Laboratoire de Mathématiques et Modélisation d'Évry

Licence Mathématiques & Applications

Rapport de stage : 2017/2018

Classification des formes quadratiques

Auteur :
El Mehdi Bouchouat

Encadrant :
M. Abdelmejid Bayad

10 janvier 2019

Remerciements

Je tiens à remercier toutes les personnes qui ont contribué à rendre mon stage enrichissant et motivant, et qui m'ont aidé lors de la rédaction de ce rapport.

En premier lieu, je tiens à remercier vivement mon maître de stage, Monsieur BAYAD Abdelmejid, Enseignant-Chercheur au sein du Laboratoire de Mathématique et de Modélisation d'Evry, pour son accueil, sa confiance, ses conseils et les connaissances qu'il a su partager avec moi. Je le remercie aussi pour sa disponibilité et la qualité de son encadrement.

Je souhaite ensuite adresser mes remerciements à tous mes enseignants, qui m'ont aidé tout au long de l'année.

Je voudrais enfin exprimer ma reconnaissance envers mes amis, collègues et ma famille qui m'ont apporté leur soutien moral et intellectuel tout au long de mon stage. Un grand merci à Ayoub ABRAICH pour ses conseils concernant le style de mon rapport de stage.

Table des matières

Introduction

L'étude des formes quadratiques remonte à plusieurs siècles et est une partie très importante de la théorie des nombres et de l'algèbre, avec des applications à d'autres parties des mathématiques, telles que la topologie.

La théorie des formes quadratiques est très vaste et dans ce mémoire je n'en mentionne qu'une très petite partie. Dans la première section, j'introduis les formes quadratiques et leurs formes bilinéaires associées et je présente quelques résultats généraux. La deuxième section est consacrée à la classification des formes quadratiques sur $\mathbb{C}$, $\mathbb{R}$, et sur les corps finis $\mathbb{F}_q$, et dans la troisième section je me concentre sur l'une des applications de la classification des formes quadratiques : La loi de réciprocité quadratique.

Je suppose quelques connaissances antérieures de la part du lecteur, la plus importante étant l'algèbre linéaire de base. Je suppose également une certaine connaissance de l'algèbre abstraite de base, tels que les concepts d'un anneau, d'un module, d'un groupe et de certaines de leurs propriétés, ainsi que quelques résultats importants sur les corps finis.

Dans ce mémoire, je me base principalement sur les livres suivants :

- **Invitation aux formes quadratique**, de *Clément de Seguins Pazzis.*
- **Cours d'algèbre**, de *Daniel Perrin.*
- **Histoires hédonistes de groupes et de géométrie, Tome premier**, de *Philippe Caldero, Jérôme Germoni.*

Chapitre 1

Rappel sur les formes quadratiques

1.1 Définitions et exemples

Définition 1.1.1. On appelle forme bilinéaire de $E \times E$ dans $\mathbb{K}$ toute application $b : E \times E \to \mathbb{K}$ telle que : b est linéraire par rapport à ces deux variables .
Soit $\mathbf{B} = (e_1, \cdot\cdot, e_n)$ une base de E , - $A = (b(e_i, e_j))_{i,j}$ est la matrice associée à la forme bilinéaire b.
- On peut représenter b matriciellement comme : $b(x, y) = {}^t XAY$
- b est symétrique $\Leftrightarrow b(x, y) = b(y, x) \ \ \forall x, y$
- b est antisymétrique $\Leftrightarrow b(x, y) = -b(y, x) \ \ \forall x, y$

Définition 1.1.2. Soit b une forme bilinéaire sur E : L'application

$$q : \begin{cases} E \to \mathbb{K} \\ x \mapsto b(x, x) \end{cases}$$

est la forme quadratique associée à b

Proposition 1.1.1 (Formule de polarisation)**.** *Soit q une forme quadratique sur E de forme bilinéaire b .Alors :*

$$\forall x, y \in E : b(x, y) = \frac{q(x + y) - q(x) - q(y)}{2}$$

- On a aussi :

$$b(x, y) = \frac{q(x) + q(y) - q(x - y)}{2} = \frac{q(x + y) - q(x - y)}{4}$$

Définition 1.1.3 (Espace quadratique)**.** On appelle espace quadratique tout couple (F, q) formé d'un $\mathbb{K}-$espace vectoriel F et d'une forme quadratique q sur F

Définition 1.1.4 (Représentation matricielle de q)**.** On appelle matrice associée à q dans $\mathbf{B}$,notée $A := M_{\mathbf{B}}(q)$ la matrice symétrique associée à sa forme bilinéaire b dans $\mathbf{B}$).
- On a aussi : $q(x) = {}^tXAX$

Définition 1.1.5 (Représentation polynomiale)**.** Soit $A = (a_{i,j})_{i,j}$ la matrice de q :

$$q(x) = \sum_{i=1}^{n} a_{i,i}x_i^2 + 2\sum_{i<j} a_{i,j}x_ix_j$$

Exemple 1.1.1. Soit b une forme bilinéaire telle que :

$$b(A, B) = tr({}^tAB),\ avec\ A, B \in M_n(\mathbb{R})$$

- La forme quadratique q associée à b :

$$q(A) = tr({}^tAA)$$

Exemple 1.1.2. Soit b une forme bilinéaire telle que :

$$b(A, B) = \frac{tr(A)tr(B) - tr(AB)}{2},\ avec\ A, B \in M_n(\mathbb{R})$$

- La forme quadratique q associée à b :

$$q(A) = \frac{tr(A)^2 - tr(A^2)}{2}$$

Cette forme quadratique est importante pour l'étude du cone nilpotent de l'algèbre $M_n(\mathbb{K})$

1.2 Problème de classification

1.2.1 L'équivalence entre formes bilinéaires

Définition 1.2.1 (Morphisme)**.** Soit (E, b) et (F, b') deux espaces bilinéaires .On appelle morphisme de (E, b) dans (F, b') toute application linéaire $u : E \to F$ telle que

$$\forall x, y \in E : b(x, y) = b'(u(x), u(y))$$

Un morphisme bijectif est appelé un isomorphisme , sa réciproque étant automatiquement un morphisme . On dit que b et b' sont équivalentes lorsque (E, b) et (F, b') sont isomorphes. On prouve facilement que l'équivalence des formes bilinéaires est une relation d'équivalence sur la collection des formes bilinéaires symétriques.

1.3 Objets associés à une forme quadratique

1.3.1 Dimension,noyau,rang

Notons $dim(q)$ la dimension de l'espace de départ E de q .

Définition 1.3.1 (Noyau/Radical)**.** On appelle *noyau* ou *radical* de q l'ensemble :

$$Ker(q) := \{x \in E \mid \forall y \in E : b(x, y) = 0\}$$

Remarque 1.3.1. *Ker(q) est un sous espace vectorielle de E.*

Définition 1.3.2 (Rang)**.** Soit A $\in$ S_n représentant q. On a :
$rg(q) = rg(A) = rg(b)$, avec b est la forme bilinéaire associé à q.
En dimension finie, $rg(q) = n - dim(Ker(q))$, avec n=dim(E). Cette valeur commune est un élément de $\{0, ..., n\}$, appelé rang de q.

Proposition 1.3.1. *Deux formes quadratiques équivalentes ont le même rang.*

Définition 1.3.3. on dit que q est **non dégénérée** quand $ker(q) = \{0\}$, ce qui équivaut à rg(q)=dim(E).

1.3.2 Cone isotrope

un vecteur est dit isotrope si q(x)=0, x $\in$ E

Définition 1.3.4. Le cône isotrope est l'ensemble : $Co(q) = \{x \in E, q(x) = 0\}$

Remarque 1.3.2. $Ker(q) \subset Co(q)$*, mais la réciproque n'est pas vrai en général.*

Remarque 1.3.3. *En général, le cône isotrope de q n'est même pas un sous-espace vectoriel de E.*

1.3.3 Déterminants

$$det : \begin{cases} formes \;\; quadratiques \to \mathbb{K}/(\mathbb{K}^*)^2 \\ q \mapsto det\ M_B(q)\ mod(\mathbb{K}^*)^2 \end{cases}$$

Définition 1.3.5. Soit q non dégénérée, on appelle **déterminant** de q tout déterminant d'une matrice de $S_n(\mathbb{K})$ représentant q.

Proposition 1.3.2. *Deux formes quadratiques non dégénérées équivalentes ont le même déterminant.*

1.3.4 Le groupe orthogonal

Définition 1.3.6. Un **automorphisme orthogonal** de (E, q) est un isomorphisme de (E, q) sur (E, q). L'ensemble des automorphismes est noté $O(q)$.
L'ensemble $O(q)$ est un $sous-groupe$ de $\mathbf{GL}(\mathbf{E})$ que l'on appelle le **groupe orthogonal** de q.

Proposition 1.3.3. *Soit q non dégénérée, on a* $\forall u \in O(q)$, *det(u)*$=\pm 1$

Preuve : Soit u $\in$ O(q), donc $\exists$ M $\in$ GL($\mathbb{K}$) telle que ${}^tMAM = A$, avec A est la matrice associée à la forme quadratique q. D'où :
ddet$({}^tMAM) = det(A) \Leftrightarrow det(M)^2 det(A) = det(A)$
$\Leftrightarrow det(M)^2 = 1$
$\Leftrightarrow det(M) = \pm 1$
$\Leftrightarrow det(u) = \pm 1$

Définition 1.3.7 (Groupe spécial orthogonal)**.** On note $SO(q) = \{u \in O(q) : det(u) = 1\}$, appelé groupe spécial orthogonole de (E,q). Ses élements sont appelés les rotations de l'espace quadratique (E,q).

1.3.5 Facteurs de similitudes

Définition 1.3.8. Deux formes quadratiques q et q' sont semblables lorsqu'il existe $\alpha \in \mathbb{K}^*$ tel que q'$\simeq \alpha q$.

Définition 1.3.9. On appelle **facteur de similitude** de q tout scalaire $\lambda \in \mathbb{K}^*$ tel que q$\simeq \lambda q$.

Définition 1.3.10. Soit q non nulle. On appelle **similitude** de l'espace quadratique (E,q) tout isomorphisme $u \in GL(E)$ pour lequel il existe un $\lambda \in \mathbb{K}^*$ tel que :

$$\forall\, x \in E, q(u(x)) = \lambda q(x)$$

.
L'ensemble des similitudes de (E,q) est noté GO(q).

1.4 L'orthogonalité pour une forme bilinéaire symétrique ou alternée

1.4.1 Noyau et rang d'une forme bilinéaire en dimension finie

(E,b) désigne un K-espace bilinéaire symétrique ou alterné. On va prolonger à b (la forme bilinéaire) les notions de noyau et de rang.

Définition 1.4.1 (noyau/radical)**.** Soit $b : E \times E \to \mathbb{K}$ une forme bilinéaire symétrique ou alternée. On appelle **noyau ou radical** de b l'ensemble :

$$Ker(b) = \{x \in E : b(x, y) = 0, \forall y \in E\}$$

.

Proposition 1.4.1 (rang)**.** *Soit E de dimension finie et b une forme bilinéaire représentée par une matrice $B \in M_n(\mathbb{K})$. Alors, dimKer(b)=n-rang(B).*
On appelle rang de b, n'importe laquelle des quantités suivantes : n-dimKer(b), rang(A), et on le note rg(b).

Définition 1.4.2 (forme bilinéaire/quadratique régulière ou non dégénérée)**.** On dit que b est régulière ou non dégénérée si $Kerb = \{0\}$. Sinon elle est dite dégénérée.
Lorsque $\mathbb{K}$ est de caractéristique différente de 2, la forme quadratique q sur E est dite régulière lorsque E est de dimension finie et $Kerq = \{0\}$.

Définition 1.4.3. Soit A un sous-espace vectoriel de E. On dit que A est un sous-espace régulier de (E,b) lorsque b_A est régulière.

Remarque 1.4.1. *En effet, si la forme quadratique q n'est pas régulière dans E, on quotiente par $Ker(q)$, car $E/Ker(q)$ est la partie régulière de E.*

1.4.2 La relation d'orthogonalité entre vecteurs, l'orthogonal d'un sous-espace vectoriel

Définition 1.4.4. Soit x et y deux vecteurs de E. On dit que x est **b-orthogonal** à y si $b(x, y) = 0$, que l'on note x$\perp$ y.

Définition 1.4.5. Soit A et B deux parties de E. On dit que A et B sont b-orthogonal, lorsque $\forall (x, y)$ *in* $A \times B, b(x, y) = 0$.

Définition 1.4.6. Soit A un ensemble de E.
On appelle **b-orthogonal** de A le sous-ensemble :

$$A^{\perp} = \{x \in E : \forall\ a \in A, b(x, a) = 0\}$$

Remarque 1.4.2. *L'orthogonal de A pour b est la plus grande partie de E qui est b-orthogonal à A.*

Proposition 1.4.2. *Soit A et B deux parties de E. On a :*
(a) $A^{\perp}$ est un sous-espace vectoriel de E contenant Ker(q).
(b) $A^{\perp} = (VectA)^{\perp}$.
(c) Si $A \subset B \Rightarrow B^{\perp} \subset A^{\perp}$.
(d) Si A est un sous-espace vectoriel de E, alors $A \cap A^{\perp} = Ker(b_A)$
(e) $A \subset (A^{\perp})^{\perp}$.

Corollaire 1.4.1. *Un sous-espace vectoriel A de E est b-régulier* $\Leftrightarrow$ $A \cap A^{\perp} = \{0\}$.

CAS D'UNE FORME REGULIERE

Théorème 1.4.3 (dimension de l'orthogonal)**.** *Soit A un sous-espace vectoriel et b une forme bilinéaire régulière, alors :*

$$dimA^{\perp} + dimA = dimE$$

Conséquence 1. *Soit A un sous-espace vectoriel de E. On suppose b régulière. Alors, A est b-régulier* $\Leftrightarrow A \oplus A^{\perp} = E$.

1.5 Réduction d'une forme quadratique

1.5.1 Réduction théorique

Définition 1.5.1 (bases orthogonales)**.** Une famille $(e_1, ..., e_n)$ de E est dite **q-orthogonale** si ses vecteurs sont deux à deux q-orthogonaux, c'est-à-dire :

$$\forall (i,j) \in [1,n]^2, i \neq j \Rightarrow b(e_i, e_j) = 0$$

Proposition 1.5.1. *Soit* $B := (e_1, \cdot\cdot, e_n)$ *une base de E. On a les équvalences suivantes :*
(a)- La base B est q-orthogonale
(b)- La matrice de q dans B est diagonale
(c)- Il existe n scalaires $a_1, \cdot\cdot, a_n$ *tels que :* $q = \sum_{k=1}^{n} a_k (e_k^*)^2$

Proposition 1.5.2. *Soit* $B := (e_1, \cdot\cdot, e_n)$ *une famille orthogonale de vecteurs anisotropes de* (E, q) *(cad :* $q(e_i) \neq 0 \forall i$*).Alors B est libre .*

Théorème 1.5.3. *Tout espace quadratique* (E, q) *de dimension finie admet une base q-orthogonale.*

Corollaire 1.5.1. *Soit* (E, q) *une espace quadratique de dimension n, alors :*
(a)- il existe une matrice diagonale représentant q
(b)- il existe des scalaires $a_1, \cdot\cdot, a_n$ *tels que* $q \simeq \langle a_1, \cdot\cdot, a_n \rangle$
(c)- il existe des scalaires $a_1, \cdot\cdot, a_n$ *et une base B dans laquelle q est représentée par le polynome* $\sum_{k=1}^{n} a_k (X_k)^2$
(d)- il existe une base $(f_1, \cdot\cdot, f_n)$ *de* E^* *et une famille* $(a_1, \cdot\cdot, a_n)$ *telles que :* $q = \sum_{k=1}^{n} a_k f_k^2$

Proposition 1.5.4. *Soit $(e_1, \cdot\cdot, e_r)$ une famille orthogonale de E telle que $q(e_i) \neq 0 \forall i$. On peut compléter $(e_1, \cdot\cdot, e_r)$ en une base orthogonale de E*

Preuve : Soit $x \in F = Vect(e_1, ..., e_r)$. Si $x \in F^{\perp}$, alors $q(x) = 0$. Or q n'a pas de vecteurs isotropes sur F, donc $x = 0$. Par suite, $E = F \oplus F^{\perp}$.

1.5.2 Mineurs principaux

Définition 1.5.2. Soit $A \in S_n(\mathbb{K})$.Pour $k \in \|1, n\|$ on appelle mineur principal d'ordre k de A le déterminant :

$$\triangle_k(A) := \begin{vmatrix} a_{1,1} & \cdots & a_{1,k} \\ \vdots & \ddots & \vdots \\ a_{k,1} & \cdots & a_{k,k} \end{vmatrix}$$

Proposition 1.5.5. *Soit $A \in S_n(\mathbb{K})$.Si $\forall k \triangle_k(A) \neq 0$,alors :*

$$A \sim Diag(\triangle_1(A), \frac{\triangle_2(A)}{\triangle_1(A)}, \cdots, \frac{\triangle_n(A)}{\triangle_{n-1}(A)})$$

1.5.3 La réduction de Gauss analytique

Soit $(f_1, \cdot\cdot, f_n)$ base de E^*.On considère une forme quadratique :

$$q := \sum_k a_k f_k^2 + \sum_{1 \leqslant i < j \leqslant n} b_{i,j} f_i f_j$$

que l'on souhaite écrire comme combinaison linéaire des carrés de n formes linéaires indépendantes.

L'algorithme de réduction de Gauss

— Premier cas : la forme quadratique contient un terme au carré x_i^2
Par symétrie de roles,supposons que ce soit x_1^2. On regroupe alors tous les termes contenant la variable x_1 et on les voit comme le début du développement d'un carré du type $(x_1 + \cdots)^2$:

$$\begin{aligned} q(x) &= a_{1,1}(x_1^2 + x_1 f(x_2, \cdots, x_n)) + g(x_2, \cdots, x_n) \\ &= a_{1,1}(x_1 + \frac{1}{2} f(x_2, \cdots, x_n))^2 + g(x_2, \cdots, x_n) - \frac{a_{1,1}}{4} f(x_2, \cdots, x_n)^2 + g(x_2, \cdots, x_n) \\ &= a_{1,1} l_1(x)^2 + q'(x) \end{aligned} \tag{1.1}$$

ou l_1 est une forme linéaire sur E définie par : $l_1(x) := x_1 + \frac{1}{2}f(x_2, \cdots, x_n)$
On continue notre algorithme sur cette nouvelle forme quadratique $q^{'}$ (ie si $q^{'}$ vérifie le premier cas ou bien le second cas)

— Second cas :l a forme quadratique ne contient aucun terme au carré x_i^2 :
On choisit deux variables qui apparaissent sous la forme $x_i x_j$,par symétrie de roles ,on suppose que le produit $x_1 x_2$ apparaisse dans l'expression de q. On a :

$$\begin{aligned} q(x) &= a_{1,2}(x_1x_2 + x_1 f(x_3, \cdots, x_n) + x_2 g(x_3, \cdots, x_n)) + h(x_3, \cdots, x_n) \\ &= a_{1,2}(x_1 + g(x_3, \cdots, x_n))(x_2 + f(x_3, \cdots, x_n)) - a_{1,2}f(x_3, , x_n)g(x_3, , x_n) + h(x_3, , x_n) \\ &= a_{1,2}l_1^{'}(x)l_2^{'}(x) + q^{'}(x) \\ &= \frac{a_{1,2}}{4}(l_1^2(x) - l_2^2(x)) + q^{'}(x) \end{aligned} \tag{1.2}$$

ou $l_1(x) := l_1^{'}(x) + l_2^{'}(x)$ et $l_2(x) := l_1^{'}(x) - l_2^{'}(x)$.
On continue l'algorithme sur la nouvelle forme $q^{'}$.

Chapitre 2

Retour au problème de classification

2.1 Matrices congruentes

Définition 2.1.1. Deux matrices A et B de $M_n(\mathbb{K})$ sont dites congruentes sur $\mathbb{K}$ quand il existe une matrice P inversible dans $M_n(\mathbb{K})$ telle que $B = {}^tPAP$.
La relation de congruence est une relation d'équivalence. Soit q une forme quadratique sur un espace vectoriel de dimension n, et A sa matrice associée dans une base ε de E. Une matrice B symétrique de taille n est congruente à A si et seulement s'il existe une base $\mathfrak{F}$ de E dans laquelle B est la matrice de q.

2.2 La classification sur $\mathbb{R}, \mathbb{C}$:

2.2.1 La classification sur $\mathbb{C}$:

Sur $\mathbb{C}$ ou plus généralement $\mathbb{K}$ avec $\mathbb{K}$ est algébriquement clos (i.e toute forme admet au moins une racine dans $\mathbb{K}$, il suffit du rang pour classifier les formes quadratiques sur $\mathbb{C}$.

Proposition 2.2.1. *Soit q une forme quadratique complexe de dimension n et de rang r. Alors q est représentée par la matrice :*

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

C'est-à-dire : q est isométrique à $< \underbrace{1, ..., 1}_{r}, 0, ..., 0 > \Leftrightarrow q(x) = \sum_{i=0}^{r} x_i^2$

$\Leftrightarrow q \simeq r. < 1 > \perp (n-r). < 0 >$

Théorème 2.2.2. *Deux formes quadratiques complexes de même dimension finie sont équivalentes si et seulement si elles ont le même rang.*

2.2.2 La classification sur $\mathbb{R}$:

Proposition 2.2.3. *Soit q une forme quadratique réelle de dimension n. Il existe deux entiers s et t tels que :*

$$q \simeq s.<1>\perp t.<-1>\perp (n-r-s).<0> \;\Leftrightarrow\; q = \sum_{i=0}^{s} x_i^2 - \sum_{i=s+1}^{s+t} x_i^2$$

Alors q est représentée par la matrice suivante :

$$\begin{pmatrix} I_r & 0 & 0 \\ 0 & -I_s & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

Définition 2.2.1 (Signature d'une forme quadratique réelle)**.** Soit (E,q) un espace quadratique réel de dimension finie.
On définit s comme la dimension maximale d'un sous-espace vectoriel F de E tel que $q_F > 0$.
On définit t comme la dimension maximale d'un sous-espace vectoriel G de E tel que $q_G < 0$.
Alors, le rang de q (que l'on note r) est : $r = s+t$, et le couple (s,t) est appelé **la signature**.

Théorème 2.2.4 (Théorème d'inertie de Sylvester)**.** *. Soit q une forme quadratique réelle de dimension n. La signature est un invariant de q.*

Théorème 2.2.5. *Deux formes quadratiques réelles sont équivalentes si et seulement si elles ont la même signature.*

2.3 La classification sur un corps fini :

Soit $\mathbb{K} = \mathbb{F}_{\text{ıı}}$ un corps fini de caractéristique différente de 2. Il existe un morphisme de groupe φ tel que :

$$\varphi : \begin{cases} (\mathbb{F}_q^*, \times) \to (\mathbb{F}_q^*, \times) \\ x \mapsto x^2 \end{cases}$$

On a :

$$Im(\varphi) = (\mathbb{F}_q^*)^2 \quad et \quad Ker(\varphi) = \left\{x \in \mathbb{F}_q^* : x^2 = 1\right\}$$
$$\Rightarrow Ker(\varphi) = \{\pm 1\}$$

Alors selon le théorème d'isomorphisme :

$$\mathbb{F}_q^*/Ker(\varphi) \simeq (\mathbb{F}_q^*)^2$$

Et comme on cherche les classes d'èquivalence de $\mathbb{F}_q^*/(\mathbb{F}_q^*)^2$ qui est isomorphe à $Ker(\varphi)$, on a donc que deux classes d'équivalence pour les formes quadratiques régulières qui sont : $\{\pm 1\}$.

Théorème 2.3.1. *Soit $\mathbb{F}_q$ avec $carac(\mathbb{F}_q) \neq 2$. Soit E un $\mathbb{F}_q$-espace vectoriel de dimension n, et $\alpha \in \mathbb{F}_q^*/(\mathbb{F}_q^*)^2$. Il y a deux classes d'équivalence de formes quadratiques non dégénérées sur E. Leur matrice dans une base adaptée est soit $Q_1 = I_n$ ou $Q_2 == \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & \vdots \\ \vdots & \vdots & \ddots & 0 \\ 0 & \cdots & 0 & \alpha \end{pmatrix}$*

Preuve : Pour démontrer le théorème(2.2.1) d'avant, on prouve d'abord les deux lemmes suivants :

Lemme 2.3.2. *Il y a $\frac{q+1}{2}$ carrés dans $\mathbb{F}_q$:*
On a

$$\mathbb{F}_q^*/Ker(\varphi) \simeq (\mathbb{F}_q^*)^2$$

Or

$$Ker(\varphi) = \pm 1, \quad donc\ Card(Ker(\varphi)) = 2$$

et comme on a : Card($\mathbb{F}_q^*$)=q-1, cela implique :

$$Card(des\ carres\ de\ \mathbb{F}_q^*) = \frac{q-1}{2} \Rightarrow \quad Card(des\ carres\ de\ \mathbb{F}_q) = \frac{q+1}{2}$$

Lemme 2.3.3. *Si $(a,b) \in \mathbb{F}_q^*$, l'équation $ax^2 + by^2 = 1$ admet des solutions dans $\mathbb{F}_q$ avec ($carac(\mathbb{F}_q) \neq 2$) : On vient de voir qu'il y a $\frac{q+1}{2}$ dans $\mathbb{F}_q$. donc la quantité $\frac{1-by^2}{a}$ prend donc $\frac{q+1}{2}$ valeurs quand y parcourt $\mathbb{F}_q$. et comme :*

$$\frac{q+1}{2} + \frac{q+1}{2} > q$$

l'un de ses valeurs est forcément un carré. (Principe des tiroirs)
L'équation admet donc des solutions dans $\mathbb{F}_q$.

Retour à la démonstration du théorème. On procède par récurrence.
Pour $n = 1$, soit $e \in \mathbb{F}_q^*$, $Q(e) \neq 0$, car Q est non dégénérée. On distingue deux cas :

— Si $Q(e) \in \mathbb{F}_q^*$, il existe $\lambda \in \mathbb{F}_q^{*2}$ tel que $Q(e) = \lambda^2$, alors $e_1 = \frac{e}{\lambda}$ convient :

$$Q(e_1) = 1$$

— Sinon $Q(e) \notin \mathbb{F}_q^{*2}$ comme $\mathbb{F}_q^{*2}$ est d'indice 2 dans $\mathbb{F}_q^*$, il existe $\lambda \in \mathbb{F}_q^*$ tel que $Q(e) = \alpha\lambda^2$, alors $e_1 = \frac{e}{\lambda}$ convient :

$$Q(e_1) = \alpha$$

Supposons que c'est vrai au rang n. Montrons le au rang $n+1$.
Soit $(e_1, ..., en+1)$ une base Q-orthogonale de E. Notons $H = Vect(e_1, e_2)$. Il existe $a, b \in \mathbb{F}_q^*$ tels que : $Q_{|H} =< a, b >$.
Or d'après le lemme, l'équation $ax^2 + by^2 = 1$ admet des solutions dans $\mathbb{F}_q$. Il existe donc $\epsilon_1 \in H$ tel que $Q(\epsilon_1) = 1$. On applique alors l'hypothèse de récurrence sur $H^\perp$ et on obtient la matrice voulue. Ce qui achève la récurrence.

Remarque 2.3.1. *Sur $\mathbb{F}_q$, deux formes quadratiques sont équivalentes si et seulement si elles ont le même rang et le même discriminant.*

Chapitre 3

Applications : La loi de réciprocité quadratique

Dans ce chapitre, on verra une des applications de la classification des formes quadratiques. Pour commencer je vais introduire quelques résultats qui nous seront utiles dans l'étude de **la loi de réciprocité**.

3.1 Définitions : Action du groupe, Orbite, Stabilisateur

Définition 3.1.1 (Action de groupe)**.** Soit G un groupe et X un ensemble. On appelle *action à gauche* ou *opération à gauche*, plus simplement, action ou opération de G sur X une application :

$$\varphi : \begin{cases} G \times X \to X \\ (g, x) \mapsto g \ . \ x \end{cases}$$

telle que :
- $\forall (g, g') \in G, \forall x \in X, g \ .(g' \ x) = (g \ . \ g').x$
- $\forall x \in X, (e \ . \ x) = x$ (où e est le neutre de G).

Définition 3.1.2 (Orbite)**.** Soit G un groupe qui agit sur un ensemble E :
L'orbite d'un élément x de E est l'ensemble des valeurs $g.x$ où g est un élément de G :

$$Orb(x) = \{g.x; g \in G\}$$

Définition 3.1.3 (Stabilisateur)**.** Le stabilisateur de x est l'ensemble des éléments de G qui laissent x fixe. Autrement dit, c'est l'ensemble des éléments $g \in G$ tel que : $g \ . \ x = x$

3.2 Loi de réciprocité quadratique

Théorème 3.2.1. *Soit p et q deux nombres premiers impairs distincts. Alors :*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

Lemme 3.2.2. *Soit $a \in \mathbb{F}_q^*$. On définit :*

$$a^{\frac{p-1}{2}} = \left(\frac{a}{p}\right) = \begin{cases} \textit{1, si a est un carré de } F_p^* \\ \textit{-1, sinon} \end{cases}$$

Avant de démontrer le théorème(3.2.1), on prouve d'abord le corollaire suivant :

Corollaire 3.2.1. *Soit p premier impair et a un élément de $\mathbb{F}_p^*$. On a :*

$$Card(\{x \in \mathbb{F}_p^*, ax^2 = 1\}) = 1 + \left(\frac{a}{p}\right)$$

Preuve : Soit $x \in \mathbb{F}_p^*$, tel que $ax^2 = 1$, en multipliant par a on a : $(ax)^2 = a$,
On pose $y = ax$, donc :

$$Card(\{x \in \mathbb{F}_p^*, ax^2 = 1\}) = Card(\{y \in \mathbb{F}_p^*, y^2 = a\})$$

Or on a $p \neq 2$, donc :

$$Card(\{y \in \mathbb{F}_p^*, y^2 = a\}) = \begin{cases} 2, \text{ si a est un carré de } \mathrm{F}_p^* \\ 0, \text{ sinon} \end{cases}$$

Or d'après le lemme précédent,

$$\left(\frac{a}{p}\right) + 1 = \begin{cases} 2, \text{ si a est un carré de } \mathrm{F}_p^* \\ 0, \text{ sinon} \end{cases}$$

D'où :

$$Card(\{x \in \mathbb{F}_p^*, ax^2 = 1\}) = 1 + \left(\frac{a}{p}\right)$$

Retour à la démonstration du théorème(3.2.1) :
Démonstration :
L'idée est de calculer de deux manière différentes le cardinal modulo p de la sphère définie sur $\mathbb{F}_q$:

$$X = \left\{(x_1, ..., x_p) \in \mathbb{F}_q^p, \ \sum_{i=1}^{p} x_i^2 = 1\right\}$$

Premièrement, on fait agir le groupe $\mathbb{Z}/p\mathbb{Z}$ par permutation cyclique sur $\mathbb{F}_q^p$:

$$\forall k \ \in \ \mathbb{Z}/p\mathbb{Z}, \forall (x_1, ..., x_p) \in \ \mathbb{F}_q^p, k.(x_1, ..., x_n) = (x_{1+k}, ..., x_{n+k}),$$

où les indices sont vus modulo p : $x_{l+p} = x_l$ pour tout l.
Les orbites de $\mathbb{Z}/p\mathbb{Z}$ dans X sont de deux types : d'un côté, les singletons $(x, ..., x)$, où $x \in \mathbb{F}_q$, ont un stabilisateur trivial, nécessairement égal à $\mathbb{Z}/p\mathbb{Z}$ entier. Le nombre d'orbites à stabilisateur non trivial est le nombre de solutions de x à l'équation : $px^2 = 1$ dans $\mathbb{F}_q$, donné par le corollaire précédent : $\left(\frac{p}{q}\right) + 1$. Le cardinal des autres orbites est divisible par p, d'où :

$$Card(X) = \left(\frac{p}{q}\right) + 1 \ \ mod \ \ p$$

Deuxièmement, on remplace la forme quadratique $\sum x_i^2$ par une forme qui lui est congruente, pour laquelle le cardinal de X est facile à calculer : On pose $d = \frac{p-1}{2}$
Les matrice $p \times p$ à coefficients dans $\mathbb{F}_q$:

$$I_p = \begin{pmatrix} 1 & & \\ & & \\ & & 1 \end{pmatrix} \quad et \quad A = \begin{pmatrix} 0 & 1 & & & & & \\ 1 & 0 & & & & & \\ & & 0 & 1 & & & \\ & & 1 & 0 & & & \\ & & & & 0 & 1 & \\ & & & & 1 & 0 & \\ & & & & & & a \end{pmatrix}$$

avec $a = (-1)^{\frac{p-1}{2}} = (-1)^d$, sont symétriques et ont le même rang p et même déterminant 1, donc selon la **Remarque 2.3.1** les matrices sont congruentes.
Un changement linéaire de variables identifie X à l'ensemble :

$$X' = \left\{(y_1, ..., y_d, z_1, ..., z_d, t) \in \mathbb{F}_q^p, \ \ 2(y_1z_1 + ... + y_dz_d) + at^2 = 1\right\}$$

On distingue deux types de points de X' :

- les points tels que $(y_1, ..., y_d) = (0, ..., 0)$: on a donc chaque valeur de t telle que $at^2 = 1$ détermine q^d tels points, ce qui par **le corollaire 3.2.1** donne : $q^d(1 + a^{\frac{q-1}{2}})$ (**1**) points en tout.
- les points tels que $(y_1, ..., y_d) \neq (0, ..., 0)$: on a donc $q^d - 1$ possibilités pour y, q^{d-1} pour z et q possibilités pour t, donc $q^d(q^d - 1)$ (**2**).

De (**1**) et (**2**), on a au total : $q^d(1 + a^{\frac{q-1}{2}}) + q^d(q^d - 1)$
Donc :

$$q^d(1 + a^{\frac{q-1}{2}}) + q^d(q^d - 1) = \left(\frac{p}{q}\right) + 1 \ \ mod \ \ p$$

$$\Leftrightarrow q^d(a^{\frac{q-1}{2}} + q^d) = \left(\frac{p}{q}\right) + 1 \ \ mod \ \ p$$

Or $a = (-1)^{\frac{p-1}{2}}$ et $\left(\frac{a}{q}\right) = a^{\frac{q-1}{2}} = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$:

$$\Leftrightarrow q^d(q^d + (-1)^{\frac{p-1}{2}\frac{q-1}{2}}) = 1 + \left(\frac{p}{q}\right) \quad mod \quad p$$

$$\Leftrightarrow \left(\frac{q}{p}\right)(\left(\frac{q}{p}\right) + (-1)^{\frac{p-1}{2}\frac{q-1}{2}}) = 1 + \left(\frac{p}{q}\right) \quad mod \quad p$$

$$\Leftrightarrow \left(\frac{q}{p}\right)^2 + (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{q}{p}\right) = 1 + \left(\frac{p}{q}\right) \quad mod \quad p$$

$$\Leftrightarrow 1 + (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{q}{p}\right) = 1 + \left(\frac{p}{q}\right) \quad mod \quad p$$

$$\Leftrightarrow (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right) \quad mod \quad p$$

$$\Leftrightarrow \left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

Conclusion

Ce rapport est le résultat des recherches réalisées au cours de la période de mon stage au sein du **laboratoire de mathématiques et modélisation d'Evry (LaMME)**, qui m'a présenté une occasion profitable pour appliquer mes connaissances dans la recherche.

Tout d'abord, j'ai fais un rappel sur les formes bilinéaires et les formes quadratiques associées, ensuite j'ai classifié ces formes sur différentes espaces : $\mathbb{C}$, $\mathbb{R}$ et sur les corps finis $\mathbb{F}_q$. Et enfin, j'ai pu découvrir l'utilité des formes quadratiques dans un exemple : La loi de réciprocité quadratique, qui est l'un des théorèmes le plus important dans la théorie des nombres.

Ce stage a été très enrichissant pour moi, car ça m'a permis de découvrir le monde de la recherche, et surtout approfondir mes connaissances en algèbre notamment en théorie des nombres, une théorie qui m'intéresse énormément.

Enfin, je tiens à exprimer ma satisfaction d'avoir pu effectuer ce stage au sein du laboratoire de recherche d'Evry.

Bibliographie

-https ://agreg-maths.fr/uploads/versions/989/Classification%20des%20formes%20quadratiques.pdf
-https ://perso.univ-rennes1.fr/michel.coste/Bil.pdf
-http ://agreg-maths.univ-rennes1.fr/documentation/docs/Quadrarev.pdf
-**Invitation aux formes quadratique**, de *Clément de Seguins Pazzis.*
-**Cours d'algèbre**, de *Daniel Perrin.*
-**Histoires hédonistes de groupes et de géométrie, Tome premier**, de -*Philippe Caldero, Jérôme Germoni.*