Master 2 : Mathématiques Générales
Université Claude Bernard
Septembre 2012

Mémoire :

Théorie de Witt et Algèbres de Clifford
Application à l'étude des formes quadratiques rationnelles

Doyen Nicolas

Sous la direction de : Philippe Caldero

Université Claude Bernard -LYON 1
Faculté des Sciences et Technologie
Département de Mathématiques .

Remerciements

Je tiens à remercier tout particulièrement mon tuteur de mémoire, M. Philippe Caldero qui m'a proposé de travailler sur ce thème original des formes quadratiques rationnelles abordées selon les théories de Witt et des algèbres de Clifford. La disponibilité et l'aide qu'il m'a apportées tout au long de cette année ont été précieuses et très appréciables, tout comme la liberté d'action et de recherche dont j'ai pu bénéficier au cours de notre collaboration.

Enfin, je tiens à remercier Chloé Bourquard pour ses conseils, notamment en ce qui concerne le LaTeX et son soutien tout au long de la rédaction de ce mémoire.

Table des matières

Introduction

Ce mémoire répond à l'invitation au voyage à travers le monde des formes quadratiques lancée par Clément de Seguins Pazzis, auteur de l'ouvrage : "*Invitation aux formes quadratiques*". Ce livre constitue la base de tout mon travail et a servi d'ouvrage référent grâce aux nombreux exercices proposés par l'auteur. A travers une sélection et un choix personnel d'exercices, j'ai tenté d'approfondir les notions du cours et surtout de m'intéresser à des prolongements et développements de celui-ci, non traîtés par l'auteur au sein des différents chapitres, mais initiés sous la forme d'exercices et problèmes de synthèse. L'étude d'une forme quadratique dépendant fondamentalement du corps de base sur lequel elle est définie, notre voyage sera l'occasion de nous promener à travers les corps $\mathbb{C}$ et $\mathbb{R}$ ainsi que les corps finis et enfin les corps p-adiques $\mathbb{Q}_p$ qui grâce aux principes de Hasse nous offriront un passage vers le corps $\mathbb{Q}$. Ce mémoire nous verra alors aborder le problème de la décomposition des formes quadratiques, l'étude de leur caractère isotrope ou anisotrope, le problème de la représentation des scalaires ainsi que l'importante question de la classification des formes quadratiques avec en ligne de mire la classification sur le corps des rationnels. Celle-ci sera alors envisagée de deux manières différentes, dans un premier temps via les outils fournis par la théorie de Witt puis dans un second temps grâce à l'angle nouveau apporté par la structure d'algèbre de Clifford. La rédaction des différents exercices qui constituent les fondations de ce mémoire ont nécessité bien souvent la maîtrise de diverses notions et théorèmes développés au sein des nombreux chapitres du livre, pour cette raison, je rappelerai de manière synthétique les résultats utiles et fondamentaux indispensables à leurs compréhensions. Néanmoins, l'originalité de ce mémoire consistant en la rédaction d'exercices originaux prolongeant le cours, certaines démonstrations et résultats seront admis puisque, présentés de manière claire et précise dans le livre de Clément de Seguins Pazzis cité précédemment.

Dans une première partie, nous étudierons les formes quadratiques grâce la théorie de Witt. Nous commencerons par aborder l'opération d'addition orthogonale de deux formes quadratiques qui, à partir de deux espaces quadratiques (E, q) et (E', q') nous permettra d'en construire un nouveau noté $(E \times E', q \perp q')$. Cette somme orthogonale nous sera alors utile pour ramener le problème de classification à celui de la classification des formes quadratiques régulières. Ensuite, la théorie de Witt nous fournira les outils nécessaires pour décomposer une forme quadratique sous la forme d'une addition orthogonale d'une forme quadratique hyperbolique, bien comprise, et d'une forme quadratique anisotrope, plus difficile à classifier. Cette décomposition de Witt sera alors d'un grand intérêt pour la suite. Nous en tirerons en particulier la notion de Witt-équivalence : deux formes quadratiques q et q' sont Witt-équivalentes lorsqu'elles sont en quelque sorte congruentes modulo leur partie hyperbolique. Nous ramènerons le problème de la classification des formes quadratiques au problème de la classification de leur partie anisotrope par le lien très simple qui existe entre l'équivalence et la Witt équivalence : deux formes quadratiques q et q' sont équivalentes si Witt-équivalentes et de même dimension. Nous revisiterons alors brièvement sous l'angle de la théorie de Witt les classifications des formes quadratiques sur $\mathbb{R}, \mathbb{C}$ et les corps finis. Ces résultats nous serons très utiles par la suite pour bien

assimiler la classification sur $\mathbb{Q}$ qui sera explicitée via :

- le test de Witt-équivalence rationnelle qui nous permettra de décider si deux formes quadratiques rationnelles sont Witt-équivalentes.
- le test d'équivalence rationnelle qui nous permettra de décider si deux formes quadratiques rationnnelles sont équivalentes.

Dans cette partie nous évoquerons aussi la représentation des scalaires par certaines formes quadratiques. Le principe du gonflement hyperbolique, aussi utilisé dans le cadre de la décomposition de Witt d'une forme quadratique et qui permet de plonger tout sous-espace totalement isotrope dans un sous-espace hyperbolique de dimension double, sera alors utilisé comme un outil pour obtenir des résultats liant isotropie et représentation des scalaires. Nous consacrerons un chapitre d'application à ce problème de la représentation, dans lequel nous appliquerons les tests d'équivalence et de Witt-équivalence sur $\mathbb{Q}$. Nous obtiendrons notamment quelques résultats intéressants en rapport avec l'écriture des entiers comme somme de carrés de rationnels.

Le principe de simplification de Witt résumé ainsi pour trois formes quadratiques q, ϕ et ψ par : $q \perp \phi \simeq q \perp \psi \Longrightarrow \phi \perp \psi$, nous sera ensuite indispensable pour définir à l'aide de la loi d'addition orthogonale, une structure de groupe sur l'ensemble des classes de Witt-équivalence de formes quadratiques régulières. Ce groupe appelé le groupe de Witt sera noté $W(\mathbb{K})$ où $\mathbb{K}$ désigne le corps de base sur lequel les formes quadratiques sont définies. De même, nous définirons une structure de monoïde abélien sur l'ensemble des classes d'isomorphies des formes quadratiques régulières, monoïde abélien que nous enrichirons d'une structure de groupe via la construction de Grothendieck. Ce groupe sera appelé le groupe de Witt-Grothendieck et noté $\widehat{W}(\mathbb{K})$ où $\mathbb{K}$ joue le même rôle que pour le groupe $W(\mathbb{K})$. La théorie de Witt consiste alors à analyser un corps à travers ses formes quadratiques, nous étudierons ainsi les groupes de Witt et Witt-Grothendieck des corps finis, des corps $\mathbb{R}$ et $\mathbb{C}$ et exploiterons ces résultats pour étudier le groupe de Witt $W(\mathbb{Q})$. Cette dernière étude nous permettra d'énoncer et de donner une justification des tests d'équivalence et de Witt-équivalence sur $\mathbb{Q}$. Cette partie nous donnera aussi l'occasion de caractériser les corps quadratiquement clos et pythagoriciens via l'étude de leur groupe de Witt et de Witt-Grothendieck. Enfin, la brève description des groupes de Witt et Witt-Grothendieck par générateurs et relations, nous sera utile pour caractériser la relation de congruence restreinte aux matrices diagonales inversibles.

Pour clore cette première partie, nous verrons le lien qui existe entre les formes quadratiques rationnelles et les formes quadratiques p-adiques. Le passage entre les corps p-adiques $\mathbb{Q}_p$ et le corps $\mathbb{Q}$ sera assuré via :

- le principe de Hasse faible qui relie la Witt équivalence sur $\mathbb{Q}$ de deux formes quadratiques rationnelles q et q' à la Witt-équivalence de ces mêmes formes quadratiques étendues à $\mathbb{R}$ et aux corps p-adiques $\mathbb{Q}_p$.
- le principe de Hasse fort qui relie l'isotropie de la forme quadratique rationnelle q à l'isotropie de cette même forme quadratique étendue à $\mathbb{R}$ et aux différents corps p-adiques $\mathbb{Q}_p$.

Nous étudierons également les groupes de Witt et Witt-Grotendieck associés aux différents corps $\mathbb{Q}_p$ et l'étude des formes quadratiques sur ces corps sera l'occasion d'obtenir de nombreux résultats essentiels concernant l'isotropie des formes quadratiques rationnelles.

Dans la seconde et dernière partie de ce mémoire, nous étudierons les formes

quadratiques du point de vue de leurs algèbres de Clifford associées. Pour (E, q) un espace quadratique, l'algèbre de Clifford associée notée $C(q)$ est un espace dans lequel se plonge E et qui nous offrira la possibilité d'étudier les formes quadratiques sous un autre regard : celui du monde des algèbres (non commutatives) graduées. L'algèbre de Clifford $C(q)$ peut ainsi être définie grossièrement comme l'algèbre la plus "*naturelle*" dans laquelle est satisfaite la condition :

$$\forall x \in E, q(x) = x^2$$

où l'on note encore x les éléments de E vus comme des éléments de $C(q)$ via l'injection $i : E \longrightarrow C(q)$. Après s'être brièvement interessé à la construction de ces algèbres graduées $C(q)$, nous les étudierons en petite dimension notamment dans le cadre de la dimension 1 où la structure d'algèbre de Clifford d'une forme quadratique q détermine q à équivalence près et dans le cadre de la dimension 2 avec les algèbres de quaternions. Ensuite, nous aborderons l'étude en dimension supérieure à l'aide du principe de décomposition d'une algèbre de Clifford, du lemme de la partie paire et du lemme de dévissage et nous évoquerons d'importants théorèmes de structures qui nous serons indispensables pour atteindre l'objectif de cette partie :

classifier les formes quadratiques rationnelles par l'algèbre de Clifford $\mathbb{Z}/2$-graduée associée.

Cette classification sera d'abord abordée par l'étude préliminaire de la classification des formes quadratiques p-adiques par l'algèbre de Clifford associée, mettant encore une fois en avant la connexion fondamentale qui existe entre les formes quadratiques p-adiques et rationnelles.

Première partie

Théorie de Witt : application à l'étude des formes quadratiques rationnelles

Chapitre 1

Explication du problème de la classification

Dans toute la suite de ce mémoire $\mathbb{K}$ désignera un corps de caractéristique différente de 2.

Ce chapitre introductif a pour but de faire quelques rappels élémentaires concernant les formes quadratiques et d'expliquer le problème de la classification de celles-ci. L'objectif majeur étant ici de donner un sens mathématiques précis à cette notion de *classification*. Pour ce faire, nous allons donner un certain nombre de définitions et revenir notamment sur la représentation matricielle des formes quadratiques. Ceci nous amènera en particulier à étudier la relation de congruence matricielle qui joue un rôle fondamental dans l'optique de cette classification.

1.1 Premières définitions et congruence matricielle

Définition 1.1.1. *On appelle* ***espace bilinéaire*** *tout couple (E, b) où E est un $\mathbb{K}$-espace vectoriel et b une forme bilinéaire sur E. De même, on appelle* ***espace quadratique*** *tout couple (E, q) où E est un $\mathbb{K}$-espace vectoriel et q une forme quadratique sur E.*

Dans toute la suite de ce mémoire, on se concentrera sur le cas où E est de dimension finie. On rappelle ainsi que :

1. une forme quadratique est associée à une unique forme bilinéaire symétrique que l'on appelle sa forme polaire.
2. une forme quadratique est une fonction polynomiale homogène du second degré de E dans $\mathbb{K}$. Dans toute base, on peut la représenter par un polynôme homogène du second degré.
3. une forme quadratique peut être représentée matriciellement dans n'importe quelle base par une application de la forme $X \mapsto {}^tXAX$ où A est une matrice symétrique sur $\mathbb{K}$.

Dans la suite on note (E, q) un espace quadratique de dimension finie et on suppose E muni d'une base $\mathbf{B} = (e_1, \cdots, e_n)$.

Définition 1.1.2. *On appelle matrice associée à q dans $\boldsymbol{B}$, la matrice* symétrique *associée à la forme polaire b dans $\boldsymbol{B}$, $M_{\boldsymbol{B}}(q) = (b(e_i, e_j))_{1 \leq i,j \leq n}$. On dit encore que cette matrice représente q dans $\boldsymbol{B}$.*

On sait alors que pour $\mathbf{B}_1$ et $\mathbf{B}_2$ deux bases de E, les matrices représentant q dans $\mathbf{B}_1$ et $\mathbf{B}_2$ sont liées pas la relation suivante :

$$M_{\mathbf{B}_2}(q) = {}^tPM_{\mathbf{B}_1}(q)P \text{ où } P \text{ est la matrice de passage de } \mathbf{B}_1 \text{ à } \mathbf{B}_2.$$

L'égalité ci-dessus nous amène à parler de congruence matricielle :

Définition 1.1.3. *Soit $n \in \mathbb{N}^*$ et A, B deux matrices de $\mathcal{M}_n(\mathbb{K})$. On dit que A est **congruente** à B et l'on écrit $A \approx B$ lorsqu'il existe une matrice inversible $P \in GL_n(\mathbb{K})$ telle que $A = PB\ {}^tP$.*

L'opération suivante :

$$(P, M) \longmapsto PM\ {}^tP$$

est alors une action de groupe et deux matrices de $\mathcal{M}_n(\mathbb{K})$ sont congruentes si et seulement si elles sont conjuguées sous cette action. La congruence matricielle nous permet ainsi de définir une action à gauche du groupe $GL_n(\mathbb{K})$ sur $\mathcal{M}_n(\mathbb{K})$ mais également une action à gauche du groupe $GL_n(\mathbb{K})$ sur $\mathcal{S}_n(\mathbb{K})$. Cette action restreinte au sous-ensemble $\mathcal{S}_n(\mathbb{K})$ est alors d'un intérêt supérieur pour tout voyageur explorant le monde des formes quadratiques ; les matrices les représentant étant des matrices symétriques. Cette action de congruence s'avère particulièrement importante : elle permet de partitionner l'ensemble des matriques symétriques en sous-ensembles disjoints (les orbites de l'action), dans lesquels deux matrices symétriques sont liées par une relation précise : celle de congruence matricielle. Ainsi, par cette partition nous pouvons "*classifier*" les matrices de $\mathcal{S}_n(\mathbb{K})$, deux matrices étant dans une même orbite et en quelque sorte identifiées si elles sont congruentes.

Voyons désormais en quoi la relation de congruence matricielle intervient dans la classification des formes quadratiques. L'étude de la représentation matricielle d'une forme quadratique q a mis en évidence que deux matrices représentant q dans deux bases différentes sont nécessairement congruentes. De ce résultat nous déduisons que l'ensemble des matrices représentant une forme quadratique q constitue une classe de congruence dans $S_n(\mathbb{K})$. A une forme quadratique q est donc associée une unique classe de congruence de matrices symétriques sur $\mathbb{K}$: l'ensemble des matrices représentant q. A la section suivante, nous verrons que classifier les formes quadratiques sur un corps $\mathbb{K}$ donné revient justement à identifier certaines formes quadratiques (celles qui sont équivalentes) et nous opérerons à cette identification lorsque les formes quadratiques ont même classe de congruence de matrices symétriques associées.

1.2 Le problème de la classification

Dans cette partie, E et F désignent deux $\mathbb{K}$-espaces vectoriels de dimension finie.

1.2.1 L'équivalence entre formes bilinéaires et l'équivalence entre formes quadratiques

Définition 1.2.1. *Soit (E, b) et (F, b') deux espaces bilinéaires. On dit que les formes b et b' sont équivalentes que l'on note $b \simeq b'$, s'il existe un isomorphisme d'espaces vectoriels $u : E \longrightarrow F$ tel que :*

$$\forall (x, y) \in E^2,\ b(x, y) = b'(u(x), u(y)).$$

On parle alors d'espaces bilinéaires isomorphes. De même, soit (E, q) et (F, q') deux espaces quadratiques, on dit que les formes quadratiques q et q' sont équivalentes que l'on note $q \simeq q'$, s'il existe un isomorphisme d'espaces vectoriels $u : E \longrightarrow F$ tel que :

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

On parle alors d'espaces quadratiques isomorphes.

On montre alors facilement que deux formes bilinéaires sont équivalentes si et seulement si elles ont la même classe de congruence de matrices symétriques associées. De même, deux formes quadratiques sont équivalentes si et seulement si les formes polaires associées le sont. Ces résultats permettent d'obtenir le résultat fondamental suivant :

deux formes quadratiques q et q' sont équivalentes si et seulement si elles ont la même classe de congruence de matrices symétriques associées.

Ainsi, classifier les formes quadratiques en dimension finie consiste à identifier les formes quadratiques qui sont équivalentes et cette classification passe par la détermination d'un représentant particulier dans la *"classe d'équivalence"* de chacune d'elles. Le problème se résume alors à la détermination d'un représentant particulier dans chaque classe de congruence de matrices symétriques, d'où l'importance de l'action de congruence matricielle. Pour conclure ce chapitre, nous allons voir comment la réduction de Gauss permet de ramener l'étude de la congruence des matrices symétriques à celles des matrices diagonales. Par le principe de diagonalisation, nous pourrons encore simplifier le problème de la classification des formes quadratiques en le ramenant à celui de la détermination d'un représentant diagonal dans chaque classe de congruence de matrices symétriques.

1.2.2 Réduction de Gauss

Définition 1.2.2. *On appelle opération symétrique élémentaire sur une matrice carrée, le procédé consistant à pratiquer une opération élémentaire sur les lignes (multiplication à gauche par une matrice inversible) suivie de l'opération symétrique correspondante sur les colonnes (multiplication à droite par la transposée de la matrice inversible précédente).*

Naturellement, agir par opérations symétriques élémentaires sur une matrice permet d'obtenir une matrice congruente à la matrice d'origine. Le théorème suivant repose justement sur l'action d'opérations symétriques élémentaires :

Théorème 1.2.1. *Soit $n \in \mathbb{N}^*$. Toute matrice de $\mathcal{M}_n(\mathbb{K})$ est congruente à une matrice triangulaire par blocs de la forme :*

$$\begin{pmatrix} A_1 & * & \cdots & * \\ 0 & A_2 & & \vdots \\ \vdots & & \ddots & * \\ 0 & \cdots & 0 & A_N \end{pmatrix}$$

où $\forall i \in [\![1, N]\!]$, $A_i \in \mathbb{K}$ *ou* $A_i = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$

Démonstration. cf.[1] I.4.1.1 page 9 □

Corollaire 1.2.1. *Toute matrice symétrique de* $\mathcal{M}_n(\mathbb{K})$ *est congruente a une matrice diagonale.*

Démonstration. Soit $A \in \mathcal{S}_n(\mathbb{K})$. Par le théorème 1.2.1, A est congruente à une matrice $B = \begin{pmatrix} A_1 & * & \cdots & * \\ 0 & A_2 & & \vdots \\ \vdots & & \ddots & * \\ 0 & \cdots & 0 & A_N \end{pmatrix}$ où $\forall i \in [\![1, N]\!]$, $A_i \in \mathbb{K}$ ou $A_i = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$.
Or, A étant symétrique, B qui lui est congruente est aussi symétrique. Comme $1 \neq -1$ ($car(\mathbb{K}) \neq 2$), B ne peut être symétrique si au moins un des blocs A_i est de la forme $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. Pour tout i, A_i est donc un scalaire et B est bien une matrice diagonale. □

Comme annoncé, nous obtenons de ce corolaire que le problème de la congruence matricielle des matrices symétriques se ramène au problème de la congruence des matrices diagonales. Ainsi, la classe de congruence de matrices symétriques associées à la forme quadratique q contient nécessairement une matrice diagonale et dans une certaine base, appelée base q-orthogonale, q est représentée par une matrice diagonale.

1.2.3 Diagonalisation des formes quadratiques

Définition 1.2.3. *Soit* $(e_1, \ldots, e_n)$ *une base de* E. *On dit que la base* $(e_1, \ldots, e_n)$ *est* q*-orthogonale si et seulement si la matrice représentant* q *dans* $(e_1, \ldots, e_n)$ *est diagonale.*

Notation 1.2.1. *On note* $\langle a_1, \ldots, a_n \rangle$ *la forme quadratique diagonale définie sur l'espace* $\mathbb{K}^n$ *par :*

$$(x_1, \ldots, x_n) \mapsto a_1 x_1^2 + \ldots + a_n x_n^2$$

Remarque 1.2.1. *Pour* $(a_1, \ldots, a_n) \in \mathbb{K}^n$ *et* $(\lambda_1, \ldots, \lambda_n) \in (\mathbb{K}^*)^n$, *il est clair que les matrices diagonales* $D(a_1, \ldots, a_n)$ *et* $D(\lambda_1^2 a_1, \ldots, \lambda_n^2 a_n)$ *sont congruentes. Les formes quadratiques* $\langle a_1, \ldots, a_n \rangle$ *et* $\langle \lambda_1^2 a_1, \ldots, \lambda_n^2 a_n \rangle$ *ont donc même classe de congruence de matrices symétriques associées et sont équivalentes. De même, en passant par la congruence des matrices diagonales associées, il est clair que pour toute permutation* $\sigma \in \mathcal{S}_n$, $\langle a_1, \ldots, a_n \rangle \simeq \langle a_{\sigma(1)}, \ldots, a_{\sigma(n)} \rangle$. *Ces résultats seront utilisés abondemment par la suite.*

Remarque 1.2.2. *Le chapitre* 6 *consacré au groupe de Witt, nous permettra de caractériser les corps pour lesquels la relation de congruence matricielle restreinte aux matrices diagonales est entièrement décrite par :*

$$D(a_1,\dots,a_n) \approx D(b_1,\dots,b_n) \Longleftrightarrow \textit{il existe } \sigma \in \mathfrak{S}_n \textit{ et } (\lambda_1,\dots,\lambda_n) \in (\mathbb{K}^*)^n \textit{ tels que } \forall k \in [\![1,n]\!], b_k = \lambda_k^2 a_{\sigma(k)}$$

ce qui peut aussi se traduire en terme de formes quadratiques par :

$$\langle a_1,\dots,a_n\rangle \simeq \langle b_1,\dots,b_n\rangle \Longleftrightarrow \textit{il existe } \sigma \in \mathfrak{S}_n \textit{ et } (\lambda_1,\dots,\lambda_n) \in (\mathbb{K}^*)^n \textit{ tels que } \forall k \in [\![1,n]\!], b_k = \lambda_k^2 a_{\sigma(k)}$$

Corollaire 1.2.2. ***Principe de diagonalisation***
Soit q une forme quadratique sur un espace E de dimension n. Il existe un n-uplet $(a_i)_{1\leq i\leq n} \in \mathbb{K}^n$ tel que :

$$q \simeq \langle a_1,\dots,a_n\rangle$$

Ainsi tout espace quadratique de dimension finie admet une base orthogonale.

Démonstration. A la forme quadratique q est associée une unique classe de congruence de matrices symétriques. Cette classe de congruence contient au moins une matrice diagonale, notée $D(a_1,\dots,a_n)$. L'application définie sur $\mathbb{K}^n$ par :

$$(x_1,\dots,x_n) \mapsto a_1x_1^2 + \dots + a_nx_n^2 = {}^tXD(a_1,\dots,a_n)X$$

est donc une forme quadratique sur $\mathbb{K}^n$ qui a même classe de congruence de matrices symétriques associées que q. En effet, $D(a_1,\dots,a_n)$ représente à la fois $\langle a_1,\dots,a_n\rangle$ dans la base canonique de $\mathbb{K}^n$ et q dans une certaine base de l'espace E sur lequel elle est définie. D'où $q \simeq \langle a_1,\dots,a_n\rangle$ □

Ce principe de diagonalisation est très important, le but de la classification des formes quadratiques sur un corps $\mathbb{K}$ étant précisément de déterminer pour chaque forme quadratique q une forme quadratique diagonale la plus simple possible qui lui soit équivalente et d'étudier les caractéristiques de cette forme diagonale. Il est par exemple bien connu (nous le redémontrerons par le biais de la théorie de Witt) que les formes quadratiques complexes sont classifiées par le rang. Pour deux formes quadratiques q, q' définies sur un $\mathbb{C}$-espace vectoriel de dimension n, la seule connaissance de leur rang suffit pour nous indiquer si elles sont équivalentes et si on peut donc les "*identifier*". Etudions un exemple simple. La forme quadratique définie sur $\mathbb{C}^n$ par $\langle \underbrace{1,\dots,1}_{\times r}, \underbrace{0,\dots,0}_{\times n-r}\rangle$ étant de rang r, toute forme quadratique complexe q définie sur un $\mathbb{C}$-espace de dimension n et de rang r, lui est équivalente. Ainsi, dans le monde des formes quadratiques complexes, une telle forme q s'apparente à $\langle 1,\dots,1,0,\dots,0\rangle$, dont l'étude générale est plus aisée.

Chapitre 2

Régularité, somme orthogonale et diagonalisation des formes quadratiques

Dans ce chapitre, nous allons donner quelques définitions élémentaires indispensables à la compréhension des chapitres suivants et définir quelques objets associés à une forme quadratique tels que le rang ou le noyau. Nous nous intéresserons ainsi à la notion de régulatité d'une forme quadratique et parlerons plus précisément de sa partie régulière. Ensuite, nous définirons l'opération de somme orthogonale de deux formes bilinéaires et de deux formes quadratiques qui se révelera d'une très grande utilité lorsque nous entrerons réellement dans l'étude de la théorie de Witt. Nous profiterons de ce chapitre pour montrer comment ramener le problème de la classification des formes quadratiques au problème de la classification des formes quadratiques régulières, à l'aide de l'opération de somme orthogonale. Enfin, nous appliquerons brièvement les propriétés d'orthogonalité pour étudier la diagonalisation théorique d'une forme quadratique entrevue au chapitre 1, en évoquant le très utile, *principe de complétion à l'aide d'un déterminant.*

2.1 Partie régulière d'une forme quadratique

Dans ce paragraphe (E, q) désigne un $\mathbb{K}$-espace quadratique et l'on note b la forme polaire associée à q. Afin de parler de la notion de régularité associée à une forme quadratique, il nous est nécessaire de rappeler un certain nombre de définitions. Les définitions qui suivent exprimées avec le vocabulaire des formes quadratiques peuvent être reformulées naturellement avec le vocabulaire des formes bilinéaires. De même, on parlera de la dimension, du noyau, du rang et de la régularité d'une forme bilinéaire.

Définition 2.1.1. *On appelle* ***noyau*** *de la forme quadratique q l'ensemble :*

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

Définition 2.1.2. *La dimension de l'espace vectoriel E associé à q est appelée la* ***dimension*** *de q et notée $dim(q)$. Le* ***rang*** *de q noté $rg(q)$ est alors l'entier*

$n - dim(Ker(q))$. Il s'agit en particulier du rang de toute matrice $A \in S_n(\mathbb{K})$ représentant q.

En dimension finie, les formes quadratiques régulières sont les formes quadratiques non dégénérées :

Définition 2.1.3. *On dit que la forme quadratique q est **non dégénérée** ou **régulière** lorsque $Ker(q) = \{0\}$, ce qui équivaut à $dim(q) = rg(q)$ ou encore à ce que la classe de congruences de matrices symétriques associées à q ne soient composé que de matrices inversibles. Dans le cas contraire, on dit naturellement que q est **dégénérée** ou **n'est pas régulière**.*

Définition 2.1.4. *Soit A un sous-espace vectoriel de E. L'espace A est dit q-régulier si la restriction de q à A notée q_A est une forme quadratique régulière sur A.*

Définition 2.1.5. *Lorsque q est non dégénérée, on appelle déterminant de q tout déterminant d'une matrice symétrique de $S_n(\mathbb{K})$ représentant q. Ces matrices étant toutes congruentes, leurs déterminants sont égaux modulo les carrés de $\mathbb{K}^*$. La classe d'équivalence des déterminants de q dans $\mathbb{K}^*/(\mathbb{K}^*)^2$ est appelée* le *déterminant de q, que l'on note $det(q)$.*

Désormais, nous allons voir comment ramener l'étude des formes bilinéaires symétriques à l'étude des formes bilinéaires symétriques non dégénérées. Ceci s'effectuera à l'aide d'une opération naturelle qui consiste à quotienter E par le noyau des formes concernées. On opérera de même en ce qui concerne les formes quadratiques.

Construction de la partie régulière

Pour b une forme bilinéaire symétrique, pour tout $(x, y) \in E^2$ et pour tout $(x_0, y_0) \in Ker(b)^2$, on a :

$$b(x + x_0, y + y_0) = b(x, y) + b(x, y_0) + b(x_0, y + y_0) = b(x, y)$$

Ainsi la valeur de $b(x, y)$ ne dépend que des classes $\overline{x}$ et $\overline{y}$ de x, y dans l'espace quotient $E/Ker(b)$ et non du choix des représentants de ces classes. Ceci permet de définir l'application $\overline{b} : E/Ker(b) \times E/Ker(b) \longrightarrow \mathbb{K}$ telle que :

$$\forall (x, y) \in E^2, \overline{b}(\overline{x}, \overline{y}) = b(x, y)$$

Cette application est une forme bilinéaire sur $E/Ker(b)$, elle aussi symétrique. L'intérêt de cette forme bilinéaire $\overline{b}$ est bien entendu qu'elle est par construction même, non dégénérée et donc régulière ($E/Ker(b)$ étant de dimension finie). En effet, pour $\overline{x} \in E/Ker(b)$ tel que $\overline{b}(\overline{x}, \overline{y}) = 0$ pour tout $\overline{y} \in E/Ker(b)$ on a :

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

Définition 2.1.6. *La forme bilinéaire $\overline{b}$ définie sur $E/Ker(b)$ est appelée la partie régulière de b.*

Pour A un supplémentaire de $Ker(b)$ dans E, la projection canonique π définie de E dans $E/Ker(b)$, induit un isomorphisme π_A par restriction de π à A (A étant un supplémentaire dans E de $Ker(b) = Ker(\pi)$). On a alors :

$$\forall (x,y) \in A^2, \overline{b}(\overline{x},\overline{y}) = \overline{b}(\pi(x),\pi(y)) = b(x,y) = b_A(x,y)$$

L'application π_A étant un isomorphisme d'espaces vectoriels, pour tout supplémentaire A dans E du noyau de b on a :

$$\overline{b} \simeq b_A.$$

Ce résultat nous sera utile pour ramener le problème de la classification des formes quadratiques à la classification des formes quadratiques régulières, à l'aide d'une décomposition orthogonale appropriée. Définissons la partie régulière associée à la forme quadratique q.

Définition 2.1.7. *A la forme polaire b de q est associée sa partie régulière $\overline{b}$. On appelle **partie régulière de** q notée $\overline{q}$, la forme quadratique associée à $\overline{b}$:*

$$\forall x \in E,\ \overline{q}(\overline{x}) = \overline{b}(\overline{x},\overline{x}) = b(x,x) = q(x)$$

Remarque 2.1.1. *Ainsi, pour A un supplémentaire de $Ker(q)$ dans E, $q_A \simeq \overline{q}$ et donc q_A est régulière et A est q-régulier.*

Terminons par donner une définition qui nous sera utile pour la suite :

Définition 2.1.8. *Soit (E,q) un espace quadratique de dimension finie. On appelle **déterminant de q**, noté $det(q)$, le déterminant de sa partie régulière $\overline{q}$.*

2.2 Décomposition orthogonale d'une forme quadratique

Dans cette partie, (E,b) et (F,b') désigne deux espaces bilinéaires symétriques.

Notation 2.2.1. *Pour A, B deux sous-espaces vectoriels de E, on utilise la notation $A \overset{\perp}{\oplus} B = E$ pour signifier que A et B sont supplémentaires dans E et également orthogonaux, c'est-à-dire que :*

$$\forall (x,y) \in A \times B,\ b(x,y) = 0 \text{ et } A \oplus B = E.$$

Notre objectif ici, est de définir un nouvel espace bilinéaire symétrique à partir des deux espaces (E,b) et (F,b') donnés. Nous souhaitons également que E et F soient (à identification près) des sous-ensembles de ce nouvel espace et cherchons à ce qu'ils soient supplémentaires orthogonaux (à identification près) pour la nouvelle forme bilinéaire créée.

Définition 2.2.1. *On appelle **somme orthogonale extérieure** de b et b' notée $b \perp b'$, la forme bilinéaire symétrique définie par :*

$$\begin{array}{rccc} b\perp b' : & (E\times F)\times(E\times F) & \longrightarrow & \mathbb{K} \\ & ((x,x'),(y,y')) & \longmapsto & b(x,y)+b'(x',y') \end{array}$$

On a alors $(E \times \{0\}) \oplus (\{0\} \times F) = E \times F$ et donc E identitifié à $E \times \{0\}$ et F identifié à $\{0\} \times F$ sont supplémentaires dans $E \times F$ et sont de plus $b \perp b'$-orthogonaux car :

$$\forall (x,y) \in E \times F,\ b\perp b'((x,0),(0,y)) = b(x,0) + b'(0,y) = 0$$

Les identifications de E avec $E \times \{0\}$ via $x \mapsto (x, 0)$ et de F avec $\{0\} \times F$ via $y \mapsto (0, y)$ sont des isomorphismes d'espaces vectoriels qui permettent de voir que :

$$b \simeq (b \perp b')_{E\times\{0\}} \text{ et } b' \simeq (b \perp b')_{\{0\}\times F}.$$

Considérons alors la somme directe orthogonale $A \overset{\perp}{\oplus} B = E$ dans l'espace bilinéaire symétrique (E, b). On considère les restrictions de b à A et B que sont b_A et b_B ainsi que la somme orthogonale $b_A \perp b_B$. L'application $w : A \times B \longrightarrow E$ définie par :

$$\begin{array}{rccc} w: & A \times B & \longrightarrow & E \\ & (x, y) & \longmapsto & x + y \end{array}$$

est un isomorphisme d'espaces vectoriels et permet de montrer que les formes bilinéaires symétriques $b_A \perp b_B$ et b sont équivalentes. En effet, pour tout couple $(x, x') \in A \times B$ et tout couple $(y, y') \in A \times B$ on a :

$$\begin{aligned} b_A \perp b_B((x, x'), (y, y')) &= b_A(x, y) + b_B(x', y') \\ &= b(x, y) + b(x', y') \\ &= b(x + y, x' + y') \\ &= b(w(x, y), w(x', y')) \end{aligned}$$

où la troisième égalité provient du fait que A et B sont b-orthogonaux. On a ainsi démontré :

Proposition 2.2.1. *Soit (E, b) un espace bilinéaire tel que $A \overset{\perp}{\oplus} B = E$. Alors,*

$$b \simeq b_A \perp b_B$$

Définition 2.2.2. *Soit (E, b) et (F, b') deux espaces bilinéaires symétriques et q et q' les formes quadratiques associées. La forme quadratique associée à la forme bilinéaire symétrique $b \perp b'$ notée $q \perp q'$ est appelée* ***la somme directe orthogonale*** *des formes quadratiques q et q' et vérifie pour tout $(x, y) \in E \times F$:*

$$\begin{aligned} (q \perp q')(x, y) &= (b \perp b')((x, y), (x, y)) \\ &= b(x, x) + b'(y, y) \\ &= q(x) + q'(y) \end{aligned}$$

Ecriture matricielle de la somme orthogonale et premières propriétés

Pour (E, q) et (F, q') deux espaces quadratiques, les espaces $E \times \{0\}$ et $\{0\} \times F$ sont $q \perp q'$ orthogonaux. Ainsi, par concaténation d'une base $\mathbf{B}$ de E identifié à $E \times \{0\}$ et d'une base **B'** de F identifié à $\{0\} \times F$, on obtient alors une base de $E \times F$ dans laquelle la matrice représentant $q \perp q'$ est diagonale par blocs, de la forme :

$$\begin{pmatrix} M & 0 \\ 0 & N \end{pmatrix} \text{ où } M = Mat_{\mathbf{B}}(q) \text{ et } N = Mat_{\mathbf{B'}}(q')$$

De cette écriture matricielle et de la définition précédente, nous déduisons les résultats suivants :

1. $rg(q \perp q') = rg(q) + rg(q')$.
2. $q \perp q'$ est régulière $\iff$ q et q' sont régulières.
3. $det(q \perp q') = det(q) det(q')$.

Exemple 2.2.1. *Pour $(a_1, \ldots, a_n) \in \mathbb{K}^n$ et $(b_1, \ldots, b_p) \in \mathbb{K}^p$, les formes diagonales $\langle a_1, \ldots, a_n \rangle$ et $\langle b_1, \ldots, b_p \rangle$ sont représentées dans les bases canoniques de $\mathbb{K}^n$ et $\mathbb{K}^p$ respectivement par $D(a_1, \ldots, a_n)$ et $D(b_1, \ldots, b_p)$. Ainsi, la forme quadratique $\langle a_1, \ldots, a_n \rangle \perp \langle b_1, \ldots, b_p \rangle$ est en particulier représentée par la matrice diagonale $D(a_1, \ldots, a_n, b_1, \ldots, b_p)$ et a donc la même classe de congruence de matrices symétiques associées que la forme quadratique $\langle a_1, \ldots, a_n, b_1, \ldots, b_p \rangle$ d'où :*

$$\langle a_1, \ldots, a_n \rangle \perp \langle b_1, \ldots, b_p \rangle \simeq \langle a_1, \ldots, a_n, b_1, \ldots, b_p \rangle$$

Proposition 2.2.2. *Soit q_1, q_1', q_2, q_2' quatre formes quadratiques. Alors,*

$$q_1 \simeq q_1' \text{ et } q_2 \simeq q_2' \Longrightarrow q_1 \perp q_2 \simeq q_1' \perp q_2'$$

et la somme orthogonale est compatible avec l'équivalence entre formes quadratiques.

Démonstration. Puisque $q_1 \simeq q_1'$ et $q_2 \simeq q_2'$, q_1 et q_1' ont même classe de congruence de matrices symétriques associées, de même pour q_2 et q_2'. Soit alors M et N représentant respectivement q_1 et q_2 dans deux bases données. La matrice diagonale par blocs $\begin{pmatrix} M & 0 \\ 0 & N \end{pmatrix}$ représente donc $q_1 \perp q_2$ dans une certaine base. Elle représente aussi $q_1' \perp q_2'$ puisque M et N représentent également q_1' et q_2' dans deux autres bases. Ainsi $q_1 \perp q_2$ et $q_1' \perp q_2'$ sont représentées par la même matrice dans deux bases éventuellement différentes et ont donc même classe de congruence de matrices symétriques associées. Soit, $q_1 \perp q_2 \simeq q_1' \perp q_2'$. □

Proposition 2.2.3. *Soit (E, q) un espace quadratique tel que $A \overset{\perp}{\oplus} B = E$. Alors,*

$$q \simeq q_A \perp q_B$$

Démonstration. On note b la forme polaire associée à q, ainsi $b_A \perp b_B$ est la forme polaire associée à $q_A \perp q_B$. Deux formes quadratiques étant équivalentes si et seulement si leurs formes polaires associées le sont, d'après la proposition 2.2.1 on a $b \simeq b_A \perp b_B$ ce qui implique $q \simeq q_A \perp q_B$. □

Notation 2.2.2. *Dans la suite on note $n.q$, la forme quadratique $q \perp q \perp \cdots \perp q$ où q apparaît n fois.*

Problème de la classification des formes quadratiques et formes quadratiques régulières

Pour terminer cette partie, nous allons voir comment décomposer une forme quadratique en une somme orthogonale d'une forme régulière et d'une forme nulle. Ceci nous permettra de nous concentrer par la suite plus spécifiquement sur l'étude de la classification des formes quadratiques régulières.

Théorème 2.2.1. *Soit q une forme quadratique sur E de dimension n telle que $rg(q) = r$. On a la décomposition suivante :*

$$q \simeq \overline{q} \perp (n-r).\langle 0 \rangle$$

Démonstration. Soit A un supplémentaire de $Ker(q)$ dans E. Alors, A est en particulier un supplémentaire orthogonal de $Ker(q)$ dans E, ce qui nous donne :

$$q \simeq q_A \perp q_{Ker(q)} \text{ et } q_A \simeq \overline{q}.$$

Or, q restreinte à son noyau est une forme nulle de dimension $n-r$ (celle du noyau), d'où $q_{Ker(q)} \simeq (n-r).\langle 0 \rangle$ et par compatibilité de l'équivalence entre formes quadratiques avec la somme orthogonale :

$$q \simeq \overline{q} \perp (n-r).\langle 0 \rangle.$$

□

2.3 Principe de complétion

Dans cette partie, on va montrer que si la restriction de q à un sous-espace $F \subset E$ de dimension p est une forme quadratique régulière, alors il existe $(b_{p+1}, \ldots, b_n) \in \mathbb{K}^{n-p}$ tel que $q \simeq q_F \perp \langle b_{p+1}, \ldots, b_n \rangle$.

Proposition 2.3.1. *Soit $(a_1, \ldots, a_p) \in (\mathbb{K}^*)^p$. On suppose qu'il existe un sous-espace vectoriel F de E de dimension p tel que $q_F \simeq \langle a_1, \ldots, a_p \rangle$, alors il existe $(b_{p+1}, \ldots, b_n) \in \mathbb{K}^{n-p}$ tel que :*

$$q \simeq q_F \perp \langle b_{p+1}, \ldots, b_n \rangle \simeq \langle a_1, \ldots, a_p, b_{p+1}, \ldots, b_n \rangle$$

Démonstration. D'après le chapitre 1, F admet une base q_F-orthogonale notée $(e_1, \ldots, e_p)$. Dans cette base, q_F est représentée par la matrice diagonale inversible (car q_F régulière) $D(q(e_1), \ldots, q(e_p))$ et donc $q_F \simeq \langle q(e_1), \ldots, q(e_p) \rangle$. Notant $a_i = q(e_i)$ on a $q_F \simeq \langle a_1, \ldots, a_p \rangle$.

Puisque F est un espace régulier on a $F \overset{\perp}{\oplus} F^\perp = E$ (cf.[1] IV.4.3.1 page 73) et on obtient donc une base orthogonale de E par juxtaposition à $(e_1, \ldots, e_p)$ d'une base orthogonale de $F^\perp$. Notant $(e_{p+1}, \ldots, e_n)$ la base orthogonale de $F^\perp$ considérée, q est donc représentée par la matrice $D(q(e_1, \ldots, q(e_p), q(e_{p+1}), \ldots, q(e_n))$ dans la base $(e_1, \ldots, e_n)$. Notant $b_j = q(e_j)$ pour $j \in [\![p+1, n]\!]$, on a bien :

$$q \simeq \langle q(e_1, \ldots, q(e_p), q(e_{p+1}), \ldots, q(e_n) \rangle \simeq \langle a_1, \ldots, a_p, b_{p+1}, \ldots, b_n \rangle.$$

□

Corollaire 2.3.1. *On suppose q régulière. Soit δ un déterminant de q et H un hyperplan de E tel que $q_H \simeq \langle a_1, \ldots, a_{n-1} \rangle$ avec $(a_1, \ldots, a_{n-1}) \in (\mathbb{K}^*)^{n-1}$. Alors :*

$$q \simeq q_H \perp \langle \delta \prod_{k=1}^{n-1} a_k \rangle \simeq \langle a_1, \ldots, a_{n-1}, \delta \prod_{k=1}^{n-1} a_k \rangle$$

Démonstration. Par la proposition 2.3.1, il existe $\lambda \in \mathbb{K}$ tel que $q \simeq q_H \perp \langle \lambda \rangle$. Or, $det(q) = \delta$ et $det(q) = det(q_H) det(\langle \lambda \rangle)$ soit $\delta = \lambda \prod_{k=1}^{n-1} a_k$ dans $\mathbb{K}^*/(\mathbb{K}^*)^2$. Notant $\pi = \prod_{k=1}^{n-1} a_k$, on a $\delta\pi = \lambda\pi^2$ soit $\delta\pi = \lambda$ dans $\mathbb{K}^*/(\mathbb{K}^*)^2$. Ainsi, on a :

$$q \simeq \langle a_1, \ldots, a_{n-1} \rangle \perp \langle \lambda \rangle \simeq \langle a_1, \ldots, a_{n-1} \rangle \perp \langle \delta\pi \rangle \simeq \langle a_1, \ldots, a_{n-1}, \delta\pi \rangle$$

□

Chapitre 3

Espaces quadratiques hyperboliques et méthodes d'étude de la représentation des scalaires par une forme quadratique

Dans tout ce chapitre (E, q) désigne un $\mathbb{K}$-espace quadratique de dimension finie.

Un des objectifs de ce chapitre est l'étude de la notion d'isotropie. Nous commencerons par nous intéresser à l'isotropie dans le cadre de la dimension 2 et nous démontrerons que tous les plans quadratiques réguliers et isotropes sont isomorphes à l'espace quadratique $(\mathbb{K}^2, (x, y) \mapsto xy)$. Nous dirons que ces plans quadratiques sont hyperboliques et à l'aide de l'opération d'addition orthogonale vue au chapitre précédent nous étendrons cette notion de forme quadratique hyperbolique, en dimension supérieure. Dans une seconde partie, nous introduirons la notion de sous-espace totalement isotrope et nous verrons justement que tout sous-espace totalement isotrope se plonge dans un sous-espace hyperbolique de dimension double. Ce dernier résultat s'appelle le principe du gonflement hyperbolique et sera défini et démontré de manière matricielle. Enfin, nous aborderons le problème de la représentation des scalaires et nous développerons des méthodes pour savoir si un scalaire $a \in \mathbb{K}^*$ est dans le domaine d'une forme quadratique q, c'est-à-dire s'il existe un $x \in E$ tel que $q(x) = a$. Nous dirons alors que le scalaire a est représenté par la forme quadratique q. Dans ce chapitre nous énoncerons simplement les outils fondamentaux dont nous aurons besoin pour étudier par la suite, sur des cas concrets, le problème de la représentation des scalaires. En effet, un chapitre spécifique y sera consacré avec l'étude de la représentation dans le cadre rationnel, mais pour ce faire il nous faudra auparavant étudier la notion de Witt-équivalence et expliciter les tests d'équivalence et de Witt-équivalence sur $\mathbb{Q}$.

3.1 Isotropie et plans quadratiques

Rappelons pour commencer la définition de la notion d'isotropie et de cône isotrope.

Définition 3.1.1. *Un vecteur $x \in E$ est dit* ***isotrope*** *pour la forme quadratique q lorsque $q(x) = 0$. Dans le cas contraire, il est dit* ***anisotrope****. On dit que q est* ***isotrope*** *lorsqu'elle admet un vecteur isotrope* non nul. *Dans le cas contraire, on dit que q est* ***anisotrope****.*

Proposition 3.1.1. *Soit q une forme quadratique anisotrope de dimension finie, alors q est nécessairement régulière.*

Démonstration. Supposons par l'absurde que q soit dégénérée. Alors, il existe $x \in E$ non nul tel que $b(x, y) = 0$ pour tout $y \in E$ où b est la forme polaire associée à q. En particulier $q(x) = b(x, x) = 0$ et donc q serait isotrope, absurde. □

Proposition 3.1.2. *Soit (E, q) et (E, q') deux espaces quadratiques isomorphes. Alors q est isotrope si et seulement si q' est isotrope. De même q est anisotrope si et seulement si q' est anisotrope.*

Démonstration. Supposons q isotrope, alors il existe $x_0 \neq 0$ tel que $q(x_0) = 0$. Puisque $q \simeq q'$, il existe un isomorphisme u tel que :

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

Ainsi, q' est aussi isotrope car $u(x_0) \neq 0$ annule q'. La réciproque est identique. D'où q isotrope $\iff$ q' isotrope et donc par négation, on obtient également, q anisotrope $\iff$ q' anisotrope. □

Définition 3.1.2. *On appelle* ***cône isotrope*** *de q l'ensemble :*

$$Co(q) = \{x \in E : q(x) = 0\}$$

Définition 3.1.3. *Un plan quadratique est dit* ***hyperbolique*** *lorsqu'il est isomorphe à $(\mathbb{K}^2, (x, y) \mapsto xy)$.*

Pour $x \neq 0$, $(x, 0)$ est clairement un vecteur isotrope pour la forme $(x, y) \longmapsto xy$, ce qui montre qu'elle est isotrope. La matrice $\begin{pmatrix} 1/2 & 0 \\ 0 & 1/2 \end{pmatrix}$ associée à cette forme dans la base canonique de $\mathbb{K}^2$ étant inversible, elle est de rang 2 et est régulière. Par définition même, tous les plans hyperboliques sont isomorphes car tous isomorphes à l'espace quadratique $(\mathbb{K}^2, (x, y) \mapsto xy)$, ils sont donc réguliers et isotropes. La réciproque est également vraie ce qui nous donne une caractérisation simple des plans hyperboliques.

Théorème 3.1.1. *Les plans hyperboliques sont les plans quadratiques réguliers isotropes.*

Démonstration. Un plan hyperoblique est, on l'a vu, un espace quadratique régulier et isotrope. Réciproquement, soit (P, q') un plan quadratique régulier isotrope. Puisque q' est isotrope, il existe $x_0 \neq 0$ vecteur isotrope dans P, que l'on complète en une base $(x_0, x_1) = \mathbf{B}$ de P. La matrice représentant q' dans la base $\mathbf{B}$ s'écrit alors $\begin{pmatrix} 0 & a \\ a & b \end{pmatrix}$ et q' s'écrit de manière analytique dans $\mathbf{B}$ par :

$$(X,Y) \mapsto (X,Y)\begin{pmatrix}0 & a\\ a & b\end{pmatrix}\begin{pmatrix}X\\ Y\end{pmatrix} = 2aXY + bY^2$$

Notant f, g les formes linéaires définies dans $\mathbf{B}$ par :

$$f : (X,Y) \mapsto 2aX + Y \text{ et } g : (X,Y) \mapsto Y$$

on a : $q'(X,Y) = f(X,Y)g(X,Y)$ dans $\mathbf{B}$, soit $q' = fg$. Puisque q' est régulière, la matrice associée à q' dans $\mathbf{B}$ est inversible et nécessairement $a \neq 0$. Les formes linéaires f, g sont alors indépendantes et forment une base de l'espace dual P^*. Notant $(e_1, e_2) = \mathbf{B}_1$ la base antéduale de (f, g) telles que $f(e_1) = 1, f(e_2) = 0$ et $g(e_1) = 0, g(e_2) = 1$, q' s'écrit analytiquement dans cette base $(x, y) \mapsto xy$. En effet, dans cette nouvelle base, pour $(\alpha, \beta) \in \mathbb{K}^2$, on a :

$$q'(\alpha e_1 + \beta e_2) = q'(\alpha, \beta) = f(\alpha e_1 + \beta e_2)g(\alpha e_1 + \beta e_2) = \alpha\beta$$

et q' est donc hyperbolique. □

Donnons quelques caractérisations simples des plans hyperboliques :

Théorème 3.1.2. *Soit (P, q) un plan quadratique régulier. Les conditions suivantes sont équivalentes :*

1. *La forme quadratique q est hyperbolique.*
2. *La forme quadratique q est isotrope.*
3. *$q \simeq \langle 1, -1\rangle$.*
4. *$q \simeq \langle a, -a\rangle$ pour $a \in \mathbb{K}^*$.*
5. *q est équivalente à $(x, y) \mapsto xy$.*
6. *q est représentée par la matrice $\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$.*
7. *$det(q) = -1$ dans $\mathbb{K}^*/(\mathbb{K}^*)^2$.*

Démonstration.

- $1 \iff 2$ est immédiate.
- $1 \iff 3, 4$ puisque $\langle 1, -1\rangle$ et $\langle a, -a\rangle$ sont toutes deux régulières et isotropes ; $(1, 1)$ étant un vecteur isotrope de ces deux formes quadratiques diagonales.
- $1 \iff 5$ puisque la forme quadratique $(x, y) \mapsto xy$ est bien régulière et isotrope ; $(1, 1)$ étant encore une fois un vecteur isotrope.
- $1 \iff 6$ puisque la matrice $\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$ représente la forme quadratique $(x, y) \mapsto 2xy$ qui est régulière et isotrope, dans la base canonique de $\mathbb{K}^2$.
- Enfin, montrons $1 \iff 7$. Puisque q est régulière, elle est en particulier non nulle et il existe $a \in \mathbb{K}^*$ et $x \neq 0$ tel que $q(x) = a$. Alors $q_{vect(x)} \simeq \langle a\rangle$ avec $vect(x)$ un hyperplan de l'espace E sur lequel est définie q. Par l'astuce de complétion a l'aide d'un déterminant, on a alors :
$$q \simeq q_{vect(x)} \perp \langle -a\rangle \simeq \langle a, -a\rangle$$
et q est donc hyperbolique. Inversement si q est hyperbolique, elle est en particulier équivalente à la forme quadratique diagonale $\langle 1, -1\rangle$ et donc de même déterminant, soit -1 dans $\mathbb{K}^*/(\mathbb{K}^*)^2$.

□

3.2 Espaces quadratiques hyperboliques

Dans cette partie, nous allons généraliser en dimension quelconque la notion d'espace quadratique hyperbolique.

Définition 3.2.1. *On appelle* ***espace quadratique hyperbolique*** *tout espace quadratique isomorphe à une somme orthogonale finie de plans hyperboliques.*

Ainsi, tout espace quadratique est régulier, comme somme orthogonale d'espaces réguliers. De plus, tout plan quadratique étant de dimension 2, tout espace hyperbolique est de dimension paire $2n$ où n désigne le nombre de plans quadratiques dans l'écriture sous la forme de somme orthogonale de plans quadratiques.

Exemple 3.2.1. ***Les espaces hyperboliques canoniques***
Soit V un $\mathbb{K}$-espace vectoriel de dimension finie n et V^* l'espace dual associé. On définit

$$\begin{array}{rccc} \mathbb{H}(V): & V\times V^* & \longrightarrow & \mathbb{K} \\ & (x,f) & \longmapsto & 2f(x) \end{array}$$

$\mathbb{H}(V)$ est alors une forme quadratique de forme polaire :

$$\begin{array}{rccc} b: & (V\times V^*)\times((V\times V^*) & \longrightarrow & \mathbb{K} \\ & ((x,f),(x',f')) & \longmapsto & f(x')+f'(x) \end{array}$$

Alors, en identifiant V avec $V\times\{0\}$ et V^* avec $\{0\}\times V^*$, on peut voir V et V^* comme deux espaces supplémentaires dans $V\times V^*$ et par concaténation d'une base $(e_1,\dots,e_n)$ de V et de sa base duale $(e_1^*,\dots,e_n^*)$, on obtient une base $(e_1,\dots,e_n,e_1^*,\dots,e_n^*)$ de $V\times V^*$ et dans cette base la matrice de $\mathbb{H}(V)$ s'écrit :

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

Nous dirons que $H(V)$ est la ***forme hyperbolique*** *associée à V. Il s'agit alors de justifier cette appelation en montrant que l'espace $(V\times V^*,\mathbb{H}(V))$ est bien hyperbolique. En notant P_k l'espace vectoriel $vect(e_k,e_k^*)$, les plans quadratiques associés $(P_k,\mathbb{H}(V)_{P_k})$ sont deux à deux orthogonaux pour $\mathbb{H}(V)$ et tels que :*

$$V\times V^* = P_1 \overset{\perp}{\oplus} \dots \overset{\perp}{\oplus} P_n.$$

En effet, pour tout $i\neq j$ on a :

$$b((\alpha_1 e_i,\beta_1 e_i^*),(\alpha_2 e_j,\beta_2 e_j^*)) = \alpha_2\beta_1 e_i^*(e_j)+\alpha_1\beta_2 e_j^*(e_i) = 0$$

avec de plus :

$$vect(e_1,e_1^*)\oplus\dots\oplus vect(e_n,e_n^*) = vect(e_1,\dots,e_n,e_1^*,\dots,e_n^*) = V\times V^*$$

D'après la proposition 2.2.3 du chapitre précédent, on a $q\simeq q_{P_1}\perp\dots\perp q_{P_n}$, où chaque espace $(P_k,\mathbb{H}(V)_{P_k})$ est hyperbolique (car de matrice associée $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ dans (e_k,e_k^*)) ce qui montre que q est hyperbolique.

Nous allons désormais donner une caractérisation des espaces hyperboliques :

Théorème 3.2.1. *Soit (E, q) un espace quadratique de dimension $2n$. Les conditions suivantes sont équivalentes.*

1. *La forme quadratique q est hyperbolique.*
2. $q \simeq n.\langle 1, -1\rangle$
3. $q \simeq \varphi\perp(-\varphi)$ *pour une certaine forme régulière* φ.
4. *La matrice* $\begin{pmatrix} 0 & I_n \\ I_n & 0 \end{pmatrix}$ *représente* q.
5. $q \simeq \mathbb{H}(V)$ *pour un certain* $\mathbb{K}$*-espace vectoriel* V *de dimension* n.

Démonstration.

- Montrons $1 \iff 2$. L'implication $2 \implies 1$ est claire par définition d'un espace hyperbolique et caractérisation des plans quadratiques. $1 \implies 2$ découle du fait que q étant hyperbolique, q s'écrit comme une somme orthogonale de plans quadratiques, chacun étant isomorphe à $(\mathbb{K}^2, \langle 1, -1\rangle)$.
- Montrons $2 \iff 3$. On suppose 2, alors notant $\varphi = n.\langle 1\rangle$, on obtient
$$q \simeq n.\langle 1, -1\rangle \simeq n.\langle 1\rangle\perp n.\langle -1\rangle$$
et donc $q \simeq \varphi\perp(-\varphi)$ et $2 \implies 3$. Réciproquement soit φ une forme quadratique régulière telle que $q \simeq \varphi\perp(-\varphi)$, par le principe de diagonalisation du chapitre 1 et par régularité $\varphi \simeq \langle a_1, \ldots, a_n\rangle$ où $a_i \neq 0$ pour tout i. Soit :
$$\begin{aligned} \varphi\perp(-\varphi) &\simeq \langle a_1, \ldots, a_n\rangle\perp\langle -a_1, \ldots, -a_n\rangle \\ &\simeq \langle a_1, \ldots, a_n, -a_1, \ldots, -a_n\rangle \\ &\simeq \langle a_1, -a_1\rangle\perp \ldots \perp\langle a_n, -a_n\rangle \\ &\simeq \langle 1, -1\rangle\perp \ldots \perp\langle 1, -1\rangle \\ &\simeq n.\langle 1, -1\rangle \end{aligned}$$
Ce qui montre $3 \implies 2$, puis $2 \iff 3$.
- Montrons $4 \iff 5$. On suppose 4, alors q est représentée dans une certaine base par la matrice $\begin{pmatrix} 0 & I_n \\ I_n & 0 \end{pmatrix}$. Pour tout espace vectoriel V de dimension n, $\mathbb{H}(V)$ est aussi représentée par cette même matrice, d'où $q \simeq \mathbb{H}(V)$ pour tout espace vectoriel V de dimension n et $4 \implies 5$. Réciproquement, si pour un certain espace V de dimension n, $q \simeq \mathbb{H}(V)$ alors $\mathbb{H}(V)$ étant représentée par la matrice $\begin{pmatrix} 0 & I_n \\ I_n & 0 \end{pmatrix}$, q l'est également et $5 \implies 4$. D'où $4 \iff 5$.
- Montons $5 \iff 1$. On suppose 5, alors q est représentée par la matrice $\begin{pmatrix} 0 & I_n \\ I_n & 0 \end{pmatrix}$ elle même congruente (par simple permutation des vecteurs de base) à la matrice diagonale par blocs $D(K, \ldots, K)$ où $K = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Or, la matrice $D(K, \ldots, K)$ représente la forme quadratique $q_1\perp \ldots \perp q_1$ où
$$q_1 : (x, y) \mapsto 2xy$$
est une forme hyperbolique par caractérisation des plans hyperboliques, soit $5 \implies 1$. Si on suppose 1, alors q est hyperbolique et donc somme orthogonale de n formes hyperboliques de dimension 2. Par caractérisation des plans hyperboliques,

$$q \simeq q_1 \perp \ldots \perp q_1 \text{ où } q_1 : (x, y) \mapsto 2xy$$

et est représentée par $D(K, \ldots, K)$ qui est congruente à $\begin{pmatrix} 0 & I_n \\ I_n & 0 \end{pmatrix}$. Ainsi $1 \Longrightarrow 4 \Longleftrightarrow 5$, puis $5 \Longleftrightarrow 1$.
On a donc $1 \Longleftrightarrow 2 \Longleftrightarrow 3$ et $4 \Longleftrightarrow 5 \Longleftrightarrow 1$, ce qui achève de montrer le théorème.

□

3.2.1 Sous-espaces totalement isotropes

Dans cette partie, on considère un espace quadratique (E, q) régulier, de forme polaire b.

Définition 3.2.2. *Un sous-espace vectoriel F de E est dit **totalement isotrope** lorsque $F \subset Co(q)$ c'est à dire : $\forall x \in F$, $q(x) = 0$.*

Donnons alors une caractérisation en terme d'orthogonalité :

Proposition 3.2.1. *Un sous-espace vectoriel F de E est totalement isotrope si et seulement si $F \subset F^{\perp}$.*

Démonstration. Supposons $F \subset F^{\perp}$. Soit $x \in F$, alors $x \in F^{\perp}$ et on a

$$b(x, y) = 0, \forall y \in F.$$

En particulier pour $y = x$, $b(x, x) = q(x) = 0$ et donc $x \in Co(q)$ soit $F \subset Co(q)$. Réciproquement, supposons F totalement isotrope. Alors, pour $x \in F$, on a

$$b(x, y) = \frac{1}{2}(q(x + y) - q(x) - q(y)) = 0, \forall y \in F$$

car x, y et $x + y$ sont dans $F \subset Co(q)$ et donc $F \subset F^{\perp}$. □

Remarque 3.2.1. *Pour (E, q) est un espace régulier, on a :*

$$dim(F^{\perp}) = dim(E) - dim(F).$$

Si F totalement isotrope, $F \subset F^{\perp}$ soit $dim(F) \leq dim(F^{\perp})$ et nécessairement :

$$dim(F) \leq \frac{1}{2} dim(E).$$

Ainsi, les sous-espaces totalement isotropes de (E, q) ont une dimension inférieure ou égale à $\dfrac{dim(E)}{2}$.

Ceci nous amène à donner la définition suivante :

Définition 3.2.3. *On appelle **lagrangien** de (E, q) tout sous-espace vectoriel totalement isotrope de E de dimension $\dfrac{dim(E)}{2}$.*

Proposition 3.2.2. *Tout espace hyperbolique possède des lagrangiens.*

Démonstration. Soit (E, q) un espace hyperbolique de dimension $2n$. D'après le théorème de caractérisation de ces espaces, il existe un espace vectoriel V de dimension n tel que $q \simeq \mathbb{H}(V)$ où $\mathbb{H}(V)$ est définie sur $V \times V^*$. Alors, les sous-espaces $V \times \{0\}$ et $\{0\} \times V^*$ (que l'on peut identifier respectivement à V et V^*) sont deux sous-espaces supplémentaires dans $V \times V^*$ de même dimension $n = \dfrac{dim(E)}{2}$. On a alors :

$$\forall x \in V,\ \mathbb{H}(V)(x, 0) = 0 \text{ et } \forall f \in V^*,\ \mathbb{H}(V)(0, f) = 2f(0) = 0$$

ce qui montre que $V \times \{0\}$ et $\{0\} \times V^*$ sont inclus dans $Co(\mathbb{H}(V))$ et sont deux lagrangiens pour $\mathbb{H}(V)$. Or (E, q) étant isomorphe à $(V, \mathbb{H}(V))$, il existe un isomorphisme d'espaces vectoriels, $u : V \times V^* \longrightarrow E$ tel que :

$$\forall (x, f) \in V \times V^*,\ q(u(x, f)) = \mathbb{H}(V)(x, f)$$

et les sous-espaces de E que sont $u(V \times \{0\})$ et $u(\{0\} \times V^*)$ sont de même dimension n et totalement-isotropes pour q. Ce sont donc des lagrangiens de (E, q). □

Définition 3.2.4. *Un sous-espace totalement isotrope de (E, q) est dit **maximal** lorsqu'il n'est strictement inclus dans aucun sous-espace totalement isotrope.*

En raison de la maximalité de la dimension, tout lagrangien est en particulier un sous-espace totalement isotrope maximal.

3.2.2 Principe du gonflement hyperbolique

Dans la suite, on considère un espace quadratique régulier (E, q) et on suppose que F est un sous-espace vectoriel de E, totalement isotrope. Nous verrons qu'il est alors possible d'injecter F dans un espace vectoriel H de dimension double et telle que la restriction q_H de q à H soit hyperbolique. Ce résultat nous sera en particulier très utile pour l'étude de l'isotropie et du domaine d'une forme quadratique régulière, notamment pour prouver que toute forme quadratique régulière isotrope est universelle, c'est-à-dire que tous les scalaires de $\mathbb{K}$ sont représentés par q.

Théorème 3.2.2. ***Version matricielle du principe de gonflement hyperbolique***
Soit (E, q) un espace quadratique régulier et F un sous-espace totalement isotrope de dimension n. Il existe alors un espace vectoriel H tel que $F \subset H$, $dim(H) = 2dim(F) = 2n$ et pour lequel :

$$Mat(q_H) = \begin{pmatrix} 0_n & I_n \\ I_n & 0_n \end{pmatrix}$$

Démonstration. En gardant les notations du théorème ci-dessus, on va montrer dans un premier temps qu'il existe H espace de dimension $2n$ tel que $F \subset H$ et pour lequel :

$$Mat(q_H) = \begin{pmatrix} 0_n & {}^tA \\ A & B \end{pmatrix} \text{ avec } A \in GL_n(\mathbb{K}) \text{ et } B \in S_n(\mathbb{K}).$$

Il restera ensuite à montrer que les matrices $\begin{pmatrix} 0_n & {}^tA \\ A & B \end{pmatrix}$ et $\begin{pmatrix} 0_n & I_n \\ I_n & 0_n \end{pmatrix}$ sont congruentes pour conclure qu'il existe une base de H dans laquelle est vérifiée l'égalité matricielle annoncée dans le théorème, ce qui montrera que (H, q_H) est un espace hyperbolique.

Commençons par construire H espace vectoriel régulier contenant F et de dimension $2n$. Puisque $F \subset F^\perp$, $F^\perp$ s'écrit $F \oplus G$ où G est un supplémentaire de F dans $F^\perp$ (non unicité de G). Alors (E, q) étant régulier on a :

$$dim(E) = dim(F) + dim(F^\perp) \text{ et } dim(E) = dim(G) + dim(G^\perp)$$

Via la somme directe $F^\perp = F \oplus G$, on a également :

$$\begin{aligned} dim(G^\perp) = & \quad dim(E) - dim(G) \\ = & \quad dim(E) - (dim(F^\perp) - dim(F)) \\ = & \quad dim(F) + (dim(E) - dim(F^\perp)) \\ = & \quad 2dim(F) \end{aligned}$$

On pose $H = G^\perp$ et il reste à montrer que H ainsi construit contient F et est un sous-espace régulier de E. Or, H est régulier si et seulement si $H^\perp$ est régulier avec $H^\perp = (G^\perp)^\perp = G$ puisque (E, q) est régulier (cf.[1] IV 4.2.4 et 4.2.8 page 72). On va ainsi montrer que q_G est régulière ce qui prouvera que q_H est régulière et donc que H est régulier. Montrons d'abord que $Ker(q_{F^\perp}) = F$. Pour b la forme polaire associée à q, on a :

$$Ker(q_{F^\perp}) = \{x \in F^\perp : b(x, y) = 0, \ \forall y \in F^\perp\}$$

Naturellement $F \subset ker(q_{F^\perp})$. Réciproquement, soit $x \in Ker(q_{F^\perp})$. En particulier, $x \in F^\perp$ et s'écrit de manière unique $x_1 + x_2$ où $(x_1, x_2) \in F \times G$. Comme pour tout $y \in F^\perp, b(x, y) = 0$ on a :

$$\begin{aligned} b(x, y) = 0 \iff & \quad b(x_1 + x_2, y) = 0 \\ \iff & \quad b(x_1, y) + b(x_2, y) = 0 \\ \iff & \quad b(x_2, y) = 0 \\ \iff & \quad x_2 \in (F^\perp)^\perp = F \end{aligned}$$

Ainsi $x_2 \in F \cap G = \{0\}$ et donc $x = x_1 \in F$, soit finalement $Ker(q_{F^\perp}) = F$. L'espace G est un supplémentaire de $F = Ker(q_{F^\perp})$ dans $F^\perp$, soit donc :

$$q_G \simeq \overline{q_{F^\perp}}.$$

Etant équivalente à une forme quadratique régulière, q_G est elle-même régulière tout comme q_H. Il reste à vérifier que $F \subset H = G^\perp$. Soit $y \in F$, pour tout $z \in G$ on a $b(y, z) = 0$ car $y \in F$ et $z \in G \subset F^\perp$ ce qui montre bien que $F \subset H$.

Ainsi H est un espace régulier contenant F et de dimension $2dim(F)$.

Soit H_1 un supplémentaire de F dans H. Par concaténation d'une base de F notée $\{f_1, f_2, \cdots, f_n\}$ et d'une base de H_1 notée $\{h_1, h_2, \cdots, h_n\}$, on obtient une base $\{f_1, f_2, \cdots, f_n, h_1, h_2, \cdots, h_n\}$ de H dans laquelle q_H est représentée par la matrice :

$$\begin{pmatrix} 0_n & {}^tA \\ A & B \end{pmatrix}$$

où $A = \begin{pmatrix} b(h_1,f_1) & \cdots & b(h_1,f_n) \\ b(h_2,f_1) & \cdots & b(h_2,f_n) \\ \vdots & \ddots & \vdots \\ b(h_n,f_1) & \cdots & b(h_n,f_n) \end{pmatrix}$ et $B = \begin{pmatrix} b(h_1,h_1) & \cdots & b(h_1,h_n) \\ b(h_2,h_1) & \cdots & b(h_2,h_n) \\ \vdots & \ddots & \vdots \\ b(h_n,h_1) & \cdots & b(h_n,h_n) \end{pmatrix}$, le bloc supérieur gauche $\begin{pmatrix} b(f_1,f_1) & \cdots & b(f_1,f_n) \\ b(f_2,f_1) & \cdots & b(f_2,f_n) \\ \vdots & \ddots & \vdots \\ b(f_n,f_1) & \cdots & b(f_n,f_n) \end{pmatrix}$ de taille $n \times n$ étant nul puisque F est totalement isotrope.

Puisque (H, q_H) est régulière, $Mat(q_H)$ est inversible et donc $A \in GL_n(\mathbb{K})$. Sinon, une des colonnes de A serait combinaison linéaire non triviale des autres colonnes de A et le bloc supérieur gauche étant nul, la colonne de $Mat(q_H)$ correspondante serait combinaison linéaire non triviale des autres n premières colonnes de $Mat(q_H)$, absurde. Quant à B, elle appartient naturellement à $S_n(\mathbb{K})$ puisque la forme polaire b est symétrique. Montrons désormais que :

$$\begin{pmatrix} 0_n & {}^tA \\ A & B \end{pmatrix} \approx \begin{pmatrix} 0_n & I_n \\ I_n & 0_n \end{pmatrix}.$$

Puisque $A \in GL_n(\mathbb{K})$, A est de rang n et il existe des matrices inversibles P, Q telles que $PAQ = I_n$. On a alors :

$$\begin{pmatrix} {}^tQ & 0_n \\ 0_n & P \end{pmatrix} \begin{pmatrix} 0_n & {}^tA \\ A & B \end{pmatrix} \begin{pmatrix} Q & 0_n \\ 0_n & {}^tP \end{pmatrix} = \begin{pmatrix} 0_n & {}^tQ\,{}^tA\,{}^tP \\ PAQ & PB\,{}^tP \end{pmatrix} = \begin{pmatrix} 0_n & I_n \\ I_n & PB\,{}^tP \end{pmatrix}$$

B étant symétrique, $PB\,{}^tP$ qui lui est congruente est aussi symétrique et au final on a montré que :

$$\begin{pmatrix} 0_n & {}^tA \\ A & B \end{pmatrix} \approx \begin{pmatrix} 0_n & I_n \\ I_n & PB\,{}^tP \end{pmatrix}$$

et le problème revient donc à montrer que pour C matrice symétrique

$$\begin{pmatrix} 0_n & I_n \\ I_n & C \end{pmatrix} \approx \begin{pmatrix} 0_n & I_n \\ I_n & 0_n \end{pmatrix}.$$

Soit donc $M = \begin{pmatrix} 0_n & I_n \\ I_n & C \end{pmatrix}$ de taille $2n$ avec $(L_i)_{1\leq i\leq 2n}$ et $(C_i)_{1\leq i\leq 2n}$ respectivement les $2n$ lignes et les $2n$ colonnes de la matrice M. On va commencer par annuler tous les coefficients non diagonaux de C via des opérations élémentaires symétriques sur les lignes et les colonnes de la matrice $C = (c_{i,j})_{1\leq i,j\leq n}$. Soit $i \neq j$ et essayons d'annuler le coefficient d'indice (i,j) de la matrice C. L'opération $C_{n+j} \longleftarrow C_{n+j} - c_{i,j}C_i$ va laisser la colonne C_{n+j} inchangée sauf le coefficient $c_{i,j}$ qui va être annulé. Son opération symétrique associée au niveau des lignes $L_{n+i} \longleftarrow L_{n+i} - c_{i,j}L_i$ va par symétrie de C laisser la ligne L_{n+i} inchangée sauf le coefficient $c_{i,j} = c_{j,i}$ qui va être annulé. Ainsi l'opération $(C,L)_{n+i} \longleftarrow (C,L)_{n+i} - c_{i,j}(C,L)_i$ annule les coeffients d'indice (i,j) et (j,i) de C. Ces opérations symétriques élémentaires correspondent à des multiplications à gauche de M par des matrices inversibles et à droite de M par les transposées de ces mêmes matrices inversibles. On effectue alors ces opérations pour i,j tels que $1 \leq j < i \leq n$ ce qui nous permet d'obtenir une matrice congruente à $\begin{pmatrix} 0_n & I_n \\ I_n & D \end{pmatrix}$ où l'on note D la matrice diagonle suivante :

$$D = \begin{pmatrix} \lambda_1 & 0 & \dots & 0 \\ 0 & \lambda_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \lambda_n \end{pmatrix}.$$

Il reste alors à annuler par des opérations symétriques élémentaires les n coefficients diagonaux de D. Pour ce faire on utilise pour $i \in [\![1, n]\!]$, les opérations $(C, L)_{n+i} \longleftarrow (C, L)_{n+i} - \frac{\lambda_i}{2}(C, L)_i$ et au final on a bien :

$$M = \begin{pmatrix} 0_n & I_n \\ I_n & C \end{pmatrix} \approx \begin{pmatrix} 0_n & I_n \\ I_n & D \end{pmatrix} \approx \begin{pmatrix} 0_n & I_n \\ I_n & 0_n \end{pmatrix}$$

On a donc montré que pour (E, q) espace régulier et F sous espace totalement isotrope de dimension n, il existait H espace contenant F de dimension $2n$ tel que (H, q_H) soit régulier avec :

$$Mat(q_H) = \begin{pmatrix} 0_n & {}^tA \\ A & B \end{pmatrix} \approx \begin{pmatrix} 0_n & I_n \\ I_n & 0_n \end{pmatrix}$$

Ainsi (H, q_H) est hyperbolique avec $F \subset H$ et $dim(H) = 2dim(F)$, ce qui finit de montrer le principe de gonflement hyperbolique. □

3.2.3 Isotropie et domaine

Dans la suite, on va s'intéresser au problème de la représentation d'un scalaire $a \in \mathbb{K}^*$ par une forme quadratique régulière q et essayer d'énoncer quelques méthodes pratiques pour aborder ce problème. Le but de cette partie est d'obtenir à l'aide entre autre du principe de gonflement hyperbolique, des méthodes d'études efficaces qui seront utilisées dans un chapitre d'application réservé à la question de la représentation des rationnels par des formes quadratiques rationnelles.

Considérons par exemple la forme quadratique diagonale q définie sur $\mathbb{Q}^2$ par :

$$q : (x, y) \longmapsto x^2 + 5y^2$$

et demandons nous si l'entier 39 est représenté par q (cette question sera solutionnée entièrement par la suite). Si tel était le cas, il existerait $(x_0, y_0) \in (\mathbb{Q}^2)^*$ tel que $q(x_0, y_0) = x_0^2 + 5y_0^2 = 39$ soit $x_0^2 + 5y_0^2 - 39 = 0$ et donc la forme diagonale $\langle 1, 5, -39\rangle \simeq q \perp \langle -39\rangle$ serait isotrope. Ainsi, le fait qu'un scalaire a soit représenté par q implique l'isotropie non pas de q, mais de la forme $q \perp \langle -a\rangle$. On a en fait un résultat plus général, l'implication précédente est une équivalence, ce qui nous fournira un critère efficace pour montrer qu'un scalaire est représenté par une forme quadratique régulière donnée. Dans un premier temps, on va voir qu'une forme quadratique régulière, isotrope représente tous les éléments de $\mathbb{K}^*$ puis, nous exposerons ce principe de représentation.

Définition 3.2.5. *Un scalaire $a \in \mathbb{K}^*$ est dit **représenté** par q lorsqu'il existe $x \in E$ tel que $a = q(x)$. On appelle **domaine** de la forme quadratique noté $\mathcal{D}(q)$ l'ensemble des valeurs non nulles prises par q. La forme q est dite **universelle** lorsque $\mathcal{D}(q) = \mathbb{K}^*$.*

Théorème 3.2.3. *Soit (E, q) un espace quadratique régulier et isotrope. Alors q est universelle.*

Démonstration. Supposons que $dim(E) = 2$. Alors q est une forme quadratique régulière isotrope et est donc hyperbolique. Elle est également équivalente à la forme quadratique q' définie par :

$$q' : \begin{cases} \mathbb{K} \times \mathbb{K} \longrightarrow \mathbb{K} \\ (x, y) \longmapsto xy \end{cases}$$

qui est clairement universelle puisque tout $x \neq 0$ s'écrit $q'(x, 1)$. Supposons $dim(q) > 2$. Alors, q étant isotrope, il existe $x \neq 0$ tel que $q(x) = 0$ et $vect(x)$ est donc un espace de dimension 1 totalement isotrope. D'après le principe de gonflement hyperbolique, on peut trouver un plan hyperbolique P tel que la restriction q_P soit hyperbolique et donc universelle d'après l'étude de la dimension 2 précédente. Ainsi, q_P universelle implique q universelle. □

Théorème 3.2.4. ***Principe de représentation***
Soit (E, q) une espace quadratique régulier et $a \in \mathbb{K}^*$. Alors a est représenté par q si et seulement si $q \perp \langle -a \rangle$ est isotrope.

Démonstration. Soit ϕ la forme quadratique régulière sur $E \times \mathbb{K}$ définie par $\phi = q \perp \langle -a \rangle$:

$$\phi : \begin{cases} E \times \mathbb{K} \longrightarrow \mathbb{K} \\ (x, \lambda) \longmapsto q(x) + \langle -a \rangle(\lambda) = q(x) - a\lambda^2 \end{cases}$$

Si $a \in \mathbb{K}^*$ est représenté par q, il existe un élément $x \neq 0$ tel que $q(x) = a$ et donc $\phi(x, 1) = q(x) - a = 0$ et donc ϕ est isotrope (puisque $(x, 1) \neq 0$). Réciproquement, supposons que ϕ est isotrope. Il existe $(x, \lambda) \neq (0, 0)$ tel que $\phi(x, \lambda) = 0$. Alors,

- Si $\lambda \neq 0$, $q(x) - a\lambda^2 = 0 \Longrightarrow q(x) = a\lambda^2$ et donc $q(\frac{x}{\lambda}) = a$ et a est représenté par q.
- Si $\lambda = 0$, alors nécessairement $x \neq 0$ et donc $\phi(x, \lambda) = \phi(x, 0) = q(x) = 0$ et q est isotrope. Ainsi, (E, q) étant régulier et isotrope, q est universelle et a est bien représenté par q.

□

Un de nos objectifs sera d'être capable de déterminer si un rationnel est représenté ou non par une forme quadratique rationnelle. Nous verrons par le test d'équivalence rationnel un critère pour déterminer si deux formes quadratiques sont équivalentes ce qui nous offrira en particulier un critère pour déterminer si une forme quadratique régulière q de dimension n est hyperbolique (en testant son équivalence avec $n.\langle 1, -1 \rangle$). En petite dimension, nous allons pouvoir aborder le problème de la détermination des scalaires représentés par une certaine forme quadratique q par l'étude du caractère hyperbolique de formes quadratiques auxiliaires de dimension 4. Cette *astuce de la dimension* 4 nous sera particulièrement utile pour étudier les formes quadratiques rationnelles régulières de dimension 2 et 3.

Théorème 3.2.5. *Une forme quadratique régulière de dimension* 4 *de déterminant égal à* 1 *est nécessairement anisotrope ou hyperbolique.*

Démonstration. Si q est isotrope, il existe $x \neq 0$ tel que $vect(x)$ soit totalement isotrope. Alors, par gonflement hyperbolique, il existe un espace hyperbolique H de dimension 2 contenant $vect(x)$. En particulier $q_H \simeq \langle 1, -1\rangle$ et par principe de complétion (corollaire 2.3.1), il existe $(a, b) \in \mathbb{K}^2$ tel que :

$$q \simeq \langle 1, -1\rangle \perp \langle a, b\rangle$$

Alors, q étant régulière, a et b sont non nuls et

$$1 = det(q) = det(\langle 1, -1\rangle)det(\langle a, b\rangle) = -ab$$

ce qui donne $ab = -1$. Par caractérisation des plans hyperboliques, $\langle a, b\rangle$ est hyperbolique et q également.

Si q n'est pas isotrope alors nécessairement, q est anisotrope. Ce qui achève de montrer le théorème. □

Théorème 3.2.6. ***Astuce de la dimension*** 4
Soit (E, q) un espace quadratique régulier de dimension 3, on note δ un déterminant de q. Alors les assertions suivantes sont équivalentes :

1. *q isotrope.*
2. *$q \perp \langle\delta\rangle$ isotrope.*
3. *$q \perp \langle\delta\rangle$ hyperbolique*

Démonstration.

- Montrons $1 \Longrightarrow 2$. Puisque q est isotrope, il existe $x \neq 0$ tel que $q(x) = 0$ et donc pour $(x, 0) \neq 0$ on a :
$$(q \perp \langle\delta\rangle)(x, 0) = q(x) + \delta \times 0^2 = q(x) = 0$$
et donc $q \perp \langle\delta\rangle$ est isotrope.
- Montrons $2 \Longrightarrow 3$. On suppose $q \perp \langle\delta\rangle$ isotrope. Alors $q \perp \langle\delta\rangle$ est de dimension 4 et de déterminant égal à 1. En effet,
$$det(q \perp \langle\delta\rangle) = det(q)det(\langle\delta\rangle) = \delta^2 = 1 \text{ dans } \mathbb{K}^*/(\mathbb{K}^*)^2.$$
Donc $q \perp \langle\delta\rangle$ étant régulière de dimension 4 et de déterminant égal à 1, elle est soit hyperbolique soit anisotrope, étant isotrope elle est hyperbolique.
- Montrons $3 \Longrightarrow 1$. Puisque $q \perp \langle\delta\rangle$ est hyperbolique, elle possède un lagrangien noté F, c'est-à-dire un sous espace vectoriel totalement isotrope de $E \times \mathbb{K}$ de dimension $\frac{4}{2} = 2$. Or, E étant de dimension 3, $E \times \{0\}$ est un sous espace de dimension 3 de $E \times \mathbb{K}$ et par la formule de Grassmann il vient :
$$\begin{aligned} dim(E \times \{0\} + F) = &\quad dim(E \times \{0\}) + dim(F) - dim(E \times \{0\} \cap F) \\ = &\quad 3 + 2 - dim(E \times \{0\} \cap F) \end{aligned}$$
Puisque $dim(E \times \{0\} + F) \leq 4$ car $E \times \{0\} \subset E \times \mathbb{K}$ on a :
$$dim(E \times \{0\} \cap F) \geq 1$$
et $E \times \{0\}$ et F possèdent au moins une droite commune. Il existe donc $x \neq 0$ tel que $(x, 0) \in F$ et F étant totalement isotrope on a :
$$q \perp \langle\delta\rangle(x, 0) = q(x) = 0 \Longrightarrow q \text{ est isotrope.}$$

□

Corollaire 3.2.1. *Soit* $(a_1, a_2) \in (\mathbb{K}^*)^2$ *et* $b \in \mathbb{K}^*$. *Les assertions suivantes sont équivalentes :*

1. b *est représenté par* $\langle a_1, a_2 \rangle$.
2. $\langle a_1, a_2, -b \rangle$ *isotrope.*
3. $\langle a_1, a_2, -b, -a_1 a_2 b \rangle$ *isotrope.*
4. $\langle a_1, a_2, -b, -a_1 a_2 b \rangle$ *hyperbolique*

Démonstration. Ceci découle immédiatement du théorème précédent et du principe de représentation, appliqué à $q = \langle a_1, a_2 \rangle$. □

Nous appliquerons alors les méthodes définies ici, dans un chapitre d'application consacré au problème de la représentation des rationnels. Nous répondrons ainsi à la question énoncée au début de cette partie et montrerons que 39 n'est pas représenté par la forme quadratique $\langle 1, 5 \rangle$. Nous mettrons aussi en avant des résulats intéressants sur la représentation des entiers, comme par exemple le fait que tout entier n s'écrit comme somme de quatre carrés de rationnels.

Chapitre 4

Simplification de Witt et décomposition de Witt d'une forme quadratique

Dans ce court chapitre, d'une très grande importance pour la suite de ce mémoire, nous aurons pour objectif de définir et démontrer de manière matricielle le théorème de simplification de Witt, puis d'appliquer ce résultat pour établir la décomposition de Witt d'une forme quadratique régulière. Nous verrons alors que cette dernière décomposition se révèle d'un grand intérêt puisqu'elle permet de ramener le problème de la classification des formes quadratiques à celui de la classification des formes quadratiques anisotropes. Les résultats obtenus dans ce chapitre seront alors utilisés pour introduire la notion de Witt-équivalence dans le prochain chapitre et permettront également de définir à l'aide de l'opération de somme orthogonale, deux groupes que nous étudierons en détail dans de prochains chapitres : le groupe de Witt $W(\mathbb{K})$ et le groupe de Witt-Grothendieck $\widehat{W}(\mathbb{K})$.

4.1 Simplification de Witt

Théorème 4.1.1. ***Principe de simplification de Witt généralisé.*** *Soit A, B_1 et B_2 trois matrices symétriques respectivement dans $S_n(\mathbb{K})$, $S_p(\mathbb{K})$ et $S_p(\mathbb{K})$. Alors :*

$$\begin{pmatrix} A & 0 \\ 0 & B_1 \end{pmatrix} \approx \begin{pmatrix} A & 0 \\ 0 & B_2 \end{pmatrix} \Longrightarrow B_1 \approx B_2$$

De part l'écriture matricielle de la somme directe orthogonale de deux formes quadratiques, pour q, ϕ et ψ trois formes quadratiques, le théorème ci-dessus se traduit en termes de formes quadratiques par le résultat fondamental suivant :

$$q \perp \phi \simeq q \perp \psi \Longrightarrow \phi \simeq \psi$$

Afin de démontrer ce résultat nous aurons besoins d'utiliser deux lemmes intermédiaires.

Lemme 4.1.1. *Soit $A, B \in S_n(\mathbb{K}) \cap GL_n(\mathbb{K})$ et $\mu \in \mathbb{K}^*$. ALors :*

$$A_1 = \begin{pmatrix} A & 0 \\ 0 & \mu \end{pmatrix} \approx B_1 = \begin{pmatrix} B & 0 \\ 0 & \mu \end{pmatrix} \Longrightarrow A \approx B$$

Démonstration. Puisque $A_1 \approx B_1$, il existe une matrice $P \in GL_{n+1}(\mathbb{K})$ notée sous la forme d'une matrice par blocs $P = \begin{pmatrix} Q & C \\ L & \alpha \end{pmatrix}$ telle que $PA_1\ {}^tP = B_1$ où $Q \in \mathcal{M}_n(\mathbb{K})$, $L \in \mathcal{M}_{1,n}(\mathbb{K})$ et $C \in \mathcal{M}_{n,1}(\mathbb{K})$. L'égalité matricielle $PA_1\ {}^tP = B_1$ s'écrit en termes de matrices blocs sous la forme :

$$\begin{pmatrix} Q & C \\ L & \alpha \end{pmatrix} \begin{pmatrix} A & 0 \\ 0 & \mu \end{pmatrix} \begin{pmatrix} {}^tQ & {}^tL \\ {}^tC & \alpha \end{pmatrix} = \begin{pmatrix} QA\ {}^tQ + \mu C\ {}^tC & QA\ {}^tL + \alpha\mu C \\ LA\ {}^tQ + \alpha\mu\ {}^tC & LA\ {}^tL + \alpha^2\mu \end{pmatrix}$$
$$= \begin{pmatrix} B & 0 \\ 0 & \mu \end{pmatrix}$$

Par identification des blocs, il vient :

1. $QA\ {}^tQ + \mu C\ {}^tC = B$
2. $LA\ {}^tQ + \alpha\mu\ {}^tC = 0$
3. $QA\ {}^tL + \alpha\mu C = 0$
4. $LA\ {}^tL + \alpha^2\mu = \mu$

Ce qui nous donne en particulier :

$QA\ {}^tQ = B - \mu C\ {}^tC$, $(CL)A\ {}^tQ = -\alpha\mu C\ {}^tC$ et $(CL)A\ {}^t(CL) = \mu(1-\alpha^2)C\ {}^tC$

On cherche à montrer qu'il existe une matrice inversible P_2 telle que

$$P_2A\ {}^tP_2 = B.$$

Pour ce faire, on va montrer qu'il existe au moins deux $\lambda \in \mathbb{K}$, (donc nécessairement un non nul) tels que :

$$(\lambda Q + CL)A\ {}^t(\lambda Q + CL) = \lambda^2 B$$

On cherche ainsi à résoudre l'équation polynomiale de degré 2 en λ donnée ci dessus. En développant, on a :

$$(\lambda Q + CL)A\ {}^t(\lambda Q + CL) = \lambda^2(QA\ {}^tQ) + 2\lambda QA\ {}^t(CL) + (CL)A\ {}^t(CL) =$$
$$\lambda^2(B - \mu C\ {}^tC) + 2\lambda(-\alpha\mu C\ {}^tC) + \mu(1-\alpha^2)C\ {}^tC$$

et donc :

$$(\lambda Q + CL)A\ {}^t(\lambda Q + CL) = \lambda^2 B \Longleftrightarrow C\ {}^tC(-\mu\lambda^2 - 2\alpha\mu\lambda + \mu(1-\alpha^2)) = 0$$

Si $C\ {}^tC = 0$, on aura l'égalité $(\lambda Q + CL)A\ {}^t(\lambda Q + CL) = \lambda^2 B$ pour tout $\lambda \in \mathbb{K}$, sinon puisque $\mathbb{K}$ est un corps, par intégrité, $\mu\lambda^2 + 2\alpha\mu\lambda + \mu(\alpha^2 - 1) = 0$. Posons $P(X) = \mu X^2 + 2\alpha\mu X + \mu(\alpha^2 - 1) \in \mathbb{K}[X]$. Le discriminant de ce polynôme est donné par : $\Delta = (2\alpha\mu)^2 - 4\mu\mu(\alpha^2 - 1) = 4\mu^2 = (2\mu)^2$ et est un carré non nul de $\mathbb{K}$. P admet donc deux racines distinctes dans $\mathbb{K}$ que sont :

$$\lambda_1 = \mu(-1 - \alpha) \text{ et } \lambda_2 = \mu(1 - \alpha)$$

avec $\mu(-1-\alpha) \neq \mu(1-\alpha)$ car sinon $-1 = 1$ dans $\mathbb{K}$, absurde car $car(\mathbb{K}) \neq 2$. D'où il existe au moins deux $\lambda \in \mathbb{K}$ tels que $(\lambda Q + CL)A\ {}^t(\lambda Q + CL) = \lambda^2 B$ et donc nécessairement un λ non nul pour lequel :

$$(Q+\lambda^{-1}CL)A\ {}^t(Q+\lambda^{-1}CL)=B$$

Puisque $A,B\in GL_n(\mathbb{K})$, on a $det(A)\neq 0$ et $det(B)\neq 0$ et donc $(Q+\lambda^{-1}CL)$ est inversible ce qui montre que A et B sont congruentes. □

Lemme 4.1.2. *Soit $A,B\in\mathcal{M}_n(\mathbb{K})$ et $p\in\mathbb{N}^*$. Alors :*

$$\begin{pmatrix}A & 0\\ 0 & 0_p\end{pmatrix}\approx\begin{pmatrix}B & 0\\ 0 & 0_p\end{pmatrix}\Longrightarrow A\approx B$$

Démonstration. Soit $A,B\in\mathcal{M}_n(\mathbb{K})$ et on suppose congruentes les matrices $A_1=\begin{pmatrix}A & 0\\ 0 & 0\end{pmatrix}$ et $B_1=\begin{pmatrix}B & 0\\ 0 & 0\end{pmatrix}$ de $\mathcal{M}_{n+1}(\mathbb{K})$. Notre but est de montrer que A et B sont également congruentes. Il existe alors $P\in GL_{n+1}(\mathbb{K})$ écrite sous la forme de matrice par blocs : $P=\begin{pmatrix}Q & C\\ L & \alpha\end{pmatrix}$, telle que $PA_1\ {}^tP=B_1$ avec $Q\in\mathcal{M}_n(\mathbb{K})$, $L\in\mathcal{M}_{1,n}(\mathbb{K})$, $C\in\mathcal{M}_{n,1}(\mathbb{K})$ et $\alpha\in\mathbb{K}$. Si on suppose Q inversible, via la relation $PA_1\ {}^tP=B_1$, on a :

$$\begin{pmatrix}Q & C\\ L & \alpha\end{pmatrix}\begin{pmatrix}A & 0\\ 0 & 0\end{pmatrix}\begin{pmatrix}{}^tQ & {}^tL\\ {}^tC & \alpha\end{pmatrix}=\begin{pmatrix}QA\ {}^tQ & QA\ {}^tL\\ LA\ {}^tQ & LA\ {}^tL\end{pmatrix}=\begin{pmatrix}B & 0\\ 0 & 0\end{pmatrix}$$

soit par identification des différents blocs $QA\ {}^tQ=B$ et A et B sont bien congruentes (car Q est inversible).

Dans la suite on suppose A_1 et B_1 congruentes avec Q non inversible. Puisque Q n'est pas inversible, elle est de rang inférieur ou égal à $n-1$. Par l'absurde on suppose que $rg(Q)\neq n-1$. Ainsi, l'espace vectoriel engendré par les vecteurs colonnes de la matrice Q est de dimension inférieure ou égale à $n-2$ et sans perte de généralité on peut supposer que les colonnes 1 et 2 notées Q_1 et Q_2 sont combinaisons linéaires des autres, c'est à dire $Q_1,Q_2\in vect(Q_3,\cdots,Q_n)$. Ainsi il existe des scalaires non tous nuls $(\lambda_i)_{3\leq i\leq n}$ et $(\lambda'_i)_{3\leq i\leq n}$ tels que :

$$Q_1=\lambda_3Q_3+\cdots+\lambda_nQ_n \text{ et } Q_2=\lambda'_3Q_3+\cdots+\lambda'_nQ_n$$

En opérant sur les colonnes de Q via les opérations suivantes :

$$Q_1\longleftarrow Q_1-\lambda_3Q_3+\cdots+\lambda_nQ_n \text{ et } Q_2\longleftarrow Q_2-\lambda'_3Q_3+\cdots+\lambda'_nQ_n$$

on va annuler les deux premières colonnes de la matrice Q. Or ces opérations correspondent à des multiplication à droite de Q, par des matrices M_1 et M_2 d'opérations élémentaires qui sont inversibles. En multipliant alors à droite de P par les matrices inversibles $\begin{pmatrix}M_1 & 0\\ 0 & 1\end{pmatrix}$ et $\begin{pmatrix}M_2 & 0\\ 0 & 1\end{pmatrix}$ on obtient une matrice P' dont les deux premières colonnes sont nulles hormis éventuellement le dernier coefficient de chaque colonne. Ces deux vecteurs colonnes sont donc nécessairement liés, ce qui impose que P' n'est pas inversible et donc de rang différent de $n+1=rg(P)$. Ceci est absurde puisque l'on ne change pas le rang d'une matrice en multipliant à droite par des matrices inversibles. D'où nécessairement si Q n'est pas inversible, $rg(Q)=n-1$.

On définit dans la suite l'ensemble :

$$G=\{\begin{pmatrix}M & C\\ 0 & \lambda\end{pmatrix},M\in GL_n(\mathbb{K}),C\in\mathcal{M}_{n,1}(\mathbb{K}) \text{ et } \lambda\in\mathbb{K}^*\}$$

G a naturellement une structure de groupe pour le produit matriciel et l'on va faire agir $G\times G$ sur $GL_{n+1}(\mathbb{K})$ via :

$$\begin{array}{rcl}(G\times G)\times GL_{n+1}(\mathbb{K}) & \longrightarrow & GL_{n+1}(\mathbb{K})\\ ((N_1,N_2),M) & \longmapsto & N_1MN_2^{-1}\end{array}$$

Notre objectif est alors de montrer que la matrice P est dans l'orbite d'une matrice de la forme : $\begin{pmatrix}1 & \cdots & 0 & 0 & 0\\ \vdots & \ddots & \vdots & \vdots & \vdots\\ 0 & \cdots & 1 & \vdots & \vdots\\ 0 & \cdots & 0 & 0 & 1\\ 0 & \cdots & 0 & 1 & \beta\end{pmatrix}$. On cherche alors $(N_1,N_2)\in G\times G$ tel que :

$$N_1PN_2^{-1}=\begin{pmatrix}1 & \cdots & 0 & 0 & 0\\ \vdots & \ddots & \vdots & \vdots & \vdots\\ 0 & \cdots & 1 & \vdots & \vdots\\ 0 & \cdots & 0 & 0 & 1\\ 0 & \cdots & 0 & 1 & \beta\end{pmatrix}$$

Comme Q est de rang $n-1$, elle est équivalente à la matrice $J_{n-1}=\begin{pmatrix}I_{n-1} & 0\\ 0 & 0\end{pmatrix}$ et donc il existe $P_1,P_2\in GL_n(\mathbb{K})$ telles que $P_1QP_2^{-1}=J_{n-1}$. On a ainsi :

$$\begin{pmatrix}P_1 & 0\\ 0 & 1\end{pmatrix}\begin{pmatrix}Q & C\\ L & \alpha\end{pmatrix}\begin{pmatrix}P_2^{-1} & 0\\ 0 & 1\end{pmatrix}=\begin{pmatrix}P_1QP_2^{-1} & P_1C\\ LP_2^{-1} & \alpha\end{pmatrix}=\begin{pmatrix}1 & \cdots & 0 & 0 & \\ \vdots & \ddots & \vdots & \vdots & P_1C\\ 0 & \cdots & 1 & \vdots & \\ 0 & \cdots & 0 & 0 & \\ & LP_2^{-1} & & & \alpha\end{pmatrix}$$

où $LP_2^{-1}\in\mathcal{M}_{1,n}(\mathbb{K})$ est une matrice ligne et $P_1C\in\mathcal{M}_{n,1}(\mathbb{K})$ est une matrice colonne. On note alors $LP_2^{-1}=(a_{n+1,1},\ldots,a_{n+1,n})$ et $P_1C=\begin{pmatrix}a_{1,n+1}\\ a_{2,n+1}\\ \vdots\\ a_{n,n+1}\end{pmatrix}$. Soit

$$\begin{pmatrix}1 & \cdots & 0 & 0 & \\ \vdots & \ddots & \vdots & \vdots & P_1C\\ 0 & \cdots & 1 & \vdots & \\ 0 & \cdots & 0 & 0 & \\ & LP_2^{-1} & & & \alpha\end{pmatrix}=\begin{pmatrix}1 & \cdots & 0 & 0 & a_{1,n+1}\\ \vdots & \ddots & \vdots & \vdots & \vdots\\ 0 & \cdots & 1 & \vdots & \vdots\\ 0 & \cdots & 0 & 0 & a_{n,n+1}\\ a_{n+1,1} & \cdots & \cdots & a_{n+1,n} & \alpha\end{pmatrix}$$

Puisque $\begin{pmatrix}P_1 & 0\\ 0 & 1\end{pmatrix}$ et $\begin{pmatrix}P_2^{-1} & 0\\ 0 & 1\end{pmatrix}$ sont deux éléments de G, il reste à opérer à gauche et à droite par des éléments de G pour annuler les $n-1$ premiers coefficients de LP_2^{-1} et annuler les $n-1$ premiers coefficients de P_1C, mais aussi obtenir un 1 en position $(n+1,n)$ et $(n,n+1)$. On remarque que les coefficients $a_{n+1,n}$ et $a_{n,n+1}$ sont non nuls car sinon la n-ème colonne serait nulle tout comme la n-ème ligne et la matrice ci-dessus serait non inversible et donc P qui lui est équivalente serait non inversible également, absurde. Puisque $a_{n+1,n}\neq 0$

et $a_{n,n+1} \neq 0$, en multipliant à droite par les matrices $I_{n+1} - \dfrac{a_{n+1,i}}{a_{n+1,n}} E_{n,i} \in G$ pour $i \in [\![1, n-1]\!]$, on annule les $n-1$ premiers coefficients de la dernière ligne. Enfin, en multipliant à droite par la matrice $\begin{pmatrix} 1 & \cdots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & 1/a_{n+1,n} & \vdots \\ 0 & \cdots & 0 & 1 \end{pmatrix} \in G$ on obtient un 1 à la place du coefficient d'indice $(n+1, n)$. De même en multipliant à gauche par $I_{n+1} - \dfrac{a_{i,n+1}}{a_{n,n+1}} E_{i,n} \in G$ pour $i \in [\![1, n-1]\!]$, on annule les $n-1$ premiers coefficients de la dernière colonne, et en multipliant à gauche par la matrice suivante $\begin{pmatrix} 1 & \cdots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & 1/a_{n,n+1} & \vdots \\ 0 & \cdots & 0 & 1 \end{pmatrix} \in G$ on obtient un 1 à la place du coefficient d'indice $(n, n+1)$. Les multiplications à gauche et à droite précédentes étant des multiplications par des éléments du groupe G, il existe bien $N_1, N_2 \in G$ telles que :

$$N_1 P N_2^{-1} = \begin{pmatrix} 1 & \cdots & 0 & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & \cdots & 1 & \vdots & \vdots \\ 0 & \cdots & 0 & 0 & 1 \\ 0 & \cdots & 0 & 1 & \beta \end{pmatrix} = J$$

Nous allons maintenant en déduire que les matrices A et B sont congruentes. Supposons que $P = \begin{pmatrix} 1 & \cdots & 0 & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & \cdots & 1 & \vdots & \vdots \\ 0 & \cdots & 0 & 0 & 1 \\ 0 & \cdots & 0 & 1 & \beta \end{pmatrix}$ telle que $B_1 = P A_1 \ {}^t P$ et montrons que nécessairement $A = B$. Alors, par identification des blocs, il vient :

1. $J_{n-1} A J_{n-1} = B$
2. $(0, 0, \cdots, 1) A J_{n-1} = 0_{1,n}$
3. $J_{n-1} A \ {}^t(0, 0, \cdots, 1) = 0_{n,1}$
4. $(0, 0, \cdots, 1) A \ {}^t(0, 0, \cdots, 1) = 0$

En notant $A = (a_{i,j})_{1 \leq i,j \leq n}$, on a :

$$(0, 0, \cdots, 1) A J_{n-1} = (a_{n,1}, a_{n,2}, \cdots, a_{n,n-1}, 0)$$

et donc $a_{n,i} = 0$, $\forall i \in [\![1, n-1]\!]$. De même :

$$J_{n-1} A \ {}^t(0, 0, \cdots, 1) = \begin{pmatrix} a_{1,n} \\ \vdots \\ a_{n-1,n} \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 0 \end{pmatrix} \text{ et } a_{i,n} = 0, \ \forall i \in [\![1, n-1]\!].$$

Enfin la relation $(0,0,\cdots,1)A\ {}^t(0,0,\cdots,1)=0$ donne $a_{n,n}=0$.
Finalement la n-ème colonne de A est nulle, tout comme la n-ème ligne et A s'écrit $\begin{pmatrix} A' & 0_{n,1} \\ 0_{1,n} & 0 \end{pmatrix}$. Ainsi :

$$B_1 = PA_1\ {}^tP = \begin{pmatrix} J_{n-1}\begin{pmatrix} A' & 0_{n,1} \\ 0_{1,n} & 0 \end{pmatrix} J_{n-1} & 0_{n,1} \\ 0_{1,n} & 0 \end{pmatrix}$$

Comme $J_{n-1}\begin{pmatrix} A' & 0_{n,1} \\ 0_{1,n} & 0 \end{pmatrix} J_{n-1} = \begin{pmatrix} A' & 0_{n,1} \\ 0_{1,n} & 0 \end{pmatrix} = A$, il vient alors :

$$B_1 = PA_1\ {}^tP = \begin{pmatrix} A & 0_{n,1} \\ 0_{1,n} & 0 \end{pmatrix} = A_1 \Longrightarrow A = B$$

Supposons ensuite P quelconque. On a vu qu'il existe $N_1, N_2 \in G$ telles que :

$$N_1PN_2^{-1} = \begin{pmatrix} 1 & \cdots & 0 & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & \cdots & 1 & \vdots & \vdots \\ 0 & \cdots & 0 & 0 & 1 \\ 0 & \cdots & 0 & 1 & \beta \end{pmatrix} \text{ et donc } P = N_1^{-1}\begin{pmatrix} 1 & \cdots & 0 & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & \cdots & 1 & \vdots & \vdots \\ 0 & \cdots & 0 & 0 & 1 \\ 0 & \cdots & 0 & 1 & \beta \end{pmatrix} N_2.$$

$N_1^{-1} \in G$ s'écrit $\begin{pmatrix} Q_1 & C_1 \\ 0 & \alpha_1 \end{pmatrix}$ et $N_2 \in G$ s'écrit $\begin{pmatrix} Q_2 & C_2 \\ 0 & \alpha_2 \end{pmatrix}$ où $Q_1, Q_2 \in GL_n(\mathbb{K})$ et $\alpha_1, \alpha_2 \neq 0$. La relation de congruence $B_1 = PA_1\ {}^tP$ nous donne :

$$B_1 = \begin{pmatrix} Q_1 & C_1 \\ 0 & \alpha_1 \end{pmatrix} J \begin{pmatrix} Q_2 & C_2 \\ 0 & \alpha_2 \end{pmatrix}\begin{pmatrix} A & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} {}^tQ_2 & 0 \\ {}^tC_2 & \alpha_2 \end{pmatrix} J \begin{pmatrix} {}^tQ_1 & 0 \\ {}^tC_1 & \alpha_1 \end{pmatrix}$$

soit

$$B_1 = \begin{pmatrix} Q_1 & C_1 \\ 0 & \alpha_1 \end{pmatrix} J \begin{pmatrix} Q_2A\ {}^tQ_2 & 0 \\ 0 & 0 \end{pmatrix} J \begin{pmatrix} {}^tQ_1 & 0 \\ {}^tC_1 & \alpha_1 \end{pmatrix}$$

Puisque $\begin{pmatrix} Q_1 & C_1 \\ 0 & \alpha_1 \end{pmatrix} \in G$ est inversible, sa transposée également et en notant $\begin{pmatrix} Q_1' & C_1' \\ 0 & \alpha_1^{-1} \end{pmatrix}$ son inverse, il vient :

$$\begin{pmatrix} Q_1' & C_1' \\ 0 & \alpha_1^{-1} \end{pmatrix} B_1 \begin{pmatrix} {}^tQ_1' & 0 \\ {}^tC_1' & \alpha_1^{-1} \end{pmatrix} = \begin{pmatrix} Q_1'B\ {}^tQ_1' & 0 \\ 0 & 0 \end{pmatrix} = J\begin{pmatrix} Q_2A\ {}^tQ_2 & 0 \\ 0 & 0 \end{pmatrix} J$$

et d'après le résultat précédent $Q_1'B\ {}^tQ_1' = Q_2A\ {}^tQ_2$. Comme Q_2 et Q_1' sont inversibles $(Q_1'^{-1}Q_2)A\ {}^t(Q_1'^{-1}Q_2) = B$ et $A \approx B$. Ainsi,

$$P\begin{pmatrix} A & 0 \\ 0 & 0 \end{pmatrix}\ {}^tP = \begin{pmatrix} B & 0 \\ 0 & 0 \end{pmatrix} \Longrightarrow A \approx B$$

et par un raisonnement par récurrence, il vient $\forall p \in \mathbb{N}^*$:

$$\begin{pmatrix} A & 0 \\ 0 & 0_p \end{pmatrix} \approx \begin{pmatrix} B & 0 \\ 0 & 0_p \end{pmatrix} \Longrightarrow A \approx B$$

où 0_p désigne la matrice nulle de taille $p \times p$ □

Revenons à la démonstration du théorème.

Démonstration. On considère A, B, C trois matrices symétriques respectivement de $S_n(\mathbb{K})$, $S_n(\mathbb{K})$ et $S_p(\mathbb{K})$ telles que : $\begin{pmatrix} A & 0 \\ 0 & C \end{pmatrix} \approx \begin{pmatrix} B & 0 \\ 0 & C \end{pmatrix}$. On souhaite montrer que $A \approx B$. On va d'abord montrer le résultat dans le cas où les matrices A, B et C sont inversibles et on va ensuite voir que le cas général s'y ramène. D'abord puisque $\begin{pmatrix} A & 0 \\ 0 & C \end{pmatrix} \approx \begin{pmatrix} B & 0 \\ 0 & C \end{pmatrix}$, les matrices ont le même rang et donc :

$$rg \begin{pmatrix} A & 0 \\ 0 & C \end{pmatrix} = rg(A) + rg(C) = rg \begin{pmatrix} B & 0 \\ 0 & C \end{pmatrix} = rg(B) + rg(C)$$

Ceci impose $rg(A) = rg(B)$. Comme les matrices A, B, C sont symétriques et inversibles, elles sont congruentes respectivement à des matrices diagonales :

$$\begin{pmatrix} \lambda_1 & \cdots & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & \lambda_n \end{pmatrix}, \begin{pmatrix} \lambda'_1 & \cdots & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & \lambda'_n \end{pmatrix} \text{ et } \begin{pmatrix} \mu_1 & \cdots & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & \mu_n \end{pmatrix}$$

où pour tout i, $\lambda_i, \lambda'_i, \mu_i \neq 0$ (d'après le corollaire 1.2.1). D'où il existe des matrices $P_1, P_2 \in GL_n(\mathbb{K})$ telles que :

$$P_1 A \, {}^t P_1 = \begin{pmatrix} \lambda_1 & \cdots & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & \lambda_n \end{pmatrix} \text{ et } P_2 C \, {}^t P_2 = \begin{pmatrix} \mu_1 & \cdots & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & \mu_n \end{pmatrix}.$$

Alors :

$$\begin{pmatrix} P_1 & 0 \\ 0 & P_2 \end{pmatrix} \begin{pmatrix} A & 0 \\ 0 & C \end{pmatrix} \begin{pmatrix} {}^t P_1 & 0 \\ 0 & P_2^t \end{pmatrix} = \begin{pmatrix} P_1 A \, {}^t P_1 & 0 \\ 0 & P_2 C \, {}^t P_2 \end{pmatrix}$$

et donc

$$\begin{pmatrix} A & 0 \\ 0 & C \end{pmatrix} \approx \begin{pmatrix} \lambda_1 & \cdots & 0 & & & \\ 0 & \ddots & 0 & & 0 & \\ 0 & 0 & \lambda_n & & & \\ & & & \mu_1 & \cdots & 0 \\ & 0 & & 0 & \ddots & 0 \\ & & & 0 & 0 & \mu_n \end{pmatrix}$$

De même

$$\begin{pmatrix} B & 0 \\ 0 & C \end{pmatrix} \approx \begin{pmatrix} \lambda'_1 & \cdots & 0 & & & \\ 0 & \ddots & 0 & & 0 & \\ 0 & 0 & \lambda'_n & & & \\ & & & \mu_1 & \cdots & 0 \\ & 0 & & 0 & \ddots & 0 \\ & & & 0 & 0 & \mu_n \end{pmatrix}$$

et d'après lemme 4.1.1, en raisonnant par récurrence, il vient :

$$A \approx \begin{pmatrix} \lambda_1 & \cdots & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & \lambda_n \end{pmatrix} \approx \begin{pmatrix} \lambda'_1 & \cdots & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & \lambda'_n \end{pmatrix} \approx B$$

Démontrons le résultat dans le cas général. A, B ont le même rang $r \leq n$ et C est de rang $l \leq p$. Puisque A est symétrique de rang r, $A \approx \begin{pmatrix} A_1 & 0 \\ 0 & 0 \end{pmatrix}$ où $A_1 \in GL_r(\mathbb{K})$ et $B \approx \begin{pmatrix} B_1 & 0 \\ 0 & 0 \end{pmatrix}$ où $B_1 \in GL_r(\mathbb{K})$ (toujours d'après le corollaire 1.2.1). De même $C \approx \begin{pmatrix} C_1 & 0 \\ 0 & 0 \end{pmatrix}$ où $C_1 \in GL_l(\mathbb{K})$. Ainsi :

$$\begin{pmatrix} A & 0 \\ 0 & C \end{pmatrix} \approx \begin{pmatrix} \boxed{\begin{matrix} A_1 & 0 \\ 0 & 0 \end{matrix}} & 0 \\ 0 & \boxed{\begin{matrix} C_1 & 0 \\ 0 & 0 \end{matrix}} \end{pmatrix} \approx \begin{pmatrix} \boxed{\begin{matrix} A_1 & 0 \\ 0 & C_1 \end{matrix}} & 0 \\ 0 & \boxed{0} \end{pmatrix}$$

et

$$\begin{pmatrix} B & 0 \\ 0 & C \end{pmatrix} \approx \begin{pmatrix} \boxed{\begin{matrix} B_1 & 0 \\ 0 & 0 \end{matrix}} & 0 \\ 0 & \boxed{\begin{matrix} C_1 & 0 \\ 0 & 0 \end{matrix}} \end{pmatrix} \approx \begin{pmatrix} \boxed{\begin{matrix} B_1 & 0 \\ 0 & C_1 \end{matrix}} & 0 \\ 0 & \boxed{0} \end{pmatrix}$$

Or

$$\begin{pmatrix} A & 0 \\ 0 & C \end{pmatrix} \approx \begin{pmatrix} B & 0 \\ 0 & C \end{pmatrix} \Longrightarrow \begin{pmatrix} \boxed{\begin{matrix} A_1 & 0 \\ 0 & C_1 \end{matrix}} & 0 \\ 0 & \boxed{0} \end{pmatrix} \approx \begin{pmatrix} \boxed{\begin{matrix} B_1 & 0 \\ 0 & C_1 \end{matrix}} & 0 \\ 0 & \boxed{0} \end{pmatrix}$$

D'après le lemme 4.1.2, $\begin{pmatrix} A_1 & 0 \\ 0 & C_1 \end{pmatrix} \approx \begin{pmatrix} B_1 & 0 \\ 0 & C_1 \end{pmatrix}$ et les matrices A_1, B_1 et C_1 étant inversibles, d'après ce qu'on a vu précédemment il vient $A_1 \approx B_1$ et donc naturellement $A = \begin{pmatrix} A_1 & 0 \\ 0 & 0 \end{pmatrix} \approx \begin{pmatrix} B_1 & 0 \\ 0 & 0 \end{pmatrix} = B$, ce qui achève de montrer le théorème. □

Nous utiliserons très souvent la caractérisation suivante du lemme de simplification de Witt :

Corollaire 4.1.1. *Soit $(a_1, \ldots, a_n) \in \mathbb{K}^n$ et deux p-uplets $(b_1, \ldots, b_p) \in \mathbb{K}^p$ et $(c_1, \ldots, c_p) \in \mathbb{K}^p$. Alors :*

$$\langle a_1, \ldots, a_n, b_1, \ldots, b_p \rangle \simeq \langle a_1, \ldots, a_n, c_1, \ldots, c_p \rangle \Longrightarrow \langle b_1, \ldots, b_p \rangle \simeq \langle c_1, \ldots, c_p \rangle.$$

On va désormais s'appuyer sur cette simplification de Witt pour montrer que toute forme quadratique régulière est équivalente à la somme orthogonale d'une forme hyperbolique (facilement caractérisable et bien comprise comme on l'a vu au chapitre précédent) et d'une forme quadratique anisotrope, dont la classification est plus complexe. On montrera de même que cette décomposition est essentiellement unique dans un sens que l'on explicitera.

4.1.1 Décomposition de Witt d'une forme quadratique régulière

Commençons par énoncer un lemme dont le résultat nous sera utile pour la démonstration du théorème de décomposition.

Lemme 4.1.3. *Soit (E, q) un espace quadratique régulier admettant un sous-espace totalement isotrope maximal de dimension p. Alors il existe une forme quadratique anisotrope q_1 telle que :*

$$q \simeq p.\langle 1, -1\rangle \perp q_1$$

Démonstration. On note F un sous espace totalement isotrope maximal de dimension p. Par le principe de gonflement hyperbolique, il existe un sous-espace H contenant F et de dimension $2p$ tel que q_H soit hyperbolique et donc équivalente à $p.\langle 1, -1\rangle$. Alors, q_H étant hyperbolique, elle est régulière et H est un sous-espace régulier pour lequel $H \overset{\perp}{\oplus} H^{\perp} = E$. D'après la proposition 2.2.3 au chapitre 2, on a :

$$q \simeq q_H \perp q_{H^{\perp}} \simeq p.\langle 1, -1\rangle \perp q_{H^{\perp}}.$$

Il reste à montrer que $q_{H^{\perp}}$ est anisotrope. Supposons par l'absurde que $q_{H^{\perp}}$ soit isotrope, alors $H^{\perp}$ admettait un vecteur isotrope non nul x, qui n'appartiendrait pas à H et donc pas non plus à F. L'espace $vect(x) \oplus F$ contiendrait alors strictement F et serait lui aussi totalement isotrope, ce qui est en contradiction avec F sous espace totalement isotrope maximal. D'où, $q_{H^{\perp}}$ anisotrope ainsi que la décomposition attendue. □

Nous pouvons désormais énoncer le théorème de décomposition de Witt :

Théorème 4.1.2. ***Décomposition de Witt d'une forme quadratique régulière***
Soit (E, q) un espace quadratique régulier. Il existe alors un entier naturel p et une forme quadratique anisotrope q_a tels que :

$$q \simeq p.\langle 1, -1\rangle \perp q_a$$

Dans l'écriture ci-dessus p est déterminé de manière unique et q_a de manière unique à équivalence près.

Démonstration. Supposons q anisotrope, alors prenant $p = 0$ et $q_a = q$, on a bien la décomposition recherchée. Supposons désormais q isotrope, alors l'espace (E, q) admet au moins un sous-espace totalement isotrope maximal que l'on note F et on note p sa dimension. Alors d'après le lemme précédent $q \simeq p.\langle 1, -1\rangle \perp q_a$ pour une certaine forme quadratique anisotrope q_a. Montrons maintenant que les sous-espaces totalement-isotropes maximaux sont nécessairement de même dimension. Si ce n'était pas le cas, il existerait deux entiers $p_1 \neq p_2$ et q_1, q_2 deux formes quadratiques régulières anisotropes telles que :

$$q \simeq p_1.\langle 1, -1\rangle \perp q_1 \simeq p_2.\langle 1, -1\rangle \perp q_2$$

On suppose $p_1 < p_2$, alors on a :

$$p_2\langle 1, -1\rangle \perp q_2 \simeq (p_2 - p_1).\langle 1, -1\rangle \perp p_1.\langle 1, -1\rangle \perp q_2$$

et par simplification de Witt :

$$(p_2 - p_1).\langle 1, -1\rangle \perp p_1.\langle 1, -1\rangle \perp q_2 \simeq p_1.\langle 1, -1\rangle \perp q_1 \Longrightarrow (p_2 - p_1).\langle 1, -1\rangle \perp q_2 \simeq q_1$$

Or $p_2 - p_1 > 0 \Longrightarrow (p_2 - p_1).\langle 1, -1\rangle \perp q_2$ a une partie hyperbolique non nulle et est isotrope. L'équivalence avec q_1 anisotrope est alors absurde. Soit donc nécessairement $p_1 = p_2$ et tous les sous-espaces totalement isotropes maximaux sont de même dimension que l'on note p et ainsi p est uniquement déterminé. Alors pour deux décompositions comme ci-dessus, $p_1 = p_2$ et donc par simplification de Witt :

$$q \simeq p_1.\langle 1, -1\rangle \perp q_1 \simeq p_1.\langle 1, -1\rangle \perp q_2 \Longrightarrow q_1 \simeq q_2$$

□

On a également montré que tout sous-espace vectoriel totalement isotrope maximal était de dimension p où p est l'unique entier tel que $q \simeq p.\langle 1, -1\rangle \perp q_a$ pour q_a anisotrope, unique à équivalence près.

Définition 4.1.1. *Avec les notations du théorème, l'entier p qui est la dimension commune de tout sous-espace totalement isotrope maximal est appelé* ***l'indice*** *de q et noté $\nu(q)$. On appelle* ***partie anisotrope*** *de q, toute forme quadratique équivalente à q_a.*

Appliquons alors le théorème de décomposition de Witt à l'étude des formes quadratiques réelles et définissons ainsi la notion de signature d'une forme quadratique réelle régulière.

Proposition 4.1.1. *Soit q une forme quadratique réelle régulière. Il existe un unique couple d'entiers (r, s) tel que $q \simeq r.\langle 1\rangle \perp s.\langle -1\rangle$. Ce couple est appelé* ***la signature*** *de la forme quadratique régulière q.*

Démonstration. Soit q une forme quadratique réelle régulière de dimension n. Alors, par diagonalisation il existe r réels strictement positifs $(a_1, \ldots, a_r)$ et s réels strictement négatifs $(b_1, \ldots, b_s)$ tels que :

$$r + s = n \text{ et } q \simeq \langle a_1, \ldots, a_r, b_1, \ldots, b_s\rangle$$

Puisque $\mathbb{R}^*/(\mathbb{R}^*)^2$ est composé de deux classes, celle des réels strictement positifs et celle des réels strictement négatifs on a : $q \simeq \langle 1, \ldots, 1, -1, \ldots, -1\rangle$, où 1 apparait r fois et -1 apparaît s fois. Montrons l'unicité du couple (r, s). Supposons que $q \simeq r_1.\langle 1\rangle \perp s_1.\langle -1\rangle$ et $q \simeq r_2.\langle 1\rangle \perp s_2.\langle -1\rangle$.

- Supposons $r_1 \leq s_1$ et $s_2 \leq r_2$ alors $q \simeq r_1.\langle 1, -1\rangle \perp (s_1 - r_1).\langle -1\rangle$ et de même $q \simeq s_2.\langle 1, -1\rangle \perp (r_2 - s_2).\langle 1\rangle$. Les formes quadratiques $(s_1 - r_1).\langle -1\rangle$ et $(r_2 - s_2).\langle 1\rangle$ étant clairement anisotropes et les formes quadratiques $r_1.\langle 1, -1\rangle$ et $s_2.\langle 1, -1\rangle$ étant clairement hyperboliques, on a alors par unicité de la décomposition de Witt $(s_1 - r_1).\langle -1\rangle \simeq (r_2 - s_2).\langle 1\rangle$, absurde (elles n'ont par exemple, clairement pas le même domaine).
- Supposons $r_1 \leq s_1$ et $r_2 \leq r_2$ alors $q \simeq r_1.\langle 1, -1\rangle \perp (s_1 - r_1).\langle -1\rangle$ et de même $q \simeq r_2.\langle 1, -1\rangle \perp (s_2 - r_2).\langle -1\rangle$. Or, les formes quadratiques $(s_1 - r_1).\langle -1\rangle$ et $(s_2 - r_2).\langle -1\rangle$ étant clairement anisotropes et les formes quadratiques $r_1.\langle 1, -1\rangle$ et $r_2.\langle 1, -1\rangle$ étant clairement hyperboliques, par unicité de la décomposition de Witt il vient $r_1.\langle 1, -1\rangle \simeq r_2.\langle 1, -1\rangle$, puis par simplification de Witt, $r_1 = r_2$ et on déduit $s_1 = s_2$. D'où l'unicité.
- Supposons $s_1 \leq r_1$ et $s_2 \leq r_2$, on montre de même $(r_1, s_1) = (r_2, s_2)$.

□

Exemple 4.1.1. *Soit ϕ une forme quadratique complexe régulière de dimension n. Alors ϕ est de rang n et par diagonalisation il existe $(a_1, \ldots, a_n) \in (\mathbb{C}^*)^n$ telle que $\phi \simeq \langle a_1, \ldots, a_n \rangle$. Or, $\mathbb{C}$ est quadratiquement clos, donc pour tout i, $a_i = 1$ dans $\mathbb{C}^*/(\mathbb{C}^*)^2$ soit $\phi \simeq \langle 1, \ldots, 1 \rangle \simeq n.\langle 1 \rangle$.*

- *Si $n = 2p$, on a $\phi \simeq p.\langle 1 \rangle \perp p.\langle 1 \rangle$ et donc comme $-1 = 1$ modulo les carrés de $\mathbb{C}^*$, $\phi \simeq p.\langle 1 \rangle \perp p.\langle -1 \rangle \simeq p.\langle 1, -1 \rangle$. La partie anisotrope de ϕ est triviale de dimension nulle notée $0.\langle 1 \rangle$ et ϕ est hyperbolique. On a aussi $\nu(\phi) = p$.*
- *Si $n = 2p + 1$, alors on a de même :*
$$\phi \simeq (2p+1).\langle 1 \rangle \simeq 2p.\langle 1 \rangle \perp \langle 1 \rangle \simeq p.\langle 1, -1 \rangle \perp \langle 1 \rangle.$$
La partie anisotrope de ϕ est donc $\langle 1 \rangle$. On a aussi $\nu(\phi) = p$.

Exemple 4.1.2. *Soit ϕ une forme quadratique réelle régulière de signature (r, s). Soit donc $\phi \simeq r.\langle 1 \rangle \perp s.\langle -1 \rangle$.*

- *Si $r \geq s$ alors $\phi \simeq s.\langle 1, -1 \rangle \perp (r-s).\langle 1 \rangle$ et la forme diagonale $(r-s).\langle 1 \rangle$ est clairement anisotrope. Ainsi par unicité de la décomposition de Witt à équivalence près, $(r-s).\langle 1 \rangle$ est la partie anisotrope de ϕ. On a aussi $\nu(\phi) = s$.*
- *Si $s \geq r$ alors $\phi \simeq r.\langle 1, -1 \rangle \perp (s-r).\langle -1 \rangle$ et la forme diagonale $(s-r).\langle -1 \rangle$ est clairement anisotrope. Ainsi, par unicité de la décomposition de Witt à équivalence près, $(s-r).\langle -1 \rangle$ est la partie anisotrope de ϕ. On a aussi $\nu(\phi) = r$.*

Au chapitre suivant, nous reverrons ces résultats en revisitant à l'aide de la décomposition de Witt et de la notion de Witt-équivalence, les classifications sur $\mathbb{C}$, $\mathbb{R}$ et les corps finis.

Remarque 4.1.1. *On peut de même décomposer toute forme quadratique q, qu'elle soit régulière ou non. En effet, notant n la dimension de q et r son rang, on a vu que $q \simeq \overline{q} \perp (n-r).\langle 0 \rangle$ et en décomposant la forme quadratique régulière $\overline{q}$, on a bien une décomposition de la forme : $q \simeq p.\langle 1, -1 \rangle \perp \overline{q}_a \perp (n-r).\langle 0 \rangle$*

Une des conséquences importantes du théorème de décomposition de Witt est le fait que :

classifier les formes quadratiques revient à classifier celles qui sont anisotropes.

On a donc dans un premier temps, ramené le problème de la classification des formes quadratiques à celui de la classification des formes quadratiques régulières, puis dans un second temps à celui de la classification des formes quadratiques anisotropes, via le théorème de décomposition de Witt.

Chapitre 5

Relation de Witt-équivalence

Ce chapitre s'inscrit dans le prolongement du chapitre précédent où l'on a énoncé l'important théorème de décomposition de Witt et a pour principal objectif de définir et d'étudier la relation de Witt-équivalence. On dira que deux formes quadratiques sont Witt-équivalentes lorsqu'elles ont des parties anisotropes équivalentes, ce qui souligne l'importance de la décomposition de Witt du chapitre précédent. Nous verrons aussi une caractérisation de la notion de Witt-équivalence en termes de somme orthogonale de formes quadratiques et étudierons le lien avec la notion d'équivalence. Enfin, ce chapitre sera également l'occasion de revisiter les classifications sur $\mathbb{C}$, $\mathbb{R}$ et les corps finis :

- les résultats usuels sur la classification des formes quadratiques réelles et complexes seront obtenus de manière très efficace en utilisant le théorème de décomposition de Witt, ainsi que la relation de Witt-équivalence.
- la classification sur les corps finis sera obtenue naturellement, après avoir défini la notion de discriminant d'une forme quadratique et étudier l'isotropie des formes quadratiques sur les corps finis en dimension $1, 2$ et 3.

5.1 La relation de Witt-équivalence

Définition 5.1.1. *Soit q et q' deux formes quadratiques régulières sur $\mathbb{K}$. On note q_a respectivement q'_a, la partie anisotrope de q, respectivement de q' définies de manière unique à équivalence près. On dit alors que q et q' sont Witt-équivalentes et on note $q \overset{W}{\sim} q'$ si et seulement si q_a et q'_a sont équivalentes.*

Proposition 5.1.1. *Toute forme quadratique régulière est Witt-équivalente à sa partie anisotrope. Deux formes quadratiques régulières anisotropes sont Witt-équivalentes si et seulement si elles sont équivalentes. Ainsi, deux formes quadratiques régulières équivalentes sont nécessairement Witt-équivalentes.*

Démonstration. Par définition même de la notion de Witt-équivalence, il est clair qu'une forme quadratique régulière est Witt-équivalente à sa partie anisotrope. De même, deux formes quadratiques anisotropes sont Witt-équivalentes si et seulement si leurs parties anisotropes sont équivalentes et donc naturellement si et seulement si elles sont équivalentes. □

Remarque 5.1.1. *Dans la suite, on s'intéressera essentiellement aux formes quadratiques régulières. On peut tout de même définir de la même façon la notion*

de Witt-équivalence entre formes quadratiques non nécessairement régulières. En effet, on a vu que l'on pouvait décomposer toute forme quadratique (de manière essentiellement unique) sous la forme d'une somme orthogonale d'une partie anisotrope, d'une partie hyperbolique et d'une partie nulle, ainsi deux formes quadratiques quelconques sont Witt-équivalentes si leurs parties régulières sont Witt-équivalentes c'est-à-dire si et seulement si elles ont des parties anisotropes équivalentes.

Voici une autre manière d'exprimer la notion de Witt-équivalence, deux formes qudratiques q et q' sont Witt-équivalentes si elles sont équivalentes modulo les formes quadratiques hyperboliques :

Proposition 5.1.2. *Soit q et q' deux formes quadratiques régulières. Alors q et q' sont Witt-équivalentes si et seulement s'il existe deux entiers naturels m et n tels que :*

$$q \perp m.\langle 1, -1\rangle \simeq q' \perp n.\langle 1, -1\rangle$$

Démonstration. Soit q et q' deux formes quadratiques régulières que l'on suppose Witt-équivalentes. D'après la définition, leurs parties anisotropes q_a et q'_a sont donc équivalentes. Par décomposition de Witt, il existe un unique couple d'entiers (p_1, p_2) tel que :

$$q \simeq p_1.\langle 1, -1\rangle \perp q_a \text{ et } q' \simeq p_2.\langle 1, -1\rangle \perp q'_a$$

Alors, supposons de plus que $p_1 \geq p_2$ (le cas $p_1 \leq p_2$ est identique aux notations près). On a alors :

$$q \simeq (p_1 - p_2).\langle 1, -1\rangle \perp p_2.\langle 1, -1\rangle \perp q_a \simeq (p_1 - p_2).\langle 1, -1\rangle \perp p_2.\langle 1, -1\rangle \perp q'_a.$$

Comme $q_a \simeq q'_a$ et $q' \simeq p_2.\langle 1, -1\rangle \perp q'_a$, on a par compatibilité de la relation d'équivalence avec la somme orthogonale : $q \simeq (p_1 - p_2).\langle 1, -1\rangle \perp q'$ ce qui donne la première implication avec $m = 0$ et $n = (p_1 - p_2)$.

Inversement, supposons qu'il existe un couple d'entiers (m, n) tel que :

$$q \perp m.\langle 1, -1\rangle \simeq q' \perp n.\langle 1, -1\rangle$$

Alors, en décomposant q et q' grâce au théorème de décomposition de Witt, il vient :

$$q \simeq p_1.\langle 1, -1\rangle \perp q_a \text{ et } q' \simeq p_2.\langle 1, -1\rangle \perp q'_a$$

Ce qui nous donne :

$$(p_1 + m).\langle 1, -1\rangle \perp q_a \simeq (p_2 + n).\langle 1, -1\rangle \perp q'_a$$

Par le théorème de décomposition de Witt, on a unicité de l'indice et donc $p_1 + m = p_2 + n$ et par simplification de Witt, nécessairement $q_a \simeq q'_a$ soit q et q' sont bien Witt-équivalentes. □

La propostition ci-dessus illustre encore une fois l'importance de la décomposition de Witt. La propostion suivante sera très utile lorsque l'on parlera du groupe de Witt associé à un corps $\mathbb{K}$.

Proposition 5.1.3. *Soit q_1, q_2, q'_1, q'_2 quatre formes quadratiques régulières. Alors :*

$$q_1 \overset{W}{\sim} q'_1 \text{ et } q_2 \overset{W}{\sim} q'_2 \Longrightarrow q_1 \perp q_2 \overset{W}{\sim} q'_1 \perp q'_2$$

Démonstration. D'après la proposition précédente, il existe deux couples d'entiers (n_1, n_1') et (n_2, n_2') tels que :

$$q_1 \perp n_1.\langle 1,-1\rangle \simeq q_1' \perp n_1'.\langle 1,-1\rangle \text{ et } q_2 \perp n_2.\langle 1,-1\rangle \simeq q_2' \perp n_2'.\langle 1,-1\rangle$$

Alors on a :

$$(q_1 \perp q_2) \perp (n_1+n_2).\langle 1,-1\rangle \simeq (q_1' \perp q_2') \perp (n_1'+n_2').\langle 1,-1\rangle$$

Ainsi $q_1 \perp q_2 \overset{W}{\sim} q_1' \perp q_2'$ □

La proposition suivante lie la notion de Witt-équivalence avec la notion d'équivalence :

Proposition 5.1.4. *Deux formes quadratiques q et q' régulières sont équivalentes si et seulement si elles sont Witt-équivalentes et de même dimension. Ainsi deux formes quadratiques régulières équivalentes sont Witt-équivalentes.*

Démonstration. Supposons que q et q' sont équivalentes. Par unicité de la décomposition de Witt (à équivalence près) q et q' ont même décomposition de Witt et ont donc même partie anisotrope (à équivalence près), d'où q et q' sont Witt-équivalentes. De plus q et q' étant équivalentes, les espaces quadratiques associés (E, q) et (E', q') sont isomorphes et donc E et E' sont en particulier isomorphes en tant qu'espaces vectoriels et nécessairement de même dimension, soit $dim(q) = dim(q')$. Inversement, si q et q' sont Witt-équivalentes et $dim(q) = dim(q')$, alors par décomposition de Witt, on a :

$$q \simeq p.\langle 1,-1\rangle \perp q_a \text{ et } q' \simeq p'.\langle 1,-1\rangle \perp q_a'$$

Comme $q_a \simeq q_a'$ par Witt-équivalence de q et q', $dim(q_a) = dim(q_a')$. D'où,

$$dim(q) = 2p + dim(q_a) = 2p' + dim(q_a') \Longrightarrow p = p'$$

Au final :

$$q \simeq p.\langle 1,-1\rangle \perp q_a \simeq p.\langle 1,-1\rangle \perp q_a' \simeq q'.$$

□

Remarque 5.1.2. *Contrairement à deux formes quadratiques équivalentes, deux formes quadratiques Witt-équivalentes n'ont pas nécessairement le même domaine. Considérons par exemple, la forme quadratique réelle $\langle 1,-1\rangle \perp \langle 1,1\rangle$ de partie anisotrope $\langle 1,1\rangle$. On a $\langle 1,-1\rangle \perp \langle 1,1\rangle \overset{W}{\sim} \langle 1,1\rangle$ et pourtant elles n'ont pas le même domaine. En effet, $\langle 1,1\rangle$ ne représente pas les réels négatifs, alors que $\langle 1,-1\rangle \perp \langle 1,1\rangle$ est universelle car $\langle 1,-1\rangle$ l'est (puisque régulière isotrope).*

Proposition 5.1.5. *La relation de Witt-équivalence entre formes quadratiques régulières est une relation d'équivalence sur la collection des formes quadratiques régulières. L'équivalence impliquant la Witt-équivalence, la relation $\overset{W}{\sim}$ est donc plus grossière que la relation d'équivalence $\simeq$.*

Démonstration. La réflexivité, tout comme la symétrie est immédiate. Enfin la transitivité est évidente elle aussi, puisque notant q_1, q_2 et q_3 trois formes quadratiques régulières telles que $q_1 \overset{W}{\sim} q_2$ et $q_2 \overset{W}{\sim} q_3$, alors pour les formes quadratiques anisotropes associées $q_{1,a} \simeq q_{2,a}$ et $q_{2,a} \simeq q_{3,a}$ et donc $q_{1,a} \simeq q_{3,a}$ par transitivité de la relation d'équivalence entre formes quadratiques régulières. Soit au final $q_1 \overset{W}{\sim} q_3$, ce qui achève de montrer le résultat. □

Les formes quadratiques régulières sur $\mathbb{K}$ ne constituent pas un ensemble, pour parler de classes d'équivalences pour la relation de Witt-équivalence, on va devoir définir la notion de Witt-équivalence sur l'ensemble des matrices symétriques à coefficients dans $\mathbb{K}$.

Notation 5.1.1. *On définit sur l'ensemble des matrices carrées symétriques, la relation de Witt-équivalence en passant par les formes quadratiques associées. Ainsi, si $A \in S_n(\mathbb{K})$ et $B \in S_p(\mathbb{K})$ sont deux matrices carrées symétriques, on dit que A et B sont Witt-équivalentes et l'on note $A \overset{W}{\approx} B$ si les formes quadratiques associées $q_A : X \mapsto {}^tXAX$ et $q_B : Y \mapsto {}^tYBY$ sont Witt-équivalentes. On note alors $W(\mathbb{K})$ l'ensemble des classes de Witt-équivalence de matrices symétriques à coefficients dans $\mathbb{K}$.*

Remarque 5.1.3. *La classe de Witt-équivalence d'une matrice $A \in S_n(\mathbb{K})$ représentant la forme quadratique q est donc :*

$$\{B \in S_p(\mathbb{K}) : q \overset{W}{\sim} q_B, p \in \mathbb{N}\}$$

Cette classe de Witt-équivalence ne dépend que de $q \simeq q_A$ à Witt-équivalence près, c'est-à-dire est égal à :

$$\{C \in S_p(\mathbb{K}) : q' \overset{W}{\sim} q_C, p \in \mathbb{N}\}$$

*pour tout q' telle que $q' \overset{W}{\sim} q$. Ainsi, on peut parler des **classes de Witt-équivalence** de formes quadratiques de dimension finie, en associant à toute forme quadratique un élément de $W(\mathbb{K})$ via la représentation matricielle.*

Notation 5.1.2. *On a vu qu'il était possible de diagonaliser toute forme quadratique, c'est-à-dire qu'à équivalence près, toute forme quadratique s'écrit sous la forme $\langle a_1, \ldots, a_n \rangle$ où les a_i sont dans $\mathbb{K}$. Alors, toute forme quadratique admet dans sa classe de congruence de matrices symétriques associées une matrice diagonale $D(a_1, \ldots, a_n)$ et on note $< a_1, \ldots, a_n >$ la classe de Witt-équivalence de cette matrice diagonale. On parle aussi de la classe de Witt-équivalence de la forme diagonale $\langle a_1, \ldots, a_n \rangle$ qui est donc également la classe de Witt-équivalence de toute forme quadratique q équivalente à $\langle a_1, \ldots, a_n \rangle$.*

5.2 Les classifications sur $\mathbb{R}$ et $\mathbb{C}$ revisitées

Au chapitre précédent, nous avons pu, grâce au théorème de décomposition de Witt, exhiber la partie anisotrope associée à une forme quadratique complexe régulière ainsi que la partie anisotrope associée à une forme quadratique réelle régulière. Nous allons poursuivre cette étude dans ce chapitre en utilisant la notion de Witt-équivalence pour retrouver les résultats classiques de la classification des formes quadratiques sur $\mathbb{R}$ et $\mathbb{C}$.

5.2.1 La classification sur $\mathbb{C}$ revisitée

Théorème 5.2.1. *Il existe à équivalence près une unique forme quadratique régulière de dimension donnée n sur $\mathbb{C}$ et toute forme quadratique régulière de dimension paire sur $\mathbb{C}$ est hyperbolique. Toute forme quadratique régulière est Witt-équivalente à la forme de dimension nulle $0.\langle 1\rangle$ ou à la forme $\langle 1\rangle$.*

Démonstration. Soit q une forme quadratique complexe régulière de dimension n. Par diagonalisation, et régularité, il existe un n-uplet $(a_i)_{1\leq i\leq n} \in (\mathbb{C}^*)^n$ tel que $q \simeq \langle a_1, \ldots, a_n\rangle$ et $\mathbb{C}$ étant quadratiquement clos $\langle a_1, \ldots, a_n\rangle \simeq \langle 1, \ldots, 1\rangle$. Ainsi, -1 étant un carré, $1 = -1$ modulo les carrés de $\mathbb{C}^*$ et donc :

- si $n = 2p$ est paire, $q \simeq 2p.\langle 1\rangle \simeq p.\langle 1, -1\rangle$ et donc q est hyperbolique et Witt-équivalente à la forme triviale $0.\langle 1\rangle$, car de partie anisotrope de dimension nulle.
- si $n = 2p + 1$ est impaire, $q \simeq (2p + 1).\langle 1\rangle \simeq p\langle 1, -1\rangle\perp\langle 1\rangle$ et q est Witt-équivalente à la forme diagonale anisotrope $\langle 1\rangle$.

Ainsi à équivalence près, $n.\langle 1\rangle$ est la seule forme quadratique régulière complexe de dimension n. Les seules formes quadratiques régulières complexes anisotropes sont alors par l'étude de la Witt-équivalence, la forme de dimension nulle $0.\langle 1\rangle$ et la forme $\langle 1\rangle$. □

5.2.2 La classification sur $\mathbb{R}$ revisitée

Nous allons encore une fois appliquer la décomposition de Witt d'une forme quadratique régulière et la notion de Witt-équivalence pour classifier les formes anisotropes réelles de dimension finie.

Proposition 5.2.1. *A équivalence près, il existe exactement deux formes quadratiques anisotropes réelles de dimension n que sont $n.\langle 1\rangle$ et $n.\langle -1\rangle$, c'est-à-dire celles de signature $(n, 0)$ dites définies positives et celles de signature $(0, n)$ dites définies négatives. Une forme quadratique régulière de signature (r, s) est Witt-équivalente à :*

- $(r - s).\langle 1\rangle$ *si* $r \geq s$
- $(s - r).\langle -1\rangle$ *si* $s \geq r$

Démonstration. Soit q une forme quadratique réelle régulière de signature (r, s). Par définition de la signature énoncée au chapitre précédent, $q \simeq r.\langle 1\rangle\perp s.\langle -1\rangle$ et alors $q \simeq r.\langle 1, -1\rangle\perp(s-r).\langle -1\rangle$ si $s \geq r$ ou $q \simeq s.\langle 1, -1\rangle\perp(r-s).\langle 1\rangle$ si $r \geq s$. La partie anisotrope de q étant alors $(s-r).\langle -1\rangle$ si $s \geq r$ ou $(r-s).\langle 1\rangle$ si $r \geq s$, ce qui donne la deuxième partie de la proposition. De plus, q est anisotrope si et seulement si sa partie hyperbolique est triviale, ce qui équivaut à $r = 0$ ou $s = 0$. Les formes quadratiques anisotropes régulière de dimension n sont donc les formes quadratiques de signature $(n, 0)$ et $(0, n)$. □

Définition 5.2.1. *Soit q une forme quadratique réelle régulière de signature (r, s). L'entier $r - s$ est appelé* ***la signature réduite*** *de q*

Proposition 5.2.2. *Deux formes quadratiques réelles, régulières, q_1 et q_2 sont Witt-équivalentes si et seulement si elles ont la même signature réduite.*

Démonstration. Soit q_1, q_2 deux formes quadratiques réelles régulières de signatures associées (r_1, s_1) et (r_2, s_2). Puisque q_1 et q_2 sont Witt-équivalentes si et seulement si leur parties anisotropes sont équivalentes on a :

- $q_1 \overset{W}{\sim} (r_1 - s_1).\langle 1\rangle$ ou $q_1 \overset{W}{\sim} (s_1 - r_1).\langle -1\rangle$ selon que $r_1 \geq s_1$ ou $s_1 \geq r_1$
- $q_2 \overset{W}{\sim} (r_2 - s_2).\langle 1\rangle$ ou $q_2 \overset{W}{\sim} (s_2 - r_2).\langle -1\rangle$ selon que $r_2 \geq s_2$ ou $s_2 \geq r_2$

Comme $\langle 1\rangle \not\simeq \langle -1\rangle$, $q_1 \overset{W}{\sim} q_2$ si et seulement si on a :

$$(r_1 - s_1).\langle 1\rangle \simeq (r_2 - s_2).\langle 1\rangle \Longleftrightarrow (r_1 - s_1) = (r_2 - s_2)$$

ou

$$(s_1 - r_1).\langle -1\rangle \simeq (s_2 - r_2).\langle -1\rangle \Longleftrightarrow (s_1 - r_1) = (s_2 - r_2)$$

D'où le résultat. □

5.3 Discriminant d'une forme quadratique

Nous allons dans la suite définir la notion de discriminant d'une forme quadratique. Il nous servira pour classifier les formes quadratiques régulières sur les corps finis et nous fournira un invariant pour la relation de Witt-équivalence entre formes quadratiques.

Définition 5.3.1. *Soit q une forme quadratique régulière de dimension n. La classe*

$$\Delta = (-1)^{\frac{n(n-1)}{2}} det(q) \in \mathbb{K}^*/(\mathbb{K}^*)^2$$

est appelé ***le discriminant*** *de q. Tout représentant de cette classe est appelé* un *discriminant de q. On appelle discriminant d'une forme quadratique non nécessairement régulière, celui de sa partie régulière.*

5.3.1 Caractérisation des plans hyperboliques par le discriminant

Proposition 5.3.1. *Un plan quadratique régulier est hyperbolique si et seulement s'il est de discriminant* 1 *dans $\mathbb{K}^*/(\mathbb{K}^*)^2$.*

Démonstration. Ceci est une application immédiate du théorème de caractérisation des plans quadratiques, avec pour q forme quadratique régulière de dimension 2, $\Delta(q) = (-1)^{\frac{2(2-1)}{2}} det(q) = -det(q)$. □

5.3.2 Discriminant et Witt-équivalence

Puisque $det(\langle 1, -1\rangle) = -1$, deux formes quadratiques Witt-équivalentes n'ont pas nécessairement le même déterminant, alors que c'est le cas pour deux formes quadratiques équivalentes. Nous montrerons que deux formes quadratiques Witt-équivalentes ont le même discriminant et pour ce faire, nous allons prouver que le discriminant est compatible avec la somme orthogonale lorsque l'on additionne des formes quadratiques de dimension paire.

Proposition 5.3.2. *Soit ϕ et ψ deux formes quadratiques régulières et on suppose ψ de dimension* 2*. Alors,*

$$\Delta(\phi \perp \psi) = \Delta(\phi)\Delta(\psi)$$

Démonstration. On note n la dimension de ϕ, alors $dim(\phi\perp\psi) = n+2$ et donc :

$$\Delta(\phi\perp\psi) = (-1)^{\frac{(n+2)(n+1)}{2}} det(\phi\perp\psi) = (-1)^{\frac{(n+2)(n+1)}{2}} det(\phi)det(\psi)$$

Or $\frac{(n+2)(n+1)}{2} = (2n+1) + \frac{n(n-1)}{2}$, soit :

$$\begin{aligned}\Delta(\phi\perp\psi) &= (-1)^{\frac{n(n-1)}{2}} (-1)^{(2n+1)} det(\phi)det(\psi)\\ &= (-1)^{\frac{n(n-1)}{2}} det(\phi)(-det(\psi))\\ &= \Delta(\phi)\Delta(\psi)\end{aligned}$$

Tout plan hyperbolique étant de discriminant 1, on a :

$$\Delta(\phi\perp n.\langle 1,-1\rangle) = \Delta(\phi)\prod_{i=1}^{n}\Delta(\langle 1,-1\rangle) = \Delta(\phi)$$

□

Proposition 5.3.3. *Deux formes quadratiques régulières Witt-équivalentes ont même discrimant.*

Démonstration. Soit q, q' deux formes quadratiques régulières que l'on suppose Witt-équivalentes. Alors, il existe deux entiers m, n tels que :

$$q\perp m.\langle 1,-1\rangle \simeq q'\perp n.\langle 1,-1\rangle$$

D'après la proposition précédente, on a alors :

$$\Delta(q) = \Delta(q\perp m.\langle 1,-1\rangle) = \Delta(q'\perp n.\langle 1,-1\rangle) = \Delta(q')$$

□

5.4 La classification sur les corps finis revisitée

Dans la suite, on note $\mathbb{K}$ un corps fini. On rappelle alors que $\mathbb{K}^*/(\mathbb{K}^*)^2$ est un groupe de cardinal 2 (l'endormorphisme $x \mapsto x^2$ défini sur $\mathbb{K}^*$ est un morphisme surjectif à valeur dans $(\mathbb{K}^*)^2$ de noyau $\{1,-1\}$). On note aussi ε un représentant de la classe des non carrés de $\mathbb{K}$.

5.4.1 Etude de l'isotropie des formes quadratiques sur les corps finis

Proposition 5.4.1. *Toute forme quadratique régulière de dimension 2 sur $\mathbb{K}$ est universelle.*

Démonstration. Soit q une forme quadratique régulière de dimension 2 et $\mathbb{K}$ un corps fini de caractéristique $p \in \mathcal{P}\backslash\{2\}$. Puisque $\mathbb{K}^*/(\mathbb{K}^*)^2 = \{\overline{1}, \overline{\varepsilon}\}$, par diagonalisation, il n'y a à équivalence près qu'au plus 3 formes quadratiques régulières de dimension 2 : $\langle 1,1\rangle$,$\langle 1,\varepsilon\rangle$ et $\langle \varepsilon,\varepsilon\rangle$. Il suffit ainsi de montrer que ces trois formes diagonales sont universelles. Or $\langle 1,\varepsilon\rangle$ représentant naturellement 1 et ε, elles représentent tous les éléments de $\mathbb{K}^*$ et est universelle. Supposons

par l'absurde $\langle 1,1\rangle$ non universelle, alors 1 étant représenté par $\langle 1,1\rangle$, nécessairement ε n'est pas représenté par $\langle 1,1\rangle$ et aucun élement de la classe $\overline{\varepsilon}$ n'est représenté. Ainsi, pour tout $x, y \in \mathbb{K}$, x^2+y^2 est un carré de $\mathbb{K}$ et l'ensemble des carrés de $\mathbb{K}$ serait donc stable par addition. Or, puisque $-1=(p-1)$ dans le corps fini $\mathbb{K}$, -1 serait alors somme de carrés et donc un carré, ce qui implique alors que $\langle 1,-1\rangle \simeq \langle 1,1\rangle$ et la forme $\langle 1,1\rangle$ serait donc hyperbolique et universelle, absurde. De même, supposons par l'absurde $\langle \varepsilon,\varepsilon\rangle$ non universelle, alors ε étant représenté par $\langle \varepsilon,\varepsilon\rangle$, nécessairement 1 n'est pas représenté par $\langle \varepsilon,\varepsilon\rangle$ et aucun élement de la classe $\overline{1}$ n'est représenté. Ainsi, pour tout $x, y \in \mathbb{K}$, $\varepsilon x^2+\varepsilon y^2$ est un non carré de $\mathbb{K}$ et l'ensemble des non carrés de $\mathbb{K}$ serait donc stable par addition. Or, puisque $-\varepsilon=(p-1)\varepsilon$ dans le corps fini $\mathbb{K}$, $-\varepsilon$ serait alors somme de non carrés et donc un non carré, ce qui implique alors que $\langle \varepsilon,-\varepsilon\rangle \simeq \langle \varepsilon,\varepsilon\rangle$ et la forme $\langle \varepsilon,\varepsilon\rangle$ serait donc hyperbolique par caractérisation des plans hyperboliques et universelle, absurde. □

Proposition 5.4.2. *Toute forme quadratique régulière de dimension au moins 3 sur $\mathbb{K}$ est isotrope.*

Démonstration. Soit q une forme quadratique régulière de dimension au moins 3. Alors, notant $n=dim(q)$, il existe par diagonalisation un n-uplet $(a_1,\ldots,a_n)$ de scalaires non nuls tel que $q \simeq \langle a_1,\ldots,a_n\rangle \simeq \langle a_1,\ldots,a_{n-1}\rangle \perp \langle a_n\rangle$. Notant $q_1=\langle a_1,\ldots,a_{n-1}\rangle$, q_1 est de dimension au moins 2 et s'écrit donc comme somme orthogonale d'une forme quadratique régulière de dimension 2 qui est d'après ce qui précède, universelle et d'une autre forme quadratique régulière. Ainsi, $q_1=\langle a_1,\ldots,a_{n-1}\rangle$ est elle aussi universelle et $-a_n$ est en particulier représenté par q_1. Par le principe de représentation vu au chapitre 3, $q=q_1\perp\langle a_n\rangle$ est isotrope.

□

Corollaire 5.4.1. *A équivalence près, les seules formes quadratiques anisotropes de dimension finie sont :* $0.\langle 1\rangle$, $\langle 1\rangle$, $\langle \varepsilon\rangle$ *et* $\langle 1,-\varepsilon\rangle$.

Démonstration. La forme triviale $0.\langle 1\rangle$ de dimension nulle est clairement anisotrope, tout comme les formes quadratiques $\langle 1\rangle$ et $\langle \varepsilon\rangle$. Si q est régulière de dimension supérieure ou égale à 3, elle est isotrope. Intéressons nous alors aux formes quadratiques régulières de dimension 2. Elles sont toutes universelles et donc notant ϕ une telle forme définie sur un $\mathbb{K}$-espace vectoriel E, il existe $x \neq 0 \in E$ tel que $\phi(x)=1$. On a donc $\phi_{vect(x)} \simeq \langle 1\rangle$ et puisque

$$\Delta(\phi) \in \mathbb{K}^*/(\mathbb{K}^*)^2 = \{\overline{1},\overline{\varepsilon}\} \text{ et que } \Delta(\phi) = -det(\phi)$$

notant δ un discriminant de ϕ choisi dans $\{1,\varepsilon\}$, on a par le principe de complétion à l'aide d'un déterminant : $\phi \simeq \langle 1,-\delta\rangle$ et donc $\phi \simeq \langle 1,-\varepsilon\rangle$ ou $\phi \simeq \langle 1,-1\rangle$. D'où, ϕ de dimension 2 régulière est soit équivalente à $\langle 1,-1\rangle$ et est donc hyperbolique, soit équivalente à $\langle 1,-\varepsilon\rangle$ et est donc anisotrope (sinon elle serait isotrope de dimension 2 et donc hyperbolique, absurde car $\Delta(\langle 1,-\varepsilon\rangle)=\varepsilon$ qui n'est pas un carré de $\mathbb{K}^*$). Ainsi en dimension 2, à équivalence près $\langle 1,-\varepsilon\rangle$ est la seule forme quadratique anisotrope. □

5.4.2 Witt-équivalence et équivalence sur les corps finis

En application du théorème de décompostion de Witt et de la partie précédente, on déduit les deux théorèmes de classification suivants :

Théorème 5.4.1. *Soit ϕ une forme quadratique régulière sur $\mathbb{K}$ et δ un discriminant. Alors,*

- *si $dim(\phi) = 2n+2$ pour un $n \in \mathbb{N}$, alors $\phi \simeq n.\langle 1,-1\rangle \perp \langle 1,-\delta\rangle$*
- *si $dim(\phi) = 2n+1$ pour un $n \in \mathbb{N}$, alors $\phi \simeq n.\langle 1,-1\rangle \perp \langle \delta\rangle$*

Démonstration. Supposons $dim(\phi) = 2n+2$. Par décomposition de Witt, il existe un entier p et une forme anisotrope ϕ_a tel que $\phi \simeq p.\langle 1,-1\rangle \perp \phi_a$. La proposition 5.3.3 donne alors :

$$\Delta(\phi) = \Delta(\phi_a) = \delta$$

En raison de l'étude des formes quadratiques anisotropes sur les corps finis et des dimensions, soit ϕ_a est de dimension nulle et donc ϕ est hyperbolique et $p = (n+1)$, soit $\phi_a \simeq \langle 1,-\varepsilon\rangle$ et $p = n$. Dans le premier cas $\Delta(\phi) = 1 = \delta$ et dans le second cas $\Delta(\phi) = \delta = \varepsilon$. Ainsi dans les deux cas, on a :

$$\phi \simeq n.\langle 1,-1\rangle \perp \langle 1,-\delta\rangle$$

Supposons $dim(\phi) = 2n+2$. Toujours par décomposition de Witt, il existe p et une forme anisotrope ϕ_a tel que $\phi \simeq p.\langle 1,-1\rangle \perp \phi_a$. En raison des dimensions et de l'étude des formes quadratiques sur les corps finis, soit $\phi_a \simeq \langle 1\rangle$ et donc $\Delta(\phi) = 1$ et $p = n$, soit $\phi_a \simeq \langle \varepsilon\rangle$ et donc $\Delta(\phi) = \varepsilon$ et $p = n$. Ainsi dans les deux cas, on a :

$$\phi \simeq n.\langle 1,-1\rangle \perp \langle \delta\rangle.$$

□

La classification des formes quadratiques sur le corps fini $\mathbb{K}$ se traduit alors en terme d'équivalence et de Witt-équivalence par le théorème suivant :

Théorème 5.4.2. *Soit $\mathbb{K}$ un corps fini. Alors,*

- *Deux formes quadratiques régulières sur $\mathbb{K}$ sont Witt-équivalentes si et seulement si elles ont des dimensions de même parité et ont même discriminant.*
- *Deux formes quadratiques régulières sur $\mathbb{K}$ sont équivalentes si et seulement si elles ont même dimension et même discriminant. Ce qui est équivalent à ce qu'elles aient même dimension et même déterminant.*

Exemple 5.4.1. *La forme quadratique $\langle 1,1,1,1\rangle$ est systématiquement hyperbolique lorsque le corps $\mathbb{K}$ est fini. En effet,*

$$\langle 1,1,1,1\rangle \simeq \langle 1,-1,1,-1\rangle$$

puisque

$$dim(\langle 1,1,1,1\rangle) = dim(\langle 1,-1,1,-1\rangle) = 4 \text{ et}$$
$$\Delta(\langle 1,1,1,1\rangle) = \Delta(\langle 1,-1,1,-1\rangle) = 1$$

avec $\langle 1,-1,1,-1\rangle \simeq 2.\langle 1,-1\rangle$.

Chapitre 6

Groupes de Witt et Witt-Grothendieck

Dans ce chapitre, nous allons utiliser les propriétés de l'opération d'addition orthogonale pour définir deux importantes structures de groupes abéliens. En effet, nous avons vu que la relation $\perp$ est compatible avec la relation d'équivalence et de Witt-équivalence entre formes quadratiques régulières, ce qui nous permet de définir :

- le groupe de Witt $W(\mathbb{K})$ associé au corps $\mathbb{K}$, de loi additive $\perp$, défini sur l'ensemble des classes de Witt-équivalence de formes quadratiques régulières.
- le groupe de Witt-Grothendieck $\widehat{W}(\mathbb{K})$ associé au corps $\mathbb{K}$, obtenu à l'aide de la loi addtitive $\perp$ et défini sur l'ensemble $FQ(\mathbb{K})$ des classes d'isomorphie de formes quadratiques régulières qui a une structure de monoïde et qui est enrichi d'une structure de groupe par la construction de Grothendieck.

La théorie de Witt nous permet alors d'analyser un corps $\mathbb{K}$ à travers ses formes quadratiques, et ce à travers deux groupes : $W(\mathbb{K})$ et $\widehat{W}(\mathbb{K})$, dont l'un voit ces formes à Witt-équivalence près et l'autre à équivalence près. Dans un premier temps, nous allons définir et exposer les constructions de ces deux structures de groupes abéliens, ce qui nous permettra, de mettre de nouveau en évidence, le rôle majeur joué par la simplification de Witt. Ensuite, nous exhiberons des parties génératrices de ces deux groupes, ce qui nous en facilitera grandement leurs études. Naturellement, nous donnerons également quelques exemples et propriétés générales telles que les propriétés universelles du groupe de Witt et Witt-Grothendieck qui nous permettront de construire des morphismes de groupes ayant pour source $W(\mathbb{K})$ ou $\widehat{W}(\mathbb{K})$. Ceci nous amènera alors à analyser sous l'angle de la théorie de Witt, les corps $\mathbb{C}$ et $\mathbb{R}$, ainsi que les corps finis ; résultats qui nous seront d'une grande utilité pour la suite, notamment pour bien assimiler le groupe $W(\mathbb{Q})$, dont l'étude nous permettra de mieux comprendre les formes quadratiques rationnelles.

Nous aurons aussi l'ocassion de voir que les groupes $W(\mathbb{K})$ et $\widehat{W}(\mathbb{K})$ sont liés par une relation simple et nous verrons alors comment déduire la structure du groupe $\widehat{W}(\mathbb{K})$, de l'étude du groupe $W(\mathbb{K})$ et de $I(\mathbb{K})$, l'un de sous-groupes d'indice 2, appelé l'idéal fondamental. Nous donnerons aussi des caractérisations

intéressantes des corps quadratiquement clos et pythagoriciens, via l'étude de leurs groupes de Witt et Witt-Grothendieck associés.

Enfin, nous terminerons par donner une présentation des groupes $W(\mathbb{K})$ et $\widehat{W}(\mathbb{K})$ par générateurs et relations, que nous utiliserons pour donner une caractérisation des corps pour lesquels la relation de congruence entre matrices diagonales inversibles est décrite par :

$$D(a_1,\dots,a_n) \approx D(b_1,\dots,b_n) \iff \text{il existe } \sigma \in \mathfrak{S}_n \text{ et } (\lambda_1,\dots,\lambda_n) \in (\mathbb{K}^*)^n \text{ tels que } \forall k \in [\![1,n]\!], b_k = \lambda_k^2 a_{\sigma(k)}$$

6.1 Le groupe de Witt

Notation 6.1.1. *Etant donné q une forme quadratique régulière sur $\mathbb{K}$, on notera*

$$[q] = \{q', q' \simeq q\}$$

sa classe dite d'isomorphie et $[q]_W$ sa classe de Witt-équivalence. Ainsi, pour deux formes quadratiques régulières q_1,q_2 on a :

- $[q_1] = [q_2] \iff q_1 \simeq q_2$
- $[q_1]_W = [q_2]_W \iff q_1 \overset{W}{\sim} q_2$

L'ensemble des classes d'isomorphie de formes quadratiques régulières sur $\mathbb{K}$ est noté $FQ(\mathbb{K})$ et on a déjà défini $W(\mathbb{K})$ qui est l'ensemble des classes de Witt-équivalence de formes quadratiques régulières et qui s'identifie alors naturellement comme l'ensemble des classes d'isomorphie de formes anisotrope de dimension finie.

La loi d'addition orthogonale $\perp$ va permettre de munir $W(\mathbb{K})$ d'une structure de groupe abélien.

Lemme 6.1.1. *L'opération :*

$$\begin{array}{rcl} W(\mathbb{K}) \times W(\mathbb{K}) & \longrightarrow & W(\mathbb{K}) \\ ([q]_W, [q']_W) & \longmapsto & [q \perp q']_W \end{array}$$

définit une loi de composition interne sur $W(\mathbb{K})$ que l'on notera $+$.

Démonstration. La proposition 5.1.3 donne directement le résultat. □

De plus, l'opération d'addition orthogonale entre formes quadratiques étant clairement commutative et associative à équivalence près, elle l'est donc aussi à Witt-équivalence près. Ainsi, la loi interne ci-dessus munit $(W(\mathbb{K}), +)$ d'une structure de monoïde abélien ayant pour élément neutre, la classe de la forme triviale de dimension nulle qui est aussi la classe de toute forme hyperbolique. Ainsi, pour tout forme quadratique régulière sur $\mathbb{K}$, on a :

$$q \perp (-q) \text{ est hyperbolique et donc } [q \perp (-q)]_W = [q]_W + [-q]_W = 0_{W(\mathbb{Q})}$$

ce qui montre que l'opposé de $[q]_W$ est $[-q]_W$ que l'on note $-[q]_W$, la loi $\perp$ étant notée additivement $+$. La proposition suivante synthétise ce que nous avons développé ci-dessus.

Proposition 6.1.1. *Muni de la loi $+$, l'ensemble $W(\mathbb{K})$ forme un groupe abélien que l'on appelle le* ***groupe de Witt*** *de $\mathbb{K}$. Son neutre est $[0]_W = [q]_W$ pour tout forme quadratique hyperbolique et pour tout forme quadratique régulière q, l'opposé de $[q]_W$ est $[-q]_W$ noté $-[q]_W$.*

Notation 6.1.2. *On définit $< a_1, \ldots, a_n >$ comme étant la classe de Witt-équivalence de la forme quadratique régulière $\langle a_1, \ldots, a_n \rangle$ (les a_i étant non nuls).*

L'étude d'un groupe est toujours facilitée par la connaissance d'une partie génératrice, la proposition suivante en exhibe une.

Proposition 6.1.2. ***partie génératrice de*** $W(\mathbb{K})$
L'ensemble des classes de Witt-équivalence $< a >$ où a parcourt un système de représentants des classes de $\mathbb{K}^*/(\mathbb{K}^*)^2$ est une partie génératrice de $W(\mathbb{K})$.

Démonstration. Soit q une forme quadratique régulière de dimension n. Par diagonalisation il existe n scalaires $a_1, \ldots, a_n$ tels que $q \simeq \langle a_1, \ldots, a_n \rangle$. En particulier $q \overset{W}{\sim} \langle a_1, \ldots, a_n \rangle$, ce qui s'exprime avec les notations précédentes, par :

$$[q]_W = [\langle a_1, \ldots, a_n \rangle]_W = [\langle a_1 \rangle \perp \ldots \perp \langle a_n \rangle]_W = < a_1 > + \ldots + < a_n >$$

Ainsi tout élément $[q]_W \in W(\mathbb{K})$ s'écrit comme somme d'élément de la forme $< a >$ où l'on a choisit dans chaque classe de $\mathbb{K}^*/(\mathbb{K}^*)^2$, un représentant a. D'où le résultat. □

En application immédiate de la proposition ci-dessus, on déduit la structure des groupes de Witt $W(\mathbb{R})$, $W(\mathbb{C})$ et $W(\mathbb{K})$ où $\mathbb{K}$ est un corps fini.

Proposition 6.1.3. Structure des groupes de Witt $W(\mathbb{C})$ et $W(\mathbb{R})$
Le groupe $W(\mathbb{C})$ est engendré par $< 1 >$ et isomorphe à $\mathbb{Z}/2$. Tandis que le groupe $W(\mathbb{R})$ est encore engendré par $< 1 >$ mais isomorphe à $\mathbb{Z}$.

Démonstration. Le corps $\mathbb{C}$ étant quadratiquement clos, $< 1 >$ engendre $W(\mathbb{C})$, qui possède donc deux éléments $< 1 >$ et $[0]_W$. Le seul groupe d'ordre 2 étant à isomorphisme près $\mathbb{Z}/2$, on a bien $W(\mathbb{C}) \simeq \mathbb{Z}/2$.

L'ensemble $\{1, -1\}$ constitue un ensemble de représentants des classes de $\mathbb{R}^*$ modulo $(\mathbb{R}^*)^2$. Ainsi, d'après la proposition précédente, $< 1 >$ et $< -1 >$ engendre $W(\mathbb{R})$. Or, $< -1 >$ est l'opposé de $< 1 >$ dans $W(\mathbb{R})$ et donc au final $< 1 >$ est un élément générateur de $W(\mathbb{R})$ qui est alors un groupe monogène. Supposons qu'il soit cyclique, alors il existe $n \in \mathbb{N}^*$ tel que $n.< 1 >= [0]_W$ et donc la forme diagonale $n.\langle 1 \rangle$ serait Witt-équivalente à la forme triviale, soit hyperbolique. Ceci est absurde car $n.\langle 1 \rangle$ est on l'a vu, anisotrope. D'où $W(\mathbb{R}) \simeq \mathbb{Z}$, car monogène, non cyclique. □

Remarque 6.1.1. *On retrouvera par la suite que $W(\mathbb{C}) \simeq \mathbb{Z}/2$. On verra en effet, que l'isomorphisme $W(\mathbb{K}) \simeq \mathbb{Z}/2$ caractérise les corps quadratiquement clos.*

Proposition 6.1.4. Structure du groupe de Witt W($\mathbb{K}$) pour $\mathbb{K}$ corps fini.
On suppose que $\mathbb{K}$ est un corps fini de cardinal q et soit ε un représentant de la classe des non carrés de $\mathbb{K}^*$. Alors :

1. $W(\mathbb{K}) \simeq \mathbb{Z}/2 \times \mathbb{Z}/2$ *si* $q \equiv 1\,[4]$.
2. $W(\mathbb{K}) \simeq \mathbb{Z}/4$ *si* $q \equiv 3\,[4]$.

Démonstration. Le groupe de Witt $W(\mathbb{K})$ est engendré par les classes de Witt équivalences des formes diagonales $\langle a\rangle$ où a parcourt l'ensemble des représentants des classes de $\mathbb{K}^*$ modulo $(\mathbb{K}^*)^2$. Ainsi $(\mathbb{K}^*)^2$ étant d'indice 2 dans $\mathbb{K}^*$ (car $\mathbb{K}$ est un corps fini), $W(\mathbb{K})$ est engendré par les deux éléments $< 1 >$ et $< \varepsilon >$ où 1 représente la classe des carrés et ε la classe des non carrés.

Si $q \equiv 1\,[4]$, -1 est un carré dans $\mathbb{K}$ et donc les formes diagonales $\langle 1, 1\rangle$, $\langle \varepsilon, \varepsilon\rangle$ sont hyperboliques sur $\mathbb{K}$ car de déterminant $1 = (\varepsilon)^2 = -1$ dans $\mathbb{K}^*/(\mathbb{K}^*)^2$ (en dimension 2 les formes quadratiques hyperboliques sont celles de déterminant -1 dans $\mathbb{K}^*/(\mathbb{K}^*)^2$). Les formes $\langle 1, 1\rangle$, $\langle \varepsilon, \varepsilon\rangle$ étant hyperboliques, on a :

$$2.< 1 > = 2.< \varepsilon >= 0_{W(\mathbb{K})}$$

et comme les formes diagonales $\langle 1\rangle$, $\langle \varepsilon\rangle$, $\langle 1, \varepsilon\rangle$ sont anisotropes sur $\mathbb{K}$, ($\langle 1, \varepsilon\rangle$ est anisotrope car de déterminant $\varepsilon \neq -1$ dans $\mathbb{K}^*/(\mathbb{K}^*)^2$, puisque l'un est un carré de $\mathbb{K}$ et l'autre non) il vient :

$$W(\mathbb{K}) = \{0_{W(\mathbb{K})}, < 1 >, < \varepsilon >, < 1, \varepsilon >\}.$$

$W(\mathbb{K})$ est donc un groupe de cardinal 4 dont 3 éléments sont d'ordres 2, d'où $W(\mathbb{K}) \simeq \mathbb{Z}/2 \times \mathbb{Z}/2$ (un groupe de cardinal 4 étant isomorphe à $\mathbb{Z}/2 \times \mathbb{Z}/2$ ou $\mathbb{Z}/4$).

Si $q \equiv 3\,[4]$, -1 n'est pas un carré dans $\mathbb{K}$ et la forme diagonale $\langle 1, \varepsilon\rangle$ est hyperbolique car de déterminant $\varepsilon = -1$ dans $\mathbb{K}^*/(\mathbb{K}^*)^2$ (car -1 et ε ne sont pas des carrés de $\mathbb{K}^*$). D'où, $< 1, \varepsilon >= 0_{W(\mathbb{K})}$, soit

$$< 1 >= - < \varepsilon >$$

et donc $W(\mathbb{K})$ est cyclique engendré par $< 1 >$. De plus, $\langle 1, 1\rangle$ n'est pas hyperbolique sur $\mathbb{K}$ car de déterminant $1 \neq -1$ dans $\mathbb{K}^*/(\mathbb{K}^*)^2$, d'où $2.< 1 >\neq 0_{W(\mathbb{K})}$. Or, $\langle 1, 1, 1, 1\rangle$ est hyperbolique sur tout corps fini $\mathbb{K}$ d'après l'exemple 5.4.1 du chapitre précédent et donc $4.< 1 >= 0_{W(\mathbb{K})}$. Ce qui montre que $< 1 >$ est un élément générateur d'ordre 4 de $W(\mathbb{K})$ et $W(\mathbb{K}) \simeq \mathbb{Z}/4$. □

On va désormais énoncer une propriété universelle, immédiate par définition du groupe de Witt et qui nous sera utile pour définir des morphismes de groupes du type $W(\mathbb{K}) \longrightarrow G$ où G désigne un autre groupe abélien.

Proposition 6.1.5. *Soit $(G, +)$ un groupe abélien et f une fonction définie sur la collection des formes quadratiques régulières sur $\mathbb{K}$ et à valeurs dans G. On suppose que pour toutes formes quadratiques régulières q_1 et q_2 on a :*

- $f(q_1 \perp q_2) = f(q_1) + f(q_2)$
- $f(q_1) = f(q_2)$ *lorsque q_1 et q_2 sont Witt-équivalentes.*

Il existe alors un unique morphisme de groupe $f : W(\mathbb{K}) \longrightarrow G$ tel que :

$$f([q]_W) = f(q), \text{ pour toute forme quadratique régulière } q \text{ sur } \mathbb{K}.$$

Nous allons appliquer la proposition précédente pour voir si l'application dicriminant Δ définit un morphisme de groupes abéliens sur $W(\mathbb{K})$.

Proposition 6.1.6. *Le discriminant $\Delta : W(\mathbb{K}) \longrightarrow \mathbb{K}^*/(\mathbb{K}^*)^2$ défini pour toute forme quadratique régulière q par :*

$$\Delta([q]_W) = (-1)^{\frac{n(n-1)}{2}} det(q), \text{ pour } n = dim(q)$$

est un morphisme de groupe si et seulement si -1 *est un carré de* $\mathbb{K}^*$.

Démonstration. On sait que deux formes quadratiques Witt-équivalentes ont même discriminant. Pour q_1,q_2 deux formes quadratiques régulières telles que $q_1 \overset{W}{\sim} q_2 \iff [q_1]_W = [q_2]_W$, on a donc : $\Delta(q_1) = \Delta(q_2)$ et l'on peut ainsi étendre à $W(\mathbb{K})$ la définition du discriminant, puisque celle-ci ne dépend pas du choix du représentant q de la classe de Witt-équivalence $[q]_W$. Puisque $W(\mathbb{K})$ est engendré par l'ensemble des $< a >$ où a parcout un système de représentants des classes de $\mathbb{K}^*$ modulo $(\mathbb{K}^*)^2$, il suffit de vérifier que Δ préserve la loi de groupe sur les générateurs. Δ est donc un morphisme de groupe si et seulement si :

$$\begin{aligned}
& \Delta(< a > + < b >) = \Delta(< a >)\Delta(< b >) \\
\iff \quad & \Delta(< a, b >) = \Delta(< a >)\Delta(< b >) \\
\iff \quad & (-1)det(\langle a, b\rangle) = det(\langle a\rangle)det(\langle b\rangle) \\
\iff \quad & -ab = ab \text{ dans } \mathbb{K}^*/(\mathbb{K}^*)^2 \\
\iff \quad & -1 \in (\mathbb{K}^*)^2
\end{aligned}$$

D'où le résultat. □

Considérons désormais q_1 et q_2 deux formes quadratiques régulières Witt-équivalentes, alors il existe deux entiers $m, n \in \mathbb{N}$ tels que :

$$\begin{aligned}
q_1 \perp m.\langle 1, -1\rangle \simeq q_2 \simeq n.\langle 1, -1\rangle \implies & \quad dim(q_1) + 2m = dim(q_2) + 2m \\
\implies & \quad dim(q_1) \equiv dim(q_2)\,[2]
\end{aligned}$$

Ainsi, deux formes quadratiques Witt-équivalentes, ont des dimensions égales modulo 2. Par additivité des dimensions et par la propriété universelle du groupe de Witt, il vient :

Proposition 6.1.7. *L'application*

$$e\colon \begin{cases} W(\mathbb{K}) \longrightarrow \mathbb{Z}/2 \\ [q]_W \longmapsto \overline{dim(q)} \end{cases}$$

est bien définie. C'est un morphisme surjectif de groupe appelé ***l'augmentation de*** $W(\mathbb{K})$.

Démonstration. e est clairement un morphisme de groupe. La surjectivité provenant notamment du fait que $e(< 1 >) = \overline{1}$ et $e(< 1, -1 >) = e([0]_W) = \overline{0}$. □

Définition 6.1.1. *Le noyau de l'augmentation est noté* $I(\mathbb{K})$ *et appelé* ***l'idéal fondamental*** *de* $W(\mathbb{K})$*, il représente l'ensemble des classes de Witt-équivalence de formes quadratiques régulières de dimension paire sur* $\mathbb{K}$.

Exemple 6.1.1. *On a naturellement* $I(\mathbb{C}) \simeq \langle 0\rangle$ *puisque*

$$W(\mathbb{C}) = \{< 1 >, [0]_W\}$$

et que $e(< 1 >) = \overline{1}$. *De même* $W(\mathbb{R}) = \{k.< 1 >, k \in \mathbb{Z}\}$ *soit donc :*

$$e(k.< 1 >) = \overline{0} \Longleftrightarrow k \in 2\mathbb{Z} \text{ et } I(\mathbb{R}) \simeq 2.\mathbb{Z}$$

Précédemment, on a eu l'occasion d'étudier la structure des groupes de Witt associés aux corps ci dessous :

1. le corps $\mathbb{C}$.
2. le corps $\mathbb{R}$.
3. les corps finis.

On a pour chaque cas exhibé un isomorphisme entre $W(\mathbb{K})$ et un groupe abélien avec des résultats bien distincts selon les corps étudiés. En revanche, on peut remarquer que les groupes de Witt associés aux corps ci-dessus ne sont jamais isomorphes à un groupe cyclique $\mathbb{Z}/n$, où n est un entier impair. On va alors formaliser cette "*intuition*", pour un corps $\mathbb{K}$ quelconque, de caractéristique différente de 2, en s'appuyant sur le morphisme d'augmentation e.

Proposition 6.1.8. *Il n'existe pas d'entier impair n , tel que le groupe de Witt de $W(\mathbb{K})$ soit isomorphe à $\mathbb{Z}/n$.*

Démonstration. Si on suppose par l'absurde qu'il existe un entier n impair tel que $W(\mathbb{K}) \simeq \mathbb{Z}/n$, alors il existerait un isomorphisme ϕ définit entre $\mathbb{Z}/n$ et $W(\mathbb{K})$ qui par composition avec le morphisme d'augmentation e, donnerait un morphisme surjectif $e \circ \phi$ de $\mathbb{Z}/n$ dans $\mathbb{Z}/2$. Or, définir un morphisme de $\mathbb{Z}/n$ dans $\mathbb{Z}/2$ revient simplement à définir l'image du générateur $\overline{1}$ de $\mathbb{Z}/n$, avec $\overline{1}$ qui est d'ordre n impair dans $\mathbb{Z}/n$. Comme $e \circ \phi$ est un morphisme surjectif (donc non nul) nécessairement $e \circ \phi(\overline{1}) = 1$ avec également,

$$\overline{0} = e \circ \phi(\overline{0}) = e \circ \phi(\overline{n}) = n \times (e \circ \phi)(\overline{1}) = n.\overline{1}$$

Puisque $\overline{1}$ est d'ordre 2 dans $\mathbb{Z}/2$, et que $n.\overline{1} = 0$ dans $\mathbb{Z}/2$, n est alors un multiple de 2, ce qui contredit l'hypothèse n impair et nous donne le résultat attendu. □

Dans la même lignée que le resultat précédent, on a la proposition suivante :

Proposition 6.1.9. *Soit $\mathbb{K}$ un corps et $a, b \in \mathbb{K}^*$ tels que $-ab \notin (\mathbb{K}^*)^2$. Alors, $\langle a, b\rangle$ n'est pas hyperbolique et $< a, b >$ n'est pas d'ordre impair dans le groupe de Witt $W(\mathbb{K})$.*

Afin de démontrer la proposition précédente on va s'appuyer sur le lemme suivant :

Lemme 6.1.2. *La restriction de l'application discriminant définit par :*

$$\Delta\colon \begin{cases} W(\mathbb{K}) \longrightarrow \mathbb{K}^*/(\mathbb{K}^*)^2 \\ [q]_W \longmapsto (-1)^{\frac{dim(q)(dim(q)-1)}{2}} det(q) \end{cases}$$

au sous groupe d'indice 2, $I(\mathbb{K})$ de $W(\mathbb{K})$ est un morphisme de groupe.

Démonstration. Dire que $[q]_W$ appartient à $I(\mathbb{K})$ signifie que $\overline{dim(q)} = 0_{\mathbb{Z}/2}$ et donc $[q]_W$ est la classe de Witt équivalence d'une forme quadratique régulière de dimension paire. Soit donc $[q_1]_W$, $[q_2]_W$ deux éléments de $I(\mathbb{K})$, on a alors : $\Delta([q_1]_W + [q_2]_W) = \Delta([q_1 \perp q_2]_W) = \Delta(q_1 \perp q_2)$ et puisque $[q_1]_W$, $[q_2]_W$ sont dans

I($\mathbb{K}$), il existe des entiers non nuls n, m tels que $\dim(q_1)$=$2n$ et $\dim(q_2)$=$2m$ avec $\dim(q_1 \perp q_2)$=$\dim(q_1)$+$\dim(q_2) = 2(n+m) \equiv 0\,[2]$. Alors :

$$\begin{aligned}\Delta([q_1]_W + [q_2]_W) = & \quad (-1)^{\frac{2(n+m)(2(n+m)-1)}{2}} det(q_1 \perp q_2) \\ = & \quad (-1)^{\frac{2(n+m)(2(n+m)-1)}{2}} det(q_1) det(q_2) \\ = & \quad (-1)^{(n+m)(2(n+m)-1)} det(q_1) det(q_2)\end{aligned}$$

et

$$\begin{aligned}\Delta([q_1]_W)\Delta([q_2]_W) = & \quad (-1)^{\frac{2n(2n-1)}{2}} det(q_1) \times (-1)^{\frac{2m(2m-1)}{2}} det(q_2) \\ = & \quad (-1)^{n(2n-1)} det(q_1) \times (-1)^{m(2m-1)} det(q_2) \\ = & \quad (-1)^{n(2n-1)+m(2m-1)} det(q_1) det(q_2)\end{aligned}$$

Puisque $n(2n-1)+m(2m-1) \equiv n+m\,[2]$ et que $(n+m)(2(n+m)-1) \equiv n+m, [2]$, on a l'égalité $\Delta([q_1]_W + [q_2]_W) = \Delta([q_1]_W)\Delta([q_2]_W)$ et donc la restriction de Δ à I($\mathbb{K}$) est bien un morphisme de groupe. □

On peut maintenant aborder la démonstration de la proposition :

Démonstration. Soit $a, b \in \mathbb{K}^*$ tels que $-ab \notin (\mathbb{K}^*)^2$. Alors, la forme diagonale $\langle a, b\rangle$ n'est pas hyperbolique sur $\mathbb{K}$ car de discriminant égal à $-ab \neq 1$ dans $\mathbb{K}^*/(\mathbb{K}^*)^2$ et donc $< a, b > \neq 0_{W(\mathbb{K})}$ n'est pas d'ordre 1 dans $W(\mathbb{K})$. Supposons que $< a, b >$ est d'ordre $n = 2k+1$ impair dans le groupe $W(\mathbb{K})$ alors,

$$n.< a, b >= (2k+1).< a, b >= 0_{W(\mathbb{K})}$$

et puisque $< a, b >$ appartient à $I(\mathbb{K})$, le lemme précédent donne :

$$\Delta(n.< a, b >) = \Delta(< a, b >)^n = (-ab)^n = (-ab)^{2k}(-ab) = -ab.$$

Comme $n.< a, b >= 0_{W(\mathbb{K})}$ on a $\Delta(n.< a, b >) = \Delta(0) = 1_{\mathbb{K}^*/(\mathbb{K}^*)^2}$, ce qui impose que $-ab = 1$ dans $\mathbb{K}^*/(\mathbb{K}^*)^2$ et donc que $-ab$ est un carré de $\mathbb{K}^*$, absurde. D'où $< a, b >$ n'est pas d'ordre impair dans $W(\mathbb{K})$. □

6.2 Le groupe de Witt-Grothendieck

Notation 6.2.1. *Pour des raisons de commodité, on notera de manière identique $\langle a_1, \ldots, a_n\rangle$ la forme quadratique diagonale et la classe d'isomorphie associée à cette forme quadratique. On n'utilisera la notation $[\langle a_1, \ldots, a_n\rangle]$ pour désigner la classe d'isomorphie, que dans les situations où il y a un risque de confusion.*

L'addition orthogonale $\perp$ permet de munir l'ensemble $FQ(\mathbb{K})$ des classes d'isomorphie de formes quadratiques régulières sur $\mathbb{K}$, d'une structure de monoïde abélien. L'opération :

$$\begin{array}{rcl} FQ(\mathbb{K}) \times FQ(\mathbb{K}) & \longrightarrow & FQ(\mathbb{K}) \\ ([q], [q']) & \longmapsto & [q \perp q'] \end{array}$$

est effectivement une loi interne, associative, commutative et à élément neutre [0] la classe d'isomorphie de la forme nulle. En revanche $(FQ(\mathbb{K}), \perp)$ n'est pas un groupe car aucun élément n'est inversible. En effet, si on suppose que pour q forme quadratique régulière, il existe q' forme quadratique régulière telle que $[q] + [q'] = [q \perp q'] = [0]$, alors $q \perp q' \simeq 0$, ce qui est absurde, en raison par exemple des dimensions. On va alors expliciter une construction qui va permettre de voir le monoïde $FQ(\mathbb{K})$ comme un sous-monoïde d'un groupe abélien qu'il engendre. Interessons nous pour commencer à la construction générale du groupe de Grothendieck $\mathcal{G}(M)$ associé au monoïde abélien $(M, +)$.

6.2.1 Construction du groupe de Grothendieck

Proposition 6.2.1. *Soit $(M, +)$ un monoïde abélien. On définit une relation binaire $\equiv$ sur l'ensembe $M \times M$ par la condition : pour tous (a, b) et (c, d) dans $M \times M$,*

$$(a, b) \equiv (c, d) \Longleftrightarrow \exists e \in M : a + d + e = b + c + e$$

Alors,

- *la relation $\equiv$ est une relation d'équivalence.*
- *$\mathcal{G}(M) = (M \times M)/\equiv$ a une structure de groupe abélien, induit par la structure de monoïde de $M \times M$.*
- *l'application :*
$$i_M : \begin{cases} M \longrightarrow \mathcal{G}(M) \\ a \longmapsto \overline{(a, 0)} \end{cases}$$
est un morphisme de monoïde.
- $\mathcal{G}(M) = \{\overline{(a, b)} = i_M(a) - i_M(b), (a, b) \in M \times M\}$

Le groupe $\mathcal{G}(M)$ est appelé le ***groupe de Grothendieck*** *associé au monoïde M.*

Démonstration. Soit $(M, +)$ un monoïde abélien d'élement neutre noté 0. La relation $\equiv$ est clairement réflexive et symétrique par commutativité sur M. Enfin, supposons $(a_1, b_1) \equiv (a_2, b_2)$ et $(a_2, b_2) \equiv (a_3, b_3)$, alors il existe e et f dans M tels que :

$$a_1 + b_2 + e = b_1 + a_2 + e \text{ et } a_2 + b_3 + f = b_2 + a_3 + f$$

d'où, $a_1 + b_3 + (b_2 + a_2 + e + f) = b_1 + a_3 + (b_2 + a_2 + e + f) \Longrightarrow (a_1, b_1) \equiv (a_3, b_3)$. Ce qui donne la réfléxivité et donc $\equiv$ est bien une relation d'équivalence.

Montrons que $(M \times M/\equiv, +)$ est un groupe abélien. On va commencer par montrer que la relation $\equiv$ est compatible avec la loi $+$ de $M \times M$. Supposons que :

$$(a_1, b_1) \equiv (a_1', b_1') \text{ et } (a_2, b_2) \equiv (a_2', b_2')$$

alors il existe e et f dans M tels que :

$$a_1 + b_1' + e = a_1' + b_1 + e \text{ et } a_2 + b_2' + f = a_2' + b_2 + f$$

et donc $(a_1 + a_2 + b_1' + b_2') + e + f = (a_1' + a_2' + b_1 + b_2) + e + f$ soit :

$$(a_1 + a_2, b_1 + b_2) \equiv (a_1' + a_2', b_1' + b_2')$$

La relation $\equiv$ est compatible avec la loi $+$ du monoïde $M \times M$. On note

$$\overline{(a,b)} = \{(c,d) \in M \times M, (a,b) \equiv (c,d)\}$$

avec donc :

$$\overline{(a,b)} + \overline{(c,d)} = \overline{(a+c, b+d)}$$

ne dépendant pas des choix des représentants. Ce qui précède permet de munir $M \times M/\equiv$ de cette même loi $+$ et donc d'une structure de monoïde commutatif d'élément neutre $\overline{(0,0)}$. L'opposé d'un élément $\overline{(a,b)}$ est l'élément $\overline{(b,a)}$ puisque $(a+b, a+b) \equiv (0,0)$. On note $-\overline{(a,b)}$ l'opposé de $\overline{(a,b)}$. D'où $(M \times M/\equiv, +)$ est un groupe abélien.

L'application i_M est clairement un morphisme de monoïde puisque :

$$i_M(a+b) = \overline{(a+b,0)} = \overline{(a,0)} + \overline{(b,0)} = i_M(a) + i_M(b).$$

Enfin,

$$\begin{aligned}
\mathcal{G}(M) = & \quad \{\overline{(a,b)}, (a,b) \in M \times M\} \\
= & \quad \{\overline{(a,0)} + \overline{(0,b)}, (a,b) \in M \times M\} \\
= & \quad \{\overline{(a,0)} - \overline{(b,0)}, (a,b) \in M \times M\} \\
= & \quad \{i_M(a) - i_M(b), (a,b) \in M \times M\}
\end{aligned}$$

□

Définition 6.2.1. *Le groupe de Witt-Grothendieck associé au monoïde abélien $FQ(\mathbb{K})$ est noté $\widehat{W}(\mathbb{K})$ et appelé* ***le groupe de Witt-Grothendieck*** *de $\mathbb{K}$. On a donc :*

$$\widehat{W}\mathbb{K} = \{\overline{([q],0)} - \overline{([q'],0)}, ([q],[q']) \in FQ(\mathbb{K}) \times FQ(\mathbb{K})\}$$

Le théorème de simplification de Witt va nous permettre de montrer que l'application $i_{FQ(\mathbb{K})}$ injecte $FQ(\mathbb{K})$ dans $\widehat{W}(\mathbb{K})$ et donc de voir $FQ(\mathbb{K})$ comme un sous-monoïde de $\widehat{W}(\mathbb{K})$.

Proposition 6.2.2. *Le morphisme $i_{FQ(\mathbb{K})}$ est injectif.*

Démonstration. Soit q et q' telles que $i_{FQ(\mathbb{K})}([q]) = i_{FQ(\mathbb{K})}([q'])$. Alors :

$$\begin{aligned}
\overline{([q],0)} = \overline{([q'],0)} \iff & \quad ([q],0) \equiv ([q'],0) \\
\iff & \quad \exists q'' \in FQ(\mathbb{K}),\ [q] + 0 + [q''] = [q'] + 0 + [q''] \\
\iff & \quad \exists q'' \in FQ(\mathbb{K}),\ [q \perp q''] = [q' \perp q''] \\
\iff & \quad \exists q'' \in FQ(\mathbb{K}),\ q \perp q'' \simeq q' \perp q'' \\
\iff & \quad q \simeq q' \\
\iff & \quad [q] = [q']
\end{aligned}$$

D'où l'injectivité de $i_{FQ(\mathbb{K})}$

□

Remarque 6.2.1. *Tout élément de $\widehat{W}(\mathbb{K})$ s'écrit $i_{FQ(\mathbb{K}}([q]) - i_{FQ(\mathbb{K}}([q'])$, mais cette écriture n'est pas unique. En effet,*

$$\begin{aligned}
& i_{FQ(\mathbb{K}}([q]) - i_{FQ(\mathbb{K}}([q']) = i_{FQ(\mathbb{K}}([q_1]) - i_{FQ(\mathbb{K}}([q'_1]) \\
\iff \quad & i_{FQ(\mathbb{K}}([q]) + i_{FQ(\mathbb{K}}([q'_1]) = i_{FQ(\mathbb{K}}([q_1]) + i_{FQ(\mathbb{K}}([q']) \\
\iff \quad & i_{FQ(\mathbb{Q}}([q] + [q'_1]) = i_{FQ(\mathbb{Q}}([q_1] + [q']) \\
\iff \quad & i_{FQ(\mathbb{Q}}([q \perp q'_1]) = i_{FQ(\mathbb{Q}}([q_1 \perp q']) \\
\iff \quad & [q \perp q'_1] = [q_1 \perp q'] \\
\iff \quad & q \perp q'_1 \simeq q_1 \perp q'
\end{aligned}$$

Remarque 6.2.2. *On a vu que tout élément de $\widehat{W}(\mathbb{K})$ s'écrivait sous la forme $i_{FQ(\mathbb{K}}([q]) - i_{FQ(\mathbb{K}}([q'])$, on pourra alors par injectivité de $i_{FQ(\mathbb{K}}$ et par commodité de notation, écrire cet élément $[q] - [q']$. L'élément $\overline{([q], 0)}$ sera noté $[q]$ dans $\widehat{W}(\mathbb{K})$ et son opposé $\overline{(0, [q])}$ sera noté $-[q]$. Ceci n'est qu'une notation car $FQ(\mathbb{K})$ n'étant qu'un monoïde, aucun élément n'est inversible et donc l'opération " $-$ " n'a pas de sens dans $FQ(\mathbb{K})$.*

Comme pour le groupe $W(\mathbb{K})$, l'étude du groupe $\widehat{W}(\mathbb{K})$ sera facilitée par la connaissance d'une partie génératrice. La proposition suivante en exhibe une. En identifiant $[q]$ et $i_{FQ(\mathbb{K})}([q])$ via l'injectivité de $i_{FQ(\mathbb{K})}$, on a :

Proposition 6.2.3. ***Partie génératrice de*** $\widehat{W}(\mathbb{K})$
Pour a parcourant un système de représentants des classes de $\mathbb{K}^*/(\mathbb{K}^*)^2$, l'ensemble des éléments $i_{FQ(\mathbb{Q})}(\langle a \rangle)$ constitue une partie génératrice de $\widehat{W}(\mathbb{K})$. Par l'identification usuelle, l'ensemble des classes d'isomorphie $\langle a \rangle$ où a parcourt un système de représentants des classes de $\mathbb{K}^*/(\mathbb{K}^*)^2$ est une partie génératrice de $\widehat{W}(\mathbb{K})$.

Démonstration. Soit q une forme quadratique régulière de dimension n. Par diagonalisation il existe n scalaires $a_1, \ldots, a_n$ tels que $q \simeq \langle a_1, \ldots, a_n \rangle$. Alors,

$$[q] = \langle a_1, \ldots, a_n \rangle = \langle a_1 \rangle \perp \ldots \perp \langle a_n \rangle = \langle a_1 \rangle + \ldots + \ldots \langle a_n \rangle \text{ dans } FQ(\mathbb{K}).$$

Ainsi, tout élément $[q]$ s'écrit comme somme d'élément de la forme $\langle a \rangle$ où l'on a choisit dans chaque classe de $\mathbb{K}^*/(\mathbb{K}^*)^2$, un représentant a. Tout élément $i_{FQ(\mathbb{K})}([q])$ s'écrit donc comme somme d'élément $i_{FQ(\mathbb{K})}(\langle a \rangle)$ ce qui permet de conclure car tout élément de $\widehat{W}(\mathbb{K})$ s'écrit sous la forme $i_{FQ(\mathbb{K})}([q]) - i_{FQ(\mathbb{K})}([q'])$. □

En identifiant $FQ(\mathbb{K})$ avec $i_{FQ(\mathbb{K})}(FQ(\mathbb{K}))$ et $-FQ(\mathbb{K})$ avec $-i_{FQ(\mathbb{K})}(FQ(\mathbb{K}))$, on a $FQ(\mathbb{K}) \subset \widehat{W}(\mathbb{K})$ et $-FQ(\mathbb{K}) \subset \widehat{W}(\mathbb{K})$ et donc :

$$FQ(\mathbb{K}) \cup (-FQ(\mathbb{K})) \subset \widehat{W}(\mathbb{K}).$$

On va s'appuyer sur la connaissance d'une partie génératrice de $\widehat{W}(\mathbb{K})$ pour étudier dans quel cas l'inclusion réciproque est vraie.

Proposition 6.2.4. *$FQ(\mathbb{K}) \cup (-FQ(\mathbb{K})) = \widehat{W}(\mathbb{K})$ si et seulement si le corps $\mathbb{K}$ est quadratiquement clos.*

Démonstration. Si $\mathbb{K}$ est quadratiquement clos, $\mathbb{K} = \mathbb{K}^2$ et donc $\widehat{W}(\mathbb{K})$ est engendré par la classe $\langle 1\rangle$ qui représente en fait l'élément $\overline{(\langle 1\rangle, 0)}$ de $\widehat{W}(\mathbb{K})$. Supposons qu'il soit cyclique, alors il existe un $n \in \mathbb{N}^*$ tel que $n.\langle 1\rangle = 0_{\widehat{W}(\mathbb{K})}$. Or, par injectivité de $i_{FQ(\mathbb{K})}$, cela revient à $n.\langle 1\rangle \simeq 0$ en termes de formes quadratiques, absurde en raison des dimensions. Ainsi, si $\mathbb{K}$ est quadratiquement clos, $\widehat{W}(\mathbb{K}) \simeq \mathbb{Z}$ car monogène, non cyclique. Tout éléménent de $\widehat{W}(\mathbb{K})$ s'écrit alors $k.\langle 1\rangle$ pour $k \in \mathbb{Z}$. Si $k \geq 0$, alors $k.\langle 1\rangle \in FQ(\mathbb{K})$, sinon $k.\langle 1\rangle = -(-k)\langle 1\rangle$ et $k.\langle 1\rangle \in -FQ(\mathbb{K})$.

Supposons désormais que $\mathbb{K}$ n'est pas quadratiquement clos. Alors, il existe au moins deux scalaires $a, b \in \mathbb{K}^*$ qui ne sont pas égaux modulo les carrés de $\mathbb{K}^*$. Pour de tels scalaires, supposons que $\langle a\rangle - \langle b\rangle \in FQ(\mathbb{K})$, alors il existe $[q] \in FQ(\mathbb{K})$ tel que :

$$\langle a\rangle - \langle b\rangle = [q]$$

Alors $\langle a\rangle = [q] + \langle b\rangle$ et en termes de formes quadratiques $\langle a\rangle \simeq \langle b\rangle \perp q$. En raison des dimensions, on a nécessairement $q = 0$ et $\langle a\rangle \simeq \langle b\rangle$, ce qui est absurde car $a \neq b$ dans $\mathbb{K}^*/(\mathbb{K}^*)^2$. De même, supposons que $\langle a\rangle - \langle b\rangle \in -FQ(\mathbb{K})$, alors il existe $[q] \in FQ(\mathbb{K})$ tel que :

$$\langle a\rangle - \langle b\rangle = -[q]$$

Alors $\langle b\rangle = [q] + \langle a\rangle$ et on conclut comme précédemment. D'où si $\mathbb{K}$ n'est pas quadratiquement clos $FQ(\mathbb{K}) \cup (-FQ(\mathbb{K})) \neq \widehat{W}(\mathbb{K})$, ce qui achève de montrer le résultat. □

De la démonstration précédente, on déduit la structure du groupe $\widehat{W}(\mathbb{C})$:

Proposition 6.2.5. *Pour tout corps $\mathbb{K}$ quadratiquement clos, $\widehat{W}(\mathbb{K}) \simeq \mathbb{Z}$ et donc $\widehat{W}(\mathbb{C}) \simeq \mathbb{Z}$.*

La structure de $\widehat{W}(\mathbb{R})$ est elle aussi facilement caractérisable :

Proposition 6.2.6. *Le groupe $\widehat{W}(\mathbb{R})$ est engendré par $\langle 1\rangle$ et $\langle -1\rangle$. Il est isomorphe à $\mathbb{Z}^2$.*

Démonstration. $\widehat{W}(\mathbb{R})$ est clairement engendré par $\langle 1\rangle$ et $\langle -1\rangle$ de part la proposition 6.2.3. Tout élément de $\widehat{W}(\mathbb{R})$ s'écrit alors $k.\langle 1\rangle + l.\langle -1\rangle$ pour $(k, l) \in \mathbb{Z}^2$. On va montrer que l'application :

$$\begin{array}{rcl} \mathbb{Z}^2 & \longrightarrow & \widehat{W}(\mathbb{K}) \\ (k,l) & \longmapsto & k.\langle 1\rangle + l.\langle -1\rangle \end{array}$$

est un isomorphisme. Il s'agit clairement d'un morphisme, il suffit de montrer l'injectivité, la surjectivité étant immédiate. Supposons que $k.\langle 1\rangle + l.\langle -1\rangle = 0$. Si $k \leq 0$ et $l \leq 0$ alors $-k \geq 0$ et $-l \geq 0$ et on a aussi $(-k).\langle 1\rangle + (-l).\langle -1\rangle = 0$. Ainsi quitte à considérer $-k$ et $-l$ on peut supposer que $k \geq 0$. Si $k, l \geq 0$ alors :

$$k.\langle 1\rangle + l.\langle -1\rangle = 0 \Longrightarrow k.\langle 1\rangle \perp l.\langle -1\rangle \simeq 0 \text{ en termes de formes quadratiques.}$$

Absurde, à cause des dimensions. Si $l \leq 0$, $k.\langle 1\rangle = -l.\langle -1\rangle$ avec $-l \geq 0$. Alors $k.\langle 1\rangle \simeq (-l).\langle -1\rangle$ en terme de formes quadratiques réelles, absurde, l'une étant définie positive, l'autre étant définie négative. □

Afin d'étudier la structure du groupe de Witt-Grothendieck pour les corps finis, on va avoir besoin de définir des morphismes ayant pour ensemble de départ $\widehat{W}(\mathbb{K})$, les deux propositions suivantes vont nous le permettre.

Proposition 6.2.7. ***Propriété unviverselle du groupe de Grothendieck*** *Soit G un groupe abélien et $(M,+)$ un monoïde abélien. Soit un morphisme de monoïde $f : FQ(\mathbb{K}) \longrightarrow G$, alors f se factorise de manière unique en un morphisme de groupe $\overline{f} : \mathcal{G}(M) \longrightarrow G$ tel que $\overline{f} \circ i_M = f$.*

Démonstration. On définit $\overline{f}$ par :

$$\overline{f}: \begin{cases} \mathcal{G}(M) \longrightarrow G \\ \overline{(a,b)} \longmapsto f(a) - f(b) \end{cases}$$

On commence par vérifier que cette définition ne dépend pas des choix des représentants. Supposons que $\overline{(a,b)} = \overline{(c,d)}$, alors il existe $e \in M$ tel que :

$$\begin{array}{rc} & a+d+e = b+c+e \\ \Longrightarrow & f(a)+f(d)+f(e) = f(b)+f(c)+f(e) \\ \Longrightarrow & \overline{f}(\overline{(a,b)}) = f(a)-f(b) = f(c)-f(d) = \overline{f}(\overline{(c,d)}) \end{array}$$

La définition de $\overline{f}$ ne dépend pas du choix des représentants. De plus pour $\overline{(a,b)}$ et $\overline{(c,d)}$ dans $\mathcal{G}(M)$ on a :

$$\begin{array}{rcc} \overline{f}(\overline{(a,b)} + \overline{(c,d)}) = & & \overline{f}(\overline{(a+c,b+d)}) \\ = & & f(a+c) - f(b+d) \\ = & & (f(a)-f(b)) + (f(c)-f(d)) \\ = & & \overline{f}(\overline{(a,b)}) + \overline{f}(\overline{(c,d)}) \end{array}$$

ce qui montre que $\overline{f}$ est bien un morphisme de groupe. De plus $\overline{f}(\overline{(a,0)}) = f(a)$, pour tout a dans M montre bien que $\overline{f} \circ i_M = f$. Enfin, si on suppose qu'il existe un autre morphisme de groupe g tel que $g \circ i_M = f$, on a nécessairement :

$$\begin{array}{rcc} g(\overline{(a,b)}) = & & g(\overline{(a,0)} + \overline{(0,b)}) \\ = & & g(\overline{(a,0)}) - g(\overline{(b,0)}) \\ = & & g(i_M(a)) - g(i_M(b)) \\ = & & f(a) - f(b) \\ = & & \overline{f}(\overline{(a,b)}) \end{array}$$

et $g = \overline{f}$, ce qui achève de montrer cette proposition. □

On en déduit la propriété universelle du groupe de Witt-Grothendieck :

Proposition 6.2.8. *Soit $(G,+)$ un groupe abélien et f une fonction définie sur la collection des formes quadratiques régulières sur $\mathbb{K}$ et à valeurs dans G. On suppose que pour toutes formes quadratiques régulières q_1 et q_2 on a :*

- $f(q_1 \perp q_2) = f(q_1) + f(q_2)$
- $f(q_1) = f(q_2)$ *lorsque q_1 et q_2 sont équivalentes.*

Il existe alors un unique morphisme de groupe $\widehat{f} : \widehat{W}(\mathbb{K}) \longrightarrow G$ tel que :

$$\widehat{f}([q]) = f(q), \text{ pour toute forme quadratique régulière } q \text{ sur } \mathbb{K}.$$

Exemple 6.2.1. *Pour deux formes quadratiques régulières q et q', on a :*

$$det(q\perp q') = det(q)det(q') \text{ et } dim(q\perp q') = dim(q)dim(q')$$

avec pour $q \simeq q'$,

$$det(q) = det(q') \text{ et } dim(q) = dim(q').$$

Ainsi, par la propriété universelle du groupe de Witt-Grothendieck, les applications "dimension" et "déterminant" induisent deux morphismes de groupes :

$$dim : \widehat{W}(\mathbb{K}) \longrightarrow \mathbb{Z} \text{ et } det : \widehat{W}(\mathbb{K}) \longrightarrow \mathbb{K}^*/(\mathbb{K}^*)^2.$$

Tout élément x de $\widehat{W}(\mathbb{K})$ s'écrivant $[q_1] - [q_2]$, pour q_1 et q_2 deux formes quadratiques régulières, on a :

$$dim(x) = dim([q_1] - [q_2]) = dim(q_1) - dim(q_2)$$

et la valeur de $dim(x)$ ne dépend pas de l'écriture de x sous la forme $[q_1] - [q_2]$. En effet, si $x = [q_1] - [q_2] = [q'_1] - [q'_2]$ alors on a vu que $q_1\perp q'_2 \simeq q'_1\perp q_2$ et donc $dim(q_1) - dim(q_2) = dim(q'_1) - dim(q'_2) = dim(x)$.

On va utiliser les deux applications *dim* et *det* définies dans l'exemple précédent, pour établir la structure du groupe de Witt-Grothendieck dans le cadre des corps finis. Nous aurons besoin d'utiliser le lemme suivant :

Lemme 6.2.1. *Soit $\mathbb{K}$ un corps fini. L'application suivante est un morphisme de groupe surjectif :*

$$f\colon \begin{cases} \widehat{W}(\mathbb{K}) \longrightarrow \mathbb{Z} \times \mathbb{K}^*/(\mathbb{K}^*)^2 \\ x \longmapsto (dim(x), det(x)) \end{cases}$$

Démonstration. Soit un élément (n, δ) de $\mathbb{Z} \times \mathbb{K}^*/(\mathbb{K}^*)^2$. On commence par supposer $n = 2k + 1$ impair. Alors,

$$dim(n.\langle\delta\rangle) = n \text{ et } det(n.\langle\delta\rangle) = det(\langle\delta\rangle)^n = \delta^{2p+1} = \delta \text{ dans } \mathbb{K}^*/(\mathbb{K}^*)^2.$$

Ainsi, (n, δ) est atteint par l'élément $n.\langle\delta\rangle$ de $\widehat{W}(\mathbb{K})$. Si n est pair, alors $n - 1$ est impair et la décomposition $n = (n - 1) + 1$ donne

$$dim((n-1).\langle\delta\rangle + \langle 1\rangle) = dim((n-1).\langle\delta\rangle) + dim(\langle 1\rangle) = (n-1) + 1 = n.$$

De plus, $det((n-1).\langle\delta\rangle + \langle 1\rangle) = det(\langle\delta\rangle)^{n-1}det(\langle 1\rangle) = \delta^{n-1} = \delta$ dans $\mathbb{K}^*/(\mathbb{K}^*)^2$ puisque $n - 1$ est impair. Ici encore (n, δ) est atteint, mais cette fois-ci par l'élément $(n-1).\langle\delta\rangle + \langle 1\rangle$ de $\widehat{W}(\mathbb{K})$. D'où la surjectivité. □

Proposition 6.2.9. Structure du groupe de Witt-Grothendieck $\widehat{W}(\mathbb{K})$, pour $\mathbb{K}$ corps fini.
On suppose que $\mathbb{K}$ est un corps fini de cardinal q et soit ε un représentant de la classe des non carrés de $\mathbb{K}^*$. Alors, $\widehat{W}(\mathbb{K}) \simeq \mathbb{Z} \times \mathbb{Z}/2$ pour $q \equiv 1\,[4]$ ou $q \equiv 3\,[4]$.

Démonstration. Pour montrer que $\widehat{W}(\mathbb{K}) \simeq \mathbb{Z} \times (\mathbb{Z}/2)$, on va prouver que le morphisme f du lemme 6.2.1 est aussi injectif dans le cadre des corps finis. Considérons un élément x dans $\widehat{W}(\mathbb{K})$ qui se trouve être également dans $Ker(f)$ et montrons que $x = 0_{\widehat{W}(\mathbb{K})}$. D'après l'écriture générique (non unique) des éléments du groupe de Witt-Grothendieck de $\mathbb{K}$, $x = [q_1] - [q_2]$ (pour q_1, q_2 deux formes régulières sur $\mathbb{K}$) et donc x étant dans le noyau de f, il vient :

$$dim([q_1]-[q_2]) = dim(q_1) - dim(q_2) = 0 \Longrightarrow dim(q_1) = dim(q_2)$$

et

$$det([q_1]-[q_2]) = det(q_1)det(q_2)^{-1} = 1 \Longrightarrow det(q_1) = det(q_2) \text{ dans } \mathbb{K}^*/(\mathbb{K}^*)^2$$

si bien que d'après la caractérisation des formes quadratiques régulières sur les corps finis on a $q_1 \simeq q_2$ soit $[q_1] = [q_2]$ et donc $x = 0$. Ce qui prouve que f est injectif et donne l'isomorphisme annoncé. □

6.2.2 L'idéal fondamental du groupe de Witt-Grothendieck

Définition 6.2.2. *Le noyau du morphisme de groupes dim* : $\widehat{W}(\mathbb{K}) \longrightarrow \mathbb{Z}$ *est appelé* ***l'idéal fondamental*** *de* $\widehat{W}(\mathbb{K})$ *et noté* $\widehat{I}(\mathbb{K})$.

Tout élément de $\widehat{W}(\mathbb{K})$ s'écrivant (de manière non unique) $[q_1]-[q_2]$, où q_1 et q_2 désignent des formes quadratiques régulières, les éléments de $\widehat{I}(\mathbb{K})$ sont alors les éléments $[q_1]-[q_2]$ où q_1 et q_2 sont de même dimension.

La proposition qui suit est très utile, elle permettra de faire le lien entre la structure du groupe de Witt et la structure du groupe de Witt-Grothendieck d'un corps $\mathbb{K}$. Par la suite, on montrera en effet que $I(\mathbb{K}) \simeq \widehat{I}(\mathbb{K})$, la proposition suivante nous fournira alors un moyen pour déterminer la structure du groupe $\widehat{W}(\mathbb{K})$ à l'aide de la connaissance du sous-groupe d'indice 2, $I(\mathbb{K})$ de $W(\mathbb{K})$.

Proposition 6.2.10. *Le morphisme "dimension" est surjectif et donne une suite exacte de groupes abéliens :*

$$\widehat{I}(\mathbb{K}) \hookrightarrow \widehat{W}(\mathbb{K}) \twoheadrightarrow \mathbb{Z}$$

qui est scindée. Ainsi, $\widehat{W}(\mathbb{K}) \simeq \mathbb{Z} \times \widehat{I}(\mathbb{K})$

Démonstration. La surjectivité du morphisme dimension est immédiate puisque pour tout k dans $\mathbb{Z}$, on a : $dim(k.\langle 1\rangle) = k$. Ceci donne alors naturellement la suite exacte courte :

$$\widehat{I}(\mathbb{K}) \hookrightarrow \widehat{W}(\mathbb{K}) \twoheadrightarrow \mathbb{Z}$$

Montrons désormais qu'elle est scindée. On cherche un morphisme

$$\phi : \mathbb{Z} \longrightarrow \widehat{W}(\mathbb{K}) \text{ tel que } \dim \circ \phi = Id_{\mathbb{Z}}$$

On considère alors, l'application ϕ définie par :

$$\phi\colon \begin{cases} \mathbb{Z} \longrightarrow \widehat{W}(\mathbb{K}) \\ k \longmapsto k.\langle 1\rangle \end{cases}$$

qui vérifie bien $\dim \circ \phi = Id_{\mathbb{Z}}$. Puisque tous les groupes considérés sont abéliens, ce scindage naturel nous donne alors $\widehat{W}(\mathbb{K}) \simeq \mathbb{Z} \times \widehat{I}(\mathbb{K})$ (cf. [2] pages 22,23). □

6.3 Identification de $I(\mathbb{K})$ avec $\widehat{I}(\mathbb{K})$

L'objectif de cette partie est d'établir l'isomorphisme entre $I(\mathbb{K})$ et $\widehat{I}(\mathbb{K})$ qui assurera via la dernière proposition de la partie précédente un passage entre les structures de $W(\mathbb{K})$ et $\widehat{W}(\mathbb{K})$. Pour ce faire, nous devrons au préalable étudier l'application canonique π qui associe à $[q]$ dans $\widehat{W}(\mathbb{K})$, l'élément $[q]_W$ dans $W(\mathbb{K})$.

6.3.1 La projection canonique

Définition 6.3.1. *L'application,*

$$\pi\colon \begin{cases} \widehat{W}(\mathbb{K}) \longrightarrow W(\mathbb{K}) \\ [q] \longmapsto [q]_W \end{cases}$$

est bien définie, c'est un morphisme de groupe appelé la ***projection canonique*** *de $\widehat{W}(\mathbb{K})$ dans $W(\mathbb{K})$.*

Démonstration. On note f définie sur la collection des formes quadratiques régulières par $f(q) = [q]_W$. Alors, on a naturellement :

- $f(q_1 \perp q_2) = [q_1 \perp q_2]_W = [q_1]_W + [q_2]_W$, pour q_1,q_2 deux formes quadratiques régulières.
- $f(q_1) = [q_1]_W = [q_2]_W = f(q_2)$ si q_1 et q_2 sont équivalentes.

De part la propriété universelle du groupe de Witt-Grothendieck, il existe un unique morphisme de groupe $\widehat{f} : \widehat{W}(\mathbb{K}) \longrightarrow W(\mathbb{K})$ tel que $\widehat{f}([q]) = f(q)$. Alors, $\pi = \widehat{f}$ est bien définie. □

Proposition 6.3.1. *Le noyau de la projection π est le sous-groupe de $\widehat{W}(\mathbb{K})$ engendré par $\langle 1, -1\rangle$. Il est isomorphe à $\mathbb{Z}$*

Démonstration. Montrons pour commencer que $\langle 1, -1\rangle \in Ker(\pi)$. Puisque la forme quadratique $\langle 1, -1\rangle$ est hyperbolique, sa classe de Witt-équivalence est nulle et donc $\pi(\langle 1, -1\rangle) =< 1, -1 >= 0$, soit $\langle 1, -1\rangle \in Ker(\pi)$, et donc $\mathbb{Z}.\langle 1, -1\rangle \subset Ker(\pi)$.

Montrons que $Ker(\pi) \subset \mathbb{Z}.\langle 1, -1\rangle$. Soit $x = [q_1] - [q_2] \in \widehat{W}(\mathbb{K})$ tel que $\pi([q_1] - [q_2]) = 0$. Il vient alors $[q_1]_W - [q_2]_W = 0$ et $[q_1]_W = [q_2]_W$ et donc q_1 et q_2 sont Witt-équivalentes. Ainsi, il existe m, n deux entiers tels que :

$$q_1 \perp m.\langle 1, -1\rangle \simeq q_2 \perp n.\langle 1, -1\rangle$$

soit dans $\widehat{W}(\mathbb{K})$, $[q_1] + m.\langle 1, -1\rangle = [q_2] + n.\langle 1, -1\rangle$. Ceci implique que :

$$[q_1] - [q_2] = (n - m).\langle 1, -1\rangle \in \mathbb{Z}.\langle 1, -1\rangle$$

D'où $Ker(\pi) = \mathbb{Z}.\langle 1, -1\rangle$.

Or, $\langle 1, -1\rangle$ n'est pas d'ordre fini dans $\widehat{W}(\mathbb{K})$, car sinon il existerait un entier non nul n tel que $n.\langle 1, -1\rangle = 0_{\widehat{W}(\mathbb{K})}$ et par application du morphisme dimension on aurait :

$$0 = dim(0) = dim(n.\langle 1, -1\rangle) = 2n$$

soit $n = 0$, absurde. D'où $Ker(\pi) \simeq \mathbb{Z}$. □

On sait que tout élément de $\widehat{W}(\mathbb{K})$ s'écrit $[q_1]-[q_2]$ avec q_1 et q_2 deux formes quadratiques régulières sur $\mathbb{K}$. Le défaut de cette écriture est sa non unicité, ici on va s'appuyer sur la proposition précédente pour donner une représentation des éléments de $\widehat{W}(\mathbb{K})$. avec unicité d'écriture. Cette écriture sera d'ailleurs très similaire à la décomposition de Witt d'une forme quadratique :

Corollaire 6.3.1. *Tout élément de $\widehat{W}(\mathbb{K})$ s'écrit de manière unique :*

$$[q]+k.\langle 1,-1\rangle,$$

où $k\in\mathbb{Z}$ et q est une forme quadratique régulière anisotrope.

Démonstration. Soit $x\in\widehat{W}(\mathbb{K})$. Alors il existe deux formes quadratiques régulières q_1, q_2 telles que $x=[q_1]-[q_2]$. Par décomposition de Witt, il existe $n_1,n_2\in\mathbb{N}$ et $q_{a,1},q_{a,2}$ anisotropes tels que :

$$q_1\simeq n_1.\langle 1,-1\rangle\perp q_{a,1} \text{ et } q_2\simeq n_2.\langle 1,-1\rangle\perp q_{a,2}$$

Dans $\widehat{W}(\mathbb{K})$, on a :

$$\begin{aligned}[q_1]-[q_2] &= [n_1.\langle 1,-1\rangle\perp q_{a,1}]-[n_2.\langle 1,-1\rangle\perp q_{a,2}]\\ &= n_1.\langle 1,-1\rangle+[q_{a,1}]-n_2.\langle 1,-1\rangle-[q_{a,2}]\\ &= (n_1-n_2).\langle 1,-1\rangle+[q_{a,1}]-[q_{a,2}]\end{aligned}$$

avec $(n_1-n_2).\langle 1,-1\rangle\in\mathbb{Z}.\langle 1,-1\rangle$. De plus, on a dans $W(\mathbb{K})$:

$$\begin{aligned}\pi([q_{a,1}]-[q_{a,2}]) &= [q_{a,1}]_W-[q_{a,2}]_W\\ &= [q_{a,1}\perp(-q_{a,2})]_W\\ &= [\phi]_W\end{aligned}$$

où ϕ désigne la partie anisotrope de la forme quadratique $q_{a,1}\perp(-q_{a,2})$ qui n'est pas nécessairement anisotrope. D'où :

$$\pi([q_{a,1}]-[q_{a,2}])=\pi([\phi]) \text{ et } \pi([q_{a,1}]-[q_{a,2}]-[\phi])=0$$

et donc il existe $p\in\mathbb{Z}$ tel que :

$$[q_{a,1}]-[q_{a,2}]=[\phi]+p.\langle 1,-1\rangle$$

soit au final $x=[q_1]-[q_2]=[\phi]+(n_1-n_2+p).\langle 1,-1\rangle$ qui est l'écriture requise.

Montrons l'unicité de cette écriture. Soit $(k,l)\in\mathbb{Z}^2$ et q,q' anisotropes tels que $x=[q]+k.\langle 1,-1\rangle=[q']+l.\langle 1,-1\rangle$. Alors dans $\widehat{W}(\mathbb{K})$, via le morphisme π, on a :

$$\pi([q]+k.\langle 1,-1\rangle)=\pi([q']+l.\langle 1,-1\rangle)\Longrightarrow [q]_W=[q']_W\ .$$

Deux formes quadratiques anisotropes et Witt-équivalentes sont équivalentes, alors $q\simeq q'$ et $[q]=[q']$ dans $\widehat{W}(\mathbb{K})$. Il vient alors :

$$k.\langle 1,-1\rangle=l.\langle 1,-1\rangle\Longrightarrow (k-l).\langle 1,-1\rangle=0_{\widehat{W}(\mathbb{K})}.$$

et par le morphisme dimension, $0=dim(0)=dim((k-l).\langle 1,-1\rangle)=2(k-l)$, soit $k=l$, ce qui donne l'unicité d'écriture. □

On est désormais en capacité de montrer le résultat important de cette partie : l'identification des deux idéaux fondamentaux.

Proposition 6.3.2. *$\widehat{I}(\mathbb{K})$ est constitué des éléments de la formes $[q]-n.\langle 1,-1\rangle$ avec q anisotrope et $dim(q)=2n$. De cette écriture découle, $I(\mathbb{K})\simeq\widehat{I}(\mathbb{K})$.*

Démonstration. Soit $x\in\widehat{I}(\mathbb{K})$, alors x s'écrit de manière unique $[q]+k\langle 1,-1\rangle$ avec q anisotrope et $k\in\mathbb{Z}$. Alors :

$$\begin{aligned} x\in\widehat{I}(\mathbb{K}) &\iff dim(x)=0\\ &\iff dim([q])+k\times dim(\langle 1,-1\rangle)=0\\ &\iff dim([q])+2k=0\\ &\iff k=-\frac{1}{2}dim([q])\\ &\iff k=-\frac{1}{2}dim(q) \end{aligned}$$

Tout élément de $\widehat{I}(\mathbb{K})$ s'écrit donc de manière unique $[q]-n.\langle 1,-1\rangle$ où

$n=\dfrac{1}{2}dim(q)$.

Définissons les applications :

$$f\colon\begin{cases} I(\mathbb{K})\longrightarrow\widehat{I}(\mathbb{K})\\ [q_a]_W\longmapsto[q_a]-\dfrac{1}{2}dim(q_a)\langle 1,-1\rangle \end{cases}$$

où q_a désigne une forme quadratique anisotrope de dimension paire et

$$g\colon\begin{cases} \widehat{I}(\mathbb{K})\longrightarrow I(\mathbb{K})\\ [q_a]-\dfrac{1}{2}dim(q_a)\langle 1,-1\rangle\longmapsto[q_a]_W \end{cases}$$

où q_a désigne une forme quadratique anisotrope.

On va commencer par montrer que les applications sont bien définies, puis qu'il s'agit de morphismes de groupes, réciproques l'un de l'autre. Tout élément $x\in W(\mathbb{K})$ s'écrit de manière unique comme la classe de Witt-équivalence d'une forme quadratique anisotrope et donc tout élément de $I(\mathbb{K})$ s'écrit de manière unique comme la classe de Witt-équivalence d'une forme quadratique anisotrope de dimension paire.

Ainsi, f est bien définie car ne dépend pas d'une choix du représentant q_a de la classe $[q_a]_W$. En effet, si q_a,q_b sont deux formes quadratiques anisotropes de dimension paire telles que $[q_a]_W=[q_b]_W$, alors $q_a\simeq q_b\Longrightarrow[q_a]=[q_b]$ dans $\widehat{W}(\mathbb{K})$ et aussi $dim(q_a)=dim(q_b)$. D'où naturellement $f([q_a]_W)=f([q_b]_W)$.

Tout élément de $\widehat{I}(\mathbb{K})$ s'écrit de manière unique $[q_a]-n.\langle 1,-1\rangle$ où q_a anisotrope et $dim(q_a)=2n$. Supposons que $[q_a]=[q_b]$ dans $\widehat{W}(\mathbb{K})$, alors en particulier $q_a\simeq q_b$ en termes de formes quadratiques et donc q_a et q_b sont en particulier Witt-équivalentes et $[q_a]_W=[q_b]_W$ dans $W(\mathbb{K})$, ce qui montre que g est bien définie.

Montrons que f est un morphisme de groupe. Soit $x,y\in I(\mathbb{K})$, alors on a : $x=[q_a]_W$, $y=[q_b]_W$ (q_a,q_b étant uniques à équivalence près), où q_a,q_b sont anisotropes, de dimension paires. Par décomposition de Witt,

$$q_a\perp q_b\simeq p.\langle 1,-1\rangle\perp\phi$$

pour ϕ anisotrope et $p \in \mathbb{N}$. Alors, dans $I(\mathbb{K})$, on a :

$$[q_a]_W + [q_b]_W = [q_a \perp q_b]_W = [p.\langle 1, -1\rangle \perp \phi]_W = [\phi]_W$$

Ainsi :

$$f([q_a]_W + [q_b]_W) = f([\phi]_W) = [\phi] - \frac{1}{2}dim(\phi).\langle 1, -1\rangle$$

et

$$\begin{aligned} f([q_a]_W) + f([q_b]_W) &= [q_a] - \frac{1}{2}dim(q_a).\langle 1, -1\rangle + [q_b] - \frac{1}{2}dim(q_b).\langle 1, -1\rangle \\ &= [q_a \perp q_b] - \frac{1}{2}(dim([q_a \perp q_b]).\langle 1, -1\rangle \\ &= [p.\langle 1, -1\rangle \perp \phi] - \frac{1}{2}(dim([q_a \perp q_b]).\langle 1, -1\rangle \\ &= [\phi] + (p - \frac{1}{2}dim([q_a \perp q_b])).\langle 1, -1\rangle \\ &= [\phi] - \frac{1}{2}dim(\phi).\langle 1, -1\rangle \\ &= f([q_a]_W + [q_b]_W) \end{aligned}$$

Ceci découlant en particulier du fait que :

$$dim(q_a \perp q_b) = dim(\phi) + 2p \Longleftrightarrow p - \frac{1}{2}dim(q_a \perp q_b) = -\frac{1}{2}dim(\phi).$$

Ceci montre que f est un morphisme de groupe.

Montrons que g est un morphisme de groupe. Soit $x, y \in \widehat{I}(\mathbb{K})$. Alors x et y s'écrivent de manière unique $x = [q_a] - n.\langle 1, -1\rangle$ et $y = [q_b] - m.\langle 1, -1\rangle$ où $m, n \in \mathbb{Z}$ et q_a, q_b anisotropes. Par décomposition de Witt, $q_a \perp q_b \simeq p.\langle 1, -1\rangle \perp \phi$ pour ϕ anisotrope et $p \in \mathbb{N}$. Alors, dans $\widehat{I}(\mathbb{K})$, on a :

$$\begin{aligned} [q_a] - n.\langle 1, -1\rangle + [q_b] - m.\langle 1, -1\rangle &= [q_a] + [q_b] - (m+n).\langle 1, -1\rangle \\ &= [q_a \perp q_b] - (m+n).\langle 1, -1\rangle \\ &= [p.\langle 1, -1\rangle \perp \phi] - (m+n).\langle 1, -1\rangle \\ &= [\phi] - (m+n-p).\langle 1, -1\rangle \end{aligned}$$

Comme,

$$g([q_a] - n.\langle 1, -1\rangle + [q_b] - m.\langle 1, -1\rangle) = g([\phi] - (m+n-p).\langle 1, -1\rangle) = [\phi]_W$$

et

$$\begin{aligned} g([q_a] - n.\langle 1, -1\rangle) + g([q_b] - m.\langle 1, -1\rangle) &= [q_a]_W + [q_b]_W \\ &= [q_a \perp q_b]_W \\ &= [p.\langle 1, -1\rangle \perp \phi]_W \\ &= [\phi]_W \end{aligned}$$

g est un morphisme de groupe. Le fait que f et g soient réciproques l'un de l'autre est immédiat par définition même de ces morphismes, d'où f et g sont des isomorphismes de groupes et $I(\mathbb{K}) \simeq \widehat{I}(\mathbb{K})$. □

On en déduit donc d'après la proposition 6.2.10 que $\widehat{W}(\mathbb{K}) \simeq \mathbb{Z} \times I(\mathbb{K})$, résultat que nous utiliserons dans la partie suivante pour étudier la structure des groupes de Witt-Grothendieck des corps pythagoriciens et des corps quadratiquement clos. Nous utiliserons également cet isomorphisme et les résultats sur les structures des groupes de Witt et Witt-Grothendieck des corps $\mathbb{R}$ et $\mathbb{C}$ ainsi que des corps finis pour établir la structure des groupes de Witt et Witt-Grothendieck des corps $\mathbb{Q}$ et des corps p-adiques dans les prochains chapitres.

6.4 Caractérisation par les groupes de Witt et Witt-Grothendieck associés, des corps pythagoriciens et quadratiquement clos

6.4.1 Application à l'étude des corps quadratiquement clos.

Théorème 6.4.1. Caractérisation des corps quadratiquement clos par les groupes de Witt et Witt-Grothendieck associés
Les assertions suivantes sont équivalentes :

1. Le corps $\mathbb{K}$ est quadratiquement clos.
2. $\widehat{W}(\mathbb{K}) \simeq \mathbb{Z}$
3. $W(\mathbb{K}) \simeq \mathbb{Z}/2\mathbb{Z}$

Démonstration. On va simplement montrer que $1 \Longrightarrow 2 \Longrightarrow 3 \Longrightarrow 1$.

- On suppose 1. On sait déjà d'après la proposition 6.2.5 que si $\mathbb{K}$ est quadratiquement clos, alors $\widehat{W}(\mathbb{K})$ est engendré par $\langle 1 \rangle$ et est isomorphe à $\mathbb{Z}$, d'où $1 \Longrightarrow 2$.
- On suppose 2. Comme $\widehat{W}(\mathbb{K}) \simeq \mathbb{Z} \times I(\mathbb{K})$ et que $\widehat{W}(\mathbb{K}) \simeq \mathbb{Z}$, nécessairement $I(\mathbb{K}) = 0_{W(\mathbb{K})}$ ce qui implique que l'application surjective :

$$e\colon \begin{cases} W(\mathbb{K}) \longrightarrow \mathbb{Z}/2 \\ [q]_W \longmapsto \overline{dim(q)} \end{cases}$$

  est aussi injective et donc que $W(\mathbb{K}) \simeq \mathbb{Z}/2$, soit $2 \Longrightarrow 3$.
- On suppose 3. Puisque $W(\mathbb{K}) \simeq \mathbb{Z}/2$, le groupe de Witt $W(\mathbb{K})$ est de cardinal 2. $W(\mathbb{K})$ étant engendré par les éléments $< a >$ où a parcourt les classes de $\mathbb{K}^*$ modulo $(\mathbb{K}^*)^2$, $W(\mathbb{K}) = \{0_{W(\mathbb{K})}, < 1 >\}$ et donc nécessairement, il n'y a qu'une seule classe modulo $(\mathbb{K}^*)^2$, ce qui donne $\mathbb{K} = \mathbb{K}^2$ et $\mathbb{K}$ est quadratiquement clos.

D'où $3 \Longrightarrow 1$ et $1 \Longrightarrow 2 \Longrightarrow 3 \Longrightarrow 1$. □

De cette caractérisation des corps quadratiquement clos par les groupes de Witt et Witt-Grothendieck associés on retrouve naturellement la structure de $W(\mathbb{C})$ et $\widehat{W}(\mathbb{C})$:

Remarque 6.4.1. *De l'étude ci-dessus, on déduit que :*

- $\widehat{W}(\mathbb{C}) \simeq \mathbb{Z}$
- $W(\mathbb{C}) \simeq \mathbb{Z}/2\mathbb{Z}$

et ces isomorphismes caractérisent donc les corps quadratiquement clos.

6.4.2 Application à l'étude des corps pythagoriciens

Dans la suite, on va étudier les groupes de Witt et de Witt-Grothendieck des corps pythagoriciens et voir que l'on peut caractériser entièrement un corps pythagoricien par les groupes de Witt et Witt-Grothendieck associés.

Définition 6.4.1. *Un corps* $\mathbb{K}$ *est dit* pythagoricien *lorsque dans* $\mathbb{K}$ *la somme de de deux carrés est toujours un carré.*

Théorème 6.4.2. Caractérisation des corps pythagoriciens par les groupes de Witt et Witt-Grothendieck associés
Les assertions suivantes sont équivalentes :

1. *Le corps* $\mathbb{K}$ *est* pythagoricien.
2. $\widehat{W}(\mathbb{K})$ *est sans torsion.*
3. $W(\mathbb{K})$ *est sans torison ou* $W(\mathbb{K}) \simeq \mathbb{Z}/2\mathbb{Z}$.

Pour démontrer le théorème de caractérisation on va s'appuyer sur les lemmes suivants :

Lemme 6.4.1. *Si* $\mathbb{K}$ *est pythagoricien et que* $-1 \in (\mathbb{K}^*)^2$ *alors* $\mathbb{K}$ *est quadratiquement clos.*

Démonstration. Supposons $\mathbb{K}$ pythagoricien et que $-1 \in (\mathbb{K}^*)^2$, c'est-à-dire qu'il existe $\alpha \in \mathbb{K}^*$ tel que $-1 = \alpha^2$. Soit $q = \langle 1, -1\rangle$, alors q est hyperbolique et donc universelle. Alors,

$$\begin{aligned} q \text{ universelle} \implies & \quad \forall a \in \mathbb{K}^*, \exists (x,y) \in \mathbb{K}\times\mathbb{K}, a = q(x,y) = x^2 - y^2. \\ \implies & \quad \forall a \in \mathbb{K}^*, \exists (x,y) \in \mathbb{K}\times\mathbb{K}, a = x^2 + \alpha^2 y^2 = x^2 + (\alpha y)^2. \\ \implies & \quad \forall a \in \mathbb{K}^*, \text{ a est un carré puisque } \mathbb{K} \text{ est pythagoricien.} \end{aligned}$$

D'où $\mathbb{K}^* \subset (\mathbb{K}^*)^2$ et donc $\mathbb{K}$ est quadratiquement clos. □

Lemme 6.4.2. *Si* $\mathbb{K}$ *n'est pas pythagoricien, le groupe* $\widehat{W}(\mathbb{K})$ *possède un élément d'ordre* 2 *et n'est donc pas sans torsion.*

Démonstration. Supposons $\mathbb{K}$ non pythagoricien, alors il existe $a \in \mathbb{K}^* \setminus (\mathbb{K}^*)^2$ tel que $a = x^2 + y^2$ pour $(x,y) \neq (0,0)$. Donc, a est représenté par $q = \langle 1, 1\rangle$ et $\langle 1, 1, -a\rangle$ est isotrope. Or, par l'astuce de la dimension 4 :

$$\begin{aligned} \langle 1,1,-a\rangle \text{ est isotrope} & \iff \langle 1,1,-a,-a\rangle \text{ est hyperbolique.} \\ & \iff < 1,1,-a,-a >= 0_{W(\mathbb{K})} \end{aligned}$$

On va montrer que l'élément $\langle 1\rangle - \langle a\rangle$ est d'ordre 2 dans $\widehat{W}(\mathbb{K})$. Par la projection canonique $\pi : \widehat{W}(\mathbb{K}) \longrightarrow W(\mathbb{K})$, on a :

$$\begin{aligned} \pi(2.(\langle 1\rangle - \langle a\rangle)) &= \pi(\langle 1\rangle - \langle a\rangle) + \pi(\langle 1\rangle - \langle a\rangle) \\ &= < 1 > - < a > + < 1 > - < a > \\ &= < 1 > + < -a > + < 1 > + < -a > \\ &= < 1, 1, -a, -a > \\ &= 0_{W(\mathbb{K})} \end{aligned}$$

Ainsi, $2.(\langle 1\rangle - \langle a\rangle) \in Ker(\pi) = \mathbb{Z}\langle 1,-1\rangle \simeq \mathbb{Z}$ et il existe $k \in \mathbb{Z}$ tel que $2.(\langle 1\rangle - \langle a\rangle) = k.\langle 1,-1\rangle$. Par le morphisme de dimension, dim : $\widehat{W}(\mathbb{K}) \longrightarrow \mathbb{Z}$, $dim(2.(\langle 1\rangle - \langle a\rangle)) = dim(k.\langle 1,-1\rangle)$ ce qui nous donne $0 = 2k$ soit $k = 0$. Ainsi, $2.(\langle 1\rangle - \langle a\rangle) = 0_{\widehat{W}(\mathbb{K})}$ et il reste alors à montrer que l'on a $\langle 1\rangle - \langle a\rangle \neq 0_{\widehat{W}(\mathbb{K})}$ pour pouvoir conclure que $\langle 1\rangle - \langle a\rangle$ est d'ordre 2 dans $\widehat{W}(\mathbb{K})$. Si on suppose que $\langle 1\rangle - \langle a\rangle = 0_{\widehat{W}(\mathbb{K})}$, alors $\langle 1\rangle = \langle a\rangle$ dans $\widehat{W}(\mathbb{K})$, ce qui par injectivité du morphisme $i_{FQ(\mathbb{K})}$ se traduit en termes de formes quadratiques par $\langle 1\rangle \simeq \langle a\rangle$, absurde puisque $a \notin (\mathbb{K}^*)^2$. D'où, $\langle 1\rangle - \langle a\rangle$ est d'ordre 2 dans $\widehat{W}(\mathbb{K})$ et $\widehat{W}(\mathbb{K})$ n'est pas sans torsion. □

Lemme 6.4.3. *Si $\mathbb{K}$ est pythagoricien mais pas quadratiquement clos alors $W(\mathbb{K})$ est sans torsion.*

Démonstration. On suppose que $\mathbb{K}$ est pythagoricien mais pas quadratiquement clos. Supposons aussi par l'absurde que $W(\mathbb{K})$ n'est pas sans torsion. Alors, il existe $m \in \mathbb{N}^*$ tel que $m.[q]_W = 0_{W(\mathbb{K})}$, pour $[q]_W$ la classe de Witt équivalence d'une forme quadratique régulière anisotrope q. Par diagonalisation, il existe des éléments non nuls $a_1, ..., a_n$ où $n = \dim(q)$ tels que $[q]_W =< a_1, ..., a_n >$ avec $\langle a_1, ..., a_n\rangle$ anisotrope et donc $m.< a_1, ..., a_n >= 0_{W(\mathbb{K})}$ et $m.\langle a_1, ..., a_n\rangle$ est hyperbolique donc isotrope. Comme la forme quadratique diagonale $m.\langle a_1, ..., a_n\rangle$ est isotrope sur $\mathbb{K}$, il existe un nm-uplet non nul $(x_1, ..., x_{nm})$ tel que :

$$a_1x_1^2 + a_1x_2^2 + ... + a_1x_m^2 + a_2x_{m+1}^2 + a_2x_{m+2}^2 + ... + a_2x_{2m}^2 + ... + a_nx_{(n-1)m+1}^2 + a_nx_{(n-1)m+2}^2 + ... + a_nx_{nm}^2 = 0$$

soit la relation $(*)$:

$$a_1(x_1^2 + ... + x_m^2) + a_2(x_{m+1}^2 + ... + x_{2m}^2) + ... + a_n(x_{(n-1)m+1}^2 + ... + x_{nm}^2) = 0$$

Or, le fait que $\mathbb{K}$ soit pythagoricien et non quadratiquement clos implique que $-1 \notin (\mathbb{K}^*)^2$, car sinon d'après le lemme 6.4.1 $\mathbb{K}$ serait quadratiquement clos. De plus, toute somme de deux carrés non nuls est un carré non nul de $\mathbb{K}$, sinon il existerait des éléments non nuls x et y tels $x^2 + y^2 = 0$ ce qui impliquerait que $x^2 = -y^2$ et donc $-1 = (xy^{-1})^2$ serait un carré de $\mathbb{K}$, absurde. Par un raisonnement par récurrence, toute somme de carrés non nuls du corps pythagoricien $\mathbb{K}$ est un carré non nul. Ainsi par $(*)$, la forme quadratique diagonale $\langle a_1, ..., a_n\rangle$ est isotrope ce qui est absurde car supposée anisotrope. D'où le résultat. □

Passons à la demonstration du théorème.

Démonstration. On va montrer que $1 \Longrightarrow 3$, $2 \Longrightarrow 1$ puis $3 \Longrightarrow 2$ ce qui montrera que $1 \Leftrightarrow 2 \Leftrightarrow 3$.

- Supposons 1. Si $\mathbb{K}$ est pythagoricien et non quadratiquement clos alors d'après le lemme 6.4.3, $W(\mathbb{K})$ est sans torsion. Si $\mathbb{K}$ est pythagoricien et quadratiquement clos, d'après le théorème de caractérisation des corps quadratiquement clos, on a $W(\mathbb{K}) \simeq \mathbb{Z}/2$ et donc $1 \Longrightarrow 3$.
- Montrons que $2 \Longrightarrow 1$ en prouvant que non $1 \Longrightarrow$ non 2. Si $\mathbb{K}$ non pythagoricien, on a d'après le lemme 6.4.2, $\widehat{W}(\mathbb{K})$ n'est pas sans torsion et donc non $1 \Longrightarrow$ non 2.

- Supposons 3. Si $W(\mathbb{K}) \simeq \mathbb{Z}/2$, alors d'après le théorème de caractérisation des corps quadratiquement clos, $\widehat{W}(\mathbb{K}) \simeq \mathbb{Z}$ et $\mathbb{Z}$ étant sans torsion $\widehat{W}(\mathbb{K})$ est sans torsion. Si $W(\mathbb{K})$ sans torsion et que par l'absurde il existe $n \in \mathbb{N}^*$ et $x \in \widehat{W}(\mathbb{K})$ tel que $x \neq 0_{\widehat{W}(\mathbb{K})}$ et $nx = 0_{\widehat{W}(\mathbb{K})}$, alors par le morphisme de projection π,
$$\pi(nx) = n\pi(x) = 0.$$
Or, si par l'absurde $\pi(x) = 0$, on a $x \in \mathbb{Z}\langle 1, -1\rangle \simeq \mathbb{Z}$ où $\mathbb{Z}$ est sans torsion. Ainsi, $x \in \mathbb{Z}\langle 1, -1\rangle$ qui est sans torsion, avec $nx = 0_{\widehat{W}(\mathbb{K})}$ pour n non nul, absurde. D'où, $\pi(x) \neq 0$ et commme $n\pi(x) = 0$, il est d'ordre fini dans $W(\mathbb{K})$ qui est par hypothèse sans torsion, absurde. Donc,
$$W(\mathbb{K}) \text{ sans torsion} \Longrightarrow \widehat{W}(\mathbb{K}) \text{ sans torsion.}$$
ce qui montre $3 \Longrightarrow 2$ et le théorème.

□

Exemple 6.4.1. *Le corps des nombres réels constructibles à la règle et au compas est pythagoricien, car stable par passage à la racine carrée. Ainsi, le groupe de Witt-Grothendieck de ce corps est sans torsion et son groupe de Witt est sans torsion ou isomorphe à* $\mathbb{Z}/2$. *De même, on peut voir qu'aucun corps fini de caractéristique différente de* 2 *n'est pythagoricien.*

6.5 Présentation de $\widehat{W}(\mathbb{K})$ et $W(\mathbb{K})$ par générateurs et relations

Dans cette section, nous allons donner des résultats (pour la plupart sans démonstrations) concernant la présentation des groupes $\widehat{W}(\mathbb{K})$ et $W(\mathbb{K})$ par générateurs et relations. Ces descriptions seront particulièrement efficaces pour définir des morphismes ayant pour source $W(\mathbb{K})$ ou $\widehat{W}(\mathbb{K})$ et nous utiliserons notamment ces résultats dans le prochain chapitre pour définir des applications ∂_p intervenant dans les tests de Witt-équivalence et de d'équivalence sur $\mathbb{Q}$.

On rappelle qu'on note $\mathbb{Z}[\mathbb{K}^*]$ le groupe abélien libre de base $\mathbb{K}^*$ dont les éléments sont les combinaisons linéaires formelles, à support fini et coefficients entiers d'éléments de $\mathbb{K}^*$. On définit deux morphismes de groupes sur la base $\mathbb{K}^*$,
$$\alpha_1 : \mathbb{Z}[\mathbb{K}^*] \longrightarrow \widehat{W}(\mathbb{K}) \text{ et } \alpha_2 : \mathbb{Z}[\mathbb{K}^*] \longrightarrow W(\mathbb{K})$$
par :
$$\forall k \in \mathbb{K}^*, \alpha_1(k) = \langle k\rangle \in \widehat{W}(\mathbb{K}) \text{ et } \forall k \in \mathbb{K}^*, \alpha_2(k) =< k >\in W(\mathbb{K})$$
Comme a vu que les familles $\{\langle a\rangle \mid a \in \mathbb{K}^*\}$ et $\{< a >\mid a \in \mathbb{K}^*\}$ sont des familles génératrices, respectivement de $\widehat{W}(\mathbb{K})$ et de $W(\mathbb{K})$, les morphismes α_1 et α_2 sont surjectifs. Il s'agit donc d'étudier les noyaux de ces deux morphismes, pour obtenir un système de relations entre générateurs.

6.5.1 Relations en dimension 1 et 2

Commençons par énoncer quelques relations évidentes en dimension 1 et 2.

Proposition 6.5.1. *Soit $a, b \in (\mathbb{K}^*)^2$, les formes quadratiques régulières $\langle a\rangle$ et $\langle b\rangle$ sont équivalentes si et seulement si $a = b$ dans $\mathbb{K}^*/(\mathbb{K}^*)^2$. Donc en dimension 1, les cas d'équivalence entre formes quadratiques régulières sont entièrement décrits par les relations :*

$$\forall (a, \delta) \in (\mathbb{K}^*)^2,\ \langle \delta^2 a\rangle = \langle a\rangle$$

et donc

$$\forall (a, \delta) \in (\mathbb{K}^*)^2,\ < \delta^2 a >=< a > \text{ dans } W(\mathbb{K})$$

et

$$\forall (a, \delta) \in (\mathbb{K}^*)^2,\ \langle \delta^2 a\rangle = \langle a\rangle \text{ dans } \widehat{W}(\mathbb{K})$$

Démonstration. Supposons $\langle a\rangle \simeq \langle b\rangle$, alors ces deux formes quadratiques ont même déterminant et donc $a = b$ dans $\mathbb{K}^*/(\mathbb{K}^*)^2$. Inversement, si $a = b$ dans $\mathbb{K}^*/(\mathbb{K}^*)^2$, on a clairement $\langle a\rangle \simeq \langle b\rangle$, d'où l'équivalence. Alors on a :

$$\forall (a, \delta) \in (\mathbb{K}^*)^2,\ \langle \delta^2 a\rangle = \langle a\rangle$$

ce qui donne de manière évidente, les relations énoncés dans $W(\mathbb{K})$ et $\widehat{W}(\mathbb{K})$ avec évidemment l'identification qui consiste à voir $FQ(\mathbb{K})$ comme un sous-monoïde de $\widehat{W}(\mathbb{K})$. □

Proposition 6.5.2. ***Relation de Witt***
Soit $(a, b) \in (\mathbb{K}^*)^2$ tel que $a + b \neq 0$. Alors :

$$\langle a, b\rangle \simeq \langle a + b, (a + b)ab\rangle$$

et en particulier,

$$< a > + < b >=< a + b > + < (a + b)ab > \text{ dans } W(\mathbb{K})$$

et

$$\langle a\rangle + \langle b\rangle = \langle a + b\rangle + \langle (a + b)ab\rangle \text{ dans } \widehat{W}(\mathbb{K})$$

Démonstration. Soit $a, b \in (\mathbb{K}^*)^2$ tels que $a + b \neq 0$. L'égalité matricielle :

$$\begin{pmatrix} 1 & 1 \\ b & -a \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \begin{pmatrix} 1 & b \\ 1 & -a \end{pmatrix} = \begin{pmatrix} a + b & 0 \\ 0 & (a + b)ab \end{pmatrix}$$

montre que les matrices diagonales $D(a, b)$ et $D(a+b, (a+b)ab)$ sont congruentes puisque $\begin{pmatrix} 1 & 1 \\ b & -a \end{pmatrix}$ est inversible car de déterminant $-(a+b) \neq 0$ par hypothèse. Alors les formes quadratiques $\langle a, b\rangle$ et $\langle a + b, (a + b)ab\rangle$ sont équivalentes car ont même classes de congruences de matrices symétriques associées. De plus,

$$\langle a, b\rangle \simeq \langle a\rangle \perp \langle b\rangle \text{ et } \langle a + b, (a + b)ab\rangle \simeq \langle a + b\rangle \perp \langle (a + b)ab\rangle$$

ce qui se traduit notamment dans le groupe $W(\mathbb{K})$ par les relations :

$$< a > + < b >=< a + b > + < (a + b)ab >$$

et dans $\widehat{W}(\mathbb{K})$, par les relations :

$$\langle a\rangle + \langle b\rangle = \langle a + b\rangle + \langle (a + b)ab\rangle$$

avec évidemment l'identification qui consiste à voir $FQ(\mathbb{K})$ comme un sous-monoïde de $\widehat{W}(\mathbb{K})$. □

La proposition suivante que nous ne démontrerons pas, donne une description des groupes $W(\mathbb{K})$ et $\widehat{W}(\mathbb{K})$ par générateurs et relations. On déduit des isomorphismes,

$$Z[\mathbb{K}^*]/(Ker(\alpha_1)) \simeq \widehat{W}(\mathbb{K}) \text{ et } Z[\mathbb{K}^*]/(Ker(\alpha_2)) \simeq W(\mathbb{K})$$

et de l'étude de $Ker(\alpha_1)$, $Ker(\alpha_2)$ (cf.[1] XVI pages 347 à 352), la proposition :

Proposition 6.5.3. *L'application α_1 induit un isomorphismes entre $\widehat{W}(\mathbb{K})$ et le groupe abélien défini par les générateurs $\overline{a}$ pour $a \in \mathbb{K}^*$, soumis aux relations :*

1. $\overline{\delta^2 a} \sim \overline{a}$ *quelque soit* $(a, \delta) \in (\mathbb{K}^*)^2$.
2. $\overline{a} + \overline{b} \sim \overline{a+b} + \overline{(a+b)ab}$ *quelque soit* $(a, b) \in (\mathbb{K}^*)^2$ *tel que* $a + b \neq 0$.

Pour décrire la structure de $W(\mathbb{K})$, il suffit d'imposer en plus que $\overline{-1} \sim -\overline{1}$.

6.5.2 Seconde propriété universelle des groupes $W(\mathbb{K})$ et $\widehat{W}(\mathbb{K})$

Dans la suite, nous utiliserons essentiellement la proposition suivante :

Proposition 6.5.4. *Soit $f : \mathbb{K}^* \longrightarrow G$ une application, où G désigne un groupe abélien. On suppose que :*

1. $f(\delta^2 a) = f(a)$ *quelque soit* $(a, \delta) \in (\mathbb{K}^*)^2$.
2. $f(a) + f(b) = f(a+b) + f((a+b)ab)$ *quelque soit* $(a, b) \in (\mathbb{K}^*)^2$ *tel que* $a + b \neq 0$.

Alors, il existe un unique morphisme de groupes

$$\overline{f} : \widehat{W}(\mathbb{K}) \longrightarrow G$$

tel que $\forall a \in \mathbb{K}^*$, $\overline{f}(\langle a \rangle) = f(a)$. Si en plus $f(-1) = -f(1)$, alors il existe un unique morphisme de groupes

$$\overline{\overline{f}} : W(\mathbb{K}) \longrightarrow G$$

tel que $\forall a \in \mathbb{K}^*$, $\overline{\overline{f}}(< a >) = f(a)$

6.5.3 Relation de congruence matricielle restreinte aux matrices diagonales inversibles

Grâce à cette proposition, on va pouvoir étudier la relation de congruence matricielle restreinte aux matrices diagonales inversibles :

Proposition 6.5.5. *La projection canonique, $f : \mathbb{Z}[\mathbb{K}^*/(\mathbb{K}^*)^2] \longrightarrow \widehat{W}(\mathbb{K})$ définie sur la base $\mathbb{K}^*/(\mathbb{K}^*)^2$ du groupe abélien libre $Z[\mathbb{K}^*/(\mathbb{K}^*)^2]$ par :*

$$\forall k \in \mathbb{K}^*,\ f(\overline{k}) = \langle k \rangle$$

est une bijection si et seulement si le corps $\mathbb{K}$ est pythagoricien et si de plus tout élément de $\mathbb{K}$ est un carré ou l'opposé d'un carré. Dans ces conditions, $\widehat{W}(\mathbb{K})$ est isomorphe à $\mathbb{Z}$ ou $\mathbb{Z}^2$.

Démonstration. L'application f est clairement un morphisme de groupes, car f a été défini sur la base $\mathbb{K}^*/(\mathbb{K}^*)^2$ de $Z[\mathbb{K}^*/(\mathbb{K}^*)^2]$ puis étendu à $Z[\mathbb{K}^*/(\mathbb{K}^*)^2]$ de manière à être compatible avec les deux structures de groupes abéliens de $Z[\mathbb{K}^*/(\mathbb{K}^*)^2]$ et $\widehat{W}(\mathbb{K})$. La surjectivité est elle aussi immédiate. Supposons que le corps $\mathbb{K}$ est pythagoricien et que tout élément de $\mathbb{K}$ est un carré ou l'opposé d'un carré. Définissons l'application g par :

$$g\colon \begin{cases} \mathbb{K}^* \longrightarrow \mathbb{Z}[\mathbb{K}^*/(\mathbb{K}^*)^2] \\ k \longmapsto \overline{k} \end{cases}$$

On cherche à vérifier les conditions de la proposition 6.5.4.

On a : $g(\delta^2 a) = \overline{\delta^2 a} = \overline{a} = g(a)$ quelque soit $(a, \delta) \in (\mathbb{K}^*)^2$. De plus, comme tout élément de $\mathbb{K}$ est un carré ou l'opposé d'un carré, on a pour $k, l \in \mathbb{K}^*$,

$$\exists \alpha, \beta \in \mathbb{K},\ k = \pm\alpha^2 \text{ et } l = \pm\beta^2.$$

Supposons $k = \alpha^2$ et $l = \beta^2$ et $k + l \neq 0$. Ainsi,

$$g(k) + g(l) = \overline{k} + \overline{l} = \overline{\alpha^2} + \overline{\beta^2} = \overline{1} + \overline{1}$$

et $\mathbb{K}$ étant pythagoricien, $k + l = \alpha^2 + \beta^2 = \delta^2$ est un carré, soit :

$$g(k + l) + g((k + l)kl) = \overline{k + l} + \overline{(k + l)kl} = \overline{\delta^2} + \overline{(\delta^2)\alpha^2\beta^2} = \overline{1} + \overline{1}$$

D'où,

$$g(k) + g(l) = g(k + l) + g((k + l)kl).$$

Supposons $k = \alpha^2$ et $l = -\beta^2$ et $k + l \neq 0$. Ainsi,

$$g(k) + g(l) = \overline{k} + \overline{l} = \overline{\alpha^2} + \overline{-\beta^2} = \overline{1} + \overline{-1}$$

et :

$$\begin{aligned} g(k + l) + g((k + l)kl) = & \quad \overline{k + l} + \overline{(k + l)kl} \\ = & \quad \overline{\alpha^2 - \beta^2} + \overline{(\alpha^2 - \beta^2) \times -\alpha^2\beta^2} \\ = & \quad \overline{\alpha^2 - \beta^2} + \overline{-(\alpha^2 - \beta^2)} \end{aligned}$$

Or, $\alpha^2 - \beta^2 \in \mathbb{K}$ est un carré ou l'opposé d'un carré et donc $\overline{\alpha^2 - \beta^2} = \overline{\pm 1}$, ce qui montre que :

$$g(k + l) + g((k + l)kl) = \overline{1} + \overline{-1} = g(k) + g(l).$$

Comme k et l jouant des rôles symétriques, le cas $k = -\alpha^2$ et $l = \beta^2$ se traîte de manière identique et au final on a montré que :

$g(a) + g(b) = g(a + b) + g((a + b)ab)$ quelque soit $(a, b) \in (\mathbb{K}^*)^2$ tel que $a + b \neq 0$

Alors, il existe un unique morphisme de groupes

$$\overline{g} : \widehat{W}(\mathbb{K}) \longrightarrow G$$

tel que $\forall k \in \mathbb{K}^*$, $\overline{g}(\langle k \rangle) = g(k) = \overline{k}$. Ainsi, $\overline{g}$ est clairement le morphisme réciproque de f, puisque pour $\mathbb{K}^*/(\mathbb{K}^*)^2$ une base du groupe abélien libre $\mathbb{Z}[\mathbb{K}^*/(\mathbb{K}^*)^2]$, on a :

$$\forall k \in \mathbb{K}^*,\ f(g(\langle k \rangle)) = f(\overline{k}) = \langle k \rangle \text{ et } g(f(\overline{k})) = g(\langle k \rangle) = \overline{k}$$

Donc, si $\mathbb{K}$ est pythagoricien tel que tout élément de $\mathbb{K}$ est un carré ou l'opposé d'un carré, la projection canonique est bijective.

Inversement, supposons que f soit bijective et on note g sa bijection réciproque définie sur l'ensemble générateur $\{\langle k\rangle \mid k \in \mathbb{K}^*\}$ de $\widehat{W}(\mathbb{K})$ par :

$$\forall k \in \mathbb{K}^*, g(\langle k\rangle) = \overline{k} \in \mathbb{Z}[\mathbb{K}^*/(\mathbb{K}^*)^2]$$

Montrons pour commencer que $\mathbb{K}$ est pythagoricien. Puisque f est bijective et que $\mathbb{Z}[\mathbb{K}^*/(\mathbb{K}^*)^2]$ est un groupe abélien libre donc sans torsion, $\widehat{W}(\mathbb{K})$ qui lui est isomorphe est aussi sans torsion. Par caractérisation des corps pythagoricien par les groupe de Witt et Witt-Grothendieck associés, ceci implique que $\mathbb{K}$ est pythagoricien. Il reste à montrer et que tout élément de $\mathbb{K}$ est un carré ou l'opposé d'un carré. Comme g est un morphisme de groupe,

$$\forall k \in \mathbb{K}^*,\ g(\langle k\rangle + \langle -k\rangle) = g(\langle k\rangle) + g(\langle -k\rangle) = \overline{k} + \overline{-k}$$

Les formes quadratiques $\langle 1, -1\rangle$ et $\langle k, -k\rangle$ étant équivalentes car hyperboliques, $\langle 1, -1\rangle = \langle k, -k\rangle$ dans $\widehat{W}(\mathbb{K})$ et donc :

$$g(\langle 1, -1\rangle) = \overline{1} + \overline{-1} = \overline{k} + \overline{-k} = g(\langle k, -k\rangle).$$

D'où,

$$\forall k \in \mathbb{K}^*, \overline{1} + \overline{-1} = \overline{k} + \overline{-k} \Longleftrightarrow \overline{1} + \overline{-1} - \overline{k} - \overline{(-k)} = 0 \text{ dans } \mathbb{Z}[\mathbb{K}^*/(\mathbb{K}^*)^2]\ (1).$$

$\mathbb{K}^*/(\mathbb{K}^*)^2$ étant une base du groupe libre $\mathbb{Z}[\mathbb{K}^*/(\mathbb{K}^*)^2]$, si k n'est pas un carré ou l'opposé d'un carré, les éléments $\overline{1}, \overline{-1}, \overline{k}, \overline{-k}$ sont tous distincts et donc pour $(n_i)_{1\leq i\leq 4} \in \mathbb{Z}^4$:

$$n_1\overline{1} + n_2 \times (\overline{-1}) + n_3\overline{k} + n_4 \times (\overline{-k}) = 0 \Longleftrightarrow n_i = 0,\ \forall i \in [\![1, 4]\!]$$

Absurde, d'après (1). D'où, tout scalaire k est un carré ou l'opposé d'un carré.

Enfin, si on suppose que $\mathbb{K}$ est pythagoricien et que tout élément de $\mathbb{K}$ est un carré ou l'opposé d'un carré, alors $\mathbb{K}^*/(\mathbb{K}^*)^2$ est trivial si -1 est un carré, et $\mathbb{K}^*/(\mathbb{K}^*)^2 \simeq \{1, -1\}$ sinon. D'où,

$$\mathbb{Z}[\mathbb{K}^*/(\mathbb{K}^*)^2] \simeq \mathbb{Z}[1] \simeq \mathbb{Z} \text{ ou } \mathbb{Z}[\mathbb{K}^*/(\mathbb{K}^*)^2] \simeq \mathbb{Z}[1, -1] \simeq \mathbb{Z}^2.$$

□

On en déduit alors :

Corollaire 6.5.1. *Pour $(a_1, \ldots, a_n)$ et $(b_1, \ldots, b_n)$ dans $(\mathbb{K}^*)^n$, la condition notée $(*)$:*

$$\langle a_1, \ldots, a_n\rangle \simeq \langle b_1, \ldots, b_n\rangle \Longleftrightarrow \textit{il existe } \sigma \in \mathfrak{S}_n \textit{ et } (\lambda_1, \ldots, \lambda_n) \in (\mathbb{K}^*)^n \textit{ tels que } \forall k \in [\![1, n]\!], b_k = \lambda_k^2 a_{\sigma(k)}\ (*)$$

est vérifiée si et seulement si $\mathbb{K}$ est pythagoricien et si tout élément de $\mathbb{K}$ est un carré ou l'opposé d'un carré. On a aussi, la condition $(**)$:

$$D(a_1, \ldots, a_n) \approx D(b_1, \ldots, b_n) \Longleftrightarrow \textit{il existe } \sigma \in \mathfrak{S}_n \textit{ et } (\lambda_1, \ldots, \lambda_n) \in (\mathbb{K}^*)^n \textit{ tels que } \forall k \in [\![1, n]\!], b_k = \lambda_k^2 a_{\sigma(k)}$$

est vérifiée si et seulement si $\mathbb{K}$ est pythagoricien et si tout élément de $\mathbb{K}$ est un carré ou l'opposé d'un carré.

Démonstration. On suppose que $\mathbb{K}$ est pythagoricien et que tout élément de $\mathbb{K}$ est un carré ou l'opposé d'un carré, alors la projection canonique f est une bijection et on veut montrer que la condition $(*)$ est vérifiée. Soit $(a_1, \ldots, a_n)$ et $(b_1, \ldots, b_n)$ dans $(\mathbb{K}^*)^n$. Remarquons d'abord que s'il existe $\sigma \in \mathfrak{S}_n$ et $(\lambda_1, \ldots, \lambda_n) \in (\mathbb{K}^*)^n$ tels que $\forall k \in [\![1, n]\!], b_k = \lambda_k^2 a_{\sigma(k)}$ alors les formes quadratiques $\langle a_1, \ldots, a_n\rangle$ et $\langle b_1, \ldots, b_n\rangle$ sont naturellement équivalentes. Pour montrer que $(*)$ est vérifiée, il suffit de montrer que si les formes quadratiques $\langle a_1, \ldots, a_n\rangle$ et $\langle b_1, \ldots, b_n\rangle$ sont équivalentes, nécessairement il existe $\sigma \in \mathfrak{S}_n$ et $(\lambda_1, \ldots, \lambda_n) \in (\mathbb{K}^*)^n$ tels que $\forall k \in [\![1, n]\!], b_k = \lambda_k^2 a_{\sigma(k)}$. Supposons donc que $\langle a_1, \ldots, a_n\rangle \simeq \langle b_1, \ldots, b_n\rangle$, alors dans $\widehat{W}(\mathbb{K})$ on a :

$$\langle a_1\rangle + \ldots + \langle a_n\rangle = \langle a_1, \ldots, a_n\rangle = \langle b_1, \ldots, b_n\rangle = \langle b_1\rangle + \ldots + \langle b_n\rangle.$$

et

$$f(\langle a_1\rangle + \ldots + \langle a_n\rangle) = \overline{a_1} + \ldots + \overline{a_n} = \overline{b_1} + \ldots + \overline{b_n} = g(\langle a_1\rangle + \ldots + \langle a_n\rangle)$$

Or, tout élément de $\mathbb{K}^*$ étant un carré ou l'opposé d'un carré, il existe deux couples d'entiers $(k_1, l_1) \in \mathbb{N}^2$ et $(k_2, l_2) \in \mathbb{N}^2$ tels que $k_1 + l_1 = n = k_2 + l_2$, avec :

$$\overline{a_1} + \ldots + \overline{a_n} = k_1\overline{1} + l_1 \times \overline{-1} = k_2\overline{1} + l_2 \times \overline{-1}$$

et $\mathbb{K}^*/(\mathbb{K}^*)^2$ étant une base de $\mathbb{Z}[\mathbb{K}^*/(\mathbb{K}^*)^2]$, ceci implique par unicité d'écriture $(k_1, l_1) = (k_2, l_2)$. Ainsi, il y a parmi $(a_1, \ldots, a_n)$, k élément qui sont des carrés et l éléments qui s'écrivent comme opposés de carrés et de même pour $(b_1, \ldots, b_n)$. A permutation près, on a donc $a_i = b_i$ modulo $(\mathbb{K}^*)^2$ et donc il existe $\sigma \in \mathfrak{S}_n$ et $(\lambda_1, \ldots, \lambda_n) \in (\mathbb{K}^*)^n$ tels que $\forall k \in [\![1, n]\!], b_k = \lambda_k^2 a_{\sigma(k)}$. Ce qui montre que $(*)$ est bien vérifiée si $\mathbb{K}$ est pythagoricien et que tout élément de $\mathbb{K}$ est un carré ou l'opposé d'un carré.

Réciproquement, supposons que $\mathbb{K}$ n'est pas pythagoricien ou qu'il existe un élément non nul de $\mathbb{K}$ qui ne soit ni un carré, ni l'opposé d'un carré. Alors, si $\mathbb{K}$ n'est pas pythagoricien, il existe $(x, y) \in (\mathbb{K}^*)^2$ tel que $x^2 + y^2 = \delta$ ne soit pas un carré. Par le principe de complétion avec un déterminant, δ étant représenté par $\langle 1, 1\rangle$, on a $\langle 1, 1\rangle \simeq \langle \delta, \delta\rangle$ et donc puisque δ n'est pas un carré, il n'existe pas de $\lambda \in \mathbb{K}^*$ tel que $\lambda^2 = \delta$ et la condition $(*)$ de la proposition n'est pas vérifiée. Supposons qu'il existe un élément de $\mathbb{K}^*$ qui ne soit ni un carré, ni l'opposé d'un carré que l'on note α. Alors $\langle 1, -1\rangle \simeq \langle \alpha, -\alpha\rangle$ et

$$1 \neq \alpha \text{ et } -1 \neq \alpha \text{ dans } \mathbb{K}^*/(\mathbb{K}^*)^2$$

prouve alors que la condition $(*)$ de la proposition n'est pas vérifiée. Ce qui achève de montrer le résultat. □

Remarque 6.5.1. *Le corollaire ci-dessus, permet de retrouver naturellement les résultats usuels sur la classification des formes quadratiques réelles et complexes. On voit de même que sur le corps $\mathbb{Q}$, la relation de congruence matricielle restreinte aux matrices diagonales n'est pas résumée par la relation ci dessus, $\mathbb{Q}$ n'étant pas pythagoricien (1 + 1 = 2 n'est pas un carré de $\mathbb{Q}$).*

Enfin, terminons par décrire le groupe $W(\mathbb{F}_2)$ que nous n'avons pas défini jusqu'alors, par générateurs et relations ($W(\mathbb{K})$ a seulement été défini dans pour des corps de caractéristique différente de 2). Nous aurons besoin de connaître cette structure, pour étudier le groupe de Witt $W(\mathbb{Q})$.

6.6 Le groupe $W(\mathbb{F}_2)$

Définition 6.6.1. *On définit $W(\mathbb{F}_2)$ comme le groupe à un générateur $< 1 >$ et soumis à la seule relation, $- < 1 > \sim < 1 >$. Il est isomorphe à $\mathbb{Z}/2$ via l'application, $\phi :< 1 > \longmapsto 1$. Ainsi, à tout n-uplet $(a_1, \ldots, a_n) \in (\mathbb{F}_2)^n$, on associe l'élément $< a_1 > + \ldots < a_n >$ de $W(\mathbb{F}_2)$ et on l'appelle sa classe dans $W(\mathbb{F}_2)$, avec $< 0 >= 0$.*

Chapitre 7

Le groupe $W(\mathbb{Q})$ et tests de Witt-équivalence et d'équivalence sur $\mathbb{Q}$

Ce chapitre sera consacré à l'étude du groupe $W(\mathbb{Q})$, avec pour objectif d'énoncer et de donner des justifications des tests de Witt-équivalence et d'équivalence sur $\mathbb{Q}$. Il s'agit de théorèmes essentiels qui constituent des résultats majeurs en termes de classification des formes quadratiques rationnelles. Nous serons en effet capable de déterminer par ces tests, si deux formes quadratiques données sont équivalentes, ou encore si deux formes quadratiques données sont Witt-équivalentes. La justification de ces tests est difficile, nous expliquerons alors simplement comment l'étude de la structure du groupe de Witt $W(\mathbb{Q})$ et l'isomorphisme suivant :

$$\Phi\colon \begin{cases} W(\mathbb{Q}) \longrightarrow W(\mathbb{R}) \oplus \bigoplus_{p\in\mathcal{P}} W(\mathbb{F}_p) \\ x \longmapsto \ x_{\mathbb{R}} + \sum_{p\in\mathcal{P}} \partial_p(x) \end{cases}$$

nous permettent d'établir un test de Witt-équivalence rationnelle. Celui d'équivalence rationnelle s'en déduira sans difficulté. Pour ce faire, nous commencerons par définir des applications ∂_p qui sont des morphismes de $W(\mathbb{Q})$ dans $W(\mathbb{F}_p)$. Ensuite, après avoir construit ces applications, nous serons en mesure d'énoncer les tests de Witt-équivalence et d'équivalence sur $\mathbb{Q}$. Afin de comprendre le morphisme Φ, nous rappellerons quelques propriétés relatives à l'extension des scalaires et expliquerons comment prolonger de manière unique une forme quadratique sur un corps $\mathbb{K}$, en une forme quadratique sur un surcorps $\mathbb{L}$ de $\mathbb{K}$. De part la présentation des groupes de Witt et Witt-Grothendieck par générateurs et relations, nous montrerons en particulier que l'extension des scalaires induit deux morphismes :

$\alpha_1 : \widehat{W}(\mathbb{K}) \longrightarrow \widehat{W}(\mathbb{L})$ et $\alpha_2 : W(\mathbb{K}) \longrightarrow W(\mathbb{L})$ où $\mathbb{L}$ est un surcorps du corps $\mathbb{K}$

et nous appliquerons ces résultats à l'extension de corps $\mathbb{Q} \subset \mathbb{R}$. Nous verrons ensuite comment l'isomorphisme (que nous n'établirons pas) :

$$\Phi : W(\mathbb{Q}) \xrightarrow{\simeq} W(\mathbb{R}) \oplus \bigoplus_{p\in\mathcal{P}} W(\mathbb{F}_p)$$

permet de justifier le test de Witt-équivalence rationnelle.

Enfin, nous étudierons plus en détail la structure de $W(\mathbb{Q})$, grâce aux résultats du chapitre précédent, concernant la structure des groupes de Witt de $\mathbb{C}$, $\mathbb{R}$ et des corps finis.

7.1 Construction des applications ∂_p

Dans cette partie, nous allons construire des applications

$$\partial_p : W(\mathbb{Q}) \longrightarrow W(\mathbb{F}_p)$$

qui nous seront d'une grande importance pour les tests de Witt-équivalence et d'équivalence sur $\mathbb{Q}$.

Notation 7.1.1. *Tout rationnel $r \in \mathbb{Q}^*$ s'écrit de manière unique :*

$$r = \pm \frac{\prod_{i=1}^{l} p_i^{\alpha_i}}{\prod_{j=1}^{m} q_j^{\beta_j}}$$

où $\forall i \in [\![1, l]\!]$, $\alpha_i \in \mathbb{N}^*$, $\forall j \in [\![1, m]\!]$, $\beta_j \in \mathbb{N}^*$ et les p_i, q_j sont des nombres premiers tels que : $\{p_1, \ldots, p_l\} \cap \{q_1, \ldots, q_m\} = \emptyset$. Alors, les valuations p-adiques sont définies par :

$$\nu_{p_i}(r) = \alpha_i \text{ et } \nu_{q_j}(r) = -\beta_j$$

et

$$\nu_p(r) = 0 \text{ si } p \nmid p_1,\ p \nmid q_1, \text{ pour } r = \pm \frac{p_1}{q_1} \text{ et } p_1 \wedge q_1 = 1.$$

On pose alors, pour $r \in \mathbb{Q}^*$:

$$s_p(r) = 0 \text{ si } \nu_p(r) \equiv 0\,[2] \text{ et } s_p(r) = 1 \text{ si } \nu_p(r) \equiv 1\,[2]$$

Ainsi, on a naturellement que pour $a, b \in \mathbb{Q}^*$,

$$s_p(a) = s_p(b) \Longleftrightarrow \nu_p(a) \equiv \nu_p(b)\,[2]$$

ce qui est évidemment le cas pour $\nu_p(a) = \nu_p(b)$.

Définition 7.1.1. *Soit r un nombre rationnel non nul. Alors, il existe un couple (p_1, q_1) tel que $r = p^{\nu_p(r)} \frac{p_1}{q_1}$ où p_1 et q_1 sont premiers avec $p \in \mathcal{P}$ et l'on définit* ***le résidu de r mod p*** *comme :*

$$res_p(r) = \overline{p_1}(\overline{q_1})^{-1} \in \mathbb{F}_p^*$$

Le couple (p_1, q_1) de la définition n'est pas unique, mais par définition de la valuation p-adique, pour un autre couple (p_2, q_2), on a $\frac{p_1}{q_1} = \frac{p_2}{q_2}$ et la définition de $res_p(r)$ est indépendante du choix effectué. On pose alors :

$$\partial_p(r) = s_p(r) res_p(r) \in \mathbb{F}_p$$

Ainsi, si $r = n$ est un entier non nul sans facteur carré,

- soit $p \mid n$, alors $n = kp$ pour $k \in \mathbb{Z}$, $k \wedge p = 1$. On a donc

$$\nu_p(n) = 1 \Longrightarrow s_p(n) = 1 \text{ et } \partial_p(n) = res_p(n) = \frac{\overline{n}}{p} = \overline{k} \in \mathbb{F}_p^*$$

- soit $p \nmid n$, alors $\nu_p(n) = 0 \Longrightarrow s_p(n) = 0$ et $\partial_p(n) = \overline{0}$

Proposition 7.1.1. *Il existe un unique morphisme de groupes noté encore ∂_p :*

$$\partial_p : W(\mathbb{Q}) \longrightarrow W(\mathbb{F}_p)$$

vérifiant :

$$\forall r \in \mathbb{Q}^*, \partial_p(< r >) =< \partial_p(r) > \in W(\mathbb{F}_p).$$

Cette proposition montre en particulier que pour ϕ forme quadratique rationnelle régulière et toute diagonalisation $\phi \simeq \langle a_1, \ldots, a_n \rangle$, de part la structure de groupe de $W(\mathbb{Q})$ et $W(\mathbb{F}_p)$, on a :

$$\begin{aligned}
\partial_p([\phi]_W) = & \quad \partial_p(< a_1, \ldots, a_n >) \\
= & \quad \partial_p(< a_1 > + \ldots + < a_n >) \\
= & \quad \partial_p(< a_1 >) + \ldots + \partial_p(< a_n >) \\
= & \quad < \partial_p(a_1) > + \ldots + < \partial_p(a_n) > \\
= & \quad < \partial_p(a_1), \ldots, \partial_p(a_n) >
\end{aligned}$$

La connaissance de l'image $\partial_p([\phi]_W)$ ne dépend pas du choix d'une diagonalisation de ϕ, puisque ∂_p étant bien définie, si $\phi \simeq \langle a_1, \ldots, a_n \rangle \simeq \langle b_1, \ldots, b_n \rangle$, alors on a :

$$[\phi]_W =< a_1, \ldots, a_n >=< b_1, \ldots, b_n >$$

et donc :

$$\partial_p([\phi]_W) =< \partial_p(a_1), \ldots, \partial_p(a_n) >=< \partial_p(b_1), \ldots, \partial_p(b_n) >$$

Remarque 7.1.1. *Pour calculer $\partial_p([\phi]_W)$, pour ϕ forme quadratique rationnelle, régulière, nous commencerons alors naturellement par diagonaliser ϕ sous la forme $\langle a_1, \ldots, a_n \rangle$, avec les a_i que nous prendrons entiers sans facteur carré et pour lesquels le calcul de $\partial_p(a_i) \in \mathbb{F}_p$ est facile. En effet, pour p un nombre premier quelconque et $k \in \mathbb{Z}$ sans facteur carré et premier avec p, on a facilement :*

$$\partial_p(0) := 0 \in \mathbb{F}_p,\ \partial_p(k) := 0 \in \mathbb{F}_p \text{ et } \partial_p(pk) := \overline{k} \in \mathbb{F}_p$$

Expliquons brièvement pourquoi une telle diagonalisation est possible. Soit ϕ une forme quadratique rationnelle de dimension finie n. Par diagonalisation, il existe un n-uplet de rationnels $(a_1, \ldots, a_n)$ tel que :

$$\phi \simeq \langle a_1, \ldots, a_n \rangle$$

Quitte à multiplier chacun des rationnels a_i, par un carré d'un rationnel bien choisi, on peut se ramener au cas où ce sont tous des entiers relatifs nuls ou sans facteur carré. En effet, si $r \in \mathbb{Q}_+^*$, alors r s'écrit de manière unique sous la forme d'une fraction irreductible, $r = \dfrac{\prod_{i=1}^{l} p_i^{\alpha_i}}{\prod_{j=1}^{m} q_j^{\beta_j}}$, où $\forall i \in [\![1, l]\!]$, $\forall j \in [\![1, m]\!]$, $\alpha_i \in \mathbb{N}^*$, $\beta_j \in \mathbb{N}^*$ et les $p_i, q_j \in \mathcal{P}$ sont tels que $\{p_1, \ldots, p_l\} \cap \{q_1, \ldots, q_m\} = \emptyset$. Alors, on pose :

1. $q_j^{'} = q_j^{\beta_j}$ si $\beta_j \equiv 0\,[2]$
2. $q_j^{'} = q_j^{\beta_j+1}$ si $\beta_j \equiv 1\,[2]$

Alors, ainsi construit, $\prod_{j=1}^{m} q_j^{'}$ est un carré de $\mathbb{Q}^*$ et

$$\prod_{j=1}^{m} q_j^{'} \times r = r \text{ dans } \mathbb{Q}^*/(\mathbb{Q}^*)^2.$$

On réduit encore $\prod_{j=1}^{m} q_j^{'} \times r$ modulo les carrés de $\mathbb{Q}^*$. Notant $\overline{\beta_j} \in \{0,1\}$ le reste de la division par 2 de β_j et $\overline{\alpha_i} \in \{0,1\}$ le reste de la division par 2 de α_i, on a :

$$\prod_{j=1}^{m} q_j^{'} \times r = \prod_{j=1}^{m} q_j^{\overline{\beta_j}} \prod_{i=1}^{l} p_i^{\overline{\alpha_i}} \text{ dans } \mathbb{Q}^*/(\mathbb{Q}^*)^2.$$

Finalement après réduction, $r = n$ dans $\mathbb{Q}^*/(\mathbb{Q}^*)^2$ où $n = \prod_{j=1}^{m} q_j^{\overline{\beta_j}} \prod_{i=1}^{l} p_i^{\overline{\alpha_i}}$ est sans facteur carré.

Remarque 7.1.2. *Nous pouvons constater que pour tout entier premier p ne divisant aucun des nombres entiers relatifs $a_1, \ldots, a_n$, on a :*

$$\begin{aligned} \partial_p(< a_1, \ldots, a_n >) &= < \partial_p(a_1), \ldots, \partial_p(a_n) > \\ &= < 0, \ldots, 0 > \\ &= 0_{W(\mathbb{F}_p)} \end{aligned}$$

Pour montrer, la proposition précédente, nous aurons besoin d'utiliser la présentation de $W(\mathbb{Q})$ par générateurs et relations et les deux lemmes qui suivent :

Lemme 7.1.1. *Pour $p \in \mathcal{P}$, l'application res_p est un morphisme de groupes de $(\mathbb{Q}^*, \times)$ dans $(\mathbb{F}_p^*, \times)$.*

Démonstration. Soit $r_1, r_2 \in \mathbb{Q}^*$ et $p \in \mathcal{P}$. Alors, il existe deux couples d'entiers (p_1, q_1) et (p_2, q_2) tels que $r_1 = p^{\nu_p(r_1)} \dfrac{p_1}{q_1}$ et $r_2 = p^{\nu_p(r_2)} \dfrac{p_2}{q_2}$, où les p_i, q_j sont premiers avec p. Ainsi, $r_1 r_2 = p^{\nu_p(r_1)+\nu_p(r_2)} \dfrac{p_1 p_2}{q_1 q_2}$ où $p_1 p_2$ et $q_1 q_2$ sont premiers avec p et donc $\nu_p(r_1 r_2) = \nu_p(r_1) + \nu_p(r_2)$, soit :

$$res_p(r_1) res_p(r_2) = \overline{p_1}(\overline{q_1})^{-1} \times \overline{p_2}(\overline{q_2})^{-1} = \overline{p_1 p_2}(\overline{q_1 q_2})^{-1} = res_p(r_1 r_2)$$

D'où le résultat. □

Lemme 7.1.2. *Soit $a, b \in \mathbb{Q}^*$.*

1. *Si $\nu_p(a) > \nu_p(b)$, alors $\nu_p(a+b) = \nu_p(b)$ et $res_p(a+b) = res_p(b)$.*
2. *Si $\nu_p(a) = \nu_p(b)$ et $\nu_p(a+b) \neq \nu_p(a)$, alors $res_p(b) = -res_p(a)$.*

Démonstration. Comme pour le lemme précédent, il existe deux couples d'entiers (p_1, q_1) et (p_2, q_2) tels que $a = p^{\nu_p(a)} \dfrac{p_1}{q_1}$ et $b = p^{\nu_p(b)} \dfrac{p_2}{q_2}$, où les p_i, q_j sont premiers avec p. Alors, si $\nu_p(a) > \nu_p(b)$:

$$(a+b) = p^{\nu_p(b)}\left(\frac{p_2}{q_2} + p^{\nu_p(a)-\nu_p(a)} \frac{p_1}{q_1}\right) = p^{\nu_p(b)}\left(\frac{p_2 q_1 + p^{\nu_p(a)-\nu_p(b)} p_1 q_2}{q_1 q_2}\right)$$

Or, $\overline{p_2 q_1 + p^{\nu_p(a)-\nu_p(b)} p_1 q_2}$ et $q_1 q_2$ sont premiers avec p, (p ne les divisant pas) avec $\overline{p_2 q_1 + p^{\nu_p(a)-\nu_p(b)} p_1 q_2} = \overline{p_2 q_1} \in \mathbb{F}_p$, ce qui donne :

$$res_p(a+b) = \overline{p_2q_1}(\overline{q_1q_2})^{-1} = \overline{p_2}(\overline{q_2})^{-1} = res_p(b)$$

Supposons $\nu_p(a) = \nu_p(b)$, alors $a+b = p^{\nu_p(a)}(\frac{p_1q_2+p_2q_1}{q_1q_2})$ et nécessairement $p \mid p_1q_2+p_2q_1$ puisque $\nu_p(a+b) \neq \nu_p(a)$ et $p \nmid q_1q_2$. Ainsi, $\overline{p_1q_2+q_1p_2} = \overline{0} \in \mathbb{F}_p$ et $\overline{p_1q_2} = -\overline{q_1p_2} \Longrightarrow \overline{p_1}(\overline{q_1})^{-1} = -\overline{p_2}(\overline{q_2})^{-1}$, soit $res_p(a) = -res_p(b)$. □

Passons à la démonstration de la proposition.

Démonstration. Pour $p \in \mathcal{P}$, on définit pour commencer une application f de $\mathbb{Q}^*$ dans $W(\mathbb{F}_p)$, par $f(r) =< \partial_p(r) >$. Le but est alors de vérifier que :

- $f(\delta^2 a) = f(a)$ quelque soit $(a,\delta) \in (\mathbb{Q}^*)^2$.
- $f(a)+f(b) = f(a+b)+f((a+b)ab)$ quelque soit $(a,b) \in (\mathbb{Q}^*)^2$ tel que $a+b \neq 0$.
- $f(-1) = -f(1)$

ce qui montrera qu'il existe une unique application $\overline{f} : W(\mathbb{Q}) \longrightarrow W(\mathbb{F}_p)$ tel que $\forall r \in \mathbb{Q}^*$, $\overline{f}(< r >) = f(r) =< \partial_p(r) >$ et ce qui prouvera la proposition. Soit alors $(r,\delta) \in (\mathbb{Q}^*)^2$, on a :

$$\begin{aligned} f(\delta^2 r) &= < \partial_p(\delta^2 r) > \\ &= < s_p(\delta^2 r) res_p(\delta^2 r) > \\ &= < s_p(\delta^2 r) res_p(\delta)^2 res_p(r) > \\ &= < s_p(r) res_p(r) res_p(\delta)^2 > \\ &= < s_p(r) res_p(r) > \\ &= f(r) \end{aligned}$$

puisque $\nu_p(\delta^2 r) = 2\nu_p(\delta)+\nu_p(r) \equiv \nu_p(r)\,[2]$ et que $res_p(\delta)^2$ est un carré non nul de $\mathbb{F}_p$. Ceci donne alors la première condition. De plus $f(-1) =< -1 >\in W(\mathbb{F}_p)$ et on sait que dans $W(\mathbb{F}_p)$, $[-q]_W = -[q]_W$, pour q régulière. Ce qui donne naturellement la troisième condition. Il reste donc simplement à vérifier que $\forall (a,b) \in (\mathbb{Q}^*)^2, a+b \neq 0$,

$$< \partial_p(a) > + < \partial_p(b) >=< \partial_p(a+b) > + < \partial_p((a+b)ab) > \text{ dans } W(\mathbb{F}_p).$$

On va montrer la validité de la relation ci-dessus, en faisant une disjonction des cas :

- si $\nu_p(a) > \nu_p(b)$ (le cas $\nu_p(b) > \nu_p(a)$ se traite de manière similaire, a et b jouant des rôles identiques dans la relation de Witt). Alors, par le premier lemme, $res_p(a+b) = res_p(b)$ et $\nu_p(a+b) = \nu_p(b) \Longrightarrow s_p(a+b) = s_p(b)$ et ν_p étant un morphisme,
  $$\nu_p((a+b)ab) = \nu_p(a+b)+\nu_p(a)+\nu_p(b) = 2\nu_p(b)+\nu_p(a),$$
  soit $s_p((a+b)ab) = s_p(a)$. D'où,
  $< \partial_p(a+b) >=< s_p(a+b) res_p(a+b) >=< s_p(b) res_p(b) >=< \partial_p(b) >$.
  De même,

$$\begin{aligned} \partial_p((a+b)ab) &= s_p((a+b)ab) res_p((a+b)ab) \\ &= s_p(a) res_p((a+b)ab) \\ &= s_p(a) res_p(a+b) res_p(a) res_p(b) \\ &= s_p(a) res_p(b) res_p(a) res_p(b) \\ &= \partial_p(a) res_p(b)^2 \end{aligned}$$

et donc $< \partial_p((a+b)ab) >=< \partial_p(a) >$ dans $W(\mathbb{F}_p)$, ce qui donne bien le résultat.

- Supposons $\nu_p(a) = \nu_p(b)$, ce qui implique $s_p(a) = s_p(b)$. Or, pour tout $r \in \mathbb{Q}^*$, $res_p(r) \in \mathbb{F}_p^*$ et donc pour $p = 2$, on a :
$$res_p(a+b) = res_p(a) = res_p(b) = resp_p((a+b)ab) = \overline{1} \in \mathbb{F}_2^*$$
et $\nu_p((a+b)ab) = \nu_p(a+b) + 2\nu_p(a) \Longrightarrow s_p((a+b)ab) = s_p(a+b)$, soit :
$$< \partial_p((a+b)ab) > + < \partial_p(a+b) >= 2 < s_p(a+b) > \text{ et}$$
$$< \partial_p(a) > + < \partial_p(b) >= 2 < s_p(a) >$$
Or $W(\mathbb{F}_2) \simeq \mathbb{Z}/2 \Longrightarrow 2 < s_p(a+b) >= 2 < s_p(a) >= 0_{W(\mathbb{F}_2)}$, ce qui achève de montrer le résultat si $p = 2$
- Soit $p \neq 2$ et $\nu_p(a) = \nu_p(b) \equiv 0\,[2]$ et $\nu_p(a+b) \equiv 0\,[2]$. Alors, les égalités :
$$s_p(a) = s_p(b) = s_p(a+b) = s_p((a+b)ab) = 0$$
impliquent
$$< \partial_p(a) >=< \partial_p(b) >=< \partial_p(a+b) >=< \partial_p((a+b)ab) >= 0$$
D'où le résultat.
- $p \neq 2$ et $\nu_p(a) = \nu_p(b) \equiv 0\,[2]$ et $\nu_p(a+b) \equiv 1\,[2]$. On a encore,
$$s_p(a) = s_p(b) = 0 \Longrightarrow < \partial_p(a) >=< \partial_p(b) >= 0$$
Puisque $\nu_p(a) \neq \nu_p(a+b)$, $res_p(a) = -res_p(b)$ et :

$$\begin{aligned}
< \partial_p((a+b)ab) >= & < s_p((a+b)ab) res_p((a+b)ab) > \\
= & < s_p(a+b) res_p((a+b)ab) > \\
= & < -s_p(a+b) res_p(a+b) res_p(a) res_p(a) > \\
= & < -\partial_p(a+b) res_p(a)^2 > \\
= & < -\partial_p(a+b) > \\
= & - < \partial_p(a+b) >
\end{aligned}$$

Ainsi $< \partial_p((a+b)ab) > + < \partial_p(a+b) >= 0$. D'où le résultat.
- $p \neq 2$ et $\nu_p(a) = \nu_p(b) \equiv 1\,[2]$ et $\nu_p(a+b) \equiv 0\,[2]$. Alors,
$$s_p(a+b) = s_p((a+b)ab) = 0 \text{ et } s_p(a) = s_p(b) = 1$$
Puisque $\nu_p(a) \neq \nu_p(a+b)$ on a $res_p(a) = -res_p(b)$ et :
$$< \partial_p(a) >=< -\partial_p(b) > \text{ et } < \partial_p(a+b) >=< \partial_p(a+b)ab >= 0$$
soit :
$$< \partial_p(a) > + < \partial_p(b) >= 0 =< \partial_p(a+b) > + < \partial_p(a+b)ab >= 0$$
D'où le résultat.
- $p \neq 2$ et $\nu_p(a) = \nu_p(b) \equiv 1\,[2]$ et $\nu_p(a+b) \equiv 1\,[2]$ On a alors :
$$s_p(a) = s_p(b) = s_p(a+b) = s_p((a+b)ab) = 1.$$
Montrons que $\langle \partial_p(a), \partial_p(b) \rangle \simeq \langle \partial_p(a+b), \partial_p((a+b)ab) \rangle$, ce qui donnera le résultat souhaité. Sur le corps fini $\mathbb{F}_p$, il suffit de montrer que les deux formes quadratiques ont même discriminant, ayant même dimension. Dans $\mathbb{F}_p^*/(\mathbb{F}_p^*)^2$,

$$\begin{aligned}
\partial_p(a+b)\partial_p((a+b)ab) = & \; res_p(a+b) res_p((a+b)ab) \\
= & \; res_p(a+b)^2 res_p(a) res_p(b) \\
= & \; res_p(a+b)^2 \partial_p(a) \partial_p(b) \\
= & \; \partial_p(a) \partial_p(b)
\end{aligned}$$

D'où le résultat.

□

7.2 Enoncé des tests de Witt-équivalence et d'équivalence sur $\mathbb{Q}$

Enonçons désormais le test de Witt-équivalence sur $\mathbb{Q}$ que nous ne démontrerons pas mais dont nous proposerons des éléments de justifications dans les sections suivantes.

Théorème 7.2.1. ***Test de Witt-équivalences sur*** $\mathbb{Q}$
Deux formes quadratiques rationnelles régulières ϕ et ψ sont Witt-équivalentes si et seulement si elles ont la même signature réduite *et si l'on a :*

$$\partial_p([\phi]_W) = \partial_p([\psi]_W)$$

pour tout nombre premier p.

Théorème 7.2.2. ***Test d'équivalence sur*** $\mathbb{Q}$
Deux formes quadratiques rationnelles régulières ϕ et ψ sont équivalentes si et seulement si elles ont même signature *et si l'on a :*

$$\partial_p([\phi]_W) = \partial_p([\psi]_W)$$

pour tout nombre premier p.

Démonstration. On note (m, n) et (m', n') les signatures associées à ϕ et ψ. Par régularité $dim(\phi) = m + n$ et $dim(\psi) = m' + n'$ et si on suppose ϕ et ψ équivalentes, alors elles sont Witt-équivalentes et de même dimension. Par le théorème ci-dessus, elles ont même dimension, même signature réduite et $\partial_p([\phi]_W) = \partial_p([\psi]_W)$ pour tout nombre premier p. Or,

$$m - n = m' - n' \text{ et } m + n = m' + n' \Longrightarrow (m, n) = (m', n')$$

et donc si ϕ et ψ sont équivalentes, elles ont même signature et pour tout nombre premier p, $\partial_p([\phi]_W) = \partial_p([\psi]_W)$. Inversement, si on suppose $(m, n) = (m', n')$ et que $\partial_p([\phi]_W) = \partial_p([\psi]_W)$ pour tout nombre premier p, alors en particulier, elles ont même signature réduite $(m - n = m' - n')$, même dimension puisque $m + n = m' + n'$ et $\partial_p([\phi]) = \partial_p([\psi])$ pour tout nombre premier p. Ceci montre qu'elles sont Witt-équivalentes d'après le test ci dessus et de même dimension, d'où équivalentes. □

Corollaire 7.2.1. *Soit $a_1, \ldots, a_n \in \mathbb{Z}^*$ sans facteur carré, tout comme $b_1, \ldots, b_n$. Alors $\langle a_1, \ldots, a_n \rangle \simeq \langle b_1, \ldots, b_n \rangle$ sur $\mathbb{Q}$ si et seulement si elles ont même signature et si pour tout $p \in \mathcal{P}$ divisant au moins un des a_i ou un des b_j, on a :*

$$< \partial_p(a_1), \ldots, \partial_p(a_n) >=< \partial_p(b_1), \ldots, \partial_p(b_n) > \in W(\mathbb{F}_p)$$

Démonstration. Ceci découle simplement du test d'équivalence rationnelle et du fait que si p ne divise aucun des a_i et aucun des b_j alors, on a déjà l'égalité :

$$0_{W(\mathbb{F}_p)} =< \partial_p(a_1), \ldots, \partial_p(a_n) >=< \partial_p(b_1), \ldots, \partial_p(b_n) >= 0_{W(\mathbb{F}_p)}$$

□

Corollaire 7.2.2. *Une forme quadratique rationnelle régulière ϕ de dimension $2m$ est hyperbolique si et seulement si sa signature est (m, m) et $\partial_p([\phi]_W) = 0$ pour tout nombre premier p.*

Démonstration. ϕ de dimension $2m$ est hyperbolique sur $\mathbb{Q}$ si et seulement si $\phi \simeq m.\langle 1,-1\rangle$. Or $m.\langle 1,-1\rangle \simeq m.\langle 1\rangle \perp m.\langle -1\rangle$ et est de signature (m,m). De plus pour tout nombre premier p, on a :

$$\partial_p(1) = \partial_p(-1) = 0 \in \mathbb{F}_p \Longrightarrow \partial_p(m. < 1,-1 >) = 0_{W(\mathbb{F}_p)}$$

D'où, d'après le théorème ci-dessus, ϕ est hyperbolique si et seulement si de signature (m,m) et si $\partial_p(\phi) = 0_{W(\mathbb{F}_p)}$ pour tout nombre premier p. □

Exemple 7.2.1. *$\langle 1,1,1,1\rangle$ est hyperbolique sur tout corps fini, en revanche étant de signature $(4,0)$, elle n'est pas hyperbolique sur $\mathbb{Q}$.*

Remarque 7.2.1. *Les énoncés de ces deux tests montrent qu'il est nécessaire de bien comprendre et de bien maîtriser la classification des formes quadratiques sur les corps finis, pour comprendre la classification sur $\mathbb{Q}$. Dans la suite de ce mémoire, nous mettrons aussi en avant qu'il est important de bien comprendre les formes quadratiques sur les corps p-adiques $\mathbb{Q}_p$ pour bien assimiler la classification rationnelle.*

7.3 Rappels sur l'extension des scalaires et application aux formes quadratiques

On va dans cette partie rappeler quelques résultats concernant l'extension des scalaires. Notre objectif étant de montrer que pour $\mathbb{K} \subset \mathbb{L}$ une extension de corps donnée et (E,q) un espace quadratique de dimension finie sur $\mathbb{K}$, il existe une unique forme quadratique sur $\mathbb{L}$, que nous noterons $q_{\mathbb{L}}$ et prolongeant q sur le $\mathbb{L}$-espace vectoriel $\mathbb{L} \otimes_{\mathbb{K}} E$.

7.3.1 Prolongement d'une forme quadratique de E à $E_{\mathbb{L}}$

Soit E un $\mathbb{K}$-espace vectoriel, alors $\mathbb{L} \otimes_{\mathbb{K}} E$ est aussi un $\mathbb{K}$-espace vectoriel que l'on munit d'une structure de $\mathbb{L}$-espace vectoriel tel que :

$$\forall (a,b,x) \in \mathbb{L}^2 \times E,\ b.(a \otimes x) = (ba) \otimes x.$$

On note alors $E_{\mathbb{L}} = \mathbb{L} \otimes_{\mathbb{K}} E$, qui est un $\mathbb{L}$-espace vectoriel de même dimension que le $\mathbb{K}$-espace vectoriel E, $(1 \otimes e_i)_{1 \leq i \leq n}$ étant une base du $\mathbb{L}$-espace vectoriel $E_{\mathbb{L}}$ si $(e_i)_{1 \leq i \leq n}$ est une base du $\mathbb{K}$-espace vectoriel E. On identifie E à un sous-$\mathbb{K}$ espace vectoriel de $E_{\mathbb{L}}$, via l'injection, $x \longrightarrow 1 \otimes x$.

Proposition 7.3.1. *Soit (E,q) un $\mathbb{K}$ espace quadratique de dimension finie. Il existe alors, une unique forme quadratique sur le $\mathbb{L}$-espace vectoriel $E_{\mathbb{L}}$, $q_{\mathbb{L}}$ prolongeant q, c'est-à-dire :*

$$\forall x \in E,\ q_{\mathbb{L}}(1 \otimes x) = q(x)$$

Dans chaque base du $\mathbb{K}$-espace vectoriel E, les formes q et $q_{\mathbb{L}}$ sont représentées par la même matrice (en identifiant la base $\boldsymbol{B}$ du $\mathbb{K}$-espace vectoriel E et la base $1 \otimes \boldsymbol{B}$ du $\mathbb{L}$-espace vectoriel $E_{\mathbb{L}}$, via l'identification $E \subset \mathbb{L} \otimes_{\mathbb{K}} E$).

Démonstration. On note b_q, la forme bilinéaire associée à q. Soit ϕ supposée solution du problème, c'est-à-dire que ϕ prolonge q sur $E_{\mathbb{L}}$. On note b_ϕ, la forme polaire associée à ϕ, alors par polarisation :

$$\forall (x,y) \in \mathbb{K}^2, b_\phi(1\otimes x, 1\otimes y) = \frac{1}{2}(\phi(1\otimes x + 1\otimes y) - \phi(1\otimes x) - \phi(1\otimes y))$$

et ϕ prolongeant q, $\forall x \in \mathbb{K}, \phi(1\otimes x) = q(x)$ et donc

$$b_\phi(1\otimes x, 1\otimes y) = \frac{1}{2}[q(x+y) - q(x) - q(y)] = b_q(x,y).$$

Ainsi, b_ϕ prolonge nécessairement b_q. Or, $1\otimes_{\mathbb{K}} E$ étant une partie génératrice de $\mathbb{L}\otimes_{\mathbb{K}} E$, si ϕ est un prolongement de q, il est unique, car sa forme polaire associée est un prolongement de b_q et est donc entièrement et uniquement déterminée sur la partie génératrice $1\otimes_{\mathbb{K}} E$.

Réciproquement, soit $\mathbf{B}$ une base de E, dans laquelle q est représentée par la matrice A. Sur le $\mathbb{L}$-espace vectoriel $E_{\mathbb{L}}$, on considère ϕ la forme quadratique représentée par A dans la base $1\otimes B$. On note $\mathbf{B} = (e_1 \ldots, e_n)$ et $n = dim(E)$. Pour $x \in E$, il existe un n-uplet de scalaires déterminé de manière unique $(\alpha_1, \ldots, \alpha_n)$ tel que $x = \alpha_1 e_1 + \ldots + \alpha_n e_n$ et donc :

$$q(x) = {}^t(\alpha_1, \ldots, \alpha_n) A (\alpha_1, \ldots, \alpha_n).$$

Alors, ϕ étant représenté par A dans $1\otimes B = (1\otimes e_1, \ldots, 1\otimes e_n)$, pour $x \in E$, $1\otimes x = 1\otimes(\alpha_1 e_1 + \ldots + \alpha_n e_n) = \alpha_1 \times (1\otimes e_1) + \ldots + \alpha_n \times (1\otimes e_n)$ et donc dans $1\otimes B$, on a :

$$\phi(1\otimes x) = {}^t(\alpha_1, \ldots, \alpha_n) A (\alpha_1, \ldots, \alpha_n) = q(x)$$

ce qui montre bien que ϕ prolonge q et est l'unique solution du problème. Enfin, si $\mathbf{B} = (e_1 \ldots, e_n)$ est une base du $\mathbb{K}$-espace vectoriel E, $1\otimes \mathbf{B}$ est une base du $\mathbb{L}$-espace vectoriel $E_{\mathbb{L}}$ et il est clair que :

$$Mat_B(q) = (bq(e_i, e_j))_{1\leq i,j\leq n} = (b_{q_{\mathbb{L}}}(1\otimes e_i, 1\otimes e_j))_{1\leq i,j\leq n} = Mat_{1\otimes B}(q_{\mathbb{L}}).$$

□

Voyons quelques propriétés :

1. si ϕ et ψ sont équivalentes sur $\mathbb{K}$, alors $\phi_{\mathbb{L}}$ et $\psi_{\mathbb{L}}$ sont équivalentes sur $\mathbb{L}$. On sait que ϕ et ψ ont même classe de congruence de matrices symétriques associées, il existe donc deux bases $\mathbf{B}$ et $\mathbf{B'}$ telles que :

   $$Mat_{1\otimes \mathbf{B'}}(\psi) = Mat_{\mathbf{B'}}(\psi) = Mat_{\mathbf{B}}(\phi) = Mat_{1\otimes \mathbf{B}}(\phi_{\mathbb{L}})$$

   Ainsi $\phi_{\mathbb{L}}$ et $\psi_{\mathbb{L}}$ ont même classe de congruence de matrices symétriques associées sur $\mathbb{L}$ et sont donc équivalentes.

2. Pour (E_1, ϕ) et (E_2, ψ) deux espaces quadratiques, en passant encore par l'étude des matrices symétriques associées, on a : $(\phi\perp\psi)_{\mathbb{L}} \simeq \phi_{\mathbb{L}}\perp\psi_{\mathbb{L}}$. En effet, notant $\mathbf{B}_1$ une base de E_1 et $\mathbf{B}_2$ une base de E_2. On définit :

   $$A = Mat_{\mathbf{B}_1}(\phi) = Mat_{1\otimes\mathbf{B}_1}(\phi_{\mathbb{L}}) \text{ et } B = Mat_{\mathbf{B}_2}(\psi) = Mat_{1\otimes\mathbf{B}_2}(\psi_{\mathbb{L}})$$

   On a donc :

   $$Mat_{(1\otimes\mathbf{B}_1, 1\otimes\mathbf{B}_2)}(\phi_{\mathbb{L}}\perp\psi_{\mathbb{L}}) = \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix} = Mat_{(\mathbf{B}_1,\mathbf{B}_2)}(\phi\perp\psi)$$
   $$= Mat_{(1\otimes\mathbf{B}_1, 1\otimes\mathbf{B}_2)}(\phi\perp\psi)_{\mathbb{L}}$$

   Ainsi, $\phi_{\mathbb{L}}\perp\psi_{\mathbb{L}}$ et $(\phi\perp\psi)_{\mathbb{L}}$ ont même classe de congruence de matrices symétriques associées et sont équivalentes.

7.3.2 Morphismes $W(\mathbb{K}) \longrightarrow W(\mathbb{L})$ et $\widehat{W}(\mathbb{K}) \longrightarrow \widehat{W}(\mathbb{L})$ induits par l'extension des scalaires

Soit $\mathbb{L}$ une extension du corps $\mathbb{K}$. Utilisons la présentation des groupes $W(\mathbb{K})$ et $\widehat{W}(\mathbb{K})$ par générateurs et relations, pour établir l'existence de deux morphismes de groupes induits par l'opération d'extension du corps de base, que nous avons appliquée dans le cadre des formes quadratiques dans la partie précédente. On définit ainsi les applications :

$$\phi_1 : \begin{cases} \mathbb{K}^* \longrightarrow W(\mathbb{L}) \\ a \longmapsto < a >_{\mathbb{L}} \end{cases}$$

et

$$\phi_2 : \begin{cases} \mathbb{K}^* \longrightarrow \widehat{W}(\mathbb{L}) \\ a \longmapsto \langle a \rangle_{\mathbb{L}} \end{cases}$$

où on note $< a >_{\mathbb{L}}$, la classe de Witt-équivalence sur $\mathbb{L}$ de la forme quadratique $\langle a \rangle_{\mathbb{L}}$ prolongée à $\mathbb{L}$ et on note encore $\langle a \rangle_{\mathbb{L}}$ la classe d'isomorphie $[\langle a \rangle_{\mathbb{L}}]$ identifiée par injectivé de $i_{FQ(\mathbb{L})}$ à l'élément $i_{FQ(\mathbb{L})}(\langle a \rangle_{\mathbb{L}}) \in \widehat{W}(\mathbb{L})$.

On va alors montrer, par la seconde propriété universelle des groupes de Witt et Witt-Grothendieck que ces deux applications induisent deux morphismes :

$$\overline{\phi_1} : W(\mathbb{K}) \longrightarrow W(\mathbb{L}) \text{ et } \overline{\phi_2} : \widehat{W}(\mathbb{K}) \longrightarrow \widehat{W}(\mathbb{L})$$

tels que $\forall a \in \mathbb{K}^*$, $\overline{\phi_1}(< a >_{\mathbb{K}}) =< a >_{\mathbb{L}}$ et $\overline{\phi_2}(\langle a \rangle_{\mathbb{K}}) = \langle a \rangle_{\mathbb{L}}$. Pour q forme quadratique régulière sur $\mathbb{K}$ et via l'identification de $[q] \in FQ(\mathbb{K})$ avec $i_{FQ(\mathbb{K})}([q])$, on aura en particulier :

$$\overline{\phi}_1([q]_W) = [q_{\mathbb{L}}]_W \text{ et } \overline{\phi_2}([q]) = [q_{\mathbb{L}}]$$

Puisque l'on a sur $\mathbb{K}$:

$$\langle \delta^2 a \rangle \simeq \langle a \rangle \text{ et } \langle a \rangle \perp \langle b \rangle \simeq \langle a+b \rangle \perp \langle (a+b)ab \rangle$$

d'après les propriétés de l'extension des scalaires vues dans la partie précédente, on a :

$$\langle \delta^2 a \rangle_{\mathbb{L}} \simeq \langle a \rangle_{\mathbb{L}} \text{ et } \langle a \rangle_{\mathbb{L}} \perp \langle b \rangle_{\mathbb{L}} \simeq \langle a+b \rangle_{\mathbb{L}} \perp \langle (a+b)ab \rangle_{\mathbb{L}}$$

et en particulier $\forall (a, \delta) \in (\mathbb{K}^*)^2$ et $(a, b) \in (\mathbb{K}^*)^2$ tels que $a + b \neq 0$:

$$\langle \delta^2 a \rangle_{\mathbb{L}} \overset{W}{\sim} \langle a \rangle_{\mathbb{L}} \text{ et } \langle a \rangle_{\mathbb{L}} \perp \langle b \rangle_{\mathbb{L}} \overset{W}{\sim} \langle a+b \rangle_{\mathbb{L}} \perp \langle (a+b)ab \rangle_{\mathbb{L}}$$

ce qui donne donc pour $i \in [\![1, 2]\!]$:

- $\phi_i(\delta^2 a) = \phi_i(a)$ quelque soit $(a, \delta) \in (\mathbb{K}^*)^2$.
- $\phi_i(a) + \phi_i(b) = \phi_i(a+b) + \phi_i((a+b)ab)$ quelque soit $(a, b) \in (\mathbb{K}^*)^2$ tel que $a + b \neq 0$.

De plus $\langle -1 \rangle \perp \langle 1 \rangle \simeq \langle 1, -1 \rangle \Longrightarrow \langle -1 \rangle_{\mathbb{L}} \perp \langle 1 \rangle_{\mathbb{L}} \simeq \langle 1, -1 \rangle_{\mathbb{L}}$ et donc dans $W(\mathbb{L})$: $< -1 >_{\mathbb{L}} + < 1 >_{\mathbb{L}} =< 1, -1 >_{\mathbb{L}} = 0_{W(\mathbb{L})}$, soit $< -1 >_{\mathbb{L}} = - < 1 >_{\mathbb{L}}$ et $\phi_2(-1) = -\phi_2(1)$. Ceci achève de montrer l'existence des deux morphismes annoncés.

7.4 Structure de $W(\mathbb{Q})$: justification du test de Witt-équivalence sur $\mathbb{Q}$

L'inclusion du corps $\mathbb{Q}$ dans $\mathbb{R}$ induit donc un morphisme canonique d'extension des scalaires, $W(\mathbb{Q}) \longrightarrow W(\mathbb{R})$. L'image d'un élément $x \in W(\mathbb{Q})$ sera noté $x_{\mathbb{R}}$. $W(\mathbb{Q})$ étant engendré par $\{< a >, a \in \mathbb{Q}^*\}$, il existe des $(a_1, \ldots, a_n) \in (\mathbb{Q}^*)^n$ tels que $x =< a_1 > + \ldots + < a_n >$ et nous avons pu constater que l'on pouvait en fait prendre les a_i dans $\mathbb{Z}^*$ et sans facteur carré. Ainsi, si $p \in \mathcal{P}$ ne divise aucun des entiers a_i, $\partial_p(a_i) = 0, \forall i \in [\![1, n]\!]$ et la suite $(\partial_p(x))_{p\in\mathcal{P}}$ est presque nulle. Ceci justifie la validité de la définition de l'application suivante :

$$\Phi\colon \begin{cases} W(\mathbb{Q}) \longrightarrow W(\mathbb{R}) \oplus \bigoplus_{p\in\mathcal{P}} W(\mathbb{F}_p) \\ x \longmapsto\ x_{\mathbb{R}} + \sum_{p\in\mathcal{P}} \partial_p(x) \end{cases}$$

où la somme directe $\bigoplus_{p\in\mathcal{P}} W(\mathbb{F}_p)$ est une somme directe externe, formée des sous-familles à support fini de $\prod_{p\in\mathcal{P}} W(\mathbb{F}_p)$. Le théorème suivant décrivant la structure de $W(\mathbb{Q})$ justifie en particulier le test de Witt-équivalence rationnelle.

Théorème 7.4.1. *L'application $\Phi : W(\mathbb{Q}) \longrightarrow W(\mathbb{R}) \oplus \bigoplus_{p\in\mathcal{P}} W(\mathbb{F}_p)$ est un isomorphisme de groupes.*

Démonstration. cf.[1] XVII, page 364. □

L'application Φ étant bijective, elle est en particulier injective. Ainsi, si ϕ et ψ sont deux formes formes quadratiques rationnelles, régulières, on a :

$$\Phi([\phi]_W) = \Phi([\psi]_W) \Longleftrightarrow [\phi]_W = [\psi]_W$$

et donc ψ et ϕ sont Witt-équivalentes si et seulement si $[\phi_{\mathbb{R}}]_W = [\psi_{\mathbb{R}}]_W$ et si $\forall p \in \mathcal{P}$, $\partial_p([\phi]_W) = \partial_p([\psi]_W)$. Sur $\mathbb{R}$, deux formes quadratiques étant Witt-équivalentes si et seulement si elles ont la même signature réduite, on a :

$$\begin{aligned} \psi \overset{W}{\sim} \phi \Longleftrightarrow\ & \phi_{\mathbb{R}} \text{ et } \psi_{\mathbb{R}} \text{ ont même signature réduite et si} \\ & \forall p \in \mathcal{P},\ \partial_p([\phi]_W) = \partial_p([\psi]_W). \end{aligned}$$

Or, en diagonalisant ϕ régulière de dimension n, il existe $a_1, \ldots, a_n \in \mathbb{Q}^* \subset \mathbb{R}^*$ tel que :

$$\phi \simeq \langle a_1, \ldots, a_n \rangle$$

et donc $\phi_{\mathbb{R}} \simeq \langle a_1, \ldots, a_n \rangle_{\mathbb{R}}$. Dans une base $\mathbf{B}$, ϕ est représentée par la matrice diagonale $D(a_1, \ldots, a_n)$ qui représente aussi la forme quadratique réelle, $\phi_{\mathbb{R}}$. Ainsi ϕ et $\phi_{\mathbb{R}}$ ont la même signature. On a donc également :

$$\begin{aligned} \psi \overset{W}{\sim} \phi \Longleftrightarrow\ & \phi \text{ et } \psi \text{ ont même signature réduite et si} \\ & \forall p \in \mathcal{P},\ \partial_p([\phi]_W) = \partial_p([\psi]_W). \end{aligned}$$

Ce qui donne bien une justification du test de Witt-équivalence rationnelle.

7.5 Structure détaillée de $W(\mathbb{Q})$ et $\widehat{W}(\mathbb{Q})$

Théorème 7.5.1. Structure du groupe de Witt W($\mathbb{Q}$) et du groupe de Witt-Grothendieck $\widehat{W}(\mathbb{Q})$.

1. $W(\mathbb{Q}) \simeq \mathbb{Z} \times (\mathbb{Z}/2)^{(\mathbb{N})} \times (\mathbb{Z}/4)^{(\mathbb{N})}$
2. $\widehat{W}(\mathbb{Q}) \simeq \mathbb{Z} \times 2\mathbb{Z} \times (\mathbb{Z}/2)^{(\mathbb{N})} \times (\mathbb{Z}/4)^{(\mathbb{N})}$

Démonstration. Pour démontrer 1) Il s'agit simplemement d'utiliser les isomorphismes suivant qui ont été précédemment établis :
- $W(\mathbb{Q}) \simeq W(\mathbb{R}) \oplus \bigoplus_{p\in\mathcal{P}} W(\mathbb{F}_p)$
- $W(\mathbb{R}) \simeq \mathbb{Z}$
- $W(\mathbb{F}_2) \simeq \mathbb{Z}/2$
- $W(\mathbb{F}_p) \simeq \mathbb{Z}/2 \times \mathbb{Z}/2$ si p $\in \mathcal{P}$ et $p \equiv 1\,[4]$
- $W(\mathbb{F}_p) \simeq \mathbb{Z}/4$ si p $\in \mathcal{P}$ et $p \equiv 3\,[4]$

On rappelle également que le premier isomorphisme est obtenu via la fonction Φ définie par :

$$\Phi\colon \begin{cases} W(\mathbb{Q}) \longrightarrow\ W(\mathbb{R}) \oplus \bigoplus_{p\in\mathcal{P}} W(\mathbb{F}_p) \\ x \longmapsto x_{\mathbb{R}} + \sum_{p\in\mathcal{P}} \partial_p(x) \end{cases}$$

D'après le théorème des nombres premiers de Dirichlet il existe une infinité de nombres premiers congrus à 1 ou à 3 modulo 4 (car $4\wedge 1 = 1, 4\wedge 3 = 1$) et donc une infinité de nombres premiers p tels $W(\mathbb{F}_p) \simeq \mathbb{Z}/2 \times \mathbb{Z}/2$ et $W(\mathbb{F}_p) \simeq \mathbb{Z}/4$, ce qui nous donne grâce aux 5 isomorphismes de groupes rappelés ci-dessus $W(\mathbb{Q}) \simeq \mathbb{Z} \times (\mathbb{Z}/2)^{(\mathbb{N})} \times (\mathbb{Z}/4)^{(\mathbb{N})}$ où l'exposant $(\mathbb{N})$ signifie qu'il s'agit de suites presque nulles. Ceci est une conséquence du fait que pour $x \in W(\mathbb{Q})$, on a vu précédemment que la suite $(\partial_p(x))_{p\in\mathcal{P}}$ est presque nulle.

Pour déduire de l'étude précédente la structure de $\widehat{W}(\mathbb{Q})$, on utilise l'isomorphisme $\widehat{W}(\mathbb{Q}) \simeq \mathbb{Z} \times I(\mathbb{Q})$ et le fait que $I(\mathbb{Q})$ soit d'indice 2 dans $W(\mathbb{Q})$. Pour déterminer la structure de $I(\mathbb{Q})$, nous allons étudier la restriction à $I(\mathbb{Q})$ de Φ. Dans un premier temps, on va montrer que Φ ainsi restreinte est à valeur dans $I(\mathbb{R}) \oplus \bigoplus_{p\in\mathcal{P}} W(\mathbb{F}_p)$, puis montrer que cet ensemble est précisément d'indice 2 dans $W(\mathbb{R}) \oplus \bigoplus_{p\in\mathcal{P}} W(\mathbb{F}_p)$, ce qui nous permettra de conclure. Pour ψ une forme quadratique rationnelle régulière, on rappelle que :

$$[\psi]_W \in I(\mathbb{Q}) \Leftrightarrow \overline{dim(\psi)} = 0 \text{ dans } \mathbb{Z}/2.$$

Or, pour q une forme quadratique régulière sur le $\mathbb{Q}$ espace vectoriel E de dimension n, on a vu qu'il existait une unique forme quadratique réelle prolongeant q et définie sur $E_{\mathbb{R}} = \mathbb{R} \otimes_{\mathbb{Q}} E$. Donc,

$$dim(q) = dim_{\mathbb{Q}}(E) = dim_{\mathbb{R}}(\mathbb{R} \otimes_{\mathbb{Q}} E) = dim(q_{\mathbb{R}})$$

et $\overline{dim(q)} = \overline{dim(q_{\mathbb{R}})}$. D'où, si $x \in I(\mathbb{Q})$ alors $x_{\mathbb{R}} \in I(\mathbb{R})$ et $I(\mathbb{Q})$ s'envoie naturellement sur $I(\mathbb{R}) \oplus \bigoplus_{p\in\mathcal{P}} W(\mathbb{F}_p)$ par Φ. On montre alors que :

$$\Phi(I(\mathbb{Q})) = I(\mathbb{R}) \oplus \bigoplus_{p\in\mathcal{P}} W(\mathbb{F}_p).$$

Comme $I(\mathbb{Q})$ est un sous-groupe d'indice 2 de $W(\mathbb{Q})$ et que Φ est un isomorphisme de groupe, $\Phi(I(\mathbb{Q}))$ est également un sous-groupe d'indice 2 de $\Phi(W(\mathbb{Q}))$. Or $W(\mathbb{R}) = I(\mathbb{R}) \sqcup (W(\mathbb{R}) \setminus I(\mathbb{R})$ ce qui donne :

$$W(\mathbb{R}) \oplus \bigoplus_{p\in\mathcal{P}} W(\mathbb{F}_p) = I(\mathbb{R}) \oplus \bigoplus_{p\in\mathcal{P}} W(\mathbb{F}_p) \sqcup (W(\mathbb{R}) \setminus I(\mathbb{R}) \oplus \bigoplus_{p\in\mathcal{P}} W(\mathbb{F}_p)$$

et $I(\mathbb{R})\oplus\bigoplus_{p\in\mathcal{P}} W(\mathbb{F}_p)$ est d'indice 2 dans $\Phi(W(\mathbb{Q}))$. Ainsi, $I(\mathbb{R})\oplus\bigoplus_{p\in\mathcal{P}} W(\mathbb{F}_p)$ et $\Phi(I(\mathbb{Q}))$ sont d'indices 2 dans $W(\mathbb{R}) \oplus \bigoplus_{p\in\mathcal{P}} W(\mathbb{F}_p)$ avec,

$$\Phi(I(\mathbb{Q})) \subset I(\mathbb{R}) \oplus \bigoplus_{p\in\mathcal{P}} W(\mathbb{F}_p)$$

ce qui donne $\Phi(I(\mathbb{Q})) = I(\mathbb{R}) \oplus \bigoplus_{p\in\mathcal{P}} W(\mathbb{F}_p)$. Comme l'injectivité de Φ est conservée par restriction à $I(\mathbb{Q})$ on a :

$$I(\mathbb{Q}) \simeq I(\mathbb{R}) \oplus \bigoplus_{p\in\mathcal{P}} W(\mathbb{F}_p)$$

et finalement :

$$\begin{aligned} \widehat{W}(\mathbb{Q}) &\simeq \mathbb{Z} \times I(\mathbb{Q}) \\ &\simeq \mathbb{Z} \times I(\mathbb{R}) \oplus \bigoplus_{p\in\mathcal{P}} W(\mathbb{F}_p) \\ &\simeq \mathbb{Z} \times 2\mathbb{Z} \times (\mathbb{Z}/2)^{(\mathbb{N})} \times (\mathbb{Z}/4)^{(\mathbb{N})} \end{aligned}$$

□

Chapitre 8

Application des tests de Witt-équivalence et d'équivalence sur $\mathbb{Q}$

Dans ce chapitre, nous allons appliquer sur des cas concrets, les tests de Witt-équivalence et d'équivalence sur $\mathbb{Q}$. Nous commencerons alors, par répondre rapidement à la question posée au chapitre 3, à savoir si l'entier 39 est oui ou non représenté par la forme quadratique diagonale $\langle 1, 5\rangle$. Ceci nous donnera notre première illustration des tests énoncés au chapitre précédent. Dans le reste de ce chapitre d'application, nous utiliserons également les méthodes d'étude de représentation des scalaires énoncées au chapitre 3 liant isotropie et domaine, notamment via l'utilisation abondante de l'astuce de la dimension 4. Ces méthodes nous seront en particulier utiles pour caractériser les rationnels représentés par des formes quadratiques rationnelles de dimension 2. Un des résultats majeurs de ce chapitre concernera la représentation des entiers, nous montrerons ainsi via la théorie des formes quadratiques que tout entier n est somme de quatre carrés de rationnels. Nous caractériserons également les entiers n qui s'écrivent comme somme de deux carrés de rationnels, ce qui nous permettra d'obtenir un résultat intéressant, via un rappel rapide sur l'étude des entiers de Gauss. Enfin, nous terminerons ce chapitre par l'étude du caractère universel d'une forme quadratique rationnelle en dimension 2, universalité que nous relierons à la notion d'isotropie.

8.1 Représentation des rationnels par des formes quadratiques rationnelles de dimension 2

Grâce aux tests de Witt-équivalence et d'équivalence sur $\mathbb{Q}$, on est désormais en capacité de répondre à la question posée au chapitre 3 :

$$\text{"}39 \textit{ est-il représenté par la forme quadratique rationnelle } q : (x, y) \longrightarrow x^2 + 5y^2 \text{ " ?}$$

Déterminer si 39 est représenté par q est donc équivalent à tester l'isotropie de $\langle 1, 5, -39\rangle$ ce qui est encore équivalent à tester le caractère hyperbolique de

$\langle 1, 5, -39, -5 \times 39\rangle$. On cherche donc à tester si $\langle 1, 5, -39, -5 \times 39\rangle$ est équivalente à la forme quadratique hyperbolique $\langle 1, -1, 1, -1\rangle$. Par le corollaire 7.2.2, $\langle 1, 5, -39, -5 \times 39\rangle \simeq \langle 1, -1, 1, -1\rangle$ si et seulement si $\langle 1, 5, -39, -5 \times 39\rangle$ est de signature $(2, 2)$ (ce qui est le cas) et si $\delta_p(< 1, 5, -39, -5 \times 39 >) = 0_{W(\mathbb{F}_p)}$ dans $W(\mathbb{F}_p)$ pour tout $p \in \mathcal{P}$. On note :

$$B_p =< \delta_p(1), \delta_p(5), \delta_p(-39), \delta_p(-5 \times 39) >= \delta_p(< 1, 5, -39, -5 \times 39 >)$$

et on cherche à vérifier si $\forall p \in \mathcal{P}, B_p = 0_{W(\mathbb{F}_p)}$. Or, $B_p = 0_{W(\mathbb{F}_p)}$ pour les $p \in \mathcal{P}$ ne divisant aucun des termes diagonaux de $\langle 1, 5, -39, -5 \times 39\rangle$, il suffit donc de tester si $B_p = 0_{W(\mathbb{F}_p)}$ pour $p \in \{3, 5, 13\}$. Pour $p = 13$ on a :

$$B_p =< \overline{0}, \overline{0}, \overline{-3}, \overline{-15} >=< \overline{-3}, \overline{-15} >$$

dans $W(\mathbb{F}_{13})$, avec :

$$\Delta(\langle \overline{-3}, \overline{-15}\rangle) = -\overline{45} = \overline{7} \text{ car } -45 \equiv 7\,[13].$$

Alors, 7 n'étant pas un carré modulo 13, la forme diagonale régulière $\langle \overline{-3}, \overline{-15}\rangle$ n'est pas de discriminant 1 et n'est pas hyperbolique sur $\mathbb{F}_3$ et $B_{13} \neq 0_{W(\mathbb{F}_{13})}$. Ainsi :

$$\langle 1, 5, -39, -5 \times 39\rangle \not\simeq_{\mathbb{Q}} \langle 1, -1, 1, -1\rangle$$

et 39 n'est pas représenté par q.

8.1.1 Problème de la représentation pour la forme quadratique ϕ

La proposition suivante donne une description des nombres rationnels qui sont représentés par la forme quadratique rationnelle :

$$\phi\colon \begin{cases} \mathbb{Q} \times \mathbb{Q} \longrightarrow \mathbb{Q} \\ (x, y) \longmapsto x^2 - 2y^2 \end{cases}$$

Proposition 8.1.1. *Soit $m \in \mathbb{Z}$ sans facteur carré et ϕ la forme quadratique diagonale $\langle 1, -2\rangle$. Alors, m est représenté par ϕ, c'est-à-dire s'écrit $x^2 - 2y^2$, $(x, y) \in \mathbb{Q} \times \mathbb{Q}$ si et seulement si les diviseurs premiers impairs de m sont crongrus à 1 ou -1 modulo 8.*

Démonstration. On note $\langle 1, -2\rangle$ la forme quadratique diagonale ϕ. Par le théorème de représentation et l'astuce de la dimension 4, $m \in \mathbb{Z}$ est représenté par $\langle 1, -2\rangle$ si et seulement si :

$$\begin{aligned} & \langle 1, -2, -m\rangle \text{ est isotrope} \\ \iff \quad & \langle 1, -2, -m, 2m\rangle \text{ est hyperbolique} \\ \iff \quad & \langle 1, -2, -m, 2m\rangle \simeq \langle 1, -1, 1, -1\rangle \text{ sur } \mathbb{Q} \end{aligned}$$

Ainsi, le problème de la représentation de l'entier sans facteur carré m revient à la recherche d'une condition nécessaire et suffisante sur le caractère hyperbolique de la forme quadratique rationnelle diagonale $\langle 1, -2, -m, 2m\rangle$. D'après le test d'équivalence rationnelle, il faut chercher une condition nécessaire et suffisante sur m pour que $\langle 1, -2, -m, 2m\rangle$ et $\langle 1, -1, 1, -1\rangle$ aient même signature et que :

$$\forall p \in \mathcal{P},\ \partial_p(< 1, -2, -m, 2m >) = \partial_p(< 1, -1, 1, -1 >) = 0_{W(\mathbb{F}_p)}.$$

Or, que m soit positif ou négatif, $\langle 1, -2, -m, 2m\rangle$ est de signature $(2, 2)$ et donc les formes $\langle 1, -2, -m, 2m\rangle$, $\langle 1, -1, 1, -1\rangle$ ont bien même signature. On remarque également qu'il suffit de vérifier l'égalité requise

$$\partial_p(< 1, -2, -m, 2m >) = 0_{W(\mathbb{F}_p)}$$

pour les nombres premiers p divisant m, puisque pour les autres p, on a déjà :

$$\partial_p(< 1, -2, -m, 2m >) = 0_{W(\mathbb{F}_p)}$$

Supposons $m = \prod_{i=1}^{l} p_i > 0$ où les p_i sont des nombres premiers deux à deux distincts, car m est sans facteur carré. Dans un premier temps on suppose que 2 divise m et que $p_1 = 2$, les p_i sont donc impairs pour $i \in [\![2, l]\!]$. Alors, comme 4 est un carré de $\mathbb{Q}^*$ on a :

$$\langle 1, -2, -m, 2m\rangle \simeq \langle 1, -2, -2\prod_{i=2}^{l} p_i, \prod_{i=2}^{l} p_i\rangle.$$

où $p_i \nmid 2\prod_{j=2, j\neq i}^{l} p_j$ qui montre que $-\overline{2}\prod_{j=2, j\neq i}^{l} \overline{p_j} \neq \overline{0}$. Ainsi, dans $W(\mathbb{F}_2)$ on a :

$$\partial_2(< 1, -2, -m, 2m >) =< \overline{0}, \overline{-1}, -\prod_{i=2}^{l} \overline{p_i}, \overline{0} >=< \overline{-1}, -\prod_{i=2}^{l} \overline{p_i} >.$$

Comme de plus $\prod_{i=2}^{l} p_i \equiv 1\,[2]$, il vient :

$$\begin{aligned} < \overline{-1}, -\prod_{i=2}^{l} \overline{p_i} >= & \quad < \overline{1}, \overline{1} > \\ = & \quad < \overline{1} > + < \overline{1} > \\ = & \quad 2. < \overline{1} > \\ = & \quad 0_{W(\mathbb{F}_2)}, \text{ car } W(\mathbb{F}_2) \text{ est d'ordre 2} \end{aligned}$$

Ainsi, il suffit de nous intéresser aux diviseurs premiers impairs de m, puisque pour $p = 2$ on a l'égalité requise $\partial_2(< 1, -2, -m, 2m >) = 0_{W(\mathbb{F}_2)}$. Pour p_i impair divisant m et toujours $p_1 = 2$, on a :

$$\begin{aligned} \partial_{p_i}(< 1, -2, -m, -2m >) = & \quad < \overline{0}, \overline{0}, -\overline{2}\prod_{j=2, j\neq i}^{l} \overline{p_j}, \prod_{j=2, j\neq i}^{l} \overline{p_j} > \\ = & \quad < -\overline{2}\prod_{j=2, j\neq i}^{l} \overline{p_j}, \prod_{j=2, j\neq i}^{l} \overline{p_j} > \end{aligned}$$

Ainsi, $\partial_{p_i}(< 1, -2, -m, -2m >) = 0_{W(\mathbb{F}_{p_i})}$ si et seulement si :

$$\begin{aligned} & < -\overline{2}\prod_{j=2, j\neq i}^{l} \overline{p_j}, \prod_{j=2, j\neq i}^{l} \overline{p_j} >= 0_{W(\mathbb{F}_{p_i})} \\ \iff & \langle -\overline{2}\prod_{j=2, j\neq i}^{l} \overline{p_j}, \prod_{j=2, j\neq i}^{l} \overline{p_j}\rangle \text{ est hyperbolique sur } \mathbb{F}_{p_i} \\ \iff & \det(\langle -\overline{2}\prod_{j=2, j\neq i}^{l} \overline{p_j}, \prod_{j=2, j\neq i}^{l} \overline{p_j}\rangle) = -1 \,\text{dans}\, \mathbb{F}_{p_i}^*/(\mathbb{F}_{p_i}^*)^2 \\ \iff & -2(\prod_{j=2, j\neq i}^{l} p_i)^2 = -1 \,\text{dans}\, \mathbb{F}_{p_i}^*/(\mathbb{F}_{p_i}^*)^2 \\ \iff & 2 = 1 \,\text{dans}\, \mathbb{F}_{p_i}^*/(\mathbb{F}_{p_i}^*)^2 \\ \iff & 2 \text{ est un carré de } \mathbb{F}_{p_i}^* \end{aligned}$$

Or, 2 est un carré de $\mathbb{F}_{p_i}^*$ si et seulement si :

$$\begin{aligned} &\iff && \left(\frac{2}{p_i}\right) = 1 \\ &\iff && (-1)^{\frac{p_i^2-1}{8}} = 1 \\ &\iff && p_i \equiv 1\,[8] \text{ ou } p_i \equiv 7\,[8] \end{aligned}$$

Donc si m est sans facteur carré et que 2 divise m, on voit que m est représenté par $\langle 1, -2\rangle$ si et seulement si pour tout diviseur premier impair p de m, p est congru à 1 ou -1 modulo 8.

Si 2 ne divise pas m, m s'écrit $\prod_{i=1}^{l} p_i$ où les p_i sont des nombres premiers impairs deux à deux distincts et on est alors amené à étudier l'équivalence sur $\mathbb{Q}$ de $\langle 1, -2, -\prod_{i=1}^{l} p_i, 2\prod_{i=1}^{l} p_i\rangle$ et $\langle 1, -1, 1, -1\rangle$. Les calculs sont tout à fait similaires à ceux effectués ci-dessus, on aboutit encore au fait que $\langle 1, -2, -\prod_{i=1}^{l} p_i, 2\prod_{i=1}^{l} p_i\rangle \simeq \langle 1, -1, 1, -1\rangle$ si et seulement si l'on a :

$$p_i \equiv 1\,[8] \text{ ou } p_i \equiv -1\,[8], \forall i \in [\![1, l]\!].$$

Enfin, si on suppose $m = -\prod_{i=1}^{n} p_i < 0$, les démarches ci-dessus se reproduisent à l'identique et on trouve encore la même condition nécessaire et suffisante, ce qui achève de montrer l'équivalence de la proposition. □

Exemple 8.1.1. *Puisque* 31 *est premier impair (donc sans facteur carré) et que* $31 \equiv -1\,[8]$*, 31 est représenté par* $\langle 1, -2\rangle$ *et l'on a par exemple* $31 = 7^2 - 2 \times 3^2$*. De même l'entier négatif* -238 *est représenté par* $\langle 1, -2\rangle$*, puisque :*

$-238 = -2 \times 7 \times 17$ *avec* $7 \equiv -1\,[8]$ *et* $17 \equiv -1\,[8]$*. On a* $-238 = 2^2 - 2 \times 11^2$*.*

En revanche $65 = 13 \times 5$ *est sans facteur carré mais ni* 5*, ni* 13 *n'est congru à* 1 *ou* -1 *modulo* 8 *et donc* 65 *ne peut s'écrire sous la forme* $x^2 - 2y^2$*,* $x, y \in \mathbb{Q}$*.*

8.1.2 Problème de la représentation pour la forme quadratique ψ

La proposition suivante donne une description des nombres rationnels positifs qui sont représentés par la forme quadratique rationnelle :

$$\psi\colon \begin{cases} \mathbb{Q} \times \mathbb{Q} \longrightarrow \mathbb{Q} \\ (x, y) \longmapsto x^2 + 3y^2 \end{cases}$$

Proposition 8.1.2. *Soit* $r \in \mathbb{Q}_+^*$*,* $r = \dfrac{\prod_{i=1}^{l} p_i^{\alpha_i}}{\prod_{j=1}^{m} q_j^{\beta_j}}$*, écriture unique sous forme d'une fraction irreductible avec,* $(p_i)_{1\le i\le l}$*,* $(q_j)_{1\le j\le m}$ *des familles de nombres premiers deux à deux distincts et* $\alpha_i \in \mathbb{N}^*$*,* $\forall i \in [\![1, l]\!]$ *et* $\beta_j \in \mathbb{N}^*$*,* $\forall j \in [\![1, m]\!]$*. Alors r est représenté par la forme quadratique rationnelle diagonale* $\langle 1, 3\rangle$ *c'est à dire s'écrit sous la forme* $x^2 + 3y^2$*,* $(x, y) \in \mathbb{Q} \times \mathbb{Q}$ *si et seulement si :*

- $\forall i \in [\![1, l]\!]$ *tels que* $\alpha_i \equiv 1\,[2]$ *et* $p_i \neq 3$ *on a :* $p_i \equiv 1\,[3]$*.*
- $\forall j \in [\![1, m]\!]$ *tels que* $\beta_j \equiv 1\,[2]$ *et* $q_j \neq 3$ *on a :* $q_j \equiv 1\,[3]$*.*

La démonstration suivante étant difficile, nous ferons figurer au coeur de cette démonstration 3 lemmes intermédiaires qui en faciliteront sa compréhension.

Démonstration. Notre but est de chercher une condition nécessaire et suffisante sur $r \in \mathbb{Q}$ pour que r s'écrive x^2+3y^2, $(x,y) \in \mathbb{Q}\times\mathbb{Q}$. Dans un premier temps, on va s'intéresser aux nombres premiers impairs représentés par ψ. Il est clair que 3 est représenté par ψ, $(3 = \psi(0,1))$, on cherche alors une condition nécessaire et suffisante pour les nombres premiers impairs différents de 3. Alors, $p \in \mathcal{P}\backslash\{2,3\}$ est représenté par ψ si et seulement si :

$$\begin{aligned} & \langle 1,3,-p\rangle \text{ est isotrope} \\ \iff \quad & \langle 1,3,-p,-3p\rangle \text{ est hyperbolique sur } \mathbb{Q} \end{aligned}$$

La première équivalence découle du principe de représentation tandis que la seconde découle de l'astuce de la dimension 4. Or, d'après le test d'équivalence rationnelle, $\langle 1,3,-p,-3p\rangle$ est hyperbolique si de signature $(2,2)$ (ce qui est le cas) et si :

$$\forall p_1 \in \mathcal{P}, \partial_{p_1}(< 1,3,-p,-3p >) = 0_{W(\mathbb{F}_{p_1})}.$$

Comme pour $p_1 \in \mathcal{P}$ ne divisant aucun des termes diagonaux de $\langle 1,3,-p,-3p\rangle$, on a :

$$\partial_{p_1}(< 1,3,-p,-3p >) = 0_{W(\mathbb{F}_{p_1})}$$

il suffit de trouver une condition nécessaire et suffisante pour que l'on ait

$$\partial_{p_1}(< 1,3,-p,-3p >) = 0_{W(\mathbb{F}_{p_1})} \text{ pour } p_1 \in \{3,p\}.$$

On remarque aussi que 2 n'est pas représenté par ψ. Pour $p = 2$ et $p_1 = 3$ on a :

$$\partial_3(< 1,3,-2,-6 >) =< \overline{0},\overline{1},\overline{0},-\overline{2} >=< \overline{1},-\overline{2} >$$

Or $\langle\overline{1},-\overline{2}\rangle$ n'est alors pas hyperbolique sur $\mathbb{F}_3$ puisque de déterminant $-2 \neq -1$ dans $\mathbb{F}_3^*/(\mathbb{F}_3^*)^2$ (2 n'étant pas un carré de $\mathbb{F}_3^*$). D'où,

$$\partial_3(< 1,3,-2,-6 >) \neq 0_{W(\mathbb{F}_3)}$$

et 2 n'est pas représenté par ψ.

Lemme 8.1.1. *$p \in \mathcal{P}\backslash\{2,3\}$ est représenté par ψ si et seulement si $p \equiv 1\,[3]$.*

Démonstration.

- Pour $p_1 = 3$, on a :

$$\begin{aligned} \partial_3(< 1,3,-p,-3p >) = & < \partial_3(1),\partial_3(3),\partial_3(-p),\partial_3(-3p) > \\ = & < \overline{0},\overline{1},\overline{0},-\overline{p} > \\ = & < \overline{1},-\overline{p} > \end{aligned}$$

  Ainsi, $< \overline{1},-\overline{p} >= 0_{W(\mathbb{F}_3)}$ si et seulement si la forme diagonale régulière $\langle\overline{1},-\overline{p}\rangle$ est hyperbolique sur $\mathbb{F}_3$. Ceci est encore équivalent à ce que son déterminant soit égal à -1 dans $\mathbb{F}_3^*/(\mathbb{F}_3^*)^2$, c'est-à-dire si et seulement si $p = 1$ dans $\mathbb{F}_3^*/(\mathbb{F}_3^*)^2$.

- Pour $p_1 = p$, on a :

$$\begin{aligned}\partial_p(< 1, 3, -p, -3p >) = & < \partial_p(1), \partial_p(3), \partial_p(-p), \partial_p(-3p) > \\ = & < \overline{0}, \overline{0}, \overline{-1}, \overline{-3} > \\ = & < \overline{-1}, \overline{-3} >\end{aligned}$$

  Ainsi, $< \overline{-1}, \overline{-3} >= 0_{W(\mathbb{F}_p)}$ si et seulement si la forme diagonale régulière $\langle \overline{-1}, \overline{-3} \rangle$ est hyperbolique sur $\mathbb{F}_p$. Ceci est encore équivalent à ce que son déterminant soit égal à -1 dans $\mathbb{F}_p^*/(\mathbb{F}_p^*)^2$, c'est-à-dire si et seulement si $-3 = 1$ dans $\mathbb{F}_3^*/(\mathbb{F}_3^*)^2$.

Ainsi, le nombre premier impair p différent de 3 est représenté par ψ :

$$\begin{aligned}\iff & \quad p = 1 \text{ dans } \mathbb{F}_3^*/(\mathbb{F}_3^*)^2 \text{ et } -3 = 1 \text{ dans } \mathbb{F}_p^*/(\mathbb{F}_p^*)^2 \\ \iff & \quad \left(\frac{p}{3}\right) = 1 \text{ et } \left(\frac{-3}{p}\right) = 1\end{aligned}$$

Or par multiplicativité du symbole de Legendre et la loi de réciprocité quadratique, on a :

$$\begin{aligned}\left(\frac{-3}{p}\right) = 1 \iff & \quad \left(\frac{-1}{p}\right) \times \left(\frac{3}{p}\right) = 1 \\ \iff & \quad (-1)^{\frac{p-1}{2}} \left(\frac{p}{3}\right) (-1)^{\frac{(p-1)}{2}\frac{(3-1)}{2}} = 1 \\ \iff & \quad (-1)^{\frac{p-1}{2}} (-1)^{\frac{p-1}{2}} \left(\frac{p}{3}\right) = 1 \\ \iff & \quad \left(\frac{p}{3}\right) = 1\end{aligned}$$

D'où au final $p \in \mathcal{P}\backslash\{2, 3\}$ est représenté par ψ si et seulement si p est un carré modulo 3, soit $p \equiv 1\,[3]$.

□

Reprenons la démonstration de la proposition. En multipliant r par le carré d'un entier approprié comme exposé dans le chapitre précédent, on a :

$$\langle 1, 3, -r, -3r \rangle \simeq \langle 1, 3, -n, -3n \rangle \text{ où } n \text{ est un entier sans facteur carré.}$$

On remarque alors qu'étudier l'équivalence de $\langle 1, 3, -n, -3n \rangle$ avec $\langle 1, -1, 1, -1 \rangle$ ne dépend pas du fait que 3 divise ou non n. En effet, si 3 divise n, alors on peut écrire $n = \prod_{i=1}^{k} p_i$, avec $p_1 = 3$, $p_i \in \mathcal{P}\backslash\{3\}$ pour $i \in [\![2, k]\!]$, les p_i étant deux à deux distincts et :

$$\langle 1, 3, -n, -3n \rangle = \langle 1, 3, -3p_2 \cdots p_k, -9p_2 \cdots p_k \rangle$$

soit alors $\langle 1, 3, -n, -3n \rangle \simeq \langle 1, 3, -3p_2 \cdots p_k, -p_2 \cdots p_k \rangle$ (9 étant un carré de $\mathbb{Q}^*$). Si 3 ne divise pas n, on peut écrire $n = \prod_{i=1}^{k} p_i$, avec, $p_i \in \mathcal{P}\backslash\{3\}$ pour $i \in [\![1, k]\!]$, les p_i étant deux à deux distincts et :

$$\langle 1, 3, -n, -3n \rangle = \langle 1, 3, -p_1 \cdots p_k, -3p_1 \cdots p_k \rangle \simeq \langle 1, 3, -3p_1 \cdots p_k, -p_1 \cdots p_k \rangle$$

qui est exactement du même type que précédemment. Dans la suite on étudiera toujours le cas où n est non divisible par 3.

Lemme 8.1.2. *Soit $n \in \mathbb{N}^*$ sans facteur carré. Alors, si n est divisible par 2, n n'est pas réprésenté par ψ.*

Démonstration. Supposons $n = \prod_{i=1}^{k} p_i$ avec $p_1 = 2$ et $p_i \in \mathcal{P}\backslash\{2,3\}$, pour $i \in [\![2,k]\!]$. Supposons par l'absurde que n est représenté par ψ. D'après tout ce qui précède on a : $\langle 1, 3, -p_1 \cdots p_k, -3p_1 \cdots p_k \rangle$ est hyperbolique et donc nécessairement, pour tout $i \in [\![2,k]\!]$:

$$\begin{aligned} \partial_{p_i}(< 1, 3, -p_1 \cdots p_k, -3p_1 \cdots p_k >) = & < \overline{0}, \overline{0}, -\overline{\prod_{j\neq i}^{k} p_j}, -3\overline{\prod_{j\neq i}^{k} p_j} > \\ = & < -\overline{\prod_{j\neq i}^{k} p_j}, -3\overline{\prod_{j\neq i}^{k} p_j} > \\ = & \quad 0_{W(\mathbb{F}_{p_i})} \end{aligned}$$

Or, $< -\overline{\prod_{j\neq i}^{k} p_j}, -3\overline{\prod_{j\neq i}^{k} p_j} >= 0_{W(\mathbb{F}_{p_i})}$ si et seulement si la forme quadratique régulière (car $p_i \nmid \prod_{j\neq i}^{k} p_j$) $\langle -\overline{\prod_{j\neq i}^{k} p_j}, -3\overline{\prod_{j\neq i}^{k} p_j} \rangle$ est hyperbolique sur $\mathbb{F}_{p_i}$. Ce qui est encore équivalent à :

$$\begin{aligned} & det(\langle -\overline{\prod_{j\neq i}^{k} p_j}, -3\overline{\prod_{j\neq i}^{k} p_j} \rangle) = -1 \text{ dans } \mathbb{F}_{p_i}^*/(\mathbb{F}_{p_i}^*)^2 \\ \iff & -3 \text{ est un carré de } \mathbb{F}_{p_i}^* \\ \iff & p_i \equiv 1\,[3] \\ \iff & p_i \text{ est représenté par } \psi \end{aligned}$$

où la dernière équivalence est une application directe du lemme 8.1.1 puisque $p_i \in \mathcal{P}\backslash\{2,3\}$. D'où, si n est représenté par ψ, tous les p_i ($i \in [\![2,k]\!]$) le sont aussi. De plus, pour $p = 3$:

$$\begin{aligned} \partial_3(< 1, 3, -p_1 \cdots p_k, -3p_1 \cdots p_k >) = & < \overline{0}, \overline{1}, \overline{0}, -\overline{\prod_{j=1}^{k} p_j} > \\ = & < \overline{1}, -\overline{\prod_{j=1}^{k} p_j} > \\ = & \quad 0_{W(\mathbb{F}_3)} \end{aligned}$$

et la forme régulière $\langle \overline{1}, -2\overline{\prod_{j=2}^{k} p_j} \rangle$ est hyperbolique sur $\mathbb{F}_3$. On en déduit donc que :

$$det(\langle \overline{1}, -2\overline{\prod_{j=2}^{k} p_j} \rangle) = -1 \text{ dans } \mathbb{F}_3^*/(\mathbb{F}_3^*)^2$$

d'où $2\prod_{j=2}^{k} p_j$ est un carré de $\mathbb{F}_3^*$. Comme pour tout $i \in [\![2,k]\!]$, p_i est représenté par ψ et est donc un carré de $\mathbb{F}_3^*$, on a :

$$\begin{aligned} \left(\frac{2\prod_{j=2}^{k} p_j}{3}\right) = 1 \iff & \left(\frac{2}{3}\right)\prod_{j=2}^{k}\left(\frac{p_j}{3}\right) = 1 \\ \iff & \left(\frac{2}{3}\right) = 1 \end{aligned}$$

Ainsi, si on suppose n représenté par ψ, nécessairement $\left(\frac{2}{3}\right) = 1$, ce qui est absurde. D'où, n n'est pas représenté par ψ, ce qui achève de montrer le lemme. □

Lemme 8.1.3. *Soit $n \in \mathbb{N}^*$ sans facteur carré, non divisible par 3. Alors, n est représenté par ψ si et seulement si tout diviseur premier de n est représenté par ψ.*

Démonstration. Supposons que n est sans facteur carré, que 3 ne divise pas et que n et est représenté par ψ. Alors, d'après le lemme précédent, 2 ne divise pas n. D'après nos hypothèses n s'écrit $n = \prod_{i=1}^{k} p_i$ avec $p_i \in \mathcal{P}\backslash\{2,3\}$ pour $i \in [\![1,k]\!]$. En appliquant le raisonnement du début de la démonstration du lemme 8.1.2, on voit que $\forall i \in [\![1,k]\!]$, on a dans $W(\mathbb{F}_{p_i})$:

$$\begin{aligned}\partial_{p_i}(< 1,3,-p_1\cdots p_k,-3p_1\cdots p_k >) = &< \overline{0},\overline{0},-\overline{\prod_{j\neq i}^{k} p_j},-\overline{3\prod_{j\neq i}^{k} p_j} >\\ = &< -\overline{\prod_{j\neq i}^{k} p_j},-\overline{3\prod_{j\neq i}^{k} p_j} >\\ = &\quad 0_{W(\mathbb{F}_{p_i})}\end{aligned}$$

et la forme diagonale régulière (car $p_i \nmid \prod_{j\neq i}^{k} p_j$) $\langle -\overline{\prod_{j\neq i}^{k} p_j},-\overline{3\prod_{j\neq i}^{k} p_j}\rangle$ est hyperbolique sur $\mathbb{F}_{p_i}$. Ceci implique alors que -3 est un carré de $\mathbb{F}_{p_i}^*$, ce qui est équivalent à $p_i \equiv 1\,[3]$ et qui montre d'après le lemme 8.1.1, que les p_i sont représentés par ψ.

Inversement, supposons que tous les diviseurs premiers de n sont représentés pas ψ. Pour p_i divisant n, on a :

$$\begin{aligned}p_i \text{ est représenté par } \psi \iff &\quad \left(\frac{p_i}{3}\right) = 1\\ \iff &\quad \left(\frac{-3}{p_i}\right) = 1\end{aligned}$$

Comme 3 ne divise pas n et que 2 n'est pas représenté par ψ, n s'écrit $\prod_{i=1}^{k} p_i$ où les p_i sont dans $\mathcal{P}\backslash\{2,3\}$. Montrer que n est représenté par ψ revient alors à montrer que $\langle 1,3,-n,-3n\rangle$ est hyperbolique sur $\mathbb{Q}$. Or, $\langle 1,3,-n,-3n\rangle$ étant de signature $(2,2)$, il faut juste vérifier que $\partial_{p_i}(< 1,3,-n,-3n >) = 0_{W(\mathbb{F}_{p_i})}$, $(i \in [\![1,k]\!])$ et que $\partial_3(< 1,3,-n,-3n >) = 0_{W(\mathbb{F}_3)}$. Or,

$$\begin{aligned}\partial_3(< 1,3,-n,-3n >) = &< \overline{0},\overline{1},\overline{0},-\overline{p_1\cdots p_k} >\\ = &< \overline{1},-\overline{p_1\cdots p_k} >\\ = &\quad 0_{W(\mathbb{F}_3)}\end{aligned}$$

car $\langle \overline{1},-\overline{p_1\cdots p_k}\rangle$ est hyperbolique, puisque de déterminant -1 dans $\mathbb{F}_3^*/(\mathbb{F}_3^*)^2$ ($\overline{p_1\cdots p_k}$ est un carré dans $\mathbb{F}_3^*$, car chacun des $\overline{p_i}$ en est un). Enfin,

$$\begin{aligned}\partial_{p_i}(< 1,3,-n,-3n >) = &< \overline{0},\overline{0},-\overline{\prod_{j\neq i}^{k} p_j},-\overline{3\prod_{j\neq i}^{k} p_j} >\\ = &< -\overline{\prod_{j\neq i}^{k} p_j},-\overline{3\prod_{j\neq i}^{k} p_j} >\\ = &\quad 0_{W(\mathbb{F}_{p_i})}\end{aligned}$$

car $\langle -\overline{\prod_{j\neq i}^{k} p_j},-\overline{3\prod_{j\neq i}^{k} p_j}\rangle$ est hyperbolique, puisque de déterminant -1. En effet, comme p_i est représenté par ψ on a alors $-3 = 1$ dans $\mathbb{F}_{p_i}^*/(\mathbb{F}_{p_i}^*)^2$ et donc $det(\langle -\overline{\prod_{j\neq i}^{k} p_j},-\overline{3\prod_{j\neq i}^{k} p_j}\rangle) = 3 = -1$. D'où l'équivalence annoncée. □

On a donc vu que $r \in \mathbb{Q}_+^*$ s'écrivant $r = \dfrac{\prod_{i=1}^{l} p_i^{\alpha_i}}{\prod_{j=1}^{m} q_j^{\beta_j}}$ est représenté par ψ si et seulement si $n = \prod_{j=1}^{m} q_j^{\overline{\beta_j}} \prod_{i=1}^{l} p_i^{\overline{\alpha_i}}$ qui est un entier sans facteur carré égal à r modulo les carrés de $\mathbb{Q}^*$ est représenté par ψ, où l'on note toujours $\overline{\beta_j} \in \{0,1\}$ le reste de la division par 2 de β_j et $\overline{\alpha_i} \in \{0,1\}$ le reste de la division par 2 de α_i (car $\langle 1,3,-r,-3r\rangle \simeq \langle 1,3,-n,-3n\rangle$). Comme le fait que n soit ou non représenté par ψ ne dépend pas du fait que 3 divise ou non n, par construction de n et le résultat du lemme 14 on a :

r est représenté par ψ si et seulement si les diviseurs premiers différents de 3 de la décompostion de n sont tous représentés pas ψ

ce qui se traduit par :

- $\forall i \in [\![1,l]\!]$ tel que $\alpha_i \equiv 1\,[2]$ et $p_i \neq 3$ on a : $p_i \equiv 1\,[3]$.
- $\forall j \in [\![1,m]\!]$ tel que $\beta_j \equiv 1\,[2]$ et $q_j \neq 3$ on a : $q_j \equiv 1\,[3]$.

□

Exemple 8.1.2.

1. $\dfrac{3}{20} = \dfrac{3}{2^2 \times 5}$ *n'est pas représenté par* ψ *car* $5 \not\equiv 1\,[3]$.
2. $\dfrac{84}{775} = \dfrac{2^2 \times 3 \times 7}{5^2 \times 31}$ *est représenté par* ψ *car* $7 \equiv 1\,[3]$ *et* $31 \equiv 1\,[3]$.
3. $\dfrac{225}{256} = \dfrac{3^2 \times 5^2}{2^8} = \left(\dfrac{3 \times 5}{2^4}\right)^2$ *est un carré de* $\mathbb{Q}^*$ *et est représenté pas* ψ *car* 1 *représentant de la classe des carrés est représenté par* ψ *puisque* $\left(\dfrac{1}{2}\right)^2 + 3\left(\dfrac{1}{2}\right)^2 = 1$.

8.2 Problème de l'universalité des formes quadratiques rationnelles en dimension 2

Nous savons déjà que sur un corps $\mathbb{K}$ de caractéristique différente de 2, toute forme quadratique régulière isotrope est universelle. On va montrer que sur le corps $\mathbb{Q}$ et en dimension 2, la réciproque est vraie :

Théorème 8.2.1. *En dimension 2 toute forme quadratique rationnelle* universelle *est* isotrope *et donc une forme quadratique rationnelle régulière de dimension 2 est* universelle *si et seulement si elle est* isotrope.

Démonstration. Soit ϕ une forme quadratique rationnelle de dimension 2, que l'on suppose universelle. Alors, par diagonalisation, il existe deux rationnels a et b tels que $\phi \simeq \langle a,b\rangle$. Quitte à multiplier a et b par les carrés de deux entiers appropriés, on peut supposer que a et b sont des entiers sans facteur carré. On va commencer par montrer que a et b sont nécessairement tous deux non nuls. Supposons par l'absurde que $a = 0$ et $b \neq 0$ (le raisonnement est identique avec $b = 0$ et $a \neq 0$). Puisque ϕ est universelle, la forme diagonale $\langle a,b\rangle$ l'est également et donc $q : (x,y) \longrightarrow by^2$ représente tous les éléments de $\mathbb{Q}^*$. Soit $p \in \mathcal{P}$ intervenant dans la décomposition en facteurs premiers de b, bp est donc atteint par q et il existe $y \in \mathbb{Q}^*$ tel que $by^2 = bp \Longleftrightarrow y^2 = p$ ($b \neq 0$) et $\sqrt{p}$ serait

donc rationnel, absurde. D'où $\phi \simeq \langle a, b\rangle$ avec $a \neq 0, b \neq 0$, des éléments de $\mathbb{Z}$ sans facteur carré. On montre alors que pour a, b précédemment définis on a :

$$v_p(a) \equiv v_p(b)\,[2],\ \forall p \in \mathcal{P}$$

Comme a et b sont des entiers sans facteur carré ceci équivaut au fait que pour tout nombre premier p, on ait :

$$p \mid a \Longleftrightarrow p \mid b.$$

Supposons alors par l'absurde que $p \mid b$ et $p \nmid a$. Sur le corps fini $\mathbb{F}_p$ deux formes quadratiques régulières sont équivalentes si et seulement si elles ont même dimension et même déterminant dans $\mathbb{F}_p^*/(\mathbb{F}_p^*)^2$. Puisque $p \mid b$ on a alors $\dfrac{b}{p} \in \mathbb{Z}$ et $\overline{\dfrac{b}{p}} \in \mathbb{F}_p^*$ est soit :

- un carré de $\mathbb{F}_p^*$ et alors $\overline{\dfrac{b}{p}} = 1$ dans $\mathbb{F}_p^*/(\mathbb{F}_p^*)^2$. Ainsi, $\langle \overline{\dfrac{b}{p}}, -\varepsilon\rangle \simeq \langle 1, -\varepsilon\rangle$ et donc $\langle \overline{\dfrac{b}{p}}, -\varepsilon\rangle$ est anisotrope, car à équivalence près $\langle 1, -\varepsilon\rangle$ est la seule forme anisotrope de dimension 2 sur $\mathbb{F}_p$
- un non carré de $\mathbb{F}_p^*$ et alors $\overline{\dfrac{b}{p}} = \varepsilon$ dans $\mathbb{F}_p^*/(\mathbb{F}_p^*)^2$ pour ε un représentant de la classe des non carrés. Ainsi, $\overline{\dfrac{b}{p}}$ n'est pas un carré et $\langle \overline{\dfrac{b}{p}}, -1\rangle \simeq \langle -1, \varepsilon\rangle$. Or $\langle -1, \varepsilon\rangle \simeq \langle 1, -\varepsilon\rangle$ car sont toutes deux de même dimension et de même déterminant. D'où $\langle \overline{\dfrac{b}{p}}, -1\rangle$ est anisotrope.

Dans les deux cas, il existe $x \in \mathbb{Z}$ non divisible par p c'est-à-dire $\overline{x} \in \mathbb{F}_p^*$ tel que $\langle \overline{\dfrac{b}{p}}, -\overline{x}\rangle$ soit anisotrope.
Soit donc un tel x. Puisque px est représenté par $\langle a, b\rangle$ on a :

$$\begin{aligned} px \text{ représenté par } \langle a, b\rangle &\Longleftrightarrow \quad \langle a, b, -px\rangle \text{ isotrope} \\ &\Longleftrightarrow \quad \langle a, b, -px, -apbx\rangle \text{ isotrope} \\ &\Longleftrightarrow \quad \langle a, b, -px, -apbx\rangle \text{ hyperbolique} \\ &\Longleftrightarrow \quad \langle a, b, -px, \frac{-abx}{p}\rangle \text{ hyperbolique} \end{aligned}$$

Les équivalences 1 et 2 découlent de l'astuce de la dimension 4 et l'équivalence 3 provient du fait que $-apbx$ et $\dfrac{-abx}{p}$ sont égaux à multiplication près par un carré de $\mathbb{Q}^*$ puisque $-apbx = p^2\dfrac{-abx}{p}$. Puisque $p \nmid a$, $p \nmid x$, $p \nmid \dfrac{b}{p}$, le test d'équivalence sur $\mathbb{Q}$ donne alors l'égalité :

$$\begin{aligned} < \partial_p(a), \partial_p(b), \partial_p(-px), \partial_p(\frac{-abx}{p}) > &= \quad < 0, \overline{\frac{b}{p}}, -\overline{x}, 0 > \\ &= \quad < \overline{\frac{b}{p}}, -\overline{x} > \\ &= \quad 0_{W(\mathbb{F}_p)} \end{aligned}$$

Ce qui implique que $\langle \overline{\frac{b}{p}}, -\overline{x} \rangle$ est hyperbolique. Or, on a vu que $\langle \overline{\frac{b}{p}}, -\overline{x} \rangle$ était anisotrope, absurde.

Ainsi $v_p(a) \equiv v_p(b)\,[2]$ et a et b sont égaux au signe près. On a donc $\phi \simeq \langle a, a \rangle$ ou $\phi \simeq \langle a, -a \rangle$, pour $a \in \mathbb{Z}^*$ sans facteur multiple. Or, la forme quadratique rationnelle diagonale $\langle 1, 1 \rangle$ est non universelle puisque les éléments strictement négatifs ne sont pas représentés par $\langle 1, 1 \rangle$. Donc, pour m non représenté par $\langle 1, 1 \rangle$, am n'est pas représenté par $\langle a, a \rangle$ et $\langle a, a \rangle$ n'est pas universelle. Ainsi, nécessairement $\phi \simeq \langle a, -a \rangle$ qui est régulière et hyperbolique et donc isotrope. D'où ϕ forme quadratique rationnelle universelle de dimension 2 est nécessairement régulière et isotrope et d'où l'équivalence du théorème puisque toute forme quadratique rationnelle régulière et isotrope est universelle. □

Corollaire 8.2.1. *Une forme quadratique rationnelle de dimension 2 qui représente tous les éléments de $\mathbb{Q}_+^*$ ou $\mathbb{Q}_-^*$ est régulière, isotrope et donc en fait universelle.*

Démonstration. Soit ϕ une forme quadratique rationnelle de dimension 2 telle que ϕ représente tous les éléments de $\mathbb{Q}_+^*$. Comme dans la démonstration du théorème précédent, il existe deux entiers sans facteur carré non nuls a et b tels que $\phi \simeq \langle a, b \rangle$ et on montre de la même façon que dans la preuve du théorème que $\forall p \in \mathcal{P}, v_p(a) \equiv v_p(b)\,[2]$ ce qui équivaut au fait que $b = \pm a$ puisque a et b sont sans facteur carré. D'où $\phi \simeq \langle a, a \rangle$ ou $\phi \simeq \langle a, -a \rangle$ et ϕ représentant tous les éléments de $\mathbb{Q}_+^*$, nécessairement $a \in \mathbb{N}^*$. Puisque $\langle 1, 1 \rangle$ ne représente pas tous les entiers (on verra au corollaire 12 que $n \in \mathbb{N}^*$ s'écrit comme somme de deux carrés de rationnels si $v_p(n) \equiv 0\,[2]$ pour tout p premier congru à 3 modulo 4), pour n non représenté par $\langle 1, 1 \rangle$, an n'est pas représenté par $\langle a, a \rangle$. Ainsi, $\phi \not\simeq \langle a, a \rangle$, et $\phi \simeq \langle a, -a \rangle$ est hyperbolique donc isotrope. D'où ϕ est régulière, isotrope et donc universelle.

Si ϕ est une forme quadratique rationnelle de dimension 2 telle que ϕ représente tous les éléments de $\mathbb{Q}_-^*$, alors $-\phi$ représente tous les éléments de $\mathbb{Q}_+^*$ et donc $-\phi$ est isotrope, régulière et universelle d'après ce qui précède et de même pour ϕ. □

8.3 Application à la représentation des entiers

8.3.1 Etude de l'équivalence entre les formes $\langle n, n, n, n \rangle$ et $\langle 1, 1, 1, 1 \rangle$

Proposition 8.3.1. *Soit $n \in \mathbb{N}^*$. Les formes quadratiques rationnelles diagonales $\langle 1, 1, 1, 1 \rangle$ et $\langle n, n, n, n \rangle$ sont équivalentes et donc tout entier naturel n s'écrit comme somme de quatre carrés de rationnels.*

Démonstration. Soit $n \in \mathbb{N}^*$, n se décompose sous la forme $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ où pour $i \in [\![1, r]\!]$, $\alpha_i \in \mathbb{N}^*$ et les p_i sont des nombres premiers deux à deux distincts. On commence par réduire n modulo les carrés de $\mathbb{Q}^*$, ainsi dans $\mathbb{Q}^*/(\mathbb{Q}^*)^2$, $n = \prod_{i=1}^{l} q_i$ où les q_i correspondent aux nombres premiers distincts p_j dans la décompositon précédente de n pour lesquels $\alpha_j \equiv 1\,[2]$. D'où,

$$\langle n, n, n, n \rangle \simeq \langle q_1 q_2 \dots q_l, q_1 q_2 \dots q_l, q_1 q_2 \dots q_l, q_1 q_2 \dots q_l \rangle$$

les q_i étant premiers, deux à deux distincts, pour $i \in [\![1, l]\!]$.

D'après le test d'équivalence rationnelle, les formes diagonales $\phi = \langle 1, 1, 1, 1\rangle$ et $\psi = \langle q_1q_2 \dots q_l, q_1q_2 \dots q_l, q_1q_2 \dots q_l, q_1q_2 \dots q_l\rangle$ sont équivalentes si et seulement si elles ont même signature et si :

$$\forall p \in \mathcal{P}, \partial_p([\phi]_W) = \partial_p([\psi]_W).$$

Or il est clair que ϕ et ψ ont la même signature et il suffit alors simplement de vérifier l'égalité $\partial_p([\phi]_W) = \partial_p([\psi]_W)$ pour les $p = q_i$, $i \in [\![1, l]\!]$. En effet, pour les autres p, on a déjà $\partial_p([\phi]_W) = \partial_p([\psi]_W) = 0_{W(\mathbb{F}_p)}$. Pour $p = q_i$,

$$< \partial_{q_i}(1), \partial_{q_i}(1), \partial_{q_i}(1), \partial_{q_i}(1) >=< 0, 0, 0, 0 >= 0_{W(\mathbb{F}_{q_i})}$$

D'où $\partial_{q_i}([\phi]_W) = \partial_{q_i}([\psi]_W)$ dans $W(\mathbb{F}_{q_i})$ si et seulement si $\partial_{q_i}([\psi]_W) = 0_{W(\mathbb{F}_{q_i})}$, c'est-à-dire si et seulement si :

$$< \partial_{q_i}(q_1q_2 \dots q_l), \partial_{q_i}(q_1q_2 \dots q_l), \partial_{q_i}(q_1q_2 \dots q_l), \partial_{q_i}(q_1q_2 \dots q_l) >= 0_{W(\mathbb{F}_{q_i})}$$

Or, $\partial_{q_i}(q_1q_2 \dots q_l) = \prod_{j\neq i} \overline{q_j} \neq \overline{0}$ ($q_i \nmid \prod_{j\neq i} q_j$ car les q_j étant deux à deux distincts) et donc $\langle \partial_{q_i}(q_1q_2 \dots q_l), \partial_{q_i}(q_1q_2 \dots q_l), \partial_{q_i}(q_1q_2 \dots q_l), \partial_{q_i}(q_1q_2 \dots q_l)\rangle$ est équivalente à $\langle 1, -1\rangle \perp \langle 1, -\delta\rangle$ sur $\mathbb{F}_{q_i}$ (cf. classification des formes quadratiques sur les corps finis) avec

$$\delta = \Delta(\langle \partial_{q_i}(q_1q_2 \dots q_l), \partial_{q_i}(q_1q_2 \dots q_l), \partial_{q_i}(q_1q_2 \dots q_l), \partial_{q_i}(q_1q_2 \dots q_l)\rangle)$$

Comme $\delta = (-1)^{\frac{4\times 3}{2}} \partial_{q_i}(q_1q_2 \dots q_l)^4 = 1$ dans $\mathbb{F}_{q_i}^*/(\mathbb{F}_{q_i}^*)^2$, on a :

$$\langle \partial_{q_i}(q_1q_2 \dots q_l), \partial_{q_i}(q_1q_2 \dots q_l), \partial_{q_i}(q_1q_2 \dots q_l), \partial_{q_i}(q_1q_2 \dots q_l)\rangle \simeq 2.\langle 1, -1\rangle$$

et est donc bien hyperbolique sur $\mathbb{F}_{q_i}$. Ceci termine de montrer que :

$$\partial_{q_i}([\phi]_W) = \partial_{q_i}([\psi]_W) \text{ dans } W(\mathbb{F}_{q_i})$$

pour tous les q_i et ϕ et ψ sont bien équivalentes. La forme diagonale ψ étant elle même équivalente à $\langle n, n, n, n\rangle$ on a par transitivité :

$$\langle n, n, n, n\rangle \simeq \langle 1, 1, 1, 1\rangle$$

Comme n est représenté par $\langle n, n, n, n\rangle$, ($\langle n, n, n, n\rangle(1, 0, 0, 0) = n$), n est aussi représenté par $\langle 1, 1, 1, 1\rangle$, deux formes quadratiques équivalentes ayant même domaine. D'où, tout entier n est somme de quatre carrés de rationnels. □

8.3.2 Etude de l'équivalence entre les formes $\langle n, n\rangle$ et $\langle 1, 1\rangle$

Proposition 8.3.2. *Pour $n \in \mathbb{N}^*$, les formes quadratiques rationnelles diagonales $\langle 1, 1\rangle$ et $\langle n, n\rangle$ sont équivalentes si et seulement si pour tout nombre premier p tel que $v_p(n)$ est impair on a $p \equiv 1[4]$.*

Démonstration. Comme précédemment, $n \in \mathbb{N}^*$ se décompose sous la forme $n = \prod_{i=1}^r p_i^{\alpha_i}$ où $\alpha_i \in \mathbb{N}^*$ et les p_i sont des nombres premiers deux à deux distincts, pour $i \in [\![1, r]\!]$. Par réduction modulo les carrés de $\mathbb{Q}^*$ on a aussi $n = \prod_{i=1}^l q_i$ dans $\mathbb{Q}^*/(\mathbb{Q}^*)^2$ où les q_i correspondent aux nombres premiers distincts p_j dans la décompositon précédente de n pour lesquels $\alpha_j \equiv 1\,[2]$. Ainsi $\langle n, n\rangle \simeq \langle \prod_{i=1}^l q_i, \prod_{i=1}^l q_i\rangle$ et on va chercher à déterminer une condition nécessaire et suffisante pour que $\langle \prod_{i=1}^l q_i, \prod_{i=1}^l q_i\rangle$ et $\langle 1, 1\rangle$ soient équivalentes sur $\mathbb{Q}$. Puisqu'elles ont même signature, elles sont équivalentes si et seulement si :

$$\forall p \in \mathcal{P}, \partial_p(< 1,1 >) = \partial_p(< \prod_{i=1}^{l} q_i, \prod_{i=1}^{l} q_i >) \text{ dans } W(\mathbb{F}_p)$$

ce qui équivaut encore au fait que :

$$\partial_p(< 1,1 >) = \partial_p(< \prod_{i=1}^{l} q_i, \prod_{i=1}^{l} q_i >) \text{ pour les } p = q_i, \text{ tels que } i \in [\![1, r]\!]$$

puisque pour les autres p, on a :

$$\partial_p(< 1,1 >) = \partial_p(< \prod_{i=1}^{l} q_i, \prod_{i=1}^{l} q_i >) = 0_{W(\mathbb{F}_p)}.$$

Pour $p = q_i$, $< \partial_{q_i}(1), \partial_{q_i}(1) >=< 0, 0 >$. D'où $\partial_{q_i}(\langle 1,1\rangle) = \partial_{q_i}(\langle \prod_{i=1}^{l} q_i, \prod_{i=1}^{l} q_i\rangle)$ dans $W(\mathbb{F}_{q_i})$ si et seulement si

$$\begin{gathered}\partial_{q_i}(< \prod_{i=1}^{l} q_i, \prod_{i=1}^{l} q_i >) = 0_{W(\mathbb{F}_{q_i})} \\ \iff \langle \partial_{q_i}(q_1 q_2 \dots q_l), \partial_{q_i}(q_1 q_2 \dots q_l)\rangle \text{ est une forme hyperbolique sur } \mathbb{F}_{q_i}\end{gathered}$$

Or $\partial_{q_i}(q_1 q_2 \dots q_l) = \prod_{j \neq i} \overline{q_j} \neq \overline{0}$ (puisque $q_i \nmid \prod_{j \neq i} q_j$, les q_j étant deux à deux distincts) et $\langle \partial_{q_i}(q_1 q_2 \dots q_l), \partial_{q_i}(q_1 q_2 \dots q_l)\rangle$ est donc une forme régulière de dimension 2 sur $\mathbb{F}_{q_i}$. Un plan quadratique régulier étant hyperbolique si et seulement si de déterminant -1, $\langle \partial_{q_i}(q_1 q_2 \dots q_l), \partial_{q_i}(q_1 q_2 \dots q_l)\rangle$ est hyperbolique :

$$\begin{aligned}
&\iff \quad det(\langle \partial_{q_i}(q_1 q_2 \dots q_l), \partial_{q_i}(q_1 q_2 \dots q_l)\rangle) = -1 \text{ dans } \mathbb{F}_{q_i}^*/(\mathbb{F}_{q_i}^*)^2 \\
&\iff \quad (\prod_{j \neq i} \overline{q_j})^2 = -1 \text{ dans } \mathbb{F}_{q_i}^*/(\mathbb{F}_{q_i}^*)^2 \\
&\iff \quad -1 \text{ est un carré de } \mathbb{F}_{q_i} \\
&\iff \quad q_i \equiv 1\,[4]
\end{aligned}$$

Ainsi $\langle \prod_{i=1}^{l} q_i, \prod_{i=1}^{l} q_i\rangle \simeq \langle 1,1\rangle$ si et seulement si $\forall i \in [\![1, l]\!]$, la forme diagonale $\langle \partial_{q_i}(q_1 q_2 \dots q_l), \partial_{q_i}(q_1 q_2 \dots q_l)\rangle$ est hyperbolique, ce qui revient au fait que

$$\forall i \in [\![1, l]\!],\ q_i \equiv 1\,[4].$$

Par définition des q_i ceci équivaut encore au fait que pour tout nombre premier p tel que $v_p(n)$ est impair on ait $p \equiv 1\,[4]$, ce qui peut encore s'écrire sous la forme $v_p(n)$ est pair pour tout nombre premier p tel que $p \equiv 3\,[4]$. □

Corollaire 8.3.1. *Soit $n \in \mathbb{N}^*$, alors n est somme de deux carrés de rationnels si et seulement si les formes quadratiques rationnelles $\langle 1,1\rangle$ et $\langle n,n\rangle$ sont équivalentes.*

Démonstration. Dans la proposition 8.3.2, on a vu que les formes $\langle 1,1\rangle$ et $\langle n,n\rangle$ sont équivalentes si et seulement si pour tout nombre premier p tel que $v_p(n)$ est impair on a $p \equiv 1\,[4]$. Supposons que les formes $\langle 1,1\rangle$ et $\langle n,n\rangle$ sont équivalentes, alors n est représenté par $\langle 1,1\rangle$ puisque n est clairement représenté par $\langle n,n\rangle$ et ceci implique alors que n est somme de deux carrés de rationnels.

Inversement, supposons que n est somme de deux carrés de rationnels, alors il existe un couple $(x,y) \in \mathbb{Q}\times\mathbb{Q}$ non nul tel que $n = \langle 1,1\rangle(x,y) = x^2+y^2$. Ainsi la restriction $\langle 1,1\rangle_{vect(x,y)}$ est équivalente à $\langle n\rangle$ et puisque $\langle 1,1\rangle$ est régulière et que $vect(x,y)$ est un hyperplan de $\mathbb{Q}^2$, par l'astuce de complétion avec un déterminant on a :

$$\langle 1,1\rangle \simeq \langle n, n\delta\rangle \text{ avec } \delta = \det(\langle 1,1\rangle)=1.$$

Soit au final $\langle n, n\rangle \simeq \langle 1, 1\rangle$ si n est somme de deux carrés de rationnels. Donc $\langle n, n\rangle \simeq \langle 1, 1\rangle$ si et seulement si n est somme de deux carrés de rationnels, ce qui est équivalent à ce que pour tout nombre premier p tel que $v_p(n)$ impair on ait $p \equiv 1[4]$. □

Remarque 8.3.1. *On peut montrer par l'étude de l'anneau des entiers de Gauss (cf.[2] 6.9 page 56) que n est somme de carrés de deux entiers si et seulement si $v_p(n)$ est pair pour tout $p \equiv 3\,[4]$, ce qui est équivalent au fait que pour tout $p \in \mathcal{P}$ tels que $v_p(n)$ est impair on ait $p \equiv 1\,[4]$. Ainsi, par le corollaire précédent, on voit qu'un entier n est somme de deux carrés de rationnels si et seulement s'il est somme de deux carrés d'entiers.*

Corollaire 8.3.2. *Pour tout $k \in \mathbb{Q}^*$, les matrices :*

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ et } \begin{pmatrix} 3 & 0 \\ 0 & k \end{pmatrix}$$

ne sont pas $\mathbb{Q}$-congruentes

Démonstration. Supposons par l'absurde qu'il existe un $k \in \mathbb{Q}^*$ tel que les matrices ci-dessus soient congruentes. Alors, pour un tel k, les formes quadratiques diagonales $\langle 1, 1\rangle$ et $\langle 3, k\rangle$ seraient équivalentes et 3 étant représenté par $\langle 3, k\rangle$, serait représenté par $\langle 1, 1\rangle$. D'après ce qui précède, 3 s'écrirait comme somme de deux carrés de rationnels et donc comme somme de deux carrés d'entiers, absurde. □

Chapitre 9

Formes quadratiques p-adiques, principes de Hasse et application à l'étude des formes quadratiques sur $\mathbb{Q}$

Dans ce chapitre, nous désignerons par $\mathcal{P}_\infty$, l'ensemble $\mathcal{P} \cup \{\infty\}$, où $\mathcal{P}$ représente l'ensemble des nombres premiers.

Nous allons commencer par introduire brièvement les corps p-adiques $\mathbb{Q}_p$ qui sont des extensions du corps $\mathbb{Q}$, dont nous étudierons au cœur du chapitre les groupes de Witt et Witt-Grothendieck associés. Nous verrons ensuite, comment les morphismes induits par l'extension des scalaires explicités au chapitre 7, appelés ici morphismes de localisation et définis de $W(\mathbb{Q}) \longrightarrow W(\mathbb{Q}_p)$, assurent un passage du rationnel au p-adique. Avec cet objectif d'étudier la connexion entre les formes quadratiques p-adiques et rationnelles, nous admettrons volontairement un certain nombre de résultats sur les formes quadratiques p-adiques (pour les démonstration cf.[1] XVIII), le but étant ici plutôt, d'appliquer ces résultats à l'étude des formes quadratiques rationnelles. Nous mettrons ainsi en avant, comment la compréhension des formes quadratiques p-adiques nous permet d'obtenir des résultats intéressants sur les formes quadratiques sur $\mathbb{Q}$, tels que :

- sur $\mathbb{Q}$, il existe une forme quadratique anisotrope et universelle.
- sur $\mathbb{Q}$, il existe une infinité de classes d'isomorphie de formes quadratiques indéfinies anisotropes et de dimension 4.

Nous admettrons alors un certain nombre de propositions en rapport avec l'étude de l'isotropie et de l'anisotropie des formes sur $\mathbb{Q}_p$, résultats qui, associés au principe de Hasse faible disant :

- qu'une forme quadratique ψ est hyperbolique si et seulement si ses localisées $\psi_p = \psi_{\mathbb{Q}_p}, \forall p \in \mathcal{P}_\infty$ sont hyperboliques

et le principe de Hasse fort disant :

- qu'une forme quadratique rationnelle ψ est isotrope si et seulement si ces localisées $\psi_p, \forall p \in \mathcal{P}_\infty$ sont isotropes

nous assurerons un passage du p-adique vers le rationnel et nous offrirons donc des outils pour aborder le problème de la vérification du caractère isotrope ou hyperbolique d'une forme quadratique rationnelle, en passant par des formes quadratiques auxiliaires que sont les localisées sur les corps p-adiques $\mathbb{Q}_p$ ainsi que sur le corps $\mathbb{R}$. Enfin, nous utiliserons le fait que toute forme quadratique rationnelle indéfinie de dimension au moins 5 est isotrope pour nous intéresser à la surjectivité du morphisme Φ et voir comment trouver un antécédent à un élément de $W(\mathbb{R}) \oplus \bigoplus_{p\in\mathcal{P}} W(\mathbb{F}_p)$ où,

$$\Phi : W(\mathbb{Q}) \xrightarrow{\simeq} W(\mathbb{R}) \oplus \bigoplus_{p\in\mathcal{P}} W(\mathbb{F}_p)$$

comme vu au chapitre précédent.

9.1 Une introduction élémentaire aux nombres p-adiques

9.1.1 Définition de $\mathbb{Q}_p$ et des lois associées à sa structure de corps

Dans cette partie, nous allons introduire brièvement les nombres p-adiques et donner quelques propriétés concernant les carrés de $\mathbb{Q}_p^*$, pour $p \in \mathcal{P}$.

Définition 9.1.1. *On appelle* ***nombre*** p***-adique*** *toute suite* $(a_k)_{k\in\mathbb{Z}}$ *d'éléments de* $[\![0, p-1]\!]$*, vérifiant,* $\exists m \in \mathbb{Z} : \forall k < m,\ a_k = 0$.

Un nombre p-adique a peut donc se représenter par un développement illimité formel :

$$a = a_m p^m + a_{m+1} p^{m+1} + \ldots + a_k p^k + \ldots$$

Le nombre entier a_k sera appelé le **chiffre de degré** k de a.

Notation 9.1.1. *Lorsque la suite* a *n'est pas nulle, l'entier relatif :*

$$\nu_p(a) = min\{k \in \mathbb{Z} : a_k \neq 0\}$$

est appelé la ***valuation*** p***-adique*** *de* a*. On convient que* $\nu_p(0) = \infty$*. On appelle* ***entiers*** p***-adiques*** *les nombres* p*-adiques de valuation positive ou nulle et* ***unités*** p***-adiques*** *les nombres* p*-adiques de valuation nulle. On note ainsi* $\mathbb{Q}_p$ *l'ensemble des nombres* p*-adiques,* $\mathbb{Z}_p$ *l'ensemble des entiers* p*-adiques et* $\mathbb{Z}_p^\times$ *celui des unités* p*-adiques.*

Naturellement, on peut associer à tout entier naturel, la suite de ses chiffres en base p, ceci nous permet d'identifier $\mathbb{N}$ à un sous-ensemble de $\mathbb{Z}_p$. Les entiers naturels qui sont des unités p-adiques sont ceux dont la valuation p-adique est nulle, soit donc les entiers naturels non divisibles par p. $\mathbb{N}$ pouvant être vu comme un sous-ensemble de $\mathbb{Q}_p$, on va définir des opérations d'addition et de multiplication qui prolongent celles de $\mathbb{N}$, en généralisant à des suites infinies, les algorithmes d'addition et de multiplication en base p.

Soit deux éléments quelconques a et b de $\mathbb{Q}_p$ et l'on note $m = min(\nu_p(a), \nu_p(b))$. On définit deux suites $(q_k)_{k\in\mathbb{Z}}$ et $(r_k)_{k\in\mathbb{Z}}$ par :

- $\forall k < m, q_k = r_k = 0$
- $\forall k \geq m$, les entiers q_k et r_k sont respectivement le quotient et le reste de $q_{k-1} + a_k + b_k$ modulo p

On pose alors $a + b = (r_k)_{k\in\mathbb{Z}}$, ce qui définit la loi additive $+$ sur $\mathbb{Q}_p$.
on définit de même deux suites $(q'_k)_{k\in\mathbb{Z}}$ et $(r'_k)_{k\in\mathbb{Z}}$ par :

- $\forall k < m, q_k = r_k = 0$
- $\forall k \geq m$, les entiers q'_k et r'_k sont respectivement le quotient et le reste de $q'_{k-1} + \sum_{j\in\mathbb{Z}} a_{k-j} + b_j$ modulo p, la somme étant finie car pour $k \geq m$ il ne reste qu'un nombre fini de termes non nuls ($a_{k-j} = 0$ si $j > k - m$ et $b_j = 0$ si $j < m$).

On pose alors $a \times b = (r'_k)_{k\in\mathbb{Z}}$, ce qui définit la loi multiplicative $\times$ sur $\mathbb{Q}_p$.

Remarque 9.1.1. *Lorsque a et b sont des entiers p-adiques, le caclcul des chiffres de la décomposition de $a \times b$ et $a + b$ en degré inférieur ou égal à n ne fait intervenir que les chiffres de a et b en degré inférieur ou égal à n. Les définitions de la loi $+$ et $\times$ sur $\mathbb{Q}_p$ prolongent l'addition et la multiplication des entiers naturels et font de $(\mathbb{Q}_p, +, \times)$ un corps commutatif contenant $\mathbb{Z}$. $\mathbb{Q}$ étant le corps des fractions de $\mathbb{Z}$, il est le plus petit corps contenant $\mathbb{Z}$, ce qui par minimalité impose donc que $\mathbb{Q}$ se plonge naturellement dans $\mathbb{Q}_p$. En particulier $\mathbb{Z}_p$ est un sous-anneau de $\mathbb{Q}_p$ dont $\mathbb{Z}_p^\times$ est le groupe des inversibles pour la loi $\times$.*

Proposition 9.1.1. *Tout élément $a \in \mathbb{Q}_p^*$ s'écrit de manière unique sous la forme $a = p^m b$ où $m \in \mathbb{Z}$ et $b \in \mathbb{Z}_p^\times$ avec nécessairement $m = \nu_p(a)$.*

Démonstration. Soit $a = a_m p^m + a_{m+1}p^{m+1} + \ldots + a_k p^k + \ldots$, où la valuation $m = \nu_p(a)$ est définie uniquement sans ambiguïté et $a_i \in [\![0, p-1]\!]$. Ainsi, on a :

$$a = p_m \times (a_m + a_{m+1}p + \ldots + a_k p^{k-m} + \ldots)$$

et $+$ et $\times$ prolongeant sur $\mathbb{Q}_p$, les lois sur les entiers, il vient $a = p^m \times b$ où $b = a_m + a_{m+1}p + \ldots + a_k p^{k-m} + \ldots \in \mathbb{Z}_p^*$ et $\times$ désigne la loi multiplicative sur $\mathbb{Q}_p$. □

Remarque 9.1.2. *Soit $r \in \mathbb{Q}^*$ et $p \in \mathcal{P}$. Alors, on sait qu'il existe p_1, q_1 entiers premiers avec p tels que $r = p^{\nu_p(r)}\dfrac{p_1}{q_1}$. Ainsi, puisque p_1, q_1 sont premiers avec p, ce sont des unités p-adiques et les lois $+$ et $\times$ de $\mathbb{Q}_p$ prolongeant celles des entiers, il vient que $p_1 q_1^{-1}$ est aussi une unité p-adique, $\mathbb{Z}_p^\times$ étant d'après la remarque précédente un groupe pour la loi $\times$. D'après l'unicité d'écriture d'un élément $a \in \mathbb{Q}^* \subset \mathbb{Q}_p^*$ décrite dans la proposition ci-dessus, la valuation p-adique de r en tant que nombre rationnel a le même sens que la valuation p-adique de r en tant que nombre p-adique.*

9.1.2 Etude des carrés de $\mathbb{Q}_p$

Carrés de $\mathbb{Q}_p$, p premier impair.

Afin de simplifier l'étude des formes quadratiques sur $\mathbb{Q}_p$, il est commode de savoir déterminer si deux éléments de $\mathbb{Q}_p^*$ sont dans la même classe modulo les carrés de $\mathbb{Q}_p^*$, notamment afin de réduire au mieux l'écriture d'une forme quadratique diagonale sur $\mathbb{Q}_p$ mais aussi connaître des systèmes de générateurs pour les groupes $W(\mathbb{Q}_p)$ et $\widehat{W}(\mathbb{Q}_p)$.

Proposition 9.1.2. *Soit a et b deux éléments de $\mathbb{Q}_p^*$. Alors, pour $m = \nu_p(a)$ et $n = \nu_p(b)$, les éléments a et b ont la même classe dans $\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2$ si et seulement si :*

$$m \equiv n\,[2] \text{ et si } a_m \text{ et } b_n \text{ sont égaux modulo les carrés de } \mathbb{F}_p^*.$$

Corollaire 9.1.1. *Soit p un nombre premier impair. Le groupe $\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2$ est de cardinal 4, ses éléments sont les classes respectives des entiers $1, \varepsilon, p, p\varepsilon$ où ε désigne un représentant dans $[\![0, p-1]\!]$ de la classe des non carrés de $\mathbb{F}_p^*$.*

Démonstration. On a :
- $\nu_p(1) = 0 \equiv 0\,[2]$ et la classe de 1 modulo p est un carré de $\mathbb{F}_p^*$.
- $\nu_p(p) = 1 \equiv 1\,[2]$ et le chiffre de degré 1 de p est 1, dont la classe modulo p est un carré de $\mathbb{F}_p^*$.
- $\varepsilon \in [\![0, p-1]\!]$, soit $\nu_p(\varepsilon) = 0 \equiv 0\,[2]$, le chiffre de degré 0 étant ε dont la classe modulo p n'est pas un carré de $\mathbb{F}_p^*$.
- $\nu_p(p\varepsilon) = 1 \equiv 1\,[2]$, le chiffre de degré 1 étant ε dont la classe modulo p n'est pas un carré de $\mathbb{F}_p^*$.

Puisque $\mathbb{Z}/2$ et $\mathbb{F}_p^*/(\mathbb{F}_p^*)^2$ sont d'ordre 2, les quatre cas exposés ci-dessus décrivent toutes les situations envisageables et $1, p, \varepsilon, p\varepsilon$ sont bien des représentants des quatre classes du groupe $\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2$. □

Remarque 9.1.3. *Par définition de la loi + sur le corps $\mathbb{Q}_p$ on a :*

$$1 + (p-1) + (p-1)p + (p-1)p^2 + \ldots + (p-1)p^n + \ldots = 0$$

et donc $-1 = (p-1) + (p-1)p + (p-1)p^2 + \ldots + (p-1)p^n + \ldots$ sur $\mathbb{Q}_p$. Ainsi, $\nu_p(-1) = 0$ et son chiffre de rang 0 est $p-1$. Comme dans $\mathbb{F}_p$, $\overline{p-1} = \overline{-1}$, il vient que :
- *$-1 = 1$ dans $\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2$ si -1 est un carré modulo p*
- *$-1 = \varepsilon$ dans $\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2$ si -1 n'est pas un carré modulo p.*

Corollaire 9.1.2. *$\{< 1 >, < \varepsilon >, < p >, < p\varepsilon >\}$ est un ensemble générateur de $W(\mathbb{Q}_p)$ et $\{\langle 1\rangle, \langle p\rangle, \langle \varepsilon\rangle, \langle p\varepsilon\rangle\}$ est un ensemble générateur de $\widehat{W}(\mathbb{Q}_p)$.*

Carrés de $\mathbb{Q}_2$

Proposition 9.1.3. *Soit, deux entiers 2-adiques a et b de valuations 2-adiques respectives m et n. Ainsi, on a :*

$$2^{-m}a = a_m + a_{m+1}2 + a_{m+2}2^2 + a_{m+3}2^3 \ldots + a_k 2^{k-m} + \ldots$$

et

$$2^{-n}b = b_n + b_{n+1}2 + b_{n+2}2^2 + b_{n+3}2^3 + \ldots + a_k p^k + \ldots$$

Alors, a et b ont la même classe dans $\mathbb{Q}_2^*/(\mathbb{Q}_2^*)^2$ si et seulement si :

$$m \equiv n\,[2] \text{ et } a_m + a_{m+1}2 + a_{m+2}2^2 \equiv b_n + b_{n+1}2 + b_{n+2}2^2\,[8]$$

où l'on note la congruence ci-dessus $2^{-m}a \equiv 2^{-n}b\,[8]$.

Corollaire 9.1.3. *L'ensemble $\mathbb{Q}_2^*/(\mathbb{Q}_2^*)^2$ contient 8 éléments qui sont les classes respectives des entiers $1, 3, 5, 7, 2, 6, 10$ et 14.*

Démonstration. Si $a \in \mathbb{Z}_2^\times$ est en entier 2-adique, alors :

$$a = 1 + a_1 2 + a_2 2^2 + \dots$$

et donc, selon que $a_1 = 0$ ou 1 et que $a_2 = 0$ ou 1, on voit que

$$1 + a_1 2 + a_2 2^2 = 1,\ 3,\ 5 \text{ ou } 7.$$

Ces éléments étant distincts modulo 8, les entiers 2-adiques $1, 3, 5, 7$ représentent donc 4 classes distinctes modulo $(\mathbb{Q}_2^*)^2$. On obtient les autres classes de $\mathbb{Q}_2^*/(\mathbb{Q}_2^*)^2$ en multipliant chacun de ces entiers par 2. Supposons en effet que $a \in \mathbb{Q}_2^*$ et $\nu_2(a) = 2k + 1 \equiv 1\,[2]$, alors :

$$a = a_{2k+1} 2^{2k+1} + a_{2k+2} 2^{2k+2} + \dots +$$

et donc :

$$2^{-(2k+1)} a = a_{2k+1} + a_{2k+2} 2 + a_{2k+3} 2^2 \dots$$

Alors $a_{2k+1} \neq 0 \Longrightarrow a_{2k+1} = 1$ et selon que $a_{2k+2} = 0$ ou 1 et que $a_{2k+3} = 0$ ou 1, on trouve que :

$$a_{2k+1} + a_{2k+2} 2 + a_{2k+3} 2^2 \equiv 1, 3, 5, 7\,[8]$$

Puisque l'on a $\nu_2(2) = \nu_2(6) = \nu_2(10) = \nu_2(14) \equiv 1\,[2]$, notant m leur valuation on retrouve $2^{-m} \equiv 1, 3, 5, 7\,[8]$ et donc les entiers $2, 6, 10$ et 14 sont des représentants des 4 autres classes de $\mathbb{Q}_2^*/(\mathbb{Q}_2^*)^2$, chaque élément de $(\mathbb{Q}_2)^*$ de valuation impaire étant modulo $(\mathbb{Q}_2^*)^2$ égal à un de ces éléments là. □

Remarque 9.1.4. *Comme dans le cas p premier impair, on a :*

$$-1 = 1 + 2 + 2^2 + 2^3 + \dots + 2^n + \dots.$$

Alors $\nu_2(-1) = 0$ *et* $1 + 2 + 2^2 \equiv 7\,[8]$*, soit* $-1 = 7$ *sur* $\mathbb{Q}_2^*/(\mathbb{Q}_2^*)^2$.

Pour les applications à venir, on aura besoin de connaître la table de multiplication de ce groupe. On l'obtient, en appliquant la règle de calcul énoncée à la proposition 9.1.3 :

Table de multiplication de $\mathbb{Q}_2^*/\left(\mathbb{Q}_2^*\right)^2$

$\times$	**1**	**3**	**5**	**7**	**2**	**6**	**10**	**14**
1	1	3	5	7	2	6	10	14
3	3	1	7	5	6	2	14	10
5	5	7	1	3	10	14	2	6
7	7	5	3	1	14	10	6	2
2	2	6	10	14	1	3	5	7
6	6	2	14	10	3	1	7	5
10	10	14	2	6	5	7	1	3
14	14	10	6	2	7	5	3	1

Corollaire 9.1.4. $\{< 1 >, < 3 >, < 5 >, < 7 >, < 2 >, < 6 >, < 10 >, < 14 >\}$ *est un système générateur de* $W(\mathbb{Q}_2)$ *et* $\{\langle 1\rangle, \langle 3\rangle, \langle 5\rangle, \langle 7\rangle, \langle 2\rangle, \langle 6\rangle, \langle 10\rangle, \langle 14\rangle\}$ *est un système générateur de* $\widehat{W}(\mathbb{Q}_2)$.

Ceci clôt cette partie introductice, nous allons maintenant nous intéresser aux différents liens qui existent entre les formes quadratiques rationnelles et p-adiques et allons voir comment obtenir des renseignements sur une forme quadratique rationnelle régulière q, à partir de l'étude de ces différentes localisées $q_p = q_{\mathbb{Q}_p}$, pour $p \in \mathcal{P}_\infty$.

9.2 Du rationnel au p-adique

9.2.1 Morphismes de localisation

Définition 9.2.1. *Soit ψ une forme quadratique régulière sur $\mathbb{Q}$ et $p \in \mathcal{P}_\infty$. On appelle **localisée** de ψ au voisinage de p que l'on note ψ_p, la forme quadratique $\psi_{\mathbb{Q}_p}$.*

Définition 9.2.2. *Pour $p \in \mathcal{P}_\infty$, on appelle morphisme de localisation, le morphisme $W(\mathbb{Q}) \longrightarrow W(\mathbb{Q}_p)$, associé canoniquement à l'extension des scalaires $\mathbb{Q} \subset \mathbb{Q}_p$. Pour $p = \infty$, ce morphisme de localisation est le morphsime d'extension des scalaires de $\mathbb{Q}$ à $\mathbb{R}$ que l'on a exhibé dans le chapitre sur le groupe de Witt $W(\mathbb{Q})$.*

Dans le chapitre sur le groupe de Witt, nous avons vu, qu'il existait un unique morphisme de $W(\mathbb{Q})$ dans $W(\mathbb{F}_p)$ tel que : $\forall r \in \mathbb{Q}^*$, $\partial_p(< r >) =< \partial_p(r) >$. Pour $p \in \mathcal{P}$, on peut définir de même, un unique morphisme de $W(\mathbb{Q}_p)$ dans $W(\mathbb{F}_p)$ noté ∂'_p et tel que $\partial'_p(< r >) =< \partial_p(r) >, \forall r \in \mathbb{Q}_p^*$, où l'application $\partial_p : \mathbb{Q}^* \longrightarrow \mathbb{F}_p^*$ vu au chapitre précédent se prolonge naturellement à $\mathbb{Q}_p^*$.

Définition 9.2.3. *Soit $a \in \mathbb{Q}_p^*$. On pose :*

$$res_p(a) = \overline{a_m} \in \mathbb{F}_p^*, \text{ où } m = \nu_p(a).$$

et

$$\partial_p(a) = res_p(a) \text{ si } \nu_p(a) \equiv 1\,[2] \text{ et } \partial_p(a) = 0 \text{ si } \nu_p(a) \equiv 0\,[2].$$

Proposition 9.2.1. *Il existe un unique morphisme de groupes*

$$\partial'_p : W(\mathbb{Q}_p) \longrightarrow W(\mathbb{F}_p)$$

vérifiant

$$\forall r \in \mathbb{Q}_p^*, \partial'_p(< r >) =< \partial_p(r) >.$$

Alors, on a :

$$\forall r \in \mathbb{Q}^*, \partial_p(< r >) =< \partial_p(r) >= \partial'_p(< r >_{\mathbb{Q}_p}) = \partial'_p(f(< r >))$$

où $f : W(\mathbb{Q}) \longrightarrow W(\mathbb{Q}_p)$ désigne le morphisme de localisation. Puisque l'ensemble, $\{< r > | \ r \in \mathbb{Q}^*\}$ est une partie génératrice de $W(\mathbb{Q})$, $\partial'_p \circ f = \partial_p$ sur une partie génératrice et donc sur $W(\mathbb{Q})$ tout entier, les applications f, ∂_p et ∂'_p étant des morphismes de groupes.

9.2.2 Principes de Hasse

Dans cette section, nous allons énoncer et démontrer le principe de Hasse faible et simplement énoncer sans démonstration le principe de Hasse fort. Nous verrons comme son nom l'indique que le principe de Hasse fort implique celui de Hasse faible et qu'en dimension 2 et 3 les deux principes sont équivalents. Nous nous attarderons également sur des applications de ces principes qui illustrerons le lien étroit qui existe entre les propriétés d'une forme quadratique rationnelle et celles de ses localisées.

Définition 9.2.4. *On note Ψ le morphisme de localisation définie par :*

$$\Psi : \begin{cases} W(\mathbb{Q}) \longrightarrow W(\mathbb{R}) \oplus \bigoplus_{p\in\mathcal{P}} W(\mathbb{Q}_p) \\ q \longmapsto \ q_{\mathbb{R}} + \sum_{p\in\mathcal{P}} q_p \end{cases}$$

où l'on garde ici, par commodité, la notation additive $\bigoplus_{p\in\mathcal{P}} W(\mathbb{Q}_p)$ pour parler du produit direct usuel d'une infinité d'ensembles.

Théorème 9.2.1. ***Principe de Hasse faible***
Deux formes quadratiques rationnelles régulières ϕ et ψ sont Witt-équivalentes si et seulement si ϕ_p et ψ_p sont Witt-équivalentes pour tout $p \in \mathcal{P}_\infty$. On peut reformuler ce théorème de la façon suivante : une forme quadratique rationnelle régulière ϕ est hyperbolique si et seulement si ϕ_p est hyperbolique quelque soit $p \in \mathcal{P}_\infty$.

Démonstration. On va montrer l'injectivité du morphisme de localisation Ψ ci-dessus ce qui montrera le résultat. En effet, si Ψ est injective, alors pour ψ et ϕ deux formes quadratiques rationnelles régulières, on a :

$$\begin{aligned} [\psi]_W = [\phi]_W &\iff \Psi([\psi]_W) = \Psi([\phi]_W) \\ &\iff \forall p \in \mathcal{P}_\infty,\ [\psi_p]_W = [\phi_p]_W \\ &\iff \forall p \in \mathcal{P}_\infty,\ \psi_p \overset{W}{\sim} \phi_p \end{aligned}$$

En composant par le morphisme :

$$Id_{W(\mathbb{R})} \oplus \bigoplus_{p\in\mathcal{P}} \partial'_p : W(\mathbb{R}) \oplus \bigoplus_{p\in\mathcal{P}} W(\mathbb{Q}_p) \longrightarrow W(\mathbb{R}) \oplus \bigoplus_{p\in\mathcal{P}} W(\mathbb{F}_p)$$

on a : $(Id_{W(\mathbb{R})} \oplus \bigoplus_{p\in\mathcal{P}} \partial'_p) \circ \Psi = \Phi$ où Φ est comme on l'a vu, un isomorphisme. Alors, si on suppose que Ψ n'est pas injective, il existe q et q' formes quadratiques rationnelles régulières telles que $[q]_W \neq [q']_W \in W(\mathbb{Q})$ et $\Psi([q]_W) = \Psi([q']_W)$. Et,

$$(Id_{W(\mathbb{R})} \oplus \bigoplus_{p\in\mathcal{P}} \partial'_p) \circ \Psi([q]_W) = (Id_{W(\mathbb{R})} \oplus \bigoplus_{p\in\mathcal{P}} \partial'_p) \circ \Psi([q']_W)$$

soit : $\Phi([q]_W) = \Phi([q']_W) \Longrightarrow [q]_W = [q']_W \in W(\mathbb{Q})$ par injectivité de Φ, absurde. D'où Ψ est injective, ce qui montre le principe de Hasse faible.

Montrons l'équivalence entre les deux formulations. Soit ϕ et ψ deux formes quadratiques rationnelles régulières. Alors, supposons que ϕ et ψ sont Witt-équivalentes si et seulement si leurs localisés ϕ_p et ψ_p sont Witt-équivalentes

pour tout $p \in \mathcal{P}_\infty$. Alors ϕ est hyperbolique si et seulement si $[\psi]_W = 0_{W(\mathbb{Q})}$ c'est à dire si et seulement si :

$$\begin{array}{rc} & \psi \overset{W}{\sim} 0 \\ \iff & \forall p \in \mathcal{P}_\infty,\, \psi_p \overset{W}{\sim} 0 \\ \iff & \forall p \in \mathcal{P}_\infty,\, \psi_p \text{ est hyperbolique} \end{array}$$

Ainsi, la première formulation du principe de Hasse faible implique la seconde formulation. Inversement, supposons que ϕ est hyperbolique si et seulement si $\forall p \in \mathcal{P}_\infty$, ϕ_p est hyperbolique et montrons que cela implique la première formulation du principe de Hasse faible. Alors,

$$\begin{array}{rc} & [\phi]_W = [\psi]_W \\ \iff & [\phi]_W - [\psi]_W = 0_{W(\mathbb{Q})} \\ \iff & [\phi \perp (-\psi)]_W = 0_{W(\mathbb{Q})} \\ \iff & \psi \perp (-\psi), \text{ est hyperbolique} \\ \iff & \forall p \in \mathcal{P}_\infty,\, (\psi \perp (-\psi))_p, \text{ est hyperbolique} \\ \iff & \forall p \in \mathcal{P}_\infty,\, \psi_p \perp (-\psi)_p, \text{ est hyperbolique} \\ \iff & \forall p \in \mathcal{P}_\infty,\, [\psi_p \perp (-\psi)_p]_W = 0_{W(\mathbb{Q}_p)} \\ \iff & \forall p \in \mathcal{P}_\infty,\, [\psi_p]_W - [\psi_p]_W = 0_{W(\mathbb{Q}_p)} \\ \iff & \forall p \in \mathcal{P}_\infty,\, [\psi_p]_W = [\phi_p]_W \end{array}$$

et la seconde formulation du principe de Hasse faible implique la première. Les deux formulations sont donc naturellement équivalentes. □

Tout comme le test de Witt-équivalence rationnelle reposait sur l'injectivité du morphisme Φ, le principe de Hasse faible repose donc sur l'injectivité du morphisme de localisation Ψ. En revanche, contrairement au morphisme Φ, le morphisme de localisation n'est pas surjectif :

Corollaire 9.2.1. *Le morphisme de localisation*

$$\Psi : W(\mathbb{Q}) \longrightarrow W(\mathbb{R}) \oplus \bigoplus_{p \in \mathcal{P}} W(\mathbb{Q}_p)$$

et sa restriction à $I(\mathbb{Q})$*,*

$$\Psi_{I(\mathbb{Q})} : I(\mathbb{Q}) \longrightarrow I(\mathbb{R}) \oplus \bigoplus_{p \in \mathcal{P}} I(\mathbb{Q}_p)$$

ne sont pas surjectifs.

Démonstration. On va prouver de manière directe que Ψ n'est pas surjectif en exhibant un élément de $W(\mathbb{R}) \oplus \bigoplus_{p \in \mathcal{P}} W(\mathbb{Q}_p)$ non atteint. Soit $< 1, 1 >_2$ dans $W(\mathbb{Q}_2)$, la localisée sur $\mathbb{Q}_2$ de $< 1, 1 > \in W(\mathbb{Q})$. On considère la suite presque nulle $(0, < 1, 1 >_2, 0, ...)$ où seul l'élément $< 1, 1 >_2$ de $W(\mathbb{Q}_2)$ est non nul. En effet, $< 1, 1 >_2 \neq 0_{W(\mathbb{Q}_2)}$ car :

$$\begin{array}{rc} < 1, 1 >_2 = 0_{W(\mathbb{Q}_2)} \iff & \langle 1, 1 \rangle \text{ est hyperbolique sur } \mathbb{Q}_2. \\ \iff & \text{-1 est un carré de } \mathbb{Q}_2 \end{array}$$

Or -1 = 7 dans $\mathbb{Q}_2^* / \left(\mathbb{Q}_2^*\right)^2$ et donc $< 1, 1 >_2 \neq 0_{W(\mathbb{Q}_2)}$.

Supposons $(0, < 1, 1 >_2, 0, ...)$ atteint par Ψ, c'est à dire qu'il existe φ forme quadratique rationnelle régulière telle que $\Psi([\varphi]_W) = (0, < 1, 1 >_2, 0, ...)$. Or la composée $(id_{W(\mathbb{R})} \oplus \bigoplus_{p\in\mathcal{P}} \partial_p^{'}) \circ \Psi$ est exactement l'isomorphisme Φ tel que :

$$\Phi\colon \begin{cases} W(\mathbb{Q}) \longrightarrow W(\mathbb{R}) \oplus \bigoplus_{p\in\mathcal{P}} W(\mathbb{F}_p) \\ x \longmapsto x_{\mathbb{R}} + \sum_{p\in\mathcal{P}} \partial_p(x) \end{cases}$$

Alors :

$$\begin{aligned} id_{W(\mathbb{R})} \oplus \bigoplus_{p\in\mathcal{P}} \partial_p^{'}(\Psi([\varphi]_W)) = \quad & id_{W(\mathbb{R})} \oplus \bigoplus_{p\in\mathcal{P}} \partial_p^{'}(0, < 1, 1 >_2, 0, ...) \\ = \quad & (0, \partial_2^{'}(< 1, 1 >_2), 0, ...). \end{aligned}$$

Or $\partial_2^{'}(< 1, 1 >_2)) =< \partial_2(1), \partial_2(1) >= 0_{W(\mathbb{F}_2)}$ ce qui nous donne :

$$\Phi([\varphi]_W) = id_{W(\mathbb{R})} \oplus \bigoplus_{p\in\mathcal{P}} \partial_p^{'}(\Psi([\varphi]_W)) = 0_{W(\mathbb{F}_2)}$$

Mais Φ étant un isomorphisme, il vient alors $[\varphi]_W = 0_{W(\mathbb{Q})}$ et donc :

$$\Psi([\varphi]_W) = 0_{W(\mathbb{R})\oplus\bigoplus_{p\in\mathcal{P}} W(\mathbb{F}_p)}$$

absurde, puisque $\Psi([\varphi]_W) = (0, < 1, 1 >_2, 0, ...) \neq 0_{W(\mathbb{R})\oplus\bigoplus_{p\in\mathcal{P}} W(\mathbb{F}_p)}$. Donc Ψ non surjectif car $(0, < 1, 1 >_2, 0, ...) \in W(\mathbb{R}) \oplus \bigoplus_{p\in\mathcal{P}} W(\mathbb{Q}_p)$ non atteint par Ψ.

Pour finir étudions la restriction de Ψ à $I(\mathbb{Q})$. Tout d'abord, il est clair que $\Psi_{I(\mathbb{Q})}$ est à valeur dans $I(\mathbb{R})\oplus\bigoplus_{p\in\mathcal{P}} I(\mathbb{Q}_p)$, puisque si $< a_1, .., a_{2n} >\in I(\mathbb{Q})$ avec $a_1, .., a_{2n} \in \mathbb{Q}^*$ alors $< a_1, .., a_{2n} >_p$ où $p \in \mathcal{P} \cup \{\infty\}$ est encore de dimension paire vue comme classe de Witt-équivalence sur $\mathbb{Q}_p$. Or,

$$(0, < 1, 1 >_2, 0, ...) \in I(\mathbb{R}) \oplus \bigoplus_{p\in\mathcal{P}} I(\mathbb{Q}_p)$$

n'est pas atteint par Ψ donc n'est pas atteint par $\Psi_{I(\mathbb{Q})}$ et

$$\Psi_{I(\mathbb{Q})} : I(\mathbb{Q}) \longrightarrow I(\mathbb{R}) \oplus \bigoplus_{p\in\mathcal{P}} I(\mathbb{Q}_p)$$

non surjectif. □

Remarque 9.2.1. *Ce premier principe de Hasse n'est pas le moyen le plus adapté pour montrer qu'une forme quadratique rationnelle de dimension $2n$ est hyperbolique, il est bien plus commode d'utiliser le test d'équivalence rationnelle et de tester l'équivalence avec la forme $n.\langle 1, -1\rangle$. Néanmois, d'un point de vue théorique, il est intéressant de voir comment des propriétés "locales", concernant les formes localisées qui sont des formes quadratiques p-adiques peuvent être associés à des propriétés "globales" sur la forme quadratique rationnelle que l'on souhaite étudier. Ce principe de Hasse faible est le premier exemple d'une telle connexion, on en verra d'autres par la suite, notamment avec le principe de Hasse fort qui suit.*

Théorème 9.2.2. *Une forme quadratique rationnelle régulière ψ est isotrope si et seulement si ψ_p est isotrope pour tout $p \in \mathcal{P}_\infty$.*

Démonstration. cf.[1] XIX page 420. □

Remarque 9.2.2. *Le test d'équivalence rationnelle ne fournit pas en revanche, de critère pour montrer qu'une forme quadratique rationnelle donnée est isotrope, (à moins de tester l'équivalence avec une forme quadratique rationnelle dont on sait déjà qu'elle est isotrope, ou d'utiliser l'astuce de la dimension* 4 *si la situation s'y prête), le principe de Hasse fort, nous permettra de tester l'isotopie d'une forme sur* $\mathbb{Q}$*, une fois que l'on aura caractériser les formes quadratiques isotropes et anisotropes sur les corps* $\mathbb{Q}_p$*.*

La proposition qui suit, justifie pourquoi le second principe de Hasse que nous avons présenté est dit "fort", alors que le premier que nous avons évoqué est dit "faible".

Proposition 9.2.2. *Le principe de Hasse fort implique le principe de Hasse faible et en dimension* 2 *et* 3 *ces deux principes sont équivalents, c'est-à-dire qu'on déduit du principe de Hasse faible, celui de Hasse fort.*

Démonstration. Montrons dans un premier temps, que le principe de Hasse fort implique le principe de Hasse faible. Soit ϕ une forme quadratique rationnelle régulière, que l'on suppose hyperbolique. On a donc :

$$\begin{aligned} \phi \text{ hyperbolique} \implies & \quad \exists n \in \mathbb{N}^*,\ \phi \simeq n.\langle 1,-1\rangle \\ \implies & \quad \exists n \in \mathbb{N}^*,\ \forall p \in \mathcal{P}_\infty,\ \phi_p \simeq (n.\langle 1,-1\rangle)_p \\ \implies & \quad \exists n \in \mathbb{N}^*,\ \forall p \in \mathcal{P}_\infty,\ \phi_p \simeq n.\langle 1,-1\rangle_p \end{aligned}$$

Or, $\langle 1,-1\rangle$ est régulière isotrope, ce qui implique d'après le principe de Hasse fort que $\langle 1,-1\rangle_p$ est aussi régulière, isotrope, pour tout $p \in \mathcal{P}_\infty$. D'où, $\langle 1,-1\rangle_p$ est hyperbolique pour tout $p \in \mathcal{P}_\infty$ d'après la caractérisation des plans hyperboliques. Comme $\phi_p \simeq n.\langle 1,-1\rangle_p$, ϕ_p est équivalente à la somme orthogonale de plans hyperboliques et est donc hyperbolique. D'où :

$$\phi \text{ hyperbolique} \implies \forall p \in \mathcal{P}_\infty, \phi_p \text{ est hyperbolique.}$$

Supposons désormais que ϕ n'est pas hyperbolique. Par décomposition de Witt, il existe $n \in \mathbb{N}$ et ϕ_a forme quadratique anisotrope telle que :

$$\phi \simeq n.\langle 1,-1\rangle \perp \phi_a$$

et donc $\phi_p \simeq (n.\langle 1,-1\rangle \perp \phi_a)_p \simeq n.\langle 1,-1\rangle_p \perp (\phi_a)_p$, pour tout $p \in \mathcal{P}_\infty$. Si on suppose que $\forall p \in \mathcal{P}_\infty$, ϕ_p est hyperbolique, il vient :

$$\forall p \in \mathcal{P}_\infty,\ n.\langle 1,-1\rangle_p \perp (\phi_a)_p \text{ hyperbolique}$$

ce qui équivaut à :

$$\forall p \in \mathcal{P}_\infty, (\phi_a)_p \text{ hyperbolique.}$$

Or $(\phi_a)_p$ hyperbolique pour tout $p \in \mathcal{P}_\infty$, implique que $(\phi_a)_p$ est isotrope pour tout $p \in \mathcal{P}_\infty$. Par le principe de Hasse fort, ceci donne ϕ_a isotrope, absurde. D'où,

$$\phi \text{ non hyperbolique} \implies \exists p \in \mathcal{P}_\infty\ \phi_p \text{ non hyperbolique}$$

ce qui montre par contraposée que :

$$\forall p \in \mathcal{P}_\infty, \phi_p \text{ hyperbolique} \implies \phi \text{ hyperbolique.}$$

ce qui achève de montrer que le principe de Hasse fort implique le principe de Hasse faible.

Montrons qu'en dimension 2 et 3, on peut déduire le principe de Hasse fort, du principe de Hasse faible. En dimension 2, une forme quadratique rationnelle régulière est hyperbolique si et seulement si elle est isotrope. Donc, d'après le principe de Hasse faible :

$$\begin{aligned} \phi \text{ est régulière isotrope} &\iff \phi \text{ est hyperbolique} \\ &\iff \forall p \in \mathcal{P}_\infty,\ \phi_p \text{ est hyperbolique} \\ &\iff \forall p \in \mathcal{P}_\infty,\ \phi_p \text{ est régulière isotrope} \end{aligned}$$

et d'où le principe de Hasse fort. En dimension 3, pour ϕ forme quadratique rationnelle régulière, de discriminant δ,

$$\begin{aligned} \phi \text{ est isotrope} &\iff \phi \perp \langle\delta\rangle \text{ est isotrope} \\ &\iff \phi \perp \langle\delta\rangle \text{ est hyperbolique} \\ &\iff \forall p \in \mathcal{P}_\infty,\ (\phi \perp \langle\delta\rangle)_p \text{ est hyperbolique} \\ &\iff \forall p \in \mathcal{P}_\infty,\ \phi_p \perp \langle\delta\rangle_p \text{ est hyperbolique} \\ &\iff \forall p \in \mathcal{P}_\infty,\ \phi_p \perp \langle\delta\rangle_p \text{ est isotrope} \\ &\iff \forall p \in \mathcal{P}_\infty,\ \phi_p \text{ est isotrope} \end{aligned}$$

Les équivalences ci-dessus découlent de l'application de l'astuce de la dimension 4 et de l'application du principe de Hasse faible. Le principe de Hasse fort est donc déduit du principe de Hasse faible en dimension 2 et 3. □

La proposition suivante est une nouvelle illustration du fait que l'on peut obtenir des renseignements sur une forme quadratique rationnelle en étudiant ces localisées associées sur les corps $\mathbb{Q}_p$. Nous appliquerons ensuite cette proposition, pour montrer qu'en dimension 2, une forme quadratique rationnelle ϕ est hyperbolique si et seulement si ces localisées sont hyperboliques, presque pour tout $p \in \mathcal{P}_\infty$.

Théorème 9.2.3. *Soit ϕ et ψ deux formes quadratiques rationnelles régulières. Si pour presque tout p de $\mathcal{P} \cup \{\infty\}$, c'est à dire pour tout p sauf éventuellement un nombre fini, les localisées au voisinage de p, ψ_p et ϕ_p sont équivalentes, alors ϕ et ψ ont même discriminant.*

Pour démontrer ce résultat on va utiliser le lemme suivant :

Lemme 9.2.1. *Soit $a \in \mathbb{Z}^* \backslash \{1\}$ sans facteur multiple, alors il existe une infinité de nombres premiers p tels que a ne soit pas un carré de $\mathbb{F}_p^*$.*

Démonstration. Soit $a \in \mathbb{N}^* \backslash \{1\}$ sans facteurs multiples, il existe alors r nombres premiers distincts tels que $a = \prod_{i=1}^r p_i$. Dans un premier temps, on suppose que 2 ne divise pas a. Alors, dire que a n'est pas un carré de $\mathbb{F}_q^*$, où q est un nombre premier impair, se traduit à l'aide du symbole de Legendre par : $\left(\frac{\prod_{i=1}^r p_i}{q}\right) = -1 \iff \prod_{i=1}^r \left(\frac{p_i}{q}\right) = -1$ par multiplicativité de celui-ci. Les p_i, $i \in [\![1, r]\!]$, étant tous des nombres premiers impairs, par la loi de réciprocité quadratique, il vient :

$$\prod_{i=1}^{r}\left(\frac{p_i}{q}\right)=\prod_{i=1}^{r}\left(\frac{q}{p_i}\right)(-1)^{\left(\frac{p_i-1}{2}\right)\left(\frac{q-1}{2}\right)}$$

Par application de la loi de réciprocité quadratique, le problème qui consistait à trouver q tel que a soit un non carré de $\mathbb{F}_q^*$ se ramène à trouver q tel que q vérifie un certain nombre d'égalités modulo p_i, avec les p_i entièrement détérminés par a. Puisque,

$$\begin{aligned}\left(\frac{a}{q}\right) &= \prod_{i=1}^{r}\left(\frac{q}{p_i}\right)(-1)^{\left(\frac{p_i-1}{2}\right)\left(\frac{q-1}{2}\right)}\\ &= \prod_{i=1}^{r}\left(\frac{q}{p_i}\right)(-1)^{\left(\frac{q-1}{2}\right)\sum_{i=1}^{r}\left(\frac{p_i-1}{2}\right)}\end{aligned}$$

pour $q\equiv 1\,[4]$ il existe $k\in\mathbb{N}^*$ tel que $q-1=4k$ et donc $\dfrac{q-1}{2}\equiv 0\,[2]$, ce qui se traduit dans l'égalité ci dessus par :

$$\begin{aligned}\left(\frac{a}{q}\right) &= \prod_{i=1}^{r}\left(\frac{q}{p_i}\right)(-1)^{\left(\frac{p_i-1}{2}\right)\left(\frac{q-1}{2}\right)}\\ &= \prod_{i=1}^{r}\left(\frac{q}{p_i}\right)\end{aligned}$$

et donc :

$$\left(\frac{a}{q}\right)=-1\iff \prod_{i=1}^{r}\left(\frac{q}{p_i}\right)=-1$$

Pour que q vérifie l'égalité ci dessus il suffit par exemple que q soit un carré modulo tous les p_i sauf un (par exemple p_r) et que q soit congru à 1 modulo 4. Ceci nous pousse alors à chercher s'il n'y aurait pas une infinité de nombres premiers impairs q vérifiant le système de congruence suivant où a_r est tel que $\overline{a_r}$ n'est pas un carré de $\mathbb{F}_{p_r}^*$.

$$(S_1)\begin{cases} q &\equiv 1\,[p_1]\\ q &\equiv 1\,[p_2]\\ q &\equiv 1\,[p_3]\\ q &\equiv 1\,[p_4]\\ \vdots &\\ q &\equiv a_r\,[p_r]\\ q &\equiv 1\,[4]\end{cases}$$

Les p_i étant impairs et deux à deux distincts, par le lemme Chinois, il existe un entier b pour lequel le système ci-dessus est équivalent à la congruence :

$$q\equiv b\,[4\textstyle\prod_{i=1}^{r}p_i]\iff q\equiv b\,[4a].$$

Si on montre que $b\wedge 4\prod_{i=1}^{r}p_i=1$ alors, par le théorème des nombres premiers de Dirichlet, on aura l'existence d'une infinité de nombres premiers q vérifiant $q\equiv b\,[4\prod_{i=1}^{r}p_i]$ et donc vérifiant le système (S1). D'après nos considérations

précédentes, ceci donnera donc une infinité de nombres premiers impairs q tels que $\left(\frac{a}{q}\right) = -1$.

Supposons par l'absurde que $b \wedge 4\prod_{i=1}^{r} p_i \neq 1$, alors b et $4\prod_{i=1}^{r} p_i$ ont un diviseur commun et donc nécessairement 2 où un des nombres premiers p_i divise b. Soit alors q tel que $q \equiv b\,[4\prod_{i=1}^{r} p_i]$ et supposons $p_i \mid b$. Comme $4\prod_{i=1}^{r} p_i \mid q-b$ on a aussi $p_i \mid q-b$, soit $q \equiv b\,[p_i]$. Or, $p_i \mid b$ et donc $b \equiv 0\,[p_i]$, absurde. En effet, on aurait sinon $q \equiv 0\,[p_i]$ ce qui est contraire au fait que par le lemme chinois q vérifie le système (S1) et donc $q \equiv 1\,[p_i]$ si $i \neq r$ et $q \equiv a_r\,[p_r]$, où a_r non nul modulo p_r. De même si $q \equiv b\,[4\prod_{i=1}^{r} p_i]$, ceci implique en particulier $q \equiv b\,[2]$. Si on suppose $2 \mid b$, alors $b \equiv 0\,[2]$, absurde car alors on aurait $q \equiv 0\,[2]$ et donc $q \not\equiv 1\,[4]$. Ceci termine l'étude du cas où $a > 0$ est sans facteur multiple, non divisible par 2.

Supposons désormais a est sans facteur mutltiple et divisible par 2. Alors a s'écrit $2\prod_{i=1}^{r} p_i$ où $r \in \mathbb{N}^*$ et les p_i sont des nombres premiers impairs, deux à deux distincts. On cherche q nombre premier impair tel que :

$$\begin{aligned}
\left(\frac{a}{q}\right) = & \quad \left(\frac{2}{q}\right)\prod_{i=1}^{r}\left(\frac{p_i}{q}\right) = -1 \\
= & \quad \left(\frac{2}{q}\right)\prod_{i=1}^{r}\left(\frac{q}{p_i}\right)(-1)^{\left(\frac{p_i-1}{2}\right)\left(\frac{q-1}{2}\right)} = -1 \\
= & \quad \left(\frac{2}{q}\right)\prod_{i=1}^{r}\left(\frac{q}{p_i}\right)(-1)^{\left(\frac{q-1}{2}\right)\sum_{i=1}^{r}\left(\frac{p_i-1}{2}\right)} = -1 \\
= & \quad (-1)^{\frac{q^2-1}{8}}\prod_{i=1}^{r}\left(\frac{q}{p_i}\right)(-1)^{\left(\frac{q-1}{2}\right)\sum_{i=1}^{r}\left(\frac{p_i-1}{2}\right)} = -1
\end{aligned}$$

Prenons alors q tel que $q \equiv 1\,[8]$, alors on a : $\frac{q^2-1}{8} \equiv 0\,[8]$ et $\frac{q-1}{2} \equiv 0\,[4]$ et :

$$\left(\frac{a}{q}\right) = -1 \iff \prod_{i=1}^{r}\left(\frac{q}{p_i}\right) = -1$$

Alors comme précédemment, on voit que, pour que q vérifie l'égalité ci dessus, il suffit qu'il vérifie le système de congruence suivant où a_r est tel que $\overline{a_r}$ n'est pas un carré de $\mathbb{F}_{p_r}^*$:

$$(S_2)\begin{cases} q & \equiv 1\,[p_1] \\ q & \equiv 1\,[p_2] \\ q & \equiv 1\,[p_3] \\ q & \equiv 1\,[p_4] \\ \vdots & \\ q & \equiv a_r\,[p_r] \\ q & \equiv 1\,[8] \end{cases}$$

Comme précédemment, les p_i étant impairs et deux à deux distincts, par le lemme Chinois, il existe un entier b tel que le système ci-dessus soit équivalent à la congruence : $q \equiv b\,[8\prod_{i=1}^{r} p_i]$. Si on montre que $b \wedge 8\prod_{i=1}^{r} p_i = 1$ alors, par le théorème des nombres premiers de Dirichlet, on aura l'existence d'une infinité de nombres premiers q vérifiant $q \equiv b\,[8\prod_{i=1}^{r} p_i]$ et donc vérifiant le système (S2). Supposons par l'absurde que $b \wedge 8\prod_{i=1}^{r} p_i \neq 1$, alors b et $8\prod_{i=1}^{r} p_i$ ont un diviseur commun et donc nécessairement 2 ou un des nombres premiers p_i divise b et on montre exactement comme précédemment que ceci est absurde. Ceci termine le cas où $a > 0$ est sans facteur multiple, divisible par 2. Le cas où $a < 0$ sans facteur multiple se montre de manière tout à fait similaire, ce qui achève la demonstration du lemme. □

Passons à la démonstration du théorème.

Démonstration. On va montrer le résultat par contraposée. Supposons ϕ et ψ deux formes quadratiques rationnelles régulières, telles que :

$$\Delta(\phi) \neq \Delta(\psi).$$

On va alors prouver qu'il existe une infinité de $p \in \mathcal{P}_\infty$ tels que :

$$\phi_p \ncong \psi_p$$

Si $dim(\phi) \neq dim(\psi)$, alors nécessairement $\phi_p \ncong \psi_p, \forall p \in \mathcal{P}_\infty$ car $\mathbb{Q} \subset \mathbb{Q}_p$ car deux formes quadratiques de dimension différente ne peuvent pas être équivalentes (ϕ,ψ ont même dimension que leurs localisées au voisinage de p). Si $dim(\phi) = dim(\psi)$ alors, comme $\Delta(\phi) \neq \Delta(\psi)$, on a $det(\phi) \neq det(\psi)$ dans $\mathbb{Q}^*/(\mathbb{Q}^*)^2$, soit en multipliant à gauche et à droite par $det(\psi)$,

$$det(\phi)det(\psi) \neq det(\psi)^2 \text{ et donc } det(\phi)det(\psi) \neq 1$$

dans $\mathbb{Q}^*/(\mathbb{Q}^*)^2$.

Si $dim(\phi) \neq dim(\psi)$, on a déjà le résultat souhaité, donc on suppose :

$$\Delta(\phi) \neq \Delta(\psi) \text{ avec } dim(\phi) = dim(\psi)$$

soit en particulier, $det(\phi)det(\psi) \neq 1$ dans $\mathbb{Q}^*/(\mathbb{Q}^*)^2$. On choisit alors un représentant de la classe de $det(\phi)det(\psi)$ dans $\mathbb{Q}^*/(\mathbb{Q}^*)^2$, que l'on peut écrire sous la forme $a = \pm\prod_{i=1}^{r} p_i$ où les p_i sont des nombres premiers deux à deux distincts. D'après le lemme 9.2.1, il existe une infinité de nombres premiers impairs tels que a ne soit pas un carré de $\mathbb{F}_q^*$. Considérons donc q un nombre premier impair, premier avec a et tel que a ne soit pas un carré de $\mathbb{F}_q^*$. On va montrer alors que :

$$\phi_q \ncong \psi_q$$

D'après l'étude des carrés du corps $\mathbb{Q}_q$, (q premier impair), on sait que :

$$a = \pm\prod_{i=1}^{r} p_i \in \mathbb{Q} \subset \mathbb{Q}_q \text{ est un carré de } \mathbb{Q}_q$$

si et seulement si $a = 1$ dans $\mathbb{Q}_q^*/(\mathbb{Q}_q^*)^2$, ce qui équivaut encore à ce que :

$$v_q(a) \equiv v_q(1)\,[2]$$

que le premier chiffre des développements q-adique de a et 1 aient la même classe dans $\mathbb{F}_q^*/(\mathbb{F}_q^*)^2$. Or 1 et a sont des unités q-adique car $1, a \in \mathbb{Z}$ et $q \nmid 1$,$q \nmid a$ ce qui donne que :

$$v_q(a) = v_q(b) = 0.$$

En revanche, $\left(\frac{a}{q}\right) = -1$ montre que a n'est pas un carré de $\mathbb{F}_q^*$, contrairement à 1 et donc $1 \neq a$ dans $\mathbb{F}_q^*/(\mathbb{F}_q^*)^2$, d'où au final a n'est pas un carré dans $\mathbb{Q}_q^*$. Or,

$$det(\phi)det(\psi) = det(\phi_q)det(\psi_q) \text{ dans } \mathbb{Q}_q^*/(\mathbb{Q}_q^*)^2$$

(ϕ et ϕ_p sont représentées par les mêmes matrices et ont donc même déterminant, cf. proposition 7.3.1) et comme a n'est pas un carré dans $\mathbb{Q}_q^*$, en termes de localisées au voisinage de q, ceci implique que :

$$\begin{aligned} & det(\phi)det(\psi) \neq 1 \text{ dans } \mathbb{Q}_q^*/(\mathbb{Q}_q^*)^2 \\ \Longrightarrow \quad & det(\phi_q)det(\psi_q) \neq 1 \text{ dans } \mathbb{Q}_q^*/(\mathbb{Q}_q^*)^2 \\ \Longrightarrow \quad & det(\phi_q) \neq det(\psi_q) \text{ dans } \mathbb{Q}_q^*/(\mathbb{Q}_q^*)^2 \\ \Longrightarrow \quad & \phi_q \not\simeq \psi_q \end{aligned}$$

Or, il y a une infinité de q tels que $q \in \mathcal{P}\backslash\{2\}, a \wedge q = 1$ et $\left(\frac{a}{q}\right) = -1$ d'après le lemme 9.2.1, soit donc une infinité de $q \in \mathcal{P} \cup \{\infty\}$ tels que $\phi_q \not\simeq \psi_q$, ce qui donne le résultat par contraposée. □

Corollaire 9.2.2. *Soit ϕ une forme quadratique rationnelle régulière de dimension 2. Si pour presque tout $p \in \mathcal{P} \cup \{\infty\}$, ϕ_p est hyperbolique alors ϕ est hyperbolique.*

Démonstration. Soit ϕ une forme quadratique rationnelle régulière de dimension 2, alors ϕ est hyperbolique si et seulement si $\Delta(\phi) = 1$ dans $\mathbb{Q}^*/(\mathbb{Q}^*)^2$. Dire que pour presque tout $p \in \mathcal{P} \cup \{\infty\}$, ϕ_p est hyperbolique est alors équivalent à dire pour presque tout $p \in \mathcal{P} \cup \{\infty\}$, $\phi_p \simeq \langle 1, -1\rangle_p$. D'après le théorème, ϕ et $\langle 1, -1\rangle$ ont alors même discriminant c'est à dire $\Delta(\phi) = 1$ dans $\mathbb{Q}^*/(\mathbb{Q}^*)^2$, ce qui comme ϕ est de dimension 2 suffit pour dire que ϕ est hyperbolique. □

Remarque 9.2.3. *Par le principe de Hasse faible, ϕ forme quadratique rationnelle régulière est hyperbolique si et seulement les localisées au voisinage de p, ϕ_p sont hyperboliques pour tout $p \in \mathcal{P}_\infty$. Ainsi, en dimension 2, pour montrer que ϕ est hyperbolique, il suffit par le corollaire précédent, de montrer que ϕ_p est hyperbolique pour presque tout p, ce qui prouve alors en fait que ϕ_p est hyperbolique pour tout p.*

9.3 Formes quadratiques sur $\mathbb{Q}_p$, $p \in \mathcal{P}\backslash\{2\}$

9.3.1 Etude des groupes $W(\mathbb{Q}_p)$ et $\widehat{W}(\mathbb{Q}_p)$, $p \in \mathcal{P}\backslash\{2\}$

Le théorème suivant, va nous permettre d'exhiber la structure du groupe de Witt $W(\mathbb{Q}_p)$, puis de son groupe de Witt-Grothendicek $\widehat{W}(\mathbb{Q}_p)$.

Théorème 9.3.1. *Soit p un nombre premier impair. Le morphisme :*

$$\alpha\colon \begin{cases} W(\mathbb{Q}_p) \longrightarrow W(\mathbb{F}_p) \times W(\mathbb{F}_p) \\ [\psi]_W \longmapsto (\partial'_p([p\psi]_W), \partial'_p([\psi]_W)) \end{cases}$$

est un isomorphisme de groupes.

Démonstration. L'application α est clairement un morphisme de groupe, puisque ∂'_p est on l'a vu un morphisme, tout comme l'application $[\psi]_W \longrightarrow [p\psi]_W$ où $p\psi : x \longrightarrow p\psi(x)$ (il suffit de montrer que $\psi \longrightarrow [p\psi]_W$ vérifie les hypothèses de la seconde propriété universelle, cf proposition 6.5.2). On va chercher à définir la réciproque de α ce qui montrera sa bijectivité et l'isomorphisme annoncé. Soit β définie par :

$$\beta\colon \begin{cases} \mathbb{F}_p^* \longrightarrow W(\mathbb{Q}_p) \\ \overline{k} \longmapsto < k > \end{cases}$$

D'abord, on doit montrer que β est bien définie, c'est-à-dire ne dépend pas du choix du représentant de la classe $\overline{k}$. En effet, soit r le reste dans la division euclidienne de k par p. On a $k = pq + r$ et via l'écriture p-adique des entiers, il vient :

$$k = r + p(a_0 + a_1 p + a_2 p^2 + \ldots)$$

Alors, $r \in [\![1, p-1]\!]$ puisque k non divisible par p, ce qui implique que k et r ont même valuation p-adique, qui est nulle. Comme $\overline{k} = \overline{r}$, k et r ont même classe modulo $(\mathbb{F}_p^*)^2$ et d'après la proposition 9.1.2, sont égaux modulo $(\mathbb{Q}_p^*)^2$. Ainsi, $\beta(\overline{k}) =< k >=< r >= \beta(\overline{r})$ et β est bien définie.

On doit maintenant vérifier les hypothèses de la proposition 6.5.4, pour étendre la définition de β à $W(\mathbb{Q}_p)$. D'après la proposition 6.5.2, β vérifie clairement ces hypothèses, et donc β induit un morphisme de $\overline{\beta} : W(\mathbb{Q}_p) \longrightarrow W(\mathbb{F}_p)$ tel que :

$$\forall k \in \mathbb{Z},\ \overline{\beta}(< \overline{k} >) =< k >\in W(\mathbb{F}_p).$$

On peut définir également à partir de $\overline{\beta}$ le morphisme :

$$\delta\colon \begin{cases} W(\mathbb{F}_p) \times W(\mathbb{F}_p) \longrightarrow W(\mathbb{Q}_p) \\ ([\phi]_W, [\psi]_W) \longmapsto \overline{\beta}([\phi]_W) + \overline{\beta}([p\psi]_W) \end{cases}$$

Ainsi, pour $(a_1, \ldots, a_m, b_1, \ldots, b_n)$ des entiers premiers avec p, on a :

$$\delta(< \overline{a_1}, \ldots, \overline{a_m} >, < \overline{b_1}, \ldots, \overline{b_n} >) =< a_1, \ldots, a_m > + < pb_1, \ldots, pb_n >$$

On a alors, si $p \wedge k = 1$,

$$(\delta \circ \alpha)(< k >) = \delta((\partial'_p(< pk >), \partial'_p(< k >)) = \delta(< \overline{k} >, < 0 >) =< k >$$

et

$$\begin{aligned} (\delta \circ \alpha)(< pk >) = &\quad \delta(\partial'_p(< p^2 k >), \partial'_p(< pk >)) \\ = &\quad \delta(\partial'_p(< k >), \partial'_p(< pk >)) \\ = &\quad \delta(< 0 >, < \overline{k} >) =< pk > \end{aligned}$$

Ainsi, $\delta \circ \alpha = Id_{W(\mathbb{Q}_p)}$, car $\delta \circ \alpha = Id$ sur une partie génératrice de $W(\mathbb{Q}_p)$, cf corollaire 9.1.1. Tout élément de $W(\mathbb{F}_p)$ pouvant s'écrire $< \overline{a_1}, \ldots, \overline{a_m} >$ où les a_i sont premiers à p, (si par exemple $\overline{a_1} = 0$ alors, $< \overline{a_1}, \ldots, \overline{a_m} >=< \overline{a_2}, \ldots, \overline{a_m} >$ et on peut opérer ainsi jusqu'à obtentir aucun terme nul), on a :

$$\begin{aligned} \alpha \circ \delta(< \overline{a_1}, \ldots, \overline{a_m} >, < \overline{b_1}, \ldots, \overline{b_n} >) = &\quad \alpha(< a_1, \ldots, a_m > + < pb_1, \ldots, pb_n >) \\ = &\quad \alpha(< a_1, \ldots, a_m, pb_1, \ldots, pb_n >) \\ = &\quad (< \overline{a_1}, \ldots, \overline{a_m} >, < \overline{b_1}, \ldots, \overline{b_n} >) \end{aligned}$$

Ce qui prouve que $\alpha \circ \delta = Id_{W(\mathbb{F}_p)\times W(\mathbb{F}_p)}$ et achève de montrer le théorème. □

Du théorème précédent et de la structure des groupes de Witt et Witt-Grothendieck sur les corps finis, on déduit :

Théorème 9.3.2. ***Structure du groupe de Witt*** $W(\mathbb{Q}_p)$ ***et du groupe de Witt-Grothendieck*** $\widehat{W}(\mathbb{Q}_p)$
Soit p un nombre premier impair.

1. *Si $p \equiv 1\,[4]$, alors $W(\mathbb{Q}_p) \simeq (\mathbb{Z}/2)^4$ et $\widehat{W}(\mathbb{Q}_p) \simeq \mathbb{Z} \times (\mathbb{Z}/2)^3$*
2. *Si $p \equiv 3\,[4]$, alors $W(\mathbb{Q}_p) \simeq (\mathbb{Z}/4)^2$ et $\widehat{W}(\mathbb{Q}_p) \simeq \mathbb{Z} \times \mathbb{Z}/2 \times \mathbb{Z}/4$*

Démonstration. La structure de $W(\mathbb{Q}_p)$ est obtenue immédiatement en utilisant les isomosphismes déjà établis :

- $W(\mathbb{Q}_p) \simeq W(\mathbb{F}_p) \times W(\mathbb{F}_p)$
- $W(\mathbb{F}_p) \simeq \mathbb{Z}/2 \times \mathbb{Z}/2$ si $p \equiv 1\,[4]$
- $W(\mathbb{F}_p) \simeq \mathbb{Z}/4$ si $p \equiv 3\,[4]$

Pour établir la structure de $\widehat{W}(\mathbb{Q}_p)$, on utilise l'isomorphisme :

$$\widehat{W}(\mathbb{Q}_p) \simeq \mathbb{Z} \times I(\mathbb{Q}_p)$$

où $I(\mathbb{Q}_p)$ est d'indice 2 dans $W(\mathbb{Q}_p)$ dont nous venons juste d'établir sa structure. Puisque, $W(\mathbb{Q}_p)$ est isomorphe à $(\mathbb{Z}/2)^4$ ou $(\mathbb{Z}/4)^2$, il s'agit d'un groupe abélien d'ordre 16 et $I(\mathbb{Q}_p)$ est alors nécessairement un groupe abélien d'ordre 8. Par le théorème de structure des groupes abéliens finis, $I(\mathbb{Q}_p)$ est isomorphe à $\mathbb{Z}/8$, $(\mathbb{Z}/2)^3$ ou $\mathbb{Z}/2 \times \mathbb{Z}/4$.

Suppons $p \equiv 1\,[4]$, alors $W(\mathbb{Q}_p) \simeq (\mathbb{Z}/2)^4$ et donc $W(\mathbb{Q}_p)$ n'a que des éléments d'ordre 2 (hormis l'élément neutre). Ansi $I(\mathbb{Q}_p)$ n'a que des éléments d'ordre 2 et nécessairement $I(\mathbb{Q}_p) \simeq (\mathbb{Z}/2)^3$. Soit finalement :

$$\widehat{W}(\mathbb{Q}_p) \simeq \mathbb{Z} \times (\mathbb{Z}/2)^3$$

Supposons $p \equiv 3\,[4]$, alors $W(\mathbb{Q}_p) \simeq (\mathbb{Z}/4)^2$ est un groupe d'ordre 16 composé de 3 éléments d'ordre 2, 12 d'ordre 4 et 1 d'ordre 1. Ainsi un sous-groupe de $(\mathbb{Z}/4)^2$ ne peut pas être isomorphe à $\mathbb{Z}/8$ qui contient des éléments d'ordre 8 et ne peut pas non plus être isomorphe à $(\mathbb{Z}/2)^3$ qui contient 7 éléments d'ordre 2. D'où $I(\mathbb{Q}_p) \simeq \mathbb{Z}/2 \times \mathbb{Z}/4$ et donc :

$$\widehat{W}(\mathbb{Q}_p) \simeq \mathbb{Z} \times \mathbb{Z}/2 \times \mathbb{Z}/4$$

□

Pour terminer, cette section, nous allons donner la structure des formes quadratiques anisotropes sur $\mathbb{Q}_p$, pour p premier impair :

Théorème 9.3.3. ***Formes quadratiques anisotropes sur*** $\mathbb{Q}_p$

1. *Etant donné deux familles $(a_1, \ldots, a_m)$ et $(b_1, \ldots, b_n)$ d'entiers premiers avec p, la forme quadratique $\langle a_1, \ldots, a_m, pb_1, \ldots, pb_n\rangle$ sur $\mathbb{Q}_p$ est anisotrope si et seulement si les formes quadratiques $\langle \overline{a_1}, \ldots, \overline{a_m}\rangle$ et $\langle \overline{b_1}, \ldots, \overline{b_n}\rangle$ sont anisotropes sur $\mathbb{F}_p$.*
2. *Il existe à isomorphisme près, une unique forme quadratique anisotrope de dimension 4 sur $\mathbb{Q}_p$ qui est $\langle 1, p, -\varepsilon, -p\varepsilon\rangle$*

3. *Toute forme quadratique sur $\mathbb{Q}_p$ de dimension supérieure ou égale à 5 est isotrope.*

On peut généraliser cette proposition de la façon suivante :

Proposition 9.3.1. *Soit $\mathbb{K}$ un corps de caractéristique différente de 2. On suppose qu'à isomorphisme près, $\langle a,b,c,d\rangle$ est la seule forme quadratique anisotrope de dimension 4, alors :*

1. *$\langle a,b,c,d\rangle$ est universelle.*
2. *$\langle a,b,c,d\rangle$ est de déterminant 1 dans $\mathbb{K}^*/(\mathbb{K}^*)^2$*
3. *Toute forme quadratique de dimension au moins 5 est isotrope.*
4. *Toute forme quadratique de dimension 3 sur $\mathbb{K}$ est équivalente à une restriction de $\langle a,b,c,d\rangle$.*
5. *l'application*
$$\Phi\colon \begin{cases} W(\mathbb{K}) \longrightarrow W(\mathbb{K}) \\ < x > \longmapsto < a,b,c,d > + < x > \end{cases}$$
est une bijection de l'ensemble des classes de Witt-équivalence de formes quadratiques anisotropes de dimension 1 sur l'ensemble des classes de Witt-équivalence de formes quadratiques anisotropes de dimension 3.

Démonstration.

1. $\forall \lambda \in \mathbb{K}^*, \langle \lambda a, \lambda b, \lambda c, \lambda d\rangle$ est anisotrope de dimension 4. En effet, sinon il existerait $(x_1,x_2,x_3,x_4) \neq 0$ dans $\mathbb{K}^4$ tel que :
$$\lambda a x_1^2 + \lambda b x_2^2 + \lambda c x_3^2 + \lambda d x_4^2 = 0$$
et puisque $\lambda \in \mathbb{K}^*$, on aurait $ax_1^2 + bx_2^2 + cx_3^2 + dx_4^2 = 0$ et donc $\langle a,b,c,d\rangle$ serait isotrope, absurde. D'où pour tout λ de $\mathbb{K}^*$, $\langle \lambda a, \lambda b, \lambda c, \lambda d\rangle$ est anisotrope et donc équivalente à $\langle a,b,c,d\rangle$, puisque par hypothèse, il n'y a qu'une seule forme quadratique anisotrope de dimension 4. Ainsi $\langle a,b,c,d\rangle$ et $\langle \lambda a, \lambda b, \lambda c, \lambda d\rangle$ ont même domaine, $\forall \lambda \in \mathbb{K}^*$. Puisque $\langle a,b,c,d\rangle \neq 0$, il existe au moins $x \in \mathbb{K}^*$ tel que $\langle a,b,c,d\rangle$ représente x et donc pour $\lambda = x^{-1}$, $\langle \lambda a, \lambda b, \lambda c, \lambda d\rangle$ représente $xx^{-1} = 1$. D'où $\langle a,b,c,d\rangle$ représente 1 et $\langle \lambda a, \lambda b, \lambda c, \lambda d\rangle$ représente λ. Ainsi $\langle a,b,c,d\rangle$ représente chaque λ de $\mathbb{K}^*$ et est donc universelle.
2. Puisque $\langle a,b,c,d\rangle$ est anisotrope, elle est non dégénérée et donc régulière. On a de plus $det(\langle a,b,c,d\rangle) = abcd$ dans $\mathbb{K}^*/(\mathbb{K}^*)^2$. Alors, l'anisotropie de $\langle a,b,c,d\rangle$ implique celle de $\langle a,b,c\rangle$, car sinon $\langle a,b,c\rangle$ admettrait un vecteur isotrope non nul (x_1,x_2,x_3) et $(x_1,x_2,x_3,0)$ serait un vecteur isotrope non nul de $\langle a,b,c,d\rangle$, absurde. Par l'astuce de la dimension 4, comme $\langle a,b,c\rangle$ est anisotrope, $\langle a,b,c,abc\rangle$ de dimension 4 l'est aussi et est donc équivalente à $\langle a,b,c,d\rangle$. D'où l'égalité des déterminants dans $\mathbb{K}^*/(\mathbb{K}^*)^2$ et donc $abcd = (abc)^2 = 1$, soit finalement $det(\langle a,b,c,d\rangle) = 1$.
3. On souhaite montrer que toute forme quadratique de dimension au moins 5 est isotrope. D'abord il est clair que toute forme quadratique non régulière de dimension 5 est isotrope, car anisotrope $\Longrightarrow$ régulière et donc non régulière $\Longrightarrow$ isotrope par contraposée. Il s'agit donc de montrer que les formes quadratiques de dimension au moins 5, régulières sont isotropes. Pour ce faire, il suffit de montrer que les formes quadratiques de

dimension 5, régulières sont isotropes. Par l'absurde, soit ϕ une forme quadratique de dimension 5 et anisotrope (donc régulière). Il existe des éléments a_i, $i \in [\![1,5]\!]$ tous non nuls, tels que $\phi \simeq \langle a_1, a_2, a_3, a_4, a_5\rangle$ et $\langle a_1, a_2, a_3, a_4, a_5\rangle$ anisotrope. Ainsi, $\langle a_1, a_2, a_3, a_4\rangle$ est aussi anisotrope sinon il existerait (x_1, x_2, x_3, x_4) non nul vecteur isotrope de $\langle a_1, a_2, a_3, a_4\rangle$ et $(x_1, x_2, x_3, x_4, 0)$ serait un vecteur isotrope de $\langle a_1, a_2, a_3, a_4, a_5\rangle$, absurde. D'où, $\langle a_1, a_2, a_3, a_4\rangle$, de dimension 4 et équivalente à $\langle a, b, c, d\rangle$. Alors, $\langle a, b, c, d\rangle$ étant universelle d'après 1), il vient que $-a_5$ est représenté par $\langle a, b, c, d\rangle$ et donc par $\langle a_1, a_2, a_3, a_4\rangle$ qui lui est équivalente. D'où, $\langle a_1, a_2, a_3, a_4\rangle \perp \langle -(-a_5)\rangle$ est isotrope d'après le principe de représentation et donc $\langle a_1, a_2, a_3, a_4, a_5\rangle$ est isotrope, ce qui est absurde. D'où nécessairement toute forme quadratique de dimension 5 est isotrope et donc toute forme ψ de dimension $n > 5$ également. En effet, par diagonalisation on a $\psi \simeq \langle a_1, a_2, \cdots, a_n\rangle$ et $\langle a_1, a_2, a_3, a_4, a_5\rangle$ étant isotrope il existe $(x_1, x_2, x_3, x_4, x_5)$ non nul, qui l'annule et $(x_1, x_2, x_3, x_4, x_5, 0, \cdots, 0)$ également non nul, annule $\langle a_1, a_2, \cdots, a_n\rangle$. Donc $\langle a_1, a_2, \cdots, a_n\rangle$ est isotrope tout comme ψ qui lui est équivalente.

4. Soit ψ une forme quadratique de dimension 3 sur $\mathbb{K}$ anisotrope. Par diagonalisation, il existe $a_1, a_2, a_3 \in \mathbb{K}^*$ tel que $\psi \simeq \langle a_1, a_2, a_3\rangle$ et par l'astuce de la dimension 4, $\langle a_1, a_2, a_3, a_1a_2a_3\rangle$ est anisotrope et donc équivalente à $\langle a, b, c, d\rangle$. Comme $h = \langle a, b, c, d\rangle$ et $g = \langle a_1, a_2, a_3, a_1a_2a_3\rangle$ sont équivalentes il existe un isomorphisme d'espace vectoriel $u : \mathbb{K}^4 \longrightarrow \mathbb{K}^4$ tel que :
$$\forall (x_1, x_2, x_3, x_4) \in \mathbb{K}^4,\ h(u((x_1, x_2, x_3, x_4))) = g((x_1, x_2, x_3, x_4))$$
Ainsi, la restriction de u à $\mathbb{K}^3 \times \{0\}$, $u_{\mathbb{K}^3\times\{0\}} : \mathbb{K}^3 \times \{0\} \longrightarrow u(\mathbb{K}^3 \times \{0\})$ est telle que $\forall (x_1, x_2, x_3, 0) \in \mathbb{K}^3 \times \{0\}$, on a :
$$h(u((x_1, x_2, x_3, 0)) = g((x_1, x_2, x_3, 0)) = \langle a_1, a_2, a_3\rangle(x_1, x_2, x_3).$$
Ceci montre bien que $\langle a_1, a_2, a_3\rangle$ est équivalente à une restriction de h tout comme ψ qui lui est équivalente.

5. Etudions l'application $\Phi :< x > \longrightarrow < a, b, c, d > + < x >$. Supposons que $x \neq y \in \mathbb{K}^*/(\mathbb{K}^*)^2$ alors naturellement :
$$< x > \neq < y > \Longleftrightarrow x \neq y \in \mathbb{K}^*/(\mathbb{K}^*)^2$$
Si $< x > \neq < y >$ alors $< a, b, c, d > + < x > \neq < a, b, c, d > + < y >$ dans le groupe $W(\mathbb{K})$, d'où l'injectivité.
Montrons la surjectivité de Φ. Supposons ϕ, anisotrope de dimension 3, alors par diagonalisation $\phi \simeq \langle a_1, a_2, a_3\rangle$ et par l'astuce de la dimension 4, $\langle a_1, a_2, a_3, a_1a_2a_3\rangle$ est anisotrope. $\langle a_1, a_2, a_3, a_1a_2a_3\rangle$ et $\langle a, b, c, d\rangle$ sont équivalentes, donc Witt-équivalentes. Soit dans $W(\mathbb{K})$:
$$\begin{aligned}
& < a_1, a_2, a_3, a_1a_2a_3 > = < a, b, c, d > \\
\Longleftrightarrow \quad & < a_1, a_2, a_3 > + < a_1a_2a_3 > = < a, b, c, d > \\
\Longleftrightarrow \quad & < a_1, a_2, a_3 > = < a, b, c, d > + < -a_1a_2a_3 > \\
\Longleftrightarrow \quad & [\phi]_W = < a, b, c, d > + < -a_1a_2a_3 > \\
\Longleftrightarrow \quad & \Phi(< -a_1a_2a_3 >) = [\phi]_W
\end{aligned}$$
Ce qui montre bien que la classe de Witt équivalence d'une forme quadratique anisotrope de dimension 3 s'écrit sous la forme $< a, b, c, d > + < x >$, d'où la surjectivité.

Pour conclure il reste à montrer que pour $x \neq 0$,

$$< a, b, c, d > + < x >=< a, b, c, d, x >$$

représente une classe de Witt-équivalence d'une forme quadratique anisotrope de dimension 3, c'est à dire peut s'écrire $[\phi]_W$, pour ϕ anisotrope de dimension 3. Pour $x \neq 0$, $\langle a, b, c, d, x\rangle$, de dimension 5 est isotrope d'après 3), son indice est donc 1 ou 2. Montrons que son indice est 1, alors on aura par décomposition de Witt :

$$\langle a, b, c, d, x\rangle \simeq \langle 1, -1\rangle \perp \psi$$

pour ψ anisotrope de dimension 3 et donc $< a, b, c, d, x >= [\psi]_W$.
Supposons par l'absurde que l'indice soit égal à 2. D'après la définition de l'indice, il existe alors un sous espace vectoriel E de $\mathbb{K}^5$ de dimension 2 totalement isotrope. Par la formule de Grassmann l'hyperplan H de $\mathbb{K}^5$ d'équation $x_5 = 0$ intersecte alors E non trivialement. En effet, si $dim(E \cap H) = 0$ comme $dim(E + H) = dim(E) + dim(H) - dim(E \cap H)$ alors,

$$dim(E + H) = 2 + 4 > dim(\mathbb{K}^5) = 5,$$

absurde. Il existe donc $(\alpha, \beta, \gamma, \delta, 0) \in E \cap H$ non nul et E étant totalement isotrope, $(\alpha, \beta, \gamma, \delta, 0)$ annule $\langle a, b, c, d, x\rangle$ soit :

$$(\alpha, \beta, \gamma, \delta) \text{ annule } \langle a, b, c, d\rangle$$

avec $\langle a, b, c, d\rangle$ anisotrope, absurde. L'indice est donc 1, ce qui achève de montrer 5).

□

9.4 Formes quadratiques sur $\mathbb{Q}_2$

Avant d'étudier la structure des groupes de Witt et Witt-Grothendieck associés au corps $\mathbb{Q}_2$, présentons sans démonstration le théorème de structure des formes quadratiques anisotropes sur $\mathbb{Q}_2$.

Théorème 9.4.1.

1. *Les formes quadratiques anisotropes de dimension* 3 *sur* $\mathbb{Q}_2$ *sont celles équivalentes à* $\langle \lambda, \lambda, \lambda\rangle$, *pour* $\lambda \in \mathbb{Q}_2^*$.
2. *La forme quadratique* $\langle 1, 1, 1, 1\rangle$ *est, à équivalence près, l'unique forme quadratique anisotrope de dimension* 4 *sur* $\mathbb{Q}_2$
3. $\langle 1, 1, 1, 1\rangle$ *est universelle et de déterminant* 1.
4. *Toute forme quadratique de dimension au moins* 5 *sur* $\mathbb{Q}_2$ *est isotrope.*

Remarque 9.4.1. *Les points* 3 *et* 4 *sont sans surprise, d'après la proposition* 59.

Toute forme quadratique de dimension au moins 5 est donc isotrope sur $\mathbb{Q}_p$ et ce pour tout $p \in \mathcal{P}$. Une forme quadratique réelle indéfinie étant isotrope, on a par le principe de Hasse fort :

Corollaire 9.4.1. *Toute forme quadratique rationnelle régulière indéfinie, de dimension au moins* 5 *est isotrope.*

9.4.1 Etude des groupes $W(\mathbb{Q}_2)$ et $\widehat{W}(\mathbb{Q}_2)$

Théorème 9.4.2. Structure du groupe de Witt $W(\mathbb{Q}_2)$ et du groupe de Witt-Grothendieck $\widehat{W}(\mathbb{Q}_2)$.

1. $W(\mathbb{Q}_2) \simeq \mathbb{Z}/8 \times \mathbb{Z}/2 \times \mathbb{Z}/2$
2. $\widehat{W}(\mathbb{Q}_2) \simeq \mathbb{Z} \times \mathbb{Z}/4 \times (\mathbb{Z}/2)^2$

Démonstration. On commence par définir une fonction Φ par :

$$\Phi\colon \begin{cases} \mathbb{Z}/8 \times \mathbb{Z}/2 \times \mathbb{Z}/2 \longrightarrow W(\mathbb{Q}_2) \\ (\overline{a}, \overline{b}, \overline{c}) \longmapsto a.< 1 > + b.< 1,3 > + c.< 1,6 > \end{cases}$$

Il s'agit alors de montrer que Φ est bien définie puis que c'est un isomorphisme de groupes. Ceci prouvera la première assertion, quant à la seconde il s'agira d'utiliser l'isomorphisme entre $\widehat{W}(\mathbb{Q}_2)$ et $\mathbb{Z} \times I(\mathbb{Q}_2)$ où $I(\mathbb{Q}_2)$ est d'indice 2 dans $W(\mathbb{Q}_2)$. Il suffira alors d'identifier $I(\mathbb{Q}_2)$ avec le sous-groupe d'indice 2 adéquat de $\mathbb{Z}/8 \times \mathbb{Z}/2 \times \mathbb{Z}/2$ pour pouvoir conclure.
Etape 1 : Φ est bien définie.
Dire que Φ est bien définie, c'est dire que Φ ne dépend pas du choix des représentants des classes d'entiers modulo 2 et 8. Pour ce faire on va prouver que les formes diagonales $8.\langle 1\rangle$, $2.\langle 1,3\rangle$ et $2.\langle 1,6\rangle$ sont hyperboliques sur $\mathbb{Q}_2$ et donc de classes de Witt-équivalence associées nulles. Ceci prouvera bien que pour $(\overline{a_1}, \overline{b_1}, \overline{c_1}) = (\overline{a_2}, \overline{b_2}, \overline{c_2})$ on a :

$$\phi(\overline{a_1}, \overline{b_1}, \overline{c_1}) = \Phi(\overline{a_2}, \overline{b_2}, \overline{c_2})$$

Etudions alors la forme diagonale $2.\langle 1,3\rangle \simeq \langle 1,1,3,3\rangle$. Elle est régulière de dimensions 4 et de déterminant 1 modulo les carrés de $\mathbb{Q}_2^*$ (9 est un carré de $\mathbb{Q}$ donc de $\mathbb{Q}_2$) et donc $\langle 1,1,3,3\rangle$ est soit anisotrope, soit hyperbolique (cf. théorème 3.2.5). On a les équivalences suivantes :

$$\begin{aligned} & \langle 1,1,3,3\rangle \text{ est isotrope} \\ \iff\ & \langle 1,1,3\rangle \text{ est isotrope d'après l'astuce de la dimension 4} \\ \iff\ & -3 = 5 \text{ dans } \mathbb{Q}_2^* \text{ est représenté par } \langle 1,1\rangle \end{aligned}$$

Puisque 5 est représenté par $\langle 1,1\rangle$ (cf.[1] page 385), $\langle 1,1,3,3\rangle$ est isotrope et donc est hyperbolique puisque l'on sait que $\langle 1,1,3,3\rangle$ est soit anisotrope soit hyperbolique, d'où $2.< 1,3 >= 0_{W(\mathbb{Q}_2)}$.

On adopte exactement le même raisonnement que ci-dessus pour prouver que $2.\langle 1,6\rangle$ est hyperbolique sur $\mathbb{Q}_2$. La forme diagonale $\langle 1,1,6,6\rangle$ est regulière, de dimension 4 et de déterminant 1 modulo les carrés de $\mathbb{Q}_2^*$, elle est soit anisotrope, soit hyperbolique. Alors, l'astuce de la dimension 4 nous indique que $\langle 1,1,6,6\rangle$ est isotrope si et seulement si $\langle 1,1,6\rangle \simeq \langle 1,1,-2\rangle$ l'est, ce qui revient au fait que 2 soit représenté par $\langle 1,1\rangle$. Comme c'est le cas (cf.[1] page 385), on en conclut le caractère hyperbolique de $2.\langle 1,6\rangle$ et le fait que $2.< 1,6 >= 0_{W(\mathbb{Q}_2)}$.

Il reste à montrer que $8.\langle 1\rangle$ est hyperbolique sur $\mathbb{Q}_2$. Supposons que cette forme diagonale ne le soit pas, alors d'après la décomposition de Witt d'une forme quadratique il existe un entier $n \in \{1,2,3\}$ et une forme quadratique anisotrope q_a tel que $8.\langle 1\rangle \simeq n.\langle 1,-1\rangle \perp q_a$

- Si $n = 1$ alors q_a est anisotrope de dimension 6, ce qui est absurde puisque toute forme quadratique sur $\mathbb{Q}_2$ de dimension ≥ 5 est isotrope.

- Si $n = 2$ alors $8.\langle 1\rangle \simeq \langle 1,-1,1,-1\rangle \perp q_a$ avec q_a anisotrope de dimension 4. Or sur $\mathbb{Q}_2$, il y a à équivalence près une unique forme quadratique anisotrope de dimension 4 qui est $\langle 1,1,1,1\rangle$. Ainsi $q_a \simeq \langle 1,1,1,1\rangle$ et par simplification de Witt :
$$8.\langle 1\rangle \simeq \langle 1,-1,1,-1\rangle \perp \langle 1,1,1,1\rangle \Longrightarrow \langle 1,1,1,1\rangle \simeq \langle 1,-1,1,-1\rangle$$
ce qui est absurde car $\langle 1,-1,1,-1\rangle$ est hyperbolique, alors que $\langle 1,1,1,1\rangle$ est anisotrope.
- Si $n = 3$, $8.\langle 1\rangle \simeq 3.\langle 1,-1\rangle \perp q_a$ où q_a est anisotrope de dimension 2. L'équivalence impliquant l'égalité des déterminants dans $\mathbb{Q}_2^*/\left(\mathbb{Q}_2^*\right)^2$ on a :
$$det(3.\langle 1,-1\rangle \perp q_a) = det(8.\langle 1\rangle) = 1 \Longrightarrow det(q_a) = -1$$
Or, q_a de dimension 2, régulière et de déterminant -1 est donc hyperbolique, ce qui est absurde. Au final, on a bien $8.\langle 1\rangle$ est hyperbolique sur $\mathbb{Q}_2$ et donc en termes de classe de Witt équivalence, $8.< 1 >= 0_{W(\mathbb{Q}_2)}$, ce qui achève de montrer que Φ est bien définie.

Etape 2 : Φ est injective

Il s'agit désormais de montrer que Φ est un isomorphisme de groupe. Le fait qu'il s'agisse d'un morphisme est clair, montrons dans un premier temps l'injectivité. Supposons que $\Phi(\overline{a},\overline{b},\overline{c}) = 0_{W(\mathbb{Q}_2)}$, avec $(\overline{b},\overline{c}) = (\overline{0},\overline{0})$). On remarque pour commencer que $2.< 1 >$ est non nul dans $W(\mathbb{Q}_2)$, puisque $2.\langle 1\rangle$ est anisotrope sur $\mathbb{Q}_2$ car de déterminant égal à $1 \neq -1$ dans $\mathbb{Q}_2^*/\left(\mathbb{Q}_2^*\right)^2$. De même $\langle 1,1,1,1\rangle$ est anisotrope sur $\mathbb{Q}_2$ et donc $4.< 1 >\neq 0_{W(\mathbb{Q}_2)}$. Enfin, $6.< 1 >\neq 0_{W(\mathbb{Q}_2)}$ puisque sinon, comme

$$0 = 8.< 1 > = 6.< 1 > + 2.< 1 > = 0_{W(\mathbb{Q}_2)}$$

on aurait $2.< 1 >= 0_{W(\mathbb{Q}_2)}$, absurde. D'où,

$$\Phi(\overline{a},\overline{0},\overline{0}) = 0_{W(\mathbb{Q}_2)} \Longleftrightarrow \overline{a} = 0.$$

Si $(\overline{b},\overline{c}) = (\overline{1},\overline{1})$ alors $< 1,3 > + < 1,6 >=< 1,1,3,6 >\neq 0_{W(\mathbb{Q}_2)}$ car la forme diagonale $\langle 1,1,3,6\rangle$ est non hyperbolique sur $\mathbb{Q}_2$ puisque de discriminant $18 = 2 \neq 1$ dans $\mathbb{Q}_2^*/\left(\mathbb{Q}_2^*\right)^2$. Or, pour $a \in \{0,2,4,6\}$ on a $a.\langle 1\rangle\perp\langle 1,3,1,6\rangle$ est de discriminant ± 2 dans $\mathbb{Q}_2^*/\left(\mathbb{Q}_2^*\right)^2$ et n'est pas hyperbolique soit

$$\text{a.}< 1 > + < 1,3 > + < 1,6 >\neq 0_{W(\mathbb{Q}_2)}.$$

Si $(\overline{b},\overline{c}) = (\overline{0},\overline{1})$ ou $(\overline{1},\overline{0})$ alors $a.\langle 1\rangle\perp\langle 1,6\rangle$ a pour discriminant $\pm 6 \neq 1$ et $a.\langle 1\rangle\perp\langle 1,3\rangle$ a pour discriminant $\pm 3 \neq 1$. Ces formes quadratiques sont donc non hyperboliques et donc $\Phi(\overline{a},\overline{1},\overline{0}), \Phi(\overline{a},\overline{0},\overline{1}) \neq 0_{W(\mathbb{Q}_2)}$. Ainsi il vient :

$$\Phi(\overline{a},\overline{b},\overline{c}) = 0 \Longleftrightarrow (\overline{a},\overline{b},\overline{c}) = (\overline{0},\overline{0},\overline{0})$$

ce qui montre l'injectivité.

Etape 3 : Φ est surjective

On montre désormais la surjectivité de Φ. Comme $W(\mathbb{Q}_2)$ est engendré par les éléments $< 1 >,< 2 >,< 3 >,< 5 >,< 6 >,< 7 >,< 10 >,< 14 >$, il suffit pour montrer la surjectivité (comme Φ est un morphisme de groupes) de prouver que les générateurs de $W(\mathbb{Q}_2)$ sont atteints. Or, pour $a \in \{1,2,3,5,6,7,10,14\}$, dans le groupe additif $W(\mathbb{Q}_2)$ on a :

$$- < a >=< -a >, \text{ pour } - < a > \text{ l'opposé de } < a >$$

Puisque,

$$-1 = 7, -2 = 14, -3 = 5, -6 = 10 \text{ dans } \mathbb{Q}_2^*/\left(\mathbb{Q}_2^*\right)^2,$$

on aura simplement besoin de chercher des antécédents par Φ aux éléments :

$$< 1 >, < 2 >, < 3 >, < 6 >.$$

On a vu précédemment que $2.< 1, 3 >= 0_{W(\mathbb{Q}_2)} \Longrightarrow < 1, 1, 3, 3 >= 0_{W(\mathbb{Q}_2)}$ et donc que

$$\begin{aligned}
& < 1, 1, 3 > + < 3 >= 0_{W(\mathbb{Q}_2)} \\
\Longrightarrow \quad & < 1, 1, 3 >= - < 3 >=< -3 > \\
\Longrightarrow \quad & < 1, 1, 3 >=< 5 > \\
\Longrightarrow \quad & < 1 > + < 1, 3 >=< 5 > \\
\Longrightarrow \quad & \Phi(\overline{1}, \overline{1}, \overline{0}) =< 5 > \\
\Longrightarrow \quad & < 5 > \text{ est atteint par } (\overline{1}, \overline{1}, \overline{0}) \\
\Longrightarrow \quad & < 3 >=< -5 > \text{ est atteint par } (\overline{-1}, \overline{-1}, \overline{0})
\end{aligned}$$

D'où, $\Phi(\overline{1}, \overline{1}, \overline{0}) =< 5 >$, $\Phi(\overline{7}, \overline{1}, \overline{0}) =< 3 >$ montrent que les générateurs $< 3 >$ et $< 5 >$ sont atteints par Φ. Par la même méthode, les égalités :

$$2.< 1, 6 >= 0_{W(\mathbb{Q}_2)} \text{ et } 8.< 1 >= 0_{W(\mathbb{Q}_2)}$$

donnent

$$\Phi(\overline{1}, \overline{0}, \overline{1}) =< 10 >, \Phi(\overline{7}, \overline{0}, \overline{1}) =< 6 > \text{ et } \Phi(\overline{1}, \overline{0}, \overline{0}) =< 1 >, \Phi(\overline{7}, \overline{0}, \overline{0}) =< 7 >.$$

Il reste donc à atteindre $< 2 >$ et $< 14 >$. Pour atteindre $< 14 >$ on cherche $(\overline{a}, \overline{b}, \overline{c})$ tel que : a.$< 1 >$ + b.$< 1, 3 >$ + c.$< 1, 6 >=< 14 >$ ce qui équivaut à :

$$\text{a.} < 1 > + \text{b.} < 1, 3 > + \text{c.} < 1, 6 > + < 2 >= 0_{W(\mathbb{Q}_2)}.$$

comme $- < 14 >=< -14 >=< 2 >$ dans $W(\mathbb{Q}_2)$. Il s'agit alors de trouver $(\overline{a}, \overline{b}, \overline{c})$, tel que la forme diagonale $a.\langle 1\rangle \perp b.\langle 1, 3\rangle \perp c.\langle 1, 6\rangle \perp \langle 2\rangle$ sur $\mathbb{Q}_2$ soit hyperbolique. Comme une forme hyperbolique se doit d'être de discriminant 1, on va chercher à tester le caractère hyperbolique des formes suivantes :

$$3.\langle 1\rangle \perp \langle 1, 3\rangle \perp \langle 1, 6\rangle \perp \langle 2\rangle \text{ et } 7.\langle 1\rangle \perp \langle 1, 3\rangle \perp \langle 1, 6\rangle + \langle 2\rangle.$$

Si on suppose la forme diagonale $\langle 1, 1, 1, 1, 1, 2, 3, 6\rangle$ non hyperbolique sur $\mathbb{Q}_2$ alors en raison du théorème de décomposition de Witt, il existe $n \in \{2, 3\}$ et une forme quadratique anisotrope q_a tels que :

$$\langle 1, 1, 1, 1, 1, 2, 3, 6\rangle \simeq n.\langle 1, -1\rangle \perp q_a$$

où $n \neq 1$ car sinon q_a serait anisotrope sur $\mathbb{Q}_2$ de dimension 6, absurde. Or $n = 3$ est également absurde, en effet, si tel était le cas, on aurait par le calcul du déterminant des deux formes équivalentes :

$$det(q_a) = -1 \text{ dans } \mathbb{Q}_2^*/\left(\mathbb{Q}_2^*\right)^2$$

avec q_a de dimension 2, qui serait donc hyperbolique, absurde. D'après ce qui précède, comme $\langle 1, 1, 1, 1, 1, 2, 3, 6\rangle$ est de dimension 8 sur $\mathbb{Q}_2$, elle est nécessairement isotrope et si on la suppose non hyperbolique, alors $n = 2$ et elle est équivalente à $2.\langle 1, -1\rangle \perp q_a$, avec q_a anisotrope de dimension 4 donc équivalente à $\langle 1, 1, 1, 1\rangle$. Ainsi, si $\langle 1, 1, 1, 1, 1, 2, 3, 6\rangle$ n'est pas hyperbolique, on a :

$$\langle 1,1,1,1,1,2,3,6\rangle \simeq \langle 1,-1,1,-1\rangle \perp \langle 1,1,1,1\rangle$$

et par simplification de Witt

$$\langle 1,2,3,6\rangle \simeq \langle 1,-1,1,-1\rangle$$

Ceci implique que $\langle 1,2,3,6\rangle$ est hyperbolique et donc que $<1,2,3,6>=0_{W(\mathbb{Q}_2)}$. Or, puisque $8.<1>=0_{W(\mathbb{Q}_2)}$ on a :

$$\begin{aligned} 7.<1>+<1,3>+<1,6>+<2>= \quad & 8.<1>+<1,2,3,6> \\ = \quad & <1,2,3,6> \\ = \quad & 0_{W(\mathbb{Q}_2)} \end{aligned}$$

dans $W(\mathbb{Q}_2)$. Récapitulons, si on suppose que :

$$3.<1>+<1,3>+<1,6>+<2>\neq 0_{W(\mathbb{Q}_2)}$$

alors $7.<1>+<1,3>+<1,6>+<2>=0_{W(\mathbb{Q}_2)}$ et donc on a nécessairement :

$$\Phi(\overline{3},\overline{1},\overline{1})=<14> \text{ ou } \Phi(\overline{7},\overline{1},\overline{1})=<14>$$

Ceci montre que $<14>$ est atteint, tout comme son inverse $<2>$ dans $W(\mathbb{Q}_2)$ et termine de montrer la surjectivité de Φ qui est donc un isomorphisme de groupe.

Etape 4 : Etude de $\widehat{W}(\mathbb{Q}_2)$

Pour l'étude de $\widehat{W}(\mathbb{Q}_2)$, on utilise le fait que $\widehat{W}(\mathbb{Q}_2)\simeq\mathbb{Z}\times I(\mathbb{Q}_2)$ avec $I(\mathbb{Q}_2)$ d'indice 2 dans $W(\mathbb{Q}_2)$. Les éléments de $I(\mathbb{Q}_2)$ sont les éléments de $W(\mathbb{Q}_2)$ de dimension paire, soit via l'isomophisme Φ les éléments suivants :

$$\begin{gathered} \Phi(\overline{0},\overline{1},\overline{0}),\ \Phi(\overline{0},\overline{0},\overline{1}),\ \Phi(\overline{0},\overline{1},\overline{1}),\ \Phi(\overline{2},\overline{1},\overline{0}),\ \Phi(\overline{4},\overline{1},\overline{0}),\ \Phi(\overline{6},\overline{1},\overline{0}),\ \Phi(\overline{0},\overline{0},\overline{0}),\\ \Phi(\overline{2},\overline{0},\overline{0}),\ \Phi(\overline{4},\overline{0},\overline{0}),\ \Phi(\overline{6},\overline{0},\overline{0}),\ \Phi(\overline{2},\overline{1},\overline{1}),\ \Phi(\overline{4},\overline{1},\overline{1}),\ \Phi(\overline{6},\overline{1},\overline{1}),\ \Phi(\overline{2},\overline{0},\overline{1}),\\ \Phi(\overline{4},\overline{0},\overline{1}),\Phi(\overline{6},\overline{0},\overline{1}). \end{gathered}$$

L'étude des ordres des éléments $(\overline{a},\overline{b},\overline{c})$ de la liste précédente montre que $I(\mathbb{Q}_2)$ est composé de 7 éléments d'ordre 2, 8 éléments d'ordre 4 et d'un élément d'ordre 1. Les sous-groupes d'indice 2 de $\mathbb{Z}/8\times\mathbb{Z}/2\times\mathbb{Z}/2$ étant isomorphes à $\mathbb{Z}/8\times\mathbb{Z}/2$ ou $\mathbb{Z}/4\times\mathbb{Z}/2\times\mathbb{Z}/2$, le groupe $I(\mathbb{Q}_2)$ est lui aussi isomorphe à un de ces deux groupes. L'étude des ordres des éléments de $I(\mathbb{Q}_2)$ montre alors que $I(\mathbb{Q}_2)\simeq\mathbb{Z}/4\times\mathbb{Z}/2\times\mathbb{Z}/2$, ce qui prouve que $\widehat{W}(\mathbb{Q}_2)\simeq\mathbb{Z}\times\mathbb{Z}/4\times(\mathbb{Z}/2)^2$ □

9.5 Application de l'étude des formes quadratiques p-adiques à l'étude des formes quadratiques rationnelles

Dans cette partie, nous utilisons les résultats des sections précédentes relatives à l'étdude des formes quadratiques sur les corps $\mathbb{Q}_p$ pour obtenir des résultats sur les formes quadratiques rationnelles.

9.5.1 Formes quadratiques rationnelles et classes d'isomorphies

Contrairement au cas du corps $\mathbb{R}$, qui ne possède à équivalence près que deux formes quadratiques de dimension 4 anisotropes, que sont :

$$\langle 1,1,1,1\rangle \text{ et } \langle -1,-1,-1,-1\rangle$$

les formes quadratiques régulières indéfinies et anisotropes de dimension 4 sur $\mathbb{Q}$ sont plus difficiles à classer :

Proposition 9.5.1. *Il existe une infinité de classes d'isomporhie de formes quadratiques régulières, indéfinies, anisotropes et de dimension* 4 *sur* $\mathbb{Q}$.

Démonstration. D'après le théorème de structure des formes quadratiques anisotropes sur $\mathbb{Q}_2$, la localisée $\langle 1,1,1\rangle_2$ est anisotrope sur $\mathbb{Q}_2$ et donc $\langle 1,1,1\rangle$ l'est sur $\mathbb{Q}$, d'après le principe de Hasse fort. Puisque $\Delta(\langle 1,1,1\rangle) = 1$, d'après l'astuce de la dimension 4, $\langle 1,1,1,-p\rangle$ est aussi anisotrope si pour $p \in \mathcal{P}$ on a $-p = 1$ dans $\mathbb{Q}_2^*/(\mathbb{Q}_2^*)^2$. Soit p un nombre premier impair, alors :

$$\begin{aligned}
& -p = 1 \text{ dans } \mathbb{Q}_2^*/\left(\mathbb{Q}_2^*\right)^2 \\
\iff \quad & p = -1 \text{ dans } \mathbb{Q}_2^*/\left(\mathbb{Q}_2^*\right)^2 \\
\iff \quad & p = 7 \text{ dans } \mathbb{Q}_2^*/\left(\mathbb{Q}_2^*\right)^2 \\
\iff \quad & v_2(p) \equiv v_2(7)\,[2] \text{ et } 2^{-v_2(p)}p \equiv 2^{-v_2(7)}7\,[8] \\
\iff \quad & p \equiv 7\,[8] \text{ puisque } v_2(p) = 0 = v_2(7)
\end{aligned}$$

D'où, pour $p \in \mathcal{P}$ tel que $p \equiv 7\,[8]$ la forme quadratique $\langle 1,1,1,-p\rangle$ est anisotrope sur $\mathbb{Q}_2$ et donc sur $\mathbb{Q}$ (par le principe de Hasse fort) et $\langle 1,1,1,-p\rangle_{\mathbb{Q}}$ est donc une forme rationnelle régulière, indéfinie, anisotrope de dimension 4. D'après le théorème des nombres premiers de Dirichlet, il y a une infinité de nombres premiers congrus à 7 modulo 8 ($7 \wedge 8 = 1$), il suffit alors pour montrer le résultat, de prouver que pour $(p_1, p_2) \in \mathcal{P}$ tels que $p_1, p_2 \equiv 7\,[8]$, $p_1 \neq p_2$ on a :

$$\langle 1,1,1,-p_1\rangle \not\simeq \langle 1,1,1,-p_2\rangle \text{ sur } \mathbb{Q}$$

Utilisons alors le test d'équivalence rationnelle. Pour $p = p_1 \neq p_2$, on a :

$$\partial_p(< 1,1,1,-p_1 >) =< 0,0,0,-1 > \text{ et } \partial_p(< 1,1,1,-p_2 >) =< 0,0,0,0 >$$

Comme $< 0,0,0,-1 >=< -1 >\neq 0_{W(\mathbb{Q}_2)}$, $\langle 1,1,1,-p_1\rangle \not\simeq \langle 1,1,1,-p_2\rangle$ dès que $p_1, p_2 \equiv 7\,[8]$ et $p_1 \neq p_2$, d'où le nombre infini de classes d'isomorphie souhaitées. □

9.5.2 Formes quadratiques rationnelles universelles et anisotropes

Théorème 9.5.1. *Toute forme quadratique rationnelle régulière indéfinie et de dimension* 4 *est universelle.*

Démonstration. Soit ψ une forme quadratique rationnelle régulière indéfinie et de dimension 4. Alors,

$$\begin{aligned}
\psi \text{ est universelle} &\iff \forall a \in \mathbb{Q}^*, \psi \text{ représente a.} \\
&\iff \forall a \in \mathbb{Q}^*, \psi \perp \langle -a \rangle \text{ est isotrope.} \\
&\iff \forall a \in \mathbb{Q}^*, \forall p \in \mathcal{P}_\infty, \psi_p \perp \langle -a \rangle_p \text{ est isotrope.} \\
&\iff \forall a \in \mathbb{Q}^*, \forall p \in \mathcal{P}, \psi_p \perp \langle -a \rangle_p \text{ est isotrope.}
\end{aligned}$$

L'équivalence entre (2) et (3) est simplement l'application du principe de Hasse fort, quant à la dernière équivalence, $3 \Longrightarrow 4$ est évidente et $4 \Longrightarrow 3$ découle du fait que ψ étant indéfinie, sa localisée $\psi_{\mathbb{R}}$ est isotrope sur $\mathbb{R}$ et donc $\forall a \in \mathbb{Q}^*$, $\psi_{\mathbb{R}} \perp \langle -a \rangle$ est isotrope, ce qui règle le cas $p = \infty$. En effet, par diagonalisation, il existe $(a_i)_{1 \leq i \leq 4} \in (\mathbb{Q}^*)^4$ tel que $\psi \simeq \langle a_1, a_2, a_3, a_4 \rangle$ et dans une base adaptée, ψ est représentée par la matrice diagonale $D(a_1, a_2, a_3, a_4)$, de même pour la localisée $\psi_{\mathbb{R}}$. Ainsi, la forme quadratique $\psi_{\mathbb{R}}$ prolongeant ψ sur $\mathbb{R}$ n'est pas de signature $(4, 0)$ ou $(0, 4)$ car les a_i ne sont pas tous strictement positifs ou tous strictement négatifs (ψ étant indéfinie) et donc d'après la classification des formes quadratiques réelles, $\psi_{\mathbb{R}}$ n'est pas anisotrope et donc isotrope.

Or, pour $p \in \mathcal{P}, \psi_p \perp \langle -a \rangle_p$ est une forme quadratique de dimension 5 sur $\mathbb{Q}_p$, elle est donc isotrope et d'après les équivalences ci-dessus ψ est bien universelle. □

Nous avons vu que si q est une forme quadratique régulière, isotrope alors q est universelle, mais la réciproque est fause :

Corollaire 9.5.1. *Il existe des formes quadratiques rationnelles régulières, universelles et anisotropes.*

Démonstration. On va utiliser le résultat précédent et essayer d'exhiber une forme quadratique rationnelle, régulière, indéfinie, de dimension 4 et anisotrope. Considérons alors la forme quadratique diagonale $q = \langle 10, 21, -15, -7 \rangle$ qui est régulière, indéfinie et de dimension 4 sur $\mathbb{Q}$. D'après le théorème ci-dessus, elle est universelle et il reste à montrer qu'elle est anisotrope. Pour ce faire, on va appliquer la proposition sur les formes quadratiques anisotropes sur $\mathbb{Q}_p$. Les nombres premiers impairs divisant au moins un des termes diagonaux étant $\{3, 5, 7\}$, on teste l'anisotropie de q sur les corps $\mathbb{Q}_p$ correspondant. Par le principe de Hasse fort, il suffit de montrer que q_p est anisotrope pour au moins un $p \in \{3, 5, 7\}$. L'étude sur $\mathbb{Q}_3, \mathbb{Q}_5$ ne permettant pas de conclure, on s'intéresse à l'étude sur $\mathbb{Q}_7$. Comme q s'écrit $q = \langle 10, 7 \times (3), -15, 7 \times (-1) \rangle$, la localisée sur $\mathbb{Q}_7$ est anisotrope :

$$\begin{aligned}
&\iff q_7 = \langle 10, 7 \times (3), -15, 7 \times (-1) \rangle_7 \text{ est anisotrope} \\
&\iff \langle \overline{10}, \overline{-15} \rangle \text{ et } \langle \overline{-1}, \overline{3} \rangle \text{ sont anisotropes sur } \mathbb{F}_7. \\
&\iff \langle \overline{3}, \overline{6} \rangle \text{ et } \langle \overline{-1}, \overline{3} \rangle \text{ sont anisotropes sur } \mathbb{F}_7. \\
&\iff \langle \overline{3}, \overline{6} \rangle \text{ et } \langle \overline{-1}, \overline{3} \rangle \text{ ne sont pas hyperboliques sur } \mathbb{F}_7.
\end{aligned}$$

Or $det(\langle \overline{3}, \overline{6} \rangle) = 18$, avec $18 = 4 = 2^2$ dans $\mathbb{F}_7$. On a donc $det(\langle \overline{3}, \overline{6} \rangle) = 1$ dans $\mathbb{F}_7^*/(\mathbb{F}_7^*)^2$ et comme $7 \equiv 1\,[4]$, on a :

$$det(\langle \overline{3}, \overline{6} \rangle) = 1 \neq -1 \text{ dans } \mathbb{F}_7^*/(\mathbb{F}_7^*)^2$$

et $\langle \overline{3}, \overline{6} \rangle$ n'est pas hyperbolique. Comme $\langle \overline{-1}, \overline{3} \rangle$ a même déterminant que $\langle \overline{3}, \overline{6} \rangle$, elle n'est pas non plus hyperbolique. La localisée sur q_7 est alors anisotrope et donc q l'est également sur $\mathbb{Q}$. Ce qui achève de montrer le résultat. □

9.5.3 Etude de la surjectivité du morphisme Φ

Nous allons désormais voir une application intéressante du principe de Hasse fort et de l'étude des formes quadratiques sur les corps $\mathbb{Q}_p$. On rappelle que le test d'équivalence rationnelle repose sur l'isomorphisme suivant :

$$\Phi : \begin{cases} W(\mathbb{Q}) \longrightarrow W(\mathbb{R}) \oplus \bigoplus_{p \in \mathcal{P}} W(\mathbb{F}_p) \\ x \longmapsto x_{\mathbb{R}} + \sum_{p \in \mathcal{P}} \partial_p(x) \end{cases}$$

Nous allons étudier plus précisément la surjectivité de celui-ci, en examinant sur un exemple concret comment trouver de manière pratique un antécédent minimal en termes de dimension, d'un élément de $W(\mathbb{R}) \oplus \bigoplus_{p \in \mathcal{P}} W(\mathbb{F}_p)$. Dans la proposition suivante et sa démonstration on notera encore k, l'élément $\overline{k} \in \mathbb{F}_p$, où $p \in \mathcal{P}$.

Proposition 9.5.2. *$y =< 1, -1 >_{\mathbb{R}} + < -1 >_{\mathbb{F}_3} + < 1, 2 >_{\mathbb{F}_5} + < 1 >_{\mathbb{F}_7}$ dans $W(\mathbb{R}) \oplus \bigoplus_{p \in \mathcal{P}} W(\mathbb{F}_p)$ admet $< 7, 10, -5, -3 >$ dans $W(\mathbb{Q})$ comme unique antécédent. De plus, il existe des rationnels non nuls a et b tels que la forme diagonale $\langle a, b \rangle$ soit anisotrope sur $\mathbb{Q}$ avec $< 7, 10, -5, -3 >=< a, b >$ dans $W(\mathbb{Q})$. Ainsi, y admet la classe de Witt équivalence d'une forme diagonale régulière, anisotrope de dimension 2, comme antécédent, et cette solution est minimale en termes de dimension.*

Démonstration. Il est clair pour commencer, que $\partial_7(< 7 >) =< 1 >$ dans $W(\mathbb{F}_7)$. En revanche $\partial_5(< 7 >) \neq< 1, 2 >_{\mathbb{F}_5}$, on va alors plutôt considérer :

$$< 7, 5, 10 >=< 7 > + < 5, 10 >$$

dont l'image par ∂_7 reste inchangée ($\partial_7(< 5, 10 >= 0_{W(\mathbb{F}_7)}$ et telle que :

$$\partial_5(< 7, 5, 10 >) =< \partial_5(7), \partial_5(5), \partial_5(10) >=< 0, 1, 2 >=< 1, 2 > \text{ dans } W(\mathbb{F}_5)$$

L'idée ici est donc d'augmenter progressivement la dimension de la classe de Witt équivalence de notre forme diagonale afin d'obtenir succesivement les bonnes images par les morphismes ∂_p pour $p \in \{3, 5, 7\}$. Puisque 3 ne divise aucun des termes diagonaux de $< 7, 5, 10 >$, on a $\partial_3(< 7, 5, 10 >) = 0_{W(\mathbb{F}_3)}$ et on va donc devoir encore augmenter la dimension de la forme diagonale. On trouve alors que $< 7, 5, 10, -3 >$ a la bonne image par ∂_3, les autres images par ∂_5, ∂_7 étant clairement inchangées. Enfin, $\langle 7, 5, 10, -3 \rangle$ est de signature réduite $3 - 1 = 2$ et par la proposition 5.2.2 on a donc $< 7, 5, 10, -3 >\neq< 1, -1 >$ dans $W(\mathbb{R})$, ce qui nous impose encore d'augmenter la dimension de la forme diagonale $\langle 7, 5, 10, -3 \rangle$ représentant la classe de Witt-équivalence $< 7, 5, 10, -3 >$ sur $\mathbb{Q}$, pour obtenir une signature réduite appropriée. Finalement, $< 7, 5, 10, -3, -1, -1 >$ est solution du problème. Ainsi, l'étude des images par les morphismes ∂_7, ∂_5, ∂_3 nous a fait passer de $< 7 >$ à $< 7, 5, 10 >$ à $< 7, 5, 10, -3 >$ puis l'étude de la signature réduite (étude correspondant au morphisme d'extension $x \longrightarrow x_{\mathbb{R}}$) nous a obligé à considérer la classe $< 7, 5, 10, -3, -1, -1 >$ qui est donc l'unique solution du problème (Φ étant un isomporphisme).

On cherche à écrire $< 7, 5, 10, -3, -1, -1 >$ de façon minimale en termes de dimension, ceci revient donc à chercher la forme diagonale anisotrope de dimension minimale dont la classe de Witt équivalence associée $< 7, 5, 10, -3, -1, -1 >$.

Etudions $\langle 7, 5, 10, -3, -1, -1\rangle$. Elle est régulière, indéfinie sur $\mathbb{Q}$, de dimension 6, donc isotrope. De plus $\langle 7, 5, 10, -3, -1, -1\rangle$ est non hyperbolique sur $\mathbb{Q}$ car a pour image par Φ l'élément y qui est non nul. Ainsi, $\langle 7, 5, 10, -3, -1, -1\rangle$ est d'indice 1 ou 2 et on peut trouver une forme quadratique régulière sur $\mathbb{Q}$, anisotrope de dimension 2 ou 4, Witt-équivalente à $\langle 7, 5, 10, -3, -1, -1\rangle$. Pour ce faire, on va extraire la partie hyperbolique de $\langle 7, 5, 10, -3, -1, -1\rangle$. Les relations de Witt : $\langle a, b\rangle \simeq \langle a + b, (a + b)ab\rangle$, $a, b \in \mathbb{Q}^*, a + b \neq 0$, nous donnent alors :

$$\begin{aligned}
\langle -3, -1 - 1\rangle &\simeq \langle -1, -1, -3\rangle \\
&\simeq \langle -1, -1\rangle \perp \langle -3\rangle \\
&\simeq \langle -4, -1\rangle \perp \langle -3\rangle \\
&\simeq \langle -5, -20\rangle \perp \langle -3\rangle \\
&\simeq \langle -5, -5\rangle \perp \langle -3\rangle \\
&\simeq \langle -5, -5, -3\rangle
\end{aligned}$$

D'où, dans $W(\mathbb{Q})$ (l'équivalence impliquant la Witt équivalence), on a :

$$\begin{aligned}
< 7, 5, 10, -3, -1, -1 > &= < 7, 5, 10 > + < -3, -1, -1 > \\
&= < 7, 5, 10 > + < -5, -5, -3 > \\
&= < 7, 10, -3, -5 > + < -5, 5 > \\
&= < 7, 10, -3, -5 >
\end{aligned}$$

où $< 5, -5 >= 0_{W(\mathbb{Q})}$ car $\langle -5, 5\rangle$ est hyperbolique sur $\mathbb{Q}$. $< 7, 10, -3, -5 >$ est donc un antécédent de y et on cherche à savoir s'il est minimal en termes de dimension, en testant le caractère isotrope de la forme $\langle 7, 10, -3, -5\rangle$. Par le principe de Hasse fort, elle est isotrope si et seulement si ses localisées sont isotropes sur les corps $\mathbb{Q}_p$ pour $p \in \mathcal{P}_\infty$. L'ensemble des diviseurs premiers des termes diagonaux étant $\{2, 3, 5, 7\}$, il nous suffit de tester l'isotropie sur $\mathbb{R}$ et les corps $\mathbb{Q}_p$ associés.

- $\langle 7, 10, -3, -5\rangle$ est isotrope sur $\mathbb{R}$ car indéfinie, ce qui règle le cas $p = \infty$.
- Sur $\mathbb{Q}_2$ la localisée de $\langle 7, 10, -3, -5\rangle$ est de déterminant $14 \neq 1$ dans $\mathbb{Q}_2/(\mathbb{Q}_2^*)^2$ (cf. table de multiplication), la seule forme quadratique anisotrope de dimension 4 sur $\mathbb{Q}_2$ étant de déterminant 1, la localisée de $\langle 7, 10, -3, -5\rangle$ sur $\mathbb{Q}_2$ est isotrope.
- Sur $\mathbb{Q}_3$, pour étudier l'isotropie de la localisée de $\langle 7, 10, 3 \times (-1), -5\rangle$, il nous suffit d'étudier l'isotropie des formes diagonales $\langle -1\rangle$ et $\langle 7, 10, -5\rangle$ sur $\mathbb{F}_3$. Or, $\langle 7, 10, -5\rangle = \langle 1, 1, 1\rangle$ est de dimension 3 régulière sur $\mathbb{F}_3$, elle est isotrope et donc la localisée de $\langle 7, 10, -3, -5\rangle$ sur $\mathbb{Q}_3$ est aussi isotrope.
- Sur $\mathbb{Q}_5$, pour étudier l'isotropie de la localisée de $\langle 7, 5 \times 2, -3, 5 \times (-1)\rangle$, il nous suffit d'étudier l'isotropie des formes diagonales $\langle -1, 2\rangle$ et $\langle 7, -3\rangle$ sur $\mathbb{F}_5$. Or, $det(\langle 7, -3\rangle) = -21 = -1 = 1$ dans $\mathbb{F}_5/(\mathbb{F}_5^*)^2$ (-1 est un carré modulo 5) et $\langle 7, -3\rangle$ est donc isotrope. Ainsi, la localisée de $\langle 7, 10, -3, -5\rangle$ sur $\mathbb{Q}_5$ est aussi isotrope.
- Sur $\mathbb{Q}_7$, pour étudier l'isotropie de la localisée de $\langle 7 \times 1, 10, -3, -5\rangle$, il nous suffit d'étudier l'isotropie des formes diagonales $\langle 1\rangle$ et $\langle 10, -3, -5\rangle$ sur $\mathbb{F}_7$.

Or, $\langle 10, -3, -5\rangle$ est de dimension 3 régulière sur $\mathbb{F}_7$, elle est isotrope et donc la localisée de $\langle 7, 10, -3, -5\rangle$ sur $\mathbb{Q}_7$ l'est aussi.

$\langle 7, 10, -3, -5\rangle$ est donc isotrope sur $\mathbb{Q}$ et n'est pas hyperbolique. Elle est d'indice 1 et admet donc une partie anisotrope de dimension 2. Il existe alors des rationnels non nuls a, b tels que $ab \neq -1$ dans $\mathbb{Q}^*/(\mathbb{Q}^*)^2$ (pour que la forme soit non hyperbolique c'est-à-dire en dimension 2 anisotrope) tels que :

$$< a, b >=< 7, 10, -3, -5 > \text{ et } \Phi(< a, b >) = y$$

□

La première partie du mémoire a donc été l'occasion d'étudier les formes quadratiques sous l'angle de la théorie de Witt. Nos différentes découvertes nous ont alors amené à quitter le monde global des formes quadratiques, pour passer dans celui plus restreint des formes régulières, avec pour destination finale le monde des formes quadratiques anisotropes. Notre trajet s'est organisé autour de quelques grands passages, la rencontre avec l'opération d'addition orthogonale, la simplification de Witt, le principe de gonflement hyperbolique et le théorème de décomposition de Witt qui ont été les éléments déclencheurs de notre future rencontre avec la relation de Witt-équivalence, elle-même décisive pour notre passage vers le monde des groupes abéliens et les structures des groupes de Witt et Witt-Grothendieck. En effet, en associant à un corps $\mathbb{K}$ donné, deux structures très importantes que sont les groupes de Witt $W(\mathbb{K})$ et de Witt-Grothendieck $\widehat{W}(\mathbb{K})$ et en nous promenant le long des corps $\mathbb{R}$, $\mathbb{C}$, des corps finis et des corps p-adiques $\mathbb{Q}_p$, nous avons pu ressentir ô combien notre trajet vers la compréhension des fomes quadratiques rationnelles se nourrissait de chacune de ces rencontres. Nous avons pu, par exemple, revisiter et retrouver de manière élégante des résultats classiques sur la classification des formes quadratiques sur les corps $\mathbb{R}$, $\mathbb{C}$ et les corps finis, qui au final, nous ont permis d'arriver à l'énonciation de tests très efficaces relatifs à la classification des formes quadratiques rationnelles. Enfin, l'arrêt effectué dans l'univers des formes p-adiques nous a permis de relier l'étude des formes quadratiques rationnelles à leurs compagnons de voyage que sont les localisées sur les différents corps $\mathbb{Q}_p$, ce qui a alors clôt cette première partie de notre voyage. Dans la seconde, nous nous arrêterons dans le vaste monde des algèbres non commutatives en dimension finie. Nous focaliserons notre attention sur l'étude d'une alègbre dont la structure dépend, à la fois du corps sur lequel est elle définie, mais aussi de la forme quadratique à laquelle elle est ratachée. Voici venu le monde des algèbres de Clifford, lieu de notre prochain arrêt qui, en deux étapes, l'une consacrée à l'étude de la construction de ces alègbres et l'autre consacrée plus globalement à l'application de ces études préliminaires, nous amènera vers le problème de la classication des formes quadratiques rationnelles abordé via l'algèbre de Clifford associée.

Deuxième partie

Algèbres de Clifford : application à l'étude des formes quadratiques rationnelles.

Chapitre 10

Algèbres $\mathbb{Z}/2$-graduées, construction et calcul des algèbres de Clifford

Ce chapitre est le premier des deux chapitres consacrés à l'étude des algèbres de Clifford, nous y introduirons la notion d'algèbre $\mathbb{Z}/2$-graduée qui est le cadre dans lequel il est nécessaire de nous placer, pour pouvoir parler d'algèbre de Clifford. Puis, après avoir introduit cette structure d'algèbre graduée, nous nous intéresserons à la construction des algèbres de Clifford et à quelques unes de ses propriétés élémentaires. Pour (E, q) un espace quadratique régulier de dimension n, nous noterons $C(q)$ l'algèbre de Clifford associée, dont nous verrons que E peut-être vu comme un sous-ensemble via une injection naturelle $E \hookrightarrow C(q)$. Ainsi, en identifiant les éléments x de E comme des éléments de $C(q)$ qui est elle, munie d'une structure d'algèbre et donc d'une loi multiplicative interne, on verra qu'on peut définir $C(q)$ comme étant l'algèbre la plus naturelle engendrée par l'espace vectoriel E et dans laquelle on a :

$$\forall x \in E, q(x)1_{C(q)} = x^2 \text{ (où } x^2 \text{ a un sens, puisque le produit } x \times x \text{ est bien défini dans } C(q))$$

Ce chapitre introductif sera l'occasion de donner des résultats et propriétés sur les algèbres de Clifford qui seront pour la plupart admis (pour les démonstrations cf.[1] XXIV). Il nous fournira les outils nécessaires pour comprendre et bien assimiler le chapitre suivant où seront regroupés des résultats originaux non établis dans le livre de Clément de Seguins Pazzis. Nous présenterons ainsi brièvement comment est construit l'algèbre de Clifford, ses propriétés universelles, nous exposerons des résultats concernant la dimension de l'algèbre $C(q)$ et en exhiberons une base usuelle. Nous nous intéresserons également au problème du calcul de l'algèbre de Clifford d'une somme orthogonale $q \perp q'$, ce qui nous permettra via les résultats sur les algèbres $C(q)$ pour q régulière de dimension 1, de mieux comprendre les algèbres de Clifford en dimension supérieure. Enfin, nous consacrerons la dernière partie de ce chapitre à l'étude de la partie paire et du centre d'une algèbre de Clifford et présenterons des résultats originaux non établis dans le livre de Clément de Seguins Pazzis.

Le but de ces deux chapitres sur les algèbres de Clifford étant d'aborder le problème de la classification des formes quadratiques sous un nouvel angle, nous ne nous attarderons pas sur les démonstrations de certains résultats et propriétés détaillées clairement dans le livre de Clément de Seguins Pazzis. En revanche dans le chapitre suivant,(après avoir présenter quelques résultats de structure sur les algèbres de Clifford), nous présenterons les résultats d'exercices et de certains problèmes de synthèse en nous plongeant dans le problème de la classification des formes quadratiques en dimension 2, 3 et 4 via l'algèbre de Clifford associée, puis en toute dimension pour les formes quadratiques p-adiques et rationnelles.

10.0.4 Algèbres $\mathbb{Z}/2$-graduées

Définition 10.0.1. *On appelle algèbre $\mathbb{Z}/2$-graduée sur le corps $\mathbb{K}$ la donnée d'une $\mathbb{K}$-algèbre $\mathcal{A}$ (associative et unitaire) et de deux sous-espaces $\mathcal{A}_0$ et $\mathcal{A}_1$ de $\mathcal{A}$ vérifiant :*

1. $1_{\mathcal{A}} \in \mathcal{A}_0$
2. $\mathcal{A}_0 \oplus \mathcal{A}_1 = \mathcal{A}$
3. $\forall (i,j) \in (\mathbb{Z}/2)^2, \mathcal{A}_i\mathcal{A}_j \subset \mathcal{A}_{i+j}$ *où $i+j$ est considéré modulo* 2.

Les sous-espaces $\mathcal{A}_0$ et $\mathcal{A}_1$ sont appelés respectivement **la partie paire** et **la partie impaire** de l'algèbre graduée $\mathcal{A}$. Si $\mathcal{A} = \mathcal{A}_0$, alors on parle de graduation triviale.

Définition 10.0.2. *Soit $\mathcal{A}$ et $\mathcal{B}$, deux algèbres $\mathbb{Z}/2$-graduées. Une application,*

$$f : \mathcal{A} \longrightarrow \mathcal{B}$$

est appelée morphisme d'algèbres graduées lorsque c'est un morphisme d'algèbres de $\mathcal{A}$ dans $\mathcal{B}$ respectuant la graduation :

$$f(\mathcal{A}_0) \subset \mathcal{B}_0 \text{ et } f(\mathcal{A}_1) \subset \mathcal{B}_1$$

Définition 10.0.3. *Soit $\mathcal{A}$ une algèbre $\mathbb{Z}/2$-graduée. Les éléments de $\mathcal{A}_0 \cup \mathcal{A}_1$ sont appelés les éléments **homogènes** de $\mathcal{A}$. On appelle **degré** d'un élément homogène non nul x de $\mathcal{A}$ l'unique entier $k \in \{0,1\}$ tel que $x \in \mathcal{A}_k$, et on le note $\delta(x)$. On convient que $\delta(0_{\mathcal{A}}) = 0$. Ainsi, par la définition d'une algèbre $\mathbb{Z}/2$-graduée, on a pour a, b homogènes non nuls dans $\mathcal{A}$:*

$$\delta(a+b) \equiv \delta(a) + \delta(b)\,[2]$$

On peut aussi mettre une structure d'algèbre graduée sur le produit tensoriel $\mathcal{A} \otimes \mathcal{B}$ de deux algèbres $\mathbb{Z}/2$-graduées, $\mathcal{A}$ et $\mathcal{B}$.

Définition 10.0.4. *Soit $\mathcal{A}$ et $\mathcal{B}$, deux algèbres $\mathbb{Z}/2$-graduées. On définit une structure d'algèbre $\mathbb{Z}/2$-graduée sur le $\mathbb{K}$-espace vectoriel $\mathcal{A} \otimes \mathcal{B}$ de la manière suivante :*

- *Pour $(a, a, b, b') \in \mathcal{A}^2 \times \mathcal{B}^2$ où a' et b sont homogènes :*
$$(a \otimes b) \times (a' \otimes b') = (-1)^{\delta(b)\delta(a')}(aa') \otimes (bb')$$

On prolonge alors la loi $\times$ de manière unique sur $\mathcal{A}\otimes\mathcal{B}$ tout entier. On distingue alors dans la $\mathbb{K}$-algèbre $(\mathcal{A} \otimes \mathcal{B}, +, ., \times)$ les sous-espaces vectoriels :

$$(\mathcal{A} \otimes \mathcal{B})_0 = (\mathcal{A}_0 \otimes \mathcal{B}_0) \oplus (\mathcal{A}_1 \otimes \mathcal{B}_1) \text{ et } (\mathcal{A} \otimes \mathcal{B})_1 = (\mathcal{A}_1 \otimes \mathcal{B}_0) \oplus (\mathcal{A}_0 \otimes \mathcal{B}_1)$$

L'algèbre $\mathbb{Z}/2$-graduée ainsi définie est noté $\mathcal{A}\widehat{\otimes}\mathcal{B}$ et est appelé le produit tensoriel gradué de $\mathcal{A}$ et $\mathcal{B}$.

Remarque 10.0.1. *Lorsqu'une des algèbres $\mathcal{A}$ et $\mathcal{B}$ est trivialement graduée, l'algèbre $\mathcal{A}\widehat{\otimes}\mathcal{B}$ est précisément le produit tensoriel habituel $\mathcal{A}\otimes\mathcal{B}$. En effet, on a alors*

$$\mathcal{A} = \mathcal{A}_0 \text{ ou } \mathcal{B} = \mathcal{B}_0$$

et donc :

$$\forall a \in \mathcal{A},\ \delta(a) = 0 \text{ ou } \forall b \in \mathcal{B},\ \delta(b) = 0$$

qui montre que la définition du produit $\times$ sur $\mathcal{A}\widehat{\otimes}\mathcal{B}$ est la définition usuelle de la loi $\times$ sur le produit tensoriel $\mathcal{A}\otimes\mathcal{B}$.

Nous sommes désormais en mesure de définir l'algèbre de Clifford $C(q)$ associé à un espace quadratique (E, q).

10.0.5 Construction des algèbres de Clifford

On note $T(E)$ l'algèbre tensorielle associé au $\mathbb{K}$-espace vectoriel E, alors,

$$T(E) = \bigoplus_{k\geq 0} T^k(E)$$

et est munie d'une structure d'algèbre $\mathbb{Z}/2$-graduée en distinguant dans $T(E)$ les sous-espaces,

$$T_0(E) = \bigoplus_{k\geq 0} T^{2k}(E) \text{ et } T_1(E) = \bigoplus_{k\geq 0} T^{2k+1}(E).$$

On note $I(q)$ l'idéal bilatère de $T(E)$ engendré par les éléments de la forme :

$$(x_1 \otimes \ldots \otimes x_n \otimes x \otimes x \otimes y_1 \otimes \ldots \otimes y_m) - q(x).x_1 \otimes \ldots \otimes x_n \otimes y_1 \otimes \ldots \otimes y_m$$

pour un couple $(m, n) \in \mathbb{N}^2$ et une famille finie $(x, x_1, \ldots, x_n, y_1, \ldots, y_m)$. On a alors :

$$I(q) = (I(q) \cap T_0(E)) \oplus (I(q) \cap T_1(E))$$

ce qui permet de munir $T(E)/I(q) = (T_0(E)/I(q)) \oplus (T_1(E)/I(q))$ d'une structure d'algèbre graduée avec :

$$(T(E)/I(q))_0 = (T_0(E)/I(q)) \text{ et } (T(E)/I(q))_1 = (T_1(E)/I(q)).$$

Ainsi pour $x \in E$, on annule tous les éléments de la forme $x \otimes x - q(x)1$ dans le quotient $T(E)/I(q)$.

Définition 10.0.5. *Soit (E, q) un espace quadratique. L'algèbre unitaire quotient $T(E)/I(q)$ est munie d'une structure d'algèbre $\mathbb{Z}/2$-graduée notée $C(q)$ et appelée* ***l'algèbre de Clifford*** *associée à q.*

Le $\mathbb{K}$-espace vectoriel E est générateur de l'algèbre tensorielle $T(E)$ en tant qu'algèbre et est naturellement vu comme un sous-espace de $T(E)$. On peut de même voir E comme un sous-espace de l'algèbre de Clifford $C(q)$:

Notation 10.0.1. *Soit (E, q) un espace quadratique, on note μ_E la restriction à E de la projection canonique $T(E) \twoheadrightarrow T(E)/I(q)$. Il s'agit d'un morphisme de $\mathbb{K}$-espaces vectoriels et comme E engendre $T(E)$ en tant qu'algèbre, $\mu_E(E)$ engendre $C(q)$ en tant qu'algèbre. On note en toute rigueur $\overline{x}$ l'image d'un élément $x \in E$ par $C(q)$.*

Proposition 10.0.3. *L'application μ_E est injective. Ainsi, E peut-être vu comme un sous-ensemble de $C(q)$ et avec cette identification E engendre $C(q)$ en tant qu'algèbre.*

Remarque 10.0.2. *Dans la suite il sera commode de noter toujours x l'élement $\overline{x}$ image de x par μ_E. Ainsi, avec cette identifcation on considérera les élements de E comme des éléments de $C(q)$.*

Remarque 10.0.3. *Par définition même de $C(q)$, on a :*

$$\forall x \in E,\ \mu_E(x)^2 = \overline{x}^2 = q(x)1_{C(q)}$$

Propriétés universelles des algèbres de Clifford

Les deux propositions suivantes sont des propriétés universelles des algèbres de Clifford et nous serons utiles pour définir des morphismes ayant pour source une algèbre de Clifford, ou plus généralement pour définir des morphismes entre algèbres de Clifford.

Proposition 10.0.4. *Soit (E, q) un espace quadratique et $\mathcal{A}$ une algèbre (associative,unitaire) sur $\mathbb{K}$, avec $\alpha : E \longrightarrow \mathcal{A}$ un morphisme de $\mathbb{K}$-espaces vectoriels. On suppose que :*

$$\forall x \in E, \alpha(x)^2 = q(x)1_{\mathcal{A}}$$

alors il existe un unique morphisme d'algèbre prolongeant α sur $C(q)$ noté $\widehat{\alpha}$: $C(q) \longrightarrow \mathcal{A}$ tel que :

$$\forall x \in E,\ \widehat{\alpha}(\mu_E(x) = \widehat{\alpha}(\overline{x}) = \alpha(x)$$

que l'on peut encore noter avec l'identification :

$$\forall x \in E,\ \widehat{\alpha}(x) = \alpha(x)$$

De plus, si $\mathcal{A}$ est $\mathbb{Z}/2$-graduée et l'image de α inclus dans $\mathcal{A}_1$, alors $\widehat{\alpha}$ est un morphisme d'algèbres $\mathbb{Z}/2$-graduées.

Remarque 10.0.4. *Puisque le morphisme α de la proposition précédente est un morphisme de $\mathbb{K}$-espace vectoriels, il préserve en particulier la loi $+$ et donc :*

$$\forall x, y \in E,\ \alpha(x+y)^2 = \alpha(x)^2 + \alpha(x)\alpha(y) + \alpha(y)\alpha(x) + \alpha(y)^2$$

et la condition :

$$\forall x \in E, \alpha(x)^2 = q(x)1_{\mathcal{A}}$$

est alors équivalente par polarisation à :

$$\forall x, y \in E,\ \alpha(x)\alpha(y) + \alpha(y)\alpha(x) = 2b_q(x, y).1_{\mathcal{A}}$$

Ainsi, puisque $\overline{x}^2 = q(x)1_{C(q)}$ on a :

$$\overline{x}\,\overline{y} + \overline{y}\,\overline{x} = 2b_q(x,y)$$

et deux vecteurs orthogonaux de E deviennent deux vecteurs qui anticommutent dans $C(q)$.

On en déduit le corollaire suivant, utile pour établir l'existence de morphismes entre algèbres de Clifford :

Corollaire 10.0.2. *Soit $f : (E,q) \longrightarrow (E',q')$ un morphisme d'espaces quadratiques, c'est-à-dire, une application linéaire de $E \longrightarrow E'$ vérifiant :*

$$\forall x \in E, q'(f(x)) = q(x).$$

Il existe alors un unique morphisme d'algèbres $\mathbb{Z}/2$-graduées :

$$C(f) : C(q) \longrightarrow C(q')$$

tel que :

$$\forall x \in E, C(f)(\mu_E(x)) = C(f)(\overline{x}) = \overline{f(x)} = \mu_{E'}(f(x)).$$

Ce corollaire nous permet d'obtenir le résultat essentiel suivant :

Corollaire 10.0.3. *Les algèbres de Clifford associées à des espaces quadratiques isomorphes sont isomorphes en tant qu'algèbres $\mathbb{Z}/2$-graduées. Ainsi*

$$q \simeq q' \Longrightarrow C(q) \simeq_{\mathbb{Z}/2} C(q')$$

où la notion $\simeq_{\mathbb{Z}/2}$ est utilisée pour désigner un isomorphisme d'algèbres $\mathbb{Z}/2$-graduées

Démonstration. Soit (E,q) et (E',q') deux espaces quadratiques isomorphes. Il existe un isomorphisme $u : E \longrightarrow E'$ tel que :

$$\forall x \in E,\ q'(u(x)) = q(x) \text{ et } \forall x' \in E',\ q(u^{-1}(x')) = q'(x')$$

Alors, il existe deux uniques morphismes d'algèbres $\mathbb{Z}/2$-graduées $C(u)$ et $C(u^{-1})$ tels que :

$$\forall x \in E, C(u)(\overline{x}) = \overline{u(x)} \text{ et } \forall x' \in E', C(u^{-1})(\overline{x'}) = \overline{u^{-1}(x')}$$

soit en particulier, $\forall x \in E$:

$$\begin{aligned} C(u^{-1}) \circ C(u)(\overline{x}) &= C(u^{-1})(\overline{u(x)}) \\ &= \overline{u^{-1}(u(x))} \\ &= \overline{x} \end{aligned}$$

et $\forall x' \in E'$:

$$\begin{aligned} C(u) \circ C(u^{-1})(\overline{x'}) &= C(u)(\overline{u^{-1}(x)'}) \\ &= \overline{u(u^{-1}(x'))} \\ &= \overline{x'} \end{aligned}$$

Ainsi $C(u) \circ C(u^{-1}) = Id$ sur la partie génératrice $\mu_{E'}(E')$ identifiée à E' donc sur $C(q')$ tout entier ($C(u)$ et $C(u^{-1})$ étant des morphismes d'algèbres) et $C(u^{-1}) \circ C(u) = Id$ sur la partie génératrice $\mu_E(E)$ identifiée à E donc sur $C(q)$ tout entier. Ainsi $C(u)$ et $C(u^{-1})$ étant gradués on a :

$$C(q) \simeq_{\mathbb{Z}/2} C(q')$$

□

Remarque 10.0.5. *Ainsi, puisqu'on on cherche à raisonner à équivalence près dans le monde des formes quadratiques, il est rassurant de voir qu'alors on raisonnera à isomorphisme gradué près dans le monde des algèbres de Clifford. Par exemple, un choix de diagonalisation pour une forme quadratique régulière q ne perturbera $C(q)$ qu'à isomorphisme gradué près.*

10.0.6 Algèbres de Clifford en dimension 1

Intéressons nous désormais aux algèbres de Clifford associées à des espaces quadratiques de dimension 1. On note E un $\mathbb{K}$-espace vectoriel de dimension 1 dont $\{v\}$ est une base. On définit alors $q : E \longrightarrow \mathbb{K}$ par, $q(v) = a$ et $\forall \lambda \in \mathbb{K}$:

$$q\colon \begin{cases} E \longrightarrow \mathbb{K} \\ \lambda v \longmapsto \lambda^2 a \end{cases}$$

Ainsi, (E, q) est en particulier isomorphe à $(\mathbb{K}, \langle a \rangle)$. Définissons alors l'application linéaire f sur E par :

$$f\colon \begin{cases} E \longrightarrow \mathbb{K}[X] \\ v \longmapsto X \end{cases}$$

qui détermine uniquement f, car définie sur la base $\{v\}$ de E. Alors par les propriétés universelles de l'algèbre tensorielle $T(E) = T(vect(v))$, il existe un unique morphisme d'algèbre sur $T(E)$ à valeurs dans $\mathbb{K}[X]$ prolongeant f sur $T(E)$ (avec l'identification $E \hookrightarrow T(E)$) noté $\overline{f}$ et tels que :

$$\forall n \in \mathbb{N},\ \overline{f}(\underbrace{v \otimes \ldots \otimes v}_{\times n}) = X^n$$

Alors $\overline{f}$ est bijectif, de bijection réciproque associée, l'application :

$$g\colon \begin{cases} \mathbb{K}[X] \longrightarrow T(E) \\ P(X) = a_0 + a_1 X + \ldots + a_n X^n \longmapsto a_0 + a_1 v + \ldots + a_n v \otimes \ldots \otimes v \end{cases}$$

Mettons alors une graduation sur $\mathbb{K}[X]$. Tout polynome $P \in \mathbb{K}[X]$, s'écrit de manière unique :

$$P(X) = a_0 + a_1 X + \ldots + a_n X^n \text{ pour } a_n \neq 0$$

et donc peut se décomposer sous la forme :

- si $n = 2l$ est pair,
  $P(X) = (a_0 + a_2 X^2 + a_4 X^4 + \ldots + a_{2l} X_{2l}) + X(a_1 + a_3 X_2 + \ldots a_{2l-1} X^{2(l-1)})$
- si $n = 2l + 1$ est impair,
  $P(X) = (a_0 + a_2 X^2 + a_4 X^4 + \ldots + a_{2l} X_{2(l-1)}) + X(a_1 + a_3 X_2 + \ldots a_{2l+1} X^{2l})$

ce qui montre par unicité d'écriture dans la base $(X^n)_{n\in\mathbb{N}}$ de $\mathbb{K}[X]$ que :

$$\mathbb{K}[X] = \mathbb{K}[X^2] + X\mathbb{K}[X^2],$$

où $\mathbb{K}[X^2]$ et $X\mathbb{K}[X^2]$ sont deux sous-espaces vectoriels de $\mathbb{K}[X]$. De plus, on a :

- $1 \in \mathbb{K}[X^2]$
- $\mathbb{K}[X^2]\mathbb{K}[X^2] \subset \mathbb{K}[X^2]$
- $\mathbb{K}[X^2]X\mathbb{K}[X^2] \subset X\mathbb{K}[X^2]$
- $X\mathbb{K}[X^2]X\mathbb{K}[X^2] \subset \mathbb{K}[X^2]$

Ce qui montre que $\mathbb{K}[X]$ est bien graduée par $\mathbb{K}[X] = \mathbb{K}[X^2] + X\mathbb{K}[X^2]$, avec :

$$\mathbb{K}[X]_0 = \mathbb{K}[X^2] \text{ et } \mathbb{K}[X]_1 = X\mathbb{K}[X^2]$$

$T(E)$ étant graduée par $T_0(E) = \bigoplus_{k\geq 0} T^{2k}(E)$ et $T_1(E) = \bigoplus_{k\geq 0} T^{2k+1}(E)$, l'isomorphsime d'algèbre $\overline{f}$ est un isomorphisme d'algèbres graduées, puisqu'on a alors naturellement :

$$\overline{f}(T_0(E)) \subset \mathbb{K}[X]_0 = \mathbb{K}[X^2] \text{ et } \overline{f}(T_1(E)) \subset \mathbb{K}[X]_1 = X\mathbb{K}[X^2]$$

De plus, E étant de dimension 1 engendré par v, $I(q)$ est alors l'idéal de $T(E)$ engendré par : $\{\underbrace{v \otimes \ldots \otimes v}_{\times n} - q(v)\underbrace{v \otimes \ldots \otimes v}_{\times n-2}, n \geq 2\}$ et donc via l'isomorphisme $\overline{f}$, $I(q)$ est envoyé sur l'idéal de $\mathbb{K}[X]$ engendré par $\{X^n - aX^{n-2}, n \geq 2\}$ soit l'idéal engendré $X^2 - a$ que l'on note usuellement $(X^2 - a)$. D'où, $\overline{f}$ étant un isomorphisme, on a :

$$\overline{f}(T(E))/(\overline{f}(I(q)) \simeq T(E)/I(q) \Longrightarrow C(q) \simeq K[X]/(X^2 - a)$$

où $\mathbb{K}[X]/(X^2 - a)$ est graduée par :

$$(\mathbb{K}[X]/(X^2 - a))_0 = \mathbb{K}[X^2]/(X^2 - a) \text{ et } (\mathbb{K}[X]/(X^2 - a))_0 = X\mathbb{K}[X^2]/(X^2 - a)$$

Proposition 10.0.5. *Soit $a \in \mathbb{K}^*$ et (E, q) espace quadratique de dimension 1 isomorphe à $(\mathbb{K}, \langle a \rangle)$, alors :*

$$C(q) \simeq \mathbb{K}[X]/(X^2 - a) \text{ et } C_0(q) \simeq \mathbb{K}$$

Démonstration. Le premier résultat a déjà été démontré dans l'étude préliminaire. Quant au deuxième isomorphisme, il découle du fait que $\overline{f}$ étant un morphisme graduée on a encore :

$$C_0(q) \simeq (\mathbb{K}[X]/(X^2 - a))_0 = \mathbb{K}[X^2]/(X^2 - a)$$

Dans $\mathbb{K}[X]/(X^2 - a)$, on a $\overline{X^2} = \overline{a}$, ce qui nous incite à définir ϕ par :

$$\phi\colon \begin{cases} \mathbb{K}[X^2] \longrightarrow \mathbb{K} \\ P(X) = a_0 + a_1X^2 + \ldots + a_nX^{2n} \longmapsto a_0 + a_1a + \ldots + a_na^n \end{cases}$$

Alors ϕ est un morphisme surjectif, de noyau $(X_2 - a)\mathbb{K}[X^2]$. En effet, si on suppose que $a_0 + a_1a + \ldots + a_{2n}a^n = 0$, on a alors :

$$P(X) = a_0 + a_1X^2 + \ldots + a_nX^{2n} = \\ a_1(X^2 - a) + a_2(X^4 - a^2) + \ldots + a_n(X^{2n} - a^n) \in (X_2 - a)\mathbb{K}[X^2]$$

Enfin, il est immédiat que $(X^2 - a)\mathbb{K}[X^2] \subset Ker(\phi)$ et donc par conséquent :

$$\mathbb{K}[X^2]/(X^2 - a) \simeq \mathbb{K}$$

□

On en déduit alors immédiatement,

Corollaire 10.0.4.

- *Si* $a \notin (\mathbb{K}^*)^2$, $C(q) \simeq \mathbb{K}[\sqrt{a}]$ *où* $\mathbb{K}[\sqrt{a}]$ *est graduée par la décomposition* $\mathbb{K} \otimes \sqrt{a}\mathbb{K}$.
- *Si* $a \in (\mathbb{K}^*)^2$, $C(q) \simeq \mathbb{K} \times \mathbb{K}$ *où l'algèbre produit* $\mathbb{K} \times \mathbb{K}$ *est graduée par la décomposition :*

$$(\mathbb{K} \times \mathbb{K})_0 = \{(x, x), x \in \mathbb{K}\} \text{ et } (\mathbb{K} \times \mathbb{K})_1 = \{(x, -x), x \in \mathbb{K}\}$$

En particulier $C(q)$ *a une structure de* $\mathbb{K}$*-espace vectoriel de dimension* 2

Le dernier résultat important concernant les algèbres de Clifford en dimension 1 est le fait que la structure d'algèbre (non graduée) de l'algèbre $C(q)$ détermine q à équivalence près. On verra par la suite, notamment via l'étude en dimension 2, 3 et 4 que cela n'est pas vrai en général.

Proposition 10.0.6. *Soit* (E, q) *et* (E', q') *deux droites quadratiques régulières. On a alors :*

$$C(q) \simeq C(q') \iff q \simeq q'$$

Remarque 10.0.6. *Puisque* $q \simeq q' \implies C(q) \simeq_{\mathbb{Z}/2} C(q')$*, en dimension* 1*, si* $C(q) \simeq C(q')$ *alors nécessairement* $C(q)$ *et* $C(q')$ *sont aussi isomorphes en tant qu'algèbres graduées, ce qui est un résultat plus fort.*

10.0.7 Décomposition d'une algèbre de Clifford

A la section précédente, nous avons étudié les algèbres de Clifford associées à des espaces quadratiques de dimension 1. Dans cette partie, nous allons donner un théorème qui permet de décomposer toute algèbre de Clifford de dimension n en un produit tensoriel gradué d'algèbres de Clifford de dimension 1 et donc d'aborder l'étude des algèbres de Clifford en dimension supérieure. Pour ce faire, on va utiliser le fait que pour toute forme quadratique régulière q de dimension n, il existe des éléments $a_1, \ldots, a_n \in \mathbb{K}^*$ tels que que $q \simeq \langle a_1, \ldots, a_n \rangle$ et qu'alors :

$$C(q) \simeq_{\mathbb{Z}/2} C\langle a_1, \ldots, a_n \rangle \simeq_{\mathbb{Z}/2} C(\langle a_1 \rangle \perp \ldots \langle a_n \rangle)$$

Ainsi, si on arrive à décomposer l'algèbre $C(q \perp q')$ comme un produit tensoriel gradué des algèbres, $C(q)$ et $C(q')$, on aura atteint notre objectif.

Proposition 10.0.7. *Soit* (E, q) *et* (E', q') *deux espaces quadratiques réguliers. Alors :*

$$C(q \perp q') \simeq_{\mathbb{Z}/2} C(q) \widehat{\otimes} C(q')$$

Ce qui donne alors immédiatement :

Corollaire 10.0.5. *Pour* $a_1, \ldots, a_n \in \mathbb{K}^*$*, on a :*

$$C\langle a_1, \ldots, a_n \rangle \simeq_{\mathbb{Z}/2} C\langle a_1 \rangle \widehat{\otimes} \ldots \widehat{\otimes} C\langle a_n \rangle$$

L'étude des algèbres de Clifford de dimension 1, nous montre alors que tout algèbre de Clifford est à isomorphisme gradué près, un produit tensoriel gradué d'algèbres de Clifford de droites quadratiques, chacune étant isomorphe à $\mathbb{K}[\sqrt{(a)}]$ pour $a \in \mathbb{K}^*$ ou $\mathbb{K} \times \mathbb{K}$. Comme pour E, F deux $\mathbb{K}$-espaces vectoriels on a $dim(E \otimes F) = dim(E)dim(F)$, il vient :

$$\text{si } dim(q) = n > 0 \text{ alors } dim(C(q)) = 2^n$$

On verra d'autres résultats relatifs à la dimension d'une algèbre de Clifford dans la section suivante.

10.0.8 Dimension et base d'une algèbre de Clifford

Notation 10.0.2. *Soit $(e_1, e_2, \ldots, e_n)$ une famille de vecteurs d'un espace quadratique (E, q), Pour tout $I = \{i_1, \ldots, i_p\} \subset [\![1, n]\!]$ avec $i_1 < i_2 < \ldots < i_p$, on note :*

$$e_I = \prod_{i=1}^{p} \overline{e_{i_k}}$$

que l'on peut aussi noter plus commodément, (comme $E \hookrightarrow C(q)$) :

$$e_I = \prod_{i=1}^{p} e_{i_k}$$

Les résultats essentiels concernant la dimension de l'algèbre de Clifford sont regroupés dans le théorème suivant :

Théorème 10.0.2. *Soit (E, q) un espace quadratique de dimension $n > 0$. Alors, l'algèbre de Clifford $C(q)$ est de dimension 2^n et pour $(e_1, \ldots, e_n)$ base de E, on a :*

- *la famille $(e_I)_{I \subset [\![1,n]\!]}$ est une base de $C(q)$*
- *$C_0(q)$ est de dimension 2^{n-1} et l'ensemble des e_I pour I partie de cardinal pair de $[\![1, n]\!]$ en est une base.*
- *$C_1(q)$ est de dimension 2^{n-1} et l'ensemble des e_I pour I partie de cardinal impair de $[\![1, n]\!]$ en est une base.*

10.0.9 Partie paire et centre d'une algèbre de Clifford

Centre d'une algèbre de Clifford

Notation 10.0.3. *Soit (E, q) un espace quadratique régulier. On notera $\mathcal{Z}(q)$ le centre de l'algèbre de Clifford, c'est-à-dire l'ensemble des éléments qui commutent à tous les autres pour la loi interne $\times$ de $C(q)$.*

Avant de passer à l'énonciation du théorème de structure relatif au centre de l'algèbre de Clifford, faisons d'abord quelques remarques bien utiles.

Remarque 10.0.7. *Pour $(e_1, \ldots, e_n)$ une base orthogonale de (E, q), nous savons d'après la section précédente que $\boldsymbol{B} = (e_I)_{I \subset [\![1,n]\!]}$ est une base de l'espace vectoriel $C(q)$. Ainsi $(e_i)_{1 \leq i \leq n}$ est une famille génératrice de $C(q)$ en tant qu'algèbre et donc pour qu'un élément x de $C(q)$ commute à tous les autres, il faut et il suffit qu'il commute avec tous les e_i. Pour étudier le centre $\mathcal{Z}(q)$, il suffit alors d'étudier comment les vecteurs e_I de la base de $C(q)$ se comporte vis à vis des éléments e_i. Or $(e_1, \ldots, e_n)$ étant une base q-othogonale, en utilisant l'identification usuelle $E \hookrightarrow C(q)$, on a :*

$$\forall i \neq j,\ e_i e_j + e_j e_i = 2b_q(e_i, e_j) = 0$$

et les vecteurs e_i anticommutent deux à deux. Ainsi, pour tout $i \in [\![1, n]\!]$ et toute partie $I \subset [\![1, n]\!]$, on a :

$$e_i e_I = (-1)^{card(I \setminus \{i\})} e_I e_i$$

On en déduit ainsi que :

- *$C(q) \neq \mathcal{Z}(q)$ puisque pour tout I non trivial, il existe un indice i tel que e_i et e_I anticommutent. Il suffit de prendre i dans I si $card(I)$ est pair car ainsi $(-1)^{card(I \setminus \{i\})} = -1$ et de prendre i dans $[\![1, n]\!] \setminus I$ si I est de cardinal impair avec toujours ainsi $(-1)^{card(I \setminus \{i\})} = -1$.*

- *si n est impair, alors $e_1e_2 \times \ldots \times e_n$ commute avec e_i pour tout $i \in [\![1, n]\!]$, donc est dans $\mathcal{Z}(q)$*
- *si n est pair alors $e_1e_2 \times \ldots \times e_n$ anticommute avec e_i pour tout $i \in [\![1, n]\!]$*

Passons à l'énonciation du théorème de structure du centre d'une algèbre de Clifford.

Théorème 10.0.3. ***théorème de structure du centre d'une algèbre de Clifford***
Soit (E, q) un espace quadratique régulier de dimension $n > 0$. On a :

1. *si n est pair, alors $\mathcal{Z}(q) = \mathbb{K}$.*
2. *si n est impair, $\mathcal{Z}(q)$ est un $\mathbb{K}$-espace vectoriel de dimension 2, dont $(1, e_1e_2 \times \ldots \times e_n)$ est une base, pour $(e_1, \ldots, e_n)$ base q-othogonale de E. Enfin, $\mathcal{Z}(q)$ est isomorphe en tant qu'algèbre $\mathbb{Z}/2$-graduée à $C\langle\delta\rangle$ pour δ un discriminant de q.*

Corollaire 10.0.6. *Soit q une forme quadratique régulière. Alors,*

$$C_0(q) \cap \mathcal{Z}(q) = \mathbb{K}.$$

Partie paire d'une algèbre de Clifford

Soit (E, q) un espace quadratique régulier de dimension n. Le résultat essentiel de cette partie est le fait que la partie paire $C_0(q)$ d'une algèbre de Clifford est elle-même isomorphe à une algèbre de Clifford. Le théorème suivant intitulé lemme de la partie paire, formalise ce résultat :

Théorème 10.0.4. ***Lemme de la partie paire***
Soit q une forme quadratique régulière de dimension n et $a \in \mathbb{K}^*$. On a alors les isomorphismes d'algèbres suivants :

$$C_0(q \perp \langle a \rangle) \simeq C(-aq)$$

et pour tout $(a_1, \ldots, a_n, a_{n+1}) \in (\mathbb{K}^*)^{n+1}$,

$$C_0\langle a_1, \ldots, a_n, a_{n+1}\rangle \simeq C\langle -a_1a_{n+1}, -a_2a_{n+1}, \ldots, -a_na_{n+1}\rangle$$

Précédemment, nous avons donc étudié la partie paire d'une algèbre de Clifford associée à un espace quadratique régulier (E, q). Nous avons alors constaté que selon la parité de la dimension de l'espace E, le centre de $C(q)$ était soit le corps de base $\mathbb{K}$, soit un espace de dimension 2 sur $\mathbb{K}$. Du lemme de la partie paire nous avons également tiré une information essentielle : la partie paire de toute algèbre de Clifford est elle-même isomorphe à une algèbre de Clifford. Dans les deux sections à venir, nous verrons deux applications de ces deux résultats majeurs.

Algèbre de Clifford et discriminant

La proposition suivante est un prolongement en toute dimension d'un résultat déjà établi dans le cadre de la dimension 1 : *"si $C(q_1)$ et $C(q_2)$ sont isomorphes alors q_1 et q_2 ont même discriminant"*, avec cette fois-ci l'hypothèse supplémentaire de l'isomorphisme gradué. Cette proposition aura une résonance toute particulière dans le cadre des corps finis.

Proposition 10.0.8. *Soit q_1, q_2 deux formes quadratiques régulières de même dimension. On suppose de plus que les algèbres de Clifford associées $C(q_1)$ et $C(q_2)$ sont isomorphes en tant qu'algèbres $\mathbb{Z}/2$-graduées, alors q_1 et q_2 ont même discriminant.*

Démonstration. On suppose dans un premier temps que q_1, q_2 sont deux formes quadratiques régulières de même dimension impaire. Alors, d'après l'étude du centre d'une algèbre de Clifford associée à une forme quadratique régulière, les centres $\mathcal{Z}(q_1)$ et $\mathcal{Z}(q_2)$ respectivement associés à $C(q_1)$ et $C(q_2)$ sont de dimension 2 et sont isomorphes respectivement aux algèbres $\mathbb{Z}/2$-graduées $C\langle\delta_1\rangle$ et $C\langle\delta_2\rangle$ où δ_1 est un discriminant de q_1 et δ_2 un discriminant de q_2. Or, puisque $C(q_1) \simeq C(q_2)$ en tant qu'algèbres (on n'utilise pas ici la structure d'algèbre graduée), les centres $\mathcal{Z}(q_1)$ et $\mathcal{Z}(q_2)$ sont naturellement isomorphes, ce qui implique :

$$\begin{aligned}
\mathcal{Z}(q_1) \simeq \mathcal{Z}(q_2) &\iff C\langle\delta_1\rangle \simeq C\langle\delta_2\rangle \\
&\iff \langle\delta_1\rangle \simeq \langle\delta_2\rangle \\
&\iff \delta_1 = \delta_2 \text{ dans } \mathbb{K}^*/(\mathbb{K}^*)^2 \\
&\iff \Delta(q_1) = \Delta(q_2)
\end{aligned}$$

en se souvenant qu'en dimension 1, les algèbres de Clifford sont isomorphes si et seulement si les formes quadratiques associées sont équivalentes. Les équivalences ci-dessus achèvent donc l'étude du cas où la dimension est impaire.

Désormais supposons, q_1 et q_2 de même dimension paire avec les algèbres de Clifford associées isomorphes en tant qu'algèbres $\mathbb{Z}/2$-graduées. En dimension paire, $C(q_1)$ et $C(q_2)$ sont centrales et il nous faut étudier les parties paires de ces algèbres de Clifford pour obtenir plus d'information. Par diagonalisation q_1 et q_2 étant de dimension $2n$, $n \in \mathbb{N}^*$, il existe des familles d'éléments non nuls de $\mathbb{K}$ notées $(a_i)_{1\leq i\leq 2n}$ et $(b_i)_{1\leq i\leq 2n}$ telles que $q_1 \simeq \langle a_1, a_2, \cdots, a_{2n}\rangle$ et $q_2 \simeq \langle b_1, b_2, \cdots, b_{2n}\rangle$. Alors, par le lemme de la partie paire, on a les résultats suivants :

1. $C(q_1) \simeq C\langle a_1, a_2, \cdots, a_{2n}\rangle$
2. $C(q_2) \simeq C\langle b_1, b_2, \cdots, b_{2n}\rangle$
3. $C_0\langle a_1, a_2, \cdots, a_{2n}\rangle \simeq C\langle -a_{2n}a_1, -a_{2n}a_2, \cdots, -a_{2n}a_{2n-1}\rangle$
4. $C_0\langle b_1, b_2, \cdots, b_{2n}\rangle \simeq C\langle -b_{2n}b_1, -b_{2n}b_2, \cdots, -b_{2n}b_{2n-1}\rangle$

Il faut ensuite utiliser le fait que les algèbres de Clifford $C(q_1)$ et $C(q_2)$ sont isomorphes en tant qu'algèbres graduées. En effet, l'isomorphisme Ψ entre $C(q_1)$ et $C(q_2)$ préserve la graduation, (ce qui est le cas ici) et assure que

$$\Psi(C_0(q_1)) \subset C_0(q_2),$$

avec $dim(C_0(q_1)) = dim(C_0(q_2)) = 2^{n-1}$, d'où $\Psi(C_0(q_1) = C_0(q_2)$ et par injectivité de Ψ, $C_0(q_1) \simeq C_0(q_2)$. Cet isomorphisme implique alors que :

$$C\langle -b_{2n}b_1, -b_{2n}b_2, \cdots, -b_{2n}b_{2n-1}\rangle \simeq C\langle -a_{2n}a_1, -a_{2n}a_2, \cdots, -a_{2n}a_{2n-1}\rangle.$$

Ainsi, d'après la première partie de la preuve, en dimension impaire, l'isomorphisme ci-dessus nous donne dans $\mathbb{K}^*/(\mathbb{K}^*)^2$:

$$\Delta(\langle -a_{2n}a_1, -a_{2n}a_2, \cdots, -a_{2n}a_{2n-1}\rangle) = \Delta(\langle -b_{2n}b_1, -b_{2n}b_2, \cdots, -b_{2n}b_{2n-1}\rangle)$$

avec

$$\begin{aligned}\Delta(\langle -a_{2n}a_1, -a_{2n}a_2, \cdots, -a_{2n}a_{2n-1}\rangle) &= (-1)^{2n-1}a_{2n}^{2n-1}a_1a_2\cdots a_{2n-1}\\ &= -a_{2n}^{2n-1}a_1a_2\cdots a_{2n-1}\\ &= -(a_{2n}^2)a_{2n}^{2n-1}a_1a_2\cdots a_{2n-1}\\ &= -a_{2n}^{2n+1}a_1a_2\cdots a_{2n-1}\\ &= -a_{2n}a_1a_2\cdots a_{2n-1}\\ &= -det(\langle a_1, a_2, \cdots, a_{2n}\rangle)\end{aligned}$$

et

$$\begin{aligned}\Delta(\langle -b_{2n}b_1, -b_{2n}b_2, \cdots, -b_{2n}b_{2n-1}\rangle) &= (-1)^{2n-1}b_{2n}^{2n-1}b_1b_2\cdots b_{2n-1}\\ &= -b_{2n}^{2n-1}b_1b_2\cdots b_{2n-1}\\ &= -(b_{2n}^2)b_{2n}^{2n-1}b_1b_2\cdots b_{2n-1}\\ &= -b_{2n}^{2n+1}b_1b_2\cdots b_{2n-1}\\ &= -b_{2n}b_1b_2\cdots b_{2n-1}\\ &= -det(\langle b_1, b_2, \cdots, b_{2n}\rangle)\end{aligned}$$

On a donc, en particulier dans $\mathbb{K}^*/(\mathbb{K}^*)^2$:

$$\begin{aligned}det(\langle a_1, a_2, \cdots, a_{2n}\rangle) &= a_{2n}a_1a_2\cdots a_{2n-1}\\ &= b_{2n}b_1b_2\cdots b_{2n-1}\\ &= det(\langle b_1, b_2, \cdots, b_{2n}\rangle)\end{aligned}$$

et puisque $dim(\langle a_1, a_2, \cdots, a_{2n}\rangle) = dim(\langle b_1, b_2, \cdots, b_{2n}\rangle)$, les formes diagonales $\langle a_1, a_2, \cdots, a_{2n}\rangle$ et $\langle b_1, b_2, \cdots, b_{2n}\rangle$ ayant même déterminant, ont même discriminant. Ce qui nous donne également :

$$\Delta(q_1) = \Delta(q_2)$$

□

Remarque 10.0.8. *Dans le cadre des corps finis, on peut obtenir d'avantage de la proposition précédente. Si $\mathbb{K}$ est un corps fini, q_1, q_2 deux formes quadratiques régulières sur $\mathbb{K}$ telles que :*

$$dim(q_1) = dim(q_2) \text{ et } C(q_1) \simeq_{\mathbb{Z}/2} C(q_2)$$

alors q_1 et q_2 ont même discriminant et même dimension et sont donc équivalentes sur $\mathbb{K}$.

Passons désormais à la seconde application du théorème de structure du centre des algèbres de Clifford.

Application des algèbres de Clifford à l'étude d'isomorphismes d'algèbres

La proposition qui suit est une illustration de l'efficacité des résultats mentionnés ci-dessus pour prouver la non existence de certains isomorphismes d'algèbres notamment avec des algèbres de matrices.

Proposition 10.0.9. *Soit $n \in \mathbb{N}^*$, aucune algèbre de Clifford réelle associée à une forme quadratique régulière n'est isomorphe à $\mathcal{M}_n(\mathbb{C}) \times \mathcal{M}_n(\mathbb{C})$.*

Démonstration. Le centre de l'algèbre $\mathcal{M}_n(\mathbb{C})$ est l'ensemble des matrices complexes de tailles $n \times n$ qui commutent à toutes les autres. Un résultat bien connu est qu'il s'agit de l'ensemble $\{\lambda I_n, \lambda \in \mathbb{C}\}$ des matrices d'homothéties, où I_n désigne la matrice identité d'ordre n. Ainsi $Z(\mathcal{M}_n(\mathbb{C}) \times \mathcal{M}_n(\mathbb{C})) \simeq \mathbb{C} \times \mathbb{C}$. Supposons par l'absurde qu'il existe une forme quadratique réelle, régulière, q telle que $C(q) \simeq \mathcal{M}_n(\mathbb{C}) \times \mathcal{M}_n(\mathbb{C})$, alors :

- Si $dim(q)$ est paire, $\mathcal{Z}(q)$ est isomorphe à $\mathbb{R}$.
- Si $dim(q)$ est impaire, alors $C(q)$ a pour centre un $\mathbb{R}$-espace vectoriel de dimension 2.

Ainsi dans les deux cas, par raison de dimension le centre $\mathcal{Z}(q)$ ne peut pas être isomorphe à $\mathbb{C} \times \mathbb{C}$ de dimension 4 sur $\mathbb{R}$, ce qui montre le résultat. □

Voici désormais une application encore plus usuelle du lemme de la partie paire. En fournissant un isomorphisme d'algèbre entre la partie paire d'une algèbre de Clifford associée à une certaine forme quadratique q_1 et l'algèbre de Clifford d'une autre forme quadratique q_2, ce lemme fondamental nous offre évidemment un outil naturel pour montrer des isomorphismes de $\mathbb{K}$-algèbres entre algèbres de Clifford. Ceci, permet notamment de montrer qu'en dehors de la dimension 1, deux formes quadratiques non équivalentes peuvent avoir des algèbres de Clifford qui sont elles, isomorphes. En voici une illustration simple :

Proposition 10.0.10. *Les $\mathbb{R}$-algèbres de Clifford $C_{4,0}$ et $C_{1,3}$ respectivement associées aux espaces quadratiques réguliers réels standards de signatures $(4,0)$ et $(1,3)$ sont isomorphes en tant que $\mathbb{R}$-algèbres.*

Pour montrer ce résultat on aura besoin du lemme suivant :

Lemme 10.0.1. *Les parties paires $C_0(q)$ et $C_0(aq)$ sont isomorphes pour q une forme quadratique régulière sur $\mathbb{K}$ de dimension au moins 2 et $a \in \mathbb{K}^*$.*

Démonstration. Puisque q est régulière de dimension au moins 2, par diagonalisation, il existe des éléments $a_1, \ldots, a_n \in \mathbb{K}^*$ tels que :

$$q \simeq \langle a_1, a_2, \cdots, a_n \rangle \text{ et } aq \simeq \langle aa_1, aa_2, \cdots, aa_n \rangle$$

Ainsi $C(q)$ et $C\langle a_1, a_2, \cdots, a_n \rangle$ sont isomorphes en tant qu'algèbres $\mathbb{Z}/2$-graduées, tout comme $C(aq)$ et $C\langle aa_1, aa_2, \cdots, aa_n \rangle$, ce qui implique en particulier que les parties paires associées sont elles aussi isomorphes. D'où :

$$C_0(q) \simeq C_0\langle a_1, a_2, \cdots, a_n \rangle \text{ et } C_0(aq) \simeq C_0\langle aa_1, aa_2, \cdots, aa_n \rangle$$

On utilise alors le lemme de la partie paire ($n \geq 2$), qui nous donne :

1. $C_0\langle a_1, a_2, \cdots, a_n \rangle \simeq C\langle -a_n a_1, -a_n a_2, \cdots, -a_n a_{n-1} \rangle$.
2. $C_0\langle aa_1, aa_2, \cdots, aa_n \rangle \simeq C\langle -a^2 a_n a_1, -a^2 a_n a_2, \cdots, -a^2 a_n a_{n-1} \rangle$.

Or $\forall i \in [\![1, n-1]\!]$, $-a^2 a_i a_n = -a_i a_n$ dans $\mathbb{K}^*/(\mathbb{K}^*)^2$ et donc :

$$C\langle -a_n a_1, -a_n a_2, \cdots, -a_n a_{n-1} \rangle \simeq C\langle -a^2 a_n a_1, -a^2 a_n a_2, \cdots, -a^2 a_n a_{n-1} \rangle$$

ce qui donne d'après les points 1 et 2 ci-dessus

$$C_0\langle a_1, a_2, \cdots, a_n \rangle \simeq C_0\langle aa_1, aa_2, \cdots, aa_n \rangle$$

puis $C_0(q) \simeq C_0(aq)$. □

Passons désormais à la démonstration de la proposition.

Démonstration. On considère les formes quadratiques diagonales réelles $\langle 1,1,1,1\rangle$ et $\langle 1,-1,-1,-1\rangle$, de signatures $(4,0)$ et $(1,3)$. Par le lemme de la partie paire appliqué à $a=-1$:

$$\begin{aligned} C\langle 1,1,1,1\rangle &\simeq C(-(-1)\langle 1,1,1,1\rangle) \\ &\simeq C_0(\langle 1,1,1,1\rangle \perp \langle -1\rangle) \\ &\simeq C_0\langle 1,1,1,1,-1\rangle \end{aligned}$$

et

$$\begin{aligned} C\langle 1,-1,-1,-1\rangle &\simeq C(-(-1)\langle 1,-1,-1,-1\rangle) \\ &\simeq C_0(\langle 1,-1,-1,-1\rangle \perp \langle -1\rangle) \\ &\simeq C_0\langle 1,-1,-1,-1,-1\rangle \end{aligned}$$

Or $-1\langle 1,1,1,1,-1\rangle \simeq \langle 1,-1,-1,-1,-1\rangle$ donc d'après le lemme ci-dessus on a $C_0\langle 1,1,1,1,-1\rangle \simeq C_0\langle 1,-1,-1,-1,-1\rangle$, d'où $C\langle 1,1,1,1\rangle \simeq C\langle 1,-1,-1,-1\rangle$. □

Chapitre 11

Application de l'étude des algèbres de Clifford à la classification des formes quadratiques sur les corps p-adiques et sur le corps $\mathbb{Q}$

Le but de ce chapitre est de réussir à classifier les formes quadratiques p-adiques et rationnelles via l'algèbre de Clifford associée. Pour ce faire, il nous faudra nous intéresser aux algèbres de Clifford en dimension 2 (algèbres de quaternions), 3 et 4 pour lesquelles, nous classifierons les formes quadratiques régulières par l'algèbre de Clifford associée. L'outil important de ce chapitre sera le lemme de dévissage qui associé aux résultats du chapitre précédent nous permettra de décomposer une algèbre de Clifford donnée, en la présentant selon la parité de la dimension, soit sous la forme d'un produit tensoriel d'algèbres de quaternions, soit sous la forme d'un produit tensoriel d'algèbres de quaternions et d'une algèbre de Clifford associée à une forme quadratique régulière de dimension 1. Nous exhiberons alors sans les démonstrations, (pour les démonstrations cf.[1] XXV) des théorèmes généraux de structures de ces algèbres en dimension paire et impaire que nous exploiterons notamment pour décrire la structure des algèbres de Clifford des formes quadratiques régulières définies sur les corps finis. Enfin, nous aborderons la question de la structure des algèbres de Clifford des formes hyperboliques, ce qui nous permettra d'avoir en main tous les ingrédients et outils nécessaires à la démonstration des deux grands résultats de ce chapitre :

- Pour ϕ et ψ deux formes quadratiques régulières définies sur $\mathbb{Q}_p$ où $p \in \mathcal{P}$:
$$\phi \simeq \psi \Longleftrightarrow C(\phi) \simeq_{\mathbb{Z}/2} C(\psi)$$
- Pour q et q' deux formes quadratiques rationnelles régulières :
$$\textit{Si } C(q) \simeq_{\mathbb{Z}/2} C(q') \textit{ et si } q \textit{ et } q' \textit{ ont même signature alors } q \simeq q'$$

Ceci nous permettra d'obtenir une nouvelle façon de classifier les formes quadratiques rationnelles et clôturera notre voyage à travers le monde des formes quadratiques.

11.0.10 Algèbres de quaternions

Définition 11.0.6. *Soit a, b deux éléments non nuls du corps $\mathbb{K}$, l'algèbre de Clifford $C\langle a, b\rangle$ associée à la forme quadratique $\langle a, b\rangle$ est notée (a, b). Ces algèbres sont appelées les* ***algèbres de quaternions****.*

Dans la suite nous allons voir quelques propriétés de ces algèbres de quaternions, notamment le fait que les plans quadratiques réguliers sont classifiés par leur discriminant et la structure de $\mathbb{K}$-algèbre de leur algèbre de Clifford. Mais avant cela il nous est nécessaire de voir quelques définitions et notations.

Commençons par fixer deux éléments a et b de $\mathbb{K}^*$. Comme vu précédemment $\mathbb{K}^2$ s'injecte dans (a, b) et ainsi e_1, e_2 les vecteurs de la base canonique de $\mathbb{K}^2$ peuvent être vus comme des éléments de l'algèbre de quaternions (a,b). On sait de plus que le $\mathbb{K}$-espace vectoriel sous-jacent à la structure de $\mathbb{K}$-algèbre de (a,b) est de dimension $2^2 = 4$ avec la famille $(1, e_1, e_2, e_3)$ qui en est une base pour $e_3 = e_1e_2$. Avec l'identification usuelle qui consiste à voir $\mathbb{K}^2$ comme un sous espace vectoriel de (a, b), les règles de calcul dans les algèbres de Clifford nous donnent :

1. $e_1^2 = a$, $e_2^2 = b$, $e_3^2 = -ab$
2. $e_1e_2 = -e_2e_1$
3. $e_1e_3 = e_1^2e_2 = a \cdot e_2 = -e_3e_1$
4. $e_2e_3 = e_2e_1e_2 = -e_2^2e_1 = -b \cdot e_1 = -e_3e_2$.

Les résultats ci-dessus nous permettent alors de calculer le produit d'éléments de (a,b) après les avoir préalablement décomposés dans la base $(1, e_1, e_2, e_3)$. On remarque également que l'algèbre $(a,b)= \mathbb{K} \oplus \mathbb{K}e_1 \oplus \mathbb{K}e_2 \oplus \mathbb{K}e_3$ est graduée de la façon suivante :

$$(a, b)_0 = \mathbb{K} \oplus \mathbb{K}e_3 \text{ et } (a, b)_1 = \mathbb{K}e_1 \oplus \mathbb{K}e_2$$

En effet, il est facile de voir que $1 \in (a, b)_0$, que $\mathbb{K} \oplus \mathbb{K}e_3 \oplus \mathbb{K}e_1 \oplus \mathbb{K}e_2 = (a,b)$ et pour finir que $(a, b)_i(a, b)_j \subset (a, b)_{i+j}$ pour $i, j \in \mathbb{Z}/2$ (cf. les résultats ci-dessus).

Par analogie avec le corps des quaternions $\mathbb{H}$, continuons de donner quelques définitions.

Définition 11.0.7. *La symétrie vectorielle de (a, b) par rapport à $\mathbb{K}$ et parallèlement à $Vect(e_1, e_2, e_3)$ est l'application :*

$$\begin{cases} (a, b) \longrightarrow (a, b) \\ x = \alpha + \beta \cdot e_1 + \gamma \cdot e_2 + \delta \cdot e_3 \longmapsto \overline{x} = \alpha - \beta \cdot e_1 - \gamma \cdot e_2 - \delta \cdot e_3 \end{cases}$$

On l'appelle la ***conjugaison quaternionique****.*

Remarque 11.0.9. *La conjugaison quaternionique est une* anti-involution *de (a, b), c'est à dire qu'il s'agit d'une involution linéaire vérifiant :*

$$\forall x, y \in (a, b)^2, \overline{xy} = \overline{y}\,\overline{x}.$$

La linéarité est évidente tout comme le fait que pour $x \in (a, b)$ on ait : $\overline{\overline{x}} = x$. Enfin, le fait que : $\forall x, y \in (a, b)^2$, $\overline{xy} = \overline{y}\,\overline{x}$ est immédiat en décomposant x, y dans la base $(1, e_1, e_2, e_3)$ via les règles de calcul rappelées ci-dessus.

Norme quaternionique

Par les règles de calcul sur les vecteurs de bases de (a,b), pour tout élément $x = \alpha + \beta \cdot e_1 + \gamma \cdot e_2 + \delta \cdot e_3$, on a également :

$$x\overline{x} = \overline{x}x = \alpha^2 - a\beta^2 - b\gamma^2 + ab\delta^2 \in \mathbb{K}.$$

Définition 11.0.8. *Etant donné $x \in (a,b)$, on pose :*

$$N(x) := x\overline{x} = \overline{x}x \in \mathbb{K},$$

appelé ***norme (quaternionique)*** *de x.*
Ainsi pour $x = \alpha + \beta \cdot e_1 + \gamma \cdot e_2 + \delta \cdot e_3$ décomposé dans la base $(1, e_1, e_2, e_3)$ de (a,b), on a :

$$N(x) = \alpha^2 - a\beta^2 - b\gamma^2 + ab\delta^2.$$

L'écriture ci-dessus de N dans la base $(1, e_1, e_2, e_3)$ de (a,b) prouve que la norme est une forme quadratique sur l'espace vectoriel sous-jacent à l'algèbre (a,b) et qu'elle est équivalente à la forme diagonale $\langle 1, -a, -b, ab\rangle$.

Remarque 11.0.10. *La norme N est un* morphisme *de $((a,b), \times)$ sur $(\mathbb{K}, \times)$. En effet, d'après la remarque précédente $\forall x, y \in (a,b)^2$, on a :*

$$\begin{aligned} N(xy) = & \quad \overline{xy}xy \\ = & \quad \overline{y}\,\overline{x}xy \\ = & \quad \overline{y}N(x)y \\ = & \quad N(x)\overline{y}y \\ = & \quad N(x)N(y) \end{aligned}$$

car $N(x), N(y) \in \mathbb{K} \subset \mathcal{Z}(\langle a,b\rangle)$.

Remarque 11.0.11. *L'égalité $\overline{x} = -x$ a lieu si et seulement si $\alpha = 0$ pour x décomposé dans la base $(1, e_1, e_2, e_3)$ sous la forme $x = \alpha + \beta \cdot e_1 + \gamma \cdot e_2 + \delta \cdot e_3$. Ainsi $\{x \in (a,b), \overline{x} = -x\} = Vect(e_1, e_2, e_3)$ et on note cet ensemble $P_{a,b}$ appelé l'espace des* ***quaternions purs****. Pour un tel x,*

$$N(x) = x\overline{x} = -x^2 = -a\beta^2 - b\gamma^2 + ab\delta^2.$$

et $N_{P_{a,b}} \simeq \langle -a, -b, ab\rangle$

Passons désormais à l'énoncé du théorème de classification des plans quadratiques réguliers à l'aide de l'algèbre de Clifford associée et du discriminant.

Classification des formes quadratiques régulières de dimension 2 par l'algèbre de quaternion associée et le discriminant

Proposition 11.0.11. *Soit (a,b) et (c,d) deux algèbres de quaternions. Les formes quadratiques $\langle a,b\rangle$ et $\langle c,d\rangle$ sont équivalentes si et seulement si les $\mathbb{K}$-algèbres (a,b) et (c,d) sont isomorphes et si $\Delta(\langle a,b\rangle) = \Delta(\langle c,d\rangle)$ dans $\mathbb{K}^*/(\mathbb{K}^*)^2$.*

Démonstration. Soit $(a,b) \in (\mathbb{K}^*)^2$. On note $N_{a,b}$ la norme de l'algèbre des quaternions (a,b). Comme indiqué dans la remarque ci-dessus, pour $x \in P_{a,b}$ on a : $N_{a,b}(x) = x\overline{x} = -x^2$. Ainsi, la restriction à $P_{a,b}$ de la norme $N_{a,b}$ coïncide avec l'application $x \longrightarrow -x^2$. On montre alors que

$$P_{a,b} = \{x \in (a,b)\backslash\mathbb{K}^* : x^2 \in \mathbb{K}\}.$$

Soit $x \in P_{a,b} = Vect(e_1, e_2, e_3)$, on a bien $x \in (a,b)\backslash\mathbb{K}^*$ et via la décomposition $x = \beta \cdot e_1 + \gamma \cdot e_2 + \delta \cdot e_3$ dans la base (e_1, e_2, e_3) de $P_{a,b}$, il vient :

$$\begin{aligned} x^2 = & \quad (\beta \cdot e_1 + \gamma \cdot e_2 + \delta \cdot e_3)^2 \\ = & \quad -N_{a,b}(x) = a\beta^2 + b\gamma^2 - ab\delta^2 \in \mathbb{K} \end{aligned}$$

D'où $x^2 \in \mathbb{K}$, soit l'inclusion $P_{a,b} \subset \{x \in (a,b)\backslash\mathbb{K}^* : x^2 \in \mathbb{K}\}$.

Inversement, supposons $x \in (a,b)\backslash\mathbb{K}^*$ et $x^2 \in \mathbb{K}$. Cette fois-ci x se décompose sous la forme $x = \alpha + \beta \cdot e_1 + \gamma \cdot e_2 + \delta \cdot e_3$ dans la base $(1, e_1, e_2, e_3)$ de (a,b) et donc :

$$\begin{aligned} x^2 = & \quad (\alpha + \beta \cdot e_1 + \gamma \cdot e_2 + \delta \cdot e_3)^2 \\ = & \quad (\alpha^2 + a\beta^2 + b\gamma^2 - ab\delta^2) + 2(\alpha\beta \cdot e_1 + \alpha\gamma \cdot e_2 + \alpha\delta \cdot e_3) \\ = & \quad (\alpha^2 + a\beta^2 + b\gamma^2 - ab\delta^2) + 2\alpha(\beta \cdot e_1 + \gamma \cdot e_2 + \delta \cdot e_3) \end{aligned}$$

et

$$\begin{aligned} x^2 \in \mathbb{K} \iff & \quad 2\alpha(\beta \cdot e_1 + \gamma \cdot e_2 + \delta \cdot e_3) = 0 \\ \iff & \quad \alpha = 0 \text{ ou } (\beta, \gamma, \delta) = (0,0,0) \end{aligned}$$

Ainsi, puisque $x \in (a,b)\backslash\mathbb{K}^*$ on a :

$$x^2 \in \mathbb{K} \iff \alpha = 0$$

et d'où l'inclusion réciproque $\{x \in (a,b)\backslash\mathbb{K}^* : x^2 \in \mathbb{K}\} \subset P_{a,b}$.

Supposons désormais que $(a,b) \simeq (c,d)$ et soit ϕ est un isomorphisme d'algèbre entre (a,b) et (c,d). On veut montrer que la restriction de ϕ à $P_{a,b}$ induit une isométrie de $(P_{a,b}, (N_{a,b})_{P_{a,b}})$ sur $(P_{c,d}, (N_{c,d})_{P_{c,d}})$. Soit donc $x \in P_{a,b}$, d'après ce qui précède $x \in (a,b)\backslash\mathbb{K}^*$ avec $x^2 \in \mathbb{K}$. Puisque ϕ est un morphisme d'algèbre $\phi(1) = 1$ et donc :

$$\phi_{|\mathbb{K}} = Id_{|\mathbb{K}}$$

Alors ϕ étant un isomorphisme, pour $y \in \mathbb{K}$, il existe un unique antécédent dans (a,b) via ϕ qui est y lui-même. D'où si on suppose $\phi(x) \in \mathbb{K}$, notant cet élément y on a :

$$\phi(x) = y = \phi(y) \iff x = y \in \mathbb{K}$$

ce qui est absurde et donc $\phi(x) \notin \mathbb{K}$. On a de plus :

$$\phi(x^2) = \phi(x)^2 = x^2 \in \mathbb{K}$$

D'où $\phi(x) \in (c,d)\backslash\mathbb{K}^*$ avec $\phi(x)^2 \in \mathbb{K}$, soit $\phi(x) \in P_{c,d}$. Ainsi, on vient de montrer que ϕ induit un isomorphisme d'espace vectoriel de $P_{a,b}$ sur $P_{c,d}$ puisque

$$\phi(P_{a,b}) \subset P_{c,d} \text{ et } dim(\phi(P_{a,b})) = dim(P_{c,d}) = 3.$$

De plus, pour $x \in P_{a,b}$, $\phi(x) \in P_{c,d}$ et donc :

$$N_{a,b}(x) = -x^2 \text{ et } N_{c,d}(\phi(x)) = -\phi(x)^2$$

Or, d'après ce qui précède $\phi(x^2) = \phi(x)^2 = x^2$ et donc :

$$N_{a,b}(x) = N_{c,d}(\phi(x)).$$

Par conséquent $\phi : P_{a,b} \longrightarrow P_{c,d}$ induit bien une isométrie de $(P_{a,b}, (N_{a,b})_{P_{a,b}})$ sur $(P_{c,d}, (N_{c,d})_{P_{c,d}})$ et donc $\langle -a, -b, ab\rangle \simeq \langle -c, -d, cd\rangle$, soit également :

$$\langle -a, -b\rangle \perp \langle ab\rangle \simeq \langle -c, -d\rangle \perp \langle cd\rangle.$$

Supposons de plus que :

$$\Delta(\langle a, b\rangle) = \Delta(\langle c, d\rangle) \text{ dans } \mathbb{K}^*/(\mathbb{K}^*)^2$$

alors $ab = cd$, $\mathbb{K}^*/(\mathbb{K}^*)^2$ et donc $\langle ab\rangle \simeq \langle cd\rangle$. Par simplification de Witt on a :

$$\langle -a, -b\rangle \simeq \langle -c, -d\rangle \Longrightarrow \langle a, b\rangle \simeq \langle c, d\rangle$$

Ainsi, si $(a, b) \simeq (c, d)$ et si $\Delta(\langle a, b\rangle) = \Delta(\langle c, d\rangle)$ alors $\langle a, b\rangle \simeq \langle c, d\rangle$. Réciproquement, si $\langle a, b\rangle \simeq \langle c, d\rangle$, on a alors immédiatement $\Delta(\langle a, b\rangle) = \Delta(\langle c, d\rangle)$ et $(a, b) \simeq (c, d)$. D'où le résultat. □

Grâce à la démonstration précédente, on va donner à l'aide de la norme quaternionique, une condition nécessaire et suffisante pour que deux algèbres de quaternions soient isomorphes.

Isomorphisme entre algèbres de quaternions et structure de ces algèbres

Proposition 11.0.12. *Les algèbres de quaternions (a, b) et (c, d) sont isomorphes si et seulement si les formes $\langle 1, -a, -b, ab\rangle$ et $\langle 1, -c, -d, cd\rangle$ sont équivalentes.*

Démonstration. On a montré dans la démonstration précédente que si les algèbres (a, b) et (c, d) sont isomorphes alors les formes quadratiques $\langle -a, -b, ab\rangle$ et $\langle -c, -d, cd\rangle$ sont équivalentes. On en déduit alors que :

$$\langle 1\rangle \perp \langle -a, -b, ab\rangle \simeq \langle 1\rangle \perp \langle -c, -d, cd\rangle \Longrightarrow \langle 1, -a, -b, ab\rangle \simeq \langle 1, -c, -d, cd\rangle.$$

Inversement, si on suppose que $\langle 1, -a, -b, ab\rangle \simeq \langle 1, -c, -d, cd\rangle$, alors par simplification de Witt, on a $\langle -a, -b, ab\rangle \simeq \langle -c, -d, cd\rangle$ et donc puisque

$$(N_{a,b})_{|P_{a,b}} \simeq \langle -a, -b, ab\rangle \text{ et } (N_{c,d})_{|P_{c,d}} \simeq \langle -c, -d, cd\rangle$$

par transitivité de la relation "être équivalente", il vient :

$$(N_{a,b})_{|P_{a,b}} \simeq (N_{c,d})_{|P_{c,d}}.$$

On note ϕ une isométrie entre $P_{a,b}$ et $P_{c,d}$ que l'on peut prolonger en un isomorphisme d'espaces vectoriels entre (a, b) et (c, d) en envoyant 1 sur 1. En effet, la base (e_1, e_2, e_3) de $P_{a,b}$ est alors envoyé par l'isométrie sur la base $(\phi(e_1), \phi(e_2), \phi(e_3))$ de $P_{c,d}$ et le prolongement de ϕ à (a, b) (que l'on note encore ϕ) envoie la base $(1, e_1, e_2, e_3)$ sur la famille $(1, \phi(e_1), \phi(e_2), \phi(e_3)$ qui est une base de (c, d) formée par concaténation d'une base de $\mathbb{K}$ et d'une base de $P_{c,d}$ avec $(c, d) = \mathbb{K} \oplus P_{c,d}$. Ainsi, le prolongement de ϕ à (a, b) est un isomorphisme d'espaces vectoriels de (a, b) sur (c, d) tel que $\phi_{|\mathbb{K}} = Id_{|\mathbb{K}}$ ce qui permet, en décomposant les éléments de (a, b) dans la base $(1, e_1, e_2, e_3)$, de vérifier facilement que ϕ est en plus un morphisme d'algèbre, ce qui montre donc que :

$$(a, b) \simeq (c, d).$$

□

Enfin, terminons cette section par l'énonciation du théorème de structure des algèbres de quaternions.

Théorème 11.0.5. ***Structure des algèbres de quaternions***
Soit $a, b \in \mathbb{K}^*$.

1. *Si la forme quadratique $\langle 1, -a, -b\rangle$ est anisotrope alors (a, b) est un corps gauche dont le centre est $\mathbb{K}$.*
2. *Si la forme quadratique $\langle 1, -a, -b\rangle$ est isotrope, alors l'algèbre (a, b) est isomorphe à $\mathcal{M}_2(\mathbb{K})$*

Dans tous les cas, (a, b) est une $\mathbb{K}$-algèbre centrale et $(a, b)_0$ est isomorphe à $C\langle -ab\rangle$.

On en déduit facilement les deux corollaires suivants :

Corollaire 11.0.7. *Pour tout $a \in \mathbb{K}^*$, $(1, a) \simeq \mathcal{M}_2(\mathbb{K})$.*

Démonstration. Sur tout corps $\mathbb{K}$ de caractéristique différente de 2, $\langle 1, -1\rangle$ est isotrope et donc pour tout $a \in \mathbb{K}^*$, $\langle 1, -1\rangle \perp \langle -a\rangle \simeq \langle 1, -1, -a\rangle$ l'est aussi. □

Corollaire 11.0.8. *Soit $\mathbb{K}$ un corps fini, pour tout $a, b \in \mathbb{K}^*$, $(a, b) \simeq \mathcal{M}_2(\mathbb{K})$.*

Démonstration. Toute forme quadratique régulière de dimension 3 est isotrope sur le corps fini $\mathbb{K}$, ce qui donne le résultat. □

On aura l'occasion d'utiliser ce théorème de structure et ces corollaires, à de nombreuses reprises, notamment dans la section à venir pour classifier les formes quadratiques à l'aide de l'algèbre de quaternion $\mathbb{Z}/2$-graduée associée et dans celle qui suit pour étudier les classes d'isomorphie d'algèbres de quaternions sur $\mathbb{Q}$ et les corps $\mathbb{Q}_p$.

11.0.11 Classification des formes quadratiques régulières de dimension 2 par la structure d'algèbre $\mathbb{Z}/2$-graduée associée

Précédemment, nous avons étudié les algèbres de Clifford associées aux plans quadratiques réguliers (algèbres de quaternions) et avons exhibé un théorème de structure de ces algèbres. Puis, nous avons mis en évidence un résultat important :

les plans quadratiques réguliers sont classifiés par leur discriminant et la structure de $\mathbb{K}$-algèbre, de leur algèbre de Clifford.

Ces deux outils, nous serons utiles pour démontrer la proposition suivante qui prend en compte la structure d'algèbre $\mathbb{Z}/2$-graduée. Nous établirons ainsi que pour q et q' deux formes quadratiques régulières de dimension 2, on a :

$$q \simeq q' \iff C(q) \simeq_{\mathbb{Z}/2} C(q').$$

Proposition 11.0.13. *Soit q_1 et q_2 deux formes quadratiques régulières de dimension 2. Les assertions suivantes sont équivalentes :*

1. *q_1 et q_2 sont équivalentes.*
2. *$C(q_1) \simeq C(q_2)$ et $C_0(q_1) \simeq C_0(q_2)$ en tant qu'algèbres.*

3. $C(q_1) \simeq C(q_2)$ *en tant qu'algèbres* $\mathbb{Z}/2$*-graduées.*

Démonstration. Puisque q_1 et q_2 sont deux formes quadratiques régulières de dimension 2, par diagonalisation, il existe des éléments non nuls a, b, c, d de $\mathbb{K}^*$ tels que :

$$q_1 \simeq \langle a, b\rangle \text{ et } q_2 \simeq \langle c, d\rangle$$

et donc également,

$$C(q_1) \simeq_{\mathbb{Z}/2} C\langle a, b\rangle \text{ et } C(q_2) \simeq_{\mathbb{Z}/2} C\langle c, d\rangle.$$

- $3 \Longrightarrow 2$ est clair, puisque si $C(q_1)$ et $C(q_2)$ sont isomorphes en tant qu'algèbres $\mathbb{Z}/2$-graduées, elles sont naturellement isomorphes en tant qu'algèbres, avec l'isomorphisme $C_0(q_1) \simeq C_0(q_2)$ qui découle du fait que l'isomorphisme d'algèbres graduées préserve la graduation.
- $1 \Longrightarrow 2$ est clair. Deux formes quadratiques régulières équivalentes ayant des algèbres de Clifford isomorphes en tant qu'algèbres graduées, ce qui donne bien les deux isomorphismes souhaités au point 2.
- $1 \Longrightarrow 3$ est clair également.
- Montrons $3 \Longrightarrow 1$. $C(q_1) \simeq C(q_2)$ en tant qu'algèbres $\mathbb{Z}/2$-graduées, ce qui donne aussi avec les notations précédentes $C\langle a, b\rangle \simeq C\langle c, d\rangle$ en tant qu'algèbres $\mathbb{Z}/2$-graduées. D'après le théorème de structure des algèbres de quaternions :
  $$C_0(\langle a, b\rangle) \simeq C\langle -ab\rangle \text{ et } C_0(\langle c, d\rangle) \simeq C\langle -cd\rangle$$
  Comme l'isomorphisme d'algèbres entre $C\langle a, b\rangle$ et $C\langle c, d\rangle$ est gradué, on a $C_0(\langle a, b\rangle) \simeq C_0(\langle c, d\rangle)$ et donc également $C\langle -ab\rangle \simeq C\langle -cd\rangle$. D'après l'étude des algèbres de Clifford associées aux formes quadratiques régulières en dimension 1, on déduit que $\langle -ab\rangle \simeq \langle -cd\rangle$ et donc :
  $$ab = cd \text{ dans } \mathbb{K}^*/(\mathbb{K}^*)^2.$$
  Ainsi les formes quadratiques régulières de dimension 2, $\langle a, b\rangle$ et $\langle c, d\rangle$ ont des algèbres de Clifford associées isomorphes et ont même discriminant ce qui montre d'après la proposition 11.0.11 que $\langle a, b\rangle \simeq \langle c, d\rangle$ soit $q_1 \simeq q_2$.
- $2 \Longrightarrow 1$ est immédiate d'après ce qu'on vient de faire ci-dessus. En effet, pour montrer $3 \Longrightarrow 1$, on a simplement eu besoin d'utiliser successivement que :
  $$C\langle a, b\rangle \simeq C\langle c, d\rangle \text{ et } C_0(\langle a, b\rangle) \simeq C_0(\langle c, d\rangle)$$
  avec $q_1 \simeq \langle a, b\rangle$ et $q_2 \simeq \langle c, d\rangle$. La même méthode que ci-dessus permet donc de conclure.

□

Etude des classes d'isomorphie d'algèbres de quaternions sur $\mathbb{Q}$ et les corps $\mathbb{Q}_p$

Pour $a, b \in \mathbb{K}^*$, on a vu que la structure de la $\mathbb{K}$-algèbre des quaternions (a, b) dépendait du caractère isotrope ou anisotrope de la forme quadratique $\langle 1, -a, -b\rangle$. La proposition suivante s'appuie sur cette forte dépendance, pour étudier le nombre de classes d'isomorphie d'algèbres de quaternions sur les corps $\mathbb{Q}$ et $\mathbb{Q}_p$, pour $p \in \mathcal{P}$.

Proposition 11.0.14. *Il y a une infinité de classes d'isomorphie d'algèbres de quaternions sur* $\mathbb{Q}$ *alors qu'il y a exactement deux types de classes d'isomorphie d'algèbres de quaternions sur les corps p-adiques* $\mathbb{Q}_p$*, où* $p \in \mathcal{P}$*.*

Démonstration. Soit $a, b \in \mathbb{Q}^*$. Si on suppose par l'absurde qu'il n'y a qu'un nombre fini de classes d'isomorphie d'algèbres de quaternions sur $\mathbb{Q}$, il n'y a qu'un nombre fini de classes d'équivalences de formes quadratiques sur $\mathbb{Q}$ de la forme $\langle 1, -a, -b, ab\rangle$, $a, b \in \mathbb{Q}^*$ (deux algèbres de quaternions sont isomorphes si et seulement si leurs normes quaternioniques associées sont équivalentes). Montrons que ceci est absurde. Considérons $p_1, p_2 \in \mathcal{P}$ tels que $p_1 \neq p_2$ avec $p_1, p_2 \equiv 3\,[4]$ et prouvons que :

$$\langle 1, -p_1, -p_1, -p_1^2\rangle \not\simeq \langle 1, -p_2, -p_2, p_2^2\rangle \text{ (cas où } a = b = p_1 \text{ puis } a = b = p_2).$$

ce qui montrera le résultat puisqu'il y a une infinité de nombres premiers congrus à 3 modulo 4. Comme p_1^2 et p_2^2 sont deux carrés de $\mathbb{Q}^*$, les formes diagonales ci-dessus sont respectivement équivalentes à $\langle 1, -p_1, -p_1, 1\rangle$ et $\langle 1, -p_2, -p_2, 1\rangle$. Par le test d'équivalence rationnelle, si $\langle 1, -p_1, -p_1, 1\rangle \simeq \langle 1, -p_2, -p_2, 1\rangle$, on a en particulier :

$$\partial_{p_1}(< 1, -p_1, -p_1, 1 >) = \partial_{p_1}(< 1, -p_2, -p_2, 1 >) \text{ dans } W(\mathbb{F}_{p_1}).$$

Or, $p_2 \neq p_1$ on a donc $\partial_{p_1}(< 1, -p_2, -p_2, 1 >) = 0_{W(\mathbb{F}_{p_1})}$ ce qui impose nécessairement :

$$0_{W(\mathbb{F}_{p_1})} =< \partial_{p_1}(1), \partial_{p_1}(-p_1), \partial_{p_1}(-p_1), \partial_{p_1}(1) >=< 0, -1, -1, 0 >.$$

Ainsi $0_{W(\mathbb{F}_{p_1})} =< -1, -1 >$ et $\langle -1, -1\rangle$ est donc hyperbolique sur $\mathbb{F}_{p_1}$. Or, puisque $\Delta(\langle -1, -1\rangle) = -1$ et que -1 n'est pas un carré de $\mathbb{F}_p^*$ (comme $p \equiv 3\,[4]$), $\langle -1, -1\rangle$ n'est pas hyperbolique et $< -1, -1 >\neq 0_{W(\mathbb{F}_{p_1})}$. Ce qui montre bien que :

$$\langle 1, -p_1, -p_1, 1\rangle \not\simeq \langle 1, -p_2, -p_2, 1\rangle \text{ sur } \mathbb{Q}.$$

Il y a ainsi une infinité de classes d'équivalence associées aux formes quadratiques du type $\langle 1, -p, -p, 1\rangle$ sur $\mathbb{Q}$ et donc aussi une infinité de classes d'équivalence associées aux formes quadratique du type $\langle 1, -a, -b, ab\rangle$ sur $\mathbb{Q}$. Ceci achève donc de montrer le résultat dans le cas du corps $\mathbb{Q}$.

Supposons $p \in \mathcal{P}$ et $a, b \in \mathbb{Q}_p^*$. Si la forme diagonale $\langle 1, -a, -b, ab\rangle$ est isotrope sur $\mathbb{Q}_p$ alors la $\mathbb{Q}_p$-algèbre des quaternions est isomorphe à $\mathcal{M}_2(\mathbb{Q}_p)$ et on a donc là le premier type d'isomorphie pour les algèbres de quaternions. Le deuxième type d'isomorphie vient alors des algèbres de quaternions (a, b) telles que $\langle 1, -a, -b, ab\rangle$ est anisotrope sur $\mathbb{Q}_p$. En effet, pour $p = 2$ ou p premier impair il n'y a à équivalence près qu'une seule forme anisotrope de dimension 4 sur $\mathbb{Q}_p$. Ainsi, si $\langle 1, -a, -b, ab\rangle$ et $\langle 1, -c, -d, cd\rangle$ sont anisotropes, pour $a, b \in \mathbb{Q}_p^*$ et $c, d \in \mathbb{Q}_p^*$, on a :

$$\langle 1, -a, -b, ab\rangle \simeq \langle 1, -c, -d, cd\rangle \Longleftrightarrow (a, b) \simeq (c, d)$$

La seconde classe d'isomorphie d'algèbres de quaternions est alors la classe de (a, b) pour $\langle 1, -a, -b, ab\rangle$ anisotrope, les deux classes mentionnées précédemment étant bien distinctes. En effet, si $a, b \in \mathbb{Q}_p^*$ et $c, d \in \mathbb{Q}_p^*$ sont tels que $\langle 1, -a, -b, ab\rangle$ est isotrope sur $\mathbb{Q}_p$ et $\langle 1, -c, -d, cd\rangle$ anisotrope sur $\mathbb{Q}_p$, on a bien $(a, b) \not\simeq (c, d)$ car sinon les formes $\langle 1, -a, -b, ab\rangle$ et $\langle 1, -c, -d, cd\rangle$ seraient équivalentes, absurde l'une étant isotrope, l'autre anisotrope. On a donc bien exactement deux types de classes d'isomorphie d'algèbres de quaternions sur les corps $\mathbb{Q}_p$. □

Corollaire 11.0.9. *Il existe à isomorphisme près, une unique algèbre de quaternions sur $\mathbb{Q}_p$ qui est un corps. On notera l'une d'entre elles $\mathbb{H}_p$.*

Démonstration. Soit $(a,b,c,d) \in (\mathbb{Q}_p^*)^4$. On suppose que les algèbres de quaternions (a,b) et (c,d) sont deux corps. On va montrer qu'elles sont nécessairement isomorphes en tant qu'algèbres. Les formes quadratiques de dimension 4, $\langle 1,-a,-b,ab\rangle$ et $\langle 1,-c,-d,cd\rangle$ sont anisotropes sur $\mathbb{Q}_p$ car sinon seraient isotropes et les algèbres (a,b) et (c,d) seraient isomorphes à $\mathcal{M}_2(\mathbb{Q}_p)$ qui n'est pas un corps. Or, à équivalence près il y a une unique forme quadratique de dimension 4 anisotrope sur $\mathbb{Q}_p$, d'où :

$$\langle 1,-a,-b,ab\rangle \simeq \langle 1,-c,-d,cd\rangle \Longleftrightarrow (a,b) \simeq (c,d).$$

Ce qui achève de montrer le résultat. □

Ainsi sur $\mathbb{Q}_p$, l'algèbre de quaternion (a,b) est soit isomorphe à $\mathcal{M}_2(\mathbb{Q}_p)$ soit isomorphe à $\mathbb{H}_p$.

11.0.12 Algèbres de Clifford en dimension 3

Après avoir étudié les algèbres de Clifford associées aux droites quadratiques et les algèbres de quaternions, nous allons examiner les algèbres de Clifford en dimension 3. Pour ce faire, on fixe un triplet $(a,b,c) \in (\mathbb{K}^*)^3$ et nous allons nous intéresser à l'algèbre $C\langle a,b,c\rangle$. Pour la forme $\langle a,b,c\rangle$ définie sur le $\mathbb{K}$-espace vectoriel $\mathbb{K}^3$, la base canonique e_1,e_2,e_3 constitue une base orthogonale. Avec l'identification usuelle $\mathbb{K}^3 \hookrightarrow C\langle a,b,c\rangle$, $(1,e_1,e_2,e_3,e_1e_2,e_1e_3,e_2e_3,e_1e_2e_3)$ est une base de $C\langle a,b,c\rangle$ où,

$$(1,e_1e_2,e_1e_3,e_2e_3) \text{ est une base de } C_0\langle a,b,c\rangle$$

et

$$(e_1,e_2,e_3,e_1e_2e_3) \text{ est une base de } C_1\langle a,b,c\rangle.$$

Passons maintenant à la description complète de la structure de $C\langle a,b,c\rangle$.

Théorème 11.0.6. *Soit $(a,b,c) \in (\mathbb{K}^*)^3$. Alors,*

1. $C_0(a,b,c) \simeq (-ac,-bc)$
2. $\mathcal{Z}\langle a,b,c\rangle = \mathbb{K} \oplus \mathbb{K}e_1e_2e_3$ *et est isomorphe à* $C\langle -abc\rangle$.
3. $C\langle a,b,c\rangle \simeq_{\mathbb{Z}/2} C_0\langle a,b,c\rangle \widehat{\otimes} \mathcal{Z}\langle a,b,c\rangle$ *où* $C_0\langle a,b,c\rangle$ *est trivialement graduée.*

On en déduit l'important lemme de dévissage suivant qui nous permettra de décomposer n'importe qu'elle algèbre de Clifford en dimension supérieure.

Corollaire 11.0.10. ***Lemme de dévissage***

1. $C\langle a,b,c\rangle \simeq (-ac,-bc) \otimes C\langle -abc\rangle$
2. $C\langle a,b,c\rangle \simeq_{\mathbb{Z}/2} (-ac,-bc)\widehat{\otimes} C\langle -abc\rangle$, *où* $(-ac,-bc)$ *est trivialement graduée.*

Nous sommes désormais en capacité de classifier les formes quadratiques de dimension 3 via l'algèbre de Clifford $\mathbb{Z}/2$-graduée associée.

Classification des formes quadratiques régulières de dimension 3 par l'algèbre de Clifford $\mathbb{Z}/2$-graduée associée

Précédemment nous avons étudié les algèbres de Clifford associées à des formes quadratiques de dimension 1 et 2 et nous avons mis en évidence que :

- Pour deux droites quadratiques (E_1, q_1) et (E_2, q_2), les aglèbres de Clifford associées $C(q_1)$ et $C(q_2)$ sont isomorphes en tant qu'algèbres (graduées) si et seulement si q_1 et q_2 sont équivalentes et donc que la structure de l'algèbre de Clifford $C(q)$ détermine à équivalence près q.
- Pour deux plans quadratiques (E_1, q_1) et (E_2, q_2), q_1 et q_2 sont équivalentes si et seulement si les algèbres de Clifford associées $C(q_1)$ et $C(q_2)$ sont isomorphes en tant qu'algèbres *et* si $\Delta(q_1) = \Delta(q_2)$.

Ainsi, dans le cadre de la dimension 2, la structure de $\mathbb{K}$-algèbre de l'algèbre de Clifford $C(q)$ ne suffit plus pour déterminer q à équivalence près, on a besoin d'une information supplémentaire qui est portée par le discriminant ou bien par la structure d'algèbre graduée. Dans le cadre de la dimension 3, on va pouvoir également classifier les formes quadratiques régulières par l'algèbre de Clifford associée, mais comme pour la dimension 2, la structure de $\mathbb{K}$-algèbre de l'algèbre de Clifford $C(q)$ sera insuffisante pour déterminer q à équivalence près, on aura alors besoin d'une information supplémentaire qui sera ici, également portée par la structure d'algèbre $\mathbb{Z}/2$-graduée de $C(q)$.

Proposition 11.0.15. *Les formes quadratiques régulières de dimension 3 sur $\mathbb{K}$ sont classifiées à isomorphisme près par leur algèbre de Clifford associée vue comme $\mathbb{Z}/2$-algèbre. Ainsi, si q_1 et q_2 sont deux formes quadratiques régulières de dimension 3, q_1 et q_2 sont équivalentes si et seulement si les algèbres $C(q_1)$ et $C(q_2)$ sont isomorphes en tant qu'algèbres $\mathbb{Z}/2$-graduées, ce que l'on peut résumer par :*

$$q_1 \simeq q_2 \iff C(q_1) \simeq_{\mathbb{Z}/2} C(q_2)$$

Pour démontrer cette proposition nous aurons besoin d'utiliser le résultat suivant :

Lemme 11.0.2. *Soit $(a, b, c, a', b', c') \in (\mathbb{K}^*)^6$. Si les algèbres de Clifford $C\langle a, b, c\rangle$ et $C\langle a', b', c'\rangle$ sont isomorphes en tant que $\mathbb{K}$-algèbres, alors les formes quadratiques $\langle a, b, c\rangle$ et $\langle a', b', c'\rangle$ ont même discriminant.*

Démonstration. Supposons que $C\langle a, b, c\rangle$ et $C\langle a', b', c'\rangle$ soient isomorphes en tant que $\mathbb{K}$-algèbres. Cela implique alors que :

$$\mathcal{Z}\langle a, b, c\rangle \simeq \mathcal{Z}\langle a', b', c'\rangle$$

et par le théorème de structure des algèbres de Clifford en dimension 3, on a :

1. $\mathcal{Z}\langle a, b, c\rangle \simeq C\langle -abc\rangle$
2. $\mathcal{Z}\langle a', b', c'\rangle \simeq C\langle -a'b'c'\rangle$

On déduit alors en particulier que $C\langle -abc\rangle \simeq C\langle -a'b'c'\rangle$, ce qui implique via l'étude des algèbres de Clifford en dimension 1 que $\langle abc\rangle$ et $\langle -a'b'c'\rangle$ sont équivalentes. Ainsi $\langle abc\rangle$ et $\langle -a'b'c'\rangle$ ont même discriminant, soit $abc = a'b'c'$ dans $\mathbb{K}^*/(\mathbb{K}^*)^2$. □

Remarque 11.0.12. *Du lemme précédent on obtient en particulier que les algèbres de Clifford $C\langle 1,1,1\rangle$ et $C\langle 1,1,\varepsilon\rangle$ sur $\mathbb{F}_q$ ne sont jamais isomorphes pour ε désignant un non carré de $\mathbb{F}_q$. En effet,*

$$\Delta(\langle 1,1,1\rangle) = -1 \text{ et } \Delta(\langle 1,1,\varepsilon\rangle) = -\varepsilon$$

avec $\varepsilon \neq 1$ dans $\mathbb{F}_q^*/(\mathbb{F}_q^*)^2$.

Passons désormais à la démonstration de la proposition.

Démonstration. On suppose que $(a,b,c,a',b',c') \in (\mathbb{K}^*)^6$ et que $C\langle a,b,c\rangle$ et $C\langle a',b',c'\rangle$ sont isomorphes en tant qu'algèbres $\mathbb{Z}/2$-graduées. Alors, par l'isomorphisme gradué, les parties paires de ces algèbres que sont $C_0\langle a,b,c\rangle$ et $C_0\langle a',b',c'\rangle$ sont également isomorphes. D'après le théorème de structure des algèbres de Clifford en dimension 3, on a :

1. $C_0\langle a,b,c\rangle \simeq (-ac,-bc)$
2. $C_0\langle a',b',c'\rangle \simeq (-a'c',-b'c')$

et donc :

$$(-ac,-bc) \simeq (-a'c',-b'c').$$

Puisque les algèbres de quaternions $(-ac,-bc)$ et $(-a'c',-b'c')$ sont isomorphes, les normes quaternioniques associées sont équivalentes d'où :

$$\langle 1,ac,bc,abc^2\rangle \simeq \langle 1,a'c',b'c',a'b'c'^2\rangle$$

puis,

$$\langle 1,ac,bc,ab\rangle \simeq \langle 1,a'c',b'c',a'b'\rangle \text{ comme } c^2,\ c'^2 \in (\mathbb{K}^*)^2.$$

Or,

$$\langle 1,ac,bc,ab\rangle \simeq \langle 1\rangle\perp\langle ac,bc,ab\rangle \text{ et } \langle 1,a'c',b'c',a'b'\rangle \simeq \langle 1\rangle\perp\langle a'c',b'c',a'c'\rangle$$

par simplification de Witt, on a alors :

$$\langle ac,bc,ab\rangle \simeq \langle a'c',b'c',a'c'\rangle.$$

Par le lemme précédent $abc = a'b'c'$ dans $\mathbb{K}^*/(\mathbb{K}^*)^2$, donc en multipliant les coefficients diagonaux par abc pour la première forme diagonale et par $a'b'c'$ pour la seconde, il vient : $\langle b(ac)^2, a(bc)^2, c(ab)^2\rangle \simeq \langle b'(a'c')^2, a'(b'c')^2, c'(a'b')^2\rangle$ soit $\langle b,a,c\rangle \simeq \langle b',a',c'\rangle$ et donc par permutation des termes diagonaux :

$$\langle a,b,c\rangle \simeq \langle a',b',c'\rangle.$$

Ceci achève de montrer la proposition puisque l'on sait également que si deux formes quadratiques q_1, q_2 sont équivalentes alors les algèbres de Clifford associées sont isomorphes en tant qu'algèbres $\mathbb{Z}/2$-graduées. □

Remarque 11.0.13. *Soit $(a,b,c,a',b',c') \in (\mathbb{K}^*)^6$. De la démonstration précédente, on déduit que si :*

- $C_0\langle a,b,c\rangle \simeq C_0\langle a',b',c'\rangle$
- $abc = a'b'c'$ *dans* $\mathbb{K}^*/(\mathbb{K}^*)^2$

alors :

$$\langle a,b,c\rangle \simeq \langle a',b',c'\rangle$$

En effet, dans la démonstration précédente, l'isomorphisme

$$C\langle a,b,c\rangle \simeq_{\mathbb{Z}/2} C\langle a',b',c'\rangle$$

ne nous sert que pour prouver que les parties paires sont isomorphes, cet isomorphisme entre les parties paires étant celui utilisé dans la suite de la démonstration. Enfin, la partie finale de la démonstration utilisait que

$$\Delta(\langle a,b,c\rangle) = \Delta(\langle a',b',c'\rangle)$$

ce que l'on avait déduit de l'isomorphisme $C\langle a,b,c\rangle \simeq C\langle a',b',c'\rangle$. *L'égalité* $\Delta(\langle a,b,c\rangle) = \Delta(\langle a',b',c'\rangle)$ *figure ici dans nos hypothèses, car il est supposé* $abc = a'b'c'$ *dans* $\mathbb{K}^*/(\mathbb{K}^*)^2$.

11.0.13 Algèbres de Clifford en dimension 4

Comme pour l'étude des algèbres en dimension 3 commençons par donner un théorème de structure des algèbres de Clifford en dimension 4.

Théorème 11.0.7. *Soit* $(a,b,c,d) \in (\mathbb{K}^*)^4$. *Il y a alors un isomorphisme d'algèbres*

$$C\langle a,b,c,d\rangle \simeq (-ac,-bc)\otimes(-abc,d)$$

et un isomorphsime d'algèbres $\mathbb{Z}/2$*-graduées*

$$C\langle a,b,c,d\rangle \simeq (-ac,-bd)\widehat{\otimes}(-abc,d)$$

dans lequel la première algèbre de quaternions $(-ac,-bd)$ *est trivialement graduée, tandis que la seconde est graduée de manière usuelle.*

A l'aide de ce théorème de structure, pour q et q' régulières de dimension 4, nous allons établir une condition nécessaire et suffisante pour que deux algèbres de Clifford $C(q)$ et $C(q')$ soient isomorphes en tant qu'algèbres graduées. Ce type de raisonnemment est donc différent de ceux exposés aux sections sur la dimension 2 et 3. En effet, on cherchera ici à établir une condition sur les formes quadratiques q et q' pour que $C(q) \simeq_{\mathbb{Z}/2} C(q')$, alors que précédemment, on a plutôt essayer de trouver une condition portant sur les algèbres de Clifford pour que q et q' soient équivalentes.

Condition nécessaire et suffisante pour que $C(q) \simeq_{\mathbb{Z}/2} C(q')$ en dimension 4

Dans cette partie, nous allons voir quelques applications du théorème de structure présenté ci-dessus. Nous montrerons par exemple qu'il existe des formes quadratiques régulières de dimension 4 non équivalentes et dont les algèbres de Clifford sont isomorphes en tant qu'algèbres $\mathbb{Z}/2$-graduées. Ceci constitue une différence importante avec le cadre des algèbres de quaternions pour lesquelles nous avons montré que deux algèbres (a,b) et (c,d) sont isomorphes en tant qu'algèbres $\mathbb{Z}/2$-graduées si et seulement si $\langle a,b\rangle$ et $\langle c,d\rangle$ sont équivalentes. Nous verrons également par la suite une condition nécessaire et suffisante pour que deux formes quadratiques q et q' régulières de dimension 4 aient des algèbres de Clifford isomorphes en tant qu'algèbres $\mathbb{Z}/2$-graduées. Ce qui nous permettra notamment de montrer que les algèbres de Clifford associées aux formes quadratiques $\langle 1,1,1,1\rangle$, $\langle 1,1,1,\varepsilon\rangle$ sur $\mathbb{F}_p$ bien qu'isomorphes, ne le sont pas en tant qu'algèbres $\mathbb{Z}/2$-graduées.

Proposition 11.0.16. *Soit q une forme quadratique régulière de dimension 4 et δ un discriminant de q. Par diagonalisation $q \simeq \langle a,b,c,d\rangle$ pour (a,b,c,d) dans $(\mathbb{K}^*)^4$ et soit α un scalaire non nul représenté par $\langle 1,-\delta\rangle$. Alors, les algèbres $C(q)$ et $C(\alpha q)$ sont isomorphes en tant qu'algèbres $\mathbb{Z}/2$-graduées.*

Démonstration. En reprenant les notations de la proposition, $q \simeq \langle a,b,c,d\rangle$ et $\delta = \Delta(\langle a,b,c,d\rangle) = abcd \in \mathbb{K}^*/(\mathbb{K}^*)^2$. Ainsi :

$$\begin{aligned} -abc\langle 1,-\delta\rangle &\simeq \langle -abc, abc\delta\rangle \\ &\simeq \langle -abc, abc\times abcd\rangle \\ &\simeq \langle -abc, (abc)^2 d\rangle \\ &\simeq \langle -abc, d\rangle \end{aligned}$$

Ainsi,

$$-abc\langle 1,-\delta\rangle \simeq \langle -abc,d\rangle \Longrightarrow C(-abc\langle 1,-\delta\rangle) \simeq_{\mathbb{Z}/2} C\langle -abc,d\rangle$$

Pour α non nul représenté par $\langle 1,-\delta\rangle$ il existe $(x,y) \in (\mathbb{K}^*)^2$ tel que $\alpha = x^2 - \delta y^2$. Notant $H = vect(x,y)$, $\langle 1,-\delta\rangle_{|H} \simeq \langle \alpha\rangle$ et par l'astuce de complétion avec un déterminant, on obtient :

$$\langle 1,-\delta\rangle \simeq \langle \alpha, -\alpha\delta\rangle \simeq \alpha\langle 1,-\delta\rangle.$$

Ainsi $\alpha q \simeq \langle \alpha a, \alpha b, \alpha c, \alpha d\rangle$ et donc par les résultats rappelés ci-dessus :

$$\begin{aligned} C(\alpha q) &\simeq (-ac\alpha^2, -bc\alpha^2)\widehat{\otimes}(-abc\alpha^3, d\alpha) \\ &\simeq (-ac,-bc)\widehat{\otimes}(-abc\alpha^3, d\alpha) \\ &\simeq (-ac,-bc)\widehat{\otimes}(-abc\alpha, d\alpha) \end{aligned}$$

Puisque $\langle 1,-\delta\rangle \simeq \alpha\langle 1,-\delta\rangle$ on a également :

$$\begin{aligned} C(-abc\langle 1,-\delta\rangle) &\simeq C(-abc\langle \alpha,-\alpha\delta\rangle) \\ &\simeq (-abc\alpha, abc\alpha\delta) \\ &\simeq (-abc\alpha, abc\alpha(abcd)) \\ &\simeq (-abc\alpha, (abc)^2\alpha d) \\ &\simeq (-abc\alpha, d\alpha) \end{aligned}$$

De plus $C(q) \simeq C\langle a,b,c,d\rangle$ avec $C\langle a,b,c,d\rangle \simeq (-ac,-bc)\widehat{\otimes}(-abc,d)$. Or ci-dessus on a montré que $C\langle -abc,d\rangle = (-abc,d) \simeq C(-abc\langle 1,-\delta\rangle)$ en tant qu'algèbres $\mathbb{Z}/2$-graduées, d'où :

$$\begin{aligned} C\langle a,b,c,d\rangle &\simeq (-ac,-bc)\widehat{\otimes}(-abc,d) \\ &\simeq (-ac,-bc)\widehat{\otimes}C(-abc\langle 1,-\delta\rangle) \\ &\simeq (-ac,-bc)\widehat{\otimes}(-abc\alpha, d\alpha) \\ &\simeq C(\alpha q) \end{aligned}$$

□

Corollaire 11.0.11. *Les algèbres de Clifford réelles $C_{4,0}$ et $C_{0,4}$ associées respectivement aux formes quadratiques $\langle 1,1,1,1\rangle$ et $\langle -1,-1,-1,-1\rangle$ sont isomorphes en tant qu'algèbres $\mathbb{Z}/2$-graduées et ainsi il existes des formes quadratiques régulières de dimension 4 non équivalentes, dont les algèbres de Clifford sont isomorphes en tant qu'algèbres $\mathbb{Z}/2$-graduées.*

Démonstration. $C_{4,0} = C\langle 1,1,1,1\rangle$ et $C_{0,4} = C\langle -1,-1,-1,-1\rangle$. On a de plus : $\langle -1,-1,-1,-1\rangle \simeq -1\langle 1,1,1,1\rangle$. Alors, $\Delta(\langle 1,1,1,1\rangle) = 1 \in \mathbb{R}^*/(\mathbb{R}^*)^2$ et -1 étant représenté par $\langle 1,-1\rangle$, d'après la proposition précédente avec $\alpha = -1$:

$$\begin{aligned} C_{4,0} = C\langle 1,1,1,1\rangle &\simeq C(-1\langle 1,1,1,1\rangle) \\ &\simeq C\langle -1,-1,-1,-1\rangle \\ &\simeq C_{0,4} \end{aligned}$$

Enfin, puisque $\langle 1,1,1,1\rangle$ et $\langle -1,-1,-1,-1\rangle$ n'ont pas la même signature, elles ne sont pas équivalentes en tant que formes quadratiques réelles. Pourtant, elles ont des algèbres associées isomorphes en tant qu'algèbres $\mathbb{Z}/2$-graduées, ce qui donne un exemple de deux formes quadratiques régulières de dimension 4 non équivalentes, dont les algèbres de Clifford associées sont isomorphes en tant qu'algèbres graduées. □

De la proposition précédente on déduit que si q et q' sont deux formes quadratiques régulières de dimension 4 avec $q' \simeq \alpha q$ pour α représenté par $\langle 1,-\delta\rangle$ où $\delta = \Delta(q)$, alors $C(q') \simeq C(q)$ en tant qu'algèbres $\mathbb{Z}/2$-graduées. On va alors étudier la véracité de la réciproque dans la proposition suivante afin d'obtenir une condition nécessaire et suffisante pour que deux formes quadratiques q et q' aient des algèbres de Clifford associées isomorphes en tant qu'algèbres graduées. Avant d'énoncer cette condition nécessaire et suffisante, voici deux lemmes qui seront utiles à la démonstration de cette future proposition.

Lemme 11.0.3. *Soit (E,q) un espace quadratique régulier. On note x, y deux élements non nuls de E, alors x et y commutent dans $C(q)$ si et seulement si x et y sont colinéaires.*

Démonstration. On note $n = dim(E) \in \mathbb{N}^*$ et $(e_i)_{1\leq i\leq n}$ une base q-orthogonale de (E,q). On décompose alors x et y dans la base $(e_i)_{1\leq i\leq n}$ de E :

$$x = \alpha_1 e_1 + \alpha_2 e_2 + \cdots + \alpha_n e_n \text{ et } y = \beta_1 e_1 + \beta_2 e_2 + \cdots + \beta_n e_n$$

Alors, on note toujours x, y les éléments de E vus comme des éléments de $C(q)$ avec comme on l'a vu $E \hookrightarrow C(q)$. On a alors :

$$\begin{aligned} xy = &\ (\alpha_1 e_1 + \alpha_2 e_2 + \cdots + \alpha_n e_n)(\beta_1 e_1 + \beta_2 e_2 + \cdots + \beta_n e_n) \\ = &\ \textstyle\sum_{i=1}^n \alpha_i\beta_i e_i^2 + \sum_{i<j}(\alpha_i\beta_j - \beta_i\alpha_j)e_ie_j \\ = &\ \textstyle\sum_{i=1}^n \alpha_i\beta_i q(e_i)1_{C(q)} + \sum_{i<j}(\alpha_i\beta_j - \beta_i\alpha_j)e_ie_j \end{aligned}$$

et

$$\begin{aligned} yx = &\ (\beta_1 e_1 + \beta_2 e_2 + \cdots + \beta_n e_n)(\alpha_1 e_1 + \alpha_2 e_2 + \cdots + \alpha_n e_n) \\ = &\ \textstyle\sum_{i=1}^n \beta_i\alpha_i e_i^2 + \sum_{i<j}(\beta_i\alpha_j - \alpha_i\beta_j)e_ie_j \\ = &\ \textstyle\sum_{i=1}^n \beta_i\alpha_i q(e_i)1_{C(q)} + \sum_{i<j}(\beta_i\alpha_j - \alpha_i\beta_j)e_ie_j \end{aligned}$$

Comme $(e_I)_{I\subset\mathcal{P}([1,n])}$ est une base de $C(q)$, $(e_ie_j)_{i<j}$ en est une famille libre. Alors, x et y commutent dans $C(q)$ si et seulement si et $xy-yx=0$, soit :

$$\begin{aligned}
xy-yx=0 &\iff \textstyle\sum_{i<j}(\alpha_i\beta_j-\beta_i\alpha_j)e_ie_j-\sum_{i<j}(\beta_i\alpha_j-\alpha_i\beta_j)e_ie_j=0\\
&\iff \textstyle\sum_{i<j}(\alpha_i\beta_j-\beta_i\alpha_j-\beta_i\alpha_j+\alpha_i\beta_j)e_ie_j=0\\
&\iff \textstyle\sum_{i<j}2(\alpha_i\beta_j-\beta_i\alpha_j)e_ie_j=0\\
&\iff \forall i<j,\ \alpha_i\beta_j-\beta_i\alpha_j=0\\
&\iff \forall i<j,\ \alpha_i\beta_j=\beta_i\alpha_j\\
&\iff x \text{ et } y \text{ sont colinéaires}
\end{aligned}$$

□

Lemme 11.0.4. *Soit (E,q) un espace quadratique régulier de dimension 4 et soit F un sous-espace vectoriel de $C_1(q)$ de dimension 4 tel que $\forall x\in F, x^2\in\mathbb{K}$. Pour (e_1,e_2,e_3,e_4), base q-orthogonale de E et $t:=e_1e_2e_3e_4\in C(q)$, il existe $(a,b)\in\mathbb{K}^2$ non nul tel que :*

$$F=\{x(a+bt),x\in E\}.$$

De plus, en supposant que la forme quadratique q_1 définie par :

$$q_1:\begin{cases}F\longrightarrow\mathbb{K}\\ x\longmapsto x^2\end{cases}$$

est régulière, il existe α non nul représenté par $\langle 1,-\delta\rangle$ tel que $q_1\simeq\alpha q$.

Démonstration. q étant régulière, il existe une base (e_1,e_2,e_3,e_4) de E, q-orthogonale, telle que $q(e_i)\neq 0$ pour $i\in[\![1,4]\!]$. On pose $t:=e_1e_2e_3e_4\in C(q)$. On va commencer par montrer dans un premier temps que tout élément de $C_1(q)$ s'écrit de manière unique $x+ty$ pour $(x,y)\in E^2$. On sait que $C(q)$ est un espace vectoriel de dimension 2^4 et donc par conséquent que $C_1(q)$ est un sous espace vectoriel de celui-ci de dimension 2^3 dont une base usuelle est donnée par $\{e_1,e_2,e_3,e_4,e_1e_2e_3,e_1e_2e_4,e_1e_3e_4,e_2e_3e_4\}$. Ainsi, pour $z\in C_1(q)$ il existe un unique octuplet $(a_i)_{1\leq i\leq 8}$ tel que :

$$z=a_1e_1+a_2e_2+a_3e_3+a_4e_4+a_5e_1e_2e_3+a_6e_1e_2e_4+a_7e_1e_3e_4+a_8e_2e_3e_4$$

De plus, par les règles de calculs dans l'algèbre de Clifford $C(q)$ on a :

1. $e_1e_2e_3=q(e_4)^{-1}te_4$
2. $e_1e_2e_4=-q(e_3)^{-1}te_3$
3. $e_1e_3e_4=q(e_2)^{-1}te_2$
4. $e_2e_3e_4=-q(e_1)^{-1}te_1$

Ce qui donne bien l'écriture : $z=x+ty$ avec $x=a_1e_1+a_2e_2+a_3e_3+a_4e_4\in E$ et $y=(a_5q(e_4)^{-1}e_4-a_6q(e_3)^{-1}e_3+a_7q(e_2)^{-1}e_2-a_8q(e_1)^{-1}e_1)\in E$. Si on suppose $z=x+ty=x'+ty'$ avec $(x,x',y,y')\in E^4$. Alors $(x-x')+t(y-y')=0$ avec $x-x'\in vect(e_1,e_2,e_3,e_4)$ et $t(y-y')\in vect(e_1e_2e_3,e_1e_2e_4,e_1e_3e_4,e_2e_3e_4)$ et par unicité de la décomposition dans la base usuelle de $C_1(q)$ rappelée ci-dessus, il vient $x-x'=0$ et $y-y'=0$ soit $(x,y)=(x',y')$, d'où l'unicité d'écriture.

On va ensuite montrer que :

$$\{z\in C_1(q),z^2\in\mathbb{K}\}=\{x(a+bt)\mid x\in E,(a,b)\in\mathbb{K}^2\}.$$

ce qui nous permettra d'exprimer F sous la forme d'un espace vectoriel de dimension 4, $F_{a,b} = \{x(a+bt), x \in E\}$ pour $(a,b) \neq (0,0)$. On prouve l'égalité des ensembles ci-dessus par double inclusion. Soit donc $z = x(a+bt)$, il vient $z = ax + xbt = ax - btx$ puisque $x \in E$ et que pour les éléments e_i de la base q-orthogonale de E, on a $e_i t = -te_i$, ($n = 4$ étant pair, le produit $t = e_1e_2e_3e_4$ anticommute avec tous les e_i, $i \in [\![1,4]\!]$) et donc :

$$z = ax - btx = ax + t(-bx) \text{ avec } (ax, -bx) \in E^2$$

ce qui nous donne $z \in C_1(q)$ d'après ce qu'on a vu précédemment. Maintenant il reste à montrer que $z^2 \in \mathbb{K}$. On a :

$$\begin{aligned} z^2 &= (x(a+bt))^2 \\ &= (ax - btx)^2 \\ &= (ax)^2 - abxtx - abtx^2 + b^2txtx \\ &= a^2x^2 + abtx^2 - abtx^2 - b^2tx^2t \\ &= a^2q(x) - b^2q(x)t^2 \\ &= a^2q(x) - b^2q(x)q(e_1)q(e_2)q(e_3)q(e_4) \in \mathbb{K} \end{aligned}$$

Donc si $z = x(a+bt)$, on a bien $z \in C_1(q)$ et $z^2 \in \mathbb{K}$, ce qui nous donne :

$$\{z \in C_1(q), z^2 \in \mathbb{K}\} \subset \{x(a+bt) \mid x \in E, (a,b) \in \mathbb{K}^2\}.$$

Réciproquement, soit $z \in C_1(q)$ tel que $z^2 \in \mathbb{K}$. Comme $z \in C_1(q)$, il existe un unique couple $(x,y) \in E^2$ tel que $z = x + ty$ et on a :

$$\begin{aligned} z^2 &= (x+ty)^2 \\ &= x^2 + xty + tyx + tyty \\ &= x^2 - txy + tyx - ty^2t \\ &= q(x) - txy + tyx - q(x)t^2 \\ &= q(x) + t(yx - xy) - q(x)q(e_1)q(e_2)q(e_3)q(e_4) \end{aligned}$$

Or $q(x) \in \mathbb{K}$ et $q(x)q(e_1)q(e_2)q(e_3)q(e_4) \in \mathbb{K}$ donc :

$$\begin{aligned} z^2 \in \mathbb{K} &\iff yx - xy = 0 \\ &\iff yx = xy \in C(q) \\ &\iff x \text{ et } y \text{ sont colinéaires} \end{aligned}$$

Pour que $z^2 \in \mathbb{K}$, il faut et il suffit que x et y soient colinéaires, et donc qu'il existe $\lambda \in \mathbb{K}$ tel que $y = \lambda x$. Ainsi, z s'écrit alors $x + t(\lambda x) = x(1 - \lambda t)$ avec $(1, -\lambda) \in \mathbb{K}^2$ ce qui nous donne l'inclusion

$$\{x(a+bt) \mid x \in E, (a,b) \in \mathbb{K}^2\} \subset \{z \in C_1(q), z^2 \in \mathbb{K}\}$$

et le résultat attendu par double inclusion. On montre ensuite :

$$\exists (a,b) \neq (0,0) \in \mathbb{K}^2, F = F_{a,b} = \{x(a+bt) \mid x \in E\}$$

On note $Z = \{z \in C_1(q), z^2 \in \mathbb{K}\} = \{x(a+bt), x \in E, (a,b) \in \mathbb{K}^2\}$ et

$$F_{a,b} = E(a+tb) = \{x(a+bt), x \in E\} \text{ pour } (a,b) \neq (0,0) \in \mathbb{K}^2.$$

$F_{a,b}$ est alors un sous espace de dimension 4 de $C_1(q)$ avec $F_{a,b} = F_{a',b'}$ si (a,b) et (a',b') sont colinéaires. On rappelle que F est un sous-espace de dimension 4 de $C_1(q)$ tel que $\forall y \in F, y^2 \in \mathbb{K}$, alors $F \subset Z$ et on va montrer qu'il existe $(a,b) \neq (0,0)$ tel que $F = F_{a,b}$. Soit donc $y \in F$ non nul. Comme $F \subset Z$, y s'écrit $x_1(a+bt)$ pour $x_1 \in E$ et $(a,b) \neq (0,0) \in \mathbb{K}^2$. Par l'absurde, on suppose que tous les éléments de F s'écrivent $x_1(a'+b't)$, où x_1 est fixé et (a',b') parcourt $\mathbb{K}^2$. Ainsi,

$$F \subset F_{x_1} = \{x_1(a+bt), (a,b) \in \mathbb{K}^2\}$$

avec F qui est de dimension 4, et F_{x_1} de dimension 2, absurde. Donc il existe dans F un autre élément noté y' tel que $y' = x'(a'+b't)$ avec x_1 et x' non colinéaires. Alors la somme $y + y' \in F$ ce qui se traduit par :

$$\begin{aligned} y + y' = & \quad x_1(a+bt) + x'(a'+b't) \\ = & \quad (ax_1 + a'x') + (bx_1 + b'x')t \\ = & \quad (ax_1 + a'x') + \lambda(ax_1 + a'x')t \end{aligned}$$

où la troisième égalité vient du fait que $y+y' \in \{x(a+bt), x \in E, (a,b) \in \mathbb{K}^2\}$ et donc s'écrit $x_2(a_2+b_2t)$. Par unicité d'écriture dans $C_1(q)$ sous la forme $x+ty$, pour $(x,y) \in E^2$ on a :

$$ax_1 + a'x' = a_2x_2 \text{ et } bx_1 + b'x' = b_2x_2$$

et sont nécessairement colinéaires. Ainsi $(bx_1 + b'x') = \lambda(ax_1 + a'x')$ ce qui donne :

$$\begin{aligned} & (b - \lambda a)x_1 + (b' - \lambda a')x' = 0 \\ \iff \quad & (b - \lambda a) = 0 \,\text{et}\, (b' - \lambda a') = 0 \,\text{car } x_1 \text{ et } x' \text{ sont indépendants} \\ \iff \quad & b = \lambda a \,\text{et}\, b' = \lambda a' \\ \implies \quad & (a,b) \,\text{et} (a',b') \,\text{sont colinéaires} \\ \implies \quad & y, y' \in F_{a,b} = F_{a',b'} \end{aligned}$$

Ainsi, pour $y' = x'(a'+b't)$ dans F tel que x_1 et x' non colinéaires on a nécessairement (a,b) et (a',b') colinéaires soit $y, y' \in F_{a,b}$. Par l'étude ci dessus, on voit donc que si deux éléments $x(a+bt)$ et $x'(a'+b't)$ de F sont tels que x et x' non colinéaires, nécessairement (a,b) et (a',b') eux le sont. Pour (a,b) fixé tel que $y = x_1(a+bt) \in F$, on note $E' = \{x \in E, x(a+bt) \in F\}$. E' est donc un sous-espace vectoriel de E tel que $E'(a+bt) \subset F$ par construction même de E'. Si on montre que $E' = E$, alors on aura $E(a+bt) = E'(a+bt) \subset F$ avec $E(a+bt)$ et F tous deux de dimension 4 ce qui nous donnera $E(a+bt) = F_{a,b} = F$.

Supposons par l'absurde que $E' \neq E$. Alors, il existe un élément de F qui n'appartient pas à $E'(a+tb)$. En effet, sinon F serait inclus dans $E'(a+bt)$ et on aurait $F = E'(a+tb)$. Or, $E'(a+bt) \subset E(a+bt)$ où $E(a+bt)$ est de dimension 4, par raison de dimension on aurait $F = E(a+bt)$ et donc $E = E'$. D'où, si $E \neq E'$, il existe $w = x(a'+b't) \in F$ qui n'est pas dans $E'(a+bt)$. On a donc (a',b') non colinéaire à (a,b), car sinon w s'écrirait $x(\lambda a + \lambda bt)$ et λx serait donc dans E' et w dans $E'(a+bt)$, absurde. Pour tout $x' \in E'$, $x'(a+bt) \in F$, tout comme $w = x(a'+b't)$, alors comme (a,b) et (a',b') sont non colinéaires, nécessairement x' et x eux le sont (on a déjà montré que si x et x' sont indépendants alors (a,b) et (a',b') sont nécessairement colinéaires, ce

qui n'est pas). Donc x est colinéaire à tous les x' de E' et les élements de E' sont tous colinéaires à x, ce qui implique que E' est une droite vectorielle. Comme $y = x_1(a+bt) \in F$ on a $x_1 \in E'$ et $E' = vect(x_1)$. D'où, si $E' \neq E$

$$E^{'}(a+bt) = vect(x_1)(a+bt) \subset F$$

et un élément w dans $F \backslash E^{'}(a+bt)$ s'écrit aussi $x_1(a'+b't)$, ce qui signifie en particulier que F est inclus dans le sous-espace engendré par x_1 et $x_1 t$ qui est de dimension 2, absurde. D'où $E' = E$ et $F = F_{a,b}$.

Soit

$$q_1 : \begin{cases} F \longrightarrow \mathbb{K} \\ y \longmapsto y^2 \end{cases}$$

La définition ci-dessus est bien licite puisque $\forall y \in F$, $y^2 \in \mathbb{K}$. Pour $y \in F = F_{a,b}$, il existe un unique $x \in E$ tel que $y = x(a+bt)$ (par unicité de l'écriture sous la forme $x + ty$ dans $C_1(q)$ avec $F \subset C_1(q)$) et alors,

$$\begin{aligned} q_1(y) &= q_1(x(a+bt)) \\ &= q_1(ax - btx) \\ &= (ax - btx)^2 \\ &= a^2 q(x) - b^2 q(x) q(e_1) q(e_2) q(e_3) q(e_4) \\ &= (a^2 - q(e_1)q(e_2)q(e_3)q(e_4)b^2) q(x) \end{aligned}$$

Or (e_1, e_2, e_3, e_4) étant une base q-orthogonale, $q \simeq \langle q(e_1), q(e_2), q(e_3), q(e_4) \rangle$ et donc $\Delta(q) = q(e_1)q(e_2)q(e_3)q(e_4) = \delta$ dans $\mathbb{K}^*/(\mathbb{K}^*)^2$. On note alors

$$\alpha = a^2 - q(e_1)q(e_2)q(e_3)q(e_4)b^2$$

qui est non nul, puisque sinon q_1 serait nulle et non régulière. α est donc représenté par la forme quadratique diagonale $\langle 1, -q(e_1)q(e_2)q(e_3)q(e_4) \rangle \simeq \langle 1, -\delta \rangle$ et donc α représenté par $\langle 1, -\delta \rangle$. Or l'application

$$u : \begin{cases} E \longrightarrow F \\ x \longmapsto x(a+bt) \end{cases}$$

est un isomorphisme d'espaces vectoriels en raison du fait que tout élément de F s'écrit sous la forme $x(a+bt)$ de manière unique (la linéarité est claire). Ainsi, on a :

$$\forall x \in E, q_1(u(x)) = \alpha q(x)$$

ce qui prouve que $q_1 \simeq \alpha q$ pour α non nul représenté par $\langle 1, -\delta \rangle$. □

Proposition 11.0.17. *Soit (E, q) et (E', q') deux espaces quadratiques réguliers de dimension 4. Alors, les algèbres de Clifford $C(q)$ et $C(q')$ sont isomorphes en tant qu'algèbres $\mathbb{Z}/2$-graduées si et seulement s'il existe deux scalaires non nuls α et β respectivement représentés par $\langle 1, -\delta \rangle$ et $\langle 1, -\delta' \rangle$ tels que $\alpha q \simeq \beta q'$, où δ et δ' désignent des discriminants respectifs de q et q'.*

Démonstration. Supposons qu'il existe deux scalaires non nuls α et β respectivement représentés par $\langle 1, -\delta \rangle$ et $\langle 1, -\delta' \rangle$ tels que $\alpha q \simeq \beta q'$, où δ et δ'. Alors, d'après la proposition 11.0.16 :

$$C(q) \simeq C(\alpha q) \text{ et } C(q') \simeq C(\beta q')$$

Puisque $\alpha q \simeq \beta q'$, on a également $C(\alpha q) \simeq C(\beta q')$ où tous les isomorphismes sont des isomorphismes d'algèbres graduées, ainsi :

$$C(q) \simeq_{\mathbb{Z}/2} C(\alpha q) \simeq_{\mathbb{Z}/2} C(\beta q') \simeq C(q')$$

ce qui donne le sens indirect de l'équivalence de la proposition. On suppose ensuite que les algèbres $C(q)$ et $C(q')$ sont isomorphes en tant qu'algèbres graduées. Ainsi, il existe un isomorphisme d'algèbres Φ tel que $\Phi : C(q) \longrightarrow C(q')$ avec

1. $\Phi(C_0(q)) = C_0(q')$
2. $\Phi(C_1(q)) = C_1(q')$

On note $\delta = q(e_1)q(e_2)q(e_3)q(e_4)$ pour $(e_i)_{1\leq i\leq 4}$ une base q-orthogonale. On choisit alors $F = \{x(a+bt), x \in E\}$ sous-espace de dimension 4 de $C_1(q)$ tel que $a^2 - \delta b^2 = \alpha$ représenté par $\langle 1, -\delta\rangle$ ne soit pas nul. On définit alors q_1 par

$$q_1 : \begin{cases} F \longrightarrow \mathbb{K} \\ y \longmapsto y^2 \end{cases}$$

et on a :

$$\forall x \in E,\ q_1(x(a+bt)) = \alpha q(x)$$

soit donc q_1 régulière sur F et $q_1 \simeq \alpha q$ d'après le lemme 11.0.4 ci-dessus. Alors, $\Phi(F)$ est également un sous espace vectoriel de dimension 4 de $C_1(q')$ tel que $\forall y \in F,\ \Phi(y)^2 = \Phi(y^2) = y^2 \in \mathbb{K}$ (car $\Phi(1) = 1$, Φ étant un morphisme d'algèbres). D'après le lemme 11.0.4, il existe $(a', b') \neq (0, 0)$ tels que :

$$\Phi(F) = \{x'(a' + b't'),\ x' \in E'\}$$

où $t' = e'_1e'_2e'_3e'_4$ pour (e'_1, e'_2, e'_3, e'_4) une base q'-orthogonale de E'. On définit alors q_2 par :

$$q_2 : \begin{cases} \Phi(F) \longrightarrow \mathbb{K} \\ z \longmapsto z^2 \end{cases}$$

Alors pour $z \in \Phi(F)$ il existe un unique $y \in F$ tel que $z = \Phi(y)$ et on a :

$$q_2(z) = q_2(\Phi(y)) = \Phi(y)^2 = \Phi(y^2) = y^2 = q_1(y)$$

soit donc

$$\forall y \in F,\ q_2(\Phi(y)) = q_1(y)$$

Or, Φ étant un isomorphisme d'espaces vectoriels entre F et $\Phi(F)$, la dernière égalité montre que

$$q_2 \simeq q_1$$

et en particulier q_2 est bien régulière. Pour $z \in \Phi(F)$, z s'écrit $x'(a' + b't')$ et on a :

$$\begin{aligned} q_2(z) &= q_2(x'(a' + b't')) \\ &= q_2(a'x' - b't'x') \\ &= (a'x' - b't'x')^2 \\ &= a'^2q'(x') - b'^2q'(x')q'(e'_1)q'(e'_2)q'(e'_3)q'(e'_4) \\ &= (a'^2 - q'(e'_1)q'(e'_2)q'(e'_3)q'(e'_4)b'^2)q'(x') \end{aligned}$$

Notant $\beta = (a'^2 - q'(e'_1)q'(e'_2)q'(e'_3)q'(e'_4)b'^2)$, β est non nul (q_2 régulière) et représenté par $\langle 1, -\delta' \rangle$ où $\delta' = q'(e'_1)q'(e'_2)q'(e'_3)q'(e'_4)$ est un discriminant de q'. On a également :

$$q_2(x'(a' + b't')) = \beta q'(x').$$

On note v l'application suivante :

$$v\colon \begin{cases} E' \longrightarrow \Phi(F) \\ x' \longmapsto x'(a' + b't') \end{cases}$$

v est ainsi un isomorphisme d'espace vectoriel puisque tout élément de $\Phi(F)$ s'écrit sous la forme $x'(a' + b't')$ de manière unique (la linéarité est claire). Ainsi,

$$\forall x' \in E',\ q_2(v(x)) = \beta q'(x')$$

ce qui prouve que $q_2 \simeq \beta q'$ pour β non nul représenté par $\langle 1, -\delta' \rangle$. Au final, il vient :

$$\beta q' \simeq q_2 \simeq q_1 \simeq \alpha q$$

où α est représenté par $\langle 1, -\delta \rangle$ et β est représenté par $\langle 1, -\delta' \rangle$. Ce qui achève de montrer la proposition. □

Application 11.0.1. *Soit $\mathbb{K}$ un corps fini et ε est un représentant de la classe des non carré. Les algèbres de Clifford $C\langle 1,1,1,1\rangle$, $C\langle 1,1,1,\varepsilon\rangle$ bien qu'isomorphes, ne le sont pas en tant qu'algèbres $\mathbb{Z}/2$-graduées.*

Démonstration. Les formes quadratiques $\langle 1,1,1,1\rangle$ et $\langle 1,1,1,\varepsilon\rangle$ ont des algèbres de Clifford associées isomorphes sur $\mathbb{K}$. En effet, par dévissage on a :

$$C\langle 1,1,1,1\rangle \simeq (-1,-1) \otimes (-1,1) \text{ et } C\langle 1,1,1,\varepsilon\rangle \simeq (-1,-1) \otimes (-1,\varepsilon)$$

et d'après l'étude des algèbre de quaternions, on a les isomorphismes d'algèbres suivants :

$$(-1,-1) \simeq \mathcal{M}_2(\mathbb{K}) \text{ et } (-1,\varepsilon) \simeq \mathcal{M}_2(\mathbb{K})$$

et donc en tant qu'algèbres, on a :

$$C\langle 1,1,1,1\rangle \simeq \mathcal{M}_2(\mathbb{K}) \otimes \mathcal{M}_2(\mathbb{K}) \text{ et } C\langle 1,1,1,\varepsilon\rangle \simeq \mathcal{M}_2(\mathbb{K}) \otimes \mathcal{M}_2(\mathbb{K}).$$

En revanche ces algèbres de Clifford ne sont pas isomorphes en tant qu'algèbres graduées. Sinon, il existerait α et β non nuls respectivement représentés par $\langle 1,-1\rangle$ et $\langle 1,-\varepsilon\rangle$ et tels que

$$\alpha\langle 1,1,1,1\rangle \simeq \beta\langle 1,1,1,\varepsilon\rangle.$$

Or, $\Delta(\beta\langle 1,1,1,\varepsilon\rangle) = \beta^4\varepsilon = \varepsilon$ et $\Delta(\alpha\langle 1,1,1,1\rangle) = \alpha^4 = 1$ dans $\mathbb{F}_p^*/(\mathbb{F}_p^*)^2$ avec $\varepsilon \neq 1$ dans $\mathbb{F}_p^*/(\mathbb{F}_p^*)^2$. D'où, $\alpha\langle 1,1,1,1\rangle \not\simeq \beta\langle 1,1,1,\varepsilon\rangle$ et les algèbres de Clifford $C\langle 1,1,1,1\rangle$ et $C\langle 1,1,1,\varepsilon\rangle$ ne sont donc pas isomorphes en tant qu'algèbres graduées.

□

11.0.14 Dévissage d'une algèbre de Clifford

Les théorèmes de structure en dimension 3 et 4 ont montré que l'on pouvait décomposer toute algèbre de Clifford en dimension 3 et 4 en un produit tensoriel gradué d'algèbres de quaternions et d'algèbres de Clifford en dimension 1. Nous allons voir que ceci se généralise en dimension quelconque avec une distinction à faire selon la parité de la dimension.

Considérons l'algèbre de Clifford $C\langle a_1, \ldots, a_n\rangle$ pour $a_1, \ldots, a_n \in \mathbb{K}^*$. Par la proposition 10.0.7, la décomposition :

$$\langle a_1, \ldots, a_n\rangle \simeq \langle a_1, a_2, a_3\rangle \perp \langle a_4, \ldots, a_n\rangle$$

donne en termes d'algèbres de Clifford, la décomposition :

$$C\langle a_1, \ldots, a_n\rangle \simeq_{\mathbb{Z}/2} C\langle a_1, a_2, a_3\rangle \widehat{\otimes} C\langle a_4, \ldots, a_n\rangle$$

L'application du lemme de dévissage nous donne :

$$C\langle a_1, \ldots, a_n\rangle \simeq_{\mathbb{Z}/2} (-a_1a_3, -a_2a_3)\widehat{\otimes} C\langle -a_1a_2a_3\rangle \widehat{\otimes} C\langle a_4, \ldots, a_n\rangle$$

où $(-a_1a_3, -a_2a_3)$ est trivialement graduée. Il s'agit ensuite de recomposer $C\langle -a_1a_2a_3\rangle \widehat{\otimes} C\langle a_4, \ldots, a_n\rangle$ sous la forme $C\langle -a_1a_2a_3, a_4, \ldots, a_n\rangle$ (via la proposition 10.0.7), puis de poursuivre les opérations de dévissage sur l'algèbre de dimension inférieure $C\langle -a_1a_2a_3, a_4, \ldots, a_n\rangle$ jusqu'à trouver comme dernier terme du produit tensoriel une algèbre de quaternions ou une algèbre de Clifford associée à une droite quadratique régulière. Ainsi, en raison des dimensions :

- si $n = 2l$ est pair, $dim(C(q)) = 2^{2l} = 4^l$ et $C(q)$ s'écrit comme un produit tensoriel gradué de l algèbres de quaternions de dimension 4.
- si $n = 2l + 1$ est impair, $dim(C(q)) = 2^{2l+1} = 2 \times 4^l$ et $C(q)$ s'écrit comme un produit tensoriel gradué de l algèbres de quaternions de dimension 4 et d'une algèbre de Clifford de dimension 2, associée à une droite quadratique régulière.

L'étude du dévissage complet d'une algèbre de Clifford a permis de mettre en évidence que toute algèbre de Clifford se décompose sous la forme d'un produit tensoriel d'algèbres de quaternions ou sous la forme d'un produit tensoriel d'algèbres de quaternions et d'une algèbre de Clifford associée à une droite quadratique. Les théorèmes de structures suivants synthétisent ces résultats.

Structure d'une algèbre de Clifford de dimension paire

Théorème 11.0.8. ***Structure de l'algèbre de Clifford régulière en dimension paire***
Soit (E, q) un espace quadratique régulier de dimension paire $n = 2m$ et de discriminant δ.

1. *L'algèbre $C(q)$ est isomorphe au produit tensoriel de m algèbres de quaternions.*
2. *L'algèbre $C(q)$ est centrale.*
3. *Si $\delta \in \mathbb{K}^2$, alors il existe une algèbre centrale $\mathcal{A}$ telle que $C_0(q) \simeq \mathcal{A} \times \mathcal{A}$.*
4. *Si $\delta \notin \mathbb{K}^2$, alors $\mathcal{Z}(C_0(q)) \simeq \mathbb{K}[\sqrt{\delta}]$.*

Structure d'une algèbre de Clifford de dimension impaire

Théorème 11.0.9. ***Structure de l'algèbre de Clifford régulière en dimension impaire***
Soit (E, q) un espace quadratique régulier de dimension impaire $n = 2m + 1$ et de discriminant δ.

1. *L'algèbre $C_0(q)$ est isomorphe au produit tensoriel de m algèbres de quaternions.*
2. *L'algèbre $C_0(q)$ est centrale.*
3. *Si $\delta \in \mathbb{K}^2$, alors $C(q) \simeq C_0(q) \times C_0(q)$.*
4. *Si $\delta \notin \mathbb{K}^2$ alors $C(q) \simeq C_0(q)\widehat{\otimes}\mathbb{K}[\sqrt{\delta}]$ et $\mathcal{Z}(q) \simeq_{\mathbb{Z}/2} C\langle\delta\rangle$.*

Structure des algèbres de Clifford sur les corps finis

Nous allons appliquer les résultats énoncés dans les théorèmes 11.0.8 et 11.0.9 au cas d'une forme régulière q sur un corps fini $\mathbb{F}_p$, où p ne désigne pas nécessairement un nombre premier mais toujours une puissance d'un nombre premier.

Proposition 11.0.18. *Soit q une forme quadratique régulière de dimension n sur le corps fini $\mathbb{F}_p$ et soit δ un discriminant de q. Alors :*

1. *Pour n pair, $C(q) \simeq \mathcal{M}_{2^{n/2}}(\mathbb{F}_p)$.*
2. *Pour n impair et $\delta \in (\mathbb{F}_p^*)^2$, $C(q) \simeq \mathcal{M}_{2^{(n-1)/2}}(\mathbb{F}_p) \times \mathcal{M}_{2^{(n-1)/2}}(\mathbb{F}_p)$.*
3. *Pour n impair et $\delta \notin (\mathbb{K}^*)^2$, $C(q) \simeq \mathcal{M}_{2^{(n-1)/2}}(\mathbb{F}_{p^2})$.*

Afin de démontrer cette proposition nous aurons besoin du lemme suivant :

Lemme 11.0.5. *Soit n, p deux entiers non nuls, $\mathbb{K}$ un corps et $\mathbb{L}$ un surcorps de $\mathbb{K}$. On a les résulats suivants :*

1. *$\mathcal{M}_n(\mathbb{K}) \otimes \mathcal{M}_p(\mathbb{K}) \simeq \mathcal{M}_{np}(\mathbb{K})$ en tant qu'algèbres.*
2. *$\mathcal{M}_n(\mathbb{K}) \otimes \mathbb{L} \simeq \mathcal{M}_n(\mathbb{L})$ en tant qu'algèbres.*

Démonstration. 1) Soit $A = (a_{i,j})_{1 \leq i,j \leq n} \in \mathcal{M}_n(\mathbb{K})$ et $B \in \mathcal{M}_p(\mathbb{K})$. On considère l'application définie par :

$$\Phi\colon \begin{cases} \mathcal{M}_n(\mathbb{K}) \times \mathcal{M}_p(\mathbb{K}) \longrightarrow \mathcal{M}_{np}(\mathbb{K}) \\ (A, B) \longmapsto \begin{pmatrix} a_{1,1}B & \dots & a_{1,n}B \\ \vdots & \ddots & \vdots \\ a_{n,1}B & \dots & a_{n,n}B \end{pmatrix} \end{cases}$$

Cette application est clairement bilinéaire et donc par la propriété universelle du produit tensoriel, il existe une unique application linéaire $\overline{\Phi}$ définie de $\mathcal{M}_n(\mathbb{K}) \otimes \mathcal{M}_p(\mathbb{K})$ à valeurs dans $\mathcal{M}_{np}(\mathbb{K})$ telle qu'on ait :

$$\forall A, B \in \mathcal{M}_n(\mathbb{K}) \times \mathcal{M}_p(\mathbb{K}),\ \overline{\Phi}(A \otimes B) = \Phi(A, B) = \begin{pmatrix} a_{1,1}B & \dots & a_{1,n}B \\ \vdots & \ddots & \vdots \\ a_{n,1}B & \dots & a_{n,n}B \end{pmatrix}.$$

Plaçons nous désormais dans le cas $n, p = 2$ et soit alors $C = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ b_1 & b_2 & b_3 & b_4 \\ c_1 & c_2 & c_3 & c_4 \\ d_1 & d_2 & d_3 & d_4 \end{pmatrix}$.

Un antécédent de C par $\overline{\Phi}$ est alors donné par :

$$\begin{pmatrix} a_1 & a_3 \\ c_1 & c_3 \end{pmatrix} \otimes E_{1,1} + \begin{pmatrix} a_2 & a_4 \\ c_2 & c_4 \end{pmatrix} \otimes E_{1,2} + \begin{pmatrix} b_1 & b_3 \\ d_1 & d_3 \end{pmatrix} \otimes E_{2,1} + \begin{pmatrix} b_2 & a_4 \\ d_1 & d_4 \end{pmatrix} \otimes E_{2,2}$$

Ce qui prouve la surjectivité de $\overline{\Phi}$ dans le cas où $n, p = 2$. On montre par le même type de raisonnement la surjectivité de $\overline{\Phi}$ dans le cadre général. Ainsi $\overline{\Phi}$ est surjective et puisque les espaces vectoriels $\mathcal{M}_n(\mathbb{K}) \otimes \mathcal{M}_p(\mathbb{K})$ et $\mathcal{M}_{np}(\mathbb{K})$ ont même dimension, on a bien l'isomorphisme d'espaces vectoriels annoncé. Il reste à montrer qu'il s'agit en fait également d'un isomorphisme d'algèbres.

Revenons au cas $n, p = 2$ et définissons les matrices A, B, C, D par :

$$A = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix},\ B = \begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix},\ C = \begin{pmatrix} c_1 & c_2 \\ c_3 & c_4 \end{pmatrix},\ D = \begin{pmatrix} d_1 & d_2 \\ d_3 & d_4 \end{pmatrix}$$

On a alors par produit matriciel par blocs :

$$\begin{aligned} \overline{\Phi}(A \otimes C)\overline{\Phi}(B \otimes D) &= \begin{pmatrix} a_1 C & a_2 C \\ a_3 C & a_4 C \end{pmatrix} \begin{pmatrix} b_1 D & b_2 D \\ b_3 D & b_4 D \end{pmatrix} \\ &= \begin{pmatrix} (a_1 b_1 + a_2 b_3) CD & (a_1 b_2 + a_2 b_4) CD \\ (a_3 b_1 + a_4 b_3) CD & (a_3 b_2 + a_4 b_4) CD \end{pmatrix} \\ &= \overline{\Phi}(AB \otimes CD). \end{aligned}$$

Ceci montre dans le cas $n, p = 2$ que l'isomorphisme d'espaces vectoriels est en fait un isomorphisme d'algèbres (il suffit de vérifier le caractère multiplicatif sur les tenseurs purs par linéarité de $\overline{\Phi}$). Dans le cadre général, le fait que $\overline{\Phi}$ soit en fait un isomorphisme d'algèbres se montre de manière identique et on a bien :

$$\mathcal{M}_n(\mathbb{K}) \otimes \mathcal{M}_p(\mathbb{K}) \simeq \mathcal{M}_{np}(\mathbb{K}) \text{ en tant qu'algèbres.}$$

2) On considère l'application :

$$\Psi : \begin{cases} \mathcal{M}_n(\mathbb{K}) \times \mathbb{L} \longrightarrow \mathcal{M}_n(\mathbb{L}) \\ (A, x) \longmapsto (a_{i,j} x)_{1 \leq i,j \leq n} \end{cases}$$

L'application Ψ étant clairement bilinéaire, par la propriété universelle du produit tensoriel, il existe une unique application linéaire $\overline{\Psi}$ définie de $\mathcal{M}_n(\mathbb{K}) \otimes \mathbb{L}$ à valeurs dans $\mathcal{M}_n(\mathbb{L})$ pour laquelle on a :

$$\forall (A, x) \in \mathcal{M}_n(\mathbb{K}) \times \mathbb{L}, \overline{\Psi}(A \otimes x) = \Psi(A, x).$$

La surjectivité de l'application $\overline{\Psi}$ découle alors simplement du fait que pour $A = (a_{i,j})_{1 \leq i,j \leq n} \in \mathcal{M}_n(\mathbb{L})$ on ait :

$$A = \Psi(\textstyle\sum_{i,j} E_{i,j} \otimes a_{i,j}), \text{ pour } a_{i,j} \in \mathbb{L} \text{ et } E_{i,j} \in \mathcal{M}_n(\mathbb{K}).$$

Les espaces d'arrivée et de départ ayant même dimension, on en déduit l'isomorphisme annoncé mais en tant qu'isomorphisme d'espaces vectoriels. Le fait qu'il soit également un isomorphisme d'algèbres est clair puisque sur les tenseurs purs, (il suffit de vérifier le caractère multiplicatif sur les tenseurs purs par linéarité de $\overline{\Psi}$) et pour $AB = (c_{i,j})_{1 \leq i,j \leq n}$, on a l'égalité :

$$\begin{aligned} \overline{\Psi}(AB \otimes xy) &= (c_{i,j} xy)_{1 \leq i,j \leq n} \\ &= (a_{i,j} x)_{1 \leq i,j \leq n} (b_{i,j} y)_{1 \leq i,j \leq n} \\ &= \overline{\Psi}(A \otimes x)\overline{\Psi}(B \otimes y) \end{aligned}$$

□

Passons désormais à la démonstration de la proposition.

Démonstration. Soit donc q une forme quadratique régulière sur le corps fini $\mathbb{F}_p$ et δ un discriminant de q.

1) On suppose que la dimension de q est paire. Alors d'après le théorème de structure de l'algèbre de Clifford régulière en dimension paire, il vient que $C(q)$ est isomorphe au produit tensoriel de $\dfrac{n}{2}$ algèbres de quaternions. Or, dans le cadre du corps $\mathbb{F}_p$, toute algèbre de quaternions (a, b) est isomorphe en tant qu'algèbre à $\mathcal{M}_2(\mathbb{F}_p)$ (corollaire 11.0.8). Ainsi,

$$C(q) \simeq \underbrace{\mathcal{M}_2(\mathbb{F}_p) \otimes \mathcal{M}_2(\mathbb{F}_p) \ldots \otimes \mathcal{M}_2(\mathbb{F}_p)}_{\times \frac{n}{2}}$$

et d'après le lemme ci-dessus on en déduit $C(q) \simeq \mathcal{M}_{2^{n/2}}(\mathbb{F}_p)$.

2) On suppose que la dimension de q est impaire et que $\delta \in (\mathbb{F}_p^*)^2$. Alors, par le théorème de structure de l'algèbre de Clifford régulière en dimension impaire, il vient que $C(q) \simeq C_0(q) \times C_0(q)$ où $C_0(q)$ est isomorphe au produit tensoriel de $\dfrac{n-1}{2}$ algèbres de quaternions. Ainsi,

$$C(q) \simeq \underbrace{\mathcal{M}_2(\mathbb{F}_p) \otimes \mathcal{M}_2(\mathbb{F}_p) \ldots \otimes \mathcal{M}_2(\mathbb{F}_p)}_{\times \frac{n-1}{2}} \times \underbrace{\mathcal{M}_2(\mathbb{F}_p) \otimes \mathcal{M}_2(\mathbb{F}_p) \ldots \otimes \mathcal{M}_2(\mathbb{F}_p)}_{\times \frac{n-1}{2}}$$

et d'après le point 1 du lemme ci-dessus,

$$C(q) \simeq \mathcal{M}_{2^{(n-1)/2}}(\mathbb{F}_p) \times \mathcal{M}_{2^{(n-1)/2}}(\mathbb{F}_p).$$

3) On suppose que la dimension de q est impaire et que $\delta \notin (\mathbb{F}_p^*)^2$. Toujours par le théorème de structure de l'algèbres de Clifford régulière en dimension impaire, il vient que $C(q) \simeq C_0(q) \otimes \mathbb{F}_p[\sqrt{\delta}]$ où donc $\mathbb{F}_p[\sqrt{\delta}]$ est un surcorps de $\mathbb{F}_p$ de degré 2, soit $\mathbb{F}_p[\sqrt{\delta}] \simeq \mathbb{F}_{p^2}$. Ainsi :

$$\begin{aligned} C(q) &\simeq C_0(q) \otimes \mathbb{F}_p[\sqrt{\delta}] \\ &\simeq \mathcal{M}_{2^{(n-1)/2}}(\mathbb{F}_p) \otimes \mathbb{F}_{p^2} \\ &\simeq \mathcal{M}_{2^{(n-1)/2}}(\mathbb{F}_{p^2}) \end{aligned}$$

La deuxième équivalence vient du fait que $C_0(q)$ est isomorphe au produit tensoriel de $\dfrac{n-1}{2}$ algèbres de quaternions que δ soit un carré de $\mathbb{F}_p$ ou non. Quant au point 3, il est justifié par la deuxième assertion du lemme ci-dessus. Ceci achève de montrer les résultats de la proposition. □

Remarque 11.0.14. *En particulier sur le corps fini $\mathbb{F}_p$, toutes les algèbres de Clifford associées à des formes quadratiques régulières de dimension 4 sont isomorphes les unes aux autres. En effet, pour ε non carré de $\mathbb{F}_p^*$, à équivalence près il n'y a que deux formes quadratiques régulières de dimension 4 sur $\mathbb{F}_p$ que sont $\langle 1, 1, 1, 1\rangle$ et $\langle 1, 1, 1, \varepsilon\rangle$ et donc $C\langle 1, 1, 1, 1\rangle \simeq C\langle 1, 1, 1, \varepsilon\rangle \simeq \mathcal{M}_4(\mathbb{F}_p)$. En revanche, nous avons déjà vu précédemment qu'elles n'étaient pas isomorphes en tant qu'algèbres $\mathbb{Z}/2$-graduées.*

11.0.15 Algèbre de Clifford d'un espace hyperbolique

Avant de passer à l'étude de la classification des formes quadratiques p-adiques et rationnelles vues sous l'angle de la théorie des algèbres de Clifford, nous allons étudier la structure des algèbres de Clifford associées aux espaces hyperboliques, via l'énonciation de deux théorèmes structurels.

Théorème 11.0.10. ***Effet de l'ajout d'un plan hyperbolique***
Soit q une forme quadratique régulière. On a alors les isomorphismes suivant :

1. $C(\langle 1,-1\rangle \perp q) \simeq_{\mathbb{Z}/2} \mathcal{M}_2(\mathbb{K})\widehat{\otimes}C(q)$ *où* $\mathcal{M}_2(\mathbb{K})$ *est trivialement graduée.*
2. $C(\langle 1,-1\rangle \perp q) \simeq \mathcal{M}_2(\mathbb{K})\widehat{\otimes}C(q)$
3. $C_0(\langle 1,-1\rangle \perp q) \simeq \mathcal{M}_2(\mathbb{K})\widehat{\otimes}C_0(q)$

Remarque 11.0.15. *Ainsi, par décomposition de Witt, on pourra ramener le calcul de l'algèbre de Clifford d'une forme quadratique régulière au calcul de l'algèbre de Clifford de sa partie anisotrope. En effet, pour q forme quadratique régulière, la décomposition de Witt,*

$$q \simeq n.\langle 1,-1\rangle \perp q_a \ (n \in \mathbb{N} \text{ et } q_a \text{ anisotrope})$$

et le théorème précédent nous donne :

$$C(q) \simeq_{\mathbb{Z}/2} \mathcal{M}_2(\mathbb{K})\widehat{\otimes}\ldots\widehat{\otimes}\mathcal{M}_2(\mathbb{K})\widehat{\otimes}C(q_a).$$

Il suffira alors de déterminer la structure de $C(q_a)$ pour connaître la structure de $C(q)$.

Théorème 11.0.11. ***Structure de l'algèbre de Clifford d'un espace hyperbolique***

1. $C(n.\langle 1,-1\rangle) \simeq \mathcal{M}_{2^n}(\mathbb{K})$
2. $C_0(n.\langle 1,-1\rangle) \simeq \mathcal{M}_{2^{n-1}}(\mathbb{K}) \times \mathcal{M}_{2^{n-1}}(\mathbb{K})$

Nous avons désormais en main tous les ingrédients pour pouvoir nous intéresser à la classification des formes p-adiques et rationnelles à l'aide de la théorie des algèbres de Clifford, ce qui clôturera ce mémoire.

11.0.16 Classification des formes quadratiques p-adiques régulières par l'algèbre de Clifford $\mathbb{Z}/2$-graduée associée

Dans les documents précédents, nous avons commencé par étudier la structure des algèbres de Clifford associées aux droites quadratiques. Puis, nous sommes passés à l'étude des formes quadratiques régulières de dimension 2 ce qui nous a amené à étudier en détail les algèbres de quaternions. Le lemme de dévissage nous a alors permis d'étudier les algèbres de Clifford en dimension supérieure, dont les résultats ont été synthétisés dans les théorèmes de structures généraux :

"*structure de l'algèbre de Clifford régulière en dimension paire et structure de l'algèbre de Clifford régulière en dimension impaire*".

Enfin, nous avons terminé par étudier l'effet de l'ajout d'un plan hyperbolique sur l'algèbre de Clifford, permettant de ramener le calcul de l'algèbre de Clifford d'une forme quadratique régulière à celui de sa partie anisotrope ; ceci soulignant de nouveau l'importance de la décomposition de Witt.

Nous allons mettre à profit ces différents résultats pour classifier les formes quadratiques rationnelles à l'aide des algèbres de Clifford associées. Nous obtiendrons ainsi un résultat majeur qui viendra compléter efficacement le test d'équivalence rationnelle, que l'on a eu l'occasion de manipuler à de multiples reprises.

Au cours des chapitres précédents on a pu voir le lien profond qui existait entre une forme quadratique rationnelle q et ses différentes localisées q_p sur $\mathbb{Q}_p$, $p \in \mathcal{P}_\infty$, notamment via les principes de Hasse faible et fort. Dans la suite, nous nous servirons de nouveau de cette importante connexion pour, à partir de la classification des formes quadratiques p-adiques par l'algèbre de Clifford associée, obtenir de manière naturelle la classification des formes quadratiques via l'algèbre de Clifford, dans le cadre du corps $\mathbb{Q}$.

Avant d'énoncer le théorème de classification sur les corps p-adiques, il nous sera nécessaire de développer trois lemmes intermédiaires.

Lemme 11.0.6. *On rappelle que $\mathbb{H}_p$ désigne à isomorphisme près l'unique algèbre de quaternions sur $\mathbb{Q}_p$ qui est un corps. Soit m et n deux entiers naturels, alors $\mathcal{M}_m(\mathbb{Q}_p)$ et $\mathcal{M}_n(\mathbb{H}_p)$ ne sont pas isomorphes en tant qu'anneaux non unitaires.*

Démonstration. On suppose par l'absurde que pour m, n deux entiers non nuls, on a $\mathcal{M}_m(\mathbb{Q}_p) \simeq \mathcal{M}_n(\mathbb{H}_p)$ en tant qu'anneaux non unitaires. On note alors Φ un isomorphisme d'anneaux non unitaires tel que $\Phi : \mathcal{M}_m(\mathbb{Q}_p) \longrightarrow \mathcal{M}_n(\mathbb{H}_p)$. On va montrer dans un premier temps que nécessairement $m = 2n$, en prouvant que Φ envoie tout sous-espace vectoriel du $\mathbb{Q}_p$-espace vectoriel $\mathcal{M}_m(\mathbb{Q}_p)$ sur un sous-espace vectoriel de même dimension du $\mathbb{Q}_p$-espace vectoriel $\mathcal{M}_n(\mathbb{H}_p)$. D'abord, montrons que :

$$\Phi(Z(\mathcal{M}_m(\mathbb{Q}_p))) = Z(\mathcal{M}_n(\mathbb{H}_p)).$$

Soit donc $A \in Z(\mathcal{M}_m(\mathbb{Q}_p))$ on a :

$$\forall B \in \mathcal{M}_m(\mathbb{Q}_p),\ \Phi(AB) = \Phi(A)\Phi(B) = \Phi(B)\Phi(A) = \Phi(BA)$$

Ainsi $\Phi(A)$ commute à tous les éléments $\Phi(B)$ et donc par surjectivité de Φ, commute à tous les éléments de $\mathcal{M}_n(\mathbb{H}_p)$ et donc $\Phi(A) \in Z(\mathcal{M}_n(\mathbb{H}_p))$. De même pour $A' \in Z(\mathcal{M}_n(\mathbb{H}_p))$, il existe un unique $A \in \mathcal{M}_m(\mathbb{Q}_p)$ tel que $A' = \Phi(A)$, soit $\Phi(A)C = C\Phi(A)$ pour tout C de $\mathcal{M}_n(\mathbb{H}_p)$. Par surjectité de Φ et son caractère multiplicatif on a alors :

$$\forall B \in \mathcal{M}_m(\mathbb{Q}_p),\ \Phi(AB) = \Phi(A)\Phi(B) = \Phi(B)\Phi(A) = \Phi(BA)$$

puis, par injectivité de Φ,

$$AB = BA \text{ pour tout } B \in \mathcal{M}_m(\mathbb{Q}_p)$$

et donc $A \in Z(\mathcal{M}_m(\mathbb{Q}_p))$, ce qui donne bien l'égalité

$$\Phi(Z(\mathcal{M}_m(\mathbb{Q}_p))) = Z(\mathcal{M}_n(\mathbb{H}_p)).$$

Or, $\mathbb{Q}_p$ étant un corps commutatif, on a $Z(\mathcal{M}_m(\mathbb{Q}_p)) = \{\lambda I_m,\ \lambda \in \mathbb{Q}_p\}$. En revanche $\mathbb{H}_p$ étant un corps non commutatif de centre $\mathbb{Q}_p$, cela nous donne $Z(\mathcal{M}_n(\mathbb{H}_p)) \subset \{\lambda I_n,\ \lambda \in \mathbb{Q}_p\}$ et donc $Z(\mathcal{M}_n(\mathbb{H}_p)) = \{\lambda I_n,\ \lambda \in \mathbb{Q}_p\}$, l'autre inclusion étant évidente. Soit F un $\mathbb{Q}_p$ sous-espace vectoriel de $\mathcal{M}_m(\mathbb{Q}_p)$ de dimension l. On note $(E_i)_{1\leq i\leq l}$ une base de F, montrons que

$$(\Phi(E_i))_{1\leq i\leq l} \text{ est une base de } \Phi(F)$$

en tant que $\mathbb{Q}_p$-espace vectoriel. Puisque $\Phi(Z(\mathcal{M}_m(\mathbb{Q}_p)) = Z(\mathcal{M}_n(\mathbb{H}_p))$, pour tout λ de $\mathbb{Q}_p$ on a l'égalité $\Phi(\lambda I_m) = \delta I_n$ pour un unique $\delta \in \mathbb{Q}_p$ et donc tout élément x de F s'écrivant de manière unique $x = \lambda_1 E_1 + \lambda_2 E_2 + \cdots + \lambda_l E_l$, on a :

$$\Phi(x) = \Phi(\lambda_1 E_1 + \lambda_2 E_2 + \cdots + \lambda_l E_l) = \delta_1\Phi(E_1) + \delta_2\Phi(E_2) + \cdots + \delta_l\Phi(E_l)$$

Ainsi, $\Phi(F) = vect_{\mathbb{Q}_p}(\Phi(E_1), \Phi(E_2), \cdots, \Phi(E_l))$ et il nous reste à montrer que la famille $(\Phi(E_i))_{1\leq i\leq l}$ est $\mathbb{Q}_p$-libre. Soit $(\delta_i)_{1\leq i\leq l} \in \mathbb{Q}_p^l$ tel que

$$\delta_1\Phi(E_1) + \delta_2\Phi(E_2) + \cdots + \delta_l\Phi(E_l) = 0$$

En notant $\delta_i I_n = \Phi(\lambda_i I_m)$ on a :

$$\begin{aligned}
& \delta_1 I_n\Phi(E_1) + \delta_2 I_n\Phi(E_2) + \cdots + \delta_l I_n\Phi(E_l) = 0 \\
\iff\quad & \Phi(\lambda_1 I_m)\Phi(E_1) + \Phi(\lambda_2 I_m)\Phi(E_2) + \cdots + \Phi(\lambda_l I_n)\Phi(E_l) = 0 \\
\iff\quad & \Phi(\lambda_1 I_m E_1 + \lambda_2 I_m E_2 + \cdots + \lambda_l I_m E_l) = 0 \\
\iff\quad & \lambda_1 E_1 + \lambda_2 E_2 + \cdots + \lambda_l E_l = 0 \\
\iff\quad & \lambda_1 = \lambda_2 = \cdots = \lambda_l = 0 \\
\iff\quad & \delta_1 = \delta_2 = \cdots = \delta_l = 0
\end{aligned}$$

puisque la famille $(E_i)_{1\leq i\leq l}$ est une base du $\mathbb{Q}_p$-espace vectoriel F et que Φ est un isomorphisme d'anneaux. Alors,

$$\begin{gathered}(\Phi(E_i))_{1\leq i\leq l} \text{ est } \mathbb{Q}_p\text{-libre et est une famille génératrice de} \\ \Phi(F) = vect_{\mathbb{Q}_p}(\Phi(E_1), \Phi(E_2), \cdots, \Phi(E_l))\end{gathered}$$

ce qui prouve que $\Phi(F)$ est un $\mathbb{Q}_p$-espace vectoriel de base $(\Phi(E_i))_{1\leq i\leq l}$ et donc de dimension l. Ainsi, le $\mathbb{Q}_p$-espace vectoriel $\mathcal{M}_m(\mathbb{Q}_p)$ de dimension m^2 est envoyé par Φ sur le $\mathbb{Q}_p$-espace vectoriel $\mathcal{M}_n(\mathbb{H}_p)$ de dimension $4n^2$ (car $\mathbb{H}_p$ est un $\mathbb{Q}_p$-espace vectoriel de dimension 4). Par égalité des dimensions :

$$(2n)^2 = m^2 \text{ et donc } 2n = m.$$

Soit A une matrice non nulle de $\mathcal{M}_n(\mathbb{H}_p)$ que l'on écrit sous la forme $(C_1, C_2, \cdots, C_n)$ où C_i désigne la i-ème colonne de A. Alors l'idéal à gauche de $\mathcal{M}_n(\mathbb{H}_p)$ engendré par A, $A\mathcal{M}_n(\mathbb{H}_p)$ est en particulier un $\mathbb{H}_p$-espace vectoriel dont une famille génératrice est donnée par $(AE_{i,j})_{1\leq i,j\leq n}$. A étant non nulle il existe une colonne $C_i \neq 0$ et ainsi $(AE_{i,j})_{1\leq i,j\leq n}$ contient le sous ensemble de n matrices indépendantes

$$\{(C_i, 0, \cdots, 0), (0, C_i, \cdots, 0), \cdots, (0, 0, \cdots, C_i)\}$$

ce qui montre que $dim_{\mathbb{H}_p}(A\mathcal{M}_n(\mathbb{H}_p)) \geq n$ et donc

$$dim_{\mathbb{Q}_p}(A\mathcal{M}_n(\mathbb{H}_p)) \geq 4n.$$

Montrons désormais qu'il existe un idéal à gauche sur $\mathcal{M}_m(\mathbb{Q}_p)$ qui soit un $\mathbb{Q}_p$ espace vectoriel de dimension m. Soit $A = (1)_{1\leq i,j\leq m} = (C_1, C_1, \cdots, C_1)$ la matrice dont tous les coefficients sont égaux à 1. L'idéal engendré par A que l'on note $I = A\mathcal{M}_m(\mathbb{Q}_p)$ est un $\mathbb{Q}_p$-espace vectoriel dont une famille génératrice est donnée par $(AE_{i,j})_{1\leq i,j\leq m}$. Or, la famille $(AE_{i,j})_{1\leq i,j\leq j}$ ne contient que m matrices distinctes

$$(C_1, 0, \cdots, 0), (0, C_1, \cdots, 0), \cdots, (0, 0, \cdots, C_1)$$

qui sont clairement indépendantes. D'où cette famille de m matrices est une base de $I = A\mathcal{M}_m(\mathbb{Q}_p)$ qui est donc un $\mathbb{Q}_p$-espace vectoriel de dimension m. Etudions alors $\Phi(I)$. Puisque Φ est un isomorphisme d'anneaux, l'image par Φ de l'idéal I est également un idéal à gauche de $\mathcal{M}_n(\mathbb{H}_p)$ qui est de même dimension en tant que $\mathbb{Q}_p$-espace vectoriel que I, soit de dimension $m = 2n < 4n$. Un idéal à gauche non trivial de $\mathcal{M}_n(\mathbb{H}_p)$ contenant nécessairement une matrice A non nulle, il contient alors également l'idéal à gauche engendré par A et est donc forcément un $\mathbb{Q}_p$-espace vectoriel de $\mathcal{M}_n(\mathbb{H}_p)$ de dimension supérieure ou égale à $4n$. On a donc de même que $\Phi(I)$ est un idéal à gauche de $\mathcal{M}_n(\mathbb{H}_p)$ de dimension au moins $4n$, absurde. Ce qui achève de montrer le lemme. □

Lemme 11.0.7. *Soit $n \in \mathbb{N}^*$ et $\mathbb{K}$ un corps. On note $\mathbb{L}_1$ et $\mathbb{L}_2$ deux extensions quadratiques de $\mathbb{Q}_p$. Alors,*

1. *$\mathcal{M}_n(\mathbb{K})$ n'admet pas d'idéal bilatère non trivial.*
2. *$\{0\} \times \mathcal{M}_n(\mathbb{K})$ et $\mathcal{M}_n(\mathbb{K}) \times \{0\}$ sont les seuls idéaux bilatères non triviaux de $\mathcal{M}_n(\mathbb{K}) \times \mathcal{M}_n(\mathbb{K})$.*
3. *$\mathcal{M}_n(\mathbb{H}_p) \times \mathcal{M}_n(\mathbb{H}_p) \ncong \mathcal{M}_{2n}(\mathbb{Q}_p) \times \mathcal{M}_{2n}(\mathbb{Q}_p)$*
4. *$\mathcal{M}_n(\mathbb{L}_1) \ncong \mathcal{M}_n(\mathbb{Q}_p) \times \mathcal{M}_n(\mathbb{Q}_p)$*
5. *$\mathcal{M}_n(\mathbb{L}_1) \ncong \mathcal{M}_{n/2}(\mathbb{H}_p) \times \mathcal{M}_{n/2}(\mathbb{H}_p)$ si n est pair.*

Démonstration. 1) On suppose que I est un idéal bilatère de $\mathcal{M}_n(\mathbb{K})$. Si I contient une matrice inversible A alors clairement $I = \mathcal{M}_n(\mathbb{K})$. Supposons I non trivial, en particulier I ne contient pas de matrice inversible et étant non nul contient nécessairement une matrice A de rang $r < n$. A étant de rang r, elle est équivalente à la matrice diagonale J_r qui possède ces r premiers termes diagonaux égaux à 1 et ces $n - r$ derniers termes nuls. Alors, A appartenant à l'idéal bilatère I, J_r qui lui est équivalente appartient également à I. Puisque $J_1 = J_r J_1$ et que $J_r \in I$, J_1 appartient à I. Comme toute matrice de rang 1 est équivalente à J_1, elle appartient aussi à I et donc I contient donc toutes les matrices de rang 1. On note $(E_{i,j})_{1\leq i,j\leq n}$ la base canonique de $\mathcal{M}_n(\mathbb{K})$ formée de n^2 matrices de rang 1. Toute matrice de $\mathcal{M}_n(\mathbb{K})$ se décompose ainsi dans cette base et s'écrit comme une somme de matrice de rang 1. I étant en particulier un groupe additif, toute matrice de $\mathcal{M}_n(\mathbb{K})$ est donc dans I, ce qui donne $\mathcal{M}_n(\mathbb{K}) = I$, absurde.

2) Soit I un idéal bilatère de $\mathcal{M}_n(\mathbb{K}) \times \mathcal{M}_n(\mathbb{K})$. Supposons qu'il existe un couple de matrices $(A, B) \in I$ avec $A \neq 0$ et $B \neq 0$. Alors, comme I est un idéal bilatère, $\langle A\rangle \times \langle B\rangle \subset I$ où l'on a noté $\langle A\rangle$ et $\langle B\rangle$ les idéaux bilatères de $\mathcal{M}_n(\mathbb{K})$ respectivement engendrés par A et B. D'après ce qu'on a vu ci-dessus :

$$\langle A\rangle = \mathcal{M}_n(\mathbb{K}) \text{ et } B = \mathcal{M}_n(\mathbb{K}) \text{ et donc } I = \mathcal{M}_n(\mathbb{K}) \times \mathcal{M}_n(\mathbb{K}).$$

Soit alors I un idéal non trivial de $\mathcal{M}_n(\mathbb{K}) \times \mathcal{M}_n(\mathbb{K})$. Par ce qui précède, I ne contient pas de couple (A, B) où A et B sont tous deux non nuls et ne contient donc que des éléments de la forme $(A, 0)$ ou de la forme $(0, B)$. I étant un groupe additif, tous ces éléments sont soit de la forme $(A, 0)$, soit de la forme $(0, B)$ car sinon par somme il existerait dans I un élément (A, B) où $A \neq 0$ et $B \neq 0$. Plaçons nous dans le cas où I est non trivial et dont tous ces éléments sont de la forme $(A, 0)$. Puisque $I \neq 0$, alors il existe $A \neq 0$ dans $\mathcal{M}_n(\mathbb{K})$ tel que $(A, 0) \in I$. I contient alors l'idéal $\langle A \rangle \times \{0\}$ où $\langle A \rangle = \mathcal{M}_n(\mathbb{K})$ car est un idéal bilatère non nul de $\mathcal{M}_n(\mathbb{K})$ ce qui nous donne :

$$I = \mathcal{M}_n(\mathbb{K}) \times \{0\}.$$

On montre de même que si J est un idéal bilatère non trivial de $\mathcal{M}_n(\mathbb{K}) \times \mathcal{M}_n(\mathbb{K})$ tel qu'il existe $B \neq 0$ pour lequel $(0, B) \in J$, alors

$$J = \{0\} \times \mathcal{M}_n(\mathbb{K})$$

et donc les deux seuls idéaux bilatères non triviaux de $\mathcal{M}_n(\mathbb{K}) \times \mathcal{M}_n(\mathbb{K})$ sont :

$$\{0\} \times \mathcal{M}_n(\mathbb{K}) \text{ et } \mathcal{M}_n(\mathbb{K}) \times \{0\}.$$

3) Supposons par l'absurde,

$$\mathcal{M}_n(\mathbb{H}_p) \times \mathcal{M}_n(\mathbb{H}_p) \simeq \mathcal{M}_{2n}(\mathbb{Q}_p) \times \mathcal{M}_{2n}(\mathbb{Q}_p) \text{ en tant qu'anneaux.}$$

Soit $\Psi : \mathcal{M}_n(\mathbb{H}_p) \times \mathcal{M}_n(\mathbb{H}_p) \longrightarrow \mathcal{M}_{2n}(\mathbb{Q}_p) \times \mathcal{M}_{2n}(\mathbb{Q}_p)$ un tel isomorphisme d'aneaux. D'après 2) l'idéal bilatère $\mathcal{M}_n(\mathbb{Q}_p) \times \{0\}$ est envoyé via l'isomorphisme Ψ sur un idéal bilatère de $\mathcal{M}_{2n}(\mathbb{Q}_p) \times \mathcal{M}_{2n}(\mathbb{Q}_p)$ qui est donc nécessairement égal à $\mathcal{M}_{2n}(\mathbb{Q}_p) \times \{0\}$ ou $\mathcal{M}_{2n}(\mathbb{Q}_p) \times \{0\}$. Naturellement,

$$\mathcal{M}_{2n}(\mathbb{Q}_p) \times \{0\} \simeq \mathcal{M}_{2n}(\mathbb{Q}_p),\ \mathcal{M}_{2n}(\mathbb{Q}_p) \times \{0\} \simeq \mathcal{M}_{2n}(\mathbb{Q}_p)$$

et

$$\mathcal{M}_n(\mathbb{H}_p) \times \{0\} \simeq \mathcal{M}_n(\mathbb{H}_p)$$

en tant qu'anneaux. Enfin,

$$\Psi(\mathcal{M}_n(\mathbb{H}_p) \times \{0\}) = \mathcal{M}_{2n}(\mathbb{Q}_p) \times \{0\} \text{ ou } \mathcal{M}_{2n}(\mathbb{Q}_p) \times \{0\}$$

et par composition d'isomorphismes d'anneaux, on a alors

$$\mathcal{M}_n(\mathbb{H}_p) \simeq \mathcal{M}_{2n}(\mathbb{Q}_p)$$

ce qui est absurde d'après le lemme 11.0.6.

4) Soit $\mathbb{L}$ une extension quadratique de $\mathbb{Q}_p$. Supposons par l'absurde que :

$$\mathcal{M}_n(\mathbb{L}) \simeq \mathcal{M}_n(\mathbb{Q}_p) \times \mathcal{M}_n(\mathbb{Q}_p) \text{ en tant qu'anneaux.}$$

Alors, comme vu précédemment, les centres $Z(\mathcal{M}_n(\mathbb{L}))$ et $Z(\mathcal{M}_n(\mathbb{Q}_p) \times \mathcal{M}_n(\mathbb{Q}_p))$ sont eux aussi isomorphes en tant que sous-anneaux. Or, $\mathbb{L}$ est un corps commutatif comme extension quadratique de $\mathbb{Q}_p$ qui est commutatif et donc

$$Z(\mathcal{M}_n(\mathbb{L})) = \{\lambda I_n, \lambda \in \mathbb{L}\}.$$

De même,

$$Z(\mathcal{M}_n(\mathbb{Q}_p) \times \mathcal{M}_n(\mathbb{Q}_p)) = \{(\lambda_1 I_n, \lambda_2 I_n), (\lambda_1, \lambda_2) \in \mathbb{Q}_p \times \mathbb{Q}_p\}$$

ce qui nous donne un isomorphisme d'anneaux entre $\mathbb{L}$ et $\mathbb{Q}_p \times \mathbb{Q}_p$, absurde car $\mathbb{L}$ est un corps alors que $\mathbb{Q}_p \times \mathbb{Q}_p$ n'en est pas un. D'où

$$\mathcal{M}_n(\mathbb{L}) \not\simeq \mathcal{M}_n(\mathbb{Q}_p) \times \mathcal{M}_n(\mathbb{Q}_p).$$

5) Supposons n pair et que $\mathcal{M}_n(\mathbb{L}) \simeq \mathcal{M}_{n/2}(\mathbb{H}_p) \times \mathcal{M}_{n/2}(\mathbb{H}_p)$. Alors il existerait un isomorphisme Φ envoyant $Z(\mathcal{M}_n(\mathbb{L}))$ sur $Z(\mathcal{M}_{n/2}(\mathbb{H}_p) \times \mathcal{M}_{n/2}(\mathbb{H}_p))$. Or $\mathbb{H}_p$ étant un corps non commutatif de centre $\mathbb{Q}_p$, on a vu que :

$$Z(\mathcal{M}_{n/2}(\mathbb{H}_p)) = \{\lambda I_{n/2}, \lambda \in \mathbb{Q}_p\} \simeq \mathbb{Q}_p$$

soit

$$Z(\mathcal{M}_{n/2}(\mathbb{H}_p) \times \mathcal{M}_{n/2}(\mathbb{H}_p)) \simeq \mathbb{Q}_p \times \mathbb{Q}_p \text{ et } Z(\mathcal{M}_n(\mathbb{L})) \simeq \mathbb{L}$$

On aurait de nouveau $\mathbb{L} \simeq \mathbb{Q}_p \times \mathbb{Q}_p$ en tant qu'anneaux, absurde. D'où

$$\mathcal{M}_n(\mathbb{L}_1) \not\simeq \mathcal{M}_{n/2}(\mathbb{H}_p) \times \mathcal{M}_{n/2}(\mathbb{H}_p).$$

□

Lemme 11.0.8. *Soit $n \in \mathbb{N}^*$ et $\mathbb{H}_p$ l'unique (à isomorphisme près) algèbre de quaternions sur $\mathbb{Q}_p$ qui soit un corps. On a alors les isomorphismes de $\mathbb{Q}_p$-algèbres suivant :*

1. $\mathcal{M}_n(\mathbb{Q}_p) \otimes_{\mathbb{Q}_p} (\mathbb{H}_p \times \mathbb{H}_p) \simeq \mathcal{M}_n(\mathbb{H}_p) \times \mathcal{M}_n(\mathbb{H}_p)$
2. $\mathbb{H}_p \otimes_{\mathbb{Q}_p} (\mathbb{Q}_p \times \mathbb{Q}_p) \simeq \mathbb{H}_p \times \mathbb{H}_p$

Démonstration. 1) On commence par définir une application Φ par :

$$\Phi\colon \begin{cases} \mathcal{M}_n(\mathbb{Q}_p) \times (\mathbb{H}_p \times \mathbb{H}_p) \longrightarrow \mathcal{M}_n(\mathbb{H}_p) \times \mathcal{M}_n(\mathbb{H}_p) \\ (A, (\lambda_1, \lambda_2)) \longmapsto (\lambda_1 A, \lambda_2 A) \end{cases}$$

$\mathbb{H}_p$ est centrale et admet donc $\mathbb{Q}_p$ pour centre, ce qui nous permet de montrer facilement que Φ est $\mathbb{Q}_p$-bilinéaire. Par la propriété universelle du produit tensoriel, il existe une unique application linéaire $\overline{\Phi}$ définie de $\mathcal{M}_n(\mathbb{Q}_p) \otimes (\mathbb{H}_p \times \mathbb{H}_p)$ à valeur dans $\mathcal{M}_n(\mathbb{H}_p) \times \mathcal{M}_n(\mathbb{H}_p)$ pour laquelle on a :

$$\forall (A, (\lambda_1, \lambda_2)) \in \mathcal{M}_n(\mathbb{Q}_p) \times (\mathbb{H}_p \times \mathbb{H}_p), \overline{\Phi}(A \otimes (\lambda_1, \lambda_2)) = \Phi(A, (\lambda_1, \lambda_2))$$

Or $\mathcal{M}_n(\mathbb{Q}_p)$ étant un $\mathbb{Q}_p$-espace vectoriel de dimension n^2 et $\mathbb{H}_p$ étant un $\mathbb{Q}_p$ espace vectoriel de dimension 4, il vient :

$$dim(\mathcal{M}_n(\mathbb{Q}_p) \otimes (\mathbb{H}_p \times \mathbb{H}_p)) = 8n^2 \text{ et } dim(\mathcal{M}_n(\mathbb{H}_p) \times \mathcal{M}_n(\mathbb{H}_p) = 8n^2$$

Par raison de dimension, pour montrer que $\overline{\Phi}$ est un isomorphisme de $\mathbb{Q}_p$-algèbres, il suffira de montrer que $\overline{\Phi}$ est surjective et qu'elle est multiplicative. Or, on a déjà prouvé au lemme 11.0.5 que pour

$$\phi\colon \begin{cases} \mathcal{M}_n(\mathbb{K}) \times \mathbb{L} \longrightarrow \mathcal{M}_n(\mathbb{L}) \\ (A, x) \longmapsto (a_{i,j}x)_{1 \leq i,j \leq n} \end{cases}$$

l'application $\overline{\phi}$ déduite de ϕ par la propriété universelle du produit tensoriel était un isomorphisme d'algèbre. En appliquant à $\mathbb{K} = \mathbb{Q}_p$ et à l'extension $\mathbb{L} = \mathbb{H}_p$, $\forall (A, (\lambda_1, \lambda_2)) \in \mathcal{M}_n(\mathbb{Q}_p) \times (\mathbb{H}_p \times \mathbb{H}_p)$ on a :

$$\begin{aligned} \overline{\Phi}(A \otimes (\lambda_1, \lambda_2)) = & \quad \Phi(A, (\lambda_1, \lambda_2)) \\ = & \quad (\phi(A \otimes \lambda_1), \phi(A \otimes \lambda_2)) \end{aligned}$$

Soit alors $(M_1, M_2) \in (\mathcal{M}_n(\mathbb{H}_p))^2$, par surjectivité de $\overline{\phi}$ il existe deux éléments de $\mathcal{M}_n(\mathbb{Q}_p)\otimes\mathbb{H}_p$ ayant respectivement M_1 et M_2 pour image par $\overline{\phi}$. Alors, notant x et y ces antécédents, ils s'écrivent comme des sommes finies de tenseurs purs et :

$$x = \sum_{i\in I} A_i \otimes \lambda_i \text{ et } y = \sum_{j\in J} B_j \otimes \lambda'_i$$

Alors, $\overline{\phi}(x) = M_1$ et $\overline{\phi}(y) = M_2$ implique que $(\overline{\phi}(x), \overline{\phi}(y)) = (M_1, M_2)$ et donc :

$$\begin{aligned}
\overline{\Phi}(\sum_{i\in I} A_i \otimes (\lambda_i, 0)) = & \quad \sum_{i\in I} \overline{\Phi}(A_i \otimes (\lambda_i, 0)) \\
= & \quad \sum_{i\in I} \Phi(A_i, (\lambda_i, 0)) \\
= & \quad \sum_{i\in I} (\lambda_i A_i, 0) \\
= & \quad \sum_{i\in I} (\overline{\phi}(A_i \otimes \lambda_i), \overline{\phi}(A_i \otimes\ 0)) \\
= & \quad (\sum_{i\in I} \overline{\phi}(A_i \otimes \lambda_i), 0)) \\
= & \quad (\overline{\phi}(\sum_{i\in I} A_i \otimes \lambda_i), 0) \\
= & \quad (\overline{\phi}(x), 0) \\
= & \quad (M_1, 0)
\end{aligned}$$

De même $\overline{\Phi}(\sum_{j\in J} B_j \otimes (0, \lambda'_j)) = (0, M_2)$, soit :

$$\overline{\Phi}(\sum_{i\in I} A_i \otimes (\lambda_i, 0) + \sum_{j\in J} B_j \otimes (0, \lambda'_j)) = (M_1, M_2)$$

D'où la surjectivité de $\overline{\Phi}$ qui est bien un isomorphisme de $\mathbb{Q}_p$-espaces vectoriels en raison des dimensions. Il reste alors à montrer que l'application est multiplicative pour montrer qu'on a un isomorphisme d'algèbres. Pour ce faire il suffit par linéraité de $\overline{\Phi}$ de vérifier que

$$\overline{\Phi}(xy) = \overline{\Phi}(x)\overline{\Phi}(y)$$

pour x et y deux tenseurs purs (tout tenseur s'écrivant comme somme finie de tenseurs purs). Or, pour $x = A \otimes (\lambda_1, \lambda_2)$ et $y = B \otimes (\lambda'_1, \lambda'_2)$ on a :

$$xy = A \otimes (\lambda_1, \lambda_2).B \otimes (\lambda'_1, \lambda'_2) = AB \otimes (\lambda_1\lambda'_1, \lambda_2\lambda'_2)$$

et donc :

$$\overline{\Phi}(xy) = (\lambda_1\lambda'_1 AB, \lambda_2\lambda'_2 AB) = (\lambda_1 A, \lambda_2 A).(\lambda'_1 B, \lambda'_2 B) = \overline{\Phi}(x)\overline{\Phi}(y)$$

D'où, $\overline{\Phi}$ est bien un isomorphisme de $\mathbb{Q}_p$-algèbres.

2) On commence par définir une application Ψ par :

$$\Psi : \begin{cases} \mathbb{H}_p \times (\mathbb{Q}_p \times \mathbb{Q}_p) \longrightarrow \mathbb{H}_p \times \mathbb{H}_p \\ (\lambda, (\delta_1, \delta_2)) \longmapsto (\lambda\delta_1, \lambda\delta_2) \end{cases}$$

$\mathbb{H}_p$ est centrale et admet donc $\mathbb{Q}_p$ pour centre, ce qui nous permet de montrer facilement que Ψ est $\mathbb{Q}_p$-bilinéaire. Par la propriété universelle du produit tensoriel, il existe une unique application linéaire $\overline{\Psi}$ définie de $\mathbb{H}_p \otimes (\mathbb{Q}_p \times \mathbb{Q}_p)$ à valeurs dans $\mathbb{H}_p \times \mathbb{H}_p$ pour laquelle on a :

$$\forall (\lambda, (\delta_1, \delta_2)) \in \mathbb{H}_p \times (\mathbb{Q}_p \times \mathbb{Q}_p), \overline{\Psi}(\lambda \otimes (\delta_1, \delta_2)) = \Psi(\lambda, (\delta_1, \delta_2))$$

Or, $\mathbb{H}_p$ est un $\mathbb{Q}_p$-espace vectoriel de dimension 4 et $\mathbb{Q}_p \times \mathbb{Q}_p$ un $\mathbb{Q}_p$ espace vectoriel de dimension 2, soit :

$$dim(\mathbb{H}_p \otimes (\mathbb{Q}_p \times \mathbb{Q}_p)) = 8 = dim(\mathbb{H}_p \times \mathbb{H}_p)$$

Ainsi, par raison de dimension, pour montrer que $\overline{\Psi}$ est un isomorphisme de $\mathbb{Q}_p$-algèbres, il suffira de montrer que $\overline{\Psi}$ est surjective et qu'elle est multiplicative. Or, pour $(\lambda_1, \lambda_2) \in \mathbb{H}_p \times \mathbb{H}_p$ on a naturellement

$$\overline{\Psi}(\lambda_1 \otimes (1,0)) = (\lambda_1, 0) \text{ et } \overline{\Psi}(\lambda_2 \otimes (0,1)) = (0, \lambda_2)$$

ce qui donne la surjectivité puisque :

$$\overline{\Psi}(\lambda_1 \otimes (1,0) + \lambda_2 \otimes (0,1)) = (\lambda_1, \lambda_2)$$

D'où, la surjectivité de $\overline{\Psi}$ qui est bien un isomorphisme de $\mathbb{Q}_p$-espaces vectoriels en raison des dimensions. Il reste à montrer que l'application est multiplicative pour montrer qu'on a un isomorphisme d'algèbres. Pour ce faire il suffit par linéraité de $\overline{\Psi}$ de vérifier que $\overline{\Psi}(xy) = \overline{\Psi}(x)\overline{\Psi}(y)$ pour x et y deux tenseurs purs. Or, pour $x = \lambda_1 \otimes (\delta_1, \delta_2)$ et $y = \lambda_2 \otimes (\delta_3, \delta_4)$, on a :

$$xy = \lambda_1\lambda_2 \otimes (\delta_1\delta_3, \delta_2\delta_4)$$

et donc,

$$\begin{aligned}
\overline{\Psi}(xy) &= (\lambda_1\lambda_2 \otimes (\delta_1\delta_3, \delta_2\delta_4)) \\
&= (\lambda_1\lambda_2\delta_1\delta_3, \lambda_1\lambda_2\delta_2\delta_4) \\
&= (\lambda_1\delta_1\lambda_2\delta_3, \lambda_1\delta_2\lambda_2\delta_4) \\
&= (\lambda_1\delta_1, \lambda_1\delta_2).(\lambda_2\delta_3, \lambda_2\delta_4) \\
&= \overline{\Psi}(\lambda_1 \otimes (\delta_1, \delta_2))\overline{\Psi}(\lambda_2 \otimes (\delta_3, \delta_4)) \\
&= \overline{\Psi}(x)\overline{\Psi}(y)
\end{aligned}$$

Les égalités ci-dessus sont justifiées par le fait que $(\delta_i)_{1 \leq i \leq 4}$ étant une famille d'éléments de $\mathbb{Q}_p = Z(\mathbb{H}_p)$, on a :

$$(\lambda_1\delta_1\lambda_2\delta_3, \lambda_2\delta_4) = (\lambda_1\delta_1, \lambda_1\delta_2).(\lambda_2\delta_3, \lambda_2\delta_4)$$

D'où le caractère multiplicatif et $\overline{\Psi}$ est donc bien un isomorphisme de $\mathbb{Q}_p$-algèbres. □

Théorème 11.0.12. *Soit ϕ et ψ deux formes quadratiques régulières sur le corps $\mathbb{Q}_p$ où p désigne un nombre premier. Alors, ϕ et ψ sont équivalentes si et seulement si les algèbres de Clifford $C(\phi)$ et $C(\psi)$ sont isomorphes en tant qu'algèbres $\mathbb{Z}/2$-graduées.*

Démonstration. Remarquons d'abord que si $\phi \simeq \psi$ alors ϕ et ψ ont nécessairement même dimension et que si $C(\phi) \simeq C(\psi)$ en tant qu'algèbres alors elles le sont en tant que $\mathbb{Q}_p$-espaces vectoriels et ont donc même dimension soit :

$$dim_{\mathbb{Q}_p}(C(\phi)) = 2^{dim(\phi)} = 2^{dim(\psi)} = dim_{\mathbb{Q}_p}(C(\psi)) \Longrightarrow dim(\phi) = dim(\psi)$$

Ainsi, pour montrer l'équivalence du théorème il suffira de montrer que si ϕ et ψ sont de même dimension impaire alors,

$$\phi \simeq \psi \Longleftrightarrow C(\phi) \simeq_{\mathbb{Z}/2} C(\psi)$$

et que si ϕ et ψ sont de même dimension paire alors,

$$\phi \simeq \psi \Longleftrightarrow C(\phi) \simeq_{\mathbb{Z}/2} C(\psi).$$

On se place pour commencer dans le cadre où ϕ et ψ sont deux formes quadratiques sur $\mathbb{Q}_p$ de même dimension impaire supérieure ou égale à 3, où $p \in \mathcal{P}$. Montrons qu'il existe $n \in \mathbb{N}^*$ et q, q' deux formes quadratiques régulières de dimension 3 tels que :

$$\phi \simeq n.\langle 1, -1\rangle \perp q \text{ et } \psi \simeq n.\langle 1, -1\rangle \perp q'.$$

Le cas $dim(\phi) = dim(\psi) = 3$ est clair (prendre $n = 1$), on suppose dans la suite $dim(\phi) = dim(\psi) > 5$. Naturellement, utilisons la décomposition de Witt, il existe un couple $(n_1, n_2) \in (\mathbb{N})^2$ et q_1, q_2 anisotropes tel que

$$\phi \simeq n_1.\langle 1, -1\rangle \perp q_1 \text{ et } \phi \simeq n_2.\langle 1, -1\rangle \perp q_2.$$

Sur $\mathbb{Q}_p$ toute forme quadratique régulière de dimension au moins 5 étant isotrope et $dim(\phi)$ étant impaire, nécessairement $(n_1, n_2) \in (\mathbb{N}^*)^2$ et

$$dim(q_1) \in \{1, 3\},\ dim(q_2) \in \{1, 3\}.$$

Supposons que $dim(q_1) = 1$ et $dim(q_2) = 1$. Alors,

$$\phi \simeq (n_1 - 1).\langle 1, -1\rangle \perp (\langle 1, -1\rangle \perp q_1) \text{ et } \psi \simeq (n_2 - 1).\langle 1, -1\rangle \perp (\langle 1, -1\rangle \perp q_2)$$

et on pose $n = n_1 - 1 = n_2 - 1$ et $q = (\langle 1, -1\rangle \perp q_1)$, $q' = (\langle 1, -1\rangle \perp q_2)$ de dimension 3. Si $dim(q_1) = dim(q_2) = 3$ on pose $q = q_1$, $q' = q_2$ et $n = n_1 = n_2$. Enfin si $dim(q_1) = 1$ et $dim(q_2) = 3$ (ou l'inverse) on a

$$\phi \simeq (n_1 - 1).\langle 1, -1\rangle \perp (\langle 1, -1\rangle \perp q_1)$$

et on pose $q = (\langle 1, -1\rangle \perp q_1)$ et $n = n_2 = n_1 - 1$. Ainsi,

$$\exists n \in \mathbb{N}^* \text{ et } q, q' \text{ régulières de dimension 3 (non nécessairement anisotropes)}$$
$$\text{tels que } \phi \simeq n.\langle 1, -1\rangle \perp q \text{ et } \psi \simeq n.\langle 1, -1\rangle \perp q'.$$

On suppose $C(\phi) \simeq C(\psi)$ en tant qu'algèbres $\mathbb{Z}/2$-graduées, alors en particulier $\Delta(\phi) = \Delta(\psi)$ (d'après la proposition 10.0.8) et :

$$\Delta(n.\langle 1, -1\rangle \perp q) = \Delta(n.\langle 1, -1\rangle)\Delta(q) \text{ et } \Delta(n.\langle 1, -1\rangle \perp q') = \Delta(n.\langle 1, -1\rangle)\Delta(q')$$

puis,

$$\Delta(q) = \Delta(q').$$

Montrons donc que $C_0(q) \simeq C_0(q')$, on aura alors :

$$dim(q) = dim(q') = 3,\ \Delta(q) = \Delta(q') \text{ et } C_0(q) \simeq C_0(q') \Longrightarrow q \simeq q'$$

d'après la remarque 11.0.13. Puis, de part les décompositions

$$\phi \simeq n.\langle 1, -1\rangle \perp q \text{ et } \psi \simeq n.\langle 1, -1\rangle \perp q'.$$

nous aurons également $\phi \simeq \psi$. Le théorème sur l'effet sur l'algèbre de Clifford de l'ajout d'un plan quadratique nous donne :

$$\begin{aligned} C_0(n.\langle 1,-1\rangle \perp q) &\simeq \mathcal{M}_2(\mathbb{Q}_p) \otimes \cdots \otimes \mathcal{M}_2(\mathbb{Q}_p) \otimes C_0(q) \\ &\simeq \mathcal{M}_{2^n}(\mathbb{Q}_p) \otimes C_0(q) \end{aligned}$$

et

$$\begin{aligned} C_0(n.\langle 1,-1\rangle \perp q') &\simeq \mathcal{M}_2(\mathbb{Q}_p) \otimes \cdots \otimes \mathcal{M}_2(\mathbb{Q}_p) \otimes C_0(q') \\ &\simeq \mathcal{M}_{2^n}(\mathbb{Q}_p) \otimes C_0(q') \end{aligned}$$

Les algèbres $C(\phi)$ et $C(\psi)$ sont isomorphes en tant qu'algèbres graduées donc les parties paires $C_0(n.\langle 1,-1\rangle \perp q)$ et $C_0(n.\langle 1,-1\rangle \perp q')$ sont isomorphes et donc :

$$\mathcal{M}_{2^n}(\mathbb{Q}_p) \otimes C_0(q) \simeq \mathcal{M}_{2^n}(\mathbb{Q}_p) \otimes C_0(q')$$

D'après le théorème de structure de l'algèbre de Clifford en dimension impaire,

$$dim(q) = dim(q') = 3 \Longrightarrow C_0(q) \text{ et } C_0(q') \text{ sont des algèbres de quaternions}$$

Supposons par l'absurde que $C_0(q) \not\simeq C_0(q')$. Alors, nécessairement une des deux algèbres de quaternions est isomorphe à $\mathcal{M}_2(\mathbb{Q}_p)$ et l'autre est isomorphe à $\mathbb{H}_p$ (corollaire 11.0.9). Prenons par exemple,

$$C_0(q) \simeq \mathcal{M}_2(\mathbb{Q}_p) \text{ et } C_0(q') \simeq \mathbb{H}_p$$

ce qui nous donne :

$$\begin{aligned} \mathcal{M}_{2^n}(\mathbb{Q}_p) \otimes C_0(q) &\simeq \mathcal{M}_{2^n}(\mathbb{Q}_p) \otimes \mathcal{M}_2(\mathbb{Q}_p) \\ &\simeq \mathcal{M}_{2^{n+1}}(\mathbb{Q}_p) \end{aligned}$$

et

$$\begin{aligned} \mathcal{M}_{2^n}(\mathbb{Q}_p) \otimes C_0(q') &\simeq \mathcal{M}_{2^n}(\mathbb{Q}_p) \otimes \mathbb{H}_p \\ &\simeq \mathcal{M}_{2^n}(\mathbb{H}_p) \end{aligned}$$

Or d'après le lemme 11.0.6, $\mathcal{M}_{2^n}(\mathbb{H}_p) \not\simeq \mathcal{M}_{2^{n+1}}(\mathbb{Q}_p)$, absurde. D'où,

$$C_0(q) \simeq C_0(q') \Longrightarrow q \simeq q' \text{ puis } \phi \simeq \psi.$$

Ainsi, pour ϕ et ψ deux formes quadratiques régulières de même dimension impaire supérieure ou égale à 3,

$$C(\phi) \simeq_{\mathbb{Z}/2} C(\psi) \Longrightarrow \phi \simeq \psi.$$

La réciproque est immédiate. De plus, si $dim(\phi) = dim(\psi) = 1$ on sait déjà que :

$$q \simeq q' \Longleftrightarrow C(\phi) \simeq C(\psi) \Longleftrightarrow C(\phi) \simeq_{\mathbb{Z}/2} C(\psi)$$

D'où, l'équivalence annoncée si ϕ et ψ sont de même dimension impaire.

On cherche désormais à montrer l'équivalence du théorème dans le cas où ϕ et ψ sont régulières et de même dimension paire. On va commencer par montrer que si q est une forme quadratique anisotrope de dimension 4 sur $\mathbb{Q}_p$, alors

$$C_0(q) \simeq \mathbb{H}_p \times \mathbb{H}_p.$$

Si $p = 2$, il n'y a dans $\mathbb{Q}_2$ à équivalence près qu'une seule forme quadratique régulière anisotrope de dimensions 4 qui est $\langle 1, 1, 1, 1\rangle$. Alors,

$$C(q) \simeq_{\mathbb{Z}/2} C\langle 1, 1, 1, 1\rangle) \Longrightarrow C_0(q) \simeq C_0\langle 1, 1, 1, 1\rangle.$$

Par le lemme de la partie paire et dévissage, il vient :

$$C_0\langle 1, 1, 1, 1\rangle \simeq C\langle -1, -1, -1\rangle \simeq (-1, -1) \otimes C\langle 1\rangle.$$

Etudions $C\langle 1\rangle$. Par l'étude des algèbres de Clifford des droites quadratiques, 1 étant un carré de $\mathbb{Q}_2^*$, on a :

$$C\langle 1\rangle \simeq \mathbb{Q}_2 \times \mathbb{Q}_2.$$

De plus, $\langle 1, 1, 1, 1\rangle$ étant anisotrope $(-1, -1)$ est un corps et est isomorphe à $\mathbb{H}_2$. Soit d'après le lemme 11.0.8 :

$$C_0\langle 1, 1, 1, 1\rangle \simeq \mathbb{H}_2 \otimes (\mathbb{Q}_2 \times \mathbb{Q}_2) \simeq \mathbb{H}_2 \times \mathbb{H}_2$$

Montrons le résultat dans le cas où p est un nombre premier impair. Pour un tel p, $\langle 1, -\varepsilon, p, -p\varepsilon\rangle$ est à équivalence près la seule forme quadratique régulière anisotrope de dimension 4 où ε est un non carré de $\mathbb{F}_p^*$. Ainsi,

$$C(q) \simeq_{\mathbb{Z}/2} C\langle 1, -\varepsilon, p, -p\varepsilon\rangle \Longrightarrow C_0(q) \simeq C_0\langle 1, -\varepsilon, p, -p\varepsilon\rangle$$

Comme précédemment, par le lemme de la partie paire et par dévissage on a :

$$C_0\langle 1, -\varepsilon, p, -p\varepsilon\rangle \simeq C\langle \varepsilon, -p, p\varepsilon\rangle \simeq (-p\varepsilon^2, p^2\varepsilon) \otimes C\langle 1\rangle \simeq (-p, \varepsilon) \otimes C\langle 1\rangle$$

Or, $\langle 1, p, -\varepsilon, -p\varepsilon\rangle$ étant anisotrope, on a :

$$(-p, \varepsilon) \text{ est un corps et } (-p, \varepsilon) \simeq \mathbb{H}_p.$$

Pour les mêmes raisons que précédemment on a encore $C\langle 1\rangle \simeq \mathbb{Q}_p \times \mathbb{Q}_p$, ce qui nous donne le résultat annoncé :

$$C_0(q) \simeq C_0\langle 1, -\varepsilon, p, -p\varepsilon\rangle \simeq \mathbb{H}_p \otimes (\mathbb{Q}_p \times \mathbb{Q}_p) \simeq \mathbb{H}_p \times \mathbb{H}_p$$

Montrons désormais que si q est une forme quadratique anisotrope de dimension 2 sur $\mathbb{Q}_p$ et $n \in \mathbb{N}$ alors,

$$C_0(n.\langle 1, -1\rangle \perp q) \ncong \mathcal{M}_{2^{n-1}}(\mathbb{H}_p) \times \mathcal{M}_{2^{n-1}}(\mathbb{H}_p).$$

Dire que q est anisotrope de dimension 2, c'est dire que q n'est pas hyperbolique, ce qui est encore équivalent à ce que

$$\delta = \Delta(q) \neq 1 \text{ dans } \mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2$$

D'après le théorème sur l'effet de l'ajout d'un plan hyerpbolique, on a :

$$C_0(n.\langle 1, -1\rangle \perp q) \simeq \mathcal{M}_n(\mathbb{Q}_p) \otimes \cdots \otimes \mathcal{M}_n(\mathbb{Q}_p) \otimes C_0(q) \simeq \mathcal{M}_{2^n}(\mathbb{Q}_p) \otimes C_0(q)$$

où $C_0(q) \simeq C\langle\delta\rangle$ comme partie paire d'une algèbre de quaternions. Etudions $C\langle\delta\rangle$. Comme $\delta \neq 1$ alors,

$$C\langle\delta\rangle \simeq \mathbb{Q}_p(\sqrt{\delta})$$

où $\mathbb{Q}_p(\sqrt{\delta})$ est une extension quadratique de $\mathbb{Q}_p$. Soit, d'après le lemme 11.0.5 :

$$C_0(n.\langle 1, -1\rangle \perp q) \simeq \mathcal{M}_{2^n}(\mathbb{Q}_p) \otimes \mathbb{Q}_p(\sqrt{\delta}) \simeq \mathcal{M}_{2^n}(\mathbb{Q}_p(\sqrt{\delta})).$$

En appliquant le lemme 11.0.7 avec $\mathbb{L} = \mathbb{Q}_p(\sqrt{\delta})$, on a aussi

$$\mathcal{M}_{2^{n-1}}(\mathbb{H}_p) \times \mathcal{M}_{2^{n-1}}(\mathbb{H}_p) \not\simeq \mathcal{M}_{2^n}(\mathbb{Q}_p(\sqrt{\delta}))$$

et donc nécessairement :

$$C_0(n.\langle 1,-1\rangle \perp q) \not\simeq \mathcal{M}_{2^{n-1}}(\mathbb{H}_p) \times \mathcal{M}_{2^{n-1}}(\mathbb{H}_p)$$

A l'aide des divers résultats intermédiaires démontrés ci dessous, on va désormais pouvoir montrer que si ϕ et ψ sont deux formes quadratiques régulières de même dimension paire sur $\mathbb{Q}_p$ telles que $C(\phi) \simeq_{\mathbb{Z}/2} C(\psi)$ alors, ϕ et ψ sont équivalentes. Par décomposition de Witt et le fait que toute forme quadratique régulière de dimension supérieure ou égale à 5 est isotrope sur $\mathbb{Q}_p$, il existe $(n_1, n_2) \in \mathbb{N}^2$ et q_1, q_2 anisotropes de dimension $0, 2$ ou 4 telles que

$$\phi \simeq n_1.\langle 1,-1\rangle \perp q_1 \text{ et } \psi \simeq n_2.\langle 1,-1\rangle \perp q_2.$$

Supposons donc que $dim(\phi) = dim(\psi) \in 2\mathbb{N}$ et $C(\phi) \simeq_{\mathbb{Z}/2} C(\psi)$. On va commencer par montrer que :

$$dim(q_1) = dim(q_2).$$

Supposons par l'absurde, $dim(q_1) = 0$ et $dim(q_2) = 2$. Alors, ϕ est hyperbolique et par la structure de l'algèbre de Clifford d'un espace hyperbolique, on a :

$$C(\phi) \simeq C(n_1.\langle 1,-1\rangle) \simeq \mathcal{M}_{2^{n_1}}(\mathbb{Q}_p)$$

et

$$C_0(n_1.\langle 1,-1\rangle) \simeq \mathcal{M}_{2^{n_1-1}}(\mathbb{Q}_p) \times \mathcal{M}_{2^{n_1-1}}(\mathbb{Q}_p)$$

Comme q_2 est anisotrope, de dimension 2 sur $\mathbb{Q}_p$, d'après ce qui précède :

$$C_0((n_1-1).\langle 1,-1\rangle \perp q_2) \not\simeq \mathcal{M}_{2^{n_1-1}}(\mathbb{Q}_p) \times \mathcal{M}_{2^{n_1-1}}(\mathbb{Q}_p),$$

avec $C_0(n_1.\langle 1,-1\rangle) \simeq \mathcal{M}_{2^{n_1-1}}(\mathbb{Q}_p) \times \mathcal{M}_{2^{n_1-1}}(\mathbb{Q}_p)$ et donc $C_0(\phi) \not\simeq C_0(\psi)$, absurde.

Supposons par l'absurde que $dim(q_1) = 0$ et $dim(q_2) = 4$. Alors, on a toujours $C_0(\phi) \simeq C_0(n_1.\langle 1,-1\rangle) \simeq \mathcal{M}_{2^{n_1-1}}(\mathbb{Q}_p) \times \mathcal{M}_{2^{n_1-1}}(\mathbb{Q}_p)$ et en raison des dimensions $n_2 = n_1 - 2$. Soit :

$$C_0(n_2.\langle 1,-1\rangle \perp q_2) = C_0((n_1-2).\langle 1,-1\rangle \perp q_2) \simeq \mathcal{M}_{2^{n_1-2}}(\mathbb{Q}_p) \otimes C_0(q_2)$$

Or, q_2 étant anisotrope de dimension 4, on a vu que :

$$C_0(q_2) \simeq \mathbb{H}_p \times \mathbb{H}_p$$

soit finalement via le lemme 11.0.8 :

$$\begin{aligned} C_0((n_1-2).\langle 1,-1\rangle \perp q_2) \simeq & \quad \mathcal{M}_{2^{n_1-2}}(\mathbb{Q}_p) \otimes (\mathbb{H}_p \times \mathbb{H}_p) \\ \simeq & \quad \mathcal{M}_{2^{n_1-2}}(\mathbb{H}_p) \times \mathcal{M}_{2^{n_1-2}}(\mathbb{H}_p) \end{aligned}$$

Par le lemme 11.0.7,

$$\mathcal{M}_{2^{n_1-2}}(\mathbb{H}_p) \times \mathcal{M}_{2^{n_1-2}}(\mathbb{H}_p) \not\simeq \mathbb{M}_{2^{n_1-1}}(\mathbb{Q}_p) \times \mathbb{M}_{2^{n_1-1}}(\mathbb{Q}_p)$$

soit $C_0((n_1-2).\langle 1,-1\rangle \perp q_2) \not\simeq C_0(n_1.\langle 1,-1\rangle)$, absurde puisque $C_0(\phi) \simeq C_0(\psi)$. Ainsi, si $C(\phi) \simeq_{\mathbb{Z}/2} C(\psi)$, ou bien ϕ et ψ sont toutes deux hyperboliques et donc équivalentes ou bien aucune des deux formes quadratiques n'est hyperbolique.

Supposons par l'absurde que $dim(q_1) = 2$ et $dim(q_2) = 4$ (ou l'inverse), alors $n_2 = n_1 - 1$ et via l'isomorphisme graduée entre $C(\phi)$ et $C(\psi)$ on a :

$$C_0(\phi) \simeq C_0(n_1.\langle 1,-1\rangle \perp q_1) \simeq C_0((n_1-1).\langle 1,-1\rangle \perp q_2) \simeq C_0(\psi)$$

Or,

$$C_0(n_1.\langle 1,-1\rangle \perp q_1) \simeq \mathcal{M}_{2^{n_1}}(\mathbb{Q}_p) \otimes C_0(q_1)$$

et $C_0((n_1-1).\langle 1,-1\rangle \perp q_2) \simeq \mathcal{M}_{2^{n_1-1}}(\mathbb{H}_p) \otimes C_0(q_2)$. Puisque q_2 est anisotrope de dimension 4, on a aussi $C_0(q_2) \simeq \mathbb{H}_p \times \mathbb{H}_p$ et finalement :

$$C_0((n_1-1).\langle 1,-1\rangle \perp q_2) \simeq \mathcal{M}_{2^{n_1-1}}(\mathbb{H}_p) \times \mathcal{M}_{2^{n_1-1}}(\mathbb{H}_p) \not\simeq C_0(n_1.\langle 1,-1\rangle \perp q_1)$$

ce qui est absurde. On a donc bien montré que :

$$C(\phi) \simeq_{\mathbb{Z}/2} C(\psi) \Longrightarrow dim(q_1) = dim(q_2).$$

Or, si $dim(q_1) = dim(q_2) = 0$, ϕ et ψ sont toutes deux hyperboliques et donc nécessairement équivalentes. De même, si $dim(q_1) = dim(q_2) = 4$, alors q_1 et q_2 étant anisotropes de dimension 4 sur $\mathbb{Q}_p$, elles sont équivalentes (il n'y a à équivalence près qu'une seule forme quadratique anisotrope de dimension 4 sur $\mathbb{Q}_p$). Il reste donc à montrer que si $C(\phi) \simeq_{\mathbb{Z}/2} C(\psi)$ et $dim(q_1) = dim(q_2) = 2$ alors $q_1 \simeq q_2$ ce qui impliquera $\phi \simeq \psi$.

Soit donc ϕ et ψ de dimension 2. Alors puisque $C(\phi) \simeq_{\mathbb{Z}/2} C(\psi)$ elles ont même discriminant et comme $dim(n_1\langle 1,-1\rangle)$ est paire on a :

$$\Delta(\phi) = \Delta(n_1.\langle -1,1\rangle)\Delta(q_1) = \Delta(n_1.\langle 1,-1\rangle)\Delta(q_2) \Longrightarrow \Delta(q_1) = \Delta(q_2).$$

Les plans quadratiques réguliers sur $\mathbb{Q}_p$ étant classifiés par leur discriminant et la structure de $\mathbb{Q}_p$-algèbre de leur algèbre de Clifford, il suffit de montrer que $C(q_1) \simeq C(q_2)$ pour prouver que $q_1 \simeq q_2$. On suppose donc par l'absurde que $C(q_1) \not\simeq C(q_2)$. Une des deux algèbres de quaternions est donc isomorphe à $\mathbb{H}_p$ (disons $C(q_2)$) et l'autre est isomorphe à $\mathcal{M}_2(\mathbb{Q}_p)$ (disons $C(q_1)$). Alors,

$$C(n_1.\langle 1,-1\rangle \perp q_1) \simeq \mathcal{M}_{2^{n_1}}(\mathbb{Q}_p) \otimes \mathcal{M}_2(\mathbb{Q}_p) \simeq \mathcal{M}_{2^{n_1+1}}(\mathbb{Q}_p)$$

et

$$C(n_1.\langle 1,-1\rangle \perp q_2) \simeq \mathcal{M}_{2^{n_1}}(\mathbb{Q}_p) \otimes \mathbb{H}_p \simeq \mathcal{M}_{2^{n_1}}(\mathbb{H}_p)$$

D'où par le lemme 11.0.7,

$$C(n_1.\langle 1,-1\rangle \perp q_1) \not\simeq C(n_1.\langle 1,-1\rangle \perp q_2) \Longrightarrow C(\phi) \not\simeq C(\psi)$$

ce qui est absurde.

Ainsi, deux formes quadratiques sur $\mathbb{Q}_p$ de même dimension paire telles que $C(\phi) \simeq_{\mathbb{Z}/2} C(\psi)$ sont nécessairement équivalentes. La récriproque est claire car en toute dimension on a déjà vu que $\phi \simeq \psi \Longrightarrow C(\phi) \simeq_{\mathbb{Z}/2} C(\psi)$. D'où l'équivalence annoncée par le théorème dans le cas où les formes quadratiques sont de même dimension paire. Le cas de la dimension impaire ayant déjà été traité, on a bien montré que :

$$\phi \simeq \psi \Longleftrightarrow C(\phi) \simeq_{\mathbb{Z}/2} C(\psi).$$

□

11.0.17 Classification des formes quadratiques rationnelles régulières par l'algèbre de Clifford $\mathbb{Z}/2$-graduée associée

La section précédente nous a permis de classifier les formes quadratiques p-adiques par la structure d'algèbre de Clifford $\mathbb{Z}/2$-graduée associée. On va utiliser le lien établit entre les formes quadratiques rationnelles et p-adiques notamment via les principes de Hasse pour obtenir un résultat similaire pour la classification des formes quadratiques rationnelles.

Lemme 11.0.9. *Soit (E, q) un espace quadratique régulier sur $\mathbb{K}$ et $\mathbb{L}$ une extension de $\mathbb{K}$. Alors,*

$$C(q_{\mathbb{L}}) \simeq_{\mathbb{Z}/2} C(q) \otimes_{\mathbb{K}} \mathbb{L}$$

Démonstration. On souhaite construire un isomorphisme d'algèbres graduées de $C(q_{\mathbb{L}})$ sur $C(q) \otimes_{\mathbb{K}} \mathbb{L}$. Pour ce faire on va construire deux morphismes de $\mathbb{L}$-algèbres.

$$\Phi_1 : C(q) \otimes_{\mathbb{K}} \mathbb{L} \longrightarrow C(q_{\mathbb{L}}) \text{ et } \Phi_2 : C(q_{\mathbb{L}}) \longrightarrow C(q) \otimes_{\mathbb{K}} \mathbb{L}$$

dont on montrera qu'ils sont réciproques l'un de l'autre, puis qu'ils sont en fait gradués. Par définition du produit tensoriel, E s'injecte naturellement dans $E \otimes_{\mathbb{K}} \mathbb{L}$ via l'application i définie par :

$$i\colon \begin{cases} E \longrightarrow E \otimes_{\mathbb{K}} \mathbb{L} \\ x \longmapsto x \otimes 1 \end{cases}$$

Alors, par définition de $q_{\mathbb{L}}$, on a :

$$q_{\mathbb{L}}(x \otimes 1) = q(x) \text{ et } q_{\mathbb{L}}(i(x)) = q(x)$$

Ceci montre alors que i est un morphisme d'espaces quadratiques entre (E, q) et $(E \otimes_{\mathbb{K}} \mathbb{L}, q_{\mathbb{L}})$. Par la propriété universelle de l'algèbre de Clifford, il existe un unique morphisme de $\mathbb{K}$-algèbres $\mathbb{Z}/2$-graduées noté $C(i) : C(q) \longrightarrow C(q_{\mathbb{L}})$ tel que pour les projections canoniques

$$\mu_E : E \longrightarrow C(q) \text{ et } \mu_{E\otimes_{\mathbb{K}}\mathbb{L}} : E \otimes_{\mathbb{K}} \mathbb{L} \longrightarrow C(q_{\mathbb{L}})$$

on ait :

$$\forall x \in E,\ C(i)(\mu_E(x)) = \mu_{E\otimes_{\mathbb{K}}\mathbb{L}}(i(x))$$

soit avec la notation usuelle :

$$\forall x \in E,\ C(i)(\overline{x}) = \overline{i(x)}$$

Grâce au morphisme de $\mathbb{K}$-algèbres $C(i)$ on définit alors un morphisme de $\mathbb{L}$-algèbres que l'on note Φ_1 de $C(q) \otimes_{\mathbb{K}} \mathbb{L}$ sur $C(q_{\mathbb{L}})$ en posant

$$\forall x \in E,\ \Phi_1(\mu_E(x) \otimes \lambda) = \lambda C(i)(x).$$

Φ_1 est donc définit sur les tenseurs purs de $\mu_E(E)\otimes_{\mathbb{K}}\mathbb{L}$ et on étend sa définition par linéarité sur tout $C(q)\otimes_{\mathbb{K}}\mathbb{L}$ grâce au fait que $\mu_E(E)\otimes_{\mathbb{K}\mathbb{L}}$ engendre $C(q)\otimes_{\mathbb{K}}\mathbb{L}$ en tant que $\mathbb{L}$-algèbre.

$$\Phi_1 \colon \begin{cases} C(q)\otimes_{\mathbb{K}}\mathbb{L} \longrightarrow C(q_{\mathbb{L}}) \\ \overline{x}\otimes\lambda = \mu_E(x)\otimes\lambda \longmapsto \lambda\mu_{E\otimes_{\mathbb{K}}\mathbb{L}}(x\otimes 1) = \lambda\overline{x\otimes 1} \end{cases}$$

Réciproquement, définissons Φ_2. Le morphisme $i : E \hookrightarrow C(q)$ nous permet de définir une application $\alpha : E\otimes_{\mathbb{K}}\mathbb{L} \longrightarrow C(q)\otimes_{\mathbb{K}}\mathbb{L}$ que l'on définit sur les tenseurs purs par :

$$\alpha \colon \begin{cases} E\otimes_{\mathbb{K}}\mathbb{L} \longrightarrow C(q)\otimes_{\mathbb{K}}\mathbb{L} \\ x\otimes\lambda \longmapsto \mu_E(x)\otimes\lambda = \overline{x}\otimes\lambda \end{cases}$$

et que l'on étend par linéarité en une application $\mathbb{L}$-linéaire sur $E\otimes_{\mathbb{K}}\mathbb{L}$. Pour pouvoir utiliser la propriété universelle de l'algèbre de Clifford (propostion 10.0.4) et ainsi prolonger α en un morphisme de $\mathbb{L}$-algèbres noté Φ_2 de $C(q_{\mathbb{L}})$ dans $C(q)\otimes_{\mathbb{K}}\mathbb{L}$ vérifiant $\Phi_2\circ\mu_{E\otimes_{\mathbb{K}}\mathbb{L}} = \alpha$, il nous faut vérifier que :

$$\forall y \in E\otimes_{\mathbb{K}}\mathbb{L},\ \alpha(y)^2 = q_{\mathbb{L}}(y)1_{C(q)\otimes_{\mathbb{K}}\mathbb{L}}$$

Commençons par vérifier cette égalité sur les tenseurs purs $x\otimes\lambda$ de $E\otimes_{\mathbb{K}}\mathbb{L}$, on a :

$$\begin{aligned} \alpha(x\otimes\lambda)^2 &= (\overline{x}\otimes\lambda)^2 \\ &= (\overline{x}\otimes\lambda)(\overline{x}\otimes\lambda) \\ &= (\overline{x}^2\otimes\lambda^2) \\ &= \lambda^2\overline{x}^2\otimes 1 \\ &= \lambda^2 q(x)1_{C(q)}\otimes 1 \\ &= \lambda^2 q_{\mathbb{L}}(x\otimes 1)1_{C(q)}\otimes 1 \\ &= q_{\mathbb{L}}(x\otimes\lambda)1_{C(q)}\otimes 1 \\ &= q_{\mathbb{L}}(x\otimes\lambda)1_{C(q)\otimes_{\mathbb{K}}\mathbb{L}} \end{aligned}$$

de même pour la somme de deux tenseurs purs on a : $\alpha(x_1\otimes\lambda_1 + x_2\otimes\lambda_2)^2$

$$\begin{aligned} &= (\overline{x_1}\otimes\lambda_1 + \overline{x_2}\otimes\lambda_2)^2 \\ &= (\overline{x_1}^2\otimes\lambda_1^2) + (\overline{x_2}^2\otimes\lambda_2^2) + (\overline{x_1x_2}\otimes\lambda_1\lambda_2 + \overline{x_2x_1}\otimes\lambda_1\lambda_2) \\ &= \overline{x_1}^2\otimes\lambda_1^2 + \overline{x_2}^2\otimes\lambda_2^2 + \overline{x_1x_2 + x_2x_1}\otimes\lambda_1\lambda_2 \\ &= q_{\mathbb{L}}(x_1\otimes\lambda_1)1_{C(q)\otimes_{\mathbb{K}}\mathbb{L}} + q_{\mathbb{L}}(x_2\otimes\lambda_2)1_{C(q)\otimes_{\mathbb{K}}\mathbb{L}} + \overline{x_1x_2 + x_2x_1}\otimes\lambda_1\lambda_2 \\ &= (q_{\mathbb{L}}(x_1\otimes\lambda_1) + q_{\mathbb{L}}(x_2\otimes\lambda_2))1_{C(q)\otimes_{\mathbb{K}}\mathbb{L}} + 2b_q(x_1,x_2)1_{C(q)}\otimes\lambda_1\lambda_2 \\ &= (q_{\mathbb{L}}(x_1\otimes\lambda_1) + q_{\mathbb{L}}(x_2\otimes\lambda_2))1_{C(q)\otimes_{\mathbb{K}}\mathbb{L}} + 2b_{q_{\mathbb{L}}}(x_1\otimes 1, x_2\otimes 1)1_{C(q)}\otimes\lambda_1\lambda_2 \\ &= (q_{\mathbb{L}}(x_1\otimes\lambda_1) + q_{\mathbb{L}}(x_2\otimes\lambda_2))1_{C(q)\otimes_{\mathbb{K}}\mathbb{L}} + 2b_{q_{\mathbb{L}}}(x_1\otimes\lambda_1, x_2\otimes\lambda_2)1_{C(q)\otimes_{\mathbb{K}}\mathbb{L}} \\ &= q_{\mathbb{L}}(x_1\otimes\lambda_1 + x_2\otimes\lambda_2)1_{C(q)\otimes_{\mathbb{K}}\mathbb{L}} \end{aligned}$$

Pour un élément de $E\otimes_{\mathbb{K}\mathbb{L}}$ s'écrivant comme somme finie de tenseurs purs sous la forme $\sum_{i\in I} x_i\otimes\lambda_i$ on a de même :

$$\alpha(\textstyle\sum_{i\in I} x_i\otimes\lambda_i)^2 = q_{\mathbb{L}}(\sum_{i\in I} x_i\otimes\lambda_i)1_{C(q)\otimes_{\mathbb{K}}\mathbb{L}}$$

Ainsi, $\alpha : E\otimes_{\mathbb{K}}\mathbb{L} \longrightarrow C(q)\otimes_{\mathbb{K}}\mathbb{L}$ est une application $\mathbb{L}$-linéaire vérifiant :

$$\forall y \in E \otimes_{\mathbb{K}} \mathbb{L},\ \alpha(y)^2 = q_{\mathbb{L}}(y)1_{C(q)\otimes_{\mathbb{K}}\mathbb{L}}$$

Il existe donc un unique morphisme de $\mathbb{L}$-algèbres noté Φ_2 tel que :

$$\Phi_2(\mu_{E\otimes_{\mathbb{K}}\mathbb{L}}(x\otimes\lambda)) = \alpha(x\otimes\lambda) = \mu_E(x)\otimes\lambda$$

soit avec la notation usuelle :

$$\Phi_2(\overline{x\otimes\lambda}) = \overline{x}\otimes\lambda$$

Il reste maintenant à montrer que nos deux morphismes de $\mathbb{L}$-algèbres précédemment définis sont réciproques l'un de l'autre. Or puisque $\mu_E(E)\otimes_{\mathbb{K}}\mathbb{L}$ engendre $C(q)\otimes_{\mathbb{K}}\mathbb{L}$ en tant que $\mathbb{L}$-algèbre et que $\mu_{E\otimes_{\mathbb{K}}\mathbb{L}}(E\otimes_{\mathbb{K}}\mathbb{L})$ engendre $C(q_{\mathbb{L}})$ en tant que $\mathbb{L}$-agèbre il suffit de montrer que : $\Phi_1\circ\Phi_2 = Id$ pour les éléments de $\mu_{E\otimes_{\mathbb{K}}\mathbb{L}}(E\otimes_{\mathbb{K}}\mathbb{L})$ et il suffit même par linéarité de le montrer pour les tenseurs purs $\overline{x\otimes\lambda}$, où $x\in E$ et $\lambda\in\mathbb{L}$. De même, il suffit de montrer que $\Phi_2\circ\Phi_1 = Id$ sur les éléments de $\mu_E(E)\otimes_{\mathbb{K}}\mathbb{L}$, puis par linéarité, il suffit en fait de le montrer pour les tenseurs purs $\overline{x}\otimes\lambda$, où $x\in E$ et $\lambda\in\mathbb{L}$.

Soit donc $x\in E$ et $\lambda\in\mathbb{L}$ on a :

$$\begin{aligned}\Phi_1\circ\Phi_2(\overline{x\otimes\lambda}) &= \Phi_1(\overline{x}\otimes\lambda)\\ &= \lambda\overline{x\otimes 1}\\ &= \overline{x\otimes\lambda}\end{aligned}$$

et

$$\begin{aligned}\Phi_2\circ\Phi_1(\overline{x}\otimes\lambda) &= \Phi_1(\overline{x\otimes\lambda})\\ &= \lambda\Phi_1(\overline{x\otimes 1})\\ &= \lambda\overline{x}\otimes 1\\ &= \overline{x}\otimes\lambda\end{aligned}$$

Ceci montre alors que

$$\Phi_1\circ\Phi_2 = Id_{C(q_{\mathbb{L}})} \text{ et } \Phi_2\circ\Phi_1 = Id_{C(q)\otimes_{\mathbb{K}}\mathbb{L}}.$$

Les morphismes Φ_1 et Φ_2 sont alors des morphismes de $\mathbb{L}$-algèbres réciproques l'un de l'autre et donc les $\mathbb{L}$-algèbres $C(q_{\mathbb{L}})$ et $C(q)\otimes_{\mathbb{K}}\mathbb{L}$ sont isomorphes. Enfin, il reste à montrer qu'elles sont isomorphes en tant qu'algèbres $\mathbb{Z}/2$-graduées. Or, on a vu ci-dessus qu'en fait $C(i)$ était un morphisme d'algèbres $\mathbb{Z}/2$-graduées et donc puisque $C(q) = C_0(q)\oplus C_1(q)$ on a

$$C(q)\otimes_{\mathbb{K}}\mathbb{L} = (C_0(q)\otimes_{\mathbb{K}}\mathbb{L})\oplus(C_1(q)\otimes_{\mathbb{K}}\mathbb{L})$$

avec naturellement :

$$(C(q)\otimes_{\mathbb{K}}\mathbb{L})_0 = (C_0(q)\otimes_{\mathbb{K}}\mathbb{L}) \text{ et } (C(q)\otimes_{\mathbb{K}}\mathbb{L})_1 = (C_1(q)\otimes_{\mathbb{K}}\mathbb{L})$$

Or, $C(i)$ étant gradué on a :

$$C(i)(C_0(q))\subset C(q_{\mathbb{L}})_0 \text{ et } C(i)(C_1(q))\subset C(q_{\mathbb{L}})_1$$

ce qui nous donne par définition de Φ_1 :

$$\Phi_1((C(q)\otimes_{\mathbb{K}}\mathbb{L})_0)\subset C(q_{\mathbb{L}})_0 \text{ et } \Phi_1((C(q)\otimes_{\mathbb{K}}\mathbb{L})_1)\subset C(q_{\mathbb{L}})_1$$

Ainsi, Φ_1 est gradué et son isomorphisme réciproque Φ_2 l'est alors nécessairement. D'où,

$$C(q) \otimes_{\mathbb{K}} \mathbb{L} \simeq_{\mathbb{Z}/2} C(q_{\mathbb{L}}).$$

□

Théorème 11.0.13. *Soit q et q' deux formes quadratiques rationnelles régulières. Si $C(q)$ et $C(q')$ sont isomorphes en tant qu'algèbres $\mathbb{Z}/2$-graduées et si q et q' ont même signature, alors q et q' sont équivalentes.*

Démonstration. Soit q et q' deux formes quadratiques rationnelles régulières de même signature. Les algèbres de Clifford $C(q)$ et $C(q')$ étant supposées isomorphes en tant qu'algèbres $\mathbb{Z}/2$-graduées, elles sont en particulier isomorphes en tant qu'algèbres et donc nécessairement $dim(q) = dim(q')$. Deux formes quadratiques régulières de même dimension étant équivalentes si elles sont Witt-équivalentes, il nous suffit de montrer que q et q' sont Witt-équivalentes. Or, q et q' ayant même signature, on a $q_{\mathbb{R}} = q_\infty \simeq q'_{\mathbb{R}} = q'_\infty$ et d'où :

$$\begin{aligned}
q \simeq q' \iff & \quad [q]_W = [q']_W \\
\iff & \quad \forall p \in \mathcal{P}_\infty,\ [q_p]_W = [q'_p]_W \\
\iff & \quad \forall p \in \mathcal{P},\ [q_p]_W = [q'_p]_W \\
\iff & \quad \forall p \in \mathcal{P},\ q_p \simeq q'_p \\
\iff & \quad \forall p \in \mathcal{P},\ C(q_p) \simeq C(q'_p) \text{ en tant qu'algèbres } \mathbb{Z}/2\text{-graduées.}
\end{aligned}$$

où les équivalences ci-dessus sont justifiées successivement par :

- l'application du principe de Hasse faible.
- le fait que q et q' aient même signature.
- le fait que $dim(q_p) = dim(q'_p)$ puisque $dim(q) = dim(q')$.
- l'application du théorème précédent sur la classification des formes p-adiques par l'algèbre de Clifford associée.

Il reste donc à montrer que :

$$\forall p \in \mathcal{P},\ C(q_p) \simeq_{\mathbb{Z}/2} C(q'_p).$$

Or, d'après le lemme ci-dessus, on a :

$$\forall p \in \mathcal{P},\ C(q_p) \simeq_{\mathbb{Z}/2} C(q) \otimes_{\mathbb{Q}} \mathbb{Q}_p \text{ et } \forall p \in \mathcal{P},\ C(q'_p) \simeq_{\mathbb{Z}/2} C(q') \otimes_{\mathbb{Q}} \mathbb{Q}_p$$

et puisque $C(q) \simeq_{\mathbb{Z}/2} C(q')$

$$\forall p \in \mathcal{P},\ C(q_p) \simeq_{\mathbb{Z}/2} C(q) \otimes_{\mathbb{Q}} \mathbb{Q}_p \simeq_{\mathbb{Z}/2} C(q') \otimes_{\mathbb{Q}} \mathbb{Q}_p \simeq_{\mathbb{Z}/2} C(q'_p)$$

Ce qui achève de montrer le résultat. □

Pour finir, utilisons ce théorème de classification et voyons alors comment retrouver très efficacement que tout entier n s'écrit comme somme de quatre carrés de rationnels.

Proposition 11.0.19. *Pour $n \in \mathbb{N}^*$, $\langle 1,1,1,1\rangle \simeq \langle n,n,n,n\rangle$ sur $\mathbb{Q}$ et ainsi tout entier n non nul est somme de quatre carrés de rationnels.*

Démonstration. $\langle 1,1,1,1\rangle$ et $\langle n,n,n,n\rangle$ ont clairement même signature, on va montrer que $C\langle 1,1,1,1\rangle \simeq_{\mathbb{Z}/2} C\langle n,n,n,n\rangle$ ce qui nous permettra de conclure. Par dévissage on a :

$$C\langle 1,1,1,1\rangle \simeq_{\mathbb{Z}/2} (-1,-1) \otimes (-1,1)$$

et

$$C\langle n,n,n,n\rangle \simeq_{\mathbb{Z}/2} (-n^2,-n^2)\otimes(-n,n) \simeq_{\mathbb{Z}/2} (-1,-1)\otimes(-n,n)$$

D'après l'étude des algèbres de quaternions, on a :

$$(-n,n) \simeq_{\mathbb{Z}/2} (-1,1)$$

puisque $\langle 1,-1\rangle$ et $\langle n,-n\rangle$ sont équivalentes. Ainsi,

$$(-1,1) \simeq_{\mathbb{Z}/2} (-n,n) \Longrightarrow C\langle 1,1,1,1\rangle \simeq_{\mathbb{Z}/2} C\langle n,n,n,n\rangle.$$

Alors, n est naturellement représenté par $\langle n,n,n,n\rangle$ et est aussi représenté par $\langle 1,1,1,1\rangle$. Ce qui achève de montrer le résultat. □

Bibliographie

[1] Clément de Seguins Pazzis. *Invitation aux formes quadratiques*. Calvage et Mounet, Mathématiques en devenir.

[2] Daniel Perrin. *Cours d'algèbre*. Ellipses, CAPES/agrégation.