U_{n+1} \cong C_p$, et donc par récurrence $Card([U_i : U_j]) = p^{j-i}$. On peut en fait être plus précis. On a pour tous $i \in \mathbb{N}^*$ ($i > 1$ dans le cas $p = 2$), $n \in \mathbb{N}$ et $\alpha \in U_i \backslash U_{i+1}$, $\alpha^{p^n} \in U_{i+n} \backslash U_{i+n+1}$, si bien que pour tout $j > i$, U_i/U_j est cylcique engendré par la classe de α dans U_i/U_j, soit $U_i/U_j \cong C_{p^{j-i}}$. On note $\theta_{\alpha,i}$ l'isomorphisme de C_{p^i} vers U_1/U_{i+1} (resp de C_{2^i} vers U_2/U_{i+2} pour $p = 2$)

On considère le polynôme $P := X^{p-1} - 1 \in Z_p[X]$. Ce dernier admet $p-1$ racines dans $\mathbb{F}_p^*$ qui se relèvent en $p-1$ solutions dans Z_p. Ces solutions forment un sous groupe V de U de cardinal $p-1$ (qui est même isomorphe à $\mathbb{F}_p^* \cong C_{p-1}$: on hérite de la structure de groupe de $(Z/p^nZ)^*$).

Lemme 7. *$U = V \bigoplus U_1$*

Démonstration. On pose $W := V \cap U_1$. Pour tout $n \in \mathbb{N}^*$, $\epsilon_n(W)$ est isomorphe à C_d pour un certain diviseur d de $p-1$ en tant que quotient de V, et est un sous groupe de U_1/U_n. Ce dernier étant d'ordre p^{n-1}, il suit $\epsilon_n(W) = 1$ et $W \subset U_n$. Ainsi $W \subset \bigcap_{n=1}^{\infty} U_n = 1$. On pose $Y := V \bigoplus U_1$. On a $Y/U_1 \cong V \cong C_{p-1}$ et donc $[U : Y] = [U : U_1]/[Y : U_1] = 1$ et $U = Y = V \bigoplus U_1$.

Lemme 8. *Soient G un groupe abélien muni d'une disgtance d complète et bornée sur G telle que $\forall a, b, c \in G$, $d(ac, bc) = d(a, b)d(1, c)$ et soit $(U_i)_{i\in\mathbb{N}^*}$ une suite décroissante de sous groupes stricts de diamètre convergeant vers 0. Alors $G \cong \varprojlim G/U_i$.*

Démonstration. Le morphisme $\psi : G \to \varprojlim G/U_i$; $g \mapsto [g]_{U_i}$ a pour noyau $Ker = \bigcap_{i\in\mathbb{N}^*} U_i$, si bien que l'unique problème à résoudre est celui de la surjectivité. Soit $y = ([g_i]_{U_i})_{i\in\mathbb{N}^*} \in \varprojlim G/U_i$, la suite $(g_i)_{i\in\mathbb{N}^*}$ est de Cauchy, et converge donc vers un certain $g \in G$, qui fournit alors un antécédent de y pour ψ.

Proposition 6. *$U_1 \cong Z_p$ si $p \neq 2$ et $U_1 \cong Z^* \times U_2$ avec $U_2 \cong Z_2$ pour $p = 2$.*

Démonstration. On a vu que pour tout $i \in N^*$ (resp $i > 1$ si $p = 2$), $U_1/U_i \cong Z/p^{i-1}Z$ (resp $U_2/U_i \cong Z/p^{i-2}Z$). On vérifie alors que les isomorphismes $\theta_{\alpha,i}$:

$Z/p^iZ \tilde{\to} U_1/U_{i+1}$ sont compatibles avec les systèmes projectifs :

$$\begin{array}{ccc} Z/p^iZ & \xrightarrow{\theta_{\alpha,i}} & U_1/U_{i+1} \\ \downarrow & & \downarrow \\ Z/p^{i-1}Z & \xrightarrow[\theta_{\alpha,i-1}]{} & U_1/U_i \end{array}$$

Par application du lemme précédent, il suit $U_1 \cong \varprojlim U_1/U_i \cong \varprojlim Z/p^iZ = Z_p$ et $U_2 \cong \varprojlim U_2/U_i \cong \varprojlim Z/2^iZ = Z_2$ Il ne reste plus qu'à démontrer que dans le cas où $p = 2$, $U_1 = \mathbb{Z}^* \bigoplus U_2$. $-1 \notin U_2$ si bien que $\{\pm 1\} \bigoplus U_2$. De plus, si $y \in U_1$, on écrit $y = 1 + 2x$. Si $x \notin U_1$ alors $x \in 2Z_2$ et $y \in U_2$, sinon x s'écrit $x = -1 + 2\tilde{x}$ d'où $y = 1 + 2(-1 + 2\tilde{x}) = -1 + 4\tilde{x} = (-1)(1 - 4\tilde{x}) \in \{\pm 1\} \bigoplus U_2$

Proposition 7. *$U \cong \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}_p$ pour $p \neq 2$ et $U \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}_2$*

Démonstration. Clair d'après les propositions précédentes.

Proposition 8. *$\mathbb{Q}_p^* \cong Z \times \mathbb{Z}_p \times \mathbb{Z}/(p-1)\mathbb{Z}$ pour $p \neq 2$ et $\mathbb{Q}_2^* \cong Z \times \mathbb{Z}_2 \times \mathbb{Z}/2\mathbb{Z}$.*

Démonstration. $\mathbb{Q}_p^* \cong Z \times U$ traduit simplement le fait que tout élément x de $\mathbb{Q}_p^*$ s'écrit de manière unique sous la forme $x = p^n \times u$ avec $n \in Z$ et $u \in U$. Le reste découle de la structure des inversibles de $\mathbb{Z}_p$.

3.6 Carrés de Q_p^*

Proposition 9. *$\mathbb{Q}_p^*/\mathbb{Q}_p^{*[2]} \cong (\mathbb{Z}/2\mathbb{Z})^2$ pour $p \neq 2$ et $\mathbb{Q}_2^*/\mathbb{Q}_2^{*[2]} \cong (\mathbb{Z}/2\mathbb{Z})^3$.*

Démonstration. Pour $p \neq 2$, on a $\mathbb{Q}_p^{*[2]} \cong 2\mathbb{Z} \times 2\mathbb{Z}_p \times 2(\mathbb{Z}/(p-1)\mathbb{Z}) = 2\mathbb{Z} \times \mathbb{Z}_p \times (2\mathbb{Z})/(p-1)\mathbb{Z}$ (car 2 est inversible dans $\mathbb{Z}_p$) d'où $\mathbb{Q}_p^*/\mathbb{Q}_p^{*[2]} \cong (Z \times \mathbb{Z}_p \times \mathbb{Z}/(p-1)\mathbb{Z})/(2\mathbb{Z} \times \mathbb{Z}_p \times 2\mathbb{Z}/(p-1)\mathbb{Z}) \cong Z/2\mathbb{Z} \times Z_p/\mathbb{Z}_p \times (\mathbb{Z}/(p-1)\mathbb{Z})/(2\mathbb{Z}/(p-1)\mathbb{Z}) \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$.
Pour $p = 2$, on a $\mathbb{Q}_2^{*[2]} \cong 2\mathbb{Z} \times 2\mathbb{Z}_2 \times 2(\mathbb{Z}/2\mathbb{Z}) = 2\mathbb{Z} \times 2\mathbb{Z}_2 \times$ (car $2(\mathbb{Z}/2\mathbb{Z}) = 0$) d'où $\mathbb{Q}_2^*/\mathbb{Q}_2^{*[2]} \cong (Z \times \mathbb{Z}_2 \times \mathbb{Z}/2\mathbb{Z})/(2\mathbb{Z} \times 2\mathbb{Z}_2 \times 0 \cong Z/2\mathbb{Z} \times Z_2/2\mathbb{Z}_2 \times (\mathbb{Z}/2\mathbb{Z})/0 \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$.

En regardant précisément ce qui se cache derrière les isomorphismes, les résultats précédents signifient que pour $p \neq 2$, $x = p^n u \in \mathbb{Q}_p^*$ est un carré si et seulement si n est pair et la classe de u modulo p est un carré, et également que le groupe $\mathbb{Q}_p^*/\mathbb{Q}_p^{*[2]}$ a pour représentants $1, p, u, up$ avec $u \in \mathbb{Q}_p^*$ tel que u n'est pas un carré modulo p. De même, pour $p = 2$, $x = 2^n u \in \mathbb{Q}_2^*$ est un carré si et seulement si n est pair et $u \equiv 1 (\mod 8)$ (ie u est un carré de $U = U_1 = \{\pm 1\} \bigoplus U_2$, c'est à dire si u est un carré de U_2 soit un élément de U_3). Enfin le groupe $\mathbb{Q}_2^*/\mathbb{Q}_2^{*[2]}$ a pour représentants $\pm 1, \pm 2, \pm 5, \pm 10$.

4 Chapitre III: Symbole de Hilbert

§1. Propriétés locales . Dans ce paragraphe, k désigne $\mathbf{R}$ ou $\mathbf{Q}_p$ avec p premier.

4.1 Définition et premières propriétés

Définition 5. *Soient $a, b \in k^*$. On définit :*

$(a, b) = 1$ si $z^2 - ax^2 - by^2 = 0$ a une solution non nulle dans k^3;
$(a, b) = -1$ dans le cas contraire.

Le nombre $(a, b) \pm 1$ s'appelle le symbole de Hilbert de a et de b, relativement à k. On peut remarquer que (a, b) ne change pas si on multiplie a et b par des carrés; le symbole de Hilbert définit ainsi une application de k^*/k^{*2} dans $\{\pm 1\}$.

Proposition 10. *Soient $a, b \in k^{*[2]}$, et soit $k_b = k(\sqrt{b})$ le corps obtenu en adjoignant à k une racine carré de b. Pour que $(a, b) = 1$, il faut et il suffit que a appartienne au groupe Nk_b^* des normes des éléments de k_b^*.*

Démonstration.
Si b est un carré d'un élement c, on a $z^2 - ax^2 - by^2 = 0$ admet comme solution $(c, 0, 1)$, et l'on a $(a, b) = 1$ d'où le proposition car dans ce cas $k_b = k$ et $Nk_b = k^*$. Sinon k_b est quadratique sur k; si β désigne une racine carré de b, tout élement $\xi \in k_b$ s'écrit $z + \beta y$, avec $y, z \in k$, et la norme $N(\xi)$ de ξ est $z^2 - by^2$. Si $a \in {Nk_b}^*$, il existe donc $y, z \in k$ tels que $a = z^2 - by^2$, on remarque alors que la forme quadratique $z^2 - ax^2 - by^2$ a un zéro $(z, 1, y)$, et l'on a donc $(a, b) = 1$. Réciproquement, si $(a, b) = 1$, cette forme quadratique a un zéro $(z, x, y) \neq (0, 0, 0)$; on a alors nécessairement $x \neq 0$ car sinon b serait un carré; on en conclut que a est norme de $\frac{z}{x} + \beta\frac{y}{x}$.

Proposition 11. *$k^*/N(k_b^*)$ est un groupe de cardinal 2, donc isomorphe à C_2, dès lors que b n'est pas un carré de k.*

Démonstration. Ce résultat est clair pour $k = \mathbb{R}$. Pour $k = \mathbb{Q}_p$, on remarque que $\pi : k^* \to k^*/Nk_b^*$ induit la surjection $s : k^*/k^{*[2]} \to k^*/Nk_b^*$ qui fait de k^*/Nk_b^* un quotient de $k^*/k^{*[2]} \cong V_4$ (groupe de Klein). Il faut et il suffit donc de montrer, dans le cas $p \neq 2$, que ce quotient est non trivial (car $k^*/k^{*[2]} \cong (\mathbb{Z}/2\mathbb{Z})^2$), c'est à dire que $k^{*[2]} \subsetneq Nk_b^* \subsetneq k^*$.
Dans le cas $p = 2$, il faut être plus précis et exhiber deux éléments distincts dans $N(\mathbb{Q}_2)_b^* \backslash \mathbb{Q}_2^{*[2]}$ ainsi donc qu'un élément de $\mathbb{Q}_2^* \backslash N(\mathbb{Q}_2)_b^*$ (car $\mathbb{Q}_2^*/\mathbb{Q}_2^{*[2]} \cong (\mathbb{Z}/2\mathbb{Z})^3$)

Faute d'un résultat général sur la structure ou même juste le cardinal du groupe k^*/Nk_b^*, on doit traiter le problème directement, en distinguant différents cas de figures. On remarque que l'on peut traiter le problème acec n'importe quel représentant de la classe de b dans $k_b^*/k^{*[2]}$ en lieu et place de b.

1) $p \neq 2$
_ Si $b = u$ pour un certain $u \in U$, alors d'une part $p \in k^* \backslash Nk_b^*$, car on aurait sinon $p = x^2 - uy^2$ pour un certain $(x, y) \in \mathbb{Q}_p^2$, si bien que $X^2 - uY^2 - pZ^2 \in \mathbb{Z}_p[X, Y, Z]$ aurait un zéro non trivial dans $\mathbb{Q}_p^3$, soit également (étant homogène) un zéro primitif (x, y, z) dans $\mathbb{Z}_p^3$, en réduisant modulo p on aurait $v(x), v(y) > 0$ et donc $v(z) > 0$ absurde (contredit le caractère primitif). De plus, la forme quadratique $X^2 - uY^2 \in \mathbb{F}_p[X, Y]$ représente tout scalaire non nul, soit à fortiori tout scalaire

$z \in k \backslash k^{[2]}$, ce qui suffit pour conclure que $k^{*[2]} \subsetneq Nk_b^*$
_ Si $b = p$, alors pour tout $u \in k^* \backslash k^{*[2]}$, $u \in k^* \backslash Nk_b^*$, sans quoi on aurait $x^2 - py^2 = u$ pour un certain couple $(x, y) \in \mathbb{Q}_p^2$ avec forcément $y \neq 0$, d'où $(x/y)^2 - (1/y)^2 u = p$ ce qui est faux d'après 1). D'autre part, $-p \in Nk_b^* \backslash k^{*[2]}$.
_ Si $b = pu$, avec $u \in U$ (qui n'est pas un carré), alors $u \in k^* \backslash Nk_b^*$ sans quoi la forme quadratique $X^2 - puY^2 - uZ^2 \in \mathbb{Z}_p[X, Y, Z]$ aurait un zéro non trivial dans $\mathbb{Q}_p^3$, donc un zéro primitif (x, y, z) dans $\mathbb{Z}_p^3$, ce qui mène en réduisant modulo p à $v(x), v(z) > 0$ puis à $v(y) > 0$ ce qui contredit le caractère primitif de (x, y, z). Enfin, $-pu \in Nk_b^* \backslash k^{*[2]}$.
2) $p = 2$
admis

Corollaire 5. *Le symbole de Hilbert est une forme bilinéaire non dégénérée sur le $\mathbb{F}_2$-espace vectoriel k/k^{*2}. L'assertion "(a, b) est non dégénérée" signifie que, si $b \in k^*$ est tel que $(a, b) = 1$ pour tout $a \in k^*$, on a $b \in k^{*2}$.*

Démonstration. C'est effectivement une conséquence immédiate de la caractérisation de $(a, b) = 1 <=> a \in Nk_b^*$ et du fait que $k^*/Nk_b^* \cong C_2$.

Corollaire 6. *Le symbole de Hilbert vérifie les propriétés suivantes :*

i) $(a, b) = (b, a)$ *et* $(a, c^2) = 1$
ii) $(a, -a) = 1$
iii) $(a, b) = 1 \implies (aa', b) = (a', b)$
iv) $(a, b) = (a, -ab) = (a, (1 - a)b)$

4.2 Calcul de (a, b)

Théorème 8.
Si $k = \mathbb{R}$ on a $(a, b) = 1$ si a ou b est > 0 et $(a, b) = -1$ si a et b sont < 0.

Si $k = \mathbb{Q}_p$, et si l'on écrit a, b sous la forme $p^\alpha u$, $p^\beta v$ où $u, v \in U$ le groupe des unités p-adiques, on a en notant $\epsilon : x \mapsto \frac{x-1}{2}$ et $\omega : x \mapsto \frac{x^2-1}{8}$,

$(a, b) = (-1)^{\alpha\beta\epsilon(p)} (\frac{u}{p})^\beta (\frac{v}{p})^\alpha$ *pour* $p \neq 2$ *et* $(a, b) = (-1)^{\epsilon(u)\epsilon(v)+\alpha\omega(v)+\beta\omega(u)}$ *sinon.*

Démonstration. Preuve pour $p \neq 2$. En posant $[.,.]$ tel que $(-1)^{\alpha\beta\epsilon(p)} (\frac{u}{p})^\beta (\frac{v}{p})^\alpha = (-1)^{[a,b]}$ pour tous $a, b \in k$, on veut montrer que les deux formes bilinéaires non dégénérées $(.,.)$ et $[.,.]$ sont égales, ce qui est équivalent à montrer qu'elles coïncident sur la base (u, p) du $\mathbb{F}_2$ plan vectoriel $\mathbb{Q}_p^*/\mathbb{Q}_p^{*[2]}$, et donc que $(u, u) = 1$, $(p, p) = (-1)^{\epsilon(p)}$, et $(u, p) = (\frac{u}{p})$.
$(u, u) = 1$ découle du fait que la forme $Q := X^2 - uY^2 - uZ^2$ représente 0 dans $\mathbb{F}_p$ et que tout vecteur isotrope dans $\mathbb{F}_p^3$ se relève en un vecteur isotrope dans $\mathbb{Z}_p^3$.
Si u n'est pas un carré, $(u, p) = -1$ sans quoi on aurait $(u, y) = 1$ pour tout $y \in Vect_{\mathbb{F}_2}(u, p) = \mathbb{Q}_p^*/\mathbb{Q}_p^{*[2]}$ ce qui contredit le caractère non dégénéré de $(.,.)$. Sinon $(u, p) = 1$.
$(p, p) = (p, -p^2) = (p, -1)$ et l'on est ramené au cas précédent avec $u = -1$.

§2. Propriétés globales .
Le corps $\mathbb{Q}$ se plonge comme sous-corps dense dans chacun des corps $\mathbb{Q}_p$ et $\mathbb{R}$. Si $a, b \in \mathbb{Q}^*$, on note $(a,b)_p$ (resp $(a,b)_\infty$ le symbole de Hilbert de leur images dans $\mathbb{Q}_p$ (resp $\mathbb{R}$). On désigne par V la réunion de l'ensemble des nombres premiers et du symbole ∞, et l'on convient que $\mathbb{Q}_\infty = \mathbb{R}$.

4.3 La formule du produit

Théorème 9. *Si $a, b \in \mathbb{Q}^*$, on a $(a,b)_v = 1$ pour presque tout $v \in V$, et $\prod_{v\in V}(a,b)_v = 1$.*

5 Chapitre IV : Formes quadratiques sur $\mathbb{Q}_p$ et sur $\mathbb{Q}$

§1. Formes quadratiques .

5.1 Définitions

Définition 6. *Soit V un module sur un anneau commutatif A. Une application $Q : V \to A$ est une forme quadratique si :*

i) $Q(ax) = a^2 x \ \forall (a,x) \in A \times V$

ii) L'application $b : (x,y) \mapsto Q(x+y) - Q(x) - Q(y)$ est une forme bilinéaire.

Le couple (V,Q) est un module quadratique.

Dans tout ce chapitre, nous nous considérerons le cas où l'anneau A est un corps k de caractéristique $\neq 2$. Le A-module V est alors un k-espace vectoriel qui sera supposé de dimension finie.

On définit le produit scalaire associé à la forme quadratique Q par :

$$x.y = \tfrac{1}{2}(Q(x+y) - Q(x) - Q(y))$$

C'est une forme bilinéaire symétrique avec $\forall x \in V, Q(x) = x.x$.

Si (V,Q) et (V',Q') sont deux modules quadratiques on appelle morphisme de (V,Q) dans (V',Q') toute application linéaire $f : V \to V'$ telle que $Q' \circ f = Q$. On a donc $\forall x, y \in V \ x.y = f(x).f(y)$.

Proposition 12. *Matrice d'une forme quadratique. Soit $(e_i)_{1\leq i\leq n}$ une base de V. On appelle matrice de Q par rapport à cette base de la matrice $A = (a_{ij})$ où $a_{ij} = e_i.e_j$; c'est une matrice symétrique. Si $x = \sum_i e_i$ est un élément de V, on a $Q(x) = \sum_{i,j} a_{i,j}x_ix_j$. En particulier en notant X, Y les vecteurs colonnes des coordonnées de x et y dans la base, on a $x.y = Y^TAX$. Si l'on modifie la base $(e_i)_{1\leq i\leq n}$ par une matrice inversible M, la matrice A' de Q dans la nouvelle base est MAM^T. On a donc $\det(A') = \det(A)\det(M)^2$, ce qui montre que $\det(A)$ est connu à une multiplication près d'un élément de $k^{*[2]}$; on l'appelle le discriminant de Q noté disc(Q).*

5.2 Orthogonalité

Définition 7. *Soit (V, Q) un module quadratique sur k.*
i) Deux éléments x, y de V sont orthogonaux si $x.y = 0$.

i)) Pour $H \subset V$ on définit l'orthogonal de H par $H^0 = \{x \in V \mid \forall y \in H, x.y = 0\}$. C'est un sous-espace vectoriel de V.

iii) Si V_1, V_2 sont deux sous-espaces vectoriels de V on dit que V_1 et V_2 sont orthogonaux si $V_1 \subset {V_2}^0$.

iv) On appelle radical de V noté $rad(V)$ l'ensemble V^0. La codimension de $rad(V)$ s'appelle rang de Q. Si $rad(V) = \{0\}$ on dit que Q est non-dégénérée ie $disc(Q) \neq 0$.

Proposition 13. *Soit U un sous-espace vectoriel de V, et soit U^* le dual de U. Soit $q_U : V \to U^*$ l'application qui associe à tout $x \in V$ la forme linéaire $x.()$. Le noyau de q_U est U^0 ainsi on remarque que Q non-dégénérée $\iff$ $q_V : V \to V^*$ est un isomorphisme.*

Démonstration. Le caractère linéaire est évident d'après la bilinéarité du produit scalaire associé à Q. En dimension finie un sous-espace vectoriel et son dual ont même dimension. Et pour une application linéaire entre deux sous-espaces vectoriels de même dimension la bijectivité est équivalente à l'injectivité elle même équivalente au fait que le noyau est réduit à $\{0\}$.

Définition 8. *Soient $U_1, ..., U_m$ des sous-espaces vectoriels de V. On dit que V est somme directe orthogonale des U_i si :*

$V = U_1 \oplus \ldots \oplus U_m$ et $U_i \subset U_j^0, \forall i \neq j \in [\![1, m]\!]$.

Dans ce cas, on note $V = U_1 \overset{\wedge}{\oplus} \ldots \overset{\wedge}{\oplus} U_m$.

Proposition 14. *Soient $U_1, ..., U_m$ des sous-espaces vectoriels de V avec $V = U_1 \overset{\wedge}{\oplus} \ldots \overset{\wedge}{\oplus} U_m$. Si $x \in V$ a pour composante x_i dans U_i on a :*

$$Q(x) = Q_1(x_1) + \ldots Q_m(x_m)$$

où Q_i est la restriction de Q à U_i.

Proposition 15. *Si U est un supplémentaire de $rad(V)$ dans V, on a $V = U \overset{\perp}{\oplus} rad(V)$.*

Démonstration. On a par hypothèse que $V = U \oplus rad(V)$ et par comme $U \subset V$, on a bien $rad(V) \subset U^0$.

Proposition 16. *Si (V, Q) est non-dégénérée. Alors :*

i) Tout morphisme métrique de V dans un module quadratique (V', Q') est injectif.

ii) Pour tout sous-espace vectoriel U de V, on a : $U^{0^0} = U$, $dim(U) + dim(U^0) = dimV$ et $rad(U) = rad(U^0) = U \cap U^0$.

iii) Pour que U soit non dégénéré, il faut et il suffit que U^0 le soit, dans ce cas $V = U \overset{\perp}{\oplus} U^0$.

iv) Si V est somme directe orthogonale de deux sous-espaces vectoriels, ceux-ci sont non dégénérés, et chacun d'eux est l'orthogonal de l'autre.

Démonstration. Si $f : V \to V'$ est un morphisme métrique, et si $f(x) = 0$ on $x.y = f(x).f(y) = 0, \forall y \in V$. Comme (V, Q) est non dégénérée on a $x = 0$. Si U est un sous-espace vectoriel de V, l'application linéaire $q_U : V \to U^*$ qui a $x \in V$ associe $x._U$ est surjective, on compose par $q_V : V \to V^*$ bijective ,car (Q, V) non dégénérée, et la surjection canonique $V^* \to U^*$. D'après le théorème du rang, on a $dim(V) = rg(q_U) + dim(Ker(q_U))$ ie $dim(V) = dim(U^*) + dim(U^0)$ or en dimension finie $dim(U^*) = dim(U)$ donc $dim(V) = dim(U) + dim(U^0)$. Ceci prouve que $dim(U) = dim(U^{0^0})$ or $U \subset U^{0^0}$ donc par égalité des dimensions on a l'égalité des 2 ensembles. Par définition $rad(U) = \{x \in U, \forall y \in U, x.y\} = U \cap U^0$. Comme $U^{0^0} = U$ on a $rad(U) = rad(U^{0^0})$. On a U non dégénéré $\iff rad(U) = \{0\}$, comme $dim(V) = dim(U) + dim(U^0)$ on a directement que la somme est directe et orthogonale par définition de U^0.

5.3 Vecteurs isotropes

Définition 9. *Soit $x \in V$ avec (V, Q) un module quadratique. On a dit que x est isotrope si $Q(x) = 0$. Un sous-espace vectoriel U de V est isotrope si tous ses éléments le sont.*

On remarque alors : U isotrope $\iff U \subset U^0 \iff Q_{|U} = 0$.

Définition 10. *On appelle plan hyperbolique tout module quadratique ayant une base formée de deux vecteurs isotropes x, y avec $x.y \neq 0$.*

Quitte à multiplier y par $\frac{1}{x.y}$ on peut supposer que $x.y = 1$. Si on considère la matrice de la forme quadratique par rapport à x, y, c'est

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

son discriminant vaut $-1 \neq 0$ donc est non dégénérée.

Proposition 17. *Soit x isotrope $\neq 0$, $\in V$ où (V, Q) est un module quadratique non dégénéré. Il existe alors un sous-espace vectoriel U de V qui contient x et qui est un plan hyperbolique.*

Démonstration. Comme (V, Q) est non dégénéré et x non nul on sait qu'il existe $z \in V$ tel que $x.z = 1$ (quitte à multiplier par un scalaire). Posons $y = 2z - (z.x)x$, y est isotrope et $x.y = 2$. Le sous-espace vectoriel $U = Vect(x, y)$ convient.

Corollaire 7. *Si (V, Q) est non dégénéré et contient un élement isotrope non nul, alors $Q(V) = k$.*

Démonstration. D'après la proposition précédente on peut se resteindre à un plan hyperbolique de base (x, y) avec x, y isotropes et $x.y = 1$. Si $a \in k$ on a $Q(x + \frac{a}{2}y) = (x + \frac{a}{y}).(x + \frac{a}{y}) = x.x + \frac{a^2}{4}y.y + 2\frac{a}{2}x.y = a$ car x et y sont isotropes et $x.y = 1$.

5.4 Bases orthogonales

Définition 11. *Une base $(e_1, \ldots, e_n)$ d'un module quadratique (V, Q) est orthogonale si elle est formée d'éléments deux à deux orthogonaux. Il est équivalent d'affirmer que la matrice de Q dans cette base est* $\begin{pmatrix} a_1 & 0 & \ldots & 0 \\ 0 & a_2 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & a_n \end{pmatrix}$.

On en déduit que si $x = \sum_{i=1}^{n} x_i e_i$, on a $Q(x) = a_1 x^2 + \ldots + a_n x^2$.

Théorème 10. *Tout module quadratique (V, Q) possède une base orthogonale.*

Démonstration. On raisonne par récurrence sur $n = dim(V)$.Si $n = 0$ trivial. Si V est isotrope, toute base de V est orthogonale. Dans le cas contraire on choisit $e_1 \in V$ tel que $e_1.e_1 \neq 0$. L'orthogonal H de e_1 est un hyperplan et comme $e_1 \notin H$, on a $V = ke_1 \overset{\wedge}{\oplus} H$. D'après l'hypothèse de récurrence, H possède une base orthogonale $(e_2, \ldots, e_n)$; par concaténation (somme directe orthogonale) $(e_1, e_2, \ldots, e_n)$ est une base de V.

5.5 Théorème de Witt.

Théorème 11. *Soient (V, Q) et (V', Q') deux modules quadratiques non dégénérés et isomorphes, soit U un sous-espace vectoriel de V, et soit $s : U \to V'$ un morphisme métrique injectif. On peut alors prolonger s en un isomorphisme de V sur V'.*

Lemme 9. *Si U est dégénéré, on peut prolonger s en un morphisme métrique injectif $s_1 : U_1 \mapsto V'$ où U_1 contient U comme hyperplan.*

Démonstration. Soient $x \in rad(U)$ non nul (existe car U dégénéré) et l une forme linéaire sur U telle que $l(x) = 1$. Or V est un espace quadratique de dimension finie non dégénéré donc il existe $y \in V$ tel que $l(z) = z.y$ pour tout $z \in U$. On peut remarquer qu'on peut choisir y isotrope en effet on remplace y par $y - \frac{y.y}{2}x$. On pose

donc $U_1 = U \oplus ky$ contient U comme hyperplan. On applique la même construction mais cette fois à $U' = s(U)$, $x' = s(x)$ et $l' = l \circ s^{-1}$.

5.6 Traductions

Soit $f(X) = \sum_{i=1}^{n} a_{ii} {X_i}^2 + 2\sum_{i<j} a_{ij} X_i X_j$ une forme quadratique avec n variables sur k. On pose $a_{ij} = a_{ji}$ pour $i < j$ pour que la matrice $A = (a_{ij})$ soit symétrique. Le couple (k^n, f) est un module quadratique associé à f (ou à la matrice A).

Définition 12. *Deux formes quadratiques f et f' sont dites équivalentes si les modules quadratiques associés sont isomorphes. Dans ce cas, on note $f \sim f'$.En notant A et A' les matrices de f et f', on a $f \sim f'$ s'il existe M une matrice inversible telle que $A' = MAM^T$.*

Définition 13. *Soient $f(X_1, \dots, X_n)$ et $g(X_1, \dots, X_m)$ deux formes quadratiques, on définit $f \dot{+} g$ la forme quadratique de $n+m$ variables $f(X_1, \dots, X_n) + g(X_{n+1}, \dots, X_m)$. On définit de manière analogue $f \dot{-} g$.*

Définition 14. *Une forme quadratique $f(X_1, X_2)$ est dite hyperbolique si l'on a : $f \sim X_1 X_2 \sim {X_1}^2 - {X_2}^2$. Le module quadratique (k^2, f) est alors un plan hyperbolique.*

Définition 15. *La forme quadratique $f(X_1, \dots, X_n$ représente $a \in k$ s'il existe $x = (x_1, \dots, x_n) \neq 0$ tel que $f(x) = a$. Ainsi f représente 0 si (k^n, f) contient un vecteur isotrope non nul.*

Proposition 18. *Si f représente 0, et est non dégénérée, on a $f \sim f_2 \dot{+} g$ avec f_2 hyperbolique. De plus f représente tout élément de k.*

Démonstration. Par hypothèse il existe x un élément isotrope non nul et f non dégénérée d'après la proposition 3 il existe un sous-espace U de V qui contient x avec U un plan hyperbolique. On note g la restriction de f à U^0 et f_2 celle restreinte à U. On a $disc(f_2) = -1 \neq 0$ donc f_2 est non dégénérée donc on a bien la somme directe orthogonale. Et on conclut avec le corollaire 6.

Corollaire 8.
Soit $g = g(X_1, \dots, X_{n-1})$ une forme quadratique non dégénérée, et soit $a \in k^*$. On a :
i) g représente a.
$\iff$
ii) On a $g \sim h \dot{+} aZ^2$ où h est une forme linéaire en $n-2$ variables.
$\iff$
La forme $f = g \dot{-} aZ^2$ représente 0.

Démonstration. On remarque directement que $ii) \implies i)$. On s'intéresse désormais à la réciproque. Si g représente a dès lors il existe $x \in V$ tel que $x.x = a$, on désigne par H l'orthogonal de x. D'après la proposition 15 (x est isotrope donc (kx, Q) est non dégénéré) on a $V = H \hat{\oplus} kx$ d'où $g \sim h + aZ^2$ où h est la forme quadratique associée à une base de H. On a aussi $ii) \implies iii)$ directement. Réciproquement, si $f = g \dot{-} aZ^2$ a un zéro non trivial $(x_1, \dots, x_{n-1}, z)$ on a soit

$z = 0$, auquel cas g représente 0 donc via la proposition 17 g représente a. Sinon $z \neq 0$ on a $g(\frac{x_1}{z}, \ldots, \frac{x_{n-1}}{z}) = a$ et donc *iii)* $\implies$ *i)*.

Corollaire 9. *Soient g et h deux formes quadratiques non dégénérées de rang ≥ 1, et soit $f = g \dot{-} h$. On a :*
i) f représente 0.
$\iff$
ii) Il existe $a \in k^*$ qui est représenté par h et par g.
$\iff$
iii) Il existe $a \in k^*$ tel que $g \dot{-} aZ^2$ et $h \dot{-} aZ^2$ représente 0.

Démonstration. D'après le corollaire précédent on a *ii)* $\iff$ *iii)*. De plus l'implication *ii)* $\implies$ *i)* est évidente. Désormais montrons que *i)* $\implies$ *ii)*. Un zéro non trivial de f peut s'écrire sous la forme (x, y), avec $g(x) = h(y)$. On note $a = g(x) = h(y)$. Si $a \neq 0$ ii) est claire. Si $a = 0$ l'une des formes représente 0. Par exemple g, ainsi d'après la proposition 17, tout élément de k est représenté par g et donc toute valeur non nulle prise par h est aussi représentée.

Théorème 12. *Décomposition des formes quadratiques en "sommes de carrés". Soit f une forme quadratique en n variables. Il existe $a_1, \ldots, a_n \in k$ tels que $f \sim a_1 {X_1}^2 + \ldots + a_n {X_n}^2$. Le rang de f*

5.7 Forme quadratique sur les corps finis

Théorème 13. *Soit k un corps de cardinal q. Tout $k-$ espace quadratique (E, Q) de dimension $n \geq 3$ est isotrope.*

Démonstration.
Il suffit de montrer le résultat pour $E = k^n$ et pour $n = 3$. Le résultat est clair si Q est dégénérée, et on la suppose donc dorénavant non dégénérée.
Soit a un élément de $k^*[2]$. Le sous groupe $k^*[2]$ étant d'indice 2 dans k, il suit en diagonalisant Q que celle ci est congruente à l'une des formes canoniquement associées à $diag(1, 1, 1)$, $diag(1, 1, a)$, $diag(1, a, a)$ et $diag(a, a, a)$. Quitte à raisonner sur aQ en lieu et place de Q, on peut se ramener aux deux cas (1) $Q \approx diag(1, 1, a)$ et (2) $Q \approx diag(1, 1, 1)$.

Cas n°1:
Si -1 est le carré d'un élément $x \in k^*$, alors le vecteur $(x, 1, 0)$ est isotrope.
Sinon, on a peut être choisi égal à -1, si bien que le vecteur $(1, 0, 1)$ est isotrope.

Cas n°2:
Si $-1 \in k^{[2]}$, on conclut comme au cas précédent. Sinon, la fonction $f : x \mapsto x + 1$ de k dans lui même ne laissant aucune partie non triviale de k stable, on déduit l'existence de c dans $k^{[2]}$ tel que $c + 1 \in k \setminus k^{[2]}$, c'est à dire de $x, y \in k$ tels que $x^2 + 1 = -y^2$, le vecteur $(x, 1, y)$ est alors isotrope.

Corollaire 10. *Soient k un corps de cardinal q et (E, Q) un espace quadratique de dimension $n \geq 2$, alors $D(Q) = k^*$.*

Démonstration. Clair.

Proposition 19. *[Classification]. Soit (E, Q) un espace quadratique non dégénéré de dimension $n \in \mathbb{N}^*$. Alors, Q est équivalente à $X_1^2 + ... + X_{n-1}^2 + X_n^2$ ou à $X_1^2 + ... + X_{n-1}^2 + aX_n^2$ où $a \in k \backslash k^{[2]}$. Notamment, deux formes quadratiques non dégénérées (de même dimension) sont équivalentes si et seulement si elles ont même discriminant.*

Démonstration. Le résultat se démontre par récurrence sur n. Pour l'hérédité, Q représente 1, on peut donc écrire $Q = Q' \bigoplus 1$ et appliquer l'hypothèse de récurrence sur Q'.

Proposition 20. *[Simplification de Witt]. Soit k un corps de caractéristique non 2. Soient $M = \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}$ et $M' = \begin{pmatrix} A' & 0 \\ 0 & B' \end{pmatrix}$ deux matrices de $S_n(k) \cap GL_n(k)$ congruentes. Alors si B et B' sont congruentes, A et A' le sont également.*

Démonstration. Le résultat se démontre par récurrence, par réduction mattricielles des matices symétriques, il suffit de traiter le cas $B = B' = \beta \in k^*$. On dispose de $P = \begin{pmatrix} P & C \\ L & q \end{pmatrix} \in GL_n(k)$ telle que $M' = PM^tP = \begin{pmatrix} PA^tP + \beta C^tC & PA^tL + \beta qC \\ LA^tP + \beta q^tC & LA^tL + \beta q^2 \end{pmatrix}$ ce qui se synthétise en le système suivante

$$\begin{cases} PA^tP = A' - \beta C^tC \\ PA^tL = -\beta qC \\ LA^tL = (1 - q^2)\beta \end{cases}$$

On pose pour tout $\lambda \in k$, $Q_\lambda := P + \lambda CL$, on va montrer qu'il existe $\lambda \in k^*$ tel que $Q_\lambda A^t Q_\lambda = \lambda^2 A'$ ce qui suffira à conclure quant à la congruence de A et A' (Q_λ sera alors automatiquement inversible, la matrice de passage sera donc $(1/\lambda)Q_\lambda$). On a pour tout $\lambda \in k$, $Q_\lambda A^t Q_\lambda = PA^tP + \lambda(PA^tL^tC + CLA^tP) + LA^tLC^tC = \lambda^2 A' - (\beta\lambda^2 + 2\beta\lambda q + (q^2 - 1)\beta)C^tC$. Le trinome $\beta X^2 + 2\beta qX + (q^2 - 1)\beta$ admet deux racines distinctes (son discriminant vaut $\Delta = \beta^2 \neq 0$), dont forcément une non nulle. Le résultat suit.

5.8 Formes quadratiques sur $\mathbb{R}$

Proposition 21. *[Classification] Soit (E, Q) un espace quadratique non dégénéré de dimension $n \in \mathbb{N}^*$. Alors, Q est équivalente à $X_1^2 + ... + X_r^2 - Y_1^2 - ... - Y_s^2$ où $(r, s) \in \mathbb{N}^2$ avec $r + s = n$. Le couple (r, s) est appelé la signature de Q notée $sgn(Q)$ et est un invariant classifiant : deux formes quadratiques non dégénérées (de même dimension) sont équivalentes si et seulement si elles ont même signature.*

Démonstration. Il y a juste à montrer que la signature est invariante. On va montrer que dans la signature $sgn(Q) = (r, s)$, les valeurs r et s s'interprètent en fait comme la dimension maximale d'un sous espace défini positif respectivement défini négatif, ce qui suffira pour conclure. Soient $\mathbf{e} = (e_1, ..., e_r, \epsilon_1, ..., \epsilon_s)$ une base dans laquelle Q se représente par $\begin{pmatrix} I_r & 0 \\ 0 & -I_s \end{pmatrix}$, $R := Vect(e_1, ..., e_r)$, $S := Vect(\epsilon_1, ..., \epsilon_s)$ et F un sous espace défini positif de dimension maximale d. Comme R est défini positif, il suit

$d \geq r$, par ailleurs, comme S est défini négatif, il suit $F \cap S = \{0\}$, d'ou $d + s \leq n$, c'est à dire $d \leq n - s = r$, et donc $d = r$.

Autre preuve:
Matrciellement, on montre que si $M := \begin{pmatrix} I_r & 0 \\ 0 & -I_s \end{pmatrix} \cong \begin{pmatrix} I_{r'} & 0 \\ 0 & -I_{s'} \end{pmatrix} =: M'$ alors $(r, s) = (r', s')$. $s = 0 <=> s' = O$ (équivaut à dire que la forme quadratique associée est définie positive), dans ce cas on a clairement l'égalité souhaitée, sinon, on a $M = \begin{pmatrix} I_r & 0 & 0 \\ 0 & -I_{s-1} & 0 \\ 0 & 0 & -1 \end{pmatrix} \cong \begin{pmatrix} I'_r & 0 & 0 \\ 0 & -I_{s'-1} & 0 \\ 0 & 0 & -1 \end{pmatrix} = M'$ et le lemme de simplification de Witt permet de conclure par récurrence.

5.9 Formes quadratiques sur $\mathbb{Q}_p$

Dans cette section, $k = \mathbb{Q}_p$.

Définition 16. *Soient (E, Q) un espace quadratique, $e = (e_1, ..., e_n)$ une base orthogonale, $a_i := Q(e_i)$ pour tout $i \in [\![1, n]\!]$. On pose $\epsilon(e) := \prod_{i<j}(a_i, a_j)$.*

Lemme 10. *Soit (E, Q) un espace quadratique non dégénéré. On dit que deux bases orthogonales $\boldsymbol{e} = (e_i)_{1\leq i\leq n}$ et $\boldsymbol{e'} = (e'_i)_{1\leq i\leq n}$ sont contigues si elles partagent un vecteur commun et l'on note $\boldsymbol{e} C \boldsymbol{e'}$, et qu'elles sont équivalentes s'il existe une chaîne de bases orthogonales $(\boldsymbol{e}_l)_{1\leq l\leq n}$ contigues deux à deux reliant $\boldsymbol{e}$ à $\boldsymbol{e'}$ ("être équivalent" est la relation d'équivalence engendrée par la relation C "être contigu". Si $n \geq 3$, deux bases orthogonales quelconques sont équivalentes.*

Démonstration. On se donne deux bases orthogonales $\mathbf{e} = (e_i)_{1\leq i\leq n}$ et $\mathbf{e'} = (e'_i)_{1\leq i\leq n}$ d'un espace quadratique (E, Q) de dimension $n \geq 3$. On distingue deux cas.
1) $\exists i, j \in [\![1, n]\!]$, $Q(e_i)Q(e'_j) - b_Q(e_i, e'_j)^2 \neq 0$:
Cela signifie qu'il existe des vecteurs e_i dans $\mathbf{e}$ et e'_j dans $\mathbf{e'}$ tel que l'espace P engendré par e_i, e'_j est un plan non dégénéré. Quitte à permuter les e_k et e'_l, on peut supposer $i = j = 1$. Dans ce cas l'orthogonal H de P est un supplémentaire de P dont on peut fixer une base orthogonale $(\epsilon_3, ..., \epsilon_n)$. En posant ϵ_2 et ϵ'_2 tels que $ke_1 \overset{\perp}{\oplus} k\epsilon_2 = P$ et $ke'_1 \overset{\perp}{\oplus} k\epsilon'_2 = P$, on a la chaîne $\mathbf{e} \to (e_1, \epsilon_2, \epsilon_3, ..., \epsilon_n) \to (e'_1, \epsilon'_2, \epsilon_3, ..., \epsilon_n) \to \mathbf{e'}$ et le résultat suit dans ce cas.
2) $\forall i, j \in [\![1, n]\!]$, $Q(e_i)Q(e'_j) - b_Q(e_i, e'_j)^2 = 0$:
Le résultat va découler du fait que l'on peut trouver un vecteur $e_x := e'_1 + xe'_2$ non isotrope et qui engendre avec e_1 un plan non dégénéré; par anisotropie de e_x, on pourra alors choisir $e''_2 \in E$ tel que (e_x, e''_2) soit une base orthogonale du plan quadratique $ke'_1 \overset{\perp}{\oplus} ke'_2$ qui se complète en la base orthogonale $\mathbf{e''} := (e_x, e''_2, e'_3, ..., e'_n)$ de E, et l'on disposera alors en vertue du cas 1) de la suite $\mathbf{e} \to \mathbf{e''} \to \mathbf{e'}$.
On a $\forall x \in k, Q(e_x) = Q(e'_1) + x^2 Q(e'_2)$ et $Q(e_1)Q(e_x) - b_Q(e_1, e_x)^2 = -2x b_Q(e_1, e'_1) b_Q(e_1, e'_2)$, de sorte que les conditions souhaitées se traduisent sur x par $x^2 \neq -Q(e'_1)/Q(e'_2)$ et $x \neq 0$. Ainsi, si k a au moins 4 éléments, le résultat suit, et il ne reste qu'à traiter le cas où $k = \mathbb{F}_3$. L'hypothèse de 2) donne $\forall i, j \in [\![1, n]\!]$, $Q(e_i)Q(e'_j) = 1$, c'est à dire $\forall i, j \in [\![1, n]\!]$, $Q(e_i) = Q(e'_j)$ de sorte que $-Q(e'_1)/Q(e'_2) = -1 \notin \mathbb{F}_3^{*[2]} = \{1\}$. Tout $x \in \mathbb{F}_3^*$ convient. Le résultat est démontré.

Proposition 22. *La quantité $\epsilon(e)$ ne dépend pas de la base orthogonale choisie.*

Démonstration. On va démontrer le résultat par récurrence. Si $n = 1$, $\epsilon(e) = 1$, et si $n = 2$, $\epsilon(e) = (a_1, a_2)$ vaut 1 si et seulement si la forme $-Z \bigoplus Q$ est isotrope, ce qui ne dépend pas de la base orthogonale choisie. Supposons à présent $n \geq 3$, d'après le lemme il suffit de montrer que ϵ est invariante pour deux bases orthogonales contingues, et étant invariant par permutation dees e_i par symétrie du symbole de Hilbert, il suffit de montrer que $\epsilon(\mathbf{e}) = \epsilon(\mathbf{e'})$ où $\mathbf{e} = (e_i)_{1 \leq i \leq n}$ et $\mathbf{e'} = (e'_i)_{1 \leq i \leq n}$ sont deux bases orhtogonales telles que $e_1 = e'_1$. On pose $a_i = Q(e_i)$ resp $a'_i = Q(e'_i)$ pour tout $i \in [\![1, n]\!]$ avec donc $a_1 = a'_1$ et $a_1 a_2 ... a_n = a'_1 a'_2 ... a'_n = disc(Q)$. On a $\epsilon(\mathbf{e}) = \prod_{i<j}(a_i, a_j) = (a_1, a_2 ... a_n) \prod_{1<i<j}(a_i, a_j) = (a_1, a_1 disc(Q)) \prod_{1<i<j}(a_i, a_j)$ par propriétés du symbole de Hilbert. De même, on trouve $\epsilon(\mathbf{e'}) = (a_1, a_1 disc(Q)) \prod_{1<i<j}(a_i, a_j)$ et l'égalité suit par hypothèse de récurrence.