THÈSE DE DOCTORAT DE
l'UNIVERSITÉ PARIS 13

Spécialité

Mathématiques

École doctorale Galilée

Présentée par

Nicolas GARREL

Pour obtenir le grade de

DOCTEUR de l'UNIVERSITÉ PARIS 13

Sujet de la thèse :

Invariants cohomologiques de groupes algébriques et d'algèbres à involution

Soutenue le 17 octobre 2018

devant le jury composé de :

Mme Anne Quéguiner	Directrice de thèse	Université Paris 13
M. Philippe Gille	Rapporteur	CNRS, Université Lyon 1
M. Michel Brion	Examinateur	CNRS, Université Grenoble-Alpes
M. Charles De Clercq	Examinateur	Université Paris 13
M. Bruno Kahn	Examinateur	CNRS, Université Paris 7
M. Jean-Pierre Tignol	Examinateur	Université Catholique de Louvain

Table des matières

Remerciements

Il était une fois un petit garçon qui aimait bien les nombres, et les énigmes. Il était une fois un adolescent qui nourrissait quelque aspiration de devenir chercheur, peut-être, qui sait. Il était une fois un jeune adulte qui, au coeur de la nuit, à la lueur vacillante d'une lampe Ikea™, se prenait la tête entre les mains, se demandant avec désespoir s'il était judicieux de séparer la proposition 2.3.9 en deux lemmes distincts, ou s'il valait mieux conserver une preuve plus longue mais un énoncé plus clair, ou bien encore aller dormir et trancher le problème le lendemain, J-3 avant la sacro-sainte date limite.

Quelle aventure que tout ceci. Comme toute belle épopée, elle a ses origines, et ses détours. Des épreuves, de l'amour, des rires, des tragédies. Et ce sentiment, en tournant la dernière page, que voilà, ah, ça y est, c'est fini. C'est un peu triste, un livre qui s'achève, on voudrait toujours qu'il y ait une suite. Il y en aura une. Mais dans ce livre-ci, vous n'avez pas droit aux épreuves, à l'amour, aux rires ou aux tragédies. Rien de tout cela n'est écrit ici, vous n'y pourrez lire que quelques théorèmes, quelques remarques, quelques exemples. Et à vrai dire, il y a des chances que vous ne les lisiez pas. Personne ne veut retenir de la Quête du Graal qu'une interminable description d'un vase en or, ou peut-être d'une pierre incandescente, ou d'un bocal à anchois. On rêve de chevalerie, et pas d'artisanat, si minutieux soit-il. C'est pourquoi, dans ces rares pages que vous lirez, je veux au moins présenter quelques personnages, quelques companions, qui m'ont accompagné dans cette quête. Dire merci aux Merlin, aux Lancelot, aux Guenièvre et aux Perceval de cette légende, qui n'y auraient pas autrement figuré.

Il me faut avant tout remercier mon jury, Charles De Clercq, Bruno Kahn, Michel Brion, Jean-Pierre Tignol, d'avoir pris le temps et la peine de venir m'écouter et de me lire, en particulier mes rapporteurs, Philipe Gille et Alexander Merkurjev, qui ont dû éplucher mon manuscrit pendant des jours que l'on consacre plus volontier aux vacances. Bien entendu il reste un nom, le plus évident, celui d'Anne, ma directrice, à qui cette thèse doit énormément, plus que je n'ai de place ici à y consacrer. Elle lui doit des mathématiques, bien sûr, mais aussi et surtout de l'écoute, du soutien, des encouragements, toutes ces choses sans lesquelles on ne peut pas envisager de passer trois ans avec un manuscrit pour horizon.

Je dois ensuite remercier ma famille, et en premier lieu mon père, qui m'a

élevé, m'a toujours soutenu même lorsqu'il n'avait pas la plus petite idée de ce dans quoi je me lançais, et m'a consacré un gros bout de sa vie. Mina aussi, qui tient une place particulière dans mon coeur. Je ne peux pas citer tous les noms, grand-parents, oncles, tantes, cousins et cousines de toutes sortes, de sang ou de coeur, toutes ces personnes qui n'ont pas toutes été nécessairement à mes côtés pendant cette thèse, mais qui toutes m'ont vu grandir, m'ont fait grandir ; et il faut bien grandir avant de partir à l'aventure.

Mes ami-e-s de Nice, Damien, Jonjon, le Baobab Rousseau, Foued-Barnabé, et bien d'autres, avec qui j'ai été très jeune et stupide, puis de moins en moins jeune, et tout aussi stupide. Je persiste à penser que l'UNSS Sloubi avait une vraie chance de succès.

Celleux de prépa, qui ont permis à deux années que l'on qualifiera pudiquement de studieuses d'être parmi les meilleures de ma vie. Que ce soient les internes de HX1 (Paul/Pierre, Fiona, Anthony, Pauline, Miguel, Benoît et les autres) ou le clan des calorifères par la suite (Charlotte lumière de mes jours, Ric le panda, ...). Je suis arrivé en prépa comme on arrive à Poudlard, les yeux écarquillés et le coeur serré, j'en suis parti avec plus de souvenirs et d'amis qu'à savoir quoi en faire.

Mes innombrables et inoubliables ami-e-s de la période ENS, qu'il m'est physiquement impossible de citer nommément ; que ce soit justement à l'École, en DG, au volley (la première équipe 2 de l'Histoire, la meilleure équipe 1 de l'Histoire), en K-Fêt, au BOcal, au COF, au BDS, au Mega, en AG, en Courô, à Montrouge, en cave 26, parfois même dans l'amphi Rataud, dans ces mille et un lieux que j'ai hantés, où j'ai hurlé, ri, bu, pleuré, trollé et où surtout je me suis senti chez moi ; dans d'autres écoles aussi puisqu'une ne me suffisait pas, et notamment à l'X (Morgane, Hugo, Bastien, ...) où j'ai si souvent trouvé bon accueil.

Enfin pour la chronologie, mes camarades de thèse, cette bande de braves qui se retrouvent au 12, Pierre, Tom, Mattia, Carlos, Anna, Marta, Jean-Michel, notre regrettée cheffe Anna-Laura, Delphin, Daniel, Didier et les autres, passés et présents, mais aussi les chercheuses et chercheurs qui ont accompagné mes premiers pas, et les membres de l'équipe de support, notamment Isabelle et Yolande qui ont compensé comme elles ont pu mes maladresses administratives.

Je n'ai pas pu rendre justice à toute la galerie de personnages qu'il m'aurait fallu évoquer, par manque de temps, par manque de place, par défaillance de ma mémoire, et si des yeux venaient à parcourir ces lignes et à ne s'y reconnaître nulle part, je tiens à m'en excuser. Mais il est un groupe qui doit figurer plus que tous les autres, ma Table Ronde, ma deuxième famille : les grotas.

Louis, seigneur de la nuit, des profondeurs, et guérisseur de machines. Paul Odieux et Puant Simon, l'ours le plus brave dont un couple de saumons pouvait rêver. Grogrodile, dont j'ai hâte d'être dans le jury de thèse, même si ça implique d'aller à Grenoble. Machin, qui doit être en train de devenir fou en triant les pages de cette thèse par couleur. Pandarion, dont le demi-médaillon est forgé non dans l'acier mais dans mon coeur. Amiel, et ses divers alter-ego qui sont autant de frères et de soeurs. Béné, mi-loutre, mi-lapin, et re-mi-loutre derrière ; nous aurons toujours Philadelphie. Grotillon, le sanglier au coeur le plus tendre parmi les hommes. Surée, qui m'a appris beaucoup sur moi-même, et aussi un peu sur le café. Hélène, qui m'a offert à la Scène, à qui j'appartiens désormais. Jonas, qui m'a autant fait découvrir de jeux que d'astuces sur le bon emploi d'un PEL. Léa, puisses-tu voler sur les ailes de tes oiseaux quand mon souffle t'appelle. Maud, pour qui je pourrais presque envisager d'aller poser les pieds en Bretagne. Marc, l'inexplicable motard sans moto, à l'hospitalité indéfectible, quoique mousticale. Marine la Bio, qui est depuis longtemps devenue simplement Marine. P4bl0, dont je suis obligé de dire du bien vu que c'est mon proprio, et mon compagnon de magret. Picomango, California Girl et co-dégé belle, grande et forte. Snoopy, mon complémentaire exemplaire, est-il besoin d'en dire davantage. Ted, dont je reconnais l'existence. Laetitia, non-malicieuse au sens très, très fort. Il n'y a pas de liste exhaustive des grotas, et j'embrasse fort celles et ceux qui pourraient y figurer, et toute la grotadhérence.

Plus que quiconque, vous êtes celles et ceux sur qui repose cette thèse, tout à la fois mon épée légendaire et le rocher d'où je l'extirpe.

Introduction

Algèbres à involution

Comme l'indique son titre, les objets centraux de cette thèse sont les algèbres à involution. On entend par là des algèbres simples centrales sur un corps munies d'un anti-automorphisme involutif (souvent noté σ ou τ, parfois θ ou ρ), l'exemple le plus élémentaire étant une algèbre de matrices munie de la transposition. *On fera toujours l'hypothèse que le corps de base k est de caractéristique différente de 2.* Excepté brièvement dans le dernier chapitre, les involutions que nous considérerons seront de *première espèce*, c'est-à-dire qu'elles agissent trivialement sur le centre. Bien que ne faisant pas nécessairement partie du bagage mathématique standard de tout algébriste, les algèbres à involution apparaissent naturellement dans de nombreux contextes, et les chemins qui y conduisent sont de nature variée.

Historiquement, les algèbres à involution ont été introduites par Albert dans les années 30 dans le contexte de la géométrie riemannienne (voir par exemple [1]). Albert a initié une étude systématique des algèbres à involution afin de caractériser les algèbres à division sur $\mathbb{Q}$ qui apparaissent comme algèbre de multiplication d'une surface de Riemann. Cette motivation historique est toutefois très éloignée des considérations qui apparaîtront dans cette thèse.

Une porte d'entrée vers les algèbres à involution revêtant une bien plus grande importance en ce qui nous concerne est à trouver dans les travaux de Weil sur les groupes algébriques ([34]). Se fondant sur les travaux de Killing, Élie Cartan avait, à la fin du 20e siècle, classifié les groupes de Lie simples sur $\mathbb{C}$ ([36]), en passant par la classification, plus simple à établir, des algèbres de Lie correspondantes. La classification se fait en terme des fameux *diagrammes de Dynkin*, associés aux systèmes de racines. On y retrouve en particulier les groupes dits *classiques*, à savoir PSL_{n+1} (correspondant au diagramme A_n), SO_{2n+1} (correspondant à B_n), PSp_{2n} (correspondant à C_n) et PSO_{2n} (correspondant à D_n) pour $n \neq 4$ (les groupes de type D_4 ne sont généralement pas considérés comme classiques à cause des phénomènes exceptionnels de *trialité*).

En ce qui concerne les groupes algébriques, Chevalley montre dans les années 50 que la classification des groupes semi-simples sur un corps algébriquement clos ne dépend pas du corps, et notamment pas de la caractéristique, et on retrouve essentiellement la même classification en terme de diagrammes de Dynkin (il faut également tenir compte des isogénies, par exemple les groupes de type A_n sont de la forme SL_{n+1}/μ_d où d divise $n+1$, le groupe PSL_{n+1} correspondant à $d = n+1$). En réalité, il apparaît rapidement que la classification est identique si on suppose non pas que le corps est algébriquement clos, mais que le groupe est *déployé* (c'est-à-dire qu'il contient un tore maximal déployé).

Si on veut tenir compte des groupes non déployés, on se rend aisément compte que les formes bilinéaires jouent un rôle primordial dans la description attendue. C'est particulièrement manifeste pour les groupes de type B_n et D_n, puisque le groupe $SO(q)$ où q est une forme quadratique est de toute évidence une forme non triviale du groupe déployé correspondant. Les groupes de type C_n sont par construction liés aux formes alternées, mais en revanche celles-ci sont entièrement caractérisées par leur dimension, même sur un corps quelconque. Quant aux groupes de type A_n, il est un peu moins évident de constater qu'ils sont liés aux formes hermitiennes : en effet, si K'/K est une extension quadratique, on dispose pour toute forme hermitienne h sur $(K', {}^-)$ (où ${}^-$ est l'automorphisme non trivial de K'/K) du groupe unitaire $SU(h)$, et SL_{n+1} correspond au cas où $K' = K \times K$, donc ces groupes sont bien des formes des groupes A_n déployés.

L'observation de Weil est qu'on peut obtenir tous les groupes classiques si on déplace notre attention des formes bilinéaires vers les involutions qu'elles induisent sur des algèbres de matrices. En effet, toute forme b symétrique, alternée ou hermitienne sur un K-espace vectoriel V induit sur $\mathrm{End}_K(V)$ une involution σ_b dite *adjointe* à la forme, qui vérifie pour tout $u \in \mathrm{End}_K(V)$ et tous $x, y \in V$

$$b(u(x), y) = b(x, \sigma_b(u)(y)),$$

et on peut définir le groupe d'isométrie de la forme comme

$$G = \{u \in \mathrm{End}_K(V) \mid u\sigma_b(u) = \mathrm{Id}\}. \tag{0.0.1}$$

De plus, toute involution sur $\mathrm{End}_K(V)$ correspond à une certaine forme b, qui est unique à un facteur près. Si l'involution est de première espèce (donc si elle fixe K), elle correspond soit à une forme symétrique (on dit que l'involution est *orthogonale*) soit à une forme alternée (on dit que l'involution est *symplectique*). Dans le cas contraire, l'involution est dite *unitaire*.

Une fois qu'on dispose de cette description, il apparaît qu'on peut remplacer $(\mathrm{End}_K(V), \sigma_b)$ par une algèbre à involution (A, σ) quelconque, et définir un groupe algébrique par l'analogue direct de la formule (0.0.1). Après extension à une clôture séparable, l'algèbre A est déployée, donc σ correspond à un certain σ_b, et le groupe est donc une forme d'un des groupes déployés classiques. Le type de σ est défini comme le type du σ_b obtenu après déploiement. Le point crucial, suivant Weil, est qu'on obtient ainsi tous les groupes classiques (on renvoie au chapitre VI de [17] pour une étude complète de la question).

Comme le met en exergue la discussion précédente sur les groupes algébriques, les algèbres à involution entretiennent des liens étroits avec les formes bilinéaires ou hermitiennes, ce qui constitue un autre point d'entrée possible dans la théorie. Précisément, on a vu qu'on pouvait naturellement associer une algèbre à involution à une forme symétrique, alternée ou hermitienne ; on peut regrouper ces trois catégories en une même définition : si K est muni d'un automorphisme τ d'ordre 2 et si $\varepsilon = \pm 1$, on peut définir une forme ε-hermitienne sur (K, τ) comme vérifiant $h(ax, by) = \tau(a)h(x, y)b$ et $h(y, x) = \varepsilon\tau(h(x, y))$. Le cas orthogonal est donné par $\tau = \mathrm{Id}$ et $\varepsilon = 1$, le cas symplectique par $\tau = \mathrm{Id}$ et $\varepsilon = -1$, et le cas unitaire par $\tau = {}^-$ et $\varepsilon = 1$. À partir d'une paire (K, τ), on peut donc définir des formes hermitiennes (V, h) qui induisent des algèbres à involution $(\mathrm{End}_K(V), \sigma_h)$. Le fait de se placer dans le cadre des algèbres à involution permet de symétriser complètement la situation : sur une algèbre à involution (A, σ), on peut définir des formes ε-hermitiennes (V, h), et alors $(\mathrm{End}_A(V), \sigma_h)$ est encore une algèbre à involution. On renvoie à [16] ainsi qu'à la partie 2.1 pour plus de détails sur ces considérations, mais on peut déjà constater que les algèbres à involution forment un cadre stable pour étudier les formes hermitiennes et leurs algèbres d'endomorphismes.

D'autre part, un certain nombre d'autres constructions classiques autour des formes quadratiques trouvent naturellement leur place au sein de la théorie des algèbres à involution. Un exemple naturel est celui des algèbres de Clifford : à toute forme quadratique q on associe une certaine algèbre $C(q)$, qui est canoniquement munie d'une involution. On ne peut pas directement étendre cette définition aux algèbres à involution orthogonale à cause d'une obstruction omniprésente dans ce type de construction : l'involution associée à une forme quadratique ne la caractérise qu'à similitude près, donc on ne peut étendre aux involutions que les constructions qui sont invariantes par similitude. Dans le cas de l'algèbre de Clifford, on peut ainsi définir l'algèbre de Clifford *paire* d'une algèbre à involution orthogonale, et ainsi à une algèbre à involution on associe une autre algèbre à involution ([17, §8]). On peut également citer l'exemple de la forme d'Albert associée à une algèbre de biquaternions, qui se généralise en l'algèbre discriminante d'une algèbre à involution unitaire ([17, §10]). La correspondance classique entre formes quadratique de dimension 6 et de discriminant 1 et algèbres de biquaternions se généralise ainsi naturellement en une correspondance entre algèbres de type D_3 et A_3 (voir [17, §15.D], ainsi que la partie 3.2 de cette thèse pour des calculs explicites).

Enfin, parmi les autres situations où les algèbres à involution peuvent jouer un rôle déterminant, on peut notamment citer la théorie des représentations de groupes, puisque l'algèbre de groupe $K[G]$ d'un groupe fini est, si K est de caractéristique nulle, une algèbre semi-simple naturellement munie d'une involution induite par $g \mapsto g^{-1}$.

Invariants

On a décrit le lien étroit entre deux des termes du titre de cette thèse, à savoir les groupes algébriques (qu'on ne présente plus) et les algèbres à involution (qu'on a présentées). Il reste donc à préciser ce qu'on entend par *invariants cohomologiques*, et à décrire le contexte dans lequel s'inscrit cette thèse.

L'origine de l'étude de ces invariants se trouve sans nul doute dans la théorie des formes quadratiques. C'est un fait très élémentaire que si le déterminant de la matrice d'une forme bilinéaire symétrique dans une certaine base n'est pas un invariant bien défini, en revanche il est bien défini modulo les carrés : c'est ce qu'on appelle le déterminant d'une forme quadratique, et c'est le premier invariant non trivial que l'on définit ; il est donc à valeurs dans $K^*/(K^*)^2$. On peut définir un deuxième invariant, à valeurs dans le groupe de Brauer $\mathrm{Br}(K)$, de deux façons différentes. Une première possibilité est de considérer la classe de Brauer $[C(q)]$ de l'algèbre de Clifford de q si q est de dimension paire, et la classe $[C_0(q)]$ si q est de dimension impaire ; c'est ce qu'on appelle l'invariant de Clifford $c(q) \in \mathrm{Br}(K)$. Une deuxième idée est de partir d'une diagonalisation $q = \langle a_1, \dots, a_r\rangle$, et de considérer $w_2(q) = \sum_{i<j}(a_i, a_j)$ où $(a_i, a_j) \in \mathrm{Br}(K)$ est la classe de Brauer de l'algèbre de quaternions correspondante ; c'est ce qu'on appelle l'invariant de Hasse-Witt de q. Ces deux invariants à valeur dans le groupe de Brauer ne sont pas égaux, mais on peut les relier par des formules simples faisant intervenir la dimension et le déterminant (voir par exemple [19, prop 3.20]).

Ces deux invariants représentent les deux directions classiques dans lesquelles on peut poursuivre la construction. Tout d'abord, on observe que le déterminant est à valeurs dans le premier groupe de cohomologie $H^1(K, \mu_2)$ (pour les prérequis sur la cohomologie galoisienne, on renvoie par exemple à [30], [12], ou au chapitre VII de [17]), tandis que les invariants de Clifford et de Hasse-Witt sont à valeurs dans $H^2(K, \mu_2)$ (qui est naturellement isomorphe à la 2-torsion de $\mathrm{Br}(K)$). Il est donc naturel de chercher à construire des invariants à valeurs dans $H^d(K, \mu_2)$ pour d de plus en plus grand ; on qualifiera logiquement ces invariants de *cohomologiques.* Notons qu'en degré 0, on peut définir $\dim_0(q) \in \mathbb{Z}/2\mathbb{Z} = H^0(K, \mu_2)$ comme la dimension modulo 2 de q.

Si on poursuit dans la direction de l'invariant de Hasse-Witt, on arrive à la construction des invariants de Stiefel-Whitney (analogues aux classes de Stiefel-Whitney en K-théorie) : pour tout $d \in \mathbb{N}$, si $q = \langle a_1, \dots, a_r\rangle$, on peut poser

$$w_d(q) = \sum_{i_1<\cdots<i_d} (a_{i_1}, \dots, a_{i_d}) \in H^d(K, \mu_2) \tag{0.0.2}$$

où $(a_{i_1}, \dots, a_{i_d}) \in H^d(K, \mu_2)$ est le symbole galoisien naturel. On revient sur ces invariants dans la partie 1.2.9.

Si on poursuit dans la direction de l'invariant de Clifford : on commence par observer que $\dim_0(q)$ ne dépend que de la classe de Witt de q (voir par exemple

[7] ou [19] pour toutes les définitions et tous les résultats standard sur l'anneau de Witt), et définit donc une application $e_0 : W(K) \to H^0(K, \mu_2)$, qui est clairement un morphisme de groupes additifs. On peut ensuite observer que si q est de dimension paire $2r$, et qu'on modifie la définition de $\det(q)$ par $\mathrm{disc}(q) = (-1)^r \det(q)$ (ce qu'on appelle le *discriminant* de q, parfois aussi appelé *déterminant signé* dans la littérature), alors $\mathrm{disc}(q)$ ne dépend que de la classe de Witt de q, et donc définit une application $e_1 : I(K) \to H^1(K, \mu_2)$, où $I(K) \subset W(K)$ est l'idéal fondamental de l'anneau de Witt $W(K)$ constitué des formes de dimension paire. De plus, on voit facilement que cette application est en réalité un morphisme de groupes additifs, et que son noyau est précisément $I^2(K)$ ([7, thm 13.7]). On constate alors que sur $I^2(K)$, $c(q)$ ne dépend encore que de la classe de Witt de q et définit un morphisme additif $e_2 : I^2(K) \to H^2(K, \mu_2)$ ([7, thm 14.3]). On voit alors la généralisation se dessiner : on souhaiterait construire pour tout $n \in \mathbb{N}$ un morphisme additif

$$e_n : I^n(K) \longrightarrow H^n(K, \mu_2) \tag{0.0.3}$$

tel que $e_{n+1}(q)$ soit défini lorsque $e_n(q) = 0$. Cela constitue une partie de la *conjecture de Milnor* (voir [23]), qui affirme notamment que e_n est surjective de noyau $I^{n+1}(K)$, et donc qu'il induit un isomorphisme de $I^n(K)/I^{n+1}(K)$ vers $H^n(K, \mu_2)$. La construction des invariants e_n est *considérablement* plus difficile que celle des invariants w_n ; l'invariant e_3 a été construit par Arason en 1975 ([2]), et l'invariant e_4 par Jacob et Rost en 1989 ([13]). La conjecture de Milnor est entièrement résolue en 2002 par Voevodsky ([33]), notamment grâce à la construction de la *cohomologie motivique*, ce qui lui vaudra la médaille Fields.

Une fois la situation des formes quadratiques en tête pour servir de motivation, on peut établir une notion générale d'invariant, et notamment d'invariant cohomologique, due à Serre dans [10]. On se fixe donc un corps de base k, et on considère $\mathbf{Field}_{/k}$ la catégorie des extensions de corps de k. Alors si F est un foncteur de $\mathbf{Field}_{/k}$ vers la catégorie des ensembles, et si H est un foncteur de $\mathbf{Field}_{/k}$ vers la catégorie des groupes abéliens, on définit

$$\mathrm{Inv}(F, H)$$

comme étant le groupe abélien des transformations naturelles de F vers H (vu par composition avec le foncteur d'oubli comme un foncteur vers les ensembles). Autrement dit, on demande simplement d'avoir pour toute extension K/k une fonction $F(K) \to H(K)$, avec pour seule condition d'avoir une compatibilité avec les extensions de scalaires. On dispose toujours au moins des invariants constants : $H(k) \subset \mathrm{Inv}(F, H)$. Si F est un foncteur vers les ensembles *pointés*, on définit le groupe des invariants *normalisés* $\mathrm{Inv}_{norm}(F, H)$ comme le sous-groupe constitué des invariants qui envoient le point distingué sur 0. On a dans ce cas toujours une décomposition

$$\mathrm{Inv}(F, H) = \mathrm{Inv}_{norm}(F, H) \oplus H(k).$$

Les invariants *cohomologiques* de F correspondent au cas où $H(K) = H^*(K,C)$ pour un certain module galoisien C défini sur k (on dit que les invariants sont « à valeurs dans C »). On note plus succintement $\mathrm{Inv}(F,C)$ ce groupe, et $\mathrm{Inv}^d(F,C)$ pour la partie de degré d (c'est-à-dire correspondant à $H(K) = H^d(K,C)$). L'exemple qui nous intéressera le plus est $C = \mu_2 = \mathbb{Z}/2\mathbb{Z}$.

On parle d'invariant (par exemple cohomologique) d'un groupe algébrique G lorsque $F(K) = H^1(K,G)$ est l'ensemble (pointé) des classes d'isomorphisme de G-torseurs sur K ; on note alors $\mathrm{Inv}(G,H)$ (et $\mathrm{Inv}(G,C)$ pour les invariants cohomologiques à valeurs dans C). On parle d'invariant d'algèbres à involution lorsque $F(K)$ est un sous-ensemble des algèbres à involution sur K (on peut par exemple se restreindre à un certain type d'involution, ou à un degré fixé, ou un indice borné, etc.). Le lien évoqué ci-dessus entre groupes classiques et algèbres à involution permet d'établir que ces deux notions sont en réalité extrêmement proches. Notamment, si (A,σ) est une algèbre à involution, alors on dispose du groupe algébrique $G = \mathrm{Aut}(A,\sigma)$ (groupe absolument presque simple de type adjoint) dont les points sont donnés par les automorphismes d'algèbre de A commutant avec σ et il est établi dans [17, 19.14] que $H^1(K,G)$ est naturellement identifié aux classes d'isomorphismes d'algèbres à involution sur K de même type que σ et de même degré que A (l'ensemble étant bien entendu pointé par (A,σ)).

La définition d'invariants cohomologiques non triviaux d'algèbres à involution ou de groupes algébriques est globalement un exercice difficile, et relativement peu d'invariants ont été construits jusqu'ici. Les seuls cas traités de façon satisfaisante sont les invariants de degré au plus 3. Il est montré dans [17, 31.15] que si G est un groupe algébrique sur k, $\mathrm{Inv}^1_{norm}(G,C)$ est canoniquement isomorphe à $\mathrm{Hom}_\Gamma(\pi_0(G_{sep}),C)$ où Γ est le groupe de Galois absolu de k, et $\pi_0(G_{sep})$ est le groupe des composantes connexes de G_{sep} ; en particulier, un groupe connexe n'a pas d'invariant de degré 1 non constant. Il est également montré ([17, 31.19]) que si n est premier à la caractéristique de k et si G est connexe alors $\mathrm{Inv}^2_{norm}(G,\mu_n)$ est naturellement isomorphe à la n-torsion du groupe de Picard $Pic(G)$; en particulier un groupe simplement connexe n'a pas d'invariant modulo n non constant de degré 1 ou 2.

Pour le cas des invariants de degré 3, jusqu'à récemment le mieux que l'on savait faire était de traiter le cas des groupes simplement connexes : $\mathrm{Inv}^3_{norm}(G,\mu_n)$ est alors un groupe cyclique muni d'un générateur distingué appelé *invariant de Rost* (voir la deuxième partie de [10] pour le détail des constructions). Mais très récemment, Merkurjev a dans une série d'articles déterminé $\mathrm{Inv}^3_{norm}(G,\mu_n)$ pour n'importe quel groupe G semi-simple (voir [21] et [22]).

On renvoie à [31] pour un recensement relativement récent des invariants cohomologiques d'algèbres à involution connus. Il apparaît que les invariants de degré au moins 4 sont quasiment inexistants excepté dans des contextes très restreints, notamment en indice au plus 2 (voir [4], sur lequel on reviendra dans la partie 3.1.3).

Contenu de la thèse

Maintenant qu'on a exposé le contexte mathématique sous-jacent, on peut décrire l'objectif de cette thèse : construire des invariants cohomologique d'algèbres à involution (et donc de groupes algébriques) de degré supérieur. La thèse suit une progression logique en trois chapitres : le premier revient sur le cas des formes quadratiques et propose une étude relativement complète des invariants de I^n, le deuxième construit des outils pour étendre ces méthodes au cas des algèbres à involution, et le troisième met ces outils en application. On décrit un peu plus en détail le contenu de chaque chapitre.

Le point de départ est la volonté d'étendre des invariants définis sur I^n à des algèbres à involution en indice 2 suivant la méthode de Berhuy ([4]). Il apparaît que pour rentabiliser cette méthode, il faut connaître le plus possible d'invariants de I^n ; or mis à part e_n, on ne disposait que de quelques constructions, notamment un invariant à valeurs dans $H^{2n}(K,\mu_2)$, construit à partir d'une opération de « carré divisé » $I^n \to I^{2n}$ (voir [9, §19]). De plus, pour étendre ces invariants il faut un certain contrôle sur leur comportement vis-à-vis des similitudes (le problème récurrent pour passer des formes quadratiques aux involutions orthogonales) et de la ramification pour des valuations discrètes de rang 1 (une considération standard quand on déploie génériquement une algèbre). On a donc entrepris d'étendre la méthode décrite dans [9, §19] pour classifier entièrement les invariants dans $\mathrm{Inv}(I^n,\mu_2)$ et décrire leurs propriétés, en utilisant des opérations $I^n \to I^{nd}$ pour tout $d \in \mathbb{N}$.

L'observation de base pour construire ces opérations est que les formes de Pfister ont un comportement régulier vis-à-vis des λ-opérations sur l'anneau de Grothendieck-Witt (voir la proposition 1.1.37), ce qui permet de « déformer » la structure de λ-anneau en une autre pour laquelle les opérations envoient I^n dans I^{nd}. Comme toutes ces constructions sont essentiellement formelles, on développe un formalisme général décrivant comment on peut déformer naturellement une structure de pré-λ-anneau, et en particulier comment obtenir une structure qui a un comportement naturel vis-à-vis d'une notion abstraite de forme de Pfister (voir le théorème 1.1.41).

On démontre ensuite (voir le théorème 1.2.40) que ces opérations $I^n \to I^{nd}$ forment une « base » des invariants $\mathrm{Inv}(I^n,W)$, et que de même les invariants cohomologiques $I^n(K) \to H^{nd}(K,\mu_2)$ qui s'en déduisent par composition avec e_{nd} forment une « base » de $\mathrm{Inv}(I^n,\mu_2)$ (les guillemets sont présents parce que des combinaisons infinies sont nécessaires). Pour éviter de dupliquer toutes les preuves on met en place un formalisme commun aux deux types d'invariants (invariants de Witt et invariants cohomologiques). Le reste de la section est consacrée à l'étude des propriétés élémentaires de ces invariants, notamment leur comportement par produit, similitude, et restriction de I^n à I^{n+1}. On consacre également une partie à l'étude des invariants de formes dans I^n qui ont une r-forme de Pfister en facteur, afin de généraliser la construction donnée dans [9, 20.8].

Enfin, une courte section expose une idée, qui sera à développer ultérieurement, consistant à décrire les invariants qui sont définis lorsqu'un invariant précédemment défini s'annule, de sorte à construire des « tours » d'invariants, à la manière des invariants e_n.

Le deuxième chapitre, indépendant du premier, décrit les outils nécessaires pour étendre les méthodes précédentes aux algèbres à involution. Un des problèmes récurrents pour passer des formes quadratiques aux involutions orthogonales, outre évidemment la complexité accrue de l'objet étudié, est le manque de structure dont on dispose. Les formes quadratiques peuvent s'additionner, se multiplier, et on dispose également des opérations λ, dont on a vu dans le chapitre précédent qu'elles étaient une clé possible pour définir des invariants. À l'inverse, on peut multiplier des algèbres à involution (par le produit tensoriel), et [17, §10] décrit comment définir des opération λ, mais on ne peut pas combiner ces opérations car on ne dispose pas a priori d'addition. Il a déjà été observé (notamment dans [18] et [6]) que si en revanche on dispose d'une équivalence de Morita entre deux algèbres à involution, alors on peut définir leur somme, par exemple en les représentant comme des formes ε-hermitiennes sur une même algèbre à involution ; si on ne dispose pas d'une équivalence de Morita explicite, les formes hermitiennes sont seulement définies à un facteur près, et la somme n'est pas bien définie.

On met en place dans ce chapitre un formalisme qui permet d'effectuer toutes les opérations que l'on souhaite sans avoir à garder un contrôle permanent sur des équivalences de Morita explicite. Précisément, pour toute algèbre à involution (A, σ) de première espèce, on définit un anneau commutatif gradué $\widetilde{GW}(A, \sigma)$ qui contient toutes les classes d'isométrie de formes ε-hermitiennes sur (A, σ), ainsi que l'équivalent $\widetilde{W}(A, \sigma)$ de l'anneau de Witt pour les formes quadratiques. On utilise pour cela des équivalences de Morita canoniques données par la forme trace d'involution T_σ. On définit également une structure de pré-λ-anneau sur $\widetilde{GW}(A, \sigma)$, qui correspond aux opérations sur les involutions décrites dans [17, §10].

Enfin, afin de préparer l'application de ces outils à la construction d'invariants cohomologiques, on définit un analogue de la filtration fondamentale de l'anneau de Witt, et on donne une description du gradué associé, qui remplace la cohomologie modulo 2 dans ce contexte (par analogie avec la conjecture de Milnor).

Pour finir, le dernier chapitre est celui où on confronte les deux premiers pour enfin construire des invariants cohomologiques d'algèbres à involution. C'est l'objet de la première partie, où les opérations contruites dans le premier chapitre sont appliquées à la filtration de $\widetilde{GW}(A, \sigma)$ (voir la proposition 3.1.1). On discute après la proposition de comment exploiter ces constructions pour construire des invariants supérieurs, notamment des invariants relatifs, et on propose une étude plus approfondie du cas des algèbres d'indice 2.

Le reste du chapitre est consacré à des phénomènes en petite dimension. La deuxième partie est dédiée à des calculs explicites concernant l'équivalence entre algèbres de type A_3 et D_3, ce qui est mis en application dans la troisième partie où on fait le lien entre nos constructions et un invariant de degré 4 défini dans [28], et où on exploite les outils du premier chapitre pour étendre au cas de l'indice 2 un certain invariant défini sur les formes quadratiques de degré 12 dans I^3 (voir [9, 20.8]).

Chapitre 1

Invariants de classes de Witt

Dans ce chapitre on propose un traitement détaillé des invariants de Witt et des invariants cohomologiques de I^n. On rappelle qu'on s'est fixé un corps de base k de caractéristique différente de 2, et que K/k désigne une extension de corps. Par « forme quadratique » on entendra *toujours* forme quadratique *non dégénérée.* On note $GW(K)$ l'anneau de Grothendieck-Witt et $W(K)$ l'anneau de Witt. Dans $GW(K)$ on note $\hat{I}(K)$ l'idéal fondamental des formes de dimension virtuelle nulle, dont la projection dans $W(K)$ est l'idéal fondamental $I(K)$. On fait la remarque importante que la projection naturelle est en réalité un isomorphisme $\hat{I}(K) \simeq I(K)$, et en particulier on identifiera systématiquement $\hat{I}^n(K)$ et $I^n(K)$. Notamment, une n-forme de Pfister $\langle\langle a_1, \ldots, a_n\rangle\rangle$ désignera sauf mention explicite du contraire un élément de $\hat{I}^n(K)$; précisément, $\langle\langle a\rangle\rangle = \langle 1\rangle - \langle a\rangle$ (et non comme on en a l'habitude $\langle 1, -a\rangle$), ce qui ne change rien pour les classes de Witt.

Notre objectif est de construire des applications naturelles $\pi_n^d : I^n(K) \to I^{nd}(K)$, vérifiant

$$\pi_n^d\left(\sum_{i=1}^r \varphi_i\right) = \sum_{i_1<\cdots<i_d} \varphi_{i_1}\cdots\varphi_{i_d}$$

pour toutes n-formes de Pfister φ_i (voir la proposition 1.2.11), et d'en déduire par composition avec e_{nd} des invariants $u_{nd}^{(n)} : I^n(K) \to H^{nd}(K, \mu_2)$. La construction des π_n^d est essentiellement formelle, ne dépendant que des relations des formes de Pfister dans le λ-anneau $GW(K)$. On donne donc une définition valable dans n'importe quel λ-anneau (voir le théorème 1.1.41).

Le résultat central du chapitre est le théorème 1.2.40, qui montre en particulier (voir le corollaire 1.2.42) que tout invariant de Witt (resp. cohomologique) peut s'écrire de façon unique comme combinaison infinie des π_n^d (resp. des $u_{nd}^{(n)}$). Pour éviter de dupliquer les preuves, on adopte un formalisme commun pour ces deux types d'invariants (voir la partie 1.2.1), dans lequel π_n^d et $u_{nd}^{(n)}$ sont tous les deux notés f_n^d. La description exacte donnée dans le théorème se fait en terme d'invariants notés g_n^d, qui sont décrits explicitement (proposition 1.2.36) et ont la propriété remarquable que toute combinaison, même infinie, donne un invariant.

Une fois ce théorème établi, on peut utiliser les propriétés particulières des f_n^d pour démontrer un certain nombre de propriétés des invariants, notamment comment exprimer le produit de deux invariants (proposition 1.2.46), la restriction d'un invariant de I^n à I^{n+1} (proposition 1.2.54), le comportement d'un invariant par similitude (proposition 1.2.65), et par résidus pour une valuation discrète (proposition 1.2.69). On étudie également le lien entre notre description des invariants de I et I^2 avec la description de Serre des invariants de formes quadratiques en dimension fixée, et on fait le lien avec une description de Vial des opérations sur la cohomologie modulo 2.

Dans la dernière partie du chapitre, on propose une réflexion sur une notion de « tours d'invariants », à savoir des suites d'invariants tels que chaque invariant est défini si les précédents sont nuls (sur le modèle des invariants e_n).

1.1 Anneaux grecs et éléments de Pfister

On présente ici des définitions et résultats classiques (voir [35]) sur les λ-anneaux, ainsi que quelques constructions qui nous seront utiles. En revanche, on change un peu le point de vue en ne privilégiant pas les λ-opérations telles que $\lambda^d(1) = 0$ pour $d \geqslant 2$; on réservera le symbole λ à celles-ci, et on utilisera plutôt le symbole α pour des opérations qui ont une action quelconque sur 1.

Pour cette raison, on choisit d'adopter une terminologie plus neutre en appelant *anneau grec* ce qui est appelé *pré-λ-anneau* dans la littérature moderne (et était initialement appelé *λ-anneau* chez Grothendieck). À un anneau grec est associée une famille d'opérations vérifiant les axiomes de pré-λ-anneau au sens de [35], chacune caractérisée par son action sur 1.

La finalité est de contruire des opérations ayant un bon comportement sur une famille fixée d'éléments (en ce qui nous concerne, les *éléments de Pfister*).

1.1.1 Anneaux grecs

Opérations grecques

Définition 1.1.1. Soit R un anneau commutatif. Une *opération grecque* sur R est une suite d'applications

$$\alpha^d : R \longrightarrow R$$

pour tout $d \in \mathbb{N}$ vérifiant les propriétés suivantes :

(i) $\forall x \in R$, $\alpha^0(x) = 1$;

(ii) $\forall x \in R$, $\alpha^1(x) = x$;

(iii) $\forall x, y \in R$, $\forall d \in \mathbb{N}$, $\alpha^d(x + y) = \sum_{k=0}^{d} \alpha^k(x)\alpha^{d-k}(y)$.

On note $\Gamma(R)$ l'ensemble des opérations grecques de R.

La définition usuelle d'un pré-λ-anneau consiste à dire dans ce langage que c'est un anneau muni d'une opération grecque ; notre définition consistera plutôt à se donner une classe d'équivalence de telles opérations.

Exemple 1.1.2. La suite (λ^d) où $\lambda^d(n) = \binom{n}{d}$ est une opération grecque sur $\mathbb{Z}$.

Exemple 1.1.3. L'exemple qui nous intéresse en premier lieu : les λ-opérations usuelles sur les formes quadratiques définissent une opération grecque sur $GW(K)$. Il est à noter que si ces opérations s'étendent bien à $GW(K)$, elles ne passent en revanche pas au quotient sur $W(K)$, ce qui explique pourquoi on ne travaille pas directement sur $W(K)$.

On propose une caractérisation plus algébrique de la définition précédente : pour tout anneau commutatif R, on définit

$$G(R) = 1 + tR[[t]] \subset R[[t]]. \tag{1.1.4}$$

Alors $G(R)$ est un groupe abélien pour la multiplication dans $R[[t]]$, et on obtient ainsi un foncteur $G : \mathbf{Ring} \to \mathbf{Ab}$. On a un morphisme naturel de groupes

$$\begin{array}{rrcl} \varepsilon_R : & G(R) & \longrightarrow & R \\ & 1 + \sum a_k t^k & \longmapsto & a_1. \end{array} \tag{1.1.5}$$

Proposition 1.1.6. *Soit $\alpha_t : R \longrightarrow G(R)$ une application. On note*

$$\alpha_t(x) = \sum_d \alpha^d(x) t^d.$$

Alors la suite d'applications (α^d) est une opération grecque si et seulement si α_t est un morphisme de groupe qui est une section de ε_R.

Démonstration. C'est une simple reformulation de la définition précédente. □

On se donnera donc une opération grecque indifféremment sous la forme d'une suite d'applications de R dans R, ou d'une unique application à valeurs dans $G(R)$.

Lettres grecques

L'idée des définitions qui suivent est la suivante : si on s'est donné une opération grecque (α^d), peut-on la « déformer » en (β^d) avec

$$\beta^d = \sum_{k=0}^{d} a_{k,d} \alpha^k$$

où les $a_{k,d}$ sont des coefficients dans R, de sorte que les β^d forment encore une opération grecque ?

Il s'avère que c'est possible, et que les $a_{k,d}$ sont entièrement déterminés par les $\beta^d(1) \in R$ pour $d \geqslant 2$. De plus, toutes les suites $(\beta^d(1))_d$ sont atteignables de cette façon, et en particulier on peut inverser le processus pour retrouver les α^d à partir des β^d par le même genre de déformation.

On prend alors le parti de dire que toutes ces opérations définissent une même structure d'*anneau grec*, et que le choix d'une opération spécifique (α^d) correspond au choix d'une suite d'éléments (qui est alors $(\alpha^d(1))$), qu'on appelle la *lettre grecque* de l'opération. On peut ainsi pour un même anneau grec passer d'une lettre grecque à l'autre pour faire varier les opérations qu'on utilise selon les propriétés qu'on désire.

Plus précisément : pour tout anneau commutatif R, on pose

$$L(R) = tG(R) = t + t^2R[[t]] \subset R[[t]]. \tag{1.1.7}$$

Alors $L(R)$ est un groupe (pas abélien) pour la composition dans $R[[t]]$, ce qui définit un foncteur $L : \mathbf{Ring} \to \mathbf{Gpe}$.

Définition 1.1.8. Soit R un anneau commutatif, et $\alpha_t : R \to G(R)$ une opération grecque. On appelle *lettre grecque* de l'opération l'élément $\alpha_t(1) - 1 \in L(R)$, ce qui définit une application naturelle $\Lambda_R : \Gamma(R) \to L(R)$ (où on rappelle que $\Gamma(R)$ désigne l'ensemble des opérations grecques sur R).

On pose aussi

$$A(R) = \{\Phi \in \mathrm{Aut}(G(R)) \,|\, \varepsilon_R \circ \Phi = \varepsilon_R\}. \tag{1.1.9}$$

Autrement dit, un élément de $A(R)$ doit préserver le terme de degré 1.

Proposition 1.1.10. *L'application*

$$\begin{array}{ccc} L(R)^{op} & \longrightarrow & A(R) \\ \tau & \longmapsto & (f \mapsto f \circ \tau) \end{array}$$

définit un morphisme de groupes injectif.

Démonstration. Quel que soit $\tau \in tR[[t]]$, l'application $f \mapsto f \circ \tau$ est un morphisme de groupe de $G(R)$.

Clairement, l'application de l'énoncé est un morphisme de monoïdes vers les endomorphismes de $G(R)$, et comme $L(R)$ est un groupe, on a bien un morphisme de groupes vers les automorphismes de $G(R)$. Il est injectif puisque l'action de τ sur $1 + t$ est $1 + \tau$.

De plus, comme le terme de degré 1 de $\tau \in L(R)$ est t, composer par τ à droite préserve le terme de degré 1, donc le morphisme est à valeurs dans $A(R)$. $\square$

Corollaire 1.1.11. *Le groupe $L(R)$ agit à droite sur $\Gamma(R)$, par $\alpha_t \cdot \tau = \alpha_{\tau(t)}$, et $\Lambda_R : \Gamma(R) \longrightarrow L(R)$ est un morphisme de $L(R)$-ensembles à droite.*

En particulier, l'action de $L(R)$ sur $\Gamma(R)$ est libre.

Démonstration. Le groupe $A(R)$ agit à gauche sur $\Gamma(R)$ par $\Phi \cdot \alpha_t = (x \mapsto \Phi(\alpha_t(x)))$; le fait que Φ soit un automorphisme de groupe montre que $\Phi \cdot \alpha_t$ est bien un morphisme de groupes $R \to G(R)$, et le fait que Φ préserve le coefficient de degré 1 montre que $\Phi \cdot \alpha_t$ est bien une section de ε_R. Comme $L(R)^{op}$ s'injecte dans $A(R)$, $L(R)$ agit à droite sur $\Gamma(R)$.

De plus, la lettre grecque de $\alpha_t \cdot \tau$ est par contruction $\alpha_{\tau(t)}(1) - 1 = (\alpha_t(1) - 1) \circ \tau$, donc l'action de $L(R)$ sur $\Gamma(R)$ est bien compatible avec Λ_R.

De façon générale, pour tout groupe G, si un G-ensemble admet un morphisme vers un G-ensemble libre, il est lui-même libre. Or $L(R)$ est bien entendu un $L(R)$-ensemble libre, donc $\Gamma(R)$ aussi. $\square$

Anneaux grecs

On en vient enfin à la définition qui nous intéresse :

Définition 1.1.12. Un *anneau grec* est un anneau commutatif R muni du choix d'une orbite d'opérations grecques sous l'action de $L(R)$.

Proposition-définition 1.1.13. *Soit R un anneau grec, et soit $\alpha \in L(R)$ une lettre grecque. Alors il existe une unique opération grecque dans l'orbite donnée par la définition qui a α pour lettre grecque. On l'appelle la α-opération de R, et on note $\alpha_t : R \longrightarrow G(R)$ et $\alpha^d : R \longrightarrow R$ les applications correspondantes.*

Démonstration. Une orbite est un $L(R)$-ensemble transitif, donc l'action étant libre la restriction de Λ_R à cette orbite doit être bijective vers $L(R)$. $\square$

Le symbole α sera généralement utilisé pour désigner une lettre grecque quelconque.

Exemple 1.1.14. On notera λ l'élément neutre de $L(\mathbb{Z})$, à savoir $t \in \mathbb{Z}[[t]]$. La λ-opération d'un anneau grec est donc celle vérifiant $\lambda^d(1) = 0$ si $d \geqslant 2$.

Les exemples 1.1.2 et 1.1.3 étaient des λ-opérations, comme la notation employée le suggérait.

Exemple 1.1.15. Dans son étude de la K-théorie, Grothendieck a introduit des opérations sur tout λ-anneau, dites γ-opérations, qui sont devenues classiques dans la théorie. Elles correspondent bien à notre notion de γ-opérations sur un anneau grec si on note γ la lettre grecque $\sum_{d \geqslant 1} t^d$ (autrement dit c'est l'opération caractérisée par $\gamma^d(1) = 1$ pour tout d).

Le fait de définir la structure d'anneau grec à partir d'une orbite d'opérations est justifié par le fait que de nombreuses constructions ne dépendent pas du choix d'une lettre grecque particulière.

Proposition-définition 1.1.16. *Soient R et S deux anneaux grecs, et soit $f : R \longrightarrow S$ un morphisme d'anneaux. Soit $\alpha \in L(R)$; on note $f(\alpha) \in L(S)$ la lettre* *grecque obtenue par fonctorialité. Alors le fait que pour tout $d \in \mathbb{N}$ et tout $x \in R$ on ait $f(\alpha^d(x)) = f(\alpha)^d(f(x))$ ne dépend pas du choix de α.*

Quand cette condition est vérifiée, on dit que f est un morphisme d'anneaux grecs.

Démonstration. Soit $\beta \in L(R)$ une autre lettre grecque, et soit $\tau \in L(R)$ tel que $\beta = \alpha \cdot \tau$. Considérons le diagramme commutatif suivant :

$$\begin{array}{ccccc} R & \xrightarrow{\alpha_t} & G(R) & \xrightarrow{\cdot\tau} & G(R) \\ \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f_*} & & \downarrow{\scriptstyle f_*} \\ S & \xrightarrow{f(\alpha)_t} & G(S) & \xrightarrow{\cdot f(\tau)} & G(S) \end{array}$$

Alors le fait que le carré de gauche commute traduit la condition voulue pour α, le carré de droite commute toujours par fonctorialité, et le fait que le grand rectangle commute traduit la condition pour β. □

Proposition-définition 1.1.17. *Soit R un anneau grec, et soit I un idéal. Soit $\alpha \in L(R)$. Alors le fait que pour tout $d \in \mathbb{N}^*$ on ait $\alpha^d(I) \subset I$ ne dépend pas du choix de α.*

Quand cette condition est vérifiée, on dit que I est un idéal grec.

Démonstration. Si β est une autre lettre grecque, alors β^d est une combinaison des α^k pour $1 \leqslant k \leqslant d$, donc si chaque α^k préserve I, β^d aussi. □

Dimension

Dans cette thèse, on utilisera le fait de changer de lettre grecque pour contrôler la dimension des éléments.

Définition 1.1.18. Soit R un anneau grec et $\alpha \in L(R)$. La α-dimension d'un élément $x \in R$ est le degré de $\alpha_t(x)$ (qui peut être infini).

Exemple 1.1.19. Dans $GW(K)$, la λ-dimension d'une forme quadratique q est sa dimension au sens usuel (aussi appelé son rang).

Exemple 1.1.20. Dans tout anneau grec, 1 est de λ-dimension 1. De façon générale, la α-dimension de 1 est le degré de α.

Bien évidemment, la α-dimension d'un élément dépend fortement du choix de α. On s'intéresse particulièrement aux éléments de dimension 1 :

Proposition 1.1.21. *Soient R un anneau grec, $X \subset R$ un sous-ensemble et $\alpha \in L(R)$. Alors il existe $\beta \in L(R)$ tel que tout $x \in X$ soit de β-dimension 1 si et seulement si il existe $\tau \in L(R)$ tel que pour tout $x \in X$*

$$\alpha_t(x) = 1 + x\tau(t),$$

c'est-à-dire qu'il existe $a_d \in R$ tels que pour tout $d \geqslant 1$ et tout $x \in X$ on ait $\alpha^d(x) = a_d x$.

Démonstration. Si β existe, on pose $\tau = \beta^{-1} \circ \alpha$, qui donne trivialement $\alpha_t(x) = 1 + x\tau(t)$ pour tout $x \in X$, et si τ existe on pose $\beta = \alpha \circ \tau^{-1}$. □

Remarque 1.1.22. La preuve montre qu'on peut prendre $\beta = \alpha \circ \tau^{-1}$. Tout autre choix de β s'écrit $\beta + \delta$ avec $\delta \in t^2 Ann_R(X)[[t]]$ (où $Ann_R(X)$ est l'idéal annulateur de X dans R).

Proposition 1.1.23. *Soit R un anneau grec, et soient $x_1, \dots, x_r \in R$ de α-dimension 1. Alors pour tout $d \in \mathbb{N}$, on a*

$$\alpha^d(x_1 + \cdots + x_r) = \sum_{i_1 < \cdots < i_d} x_{i_1} \cdots x_{i_d}.$$

En particulier, si $r < d$ alors $\alpha^d(x_1 + \cdots + x_r) = 0$.

Démonstration. De façon générale, on voit par récurrence que quels que soient $x_1, \dots, x_r$ on a

$$\alpha^d(x_1 + \cdots + x_r) = \sum_{k_1 + \cdots + k_r = d} \alpha^{k_1}(x_1) \cdots \alpha^{k_r}(x_r).$$

On spécialise alors au cas où les x_i sont de α-dimension 1, et donc il ne reste que les $k_i = 0$ ou 1. □

Semi-anneaux et graduations

On aura besoin dans le chapitre suivant de travailler avec des semi-anneaux, et en particulier des semi-anneaux gradués. On consacre donc cette courte partie à généraliser les définitions précédentes à ce cadre, qui ne servira pas dans la suite de ce chapitre.

Soit S un semi-anneau commutatif, et soit Γ un groupe commutatif, noté additivement. Une Γ-graduation sur S est une décomposition $S = \bigoplus_{g \in \Gamma} S_g$ en tant que monoïde additif telle que $S_g S_h \subset S_{g+h}$. Notamment, tout semi-anneau commutatif peut tautologiquement être vu comme gradué sur le groupe trivial.

Lemme 1.1.24. *Soit R le groupe de Grothendieck de S, muni de sa structure naturelle d'anneau commutatif. Alors toute Γ-graduation de S s'étend de façon unique à R.*

Démonstration. Si R_g est le groupe de Grothendieck de S_g, alors la propriété universelle montre que $R = \bigoplus_{g \in G} R_g$, et aussi que $R_g R_h \subset R_{g+h}$. □

Si S est Γ-gradué, on définit une opération grecque homogène sur S comme un morphisme de monoïdes $\alpha_t : S \longrightarrow G(S)$ tel que $\alpha^d(S_g) \subset S_{dg}$.

Lemme 1.1.25. *Soit S un semi-anneau commutatif Γ-gradué, et soit R son anneau de Grothendieck. Alors toute opération grecque homogène sur S s'étend de façon unique en une opération grecque homogène sur R.*

Démonstration. On dispose d'un morphisme naturel de monoïdes $G(S) \to G(R)$, ce qui induit $\alpha_t : S \to G(R)$ par composition, et par propriété universelle on a une unique extension $R \to G(R)$ en un morphisme de groupes. Comme R_g est engendré par S_g, on voit facilement que $\alpha^d(R_g) \subset R_{dg}$. □

Si un anneau gradué R est muni d'une opération grecque homogène, alors sa lettre grecque est dans $L(R_0)$. De plus, si R est un anneau grec, et si $\alpha, \beta \in L(R_0)$, alors α_t est homogène si et seulement si β_t l'est. On peut donc adapter les constructions précédentes au cas gradué en définissant un anneau grec gradué comme un anneau gradué muni d'une structure d'anneau grec telle que les opérations dont la lettre grecque est dans $L(R_0)$ soient homogènes. Le cas non gradué se retrouve directement en prenant la graduation triviale.

On définit un morphisme d'anneaux grecs Γ-gradués comme un morphisme d'anneau grecs qui est un morphisme homogène, ce qui définit clairement une catégorie des anneaux grecs Γ-gradués.

Exemple 1.1.26. Si on pose $GW^{\pm}(K) = GW(K) \oplus GW^{-}(K)$, alors c'est un anneau grec $\mathbb{Z}/2\mathbb{Z}$-gradué.

Exemple 1.1.27. Si R est un anneau grec et A un groupe commutatif, alors l'anneau de groupe $R[A]$ est naturellement un anneau grec A-gradué, en posant pour tout $\alpha \in L(R)$ $\alpha^d(xa) = \alpha^d(x)(da)$ si $x \in R$ et $a \in A$.

Exemple 1.1.28. De façon plus précise, si R est un anneau grec B-gradué, alors $R[A]$ est un anneau grec $A \times B$-gradué. Notamment, $GW^{\pm}(K)[\mathbb{Z}/2\mathbb{Z}]$ est naturellement un anneau grec gradué sur le groupe de Klein.

1.1.2 λ-anneaux

La plupart des anneaux grecs que l'on rencontre « dans la nature » (et en particulier $GW(K)$) satisfont des propriétés supplémentaires, qui cette fois s'expriment spécifiquement en fonction des opérations λ.

Proposition 1.1.29. *Le groupe abélien $(G(R), +_G)$ (où $+_G$ est le produit des séries formelles) est muni d'un unique produit $\times_G$ naturel en R tel que $(G(R), +_G, \times_G)$ soit un anneau commutatif, et tel que pour tout $f(t) \in G(R)$ et tout $a \in R$, on ait*

$$f(t) \times_G (1 + at) = f(at).$$

Démonstration. Pour montrer l'unicité, il suffit par naturalité de montrer que pour $R = \mathbb{Z}[\sigma_1, \sigma_2, \dots ; s_1, s_2, \dots]$ (où les σ_i, s_i sont des indéterminées) le produit $f(t) \times_G g(t)$ est uniquement déterminé, avec $f(t) = 1 + \sum_i \sigma_i t^i$ et $g(t) = 1 + \sum_i s_i t^i$.

Pour cela, il suffit de montrer que $p_n(f(t) \times_G g(t))$ est uniquement déterminé pour tout n, où $p_n : R \to R_n = \mathbb{Z}[\sigma_1, \dots, \sigma_n; s_1, \dots, s_n]$ est la projection naturelle. Par naturalité, $p_n(f(t) \times_G g(t))$ est

$$(1 + \sum_{i=1}^{n} \sigma_i t^i) \times_G (1 + \sum_{i=1}^{n} s_i t^i) \in R_n.$$

Or on sait qu'on a une inclusion $R_n \subset \mathbb{Z}[x_1, \ldots, x_n; y_1, \ldots, y_n]$ de sorte que σ_i soit la i-ème fonction symétrique sur les x_i, et s_i celle sur les y_i. On a alors

$$1 + \sum_{i=1}^{n} \sigma_i t^i = \prod_{i=1}^{n} (1 + x_i t)$$

et de même pour les s_i, d'où, en se souvenant que le produit des polynômes est la somme $+_G$ dans $G(R_n)$ et que donc $\times_G$ est distributif sur cette opération :

$$(1 + \sum_{i=1}^{n} \sigma_i t^i) \times_G (1 + \sum_{i=1}^{n} s_i t^i) = \prod_{i,j} (1 + x_i t) \times_G (1 + y_j t) = \prod_{i,j} (1 + x_i y_j t).$$

Pour l'existence, il faut vérifier que cela définit bien un produit associatif naturel sur $G(R)$, voir [35, thm 2.5]. □

Proposition 1.1.30. *L'anneau $G(R)$ est muni d'une unique structure d'anneau grec naturelle en R telle que pour tout $a \in R$ l'élément $1 + at$ soit de λ-dimension 1.*

Démonstration. Comme pour la proposition précédente, on se ramène à montrer que les $\lambda^d(1 + \sum_{i=1}^n \sigma_i t^i)$ sont uniquement déterminés, et comme $1 + \sum_{i=1}^n \sigma_i t^i = (1 + x_1 t) +_G \cdots +_G (1 + x_n t)$, on a

$$\lambda^d(1 + \sum_{i=1}^{n} \sigma_i t^i) = \prod_{i_1 < \cdots < i_d} (1 + x_{i_1} \cdots x_{i_d} t).$$

Le fait que cela définisse bien une structure d'anneau grec est encore montré dans [35, thm 2.6]. □

Définition 1.1.31. Soit R un anneau grec. On dit que R est un λ-anneau si $\lambda_t : R \longrightarrow G(R)$ est un morphisme d'anneaux grecs.

Remarque 1.1.32. Cela correspond bien à la définition usuelle : on requiert que $\lambda_t(xy) = \lambda_t(x) \times_G \lambda_t(y)$ et $\lambda_t(\lambda^d(x)) = \lambda^d(\lambda_t(x))$, ce qui donne les formules usuelles pour $\lambda^d(xy)$ et $\lambda^n(\lambda^m(x))$ étant donné la structure d'anneau grec $G(R)$.

Exemple 1.1.33. Les anneaux $\mathbb{Z}$ et $GW(K)$ sont des λ-anneaux. De façon plus générale, pour une large classe de catégories abéliennes monoïdales symétriques $\mathbf{C}$, l'anneau de Grothendieck $K(\mathbf{C})$ est un λ-anneau ($\mathbb{Z}$ correspondant par exemple à une catégorie d'espaces vectoriels, et $GW(K)$ à la catégorie des espaces bilinéaires symétriques non dégénérés sur K).

Exemple 1.1.34. L'anneau $\mathbb{Z}[x_1, x_2, \ldots]$ admet une unique structure de λ-anneau telle que $\lambda^d(x_1) = x_d$. Cette structure fait de cet anneau le λ-anneau libre sur un élément (voir [35, thm 2.25]).

De même, on peut construire le λ-anneau libre sur n éléments en prenant n jeux de variables indépendantes.

1.1.3 Éléments de Pfister

Notre but est de montrer que les n-formes de Pfister sont de π_n-dimension 1 dans $GW(K)$ pour une certaine lettre grecque π_n (indépendante de K). On va aboutir à ce résultat en abstrayant la notion de n-forme de Pfister à un anneau grec quelconque, à partir de na notion de 1-forme de Pfister.

Définition 1.1.35. Soient R un anneau grec, $\alpha \in L(R)$ et $x \in R$. On dit que x est un α-élément de Pfister si $x^2 = 2x$ et pour tout $d \in \mathbb{N}^*$, $\alpha^d(x) = x$.

Si $\alpha = \lambda$, on parlera simplement d'élément de Pfister.

Un n-élément de Pfister est le produit de n élements de Pfister (en particulier 1 est l'unique 0-élément de Pfister, et un 1-élément de Pfister est simplement un élément de Pfister). On note $\mathrm{Pf}_n(R)$ l'ensemble des n-éléments de Pfister de R ; Pf_n est un foncteur des anneaux grecs dans les ensembles.

Remarque 1.1.36. En utilisant la proposition 1.1.21, on voit que les éléments de R qui sont des α-éléments de Pfister pour un certain α sont exactement ceux qui vérifient $x^2 = 2x$ et sont de β-dimension 1 pour un certain β.

On peut préciser ça dans le cas $\alpha = \lambda$:

Proposition 1.1.37. *Soit R un anneau grec. Les éléments de Pfister de R sont exactement les $x \in R$ vérifiant $x^2 = 2x$ et de π-dimension au plus 1, où $\pi = \sum(-1)^{d+1}t^d$.*

De plus, ce sont exactement les éléments de la forme $1 - a$ où a est de λ-dimension 1 et vérifie $a^2 = 1$.

Démonstration. Les éléments de Pfister sont ceux qui vérifient $x^2 = 2x$ et $\lambda_t(x) = 1+x\tau(t)$ où $\tau(t) = \sum_{d\geqslant 1} t^d$. Cette dernière condition est équivalente à $\pi_t(x) = 1+xt$ si $\pi = \tau^{-1}$. Or $\tau = \frac{t}{1-t}$, donc il est facile de voir que sa réciproque est $\pi = \frac{t}{1+t}$, comme annoncé.

Soit $x \in R$, et $a = 1-x$. Alors $x^2 = 2x$ est équivalent à $a^2 = 1$. Comme λ_t est un morphisme de groupe, $\lambda_t(a) = \frac{\lambda_t(1)}{\lambda_t(x)} = \frac{1+t}{\lambda_t(x)}$ donc le fait que a soit de λ-dimension 1 est équivalent à $\lambda_t(x) = \frac{1+t}{1+at}$ et comme $a^2 = 1$ cela donne $\lambda_t(x) = 1+\sum_{d\geqslant 1}(1-a)t^d$, donc à $\lambda^d(x) = x$ pour tout $d \geqslant 1$. □

Exemple 1.1.38. Soit $\varphi \in I(K)$ la classe de Witt d'une n-forme de Pfister, et soit $x \in \hat{I}(K)$ son unique relevé. Alors x est un n-élément de Pfister dans $GW(K)$ (et ce sont en fait les seuls). C'est ce qui explique qu'on choisisse comme convention dans cette thèse d'appeler « forme de Pfister » les éléments de cette forme plutôt que la classe dans $GW(K)$ d'une forme de Pister au sens usuel.

Exemple 1.1.39. Le foncteur Pf est représentable si on le restreint aux λ-anneaux : si on considère $U = \mathbb{Z}[x_1, x_2, \dots]$ le λ-anneau libre sur un élément (voir exemple 1.1.34), on peut construire P comme le quotient de U par l'idéal grec engendré par $x_1^2 - 2x_1$ et $x_d - x_1$ (pour $d \geqslant 2$). Alors l'image de x_1 dans P est l'élément de Pfister universel.

On peut préciser la structure de P : si on considère P' le quotient de U par l'idéal engendré par $x_1^2 - 2x_1$ et $x_d - x_1$, alors P est en tant qu'anneau un quotient de P'. Or $P' = \mathbb{Z} \oplus \mathbb{Z}x_1$, donc si P n'est pas isomorphe à P' on doit avoir $a, b \in \mathbb{Z}$ tels que pour tout élément de Pfister x dans un λ-anneau on ait $ax = b$; mais l'exemple des formes de Pfister dans un $GW(K)$ nous permet de voir que c'est faux. Donc $P = \mathbb{Z} \oplus \mathbb{Z}x_1$.

Exemple 1.1.40. De même, le foncteur Pf^n est représentable sur les λ-anneaux, et l'anneau P_n qui le représente est isomorphe à $(\mathbb{Z} \oplus \mathbb{Z}x)^{\otimes n}$.

Cela signifie que tout n-élément de Pfister dans un λ-anneau est l'image d'un élément de cet anneau par un certain morphisme, mais qui n'est pas unique, donc on ne peut pas en conclure que Pf_n est représentable. On peut parler d'un n-élément de Pfister *versel*.

Pour généraliser la proposition 1.1.37 aux n-éléments de Pfister, on va se restreindre aux λ-anneaux.

Théorème 1.1.41. *Soit $n \in \mathbb{N}^*$. Il existe une unique lettre grecque $\pi_n \in L(\mathbb{Z})$ telle que pour tout λ-anneau R, tout n-élément de Pfister de R est de π_n-dimension 1.*

Précisément :

$$\pi_n = 1 - \frac{2}{1 + (1 + 2^n t)^{\frac{1}{2^{n-1}}}},$$

soit :

$$\pi_{n+1} = \pi_n \circ (tC(-2^{n-1}t)), \quad \pi_n = \pi_{n+1} \circ (t + 2^{n-1}t^2)$$

où $C(t)$ est la série génératrice des nombres de Catalan, soit $C(t) = \frac{1-\sqrt{1-4t}}{2t}$.

Démonstration. On vérifie que si π_n est donné par la formule ci-dessus, alors

$$\pi_n^{-1} = \frac{1}{2^n}\left[\left(\frac{1+t}{1-t}\right)^{2^{n-1}} - 1\right].$$

On doit donc montrer que si φ est un n-élément de Pfister alors $\lambda_t(\varphi) = 1 + \varphi\pi_n^{-1}(t)$ avec π_n^{-1} donné ci-dessus.

On procède par récurrence sur n. Pour $n = 1$, il s'agit juste de la proposition 1.1.37. On suppose que la propriété est vraie jusqu'à $n \geqslant 1$. D'après l'exemple 1.1.40, on peut se ramener au cas d'un n-élément de Pfister versel dans l'anneau P_n, qui a la particularité d'être sans torsion. En particulier, P_n se plonge dans $R = P_n \otimes_{\mathbb{Z}} \mathbb{Q}$, et d'après [35, prop 3.50], on peut étendre la structure de λ-anneau de P_n à R ; on s'est donc ramené au cas d'un n-élément de Pfister dans un anneau où 2 est inversible.

On peut alors facilement observer par définition d'un élément de Pfister que pour tout n-élément de Pfister x, $(\frac{x}{2^n})^i = \frac{x}{2^n}$, donc pour tout $f \in tR[[t]]$,

$$\frac{x}{2^n} f(t) = f(\frac{x}{2^n} t). \tag{1.1.42}$$

En particulier, si x est un 1-élément de Pfister, on a

$$\lambda_t(x) = 1 + x\pi_1^{-1}(t) = 1 + 2\pi_1^{-1}(\frac{xt}{2}) = \frac{1 + \frac{xt}{2}}{1 - \frac{xt}{2}}.$$

De là, soit $\varphi \in \mathrm{Pf}_{n+1}(R)$, avec $\varphi = xy$ où $x \in \mathrm{Pf}_1(R)$ et $y \in \mathrm{Pf}_n(R)$. Alors :

$$\begin{aligned}
\lambda_t(\varphi) &= \lambda_t(xy) \\
&= \lambda_t(x) \times_G \lambda_t(y) \\
&= \left[(1 + \frac{x}{2}t) -_G (1 - \frac{x}{2}t)\right] \times_G (1 + y\pi_n^{-1}(t)) \\
&= (1 + y\pi_n^{-1}(\frac{xt}{2})) -_G (1 + y\pi_n^{-1}(-\frac{xt}{2})) \\
&= \frac{1 + 2^n\pi_n^{-1}(\frac{\varphi t}{2^{n+1}})}{1 + 2^n\pi_n^{-1}(-\frac{\varphi t}{2^{n+1}})} \\
&= 1 + \frac{\varphi}{2^{n+1}} \left(\frac{1 + 2^n\pi_n^{-1}(t)}{1 + 2^n\pi_n^{-1}(-t)} - 1 \right)
\end{aligned}$$

où la dernière égalité vient de (1.1.42) appliqué à $f = \frac{1+2^n\pi_n^{-1}(t)}{1+2^n\pi_n^{-1}(-t)} - 1$. Or

$$\begin{aligned}
\frac{1 + 2^n\pi_n^{-1}(t)}{1 + 2^n\pi_n^{-1}(-t)} &= \frac{\left(\frac{1+t}{1-t}\right)^{2^{n-1}}}{\left(\frac{1-t}{1+t}\right)^{2^{n-1}}} \\
&= \left(\frac{1+t}{1-t}\right)^{2^n}
\end{aligned}$$

donc on trouve bien $\lambda_t(\varphi) = 1 + \varphi\pi_{n+1}^{-1}(t)$.

Il faut ensuite vérifier que les formules de récurrence donnent bien la bonne formule pour π_n. Tout d'abord, on montre facilement que $tC(-2^{n-1}t)$ et $t + 2^{n-1}t^2$ sont réciproques l'une de l'autre, puis :

$$\begin{aligned}
\pi_{n+1} \circ (t + 2^{n-1}t^2) &= 1 - \frac{2}{1 + (1 + 2^{n+1}(t + 2^{n-1}t^2))^{\frac{1}{2^n}}} \\
&= 1 - \frac{2}{1 + ((1 + 2^n t)^2)^{\frac{1}{2^n}}} \\
&= \pi_n.
\end{aligned}$$

$\square$

Corollaire 1.1.43. *On a les relations explicites :*

$$\pi_1^d = \sum_{k=1}^{d} (-1)^{d-k} \binom{d-1}{k-1} \lambda^k$$

$$\pi_{n+1}^d = \sum_{k=1}^{d} (-1)^{d-k} 2^{(d-k)(n-1)} \frac{k}{d} \binom{2d-k-1}{d-1} \pi_n^k$$

$$\pi_n^d = \sum_{\frac{d}{2} \leqslant k \leqslant d} \binom{k}{d-k} 2^{(d-k)(n-1)} \pi_{n+1}^k.$$

Démonstration. Par construction, si $\alpha = \beta \circ \tau$, alors si $\tau^k = \sum_d a_{k,d} t^d$, on a $\alpha^d = \sum_k a_{k,d} \beta^k$.

Les équations ci-dessus se traduisent donc par

$$\left(\frac{t}{1+t}\right)^k = \sum_{d \geqslant k} (-1)^{d-k} \binom{d-1}{k-1} t^d,$$

$$\big(tC(-2^{n-1}t)\big)^k = \sum_{d \geqslant k} (-1)^{d-k} 2^{(d-k)(n-1)} \frac{k}{d} \binom{2d-k-1}{d-1} t^d,$$

et

$$(t + 2^{n-1}t^2)^k = \sum_{k \leqslant d \leqslant 2k} \binom{k}{d-k} 2^{(d-k)(n-1)} t^d.$$

La première vient directement du développement en série de $(1+t)^{-n}$ et la troisième du binôme de Newton. On peut se concentrer sur la deuxième, qui se réécrit

$$C(t)^k = \sum_{d \geqslant 0} \frac{k}{d+k} \binom{2d+k-1}{d+k-1} t^d.$$

On la montre sans difficulté par récurrence en utilisant l'équation fonctionnelle $C(t) = 1 + tC(t)^2$, qui donne $C(t)^{k+1} = \frac{C(t)^k - C(t)^{k-1}}{t}$. □

Corollaire 1.1.44. *Soit R un λ-anneau. Soient $x \in \mathrm{Pf}_n(R)$ et $a \in R$ de λ-dimension 1 tel que $a^2 = 1$. Alors si $d \geqslant 2$:*

$$\pi_n^d(ax) = (-1)^d 2^{n(d-1)-1}(1-a)x.$$

Démonstration. On a $\lambda_t(ax) = (1+at) \times_G \lambda_t(x) = 1 + x\pi_n^{-1}(at)$, donc en faisant agir π_n à gauche $(\pi_n)_t(ax) = 1 + x\pi_n^{-1}(a\pi_n(t))$. On doit donc montrer

$$\pi_n^{-1}(a\pi_n(t)) = at + \sum_{d \geqslant 2} (-1)^d 2^{n(d-1)-1}(1-a)t^d.$$

On montre en utilisant $(1-a)^m = 2^{m-1}(1-a)$ et $a(1-a)^n = -(1-a)^n$ que le membre de droite donne $\frac{at}{1+2^{n-1}(1-a)t}$.

Pour le membre de gauche : on a

$$\begin{aligned}
\frac{1+a\pi_n(t)}{1-a\pi_n(t)} &= \frac{1+a\frac{(1+2^nt)^{\frac{1}{2^{n-1}}}-1}{(1+2^nt)^{\frac{1}{2^{n-1}}}+1}}{1-a\frac{(1+2^nt)^{\frac{1}{2^{n-1}}}-1}{(1+2^nt)^{\frac{1}{2^{n-1}}}+1}} \\
&= \frac{(1+2^nt)^{\frac{1}{2^{n-1}}}(1+a)+(1-a)}{(1+2^nt)^{\frac{1}{2^{n-1}}}(1-a)+(1+a)}.
\end{aligned}$$

Or comme $(1+a)(1-a)=0$, on a $(y(1+a)+(1-a))^m = 2^{m-1}(y^m(1+a)+(1-a))$ pour tous $y \in R$ et $m \in \mathbb{N}^*$, et de même en échangeant les $1+a$ et $1-a$. De là :

$$\begin{aligned}
\pi_n^{-1}(a\pi_n(t)) &= \frac{1}{2^n}\left(\frac{(1+2^nt)(1+a)+(1-a)}{(1+2^nt)(1-a)+(1+a)} - 1\right) \\
&= \frac{1}{2^n}\left(\frac{2+2^n(1+a)t}{2+2^n(1-a)t} - 1\right) \\
&= \frac{at}{1+2^{n-1}(1-a)t}
\end{aligned}$$

comme souhaité. □

1.2 Invariants de I^n

Dans cette partie on étudie les invariants de I^n à valeurs dans l'anneau de Witt $W(K)$ (invariants de Witt), et dans $H^*(K,\mu_2)$ (invariants cohomologiques).

Il s'avère que les résultats sont extrêmement proches dans les deux cas, mais qu'il est délicat de passer de l'un à l'autre directement. On choisit donc d'opter pour une approche hybride, qui englobe les deux types d'invariants, en étudiant des invariants à valeurs dans un anneau $A(K)$ qui vérifie un certain nombre de propriétés formelles qui sont exactement celles qui font fonctionner les résultats. La généralisation est un peu artificielle dans la mesure où il n'est pas évident que des exemples intéressants autres que l'anneau de Witt et l'anneau de cohomologie soient couvert par ces définitions, mais l'artifice a le mérite d'une certaine simplicité et lisibilité, et évite à tout le moins de répéter des arguments presque identiques pour les deux cas qui nous intéressent.

1.2.1 Contexte

On se fixe donc dans cette toute partie un foncteur $A : \mathbf{Field}_{/k} \longrightarrow \mathbf{FRing}$, où $\mathbf{FRing}$ est la catégorie des anneaux filtrés. On a donc une filtration $A(K) =$

$A^0(K) \supset A^1(K) \supset \ldots$, naturelle en K, qu'on suppose par ailleurs séparée, ie $\bigcap_n A^n(K) = 0$.

On suppose également qu'on dispose d'une application naturelle $f_1 : I^1(K) \longrightarrow A^1(K)$ vérifiant les conditions suivantes :

(i) l'association

$$\langle\langle a_1, \ldots, a_n\rangle\rangle \mapsto \{a_1, \ldots, a_n\} := f_1(\langle\langle a_1\rangle\rangle) \cdots f_1(\langle\langle a_n\rangle\rangle)$$

définit une fonction injective $\mathrm{Pf}_n(K) \longrightarrow A^n(K)$;

(ii) pour tout $n \in \mathbb{N}^*$, cette fonction se prolonge en un morphisme de groupes $f_n : I^n(K) \longrightarrow A^n(K)$;

(iii) si $x \in A(K)$ vérifie $\{a\} \cdot x \in A^{d+1}(L)$ pour tout $a \in L^*$, pour toute extension L/K, alors $x \in A^d(K)$;

(iv) $\mathrm{Inv}(\mathrm{Pf}_n, A) = A(K) \oplus A(K) \cdot f_n$ où on considère les invariants définis sur K.

Notons que la condition (iii) est équivalente à :

$$\forall n \in \mathbb{N}^*, \ \big(\forall L/K, \forall \varphi \in \mathrm{Pf}_n(K), f_n(\varphi) \cdot x \in A^{d+n}(L)\big) \Longrightarrow x \in A^d(K) \qquad (1.2.1)$$

et en particulier par séparation implique

$$\forall n \in \mathbb{N}^*, \ (\forall L/K, \forall \varphi \in \mathrm{Pf}_n(K), f_n(\varphi) \cdot x = 0) \Longrightarrow x = 0. \qquad (1.2.2)$$

On peut également remarquer que par construction, pour tous $x \in I^n(K)$, $y \in I^m(K)$, on a :

$$f_n(x) \cdot f_m(y) = f_{n+m}(xy) \qquad (1.2.3)$$

Exemple 1.2.4. Le premier exemple, tautologique, est $A(K) = W(K)$ (on notera $A = W$), muni de la filtration fondamentale $A^n(K) = I^n(K)$, et de $f_1 = \mathrm{Id}$ (donc $f_n = \mathrm{Id}$). Les deux premières propriétés sont évidentes, la troisième se montre en prenant pour a un élément générique, et la quatrième est un résultat de Serre ([10, ex 27.17]). Dans cet exemple, $\{a_1, \ldots, a_n\} = \langle\langle a_1, \ldots, a_n\rangle\rangle$.

Exemple 1.2.5. Le deuxième exemple est $A(K) = H^*(K, \mu_2)$ (on notera $A = H$), muni de la filtration $A^n(K) = \bigoplus_{d \geqslant n} H^n(K, \mu_2)$, et de $f_1 = e_1$ (et donc $f_n = e_n$). Les deux premières propriétés découlent de la conjecture de Milnor, la troisième se démontre encore en prenant un élément générique, et la quatrième est encore un résultat de Serre ([10, thm 18.1]). Dans cet exemple, $\{a_1, \ldots, a_n\} = (a_1, \ldots, a_n)$.

Remarque 1.2.6. En revanche, $A(K) = GW(K)$ ne convient pas : la condition (iii) n'est pas remplie. En effet, si $x \in GW(K)$ vérifie $x\langle\langle a\rangle\rangle = 0$ pour tout $a \in L^*$, on peut seulement conclure que x est hyperbolique, et non $x = 0$, ce qui est en contradiction avec (1.2.2).

1.2.2 Les invariants f_n^d

On met en application le théorème 1.1.41, dans le cas du λ-anneau $GW(K)$. On dispose donc pour tous $n \in \mathbb{N}^*$ et $d \in \mathbb{N}$ d'applications $\pi_n^d : GW(K) \longrightarrow GW(K)$, naturelles en K.

Définition 1.2.7. Pour tous $n, d \in \mathbb{N}^*$, on définit $f_n^d \in \mathrm{Inv}^{nd}(I^n, A)$ par $f_n^d = f_{nd} \circ \pi_n^d$. On pose aussi $f_n^0 = 1$.

Exemple 1.2.8. Si $A(K) = W(K)$, alors $f_n^d = \pi_n^d$ (restreint à $I^n(K)$). Si $A(K) = H^*(K, \mu_2)$, alors on notera $u_{nd}^{(n)} = f_n^d = e_{nd} \circ \pi_n^d$.

En ce qui concerne la notation, on aurait pu choisir d'utiliser u_n^d pour être plus cohérent avec les autres notations, mais on a choisi de suivre la tradition de noter le degré d'un invariant cohomologique en indice. L'exposant sert alors à distinguer les invariants de même degré, par exemple $u_6^{(2)}$ et $u_6^{(3)}$, définis respectivement sur I^2 et I^3 (et dont l'un n'est absolument pas la restriction de l'autre, par ailleurs).

Les propriétés de base de ces invariants sont les suivantes :

Proposition 1.2.9. *Pour tout $n \in \mathbb{N}^*$, on a :*

(i) $f_n^0 = 1$ et $f_n^1 = f_n$;

(ii) pour tous $q, q' \in I^n(K)$:

$$f_n^d(q + q') = \sum_{k=0}^{d} f_n^k(q) \cdot f_n^{d-k}(q');$$

(iii) pour tous $\varphi \in Pf_n(K)$ et $d \geqslant 2$, $f_n^d(\varphi) = 0$.

En particulier, $f_n^d(I^n(K)) \subset A^{nd}(K)$.

Démonstration. Les trois propriétés sont une reformulation du fait que π_n est une opération grecque telle que les n-formes de Pfister sont de dimension 1 (voir 1.1.41), en utilisant la formule (1.2.3).

Pour la dernière assertion, par la formule (ii), il suffit de montrer que $f_n^d(x) \in A^{nd}(K)$ si x est une n-forme de Pfister ou l'opposé d'une telle forme. Or pour une forme de Pfister cela découle directement des formules ci-dessus, et pour l'opposé d'une n-forme de Pfister on peut utiliser le corollaire 1.1.44 avec $a = -1$. □

Proposition 1.2.10. *Si $\varphi \in Pf_n(K)$, $a \in K^*$, $d \geqslant 2$, alors*

$$f_n^d(\langle a\rangle\varphi) = (-1)^d\{-1\}^{n(d-1)-1}\{a\}f_n(\varphi).$$

Démonstration. C'est une application directe du corollaire 1.1.44. □

Proposition 1.2.11. *Si $q = \sum_{i=1}^r \varphi_i \in I^n(K)$ où φ_i est une n-forme de Pfister, alors pour tout $d \geqslant 1$:*

$$f_n^d(q) = \sum_{1 \leqslant i_1 < \cdots < i_d \leqslant r} f_n(\varphi_{i_1}) \cdots f_n(\varphi_{i_d}),$$

et en particulier $f_n^d(q) = 0$ si q est une somme de k n-formes de Pfister avec $k < d$.

Démonstration. C'est une conséquence directe de la proposition 1.1.23. □

Corollaire 1.2.12. *Si -1 est un carré dans K, alors pour tout $q \in I^n(K)$, $f_n^d(q) = 0$ pour d assez grand.*

Démonstration. Quand -1 est un carré, tout $q \in I^n$ est une somme de n-formes de Pfister, donc ça découle de la proposition. □

Remarque 1.2.13. On peut montrer que, pour K/k fixé, (f_n^d) est la seule famille d'applications $I^n(K) \longrightarrow A(K)$ à vérifier les conditions de la proposition 1.2.9. En effet, toute famille (a_n^d) qui vérifie (i) et (ii) doit satisfaire les conclusions de la proposition 1.2.11, donc ses valeurs sont fixées sur les sommes de formes de Pfister. En développant $a_n^d(q - q)$ pour un tel q avec (ii) on trouve par récurrence que $a_n^d(-q)$ est aussi déterminé, et donc par somme les valeurs sont déterminées sur un élément quelconque.

On présente une application de la proposition 1.2.11, qui utilise le cas $A(K) = W(K)$:

Proposition 1.2.14. *Si toute forme dans $I^n(K)$ peut s'écrire comme somme d'au plus r n-formes de Pfister pour un certain $r \in \mathbb{N}^*$, alors $I^d(K) = 0$ pour tout $d \geqslant n(r+1)$.*

Démonstration. Tout d'abord il suffit de montrer que $I^{n(r+1)}(K) = 0$, puisque de façon générale si $I^d(K) = 0$ alors $I^{d+1}(K) = 0$.

Il suffit donc de montrer que toute $n(r+1)$-forme de Pfister est nulle. Or une telle forme s'écrit $\varphi = \varphi_1 \cdots \varphi_{r+1}$ où les φ_i sont des n-formes de Pfister.

De là, $\varphi = \pi_n^{r+1}(q)$ avec $q = \varphi_1 + \cdots + \varphi_{r+1}$. Or par hypothèse q peut s'écrire comme une somme d'au plus r n-formes de Pfister, donc d'après la proposition 1.2.11 $\pi_n^{r+1}(q) = 0$. □

Remarque 1.2.15. Cette proposition peut être démontrée indépendamment en utilisant le Hauptsatz de Pfister.

1.2.3 L'opérateur de décalage

Pour alléger les notations, on se fixe un $n \in \mathbb{N}^*$, et on pose $M = \mathrm{Inv}(I^n, A)$ ainsi que $M^d = \mathrm{Inv}(I^n, A^d)$.

Proposition-définition 1.2.16. *Soit $\varepsilon = \pm 1$. Il existe un unique morphisme de $A(k)$-modules filtrés, de degré $-n$,*

$$\begin{array}{rccc} \Phi^\varepsilon : & M & \longrightarrow & M \\ & \alpha & \longmapsto & \alpha^\varepsilon, \end{array}$$

tel que

$$\alpha(q + \varepsilon\varphi) = \alpha(q) + \varepsilon f_n(\varphi) \cdot \alpha^\varepsilon(q) \tag{1.2.17}$$

pour tous $\alpha \in M$, $q \in I^n(K)$ et $\varphi \in \mathrm{Pf}_n(K)$.

Démonstration. Soient $\alpha \in M$ et $q \in I^n(K)$. Pour toute extension L/K et tout $\varphi \in \mathrm{Pf}_n(L)$, on pose

$$\beta_q(\varphi) = \alpha(q + \varepsilon\varphi).$$

Alors $\beta_q \in \mathrm{Inv}(\mathrm{Pf}_n, A)$, défini sur K. D'après la condition (iv) sur A, il existe d'uniques $x_q, y_q \in A(K)$ tels que $\beta_q = x_q + y_q \cdot f_n$.

En prenant $\varphi = 0$ on voit que $x_q = \alpha(q)$, et on pose alors $\alpha^\varepsilon(q) = \varepsilon y_q$, ce qui nous donne bien la formule voulue, ainsi que l'unicité.

Ainsi défini, Φ^ε est clairement un morphisme de $A(k)$-modules, et il est bien de degré $-n$ car si $\alpha \in M^d$, alors pour tout $q \in I^n(K)$, $f_n(\varphi) \cdot \alpha^\varepsilon(q) \in A^d(L)$ pour tout $\varphi \in Pf_n(L)$ et toute extension L/K, donc $\alpha^\varepsilon(q) \in A^{d-n}(K)$ par la condition (iii) sur A. □

Remarque 1.2.18. Les opérateurs Φ^ε dépendent de n, mais on le passe sous silence dans la notation, aucune confusion n'étant susceptible d'advenir.

On a des liens naturels entre Φ^+ et Φ^-, traduisant le fait que l'addition et la soustraction commutent, et qu'elles sont inverses l'une de l'autre :

Proposition 1.2.19. *Les opérateurs Φ^+ et Φ^- commutent, et de plus pour tout $\alpha \in \hat{M}$ on a*

$$\alpha^+ - \alpha^- = \{-1\}^n \alpha^{+-} = \{-1\}^n \alpha^{-+}.$$

Démonstration. Soient $q \in I^n(K)$, et $\varphi, \psi \in \mathrm{Pf}_n(L)$. On a

$$\begin{aligned} \alpha(q + \varphi - \psi) &= \alpha(q + \varphi) - f_n(\psi)\alpha^-(q + \varphi) \\ &= \alpha(q) + f_n(\varphi)\alpha^+(q) - f_n(\psi)\alpha^-(q) - f_n(\varphi)f_n(\psi)\alpha^{-+}(q) \end{aligned}$$

mais aussi

$$\begin{aligned} \alpha(q + \varphi - \psi) &= \alpha(q - \psi) + f_n(\varphi)\alpha^+(q - \psi) \\ &= \alpha(q) - f_n(\psi)\alpha^-(q) + f_n(\varphi)\alpha^+(q) - f_n(\varphi)f_n(\psi)\alpha^{+-}(q) \end{aligned}$$

donc $f_n(\varphi)f_n(\psi)\alpha^{-+}(q) = f_n(\varphi)f_n(\psi)\alpha^{+-}(q)$, et comme c'est vrai pour tous φ, ψ sur toute extension, par la condition (1.2.2) on a $\alpha^{+-} = \alpha^{-+}$.

Si maintenant on prend $\varphi = \psi$, la formule ci-dessus donne

$$f_n(\varphi)\alpha^+(q) - f_n(\varphi)\alpha^-(q) = f_n(\varphi)f_n(\varphi)\alpha^{+-}(q)$$

ce qui permet de conclure en utilisant $f_n(\varphi)f_n(\varphi) = \{-1\}^n f_n(\varphi)$ et encore la condition (1.2.2). □

Comme les opérateurs commutent, pour tous $s, t \in \mathbb{N}$ et tout $\alpha \in M$ on définit

$$\alpha^{s+,t-} = (\Phi^+)^s \circ (\Phi^-)^t(\alpha), \tag{1.2.20}$$

qui ne dépend en réalité pas de l'ordre d'application des opérateurs.

On appelle $\Phi = \Phi^+$ l'*opérateur de décalage*, comme le justifie le résultat élémentaire suivant :

Proposition 1.2.21. *Pour tout $d \in \mathbb{N}$, $\Phi(f_n^{d+1}) = f_n^d$ (et $\Phi(f_n^0) = 0$).*

Démonstration. Il faut montrer que $f_n^{d+1}(q+\varphi) = f_n^{d+1}(q) + f_n(\varphi) \cdot f_n^d(q)$, ce qui est une conséquence immédiate de la proposition 1.2.9. □

L'action de Φ^- sur les f_n^d est plus compliquée, reflétant ainsi le fait que les f_n^d se comportent bien mieux vis-à-vis des sommes des formes de Pfister que des soustractions de telles formes.

Proposition 1.2.22. *Soit $d \in \mathbb{N}^*$. Alors*

$$(f_n^d)^- = \sum_{k=0}^{d-1} (-1)^{d-k-1}\{-1\}^{n(d-k-1)} f_n^k.$$

Démonstration. Soient $q \in I^n(K)$ et $\varphi \in \mathrm{Pf}_n(K)$. Alors

$$\begin{aligned} f_n^d(q-\varphi) &= \sum_{k=0}^{d} f_n^k(q) f_n^{d-k}(-\varphi) \\ &= f_n^d(q) + \sum_{k=0}^{d-1} (-1)^{d-k}\{-1\}^{n(d-k-1)} f_n(\varphi) f_n^k(q) \end{aligned}$$

en utilisant la proposition 1.2.10 avec $a = -1$. □

Outre son comportement vis-à-vis des invariants f_n^d, la principale propriété de Φ est la suivante :

Proposition 1.2.23. *Le morphisme Φ^ε induit un morphisme $M/M^{d+n} \to M/M^d$ pour tout $d \in \mathbb{N}$, qui donne la suite exacte suivante :*

$$0 \longrightarrow A(k)/A^{d+n}(k) \longrightarrow M/M^{d+n} \longrightarrow M/M^d.$$

En particulier, le noyau de Φ^ε est le sous-module des invariants constants.

Démonstration. Si $\alpha, \beta \in M$ sont congrus modulo M^{d+n}, alors comme

$$\Phi^\varepsilon(M^{d+n}) \subset M^d,$$

$\Phi^\varepsilon(\alpha)$ et $\Phi^\varepsilon(\beta)$ sont congrus modulo M^d, ce qui montre la première affirmation.

Soit $\alpha \in M$ tel que $\alpha^\varepsilon \in M^d$. Alors pour tout $q \in I^n(K)$ et tout $\varphi \in \mathrm{Pf}_n(K)$, on a $\alpha(q + \varepsilon\varphi) \equiv \alpha(q)$ modulo $A^{n+d}(K)$. Donc en écrivant $q = q_1 - q_2$ où les q_i sont des sommes de n-formes de Pfister, on voit par une simple récurrence sur le nombre de termes dans chaque somme que $\alpha \equiv \alpha(0)$ modulo M^{d+n} (où $\alpha(0)$ est vu comme invariant constant).

Pour la dernière assertion, en prenant d assez grand, et comme la filtration sur $A(K)$ est séparée, on voit que si $\alpha^\varepsilon = 0$ alors $\alpha = \alpha(0)$. □

Remarque 1.2.24. On peut montrer directement que $\mathrm{Ker}(\Phi) = A(k)$ avec le même schéma de preuve, mais la version filtrée, plus fine, nous sera utile dans la suite.

Corollaire 1.2.25. *Soit M' le sous-module de M engendré par les f_n^d pour $d \in \mathbb{N}$. Alors Φ^ε induit une suite exacte*

$$0 \to A(k) \longrightarrow M' \longrightarrow M'[-n] \longrightarrow 0.$$

Démonstration. Seule la surjectivité reste à montrer, mais on le déduit facilement des propositions 1.2.21 pour Φ^+, et 1.2.22 pour Φ^-. □

Remarque 1.2.26. Tout ceci implique que Φ peut être vu comme une sorte d'opérateur différentiel : si on connaît α^+ pour un certain invariant α, on peut « intégrer » pour trouver α, avec une certaine constante d'intégration. Précisément, on montrera dans la partie suivante qu'on peut toujours écrire $\alpha^+ = \sum a_d f_n^d$; alors $\alpha = \alpha(0) + \sum a_d f_n^{d+1}$.

On utilisera très souvent cette méthode pour calculer α par récurrence en passant par α^+, ce qu'on qualifiera de « récurrence sur le décalage ».

On peut tirer une conséquence élémentaire de ce qui précède :

Corollaire 1.2.27. *Soit $\alpha \in M$ additif (c'est-à-dire que $\alpha(q+q') = \alpha(q) + \alpha(q')$ pour tous q, q'). Alors $\alpha = af_n$ pour un unique $a \in A(k)$.*

Démonstration. Pour tous $q \in I^n(K)$, $\varphi \in \mathrm{Pf}_n(K)$, on a $\alpha(q + \varphi) = \alpha(q) + \alpha(\varphi)$ donc $\alpha(\varphi) = f_n(\varphi)\alpha^+(q)$. En particulier, $f_n(\varphi)\alpha^+(q) = f_n(\varphi)\alpha^+(q')$ pour tout q', et comme c'est vrai pour tout φ sur toute extension, α^+ est un invariant constant, disons $a \in A(k)$. Alors $\alpha^+ = (af_n)^+$, et comme par additivité $\alpha(0) = 0$, on a bien $\alpha = af_n$. Comme $a = \alpha^+(0)$, il est uniquement déterminé. □

1.2.4 Classification des invariants

On rappelle qu'on s'est donné $n \in \mathbb{N}^*$, et qu'on a posé $M = \mathrm{Inv}(I^n, A)$ et $M^d = \mathrm{Inv}(I^n, A^d)$.

On souhaite montrer que tout élément de M peut s'écrire de façon unique comme une combinaison $\sum a_d f_n^d$, ce qui est suggéré par :

Proposition 1.2.28. *Le $A(k)/A^d(k)$-module M/M^d est engendré par les f_n^k avec $nk < d$.*

Démonstration. On raisonne par récurrence sur d. Pour $d = 0$, c'est trivial puisque $M^0 = M$. Supposons que la propriété tienne jusqu'à $d-1$, et soit $\alpha \in M$; on note $\bar{\alpha} \in M/M^d$. Par hypothèse de récurrence, $\Phi(\bar{\alpha}) = \sum a_k f_n^k$ avec $nk < d - n$, donc si on pose $\beta = \alpha - \sum a_k f_n^{k+1}$ on a $\Phi(\bar{\beta}) = 0$. De là, d'après la proposition 1.2.23, β est congru modulo M^d à un invariant constant a_{-1}, d'où $\bar{\alpha} = \sum a_{k-1} f_n^k$ avec $nk < d$. □

Remarque 1.2.29. Cela montre au passage que la suite exacte de la proposition 1.2.23 peut être complétée à droite par un 0, puisque tous les f_n^d sont dans l'image des Φ^ε (même argument que pour le corollaire 1.2.25).

Le problème est que pour exprimer un invariant en fonction des f_n^d il est en général nécessaire d'utiliser une combinaison infinie, comme le souligne l'exemple suivant.

Exemple 1.2.30. On se place dans le cas $A = W$. Soit $\alpha(q) = \langle \mathrm{disc}(q) \rangle$; c'est un invariant de Witt de I. Alors $\alpha^+ = -\alpha$; en effet :

$$\langle \mathrm{disc}(q + \langle\langle a \rangle\rangle) \rangle = \langle \mathrm{disc}(q)a \rangle = \langle \mathrm{disc}(q) \rangle - \langle\langle a \rangle\rangle \langle \mathrm{disc}(q) \rangle.$$

De là, α ne peut s'écrire comme une combinaison finie des f_1^d, puisque la longueur d'une telle combinaison diminue strictement quand on applique Φ^+. En revanche, on peut imaginer écrire, au moins formellement pour l'instant (mais les résultats de cette partie permettent de montrer que c'est effectivement valide)

$$\alpha = \sum_{d \in \mathbb{N}} (-1)^d f_1^d.$$

Cependant, une telle combinaison infinie pourrait ne pas toujours être bien définie. Comme f_n^d est à valeur dans des rangs strictement croissants de la filtration de A, toute somme $\sum_{d \in \mathbb{N}} a_d f_n^d$ définit bien un invariant à valeurs dans la complétion de A, mais a priori pas dans A lui-même.

Exemple 1.2.31. Si k est formellement réel, alors $\sum_d f_1^d$ envoie $-\langle\langle -1 \rangle\rangle$ sur $\sum_{d \in \mathbb{N}} (-1)^d \{-1\}^d$, qui n'est pas un élément de $A(k)$ pour $A = W$ ou $A = H$.

Comme cet exemple le souligne, le problème est le mauvais comportement des f_n^d avec les opposés de formes de Pfister (en effet, toute somme $\sum_{d\in\mathbb{N}} a_d f_n^d$ est en revanche à valeur dans A si on la restreint aux *sommes* de formes de Pfiser). Pour obtenir une description satisfaisante de M, on va introduire une nouvelle famille, dont la définition équilibre les sommes et les différences de formes de Pfister, et on montrera que toute combinaison, même infinie, des éléments de cette famille est cette fois à valeur dans A.

Définition 1.2.32. Pour tout $d \in \mathbb{N}$, on définit $g_n^d \in \mathrm{Inv}(I^n, A^{nd})$ par :

- $g_n^0 = 1$;
- si $d \in \mathbb{N}$ est pair, $(g_n^{d+1})^- = g_n^d$ et $g_n^{d+1}(0) = 0$;
- si $d \in \mathbb{N}$ est impair, $(g_n^{d+1})^+ = g_n^d$ et $g_n^{d+1}(0) = 0$.

Le corollaire 1.2.25 montre que ces conditions définissent bien les g_n^d de façon unique. Notons par ailleurs que $g_n^1 = f_n$.

Remarque 1.2.33. On observe que si -1 est un carré dans k, alors $g_n^d = f_n^d$. C'est cohérent avec le fait que si -1 est un carré, tout élément de $I^n(K)$ est une somme de formes de Pfister, donc les problèmes soulevés précédemment n'apparaissent pas.

Exemple 1.2.34. Dans le cas où $A(K) = H^*(K, \mu_2)$, on notera $g_n^d = v_{nd}^{(n)}$ pour garder une cohérence avec notre façon de noter les invariants cohomologiques.

Cette définition, qui équilibre Φ et Φ^-, donne un comportement raisonnable pour les deux opérateurs à la fois :

Proposition 1.2.35. *Soit $d \in \mathbb{N}$. Alors :*

$$(g_n^{d+2})^{+-} = (g_n^{d+2})^{-+} = g_n^d;$$

$$(g_n^{d+1})^+ = \begin{cases} g_n^d & \textit{si } d \textit{ impair} \\ g_n^d + \{-1\}^n g_n^{d-1} & \textit{si } d \textit{ pair}; \end{cases}$$

$$(g_n^{d+1})^- = \begin{cases} g_n^d & \textit{si } d \textit{ pair} \\ g_n^d - \{-1\}^n g_n^{d-1} & \textit{si } d \textit{ impair}. \end{cases}$$

Démonstration. D'après la définition 1.2.32, si d est impair, alors $(g_n^{d+2})^- = g_n^{d+1}$ et $(g_n^{d+1})^+ = g_n^d$, et si d est pair, $(g_n^{d+2})^+ = g_n^{d+1}$ et $(g_n^{d+1})^- = g_n^d$. Dans tous les cas on vérifie la première formule, puisque les deux opérateurs commutent.

Pour les deux suivantes, on utilise $(g_n^{d+1})^+ - (g_n^{d+1})^- = \{-1\}^n g_n^{d-1}$ qui vient de la proposition 1.2.19. On conclut en distinguant selon la parité de d. □

Le lien entre les f_n^d et g_n^d est donné par :

Proposition 1.2.36. *Pour tout $d \in \mathbb{N}^*$, on a :*

$$g_n^d = \sum_{k=\lfloor \frac{d}{2} \rfloor +1}^{d} \binom{\lfloor \frac{d-1}{2} \rfloor}{k - \lfloor \frac{d}{2} \rfloor - 1} \{-1\}^{n(d-k)} f_n^k$$

$$f_n^d = \sum_{k=1}^{d} (-1)^{d-k} \binom{d - \lfloor \frac{k+1}{2} \rfloor - 1}{\lfloor \frac{k}{2} \rfloor - 1} \{-1\}^{n(d-k)} g_n^k.$$

Démonstration. Notons α_d les invariants définis par la partie droite de la première formule. Si $d = 2m$, la formule s'écrit

$$\alpha_d = \sum_{k=m+1}^{2m} \binom{m-1}{k-m-1} \{-1\}^{n(2m-k)} f_n^k$$

ce qui donne

$$\alpha_d^+ = \sum_{k=m+1}^{2m} \binom{m-1}{k-m-1} \{-1\}^{n(2m-k)} f_n^{k-1},$$

et si $d = 2m+1$ alors la formule devient

$$\alpha_d = \sum_{k=m+1}^{2m+1} \binom{m}{k-m-1} \{-1\}^{n(2m+1-k)} f_n^k$$

d'où

$$\alpha_d^+ = \sum_{k=m+1}^{2m+1} \binom{m}{k-m-1} \{-1\}^{2m+1-k} f_n^{k-1}.$$

Il faut donc vérifier que dans les deux cas on trouve pour α_{d+1}^+ la récurrence définissant les g_n^d. C'est immédiat si $d = 2m+1$, et si $d = 2m$ on doit comparer

$$\sum_{k=m}^{2m} \binom{m}{k-m} \{-1\}^{n(2m-1)} f_n^k$$

et

$$\sum_{k=m+1}^{2m} \binom{m-1}{k-m-1} \{-1\}^{n(2m-k)} f_n^k + \sum_{k=m}^{2m-1} \binom{m-1}{k-m-2} \{-1\}^{n(2m-k)} f_n^k$$

dont on voit facilement qu'ils sont égaux.

Pour montrer la deuxième formule, on peut soit inverser la première, soit procéder de la même façon. On pose β_d défini par la partie droite de la deuxième formule. On a alors :

$$\begin{aligned}
\beta_d^+ &= (-1)^d \sum_m \binom{d-m-1}{m-1} \{-1\}^{n(d-2m)} (g_n^{2m})^+ \\
&+ (-1)^{d+1} \sum_m \binom{d-m-2}{m-1} \{-1\}^{n(d-2m-1)} (g_n^{2m+1})^+ \\
&= (-1)^d \sum_m \binom{d-m-1}{m-1} \{-1\}^{n(d-2m)} g_n^{2m-1} \\
&+ (-1)^{d+1} \sum_m \binom{d-m-2}{m-1} \{-1\}^{n(d-2m-1)} (g_n^{2m} + \{-1\}^n g_n^{2m-1}) \\
&= (-1)^{d+1} \sum_m \binom{d-m-2}{m-1} \{-1\}^{n(d-2m-1)} g_n^{2m} \\
&+ (-1)^d \sum_m \left(\binom{d-m-1}{m-1} - \binom{d-m-2}{m-1} \right) \{-1\}^{n(d-2m)} g_n^{2m-1} \\
&= (-1)^{d-1} \sum_m \binom{d-1-m-1}{m-1} \{-1\}^{n(d-1-2m)} g_n^{2m} \\
&+ (-1)^{d-1+1} \sum_m \binom{d-m-1}{m-2} \{-1\}^{n(d-2m)} g_n^{2m-1}
\end{aligned}$$

ce qui donne bien β_{d-1}. □

Corollaire 1.2.37. *En particulier, $(f_n^i)_{i\leqslant d}$ et $(g_n^i)_{i\leqslant d}$ engendrent le même sous-module de M.*

Démonstration. On voit que la matrice de transition est triangulaire avec des 1 sur la diagonale. □

La conséquence cruciale de l'équilibre des signes dans la définition des g_n^d est donnée par :

Proposition 1.2.38. *Soit $q \in I^n(K)$, qui s'écrit $q = \sum_{i=1}^s \varphi_i - \sum_{i=1}^t \psi_i$, où $\varphi_i, \psi_i \in \mathrm{Pf}_n(K)$. Alors pour tout $d > 2\max(s,t)$, $g_n^d(q) = 0$.*

Démonstration. On peut ajouter des formes hyperboliques dans une des sommes de sorte que $s = t$. On prouve alors l'énoncé par récurrence sur s : si $s = 0$ alors $q = 0$, donc pour $d > 0$ on a en effet $g_n^d(q) = 0$ par construction.

Si le resultat tient jusqu'à $s-1$ pour un certain $s \in \mathbb{N}^*$, alors on écrit $q' = q - \varphi_s$ et $q'' = q' + \psi_s$. On a

$$\begin{aligned}
g_n^d(q) &= g_n^d(q') + f_n(\varphi_s)(g_n^d)^+(q') \\
&= g_n^d(q'') - f_n(\psi_s)(g_n^d)^-(q'') + f_n(\varphi_s)(g_n^d)^+(q'') \\
&- f_n(\varphi_s)f_n(\psi_s)(g_n^d)^{+-}(q'').
\end{aligned}$$

Or d'après la proposition 1.2.35, $(g_n^d)^-$, $(g_n^d)^+$ et $(g_n^d)^{+-}$ peuvent tous s'exprimer comme combinaisons des g_n^k avec $k \geqslant d-2$, donc on peut appliquer l'hypothèse de récurrence à q''. □

Corollaire 1.2.39. *Si $q \in I(K)$ est la classe de Witt d'une forme de dimension $2m$, alors $g_1^d(q) = 0$ pour tout $d > 2m$.*

Démonstration. Si $q = \langle a_1, b_1, \dots, a_m, b_m\rangle$, alors $q = \sum_{i=1}^m \langle\langle -a_i\rangle\rangle - \langle\langle b_i\rangle\rangle$, ce qui conclut d'après la proposition. □

On peut à présent montrer le théorème central :

Théorème 1.2.40. *Soit $N = A(k)^{\mathbb{N}}$, qui est un $A(k)$-module filtré pour la filtration $N^m = \{(a_d)_{d\in\mathbb{N}} \mid a_d \in A^{m-nd}\}$.*

Les applications suivantes sont des isomorphismes mutuellement réciproques de $A(k)$-modules filtrés :

$$\begin{array}{rrcl} F: & N & \xrightarrow{\sim} & M \\ & (a_d) & \longmapsto & \sum_d a_d g_n^d, \end{array}$$

$$\begin{array}{rrcl} G: & M & \xrightarrow{\sim} & N \\ & \alpha & \longmapsto & (\alpha^{[d]}(0))_d. \end{array}$$

où on note $\alpha^{[d]} = \alpha^{s+,s-}$ si $d = 2s$, et $\alpha^{[d]} = \alpha^{(s+1)+,s-}$ si $d = 2s+1$.

Démonstration. Déjà, l'application F est bien définie, puisque d'après la proposition 1.2.38, pour tout $q \in I^n(K)$ fixé on a $g_n^d(q) = 0$ pour d assez grand. Alors F et G sont clairement des morphismes de modules, et le fait qu'ils respectent les filtrations est juste une reformulation du fait que g_n^d est à valeurs dans A^{nd}, et que Φ^ε est de degré $-n$.

En utilisant la proposition 1.2.35, on voit facilement que si $\alpha = \sum_d a_d g_n^d$, alors $a_{2s} = \alpha^{s+,s-}(0)$ et $a_{2s+1} = \alpha^{(s+1)+,s-}(0)$. Donc $G \circ F = \mathrm{Id}$.

On prouve à présent que G est injectif, ce qui achève la preuve du théorème. Soient $\alpha \in \mathrm{Ker}(G)$ et $d \in \mathbb{N}$. D'après la proposition 1.2.28 et le corollaire 1.2.37, on voit que α est congru à une certaine combinaison $\sum_{nk<d} a_k g_n^k$ modulo M^d. De là, la suite exacte de la proposition 1.2.23 permet de voir que $a_k \equiv \alpha^{[k]}(0)$ modulo $A^{d-nk}(k)$, donc, puisque $\alpha^{[k]}(0) = 0$, $a_k \in A^{d-nk}(k)$. Cela implique que $\sum_{nk\leqslant d} a_k g_n^k \in M^d$, et donc $\alpha \in M^d$. Comme c'est vrai pour tout $d \in \mathbb{N}$, on peut conclure que $\alpha = 0$. □

On en déduit aisément le résultat suivant, important pour les invariants cohomologiques :

Corollaire 1.2.41. *Tout invariant de I^n à valeur dans $H^d(K, \mu_2)$ se relève en un invariant à valeurs dans $I^d(K)$.*

Démonstration. Cela vient simplement du fait que les $u_{nd}^{(n)}$, qui sont les f_n^d dans le cas $A = H$, se relèvent en π_n^d. □

Corollaire 1.2.42. *Tout $\alpha \in M$ peut s'écrire de façon unique comme $\sum a_d f_n^d$ avec $a_d \in A(k)$, en prenant $a_d = \alpha^{d+}(0)$. En particulier, α est déterminé par ses valeurs sur les sommes de formes de Pfister.*

Démonstration. En utilisant les formules de la proposition 1.2.36, on voit qu'une combinaison à coefficients dans $A(k)$ des g_n^d donne encore une telle combinaison des f_n^d. La formule pour a_d est claire, et comme les $\Phi^d(\alpha)(0)$ sont entièrement déterminés par les valeurs de α sur les sommes de formes de Pfister, on en déduit le résultat. □

Remarque 1.2.43. Comme on l'a déjà mentionné, si on prend une combinaison infinie des f_n^d, on trouve en général un invariant à valeurs dans $\hat{A}$, la complétion de A vis-à-vis de sa filtration. On peut adapter les preuves ci-dessus pour montrer que les $\mathrm{Inv}(I^n, \hat{A})$ sont exactement les combinaisons $\sum a_d f_n^d$ avec $a_d \in \hat{A}(k)$, ou alternativement les combinaisons $\sum a_d g_n^d$, cela ne fait plus de différence.

Une façon de voir : si on observe les formules de la proposition 1.2.36, on constate que si on exprime $\sum a_d g_n^d$ avec $a_d \in A(k)$ en fonction des f_n^d, on trouve $\sum b_d f_n^d$ avec $b_d \in A(k)$, tandis que si on part de $\sum a_d f_n^d$ avec $a_d \in A(k)$, on trouve en général $\sum b_d g_n^d$ avec $b_d \in \hat{A}(k)$ (parce que l'expression de f_n^d en fonction des g_n^k fait intervenir des k arbitrairement petits, ce qui n'est pas le cas dans l'autre sens).

Remarque 1.2.44. Si k n'est pas formellement réel, alors $\{-1\}^d = 0$ pour d assez grand, et donc par la proposition 1.2.10 $f_n^d(-\varphi) = 0$ pour tout $\varphi \in \mathrm{Pf}_n(K)$. On voit donc que dans ce cas, pour tout $q \in I^n(K)$ on a $f_n^d(q) = 0$ pour d assez grand (pour les mêmes raisons que dans la proposition 1.2.11), et donc on peut utiliser les f_n^d au lieu des g_n^d dans le théorème (avec $G(\alpha) = (\alpha^{d+}(0))_d$). Dans le cas extrême où -1 est un carré dans k, on a même $f_n^d = g_n^d$, comme le montre la proposition 1.2.36. De façon générale, quand k n'est pas formellement réel, cette proposition montre qu'une somme $\sum a_d f_n^d$ s'écrit cette fois $\sum b_d g_n^d$ avec $b_d \in A(k)$ contrairement à ce qu'on avait noté dans la remarque précédente.

D'un autre côté, l'exemple 1.2.31 montre qu'on ne peut pas utiliser les f_n^d si k est formellement réel, donc on peut établir une caractérisation exacte : toute combinaison des f_n^d est à valeurs dans A si et seulement si k n'est pas formellement réel.

Remarque 1.2.45. On voit qu'on peut construire des invariants cohomologiques α (par exemple $\alpha = \sum_d v_{nd}^{(n)}$) tels que, bien que le degré cohomologique de $\alpha(q)$ soit borné pour tout q fixé, il n'est pas uniformément borné quand q varie (donc α est bien à valeurs dans $H^*(K, \mu_2)$ mais dans aucun $H^d(K, \mu_2)$). Cela reflète en un certain sens la nature « infinie » de I^n, et c'est un comportement qui n'apparaît jamais pour les invariants de groupes algébriques.

Le sous-module M' des invariants cohomologiques de degré uniformément borné est précisément le sous-module engendré (finiment) par les f_n^d (ou les g_n^d).

1.2.5 Structure d'algèbre

Comme $\mathrm{Inv}(I^n, A)$ n'est pas seulement un $A(k)$-module, mais également une algèbre, on souhaite comprendre comment le produit s'exprime en fonction des éléments de base f_n^d.

On rappelle que le coefficient multinomial $\binom{n}{a_1,\dots,a_r}$ (où $a_1 + \cdots + a_r = n$) est défini comme $\frac{n!}{a_1!\cdots a_r!}$ (et en particulier, le coefficient binomial usuel $\binom{n}{m}$ est $\binom{n}{m,n-m}$). Quand $m < 0$ ou $m > n$, on s'autorise quand même à écrire $\binom{n}{m}$, qui vaut alors 0.

Proposition 1.2.46. *Soient $s, t \in \mathbb{N}$. On a*

$$f_n^s \cdot f_n^t = \sum_{d=\max(s,t)}^{s+t} \binom{d}{s+t-d, d-s, d-t} \{-1\}^{n(s+t-d)} f_n^d.$$

Démonstration. Soient $q \in I^n(K)$ et $\varphi \in \mathrm{Pf}_n(K)$. Alors on a

$$(f_n^s \cdot f_n^t)(q+\varphi) = (f_n^s(q) + f_n(\varphi) f_n^{s-1}(q)) \cdot (f_n^t(q) + f_n(\varphi) f_n^{t-1}(q))$$

d'où

$$\Phi\left(f_n^s \cdot f_n^t\right) = f_n^s \cdot f_n^{t-1} + f_n^{s-1} \cdot f_n^t + \{-1\}^n f_n^{s-1} \cdot f_n^{t-1}. \tag{1.2.47}$$

On procède par récurrence, disons sur (s,t) avec l'ordre lexicographique. Déjà le résultat est clair si $s = 0$ ou $t = 0$. Par symétrie on peut supposer $s > t$ (il reste alors le cas $s = t$ qui se traite de façon similaire).

Alors par récurrence on peut remplacer chaque terme dans (1.2.47), et réarranger les termes pour trouver

$$\begin{aligned}\Phi\left(f_n^s \cdot f_n^t\right) = &\binom{s}{t} \cdot \{-1\}^{nt} f_n^{s-1} + \binom{s+t}{t} f_n^{s+t-1} \\ &+ \sum_{d=s}^{s+t-2} \binom{d+1}{s+t-d-1, d-s+1, d-t+1} \{-1\}^{n(s+t-d-1)} f_n^d\end{aligned}$$

où pour le coefficient devant f_n^{s-1} on utilise $\binom{s-1}{t} + \binom{s-1}{t-1} = \binom{s}{t}$, pour celui de f_n^{s+t-1} on se sert de $\binom{s+t-1}{t} + \binom{s+t-1}{t-1} = \binom{s+t}{t}$, et pour les autres termes on emploie $\binom{d}{s+t-1-d, d-s+1, d-t} + \binom{d}{s+t-1-d, d-s, d-t+1} + \binom{d}{s+t-d-2, d-s+1, d-t+1} = \binom{d+1}{s+t-d-1, d-s+1, d-t+1}$.

On exploite alors l'idée dans la remarque 1.2.26 pour trouver la formule attendue pour $f_n^s \cdot f_n^t$. □

On peut noter quelques cas particuliers simples, qui s'appliquent notamment à la cohomologie. On introduit quelques notations : si $s, t \in \mathbb{N}$, on notera $s \vee t$ et $s \wedge t$ les entiers obtenus en appliquant respectivement un *OU* et un *ET* logiques sur les représentations binaires de s et t. En particulier, $s \vee t + s \wedge t = s + t$. Si $s \wedge t = 0$, on dit que s et t ont des représentations binaires *disjointes*.

Corollaire 1.2.48. *Si $A(k)$ est de caractéristique 2, alors :*

$$f_n^s \cdot f_n^t = \{-1\}^{s\wedge t} f_n^{s\vee t}.$$

Si -1 est un carré dans k, alors $f_n^s \cdot f_n^t$ vaut f_n^{s+t} si s et t ont des représentations binaires disjointes, et 0 sinon.

Démonstration. Pour le premier point, il faut appliquer le lemme combinatoire 1.2.49. Pour le deuxième, on montre plus loin (voir 1.2.53) que si -1 est un carré alors $A(k)$ est de caractéristique 2. □

Lemme 1.2.49. *Le coefficient multinomial $\binom{m}{s+t-m, m-s, m-t}$ est impair si et seulement si $m = s \vee t$.*

Démonstration. Il est connu que pour tout $a \in \mathbb{Z}$, la valuation 2-adique de $a!$ est $a - \nu(a)$ où $\nu(a)$ est le nombre de 1 dans la représentation binaire de a. Alors :

$$\begin{aligned} v_2\binom{m}{s+t-m, m-s, m-t} &= (m-\nu(m)) - (s+t-m-\nu(s+t-m)) \\ &\quad - (m-s-\nu(m-s)) - (m-t-\nu(m-t)) \\ &= \nu(s+t-m) + \nu(m-s) + \nu(m-t) - \nu(m). \end{aligned}$$

Mais il est facile de voir que pour tous $a, b \in \mathbb{Z}$, $\nu(a+b) \leqslant \nu(a) + \nu(b)$, avec égalité ssi $a \wedge b = 0$. Donc $\binom{m}{s+t-m, m-s, m-t}$ est impair si et seulement si $s+t-m$, $m-s$ et $m-t$ ont tous des représentations binaires disjointes deux à deux.

On affirme que c'est équivalent à $m = s \vee t$. En effet, si $m = s \vee t$ c'est évident, et si $m \neq s \vee t$, considérons le bit le plus faible où m et $s \vee t$ diffèrent ; on a plusieurs possibilités pour les bits de s, t et m à cet emplacement : s a un 1 et m un 0, t a un 1 et m un 0, ou s et t ont un 0 et m un 1. Dans tous ces cas, au moins deux nombres parmi $m-s$, $m-t$ et $s+t-m$ ont un 1 à cet emplacement, et leurs représentations binaires ne sont pas disjointes. □

Remarque 1.2.50. Dans le cas où $A(k)$ est de caractéristique 2, on obtient une présentation d'algèbre très simple pour M', le sous-module des invariants qui est constitué des combinaisons *finies* des f_n^d (il est plus délicat de parler de présentation pour $\mathrm{Inv}(I^n, A)$ puisqu'il faut utiliser des sommes infinies pour représenter un élément quelconque en fonction des f_n^d).

En effet, la $A(k)$-algèbre M' a pour générateurs les $x_i = f_n^{2^i}$, et les relations sur ces générateurs sont données par $x_i^2 = \{-1\}^{n2^i} x_i$.

1.2.6 Restriction de I^n à I^{n+1}

On dispose bien évidemment d'un morphisme de restriction de $\mathrm{Inv}(I^n, A)$ vers $\mathrm{Inv}(I^{n+1}, A)$, et on notera $\alpha_{|I^{n+1}}$ la restriction de $\alpha \in \mathrm{Inv}(I^n, A)$.

Le comportement de la restriction dépend dans une certaine mesure de la nature de A :

Proposition 1.2.51. *Il existe un unique $\delta(A) \in A(k)$ tel que $(f_1)_{I^2} = \delta(A) f_2$, vérifiant $\{-1\}\delta(A) = 2$.*

De plus, pour tous $n \in \mathbb{N}^*$ et $d \in \mathbb{N}$ on a $(f_n)_{I^{n+d}} = \delta(A)^d f_{n+d}$

Démonstration. On rappelle que $f_1 = f_1^1$ est un morphisme de groupes. Notons $\alpha = (f_1)_{I^2}$; c'est un invariant de I^2 et d'après le corollaire 1.2.27, on a bien existence et unicité de $\delta(A)$.

On a $f_1(2q) = 2f_1(q)$ et $f_1(2q) = f_1(\langle\langle -1\rangle\rangle q) = \delta\{-1\}f_1(q)$, donc $2f_1 = \{-1\}\delta f_1$, d'où $\{-1\}\delta = 2$.

D'après le corollaire 1.2.42, pour établir $(f_n)_{I^{n+d}} = \delta(A)^d f_{n+d}$, il suffit de montrer qu'ils ont la même valeur sur les $(n+d)$-formes de Pfister, donc que $f_n(\langle\langle a_1, \dots, a_{n+d}\rangle\rangle) = \delta(A)^d\{a_1, \dots, a_{n+d}\}$. Or :

$$\begin{aligned} f_n(\langle\langle a_1, \dots, a_{n+d}\rangle\rangle) &= f_{n-1}(\langle\langle a_1, \dots, a_{n-1}\rangle\rangle) f_1(\langle\langle a_n, \dots a_{n+d}\rangle\rangle) \\ &= \{a_1, \dots, a_{n-1}\} f_1(\langle\langle a_n, \dots, a_{n+d}\rangle\rangle) \end{aligned}$$

et on montre facilement par récurrence que

$$f_1(\langle\langle a_n, \dots a_{n+d}\rangle\rangle) = \delta(A)^d\{a_n, \dots, a_{n+d}\}.$$

□

Exemple 1.2.52. Si $A(K) = W(K)$, alors f_1 et f_2 sont l'identité donc $\delta(A) = 1$. En revanche, si $A(K) = H^*(K, \mu_2)$, $f_1^n = e_1$ est nul sur $I^2(K)$, donc $\delta(A) = 0$.

Remarque 1.2.53. Si $\delta(A) = 0$ ou si -1 est un carré dans K, $A(K)$ est de caractéristique 2.

Quand il n'y a pas d'ambiguité on écrira $\delta = \delta(A)$. Une fois ces notations posées, on peut écrire :

Proposition 1.2.54. *Pour tout $n \in \mathbb{N}^*$ et tout $d \in \mathbb{N}^*$:*

$$(f_n^d)_{I^{n+1}} = \sum_{\frac{d}{2} \leqslant k \leqslant d} \binom{k}{d-k} \delta(A)^{2k-d}\{-1\}^{(d-k)(n-1)} f_{n+1}^k$$

Démonstration. Il suffit d'appliquer f_{nd} à la formule du corollaire 1.1.43 exprimant π_n^d en fonction des π_{n+1}^k. □

Corollaire 1.2.55. *Si $\delta = 0$ (et en particulier quand $A(K) = H^*(K, \mu_2)$), on a :*

$$(f_n^d)_{|I^{n+1}} = \begin{cases} \{-1\}^{m(n-1)} f_{n+1}^m & \text{si } d = 2m \\ 0 & \text{si } d \text{ impair} \end{cases}$$

Corollaire 1.2.56. *Si -1 est un carré dans k, on a $(f_n^d)_{|I^{n+1}} = \delta^d f_{n+1}^d$ pour tout $n \geqslant 2$, et donc $(f_2^d)_{|I^n} = \delta^{(n-2)d} f_n^d$.*

Si en plus $\delta = 0$, alors $(f_n^d)_{|I^{n+1}} = 0$ si $d \geqslant 1$, sauf quand $n = 1$ et $d = 2m$, auquel cas $(f_1^{2m})_{|I^2} = f_2^m$.

On peut tirer quelques conséquences dans le cas des invariants cohomologiques.

Remarque 1.2.57. En particulier, on obtient la formule $(u_{2d}^{(1)})_{|I^2} = u_{2d}^{(2)}$ (quel que soit k), qui montre que tout invariant de I^2 s'étend à I (pas de façon unique). En revanche, si $n \geqslant 3$ alors pour $d \geqslant 1$ $u_{nd}^{(n)}$ ne s'étend jamais à I^{n-1}.

On retrouve notamment comme cas particulier le fait bien connu que e_2 s'étend à tout I alors que e_3 ne s'étend pas à I^2.

Remarque 1.2.58. On peut observer que si $(-1) \in H^1(k, \mu_2)$ n'est pas un diviseur de zéro dans $H^*(k, \mu_2)$ alors le noyau de la restriction des invariants de I^n à I^{n+1} est exactement l'idéal engendré par e_n, mais en général il est plus gros (quand -1 est un carré, il est même constitué de tous les invariants normalisés). C'est notable dans la mesure où on aurait pu s'attendre à ce que les invariants nuls sur les formes vérifiant $\alpha(q) = 0$ soient exactement les multiples de α.

1.2.7 Similitudes

Dans cette partie on étudie le comportement des invariants vis-à-vis des similitudes.

Proposition-définition 1.2.59. *Il existe un unique morphisme de $A(k)$-modules filtrés, de degré -1,*

$$\begin{array}{rccc} \Psi : & M & \longrightarrow & M \\ & \alpha & \longmapsto & \widetilde{\alpha} \end{array}$$

tel que

$$\alpha(\langle\lambda\rangle q) = \alpha(q) + \{\lambda\}\widetilde{\alpha}(q) \tag{1.2.60}$$

pour tous $\alpha \in M$, $q \in I^n(K)$ et $\lambda \in K^*$.

Démonstration. Soient $\alpha \in \mathrm{Inv}(I^n, A)$ et $q \in I^n(K)$. Pour tout $\lambda \in L^*$, avec L/K extension de corps, on pose $\beta_q(\lambda) = \alpha(\langle\lambda\rangle q)$.

Alors β_q est un invariant sur K des classes de carrés à valeurs dans A. Or le foncteur des classes de carrés est isomorphe à Pf_1, donc on peut appliquer la condition (iv) sur A : il existe d'uniques $x_q, y_q \in A(K)$ tels que $\beta_q(\lambda) = x_q + \{\lambda\}\cdot y_q$. En prenant $\lambda = 1$ on voit que $x_q = \alpha(q)$, et on pose $\tilde{\alpha}(q) = y_q$.

L'unicité de y_q permet de voir que $\tilde{\alpha} \in \mathrm{Inv}(I^n, A)$. □

Remarque 1.2.61. On peut remarquer que $\tilde{\alpha}$ est toujours un invariant normalisé.

La composition des similitudes donne le résultat intéressant suivant :

Proposition 1.2.62. *On a $\Psi^2 = -\delta(A)\Psi$.*

Démonstration. On note que

$$\{\lambda\mu\} = \{\lambda\} + \{\mu\} - \delta(A)\{\lambda, \mu\}. \tag{1.2.63}$$

De là,

$$\begin{aligned}\alpha(\langle\lambda\mu\rangle q) &= \alpha(\langle\lambda\rangle q) + \{\mu\}\widetilde{\alpha}(\langle\lambda\rangle q)\\ &= \alpha(q) + \{\lambda\}\widetilde{\alpha}(q) + \{\mu\}\widetilde{\alpha}(q) + \{\lambda,\mu\}\widetilde{\widetilde{\alpha}}(q)\\ &= \alpha(q) + \{\lambda\mu\}\widetilde{\alpha}(q) + \delta(A)\{\lambda,\mu\}\widetilde{\alpha}(q) + \{\lambda,\mu\}\widetilde{\widetilde{\alpha}}(q)\end{aligned}$$

et également

$$\alpha(\langle\lambda\mu\rangle q) = \alpha(q) + \{\lambda\mu\}\widetilde{\alpha}(q)$$

donc $\{\lambda,\mu\}(\delta(A)\widetilde{\alpha}(q) + \widetilde{\widetilde{\alpha}}(q)) = 0$. Comme c'est vrai pour tous λ, μ sur toute extension on peut conclure que $\widetilde{\widetilde{\alpha}} = -\delta(A)\widetilde{\alpha}$. □

Remarque 1.2.64. Par définition, $\widetilde{\alpha} = 0$ si et seulement si $\alpha(\langle\lambda\rangle q) = \alpha(q)$, ce qu'on qualifiera d'*invariance par similitude*. Mais la proposition précédente suggère qu'il est intéressant d'étudier aussi la propriété $\widetilde{\alpha} = -\delta(A)\alpha$, qui est notamment vérifiée par tout élément de la forme $\widetilde{\beta}$. Dans le cas des invariants cohomologiques, on retrouve la même propriété puisque $\delta = 0$, mais dans le cas des invariants de Witt elle est équivalente à $\alpha(\langle\lambda\rangle q) = \langle\lambda\rangle\alpha(q)$; on dira alors que α est *compatible avec les similitudes.*

Lorsque $\delta \neq 0$ (et donc en particulier pour les invariants de Witt), la proposition montre alors que tout α peut être décomposé de façon unique en $\alpha = \beta + \gamma$ où β est compatible avec les similitudes, et γ est invariant par similitudes ; précisément, $\beta = -\widetilde{\alpha}$ et $\gamma = \alpha + \widetilde{\alpha}$.

De façon moins intrinsèque, tout invariant de Witt α est une combinaison des λ^d (puisque c'est le cas des π_n^d), et alors β correspond aux termes avec d impair, et γ aux termes avec d pair (pour cette raison on parlera parfois de *partie paire* et *partie impaire* de α).

On veut maintenant étudier l'action de Ψ sur les g_n^d, qui s'avèrent avoir un bien meilleur comportement que les f_n^d relativement aux similitudes (ce qui n'est pas surprenant si on considère la cas de la mutliplication par $\langle -1\rangle$).

Proposition 1.2.65. *Soient $n \in \mathbb{N}^*$, $d \in \mathbb{N}$. Alors*

$$\widetilde{g_n^d} = \begin{cases} -\delta(A) g_n^d & \text{si } d \text{ est impair}\\ \{-1\}^{n-1} g_n^{d-1} & \text{si } d \text{ est pair.}\end{cases}$$

Démonstration. On procède par récurrence sur d, les cas $d = 0, 1$ étant triviaux. Si $q \in I^n(K)$, $\varphi \in \mathrm{Pf}_n(K)$ et $\lambda \in K^*$, alors

$$\begin{aligned} g_n^d(\langle\lambda\rangle(q+\varphi)) &= g_n^d(q+\varphi) + \{\lambda\}\widetilde{g_n^d}(q+\varphi)\\ &= g_n^d(q) + f_n(\varphi)(g_n^d)^+(q) + \{\lambda\}\widetilde{g_n^d}(q) + \{\lambda\}f_n(\varphi)\widetilde{g_n^d}^+(q).\end{aligned}$$

D'un autre côté, si on écrit $\varphi = \langle\langle a\rangle\rangle\psi$:

$$\begin{aligned}
g_n^d(\langle\lambda\rangle(q+\varphi)) &= g_n^d(\langle\lambda\rangle q + \langle\langle\lambda a\rangle\rangle\psi - \langle\langle\lambda\rangle\rangle\psi) \\
&= g_n^d(\langle\lambda\rangle q - \langle\langle\lambda\rangle\rangle\psi) + \{\lambda a\} f_{n-1}(\psi)(g_n^d)^+(\langle\lambda\rangle q - \langle\langle\lambda\rangle\rangle\psi) \\
&= g_n^d(\langle\lambda\rangle q) - \{\lambda\} f_{n-1}(\psi)(g_n^d)^-(\langle\lambda\rangle q) \\
&+ \{\lambda a\} f_{n-1}(\psi)(g_n^d)^+(\langle\lambda\rangle q) - \{\lambda, \lambda a\}\{-1\}^{n-1} f_{n-1}(\psi)(g_n^d)^{+-}(\langle\lambda\rangle q) \\
&= g_n^d(q) + \{\lambda\}\widetilde{g_n^d}(q) - \{\lambda\} f_{n-1}(\psi)(g_n^d)^-(q) - \{\lambda,\lambda\} f_{n-1}(\psi)\widetilde{(g_n^d)^-}(q) \\
&+ \{\lambda a\} f_{n-1}(\psi)(g_n^d)^+(q) - \{\lambda, \lambda a\}\{-1\}^{n-1} f_{n-1}(\psi)(g_n^d)^{+-}(q) \\
&+ \{\lambda, \lambda a\} f_{n-1}(\psi)\widetilde{(g_n^d)^+}(q) - \{\lambda,\lambda,\lambda a\}\{-1\}^{n-1} f_{n-1}(\psi)\widetilde{(g_n^d)^{+-}}(q).
\end{aligned}$$

En prenant λ, a et ψ génériques et en considérant les résidus, on trouve :

$$\widetilde{g_n^d}^{\,+} = -\delta(g_n^d)^+ - \widetilde{(g_n^d)^+} + \{-1\}^{n-1}(g_n^d)^{+-} + \{-1\}^n \widetilde{(g_n^d)^{+-}}$$

en utilisant plusieurs fois l'équation (1.2.63) et le fait que $\delta\{-1\} = 2$.

Si d est pair, alors $(g_n^d)^+ = g_n^{d-1}$, donc $\widetilde{(g_n^d)^+} = -\delta g_n^{d-1}$, et $(g_n^d)^{+-} = g_n^{d-2}$ donc $\widetilde{(g_n^d)^{+-}} = \{-1\}^{n-1} g_n^{d-3}$. On obtient donc :

$$\begin{aligned}
\widetilde{g_n^d}^{\,+} &= -\delta g_n^{d-1} + \delta g_n^{d-1} + \{-1\}^{n-1}(g_n^{d-2} + \{-1\}^n g_n^{d-3}) \\
&= \{-1\}^{n-1}(g_n^{d-1})^+
\end{aligned}$$

ce qui permet de conclure puisque $\widetilde{g_n^d}$ est normalisé (voir la remarque (1.2.61)).

De même, si d est impair, $(g_n^d)^+ = g_n^{d-1} + \{-1\}^n g_n^{d-2}$, donc $\widetilde{(g_n^d)^+} = \{-1\}^{n-1} g_n^{d-2} - \delta\{-1\}^n g_n^{d-2} = -\{-1\}^{n-1} g_n^{d-2}$, et $(g_n^d)^{+-} = g_n^{d-2}$ so $\widetilde{(g_n^d)^{+-}} = -\delta g_n^{d-2}$. Alors

$$\begin{aligned}
\widetilde{g_n^d}^{\,+} &= -\delta(g_n^d)^+ + \{-1\}^{n-1} g_n^{d-2} + \{-1\}^{n-1} g_n^{d-2} - \delta\{-1\}^n g_n^{d-2} \\
&= -\delta(g_n^d)^+
\end{aligned}$$

ce qui permet encore de conclure. □

Ce comportement très simple permet quelques observations :

Remarque 1.2.66. On retrouve facilement en utilisant les g_n^d le fait que tout invariant α de la forme $\widetilde{\beta}$ est compatible avec les similitudes (au sens de la remarque 1.2.64). On peut également répondre à la question légitime de savoir si ces deux conditions sont équivalentes. Si $\alpha = \sum a_d g_n^d$, alors α est invariant par similitude si et seulement si pour tout d pair, $\delta(A)a_d = 0$ et $\{-1\}^{n-1}a_d = 0$ (si $d \geqslant 2$) ; en revanche α est de la forme $\widetilde{\beta}$ pour un certain β si et seulement si $a_d = 0$ pour d pair, et $a_d = \{-1\}^{n-1}x_d - \delta(A)y_d$ pour certains x_d, y_d si d est impair. En particulier, les conditions sont équivalentes si $\delta(A) = 1$ (donc pour les invariants de Witt), et dans ce cas elles correspondent au fait d'être une combinaison des g_n^d avec d impair, mais elles ne sont jamais équivalentes si $\delta(A) = 0$ (donc pour les invariants cohomologiques) et $n > 1$.

Remarque 1.2.67. On a défini deux opérateurs, Φ et Ψ, qui contrôlent respectivement le comportement des invariants vis-à-vis des sommes et des similitudes. Il est tentant d'essayer d'établir un lien entre $\Phi \circ \Psi$ et $\Psi \circ \Phi$, mais en fait il est relativement facile de vérifier en utilisant la base des g_n^d que lorsque $\delta(A) = 0$ ces deux compositions sont complètement décorrélées, au sens suivant : si β est n'importe quel invariant dans l'image de $\Phi \circ \Psi$, et γ dans l'image de $\Psi \circ \Phi$, alors il existe α tel que $\beta = (\widetilde{\alpha})^+$ et $\gamma = \widetilde{(\alpha^+)}$.

Remarque 1.2.68. On peut également établir des formules pour l'action de Ψ sur les f_n^d, soit directement par des méthodes similaires, soit en utilisant les formules de passage de la proposition 1.2.36. On ne détaillera pas le calcul ici, mais on peut donner ces formules à titre indicatif :

$$\widetilde{f_n^d} = (-1)^d \sum_{k=1}^{d-1} \binom{d-1}{k-1} \{-1\}^{n(d-k)-1} f_n^k + \left\{ \begin{array}{cl} 0 & \text{si } d \text{ pair} \\ -\delta(A) f_n^d & \text{si } d \text{ impair.} \end{array} \right.$$

1.2.8 Ramification des invariants

Dans cette courte partie on étudie le comportement des invariants par rapport aux résidus de valuations discrètes. Soit donc (K, v) un corps valué, où v est une k-valuation discrète de rang 1.

Pour éviter d'avoir à introduire une notion abstraite de ramification sur un A général vérifiant nos conditions, on se restreint ici explicitement à $A(K) = W(K)$ ou $A(K) = H^*(K, \mu_2)$.

Proposition 1.2.69. *Soient $n \in \mathbb{N}^*$ et $q \in I^n(K)$. Si q est non ramifiée, alors $\alpha(q)$ est non ramifiée pour tout $\alpha \in \mathrm{Inv}(I^n, A)$.*

Démonstration. Comme v est une k-valuation, il suffit de montrer le résultat pour $\alpha = f_n^d$. Soit $q \in I^n(K)$ non ramifiée. Comme on peut écrire $q = \langle a_1, \ldots, a_r \rangle$ avec $a_i \in \mathcal{O}_K$, $\lambda^k(q)$ est également non ramifiée pour tout $k \in \mathbb{N}$, et donc $\pi_n^d(q)$ aussi. Comme e_{nd} envoie une forme non ramifiée sur une classe de cohomologie non ramifiée, $u_{nd}^{(n)}(q)$ est également non ramifié. $\square$

1.2.9 Invariants en dimension fixée

Dans cette partie, on décrit les restrictions des invariants de I^n en dimension fixée pour $n = 1$ et 2.

Invariants de I

Dans [10, thm 17.3, thm 28.5], Serre décrit les invariants cohomologiques ainsi que les invariants de Witt de Quad_{2r} (les formes quadratiques en dimension fixée $2r$). On trouve dans les deux cas un $A(k)$-module libre de rang $n+1$, respectivement sur les classes de Stiefel-Whitney w_k et sur les λ^k, pour $0 \leqslant k \leqslant n$ (on rappelle que $w_k(\langle a_1, \dots, a_n\rangle) = \sum_{i_1<\dots<i_k}(a_{i_1}, \dots, a_{i_k})$). Comme on peut restreindre les invariants de I à Quad_{2r}, on peut se demander comment ils se décomposent en fonction des classes de Stiefel-Whitney et des λ-opérations.

Il faut ici faire attention aux définitions que l'on utilise : quand on écrit (par exemple) que $\pi_1^2(q) = \lambda^2(q) - \lambda^1(q)$, on travaille au niveau des classes de Witt, ramenées dans $GW(K)$ par l'isomorphisme canonique $\hat{I}(K) \simeq I(K)$. Si q est de dimension $n = 2r$, on applique donc en réalité les λ^k à $q - r\langle\langle 1\rangle\rangle \in \hat{I}(K)$. Pour dissiper les ambiguïtés de notations, on utilisera dans cette partie $\hat{\lambda}^k$ pour désigner cette opération, par opposition à λ^k qui désignera directement l'opération sur $GW(K)$ (en particulier, λ^k n'est pas bien défini sur les classes de Witt, par opposition à $\hat{\lambda}^k$). On peut passer de l'un à l'autre de la façon suivante :

Lemme 1.2.70. *Soit q une forme quadratique de dimension $2r$ sur K. Alors pour tout $d \in \mathbb{N}$, on a dans $W(K)$:*

$$\lambda^d(q) = \sum_{\substack{i=0 \\ i\equiv d mod 2}}^{d} \binom{r}{\frac{d-i}{2}}(-1)^{\frac{d-i}{2}}\hat{\lambda}^i(q)$$

et

$$\hat{\lambda}^d(q) = \sum_{\substack{i=0 \\ i\equiv d mod 2}}^{d} \binom{r+\frac{d-i}{2}-1}{\frac{d-i}{2}}\lambda^i(q).$$

Démonstration. On note, similairement à la notation familière $\lambda_t(q) \in W(K)[[t]]$, $\hat{\lambda}_t(q) = \sum_{d\in\mathbb{N}} \hat{\lambda}^d(q)t^d$. On a alors dans $W(K)$:

$$\begin{aligned}\lambda_t(\langle\langle 1\rangle\rangle) &= \lambda_t(\langle 1\rangle)\lambda_t(\langle -1\rangle)\\ &= (1+t)(1-t)\\ &= 1-t^2\end{aligned}$$

donc $\hat{\lambda}_t(q) = \lambda_t(q - r\langle\langle 1\rangle\rangle) = (1-t^2)^{-r}\lambda_t(q)$, et réciproquement $\lambda_t(q) = (1-t^2)^r\hat{\lambda}_t(q)$, ce qui donne les formules voulues en développant $(1-t^2)^r$ et $(1-t^2)^{-r}$. □

On peut exprimer les g_1^d à partir des opérations λ :

Proposition 1.2.71. *Soit q une forme quadratique de dimension $2r$ sur K. Alors pour tout $m \in \mathbb{N}^*$, on a*

$$g_1^{2m}(q) = \sum_{i=0}^{2m} (-1)^i \binom{r - \lceil \frac{i}{2} \rceil}{m - \lceil \frac{i}{2} \rceil} \lambda^i(q)$$

et pour tout $m \in \mathbb{N}$:

$$g_1^{2m+1}(q) = \sum_{i=0}^{m} \binom{r-1-i}{m-i} \lambda^{2i+1}(q).$$

Démonstration. On pose $\alpha_d(q)$ défini par le terme de droite des équations de l'énoncé. A priori ce n'est pas un invariant de classes de Witt mais simplement un invariant de classes d'isométrie défini en toute dimension paire $2r$. On va montrer que $\alpha_{2m+2}(q + \langle\langle a \rangle\rangle) = \alpha_{2m}(q) + \langle\langle a \rangle\rangle \alpha_{2m+1}(q)$ et $\alpha_{2m+1}(q + \langle\langle a \rangle\rangle) = \alpha_{2m+1}(q) + \langle\langle a \rangle\rangle (\alpha_{2m}(q) + \langle\langle -1 \rangle\rangle \alpha_{2m-1}(q)$, ce qui montre à la fois que α_d est bien défini sur les classes de Witt en prenant $a = 1$, et qu'ils vérifient la même récurrence que les g_1^d.

On voit facilement que

$$\lambda^i(q + \langle\langle a \rangle\rangle) = \lambda^i(q) - \lambda^{i-2}(q) + \langle\langle a \rangle\rangle (\lambda^{i-1}(q) + \lambda^{i-2}(q).$$

De là :

$$\begin{aligned}
&\alpha_{2m+2}(q + \langle\langle a \rangle\rangle) \\
&= \sum_j \binom{r+1-j}{m+1-j} \lambda^{2j}(q + \langle\langle a \rangle\rangle) - \sum_j \binom{r-j}{m-j} \lambda^{2j+1}(q + \langle\langle a \rangle\rangle) \\
&= \sum_j \binom{r+1-j}{m+1-j} (\lambda^{2j}(q) - \lambda^{2j-2}(q)) - \sum_j \binom{r-j}{m-j} (\lambda^{2j+1}(q) - \lambda^{2j-1}(q)) \\
&+ \langle\langle a \rangle\rangle \left(\sum_j \binom{r+1-j}{m+1-j} (\lambda^{2j-1}(q) + \lambda^{2j-2}(q)) - \sum_j \binom{r-j}{m-j} (\lambda^{2j}(q) + \lambda^{2j-1}(q)) \right) \\
&= \sum_j \left(\binom{r+1-j}{m+1-j} - \binom{r-j}{m-j} \right) \lambda^{2j}(q) - \sum_j \left(\binom{r-j}{m-j} - \binom{r-j-1}{m-j-1} \right) \lambda^{2j+1}(q) \\
&+ \langle\langle a \rangle\rangle \sum_j \left(\binom{r+1-j}{m+1-j} - \binom{r-j}{m-j} \right) \lambda^{2j-1}(q) \\
&= \sum_j \binom{r-1}{m+1-j} \lambda^{2j}(q) - \sum_j \binom{r-j-1}{m-j} \lambda^{2j+1}(q) + \langle\langle a \rangle\rangle \sum_j \binom{r-j}{m+1-j} \lambda^{2j-1}(q) \\
&= \alpha_{2m+2}(q) + \langle\langle a \rangle\rangle \alpha_{2m+1}(q).
\end{aligned}$$

De même :

$$\begin{aligned}
&\alpha_{2m+1}(q+\langle\langle a\rangle\rangle)\\
&=\sum_i \binom{r-i}{m-i}\lambda^{2i+1}(q+\langle\langle a\rangle\rangle)\\
&=\sum_i \binom{r-i}{m-i}(\lambda^{2i+1}(q)-\lambda^{2i-1}(q))+\langle\langle a\rangle\rangle\sum_i\binom{r-i}{m-i}(\lambda^{2i}(q)+\lambda^{2i-1}(q))\\
&=\sum_i\left(\binom{r-i}{m-i}-\binom{r-1-i}{m-1-i}\right)\lambda^{2i+1}(q)\\
&+\langle\langle a\rangle\rangle\left(\sum_i\binom{r-i}{m-i}\lambda^{2i}(q)-\sum_i\binom{r-1-i}{m-1-i}\lambda^{2i+1}(q)+2\sum_i\binom{r-1-i}{m-1-i}\lambda^{2i+1}(q)\right)\\
&=\alpha_{2m+1}(q)+\langle\langle a\rangle\rangle(\alpha_{2m}(q)+2\alpha_{2m-1}(q)).
\end{aligned}$$

□

Remarque 1.2.72. En particulier, on retrouve le fait que à r fixé, g_1^d est nul pour $d > 2r$.

Remarque 1.2.73. On rappelle (voir corollaire 1.1.43) que

$$\pi_1^d=\sum_{k=1}^{d}(-1)^{d-k}\binom{d-1}{k-1}\hat{\lambda}^k.$$

En revanche, il est assez pénible d'exprimer les π_n^d en fonction des λ^k, ce qui est cohérent avec le fait que les π_n^d se comportent moins bien en dimension fixée.

On veut également exprimer les $u_d^{(1)}$ et $v_d^{(1)}$ en fonction des invariants de Stiefel-Whitney, et pour cela on propose un formalisme qui s'applique également aux invariants de Witt, donnant ainsi des formules valables dans tous les cas.

Définition 1.2.74. Pour tout $d\in\mathbb{N}$, on définit $P^d : \mathrm{Quad}_n \longrightarrow W$ par :

$$P^d(q)=\sum_{i=0}^{d}(-1)^i\binom{n-i}{d-i}\lambda^i(q).$$

Comme la matrice de passage de (λ^d) à (P^d) est triangulaire avec des 1 sur la diagonale, $(P^d)_{0\leqslant d\leqslant n}$ est aussi une $W(k)$-base de $\mathrm{Inv}(\mathrm{Quad}_n, W)$. Sa définition est motivée par la formule suivante :

Proposition 1.2.75. *Pour tous $a_i\in K^*$, $1\leqslant i\leqslant n$, on a*

$$P^d(\langle a_1,\dots,a_n\rangle)=\sum_{i_1<\cdots<i_d}\langle\langle a_{i_1},\dots,a_{i_d}\rangle\rangle$$

dans $W(K)$. En particulier, $P^d\in\mathrm{Inv}(\mathrm{Quad}_n, I^d)$, et $w_d=e_d\circ P^d$.

Démonstration. Si on développe $\langle\langle a_{i_1}, \ldots, a_{i_d}\rangle\rangle$ on trouve

$$\sum_{I\subset\{i_1,\ldots,i_d\}} (-1)^{|I|} \prod_{i\in I} \langle a_i\rangle$$

et pour I fixé le terme $\prod_{i\in I}\langle a_i\rangle$ apparaît $\binom{n-i}{d-i}$ fois dans $\sum_{i_1<\cdots<i_d}\langle\langle a_{i_1}, \ldots, a_{i_d}\rangle\rangle$. □

On peut donc otenir des énoncés unifiés pour $A = W$ et $A = H$, en posant $h^d = P^d$ dans le premier cas, et $h^d = w_d$ dans le second. On peut alors exprimer nos invariants en fonction des h^d :

Proposition 1.2.76. *Soient $d \in \mathbb{N}$ et $q \in \mathrm{Quad}_n(K)$. Alors (si $A = W$ ou $A = H$) :*

$$f_1^d(q) = \sum_{i=0}^{d} (-1)^i \binom{r-i}{d-i} \{-1\}^{d-i} h^i(q);$$

$$g_1^d(q) = \sum_{i=0}^{d} (-1)^i \binom{r-i-1+\lfloor\frac{d+1}{2}\rfloor}{d-i} \{-1\}^{d-i} h^i(q).$$

Démonstration. On prouve l'énoncé concernant f_1^d ; le cas des g_n^d peut s'en déduire en utilisant la proposition 1.2.36, ou directement en utilisant la même méthode.

On note α_d pour l'invariant défini par le terme de droite de l'équation. A priori ce ne sont pas des invariants de classes de Witt mais simplement des invariants de classes d'isométrie en toute dimension paire.

Il est clair par définition que $\alpha_0 = 1 = f_1^0$. On doit alors montrer que pour tout $d \in \mathbb{N}^*$, $\alpha_d(q) = 0$ si q est hyperbolique, et que

$$\alpha_d(q + \langle\langle a\rangle\rangle) = \alpha_d(q) + \{a\}\alpha_{d-1}(q) \tag{1.2.77}$$

pour tout $a \in K^*$, ce qui montre à la fois que α_d est un invariant de classes de Witt (en prenant $a = 1$), et que $\alpha_d^+ = \alpha_{d-1}$, ce qui permet de conclure par récurrence sur le décalage.

On obtient

$$h^i(r\langle\langle 1\rangle\rangle) = \binom{r}{i} \{-1\}^i \tag{1.2.78}$$

et

$$\begin{aligned} h^i(q + \langle\langle a\rangle\rangle) &= h^i(q) + \{-a\}h^{i-1}(q) \\ &= \big(h^i(q) + \{-1\}h^{i-1}(q)\big) - \{a\}h^{i-1}(q). \end{aligned} \tag{1.2.79}$$

Soit q hyperbolique en dimension $n = 2r$. D'après l'équation (1.2.78),

$$\alpha_d(q) = \left(\sum_{i=0}^{d} (-1)^i \binom{d-r}{d-i} \binom{r}{i}\right) \{-1\}^d = 0$$

en utilisant une formule combinatoire simple.

Alors pour (1.2.77), on pose q de dimension $2r$, et on utilise l'équation (1.2.79) pour trouver :

$$\begin{aligned}
\alpha_d(q+\langle\langle a\rangle\rangle) &= \sum_{i=0}^{d}(-1)^i\binom{r+1-i}{d-i}\{-1\}^{d-i}\left(h^i(q)+\{-1\}h^{i-1}(q)\right)\\
&-\{a\}\sum_{i=0}^{d}(-1)^i\binom{r+1-i}{d-i}\{-1\}^{d-i}h^{i-.1}(q)\\
&=\sum_{i=0}^{d-1}\left((-1)^i\binom{r-i+1}{d-i}+(-1)^{i+1}\binom{r-i}{d-i-1}\right)\{-1\}^{d-i}h^i(q)\\
&+(-1)^dh^d(q)-\{a\}\sum_{i=0}^{d-1}(-1)^{i+1}\binom{r-i}{d-i-1}\{-1\}^{d-i-1}h^i(q)\\
&=\sum_{i=0}^{d}(-1)^i\binom{r-i}{d-i}\{-1\}^{d-i}h^i(q)\\
&+\{a\}\sum_{i=0}^{d-1}(-1)^i\binom{r-i}{d-1-i}\{-1\}^{d-1-i}h^i(q)
\end{aligned}$$

ce qui donne la formule attendue. □

Remarque 1.2.80. Si -1 est un carré dans k, alors $f_1^d = g_1^d = h^d$.

Corollaire 1.2.81. *Pour tout* $m \in \mathbb{N}$, $\mathrm{Inv}(\mathrm{Quad}_{2m}, \mu_2)$ *est le* $H^*(k,\mu_2)$*-module libre sur les* $u_d^{(1)}$ *pour* $0 \leqslant d \leqslant 2m$.

En particulier, tout invariant de Quad_{2m} *peut être étendu en un invariant de* I.

Démonstration. On voit que la matrice de passage entre les $u_d^{(1)}$ et les w_d est triangulaire avec des 1 sur la diagonale. □

Invariants de I^2

Dans [10, thm 20.6], Serre décrit également les invariants cohomologiques de Quad'_{2r}, le foncteur des formes de dimension $2r$ et de discriminant trivial. Spécifiquement, $\mathrm{Inv}(\mathrm{Quad}'_{2r}, \mu_2)$ est la somme directe de l'image de $\mathrm{Inv}(\mathrm{Quad}_{2r}, \mu_2)$ par restriction à Quad'_{2r}, et de $I_{(-1)^r}$ où $I_\delta = \{x \in H^*(k,\mu_2) \mid (\delta)\cup x = 0\}$. L'invariant correspondant à $x \in I_{(-1)^r}$ est b_x qui envoie $\langle a_1,\dots,a_{2r}\rangle$ sur $(a_1,\dots,a_{2r-1})\cup x$.

En particulier, sauf dans des cas très exceptionnels (quand $I_{(-1)^r} = 0$), il existe des invariants de Quad'_{2r} qui ne sont pas la restriction d'un invariant de Quad_{2r}. Or, d'après la remarque 1.2.57, tout invariant de I^2 s'étend à I, donc il existe des invariants de $\mathrm{Quad}'_{2r} = \mathrm{Quad}_{2r} \cap I^2$ qui ne s'étendent pas à I^2 (et l'obstruction est précisément $I_{(-1)^r}$).

1.2.10 Opérations sur la cohomologie

Dans cette partie on s'intéresse spécifiquement au cas des invariants cohomologiques. Il a été observé par Serre qu'on pouvait définir des sortes de carrés divisés sur la cohomologie modulo 2 :

$$\begin{array}{rcl} H^n(K,\mu_2) & \longrightarrow & H^{2n}(K,\mu_2)/(-1)^{n-1}\cup H^{n+1}(K,\mu_2) \\ \sum_i \alpha_i & \longmapsto & \sum_{i<j} \alpha_i \cup \alpha_j. \end{array}$$

Le quotient à droite est nécessaire pour que l'application soit bien définie. De même, on peut définir des puissances divisées de degré supérieur :

$$\begin{array}{rcl} H^n(K,\mu_2) & \longrightarrow & H^{dn}(K,\mu_2)/(-1)^{n-1}\cup H^{(d-1)n+1}(K,\mu_2) \\ \sum_i \alpha_i & \longmapsto & \sum_{i_1<\cdots<i_d} \alpha_{i_1} \cup \cdots \cup \alpha_{i_d}. \end{array}$$

D'un autre côté, Vial ([32]) caractérise les opérations

$$K_n^M(K)/2 \longrightarrow K_*^M(K)/2$$

en fonction de certaines puissances divisées. En utilisant la conjecture de Milnor, cela se traduit par la classification des opérations

$$H^n(K,\mu_2) \longrightarrow H^*(K,\mu_2).$$

De même que pour les opérations de Serre il était nécessaire de considérer un quotient à droite, il faut ici s'attendre à une certaine restriction sur l'ensemble de départ. De fait, l'énoncé de Vial est le suivant :

Proposition 1.2.82 ([32], Thm 2)**.** *Si $n \in \mathbb{N}^*$, le module des opérations $H^n(K,\mu_2) \to H^*(K,\mu_2)$ est le $H^*(k,\mu_2)$-module*

$$H^*(k,\mu_2)\cdot 1 \oplus H^*(k,\mu_2)\cdot \mathrm{Id} \oplus \bigoplus_{d\in\mathbb{N}} \mathrm{Ker}(\tau_n)\cdot\gamma_d$$

où $\tau_n : H^*(k,\mu_2) \longrightarrow H^*(k,\mu_2)$ est défini par $\tau_n(x) = (-1)^{n-1}\cup x$ et si $a \in \mathrm{Ker}(\tau_n)$, alors

$$a\cdot\gamma_d\left(\sum_{1\leqslant i\leqslant r} x_i\right) = a\cdot \sum_{i_1<\cdots<i_d} x_{i_1}\cup\cdots\cup x_{i_d}$$

où les x_i sont des symboles.

Dans les deux cas, il est nécessaire pour que les opérations soient bien définies d'annuler certaines puissances de (-1), que ce soit par un noyau à gauche ou un conoyau à droite.

Les invariants $u_{nd}^{(n)}$ peuvent être vus comme des relevés de ces opérations de puissances divisées au niveau de I^n. Le phénomène remarquable qui se produit alors est que ces opérations y sont définies sans aucune restriction.

De plus, on peut sans difficulté retrouver la classification de Vial en utilisant notre analyse des invariants de I^n : les opérations sur $H^n(K,\mu_2)$ ne sont rien d'autre que les invariants dans $\mathrm{Inv}(I^n,\mu_2)$ qui vérifient la condition

$$\alpha(q+\varphi)=\alpha(q) \quad \forall q\in I^n(K), \varphi\in \mathrm{Pf}_{n+1}(K). \tag{1.2.83}$$

On peut maintenant utiliser le fait que, d'après le corollaire 1.2.55, $u_{nk}^{(n)}(\varphi)$ vaut 1 si $k=0$, $(-1)^{n-1}\cup e_{n+1}(\varphi)$ si $k=2$, et 0 autrement ; couplé à la formule d'addition, on obtient

$$u_{nd}^{(n)}(q+\varphi)=u_{nd}^{(n)}(q)+(-1)^{n-1}\cup e_{n+1}(\varphi)\cup u_{n(d-2)}^{(n)}(q).$$

En écrivant α comme combinaison des $u_{nd}^{(n)}$, on obtient

$$\alpha(q+\varphi)=\alpha(q)+(-1)^{n-1}\cup e_{n+1}(\varphi)\cup \alpha^{++}(q).$$

De là, α vérifie la condition (1.2.83) si et seulement si $(-1)^{n-1}\cup\alpha^{++}=0$, ce qui revient précisément à dire que le coefficient devant $u_{nd}^{(n)}$ pour $d\geqslant 2$ est dans le noyau de τ_n, et on retrouve exactement l'énoncé de Vial.

1.2.11 Invariants de formes semi-factorisées

Dans [9, def 20.8], Garibaldi définit un invariant cohomologique sur les formes de rang 12 dans I^3 de la façon suivante : toute telle forme peut s'écrire $q=\langle\langle c\rangle\rangle q'$ où $q'\in I^2(K)$, et on pose $a_5(q)=e_5(\langle\langle c\rangle\rangle\pi_2^2(q))$ (en utilisant notre notation). Bien entendu, l'ingrédient non trivial est que $\langle\langle c\rangle\rangle\pi_2^2(q)$ est indépendant de la décomposition de q.

On souhaite, notamment en vue d'application aux algèbres à involution, couvrir ce type de construction. Notamment, cet invariant a_5 peut se définir sur tout élément de I^3 qui s'écrit comme le produit d'une 1-forme de Pfister et d'un élément de I^2 ; il est donc naturel de travailler au niveau des classes de Witt.

De façon plus générale, on pose :

Définition 1.2.84. On pose $I^{n,r}(K)=\{\varphi\cdot q\,|\,\varphi\in\mathrm{Pf}_r(K),\ q\in I^{n-r}(K)\}$, pour tous $n\in\mathbb{N}^*$ et $0\leqslant r<n$.

En particulier, $I^{n,0}=I^n$.

Proposition-définition 1.2.85. *Il existe un unique morphisme de $A(k)$-modules filtrés*

$$\begin{array}{rccc}\Delta^{n,r}: & \mathrm{Inv}_{norm}(I^{n,r},A) & \longrightarrow & \mathrm{Inv}_{norm}(I^{n-r},A)\\ & \alpha & \longmapsto & \alpha^{(r)},\end{array}$$

injectif et de degré $-r$, tel que

$$\alpha(\varphi\cdot q)=f_r(\varphi)\cdot\alpha^{(r)}(q)$$

pour tous $\alpha\in\mathrm{Inv}_{norm}(I^{n,r},A)$, $\varphi\in\mathrm{Pf}_r(K)$ et $q\in I^{n-r}(K)$.

Démonstration. Soient $\alpha \in \mathrm{Inv}(I^{n,r}, A)$ et $q \in I^{n-r}(K)$. On peut alors définir un invariant sur K des r-formes de Pfister par $\varphi \mapsto \alpha(\varphi \cdot q)$. D'après la condition (iv) sur A, il y a d'uniques $x(q), y(q) \in A(K)$ tels que

$$\alpha(\varphi \cdot q) = x(q) + f_n(\varphi) \cdot y(q)$$

et par unicité ce sont des invariants de Witt de I^{n-r}, avec $x = \alpha(0)$ constant. On pose $\alpha^{(r)} := y$. $\square$

Comme $I^{n,r} \subset I^n$, on peut se poser la question de la restriction des invariants de I^n à $I^{n,r}$. On a le résultat élémentaire suivant :

Proposition 1.2.86. *Soient $n \in \mathbb{N}^*$ et $0 \leqslant r < n$. Alors pour tout $d \in \mathbb{N}^*$,*

$$\Delta^{n,r}(f_n^d) = \{-1\}^{r(d-1)} f_{n-r}^d.$$

Cette proposition découle immédiatement, par récurrence sur le décalage, de la proposition suivante, qui est indépendamment intéressante.

Proposition 1.2.87. *Soit $\alpha \in \mathrm{Inv}_{norm}(I^n, A)$. Alors*

$$(\alpha^{(r)})^+ = \{-1\}^r (\alpha^+)^{(r)}.$$

Démonstration. Soit $\alpha \in \mathrm{Inv}_{norm}(I^n, A)$. Si $\varphi \in \mathrm{Pf}_r(K)$, $q \in I^{n-r}(K)$ et $\psi \in \mathrm{Pf}_{n-r}(K)$, on a

$$\alpha(\varphi(q+\psi)) = \alpha(\varphi q) + f_n(\varphi\psi)\alpha^+(\varphi q) = f_r(\varphi)\alpha^{(r)}(q) + \{-1\}^r f_n(\varphi\psi)(\alpha^+)^{(r)}(q)$$

ainsi que

$$\alpha(\varphi(q+\psi)) = f_r(\varphi)\alpha^{(r)}(q+\psi) = f_r(\varphi)\alpha^{(r)}(q) + f_r(\varphi) f_{n-r}(\psi)(\alpha^{(r)})^+(q)$$

d'où la formule. $\square$

La question qu'on peut alors se poser est : l'application $\Delta^{n,r}$ est-elle surjective ? Autrement dit, tout invariant de I^{n-r} permet-il de définir un invariant de $I^{n,r}$ comme on l'a illustré avec a_5 ?

On ne dispose pas de réponse en toute généralité, mais on peut quand même traiter un cas particulier :

Proposition 1.2.88. *Pour tout $n \geqslant 2$, $\Delta^{n,1}$ est un isomorphisme.*

Démonstration. Il suffit de montrer que f_{n-1}^d est dans l'image pour tout $d \geqslant 1$. On doit donc montrer que $\langle\langle a \rangle\rangle q \mapsto \{a\} f_{n-1}^d(q)$ est un invariant bien défini, autrement dit que si $q, q' \in I^{n-1}(K)$ et $a, b \in K^*$, alors $\langle\langle a \rangle\rangle q = \langle\langle b \rangle\rangle q'$ implique que $\{a\} f_{n-1}^d(q) = \{b\} f_{n-1}^d(q')$.

Supposons d'abord que $a = b$. Alors d'après [7, thm 41.3],

$$q - q' = \sum_{i\in J} \langle\langle c_i\rangle\rangle \varphi_i$$

où c_i est représenté par $\langle\langle a\rangle\rangle$. On peut alors raisonner par récurrence sur $|J|$, et on est donc réduit au cas où $q' = q + \langle\langle c\rangle\rangle\varphi$ avec c représenté par $\langle\langle a\rangle\rangle$.

Or pour tout $k \in \mathbb{N}^*$, $f_{n-1}^k(\langle\langle c\rangle\rangle\varphi)$ est un multiple de $\{c\}$, et donc $\{a\}f_{n-1}^k(\langle\langle c\rangle\rangle\varphi) = 0$. De là :

$$\{a\}f_{n-1}^d(q') = \{a\}\sum_{k=0}^{d} f_{n-1}^k(q) f_{n-1}^{d-k}(\langle\langle c\rangle\rangle\varphi) = \{a\}f_{n-1}^d(q).$$

Supposons maintenant $a \neq b$. Alors d'après l'appendice B de [9], on a

$$\langle\langle a\rangle\rangle q = \langle\langle a\rangle\rangle\varphi = \langle\langle b\rangle\rangle\varphi = \langle\langle b\rangle\rangle q'$$

avec $\varphi = \sum_{i\in J}\langle\lambda_i\rangle\langle\langle c_i\rangle\rangle$, et c_i représenté par $\langle\langle ab\rangle\rangle$.

La discussion précédente montre que $\{a\}f_{n-1}^d(q) = \{a\}f_{n-1}^d(\varphi)$ et $\{b\}f_{n-1}^d(q) = \{b\}f_{n-1}^d(\varphi)$, donc il suffit de montrer que $\{a\}f_{n-1}^d(\varphi) = \{b\}f_{n-1}^d(\varphi)$ pour tout φ ayant une décomposition comme ci-dessus, ce qui constitue précisément l'énoncé du lemme ci-après. $\square$

Lemme 1.2.89. *Soient $a, b \in K^*$, et soit $q \in I^n(K)$ de la forme*

$$q = \sum_{i=1}^{r}\langle\lambda_i\rangle\langle\langle c_i\rangle\rangle$$

où c_i est représenté par $\langle\langle ab\rangle\rangle$. Alors pour tout $d \geqslant 1$,

$$\{a\}f_n^d(q) = \{b\}f_n^d(q).$$

Démonstration. On se ramène au cas où $A = W$, puisque si

$$\langle\langle a\rangle\rangle\pi_n^d(q) = \langle\langle b\rangle\rangle\pi_n^d(q)$$

alors on peut appliquer f_{d+1} pour obtenir le résultat voulu. Dans le cas $A = W$, on montre une propriété plus forte : on suppose seulement $q \in I(K)$ (ce qui a un sens puisqu'on peut appliquer π_n^d à n'importe quel élément de $GW(K)$).

On raisonne par récurrence sur r. Si $r = 0$, le résultat est trivial puisque $q = 0$. Pour le cas $r = 1$: on écrit $\pi_n^d = \sum_{k=1}^d x_k\pi_1^k$ avec $x_k \in \mathbb{Z}$, et $q = \langle\lambda\rangle\langle\langle c\rangle\rangle$; alors par hypothèse $\langle\langle a, c\rangle\rangle = \langle\langle b, c\rangle\rangle$ donc le résultat vaut clairement pour $k = 1$, et si $k \geqslant 2$:

$$\begin{aligned}\langle\langle a\rangle\rangle\pi_1^k(\langle\lambda\rangle\langle\langle c\rangle\rangle) &= (-1)^k\langle\langle a\rangle\rangle\langle\langle -1\rangle\rangle^{k-2}\langle\langle \lambda, c\rangle\rangle\\ &= (-1)^k\langle\langle b\rangle\rangle\langle\langle -1\rangle\rangle^{k-2}\langle\langle \lambda, c\rangle\rangle\\ &= \langle\langle b\rangle\rangle\pi_1^k(\langle\lambda\rangle\langle\langle c\rangle\rangle)\end{aligned}$$

et donc on conclut par combinaison linéaire.

Si le résultat vaut jusqu'à $r \geqslant 1$, on écrit $q = q_0 + \langle\lambda\rangle\langle\langle c\rangle\rangle$, où q_0 correspond à une écriture de longueur r et c est représenté par $\langle\langle ab\rangle\rangle$. Alors par hypothèse de récurrence on a

$$\langle\langle a\rangle\rangle\pi_n^k(q_0) = \langle\langle b\rangle\rangle\pi_n^k(q_0), \quad \langle\langle a\rangle\rangle\pi_n^k(\langle\lambda\rangle\langle\langle c\rangle\rangle) = \langle\langle b\rangle\rangle\pi_n^k(\langle\lambda\rangle\langle\langle c\rangle\rangle)$$

donc

$$\begin{aligned}\langle\langle a\rangle\rangle\pi_n^d(q) &= \sum_{k=0}^{d}\langle\langle a\rangle\rangle\pi_n^k(q_0)\pi_n^{d-k}(\langle\lambda\rangle\langle\langle c\rangle\rangle)\\ &= \sum_{k=0}^{d}\langle\langle b\rangle\rangle\pi_n^k(q_0)\pi_n^{d-k}(\langle\lambda\rangle\langle\langle c\rangle\rangle)\\ &= \langle\langle b\rangle\rangle\pi_n^d(q).\end{aligned}$$

□

1.3 Tours d'invariants cohomologiques

On peut réinterpréter les invariants cohomologiques qu'on a construit dans le cadre suivant : on part de I, et on a un certain nombre d'invariants, dont e_1 (qui peut d'ailleurs être caractérisé par le fait que c'est l'invariant normalisé non nul de plus petit degré). On considère alors l'ensemble des formes sur lesquelles cet invariant s'annule, à savoir I^2. On a également classifié les invariants sur I^2, parmi lesquels e_2 (qui peut encore être caractérisé par sa minimalité parmi les invariants normalisés), et on regarde encore les formes sur lesquelles il s'annule, soit I^3. Et ainsi de suite.

On peut donc voir nos constructions comme définissant des *tours d'invariants* :

Définition 1.3.1. Soit F et H deux foncteurs sur une catégorie $\mathbf{C}$ à valeurs dans $\mathbf{Set}$ et $\mathbf{Set}_*$ respectivement (on note 0 le point base des ensembles pointés). Une tour d'invariant sur F à valeurs dans H est une suite finie $(\alpha_1, \dots, \alpha_r)$ telle que α_i est un invariant de F_i à valeurs dans H, où $F_1 = F$, et $F_{i+1}(X) = \{x \in F_i(X) \,|\, \alpha_i(x) = 0\}$.

Dans notre cas, un invariant cohomologique de I^n peut être vu comme s'insérant dans une tour d'invariants $(e_1, e_2, \dots, e_{n-1}, \alpha)$ sur I.

On peut alors se poser la question des tours d'invariants cohomologiques générales sur I. Notamment, si $\alpha \in \mathrm{Inv}(I^n, \mu_2)$, quels sont les invariants définis sur $I_\alpha(K) = \{q \in I^n(K) \,|\, \alpha(q) = 0\}$? On a déjà la restriction des invariants définis sur I^n, mais en général (comme nous le suggère l'exemple $\alpha = e_n$) il y en a bien d'autres.

On utilise l'idée suivante : supposons que α soit homogène de degré d. On peut choisir un invariant $\hat{\alpha} \in \mathrm{Inv}(I^n, I^d)$ tel que $\alpha = e_n \circ \hat{\alpha}$ (il est bien défini modulo $\mathrm{Inv}(I^n, I^{d+1})$). Alors pour $q \in I^n(K)$, $\alpha(q) = 0$ si et seulement si $\hat{\alpha}(q) \in I^{d+1}(K)$. On peut alors définir $\beta(\hat{\alpha}(q))$ pour tout $\beta \in \mathrm{Inv}(I^{d+1}, \mu_2)$, ce qui définit un invariant de I_α. Bien évidemment, cet invariant dépend du choix de $\hat{\alpha}$. En revanche, on montre que l'ensemble des invariants qu'on obtient ainsi en faisant varier β ne dépend pas de ce choix.

Si on veut itérer la construction, on se heurte à une difficulté : si α_2 est un invariant de I_α, on ne sait pas garantir que α_2 se relève à un invariant de Witt. À défaut, on va se restreindre à ce type d'invariant :

Définition 1.3.2. Soit F un foncteur de $\mathbf{Field}_{/k}$. On dit qu'un invariant $\alpha \in \mathrm{Inv}^d(F, \mu_2)$ est *spécial* s'il existe $\widetilde{\alpha} \in \mathrm{Inv}(F, I^d)$ tel que $\alpha = e_d \circ \widetilde{\alpha}$.

Un invariant $\alpha \in \mathrm{Inv}(F, \mu_2)$ est spécial si toutes ses composantes homogènes le sont. On note $\mathrm{Inv}_s(F, \mu_2)$ le module des invariants spéciaux.

Une tour d'invariant est spéciale si tous les invariants de la tour le sont.

Remarque 1.3.3. D'après le corollaire 1.2.41, tout invariant cohomologique de I^n est spécial.

On peut alors préciser notre construction :

Proposition 1.3.4. *Soit F un foncteur de $\mathbf{Field}_{/k}$ vers $\mathbf{Set}$, et soit $\alpha \in \mathrm{Inv}_s^d(F, \mu_2)$ un invariant spécial. On pose $F_\alpha(K) = \{x \in F(K) \mid \alpha(x) = 0\}$. On choisit $\hat{\alpha} \in \mathrm{Inv}(F, I^d)$ tel que $\alpha = e_d \circ \hat{\alpha}$, et on pose*

$$\begin{array}{rccc} \Phi_{\hat{\alpha}} : & \mathrm{Inv}(I^{d+1}, \mu_2) & \longrightarrow & \mathrm{Inv}_s(F_\alpha, \mu_2) \\ & \beta & \longmapsto & \beta \circ \hat{\alpha}. \end{array}$$

Alors la sous-algèbre de $\mathrm{Inv}_s(F_\alpha, \mu_2)$ engendrée par $\mathrm{Inv}_s(F, \mu_2)$ et par l'image de $\Phi_{\hat{\alpha}}$ ne dépend pas du choix de $\hat{\alpha}$.

Démonstration. Soit $\hat{\alpha}'$ un autre relevé de α. Il suffit alors de montrer que $\Phi_{\hat{\alpha}'}(u_{m(d+1)}^{(d+1)})$ est dans l'algèbre engendrée par $\mathrm{Inv}(F, \mu_2)$ et l'image de $\Phi_{\hat{\alpha}}$.

Soit $\gamma \in \mathrm{Inv}(F, I^{d+1})$ tel que $\hat{\alpha}' = \hat{\alpha} + \gamma$. On a pour tout $q \in F_\alpha(K)$:

$$\begin{aligned} \Phi_{\hat{\alpha}'}(u_{m(d+1)}^{(d+1)}) &= u_{m(d+1)}^{(d+1)} \circ (\hat{\alpha} + \gamma) \\ &= \sum_{k=0}^{m} \left(u_{(m-k)(d+1)}^{(d+1)} \circ \gamma\right) \cup \left(u_{k(d+1)}^{(d+1)} \circ \hat{\alpha}\right) \\ &= \sum_{k=0}^{m} \gamma_{m-k} \cup \Phi_{\hat{\alpha}}(u_{k(d+1)}^{(d+1)}) \end{aligned}$$

où $\gamma_k = u_{k(d+1)}^{(d+1)} \circ \gamma$ est un invariant spécial de F. $\square$

Comme cette construction donne des invariants qui sont eux-mêmes spéciaux par définition, on peut itérer la construction pour définir des tours d'invariants (spéciaux).

Dans le cas qui nous intéresse, on part de $F = I$. On part de n'importe quel invariant homogène α de I, qui est forcément spécial. Le procédé ci-dessus donne alors toute une algèbre d'invariants spéciaux de I_α (qui est canoniquement déterminée par α). Si on en choisit un, disons β, on peut encore utilise ce procédé pour construire des invariants (spéciaux) de $I_{\alpha,\beta}$, et ainsi de suite.

Il se pose alors naturellement un certain nombre de questions : obtient-on ainsi toutes les tours d'invariants de I ? Toutes les tours d'invariants spéciales ?

Chapitre 2

Anneaux de Witt mixtes

L'objectif de ce chapitre est de définir des anneaux commutatifs $\widetilde{GW}(A,\sigma)$ et $\widetilde{W}(A,\sigma)$ pour tout algèbre à involution (A,σ) de première espèce, qui contiennent les classes d'isométrie des formes ε-hermitiennes sur (A,σ). Précisément, on note $GW^{\varepsilon}(A,\sigma)$ le groupe de Grothendieck-Witt des formes ε-hermitiennes sur (A,σ), et $GW^{\pm}(A,\sigma) = GW(A,\sigma) \oplus GW^{-}(A,\sigma)$, et alors

$$\widetilde{GW}(A,\sigma) = GW^{\pm}(K) \oplus GW^{\pm}(A,\sigma).$$

L'idée est qu'on peut définir à travers une équivalence de Morita canonique (on développe au préalable un formalisme de théorie de Morita hermitienne dans la première partie) le produit de deux formes ε-hermitiennes, mais que l'élément résultant est alors une forme bilinéaire sur K ; on peut donc définir une structure stable par produit en rassemblant ces deux types d'éléments dans un seul ensemble. On montre dans le théorème 2.2.8 qu'on obtient effectivement une structure d'anneau commutatif en procédant de la sorte. On définit également un analogue de l'anneau de Witt $\widetilde{W}(A,\sigma)$ en quotientant par les formes hyperboliques.

On définit également sur $\widetilde{GW}(A,\sigma)$ une structure de pré-λ-anneau (ou d'anneau grec selon la terminologie du premier chapitre), voir la proposition 2.3.22. Un point important est que toutes nos constructions sont naturellement compatibles avec les équivalences de Morita hermitiennes (voir la proposition 2.3.23). On étudie en particulier le cas des algèbres de quaternions munies de leur involution canonique, ainsi que le cas des algèbres déployées. Il est à noter que ce cas des algèbres de quaternions avait en réalité déjà été traité par Lewis dans [20], bien qu'il ne donne pas de preuve de l'associativité de l'anneau (qui n'a rien d'une évidence) et ne construise pas les λ-opérations. Cependant les arguments de Lewis sont basés sur l'existence de la forme norme des algèbres de quaternions, qui contrairement à la forme trace d'involution ne se généralise pas au cas d'une algèbre à involution quelconque.

Enfin, la dernière partie met en place une filtration « fondamentale » $\widetilde{I}^n(A,\sigma)$ de $\widetilde{W}(A,\sigma)$, par analogie avec le cas des formes quadratiques (voir la définition

2.4.3), et définit par analogie avec la conjecture de Minor une « cohomologie mixte » $\widetilde{H}^n(A,\sigma)$ comme le gradué associé. Cette filtration et ce gradué sont alors étudiés, avec une dichotomie importante entre les cas déployé et non déployé.

2.1 Théorie de Morita hermitienne

La théorie de Morita classique admet un analogue hermitien bien connu (voir par exemple [16, §9]). On peut encoder cette théorie dans une structure assez compacte, qu'on appelera le *2-groupe de Brauer hermitien* de K. Il s'agit d'une catégorie monoïdale symétrique, qui a de plus de bonnes propriétés d'inversibilité. On n'utilisera pas la notion de 2-groupe dans la suite, et on ne rentrera donc pas dans les détails de la définition, mais on se servira en revanche librement du formalisme des catégories monoïdales, qui permet une unification et une simplification des notations.

2.1.1 Le 2-groupe de Brauer

En guise de motivation et d'introduction, on commence par décrire la version non hermitienne, qui correspond à la théorie usuelle des algèbres simples centrales et du groupe de Brauer. On définit donc une certaine catégorie $\mathbf{Br}(K)$ qu'on appelle le 2-groupe de Brauer de K :

— Les objets sont les algèbres simples centrales sur K. Le produit monoïdal de $\mathbf{Br}(K)$ est simplement le produit tensoriel des algèbres sur K, l'objet unité étant l'algèbre triviale K.

— Si A et B sont deux algèbres simples centrales sur K, un morphisme de B vers A dans $\mathbf{Br}(K)$ est une classe d'isomorphisme de B-A-bimodule U sur K, (donc une classe d'isomorphisme de $B\otimes_K A^{op}$-module) tel que $B \simeq \mathrm{End}_A(U)$, ce qui est équivalent à $A \simeq \mathrm{End}_B(U)$ (où comme on en a l'habitude, si U est un B-module à gauche $\mathrm{End}_B(U)$ désigne l'algèbre opposée à l'algèbre d'endomorphismes « naïve », de sorte à ce que $\mathrm{End}_B(U)$ agisse naturellement à *droite* sur U).

  La composition est donnée par le produit tensoriel des modules : la composition de $C \xrightarrow{U} B$ et $B \xrightarrow{V} A$ est $C \xrightarrow{U\otimes_B V} A$. L'identité de A est A lui-même vu canoniquement comme un A-A-bimodule. L'action du produit monoïdal sur les morphismes est celle qu'on attend : si on dispose de $B \xrightarrow{U} A$ et $B' \xrightarrow{V} A'$ alors on obtient $B \otimes_K B' \xrightarrow{U\otimes_K V} A \otimes_K A'$.

On voit aisément le lien avec la théorie de Morita usuelle : il existe un morphisme entre A et B si et seulement si A et B sont Brauer-équivalentes, ce qu'on notera $A \sim B$, et la donnée d'un morphisme spécifique correspond à une donnée de Morita. Les propriétés d'associativité et de symétrie requises correspondent aux propriétés usuelles des produits tensoriels.

Remarque 2.1.1. On peut observer que la définition s'étend manifestement pour tout anneau commutatif R à une catégorie $\mathbf{Mor}(R)$ dont les objets sont des R-algèbres quelconques, et les morphismes des bimodules quelconques.

Le fait de restreindre la définition comme on l'a fait correspond à considérer des éléments « inversibles », ce qui justifie la terminologie de « groupe ». La question de l'inversibilité des objets dans les catégories monoïdales est délicate (voir par exemple [3]) ; on évitera donc de se perdre dans des considérations générales, et on donne simplement les notations qui nous seront utiles.

Si U est un B-A-bimodule, alors $\mathrm{Hom}_A(U,A)$ et $\mathrm{Hom}_B(U,B)$ sont naturellement munis d'une structure de A-B-bimodule, définie respectivement par $(a\varphi b)(x) = a\varphi(bx)$ et $(a\varphi b)(x) = \varphi(xa)b$. Alors on a un isomorphisme naturel

$$\begin{array}{rcl} \mathrm{Hom}_B(U,B) & \overset{\sim}{\longrightarrow} & \mathrm{Hom}_A(U,A) \\ \varphi & \longmapsto & (u \mapsto (v \mapsto \varphi(v)u)) \end{array} \tag{2.1.2}$$

où on utilise l'identification $A \simeq \mathrm{End}_B(U)$. On considèrera cet isomorphisme comme une identification, et on utilise U^* pour dénoter l'un ou l'autre de ces bimodules, indifféremment. On dispose donc d'un B-B-bimodule $U \otimes_A U^*$, et d'un A-A-bimodule $U^* \otimes_B U$. Un résultat classique de théorie de Morita affirme alors que si U est un bimodule simple, alors U^* aussi et on a des isomorphismes naturels de bimodules $U \otimes_A U^* \simeq B$ et $U^* \otimes_B U \simeq A$. On peut donc dire que U^* est un inverse de U dans $\mathbf{Br}(K)$, puisque la composition de U et U^* (vus comme morphismes) dans un sens comme dans l'autre est isomorphe (donc égale) à l'identité.

Si A est un objet de $\mathbf{Br}(K)$, alors l'algèbre opposée A^{op} est un inverse faible de A pour la structure monoïdale, au sens où on dispose d'un isomorphisme naturel $A \otimes_K A^{op} \simeq K$ dans $\mathbf{Br}(K)$, donnée par le bimodule A muni à gauche de l'action « sandwich » de $A \otimes_K A^{op}$, et à droite de l'action tautologique de K.

2.1.2 Le 2-groupe de Brauer hermitien

On présente maintenant la version hermitienne de la construction précédente, qu'on note $\mathbf{Br}_h(K)$.

- Les objets sont les algèbres à involution (A,σ) de première espèce sur K. Le produit monoïdal de $\mathbf{Br}_h(K)$ est encore le produit tensoriel sur K, à savoir $(A,\sigma) \otimes (B,\tau) = (A \otimes_K B, \sigma \otimes \tau)$, et l'objet unité est (K, Id).
- Un morphisme de (B,τ) vers (A,σ) est une classe d'isométrie de B-A-bimodule simple *ε-hermitien*, à savoir un couple (U,h) où U est un B-A-bimodule simple, et $h : U \times U \longrightarrow A$ est une forme ε-hermitienne (où $\varepsilon = \pm 1$) relativement à σ telle que à travers l'identification $B = \mathrm{End}_A(U)$ l'involution adjointe de h soit τ.

La composition de $(C,\theta) \xrightarrow{(U,h)} (B,\tau)$ et $(B,\tau) \xrightarrow{(V,g)} (A,\sigma)$ est

$$(C,\theta) \xrightarrow{(U\otimes_B V,f)} (A,\sigma)$$

où

$$f(u\otimes v, u'\otimes v') = g(v, h(u,u')v'). \tag{2.1.3}$$

Si h est ε-hermitienne et g ε'-hermitienne, alors f est $\varepsilon\varepsilon'$-hermitienne. L'identité de (A,σ) est le A-A-bimodule A, muni de

$$\begin{array}{rccc} h_A: & A\times A & \longrightarrow & A \\ & (x,y) & \longmapsto & \sigma(x)y \end{array}. \tag{2.1.4}$$

L'action du produit monoïdal sur les morphismes est donnée naturellement par le produit tensoriel.

On a de façon évidente un foncteur canonique (« d'oubli ») de $\mathbf{Br}_h(K)$ vers $\mathbf{Br}(K)$, qui est monoïdal.

Le fait que la composition des morphismes dans $\mathbf{Br}_h(K)$ soit bien définie et associative est une simple reformulation de la théorie de Morita hermitienne telle qu'elle est présentée dans [16].

Remarque 2.1.5. Il existe un (iso)morphisme entre (A,σ) et (B,τ) si et seulement si $A\sim B$ (voir par exemple [17, 4.2]) ; si σ et τ sont de même type, le bimodule donnant le morphisme sera hermitien, et anti-hermitien si σ et τ sont de type différent. De plus, tandis que dans $\mathbf{Br}(K)$ on a au plus un morphisme entre deux objets, ici si $A\sim B$ deux morphismes entre A et B correspondent à deux modules hermitiens semblables, et en général non isomorphes.

Les propriétés d'inversibilité dans $\mathbf{Br}_h(K)$ sont en un certain sens plus fortes que dans $\mathbf{Br}(K)$, reflétant un phénomène d'auto-dualité caractéristique des théories hermitiennes et des involutions.

En effet, comme inverse faible de (A,σ), on peut choisir (A,σ) lui-même : on dispose d'une équivalence $(A\otimes_K A, \sigma\otimes\sigma)\simeq(K,\mathrm{Id})$ donnée par le bimodule A, où l'action de K à droite est tautologique, et $A\otimes_K A$ agit à gauche par l'action sandwich tordue par σ :

$$(a\otimes b)\cdot x = ax\sigma(b). \tag{2.1.6}$$

La structure hermitienne, correspondant en l'occurence à une forme bilinéaire symétrique, est donnée par la forme trace d'involution (voir [17, 11.1])

$$\begin{array}{rccc} T_\sigma: & A\times A & \longrightarrow & K \\ & (x,y) & \longmapsto & \mathrm{Trd}_A(\sigma(x)y) \end{array}. \tag{2.1.7}$$

Quant aux inverses de morphismes, si $(B,\tau) \xrightarrow{(U,h)} (A,\sigma)$ est un morphisme dans $\mathbf{Br}_h(K)$, il admet comme inverse $({}^\sigma U^\tau, h^*)$, où ${}^\sigma U^\tau$ est le A-B-bimodule donné par U muni de l'action tordue

$$a\cdot u\cdot b = \tau(b)\cdot u\cdot\sigma(a), \tag{2.1.8}$$

et
$$h^* : {}^\sigma U^\tau \times {}^\sigma U^\tau \longrightarrow B$$
est définie par
$$h^*(x,y)u = xh(y,u). \tag{2.1.9}$$

Remarque 2.1.10. Dans la lignée de la remarque 2.1.1, On peut étendre cette définition à une catégorie $\mathbf{Mor}_h(R,\iota)$ où (R,ι) est un anneau commutatif muni d'une involution, auquel cas les objets sont les R-algèbres A munies d'une involution σ telles que $\sigma_{|R} = \iota$. On perd alors les propriétés d'inversibilité, mais on obtient toujours une catégorie monoïdale. Notons que dans ce contexte une forme peut être ε-hermitienne sur (A,σ) pour tout $\varepsilon \in Z(A)^*$ tel que $\varepsilon\sigma(\varepsilon) = 1$.

Si on dispose de deux morphismes f et f' vers (A,σ) correspondant à des modules ε-hermitiens, on peut former la somme directe orthogonale $f \oplus f'$, qui est encore un morphisme vers (A,σ) correspondant à un module ε-hermitien.

Lemme 2.1.11. *Soient f, f' morphismes dans $\mathbf{Br}_h(K)$ vers (B,τ) de même signe, et soit $g : (B,\tau) \longrightarrow (A,\sigma)$. Alors*
$$(f \oplus f') \circ g = (f \circ g) \oplus (f' \circ g).$$

Démonstration. Cela découle directement de la définition à partir du produit tensoriel. □

2.2 L'anneau de Witt mixte

2.2.1 Anneau de Grothendieck-Witt mixte

Définition

On définit d'abord l'analogue de l'anneau de Grothendieck-Witt, qui est en un sens plus fondamental que l'anneau de Witt, et sur lequel on définira plus tard les opération λ^d. Comme dans le cas de l'anneau de Grothendieck-Witt usuel, on le définit à partir d'un certain semi-anneau, qui dans notre cas est gradué. Ce semi-anneau n'est pas le plus intéressant en soi, mais il est pratique de l'utiliser pour les preuves car tous les éléments sont représentés par des modules hermitiens, puis de transférer les résultats à l'anneau.

Définition 2.2.1. Soit (A,σ) une algèbre à involution de première espèce sur K. On définit les monoïdes additifs commutatifs suivants, tous munis de la somme orthogonale : $SGW(K)$ est constitué des classes d'isométrie de modules bilinéaires symétriques non dégénérés sur K, $SGW^-(K)$ est constitué des classes d'isométrie de modules bilinéaires alternés, $SGW^+(A,\sigma)$ des classes d'isométrie de modules hermitiens (à droite) sur (A,σ), et $SGW^-(A,\sigma)$ des classes d'isométrie de modules anti-hermitiens.

On pose alors

$$\widetilde{SGW}(A,\sigma) = SGW(K) \oplus SGW^-(K) \oplus SGW^+(A,\sigma) \oplus SGW^-(A,\sigma)$$

ainsi que son groupe de Grothendieck, qu'on appelle le groupe de Grothendieck-Witt *mixte* de (A,σ) :

$$\widetilde{GW}(A,\sigma) = GW(K) \oplus GW^-(K) \oplus GW^+(A,\sigma) \oplus GW^-(A,\sigma).$$

Pour l'instant $\widetilde{SGW}(A,\sigma)$ est seulement un monoïde additif, et $\widetilde{GW}(A,\sigma)$ un $GW(K)$-module. Notons que comme les modules ε-hermitiens sur une algèbre à involution vérifient le théorème de décomposition de Witt, $\widetilde{SGW}(A,\sigma)$ est un monoïde à simplification, et donc le morphisme naturel $\widetilde{SGW}(A,\sigma) \longrightarrow \widetilde{GW}(A,\sigma)$ est injectif.

Graduation

On définit le groupe

$$\Gamma = \{+,-,o,s\}, \tag{2.2.2}$$

isomorphe au groupe de Klein $(\mathbb{Z}/2\mathbb{Z})^2$ de sorte que $+$ soit l'élément neutre. Les symboles sont à interpréter respectivement comme *symétrique*, *alterné*, *orthogonal* et *symplectique*, correspondant aux différents types de formes bilinéaires et d'involutions.

On munit alors $\widetilde{SGW}(A,\sigma)$ d'une Γ-graduation : la composante $\widetilde{SGW}(A,\sigma)_+$ est $SGW(K)$, la composante $\widetilde{SGW}(A,\sigma)_-$ est $SGW^-(K)$. La composante $\widetilde{SGW}(A,\sigma)_o$ est $SGW^+(A,\sigma)$ si σ est orthogonale et $SGW^-(A,\sigma)$ si σ est symplectique, de sorte que si un élément de $\widetilde{SGW}(A,\sigma)_o$ représente un certain A-module ε-hermitien (U,h), alors l'involution adjointe σ_h est orthogonale. Inversement, l'involution adjointe d'un élément de $\widetilde{SGW}(A,\sigma)_s$ est symplectique.

Cette graduation s'étend de façon unique à $\widetilde{GW}(A,\sigma)$ (voir lemme 1.1.24).

Produit

On veut maintenant donner une structure de semi-anneau gradué à $\widetilde{SGW}(A,\sigma)$. Il suffit de définir le produit et de vérifier distributivité et associativité composante par composante vis-à-vis de la Γ-graduation : on veut des applications $\widetilde{SGW}(A,\sigma)_{\gamma_1} \times \widetilde{SGW}(A,\sigma)_{\gamma_2} \longrightarrow \widetilde{SGW}(A,\sigma)_{\gamma_1+\gamma_2}$ pour tous $\gamma_1,\gamma_2 \in \Gamma$.

Comme les éléments de $\widetilde{SGW}(A,\sigma)_{\gamma_i}$ correspondent à des modules ε_i-hermitiens sur une certaine algèbre à involution (A_i,σ_i) (qui vaut (A,σ) si γ_i est o ou s, et (K,Id) si γ_i est $+$ ou $-$), donc à des morphismes vers (A_i,σ_i) dans $\mathbf{Br}_h(K)$, on peut déjà utiliser la structure monoïdale de $\mathbf{Br}_h(K)$ pour définir un morphisme vers $\widetilde{(A_1 \otimes_K A_2, \sigma_1 \otimes \sigma_2)}$. Si un des A_i est égal à K, on obtient alors bien un élément de $\widetilde{SGW}(A, \sigma)$.

Il reste donc à traiter le cas $\gamma_1, \gamma_2 \in \{o, s\}$. Dans ce cas on obtient un morphisme vers $(A \otimes_K A, \sigma \otimes \sigma)$; or on dispose d'un isomorphisme canonique dans $\mathbf{Br}_h(K)$ de cet objet vers (K, Id), à savoir l'espace bilinéaire symétrique (A, T_σ) (voir (2.1.7)), qui nous permet de transporter par composition des morphismes vers $(A \otimes_K A, \sigma \otimes \sigma)$ sur des morphismes vers (K, Id), et donc des éléments de $\widetilde{SGW}(A, \sigma)$. On explicite cette définition :

Définition 2.2.3. Soient (U, h) et (V, g) des modules respectivement ε-hermitien et ε'-hermitien à droite sur (A, σ). Alors $(U, h) \cdot (V, g)$, qu'on notera souvent $h \cdot g$, est le K-espace bilinéaire donné par

$$\begin{array}{rrcl} h \cdot g : & W \times W & \longrightarrow & K \\ & ((u \otimes v) \otimes a, (u' \otimes v') \otimes a') & \longmapsto & \mathrm{Trd}_A\left(\sigma(a) h(u, u') a' \sigma(g(v, v'))\right) \end{array} \tag{2.2.4}$$

où $W = (U \otimes_K V) \otimes_{A \otimes_K A} A$.

La définition vient de la formule (2.1.3), sachant que

$$h(u, u') \otimes g(v, v') \cdot a' = h(u, u') a' \sigma(g(v, v')).$$

Lemme 2.2.5. *Le produit ainsi défini est commutatif et biadditif, et s'étend de façon unique en un produit commutatif et distributif sur $\widetilde{SGW}(A, \sigma)$ et $\widetilde{GW}(A, \sigma)$.*

Démonstration. Soient (V_i, h_i) modules ε_i-hermitiens sur (A, σ), pour $i = 1, 2, 3$. Alors

$$(V_1 \otimes_K V_2, h_1 \otimes h_2) \simeq (V_2 \otimes_K V_1, h_2 \otimes h_1)$$

donc par composition avec T_σ on obtient la commutativité. On a également

$$((V_1, h_1) \oplus (V_2, h_2)) \otimes_K (V_3, h_3) \simeq (V_1 \otimes_K V_3, h_1 \otimes h_3) \oplus (V_2 \otimes_K V_3, h_1 \otimes h_3)$$

donc on obtient la biadditivité par application du lemme 2.1.11. On a finalement bien construit un produit sur toutes les composantes de $\widetilde{SGW}(A, \sigma)$, et la commutativité et la distributivité sont vérifiées composantes par composantes. L'assertion sur $\widetilde{GW}(A, \sigma)$ s'en déduit par propriété universelle du groupe de Grothendieck. □

Associativité

Par utilisation successive de l'isomorphisme canonique entre $(A \otimes_K A, \sigma \otimes \sigma)$ et (K, Id), on obtient pour tout $d \in \mathbb{N}$ un isomorphisme dans $\mathbf{Br}_h(K)$ de $(A, \sigma)^{\otimes d}$ vers (A, σ) si d est impair, et vers (K, Id) si d est pair. A priori, cet isomorphisme dépend de la façon dont on regroupe les termes, et il faut vérifier une certaine condition d'associativité.

On aura besoin par la suite d'étudier le rôle de l'élément de Goldman (voir [17, 3.5]) dans notre contexte.

Lemme 2.2.6. *On considère l'action tordue à gauche de $A\otimes_K A$ sur le K-espace vectoriel A, donnée par $(a\otimes b)\cdot x = ax\sigma(b)$. Alors l'élément de Goldman $g\in A\otimes_K A$ vérifie, pour tout $x\in A$, $(\mathrm{Id}\otimes\sigma)(g)\cdot x = \mathrm{Trd}_A(x)$ et $g\cdot x = \varepsilon\sigma(x)$ où $\varepsilon = 1$ si σ est orthogonale et -1 si elle est symplectique. Par ailleurs, $(\sigma\otimes\sigma)(g) = g$, et donc $(\sigma\otimes\mathrm{Id})(g)\cdot x = \mathrm{Trd}_A(x)$ et $(\sigma\otimes\sigma)(g)\cdot x = \varepsilon\sigma(x)$.*

Démonstration. La première formule est essentiellement la définition de g, puisqu'il est défini pour agir comme la trace pour l'action sandwich non tordue. Pour la deuxième, on se ramène au cas où A est déployée. Alors $A = \mathrm{End}_K(V)$ pour un certain espace vectoriel V, et $\sigma = \sigma_b$ où b est ε-symétrique. On dispose alors de l'isomorphisme canonique $A\simeq V\otimes V$, tel que $(v\otimes w)(v'\otimes w') = b(w,v')v\otimes w'$ et $\sigma(v\otimes w) = \varepsilon w\otimes v$. Soit (e_i) une base de V, et (e_i^*) sa base duale pour b (si σ est orthogonale, on peut prendre pour (e_i) une base orthogonale, auquel cas $e_i = e_i^*$). Alors $g = \sum_{i,j} e_i\otimes e_j^*\otimes e_j\otimes e_i^*$ (voir la preuve de [17, 3.6]), donc

$$\begin{aligned} g\cdot(v\otimes w) &= \sum_{i,j}(e_i\otimes e_j^*)\cdot(v\otimes w)\cdot\varepsilon(e_i^*\otimes e_j)\\ &= \varepsilon\sum_{i,j} b(e_j^*,v)b(w,e_i^*)e_j\otimes e_j\\ &= \left(\sum_i b(e_i^*,w)e_i\right)\otimes\left(\sum_j b(e_j^*,v)e_j\right)\\ &= w\otimes v.\end{aligned}$$

Pour la dernière affirmation, on renvoie à [17, 10.19]. □

Proposition 2.2.7. *L'isomorphime $\varphi^{(d)}_{(A,\sigma)}$ de $(A,\sigma)^{\otimes d}$ vers (A,σ) ou (K,Id) dans $\mathbf{Br}_h(K)$ est canonique et ne dépend pas de l'ordre de regroupement des termes.*

Démonstration. Clairement, comme pour toute forme d'associativité il suffit de le vérifier pour trois termes. Il faut donc montrer qu'on a un carré commutatif dans $\mathbf{Br}_h(K)$

$$\begin{array}{ccc} (A\otimes_K A\otimes_K A,\sigma\otimes\sigma\otimes\sigma) & \longrightarrow & (K\otimes A,\mathrm{Id}\otimes\sigma)\\ \downarrow & & \downarrow\\ (A\otimes K,\sigma\otimes\mathrm{Id}) & \longrightarrow & (A,\sigma)\end{array}$$

ce qui revient à construire une isométrie entre les bimodules hermitiens $(A\otimes_K A,h_1)$ et $(A\otimes_K A,h_2)$ où l'action de $A\otimes_K A\otimes_K A$ à gauche et de A à droite est dans le premier cas

$$(a\otimes b\otimes c)\cdot_1(x\otimes y)\cdot_1 d = (ax\sigma(b))\otimes(cyd)$$

et dans le deuxième cas

$$(a\otimes b\otimes c)\cdot_2(x\otimes y)\cdot_2 d = (axd)\otimes(by\sigma(c))$$

et où les formes hermitiennes sont

$$h_1(x \otimes y, x' \otimes y') = \mathrm{Trd}_A(\sigma(x)x')\sigma(y)y'$$

et

$$h_2(x \otimes y, x' \otimes y') = \mathrm{Trd}_A(\sigma(y)y')\sigma(x)x'.$$

Soit $g \in A \otimes_K A$ l'élément de Goldman ; si $g = \sum_i a_i \otimes b_i$, on définit notre isométrie de h_1 vers h_2 par

$$\begin{array}{rccl} \varphi : & A \otimes_K A & \longrightarrow & A \otimes_K A \\ & x \otimes y & \longmapsto & \sum_i (xa_iy) \otimes \sigma(b_i). \end{array}$$

Notons que $1 \otimes 1$ est envoyé sur $g' = (\mathrm{Id} \otimes \sigma)(g)$. Comme le bimodule $A \otimes_K A$ est engendré par l'élément $1 \otimes 1$ pour les deux action définies ci-dessus, cela suffit à caractériser φ, mais il faut vérifier que g' est un élément admissible pour l'image de $1 \otimes 1$, ce qui revient à vérifier qu'on a bien défini un morphisme de bimodules. On a

$$\begin{aligned} \varphi\left((a \otimes b \otimes c) \cdot_1 (x \otimes y) \cdot_1 d\right) &= \varphi\left((ax\sigma(b)) \otimes (cyd)\right) \\ &= \sum_i (ax\sigma(b)a_icyd) \otimes \sigma(b_i) \end{aligned}$$

et

$$\begin{aligned} (a \otimes b \otimes c) \cdot_2 \varphi(x \otimes y) \cdot_2 d &= \sum_i (a \otimes b \otimes c) \cdot_2 (xa_iy) \otimes \sigma(b_i) \cdot_2 d \\ &= \sum_i (axa_iyd) \otimes (b\sigma(b_i)\sigma(c)). \end{aligned}$$

On est donc amené à montrer que

$$\sum_i \sigma(b)a_ic \otimes \sigma(b_i) = \sum_i a_i \otimes b\sigma(b_i)\sigma(c),$$

ce qui revient à

$$(\mathrm{Id} \otimes \sigma)((\sigma(b) \otimes 1)g(c \otimes 1)) = (\mathrm{Id} \otimes \sigma)((1 \otimes c)g(1 \otimes \sigma(b)))$$

qui découle des propriétés de l'élément de Goldman (voir [17, 3.6], ou le lemme 2.3.2). Donc φ définit bien un morphisme de bimodules, et comme g' est inversible c'est bien un isomorphisme.

Il reste à vérifier que φ réalise une isométrie de h_1 vers h_2. On a

$$\begin{aligned}
h_2(\varphi(x \otimes y), \varphi(x' \otimes y')) &= \sum_{i,j} h_2((xa_iy) \otimes \sigma(b_i), (x'a_jy') \otimes \sigma(b_j)) \\
&= \sum_{i,j} \mathrm{Trd}_A(b_i\sigma(b_j))\sigma(y)\sigma(a_i)\sigma(x)x'a_jy' \\
&= \sum_{i,j,k} \sigma(y)\sigma(a_i)\sigma(x)x'a_jy'a_kb_i\sigma(b_j)b_k \\
&= \varepsilon \sum_{i,k} \sigma(y)\sigma(a_i)\sigma(x)x'\sigma(b_i)\sigma(a_k)\sigma(y')b_k \\
&= \varepsilon\sigma(y)\,\mathrm{Trd}_A(\sigma(x)x')\varepsilon y' \\
&= h_1(x \otimes y, x' \otimes y')
\end{aligned}$$

en utilisant les relations du lemme 2.2.6.

□

En conséquence :

Théorème 2.2.8. *L'application $\widetilde{SGW}(A,\sigma) \times \widetilde{SGW}(A,\sigma) \longrightarrow \widetilde{SGW}(A,\sigma)$ définie dans la partie précédente munit $\widetilde{SGW}(A,\sigma)$ d'une structure de semi-anneau commutatif gradué, et induit sur $\widetilde{GW}(A,\sigma)$ une structure de $GW(K)$-algèbre commutative graduée.*

Démonstration. Par propriété universelle des groupes de Grothendieck (voir notamment le lemme 1.1.24), il suffit de montrer les affirmations sur $\widetilde{SGW}(A,\sigma)$. Tout ce qu'il reste à démontrer pour ça est l'associativité, qui se vérifie composante par composante pour la Γ-graduation.

On pose donc pour $1 \leqslant i \leqslant 3$ (U_i, h_i) module ε_i-hermitien à droite sur (A_i, σ_i), où (A_i, σ_i) est soit (A, σ) soit (K, Id). Par construction du produit, $(h_1 \cdot h_2) \cdot h_3$ et $h_1 \cdot (h_2 \cdot h_3)$ sont chacun obtenus à partir d'un module $\varepsilon_1\varepsilon_2\varepsilon_3$-hermitien sur $(A_1 \otimes A_2 \otimes A_3, \sigma_1 \otimes \sigma_2 \otimes \sigma_3)$, transporté par composition à travers certains isomorphismes dans $\mathbf{Br}_h(K)$. De plus ces deux modules hermitiens sont isométriques par associativité du produit tensoriel. Il faut donc montrer qu'on a un carré commutatif dans $\mathbf{Br}_h(K)$

$$\begin{tikzcd}
(A_1 \otimes A_2 \otimes A_3, \sigma_1 \otimes \sigma_2 \otimes \sigma_3) \arrow[r] \arrow[d] & (B_1 \otimes A_3, \tau_1 \otimes \sigma_3) \arrow[d] \\
(A_1 \otimes B_2, \sigma_1 \otimes \tau_2) \arrow[r] & (C, \theta)
\end{tikzcd}$$

où les (B_i, τ_i) et (C, θ) sont soit (A, σ) soit (K, Id) selon la nature des (A_i, σ_i), et les morphismes sont les identifications canoniques de la forme $(A,\sigma)\otimes(K,\mathrm{Id}) \simeq (A,\sigma)$, $(K,\mathrm{Id}) \otimes (K,\mathrm{Id}) \simeq (K,\mathrm{Id})$ ou $(A,\sigma) \otimes (A,\sigma) \simeq (K,\mathrm{Id})$.

Le cas où un des A_i vaut K est simplement une conséquence du fait que (K, Id) est une identité pour la structure monoïdale de $\mathbf{Br}_h(K)$, et le cas où tous les A_i sont A se ramène exactement à la proposition 2.2.7. $\square$

Par construction, pour toute extension L/K on a un morphisme de $GW(K)$-algèbres graduées $\widetilde{GW}(A,\sigma) \longrightarrow \widetilde{GW}(A_L,\sigma_L)$.

Exemple 2.2.9. Dans $\widetilde{GW}(A,\sigma)$, on a certains éléments privilégiés qui sont les formes diagonales $\langle a\rangle$ où $a \in A$ est un élément inversible symétrique ou antisymétrique. On notera parfois $\langle a\rangle_\sigma$ ou $\langle a\rangle_A$ s'il y a un risque de confusion. Si A est à division, ces formes engendent additivement $GW^{\pm}(A,\sigma)$. Alors par construction du produit :

$$\langle a\rangle \cdot \langle b\rangle = ((x,y) \mapsto \mathrm{Trd}_A(\sigma(x)ay\sigma(b)))\,.$$

En particulier, on dispose de $\langle 1\rangle_\sigma \in GW^+(A,\sigma)$, qui est l'identité de A dans $\mathbf{Br}_h(K)$. Alors

$$\langle a\rangle \cdot \langle 1\rangle = T_{\sigma,a}$$

où $T_{\sigma,a}$ est la forme bilinéaire définie dans [17, §11] par

$$T_{\sigma,a}(x,y) = \mathrm{Trd}_A(\sigma(x)ay). \tag{2.2.10}$$

Notamment, $\langle 1\rangle_\sigma^2 = T_\sigma$, la forme trace d'involution.

2.2.2 Anneau de Witt mixte

On peut également former l'équivalent de l'anneau de Witt, qui est généralement plus facilement manipulable, bien qu'il ait moins de structure.

Définition 2.2.11. Soit (A,σ) une algèbre à involution de première espèce sur K. On définit le $W(K)$-module

$$\widetilde{W}(A,\sigma) = W(K) \oplus W^+(A,\sigma) \oplus W^-(A,\sigma).$$

On munit $\widetilde{W}(A,\sigma)$ d'une Γ-graduation analogue à celle de $\widetilde{GW}(A,\sigma)$, avec une composante nulle pour l'élément $- \in \Gamma$ (puisque $W^-(K) = 0$).

On dispose manifestement d'un morphisme surjectif canonique de $GW(K)$-modules gradués $\widetilde{GW}(A,\sigma) \to \widetilde{W}(A,\sigma)$ donné par la projection naturelle sur chaque composante.

Proposition 2.2.12. *Le noyau de l'application canonique $\widetilde{GW}(A,\sigma) \to \widetilde{W}(A,\sigma)$ est l'idéal* $\mathrm{Hyp}(A,\sigma)$ *engendré par les formes hyperboliques dans chaque composante. En particulier, $\widetilde{W}(A,\sigma)$ est muni d'une unique structure d'anneau telle que l'application précédente soit un morphisme d'anneau.*

Démonstration. Par définition des divers groupes de Witt concernés, le noyau est constitué des éléments dont toutes les composantes sont hyperboliques. Il s'agit donc de montrer que ce sous-module est un idéal, ce qui revient à montrer que le produit d'une forme hyperbolique avec n'importe quelle forme est hyperbolique. À part pour les composantes de la forme $GW^-(K)$, le résultat est clair puisque toute forme hyperbolique est de la forme $h \perp \langle -1 \rangle h$, donc le produit avec n'importe quel élément x est de la forme $(xh) \perp \langle -1 \rangle (xh)$, donc est hyperbolique. Pour le cas des formes bilinéaires alternées (qui sont toutes hyperboliques) on peut se ramener au cas d'un plan, qui a pour matrice $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, et donc son produit avec une forme h est de la forme $\begin{pmatrix} 0 & h \\ \langle -1 \rangle h & 0 \end{pmatrix}$ ce qui donne une forme hyperbolique. □

Le morphisme d'extension des scalaires est manifestement compatible avec la projection, de sorte que pour toute extension L/K on a un morphisme de $W(K)$-algèbres graduées $\widetilde{W}(A, \sigma) \longrightarrow \widetilde{W}(A_L, \sigma_L)$.

2.2.3 Équivalences de Morita

Les structures d'anneau sur $\widetilde{GW}(A, \sigma)$ et $\widetilde{W}(A, \sigma)$ sont définies à partir du produit tensoriel grâce aux isomorphismes $\varphi^{(d)}_{(A,\sigma)}$ décrits par la proposition 2.2.7. On va établir la compatibilité de ces isomorphismes avec les équivalences de Morita hermitiennes.

Proposition 2.2.13. *Soit $f : (B, \tau) \longrightarrow (A, \sigma)$ un morphisme dans $\mathbf{Br}_h(K)$ (correspondant à une équivalence de Morita hermitienne). Pour tout $d \in \mathbb{N}$ on a alors un carré commutatif dans $\mathbf{Br}_h(K)$*

$$\begin{array}{ccc} (B^{\otimes d}, \tau^{\otimes d}) & \xrightarrow{\varphi^{(d)}_{(B,\tau)}} & (B, \tau) \\ \big\downarrow{\scriptstyle f^{\otimes d}} & & \big\downarrow{\scriptstyle f} \\ (A^{\otimes d}, \sigma^{\otimes d}) & \xrightarrow{\varphi^{(d)}_{(A,\sigma)}} & (A, \sigma) \end{array}$$

si d est impair, et

$$\begin{array}{ccc} (B^{\otimes d}, \tau^{\otimes d}) & \xrightarrow{\varphi^{(d)}_{(B,\tau)}} & (K, \mathrm{Id}) \\ \big\downarrow{\scriptstyle f^{\otimes d}} & & \big\downarrow{\scriptstyle \mathrm{Id}} \\ (A^{\otimes d}, \sigma^{\otimes d}) & \xrightarrow{\varphi^{(d)}_{(A,\sigma)}} & (K, \mathrm{Id}) \end{array}$$

si d est pair.

Démonstration. Si $d = 0$, le carré est entièrement constitué d'égalités, et si $d = 1$ les flèches verticales sont identiques et les flèches horizontales sont des égalités. En utilisant la proposition 2.2.7, on voit qu'on peut se ramener par récurrence au cas $d = 2$, et il faut donc construire une isométrie entre les modules correspondant à $\varphi^{(2)}_{(A,\sigma)} \circ f^{\otimes 2}$ et $\varphi^{(2)}_{(A,\sigma)}$.

On définit alors le morphisme de $(B \otimes_K B)$-K-bimodule suivant, où f correspond au bimodule ε-hermitien (V, h) :

$$\begin{array}{rrcl} \psi : & (V \otimes_K V) \otimes_{A \otimes_K A} A & \longrightarrow & B = \mathrm{End}_A(V) \\ & (v \otimes w) \otimes a & \longmapsto & \varphi_h(va \otimes w). \end{array}$$

où $\varphi_h : V \otimes_K V \to B$ correspond l'identification canonique $V \otimes_A {}^{\tau}V \to B$ (voir [17, 5.1]), et est donnée par

$$\varphi_h(v \otimes w)(x) = vh(w, x).$$

Pour montrer que c'est une isométrie, on doit établir une égalité entre d'une part

$$\begin{aligned} &\mathrm{Trd}_B\left(\tau\left(\psi((v \otimes w) \otimes a)\right) \cdot \psi(((v' \otimes w') \otimes b))\right) \\ &= \mathrm{Trd}_B\left(\tau(\varphi_h(va \otimes w)) \cdot \varphi_h(v'b \otimes w')\right) \end{aligned}$$

et d'autre part

$$\begin{aligned} &\mathrm{Trd}_A\left(\sigma(a)(h \otimes h)(v \otimes w, v' \otimes w') \cdot b\right) \\ &= \varepsilon\,\mathrm{Trd}_A(\sigma(a)h(v, v')bh(w', w)). \end{aligned}$$

Or en appliquant successivement les formules du théorème [17, 5.1], on obtient :

$$\begin{aligned} &\mathrm{Trd}_B\left(\tau(\varphi_h(va \otimes w)) \cdot \varphi_h(v'b \otimes w')\right) \\ &= \varepsilon\,\mathrm{Trd}_B\left(\varphi_h(w \otimes va) \cdot \varphi_h(v'b \otimes w')\right) \\ &= \varepsilon\,\mathrm{Trd}_B\left(\varphi_h(wh(va, v'b) \otimes w')\right) \\ &= \varepsilon\,\mathrm{Trd}_A\left(h(w', wh(va, v'b))\right) \\ &= \varepsilon\,\mathrm{Trd}_A\left(h(w', w)\sigma(a)h(v, v')b\right). \end{aligned}$$

□

Cette compatibilité entraîne un comportement remarquable pour les algèbres $\widetilde{GW}$ et $\widetilde{W}$: soient (A, σ) et (B, τ) munies d'un morphisme $f : (B, \tau) \to (A, \sigma)$ dans $\mathbf{Br}_h(K)$; on peut alors définir une application

$$f_* : \widetilde{SGW}(B, \tau) \longrightarrow \widetilde{SGW}(A, \sigma)$$

comme l'identité sur les composantes $SGW^{\pm}(K)$, et la composition avec f sur les composantes $SGW^{\pm}(B, \tau)$, en interprétant les modules ε-hermitiens comme des morphismes vers (B, τ) dans $\mathbf{Br}_h(K)$.

Théorème 2.2.14. *L'association $(A,\sigma) \mapsto \widetilde{SGW}(A,\sigma)$ et $f \mapsto f_*$ définit un foncteur de $\mathbf{Br}_h(K)$ vers la catégorie des semi-anneaux Γ-gradués. En particulier, $\mathbf{Br}_h(K)$ étant un groupoïde, f_* est un isomorphisme de semi-anneaux.*

De plus, ce foncteur induit naturellement des foncteurs $(A,\sigma) \mapsto \widetilde{GW}(A,\sigma)$ et $(A,\sigma) \mapsto \widetilde{W}(A,\sigma)$ de $\mathbf{Br}_h(K)$ vers respectivement les $GW(K)$-algèbres graduées et les $W(K)$-algèbres graduées.

Démonstration. Les énoncés concernant $\widetilde{GW}$ et $\widetilde{W}$ découlent directement de celui à propos de $\widetilde{SGW}$, puisqu'on vérifie facilement que f_* préserve les sommes orthogonales (voir 2.1.11) et les formes hyperboliques.

D'un point de vue ensembliste, il est clair par définition que $(g \circ f)_* = g_* \circ f_*$. Le fait que f_* préserve la graduation est évident pour les composantes $+$ et $-$, et pour les composantes o et s cela vient de notre choix de graduation : si f correspond à un module hermitien, alors σ et τ sont de même type, et la composition avec f préserve le signe des modules, alors que si f correspond à un module anti-hermitien, alors σ et τ sont de type différent, et la composition avec f inverse le signe des modules. Dans tous les cas la graduation est préservée.

Il faut donc montrer que f_* préserve le produit. On se ramène à des modules ε_i-hermitiens sur (B_i,τ_i), qui vaut soit (B,τ) soit (K,Id), et on doit montrer que le diagramme naturel suivant commute :

$$\begin{array}{ccc}
GW^{\varepsilon_1}(B_1,\tau_1) \times GW^{\varepsilon_2}(B_2,\tau_2) & \longrightarrow & GW^{\varepsilon\varepsilon_1}(A_1,\sigma_1) \times GW^{\varepsilon\varepsilon_2}(A_2,\sigma_2) \\
\downarrow & & \downarrow \\
GW^{\varepsilon_1\varepsilon_2}(B_1 \otimes_K B_2, \tau_1 \otimes \tau_2) & \longrightarrow & GW^{\varepsilon_1\varepsilon_2}(A_1 \otimes_K A_2, \sigma_1 \otimes \sigma_2) \\
\downarrow & & \downarrow \\
GW^{\varepsilon_1\varepsilon_2}(B_3,\tau_3) & \longrightarrow & GW^{\varepsilon_1\varepsilon_2}(A_3,\sigma_3).
\end{array}$$

Le carré du haut commute toujours par propriété du produit tensoriel, et celui du bas ne pose pas de problème si un des B_i vaut K. On doit donc montrer que le carré du bas commute dans la configuration suivante :

$$\begin{array}{ccc}
GW^{\varepsilon_1\varepsilon_2}(B \otimes_K B, \tau \otimes \tau) & \longrightarrow & GW^{\varepsilon_1\varepsilon_2}(K) \\
\downarrow & & \downarrow \\
GW^{\varepsilon_1\varepsilon_2}(A \otimes_K A, \sigma \otimes \sigma) & \longrightarrow & GW^{\varepsilon_1\varepsilon_2}(K)
\end{array}$$

ce qui est une conséquence directe de la proposition 2.2.13. □

Ce théorème implique notamment qu'à isomorphisme près, $\widetilde{GW}(A,\sigma)$ et $\widetilde{W}(A,\sigma)$ ne dépendent que de la classe de Brauer de A. En revanche, comme on prend en compte les formes hermitiennes et anti-hermitiennes, ils ne dépendent pas du type de l'involution. En particulier, on peut toujours se ramener au cas d'une algèbre à division, munie d'une involution du type que l'on veut.

Exemple 2.2.15. Dans la situation du théorème, si $f : (B,\tau) \longrightarrow (A,\sigma)$ est représenté par (V,h), alors $f_*(\langle 1\rangle_\tau) = h$ (où $\langle 1\rangle_\tau$ est la forme diagonale, voir exemple 2.2.9). Par conséquent, si $h \in GW^\varepsilon(A,\sigma)$ représente un module ε-hermitien non nul, alors il existe un isomorphisme $\widetilde{GW}(B,\tau) \xrightarrow{\sim} \widetilde{GW}(A,\sigma)$ qui envoie $\langle 1\rangle_\tau$ sur h. On a le même résultat pour $h \in W^\varepsilon(A,\sigma)$ non nul quelconque (tous les éléments de $W^\varepsilon(A,\sigma)$ sont représentés par des modules ε-hermitiens). On peut donc dans une certaine mesure toujours se ramener à étudier des formes du type $\langle 1\rangle_\tau$.

Exemple 2.2.16. Soient h et h' formes respectivement ε-hermitienne et ε'-hermitienne sur (A,σ), de même dimension. D'après l'exemple précédent on peut se ramener par équivalence de Morita hermitienne à $h = \langle 1\rangle_\tau$, sur (B,τ). Alors par hypothèse sur la dimension h' est de la forme $\langle b\rangle_\tau$ avec $b \in B$, et donc $h \cdot h' = T_{\tau,b}$ (voir exemple 2.2.9). Ces formes traces d'involution « tordues » étudiées dans [17, §11] sont donc l'exemple universel de produit de deux formes de même dimension.

2.2.4 Algèbres déployées

Dans le cas où A est déployée, le théorème 2.2.14 permet de se ramener (mais de façon non canonique) à $(A,\sigma) = (K,\mathrm{Id})$. Or dans ce cas, on a par définition

$$\widetilde{GW}(K) := \widetilde{GW}(K,\mathrm{Id}) = GW(K) \oplus GW^-(K) \oplus GW(K) \oplus GW^-(K) \quad (2.2.17)$$

donc les différentes composantes ne sont plus toutes distinguables. On a en réalité

$$\widetilde{GW}(K) = GW^\pm(K)[\mathbb{Z}/2\mathbb{Z}]$$

où $GW^\pm(K) = GW(K) \oplus GW^-(K)$ est l'anneau habituel des formes bilinéaires, et où $R[G]$ désigne l'anneau de groupe de G si R est un anneau commutatif. De même,

$$\widetilde{W}(K) := \widetilde{W}(K,\mathrm{Id}) = W(K)[\mathbb{Z}/2\mathbb{Z}]. \quad (2.2.18)$$

Pour $R = GW^\pm(K)$ ou $W(K)$ (ou de façon générale pour un anneau commutatif), on dispose d'un isomorphisme tautologique

$$\Phi : R \oplus R \xrightarrow{\sim} R[\mathbb{Z}/2\mathbb{Z}] \quad (2.2.19)$$

d'inverse $\Phi^{-1} = (\pi_0,\pi_1)$ où π_0,π_1 sont les projections sur les composantes homogènes. Cependant, on va plutôt utiliser un autre isomorphisme qui sera plus naturellement compatible avec les opérations qu'on souhaite exploiter. Notons $\Phi(x,0) = x_{(0)}$ et $\Phi(0,x) = x_{(1)}$. On pose

$$\begin{array}{rccc} \Delta : & R & \longrightarrow & R[\mathbb{Z}/2\mathbb{Z}] \\ & x & \longmapsto & x_{(0)} - x_{(1)} \end{array} \quad (2.2.20)$$

qu'on appelle *plongement diagonal* de R dans $R[\mathbb{Z}/2\mathbb{Z}]$. On définit alors

$$\begin{array}{rccc} \Psi : & R \oplus R & \xrightarrow{\sim} & R[\mathbb{Z}/2\mathbb{Z}] \\ & (x,y) & \longmapsto & x_{(0)} + \Delta(y), \end{array} \tag{2.2.21}$$

qui vérifie $\Psi^{-1} = (\pi_0 + \pi_1, -\pi_1)$. Notons que $\Phi(x,0) = \Psi(x,0) = x_{(0)}$.

On a alors de façon immédiate :

$$\Phi(x_1,y_1) \cdot \Phi(x_2,y_2) = \Phi(x_1x_2 + y_1y_2, x_1y_2 + x_2y_1) \tag{2.2.22}$$

et (en utilisant $\Delta(x) \cdot \Delta(y) = 2\Delta(xy)$)

$$\Psi(x_1,y_1) \cdot \Psi(x_2,y_2) = \Psi(x_1x_2, x_1y_2 + x_2y_1 + 2y_1y_2). \tag{2.2.23}$$

2.2.5 Algèbres de quaternions

On peut également donner une description concrète de l'anneau de Witt pour une algèbre de quaternion. Soit donc $(Q,^-)$ une algèbre de quaternions sur K, munie de son involution canonique. Il suffit pour décrire $\widetilde{GW}(Q,^-)$ de donner les produits des formes diagonales élémentaires $\langle z\rangle_Q$ où z est soit un scalaire soit un quaternion pur (voir exemple 2.2.9).

On commence par définir une certaine forme de Pfister qui sera importante dans la suite :

Proposition-définition 2.2.24. *Soient $z_1, \ldots, z_r$ des quaternions purs dans Q^*, avec $r \geqslant 2$. Il existe alors une unique r-forme de Pfister $\varphi_{z_1,\ldots,z_r}$ telle que dans $W(K)$:*

$$\varphi_{z_1,\ldots,z_r} = \langle\langle z_1^2, \ldots, z_r^2\rangle\rangle - \langle\langle -1\rangle\rangle^{r-2} n_Q.$$

Si deux des z_i anti-commutent, $\varphi_{z_1,\ldots,z_r}$ est hyperbolique. De plus, si $z_{r+1}, \ldots, z_{r+s}$ sont des quaternions purs, alors

$$\varphi_{z_1,\ldots,z_r}\langle\langle z_{r+1}^2, \ldots, z_{r+s}^2\rangle\rangle = \varphi_{z_1,\ldots,z_{r+s}}.$$

Démonstration. On a $\langle\langle z_{r+1}^2, \ldots, z_{r+s}^2\rangle\rangle \cdot \langle\langle -1\rangle\rangle^{r-2} n_Q = \langle\langle -1\rangle\rangle^{r+s-2} n_Q$, d'où la dernière affirmation.

De là, pour montrer que $\varphi_{z_1,\ldots,z_r}$ est une r-forme de Pfister, il suffit de montrer que $\langle\langle z_1^2, z_2^2\rangle\rangle - n_Q$ est une 2-forme de Pfister. Or si z_0 est un quaternion pur qui anti-commute avec z_1, on a dans $W(K)$:

$$\begin{aligned} \langle\langle z_1^2, z_2^2\rangle\rangle - n_Q &= \langle\langle z_1^2, z_2^2\rangle\rangle + n_Q - \langle\langle z_2^2\rangle\rangle n_Q \\ &= \langle\langle z_1^2, z_2^2\rangle\rangle + \langle\langle z_1^2, z_0^2\rangle\rangle - \langle\langle z_1^2, z_0^2, z_2^2\rangle\rangle \\ &= \langle\langle z_1^2, z_2^2 z_0^2\rangle\rangle. \end{aligned}$$

Si z_i et z_j anti-commutent, alors $\langle\langle z_i^2, z_j^2\rangle\rangle = n_Q$, donc $\langle\langle z_1^2, \ldots, z_r^2\rangle\rangle = \langle\langle -1, \ldots, -1\rangle\rangle n_Q$. $\square$

Remarque 2.2.25. Dans cet énoncé, on parle de forme de Pfister au sens usuel, c'est-à-dire que $\varphi_{z_1,\dots,z_r}$ est bien une forme quadratique de dimension 2^r, et non un élément de $\hat{I}^r(K)$.

Proposition 2.2.26. *Soient $z_1, z_2 \in Q$ des quaternions purs. Alors on a dans $\widetilde{GW}(Q, ^-)$:*

$$\langle z_1 \rangle \cdot \langle z_2 \rangle = \langle -\operatorname{Trd}_Q(z_1 z_2)\rangle \varphi_{z_1,z_2}$$

où si z_1 et z_2 anti-commutent on sous-entend que la forme est hyperbolique.

Si $a, b \in K^*$, alors :

$$\langle a \rangle_Q \cdot \langle b \rangle_Q = \langle 2ab \rangle n_Q.$$

Démonstration. D'après l'exemple 2.2.9, $\langle z_1 \rangle \cdot \langle z_2 \rangle = b$ où b est la forme bilinéaire symétrique sur le K-espace vectoriel Q telle que $b(x, y) = \operatorname{Trd}_Q(xz_1\overline{yz_2})$.

Soit z_0 un quaternion pur qui anti-commute avec z_1 et z_2 (ce qui existe toujours, et si z_1 et z_2 ne commutent pas on peut prendre la partie pure de z_1z_2). On voit facilement que $\varphi_{z_1,z_2} = \langle\langle z_2^2 z_0^2, z_1^2 \rangle\rangle$ puisque ce sont des 2-formes de Pfister avec le même invariant e_2 (ou voir la preuve de la proposition précédente). Dans la base $(1, z_0, z_1, z_1z_0)$ la matrice de b est :

$$\begin{pmatrix} -Tr_Q(z_1z_2) & Tr_Q(z_1z_2z_0) & 0 & 0 \\ Tr_Q(z_1z_2z_0) & -z_0^2 Tr_Q(z_1z_2) & 0 & 0 \\ 0 & 0 & z_1^2 Tr_Q(z_1z_2) & -z_1^2 Tr_Q(z_1z_2z_0) \\ 0 & 0 & -z_1^2 Tr_Q(z_1z_2z_0) & z_1^2 z_0^2 Tr_Q(z_1z_2) \end{pmatrix}.$$

Soit Δ le déterminant du bloc supérieur gauche. Alors b est équivalente à

$$\langle -Tr_Q(z_1z_2)\rangle\langle 1, \Delta, -z_1^2, -z_1^2\Delta\rangle = \langle -Tr_Q(z_1z_2)\rangle\langle\langle -\Delta, z_1^2\rangle\rangle$$

au sens où b est hyperbolique si $Tr_Q(z_1z_2) = 0$, et sinon b est isométrique à la forme ci-dessus. On va donc montrer que $\langle\langle -\Delta, z_1^2\rangle\rangle = \varphi_{z_1,z_2}$.

On a

$$\Delta = z_0^2 Tr_Q(z_1z_2)^2 - Tr_Q(z_1z_2z_0)^2$$

donc on peut distinguer deux cas : si z_1 et z_2 commutent (ce qui revient à dire qu'ils sont colinéaires), alors $Tr_Q(z_1z_2z_0) = 0$ et $\Delta = z_0^2 Tr_Q(z_1z_2) = 4z_0^2z_1^2z_2^2$; si maintenant z_1 et z_2 ne commutent pas, alors on peut choisir $z_0 = (z_1z_2)_0$, donc $z_1z_2 = \lambda + z_0$ pour un certain $\lambda \in k^*$. Alors :

$$\begin{aligned} \Delta &= z_0^2 \operatorname{Trd}_Q(\lambda + z_0)^2 - \operatorname{Trd}_Q((\lambda + z_0)z_0)^2 \\ &= 4z_0^2\lambda^2 - \operatorname{Trd}_Q(z_0^2)^2 \\ &= 4z_0^2(\lambda^2 - z_0^2) \\ &= 4z_0^2 \operatorname{Nrd}_Q(z_1z_2) \\ &= 4z_0^2z_1^2z_2^2 \end{aligned}$$

donc dans tous les cas on trouve $\langle\langle -\Delta, z_1^2\rangle\rangle = \langle\langle -z_1^2 z_2^2 z_0^2, z_1^2\rangle\rangle$ ce qui donne bien φ_{z_1,z_2}.

Pour le calcul de $\langle a\rangle_Q \cdot \langle b\rangle_Q$ avec $a, b \in K^*$ on se ramène immédatement au cas $a = b = 1$, et d'après l'exemple 2.2.9 on trouve la forme trace d'involution, qui a pour diagonalisation $\langle 2, -2u, -2v, 2uv\rangle = \langle 2\rangle\langle\langle u, v\rangle\rangle$ si $Q = (u, v)$, et donc qui est isométrique à $\langle 2\rangle n_Q$. □

2.3 Opérations λ

L'ingrédient clé des constructions d'invariants de classes de Witt dans le chapitre précédent était la structure de λ-anneau de $GW(K)$. On veut définir une structure semblable sur $\widetilde{GW}(A, \sigma)$.

2.3.1 Puissances alternées d'un module

Groupes symétriques et mélanges

On commence par un petit rappel sur les mélanges. Soit $d \in \mathbb{N}$ et soient $p, q \in \mathbb{N}$ tels que $p + q = d$. On dispose alors du sous-groupe $\mathfrak{S}_{p,q} \subset \mathfrak{S}_d$ constitué des permutations qui préservent les p premiers (et donc les q derniers) éléments. On a naturellement $\mathfrak{S}_{p,q} \simeq \mathfrak{S}_p \times \mathfrak{S}_q$, et la signature à gauche correspond au produit des signatures à droite.

On définit aussi l'ensemble des (p, q)-mélanges $Sh(p, q) \subset \mathfrak{S}_d$, qui sont les permutations (strictement) croissantes sur les p premiers et sur les q derniers éléments.

Lemme 2.3.1. *Tout élément de $\mathfrak{S}_d$ s'écrit de façon unique comme $\pi\sigma$ avec $\pi \in Sh(p, q)$ et $\sigma \in \mathfrak{S}_{p,q}$.*

Démonstration. Soit $\tau \in \mathfrak{S}_d$. Soient $\sigma_1 \in \mathfrak{S}_p$ et $\sigma_2 \in \mathfrak{S}_q$ définies par $\tau(\sigma_1^{-1}(1)) < \cdots < \tau(\sigma_1^{-1}(p))$ et $\tau(\sigma_2^{-1}(p + 1)) < \cdots < \tau(\sigma_2^{-1}(p + q))$; autrement dit, σ_1 est obtenue en ordonnant $\tau(1), \ldots, \tau(p)$ dans l'ordre croissant, et de même pour σ_2 avec $\tau(p+1), \ldots, \tau(p+q)$. On pose $\sigma \in \mathfrak{S}_{p,q}$ correspondant à (σ_1, σ_2), et $\pi = \tau\sigma^{-1}$. Alors par construction $\pi(1) < \cdots < \pi(p)$ et $\pi(p + 1) < \cdots < \pi(p + q)$, donc $\pi \in Sh(p, q)$. Si on dispose d'une autre décomposition $\tau = \sigma'\pi'$, alors comme $\pi' \in Sh(p, q)$ on doit avoir $\tau((\sigma_1')^{-1}(1)) < \cdots < \tau((\sigma_1')^{-1}(p))$ et $\tau((\sigma_2')^{-1}(p+1)) < \cdots < \tau((\sigma')_2^{-1}(p + q))$, et donc $\sigma' = \sigma$ (et $\pi' = \pi$). □

Puissances alternées

Si V est un K-espace vectoriel, le fait que K soit de caractéristique différente de 2 nous permet de voir la puissance extérieure $\Lambda^d V$ de deux façons : soit comme un quotient (ce qui est la construction canonique), soit comme un sous-espace de $V^{\otimes d}$. Précisément, pour tout $\pi \in \mathfrak{S}_d$ on pose

$$\begin{array}{rrcl} g_\pi : & V^{\otimes d} & \longrightarrow & V^{\otimes d} \\ & v_1 \otimes \cdots \otimes v_d & \longmapsto & v_{\pi^{-1}(1)} \otimes \cdots \otimes v_{\pi^{-1}(d)}, \end{array}$$

et on définit l'application d'antisymétrisation

$$s_d = \sum_{\pi \in \mathfrak{S}_d} (-1)^\pi g_\pi$$

où $(-1)^\pi$ désigne la signature de la permutation π. Alors l'application s_d est alternée, donc on obtient par propriété universelle une application induite $\Lambda^d V \longrightarrow \mathrm{Alt}^d(V)$, où $\mathrm{Alt}^d(V) \subset V^{\otimes d}$ est l'image de s_d, et un résultat classique d'algèbre linéaire affirme que c'est un isomorphisme, qu'on peut expliciter comme $v_1 \wedge \cdots \wedge v_d \mapsto s_d(v_1 \otimes \cdots \otimes v_d)$.

On va adapter cette contruction dans le cadre des modules sur des algèbres simples centrales. Soit donc A une algèbre simple centrale sur K. Suivant [17, 10.1], on définit pour tout $d \in \mathbb{N}$ un morphisme de groupes $\mathfrak{S}_d \longrightarrow (A^{\otimes d})^*$, qu'on note $\pi \mapsto g_A(\pi)$ (on écrira $g(\pi)$ s'il n'y a pas de confusion possible), caractérisé par $g_A((i\, i+1)) = 1 \otimes 1 \otimes \cdots \otimes g_A \otimes 1 \otimes \cdots \otimes 1$ où $g_A \in A^{\otimes 2}$ est l'élément de Goldman. Pour $d = 0, 1$, il s'agit du morphisme trivial. On énonce quelques propriétés de base de ces éléments :

Lemme 2.3.2. *Soit V un B-A-bimodule simple. Alors si $v_1, \ldots, v_d \in V$ et $\pi \in \mathfrak{S}_d$, on a*

$$g_B(\pi) \cdot (v_1 \otimes \cdots \otimes v_d) = (v_{\pi^{-1}(1)} \otimes \cdots \otimes v_{\pi^{-1}(d)}) \cdot g_A(\pi).$$

Démonstration. On se ramène facilement au cas où A et B sont déployées et $d = 2$, avec $g_B(\pi) = g_B$ et $g_A(\pi) = g_A$. On a alors $A \simeq \mathrm{End}_K(U)$, $B \simeq \mathrm{End}_K(W)$, et $V \simeq \mathrm{Hom}_K(U, W)$ avec les actions évidentes, et :

$$\begin{aligned}(g_B \cdot f \otimes g)(u \otimes u') &= g_B(f(u) \otimes g(u')) \\ &= g(u') \otimes f(u) \\ &= (g \otimes f)(g_A(u \otimes u')) \\ &= (g \otimes f \cdot g_A)(u \otimes u').\end{aligned}$$

□

Lemme 2.3.3. *Soient V_1 et V_2 deux A-modules à droite, et soient $B_i = \mathrm{End}_A(V_i)$ et $B = \mathrm{End}_A(V_1 \oplus V_2)$. Soit $\pi \in \mathfrak{S}_{p,q}$, correspondant au produit de $\pi_1 \in \mathfrak{S}_p$ et $\pi_2 \in \mathfrak{S}_q$. Soient $x \in V_1^{\otimes p}$ et $y \in V_2^{\otimes q}$. Alors :*

$$g_B(\pi) \cdot (x \otimes y) = (g_{B_1}(\pi_1) \cdot x) \otimes (g_{B_2}(\pi_2) \cdot y).$$

Démonstration. On se ramène au cas où A est déployée, auquel cas le résultat est clair par construction. □

On définit alors comme dans [17, §10.A] $s_{d,A} = s_d \in A^{\otimes d}$ par :

$$s_d = \sum_{\pi \in \mathfrak{S}_d} (-1)^\pi g(\pi). \tag{2.3.4}$$

Définition 2.3.5. Soit V un A-module à droite, avec $B = \mathrm{End}_A(V)$. On pose

$$\mathrm{Alt}^d(V) = s_{B,d}V^{\otimes d} \subset V^{\otimes d}$$

$A^{\otimes d}$-module à droite, avec en particulier $\mathrm{Alt}^0(V) = K$ et $\mathrm{Alt}^1(V) = V$

Notons que si $A = K$, alors on retrouve la construction ci-dessus pour les espaces vectoriels.

Remarque 2.3.6. Dans le cas où $V = A$ muni de l'action tautologique, on peut caractériser l'algèbre $\lambda^d(A)$ définie dans [17, 10.4] par le fait que $\mathrm{Alt}^d(A)$ est un isomorphisme dans $\mathbf{Br}(K)$ de $\lambda^d(A)$ vers $A^{\otimes d}$.

Produit de mélange

Si $p + q = d$, on définit un morphisme de $A^{\otimes d}$-modules $V^{\otimes p} \otimes_K V^{\otimes q} \to V^{\otimes d}$, qu'on appelle *produit de mélange* et qu'on note $x\#y$, par

$$x\#y = sh_{p,q}(x \otimes y) \tag{2.3.7}$$

où on définit l'application de mélange

$$\begin{array}{rccl} sh_{p,q} : & V^{\otimes d} & \longrightarrow & V^{\otimes d} \\ & x & \longmapsto & \sum_{\pi \in Sh(p,q)} (-1)^\pi g_B(\pi) \cdot x. \end{array} \tag{2.3.8}$$

On voit facilement par définition que le produit de mélange est associatif et alterné, et en particulier anti-symétrique.

Proposition 2.3.9. *Le produit de mélange induit un diagramme commutatif*

$$\begin{array}{ccc} V^{\otimes p} \otimes_K V^{\otimes q} & \xrightarrow{\otimes} & V^{\otimes d} \\ \downarrow & & \downarrow \\ \mathrm{Alt}^p(V) \otimes_K \mathrm{Alt}^q(V) & \xrightarrow{\#} & \mathrm{Alt}^d(V). \end{array}$$

Démonstration. On doit vérifier que pour tout $x \in V^{\otimes p}$ et tout $y \in V^{\otimes q}$ on a $(s_p x)\#(s_q y) = s_d(x \otimes y)$. Or :

$$\begin{aligned} (s_p x)\#(s_q y) &= sh_{p,q}(s_p x \otimes s_q y) \\ &= \sum_{\pi \in Sh(p,q)} (-1)^\pi g_B(\pi)(s_p x \otimes s_q y) \\ &= \sum_{\pi \in Sh(p,q)} (-1)^\pi g_B(\pi) \left(\sum_{\sigma \in \mathfrak{S}_{p,q}} (-1)^\sigma g_B(\sigma)(x \otimes y) \right) \\ &= \sum_{\pi \in Sh(p,q), \sigma \in \mathfrak{S}_{p,q}} (-1)^{\pi\sigma} g_B(\pi\sigma)(x \otimes y) \\ &= s_d(x \otimes y) \end{aligned}$$

en utilisant les lemmes 2.3.3 et 2.3.1. $\square$

On montre maintenant l'analogue de la formule d'addition bien connue pour les puissances extérieures d'espaces vectoriels :

Proposition 2.3.10. *Soient U et V deux A-modules à droite. Alors pour tout $d \in \mathbb{N}$ le produit de mélange induit un isomorphisme de $A^{\otimes d}$-modules :*

$$\bigoplus_{k=0}^{d} \mathrm{Alt}^k(U) \otimes_K \mathrm{Alt}^{d-k}(V) \xrightarrow{\sim} \mathrm{Alt}^d(U \oplus V).$$

Démonstration. En utilisant la proposition précédente, on établit facilement que $\mathrm{Alt}^d(U \oplus V)$ est linéairement engendré par les éléments de la forme $x_1 \# \cdots \# x_d$, et par bilinéarité du produit de mélange, on peut clairement prendre $x_i \in U$ ou V. Alors comme le produit de mélange est anti-symétrique, on peut permuter les x_i jusqu'à se ramener à $x_1, \ldots, x_k \in U$ et $x_{k+1}, \ldots, x_d \in V$. Or tout élément de cette forme est clairement dans l'image de l'application de l'énoncé, de sorte qu'elle surjective. On peut alors conclure qu'elle est bijective en comparant les dimensions sur K. □

2.3.2 Puissances alternées d'une forme ε-hermitienne

On suppose maintenant que A est munie d'une involution de première espèce σ, et que V est munie d'une forme ε-hermitienne h relativement à σ. On note τ l'involution adjointe sur B.

Lemme 2.3.11. *L'élément $s_d \in B^{\otimes d}$ est symétrique pour l'involution $\tau^{\otimes d}$, et pour tous $x, y \in V$ on a*

$$h^{\otimes d}(x, s_d y) = h^{\otimes d}(s_d x, y).$$

Démonstration. La première affirmation se ramène par construction au fait que l'élément de Goldman est symétrique pour $\tau \otimes \tau$, ce qu'on a déjà observé dans le lemme 2.2.6 (voir aussi directement [17, 10.19]), et la deuxième découle directement de ce fait puisque $\tau^{\otimes d}$ est l'involution adjointe à $h^{\otimes d}$. □

Définition 2.3.12. Le lemme précédent permet alors de poser :

$$\begin{array}{rrcl} \mathrm{Alt}^d(h) : & \mathrm{Alt}^d(V) \times \mathrm{Alt}^d(V) & \longrightarrow & A^{\otimes d} \\ & (s_d x, s_d y) & \longmapsto & h^{\otimes d}(x, s_d y) = h^{\otimes d}(s_d x, y). \end{array}$$

Proposition 2.3.13. *L'application $\mathrm{Alt}^d(h)$ est une forme ε^d-hermitienne sur $(A^{\otimes d}, \sigma^{\otimes d})$.*

Démonstration. On a

$$\begin{aligned} \mathrm{Alt}^d(h)(s_d x \cdot a, s_d y \cdot b) &= h^{\otimes d}(xa, s_d y b) \\ &= \sigma^{\otimes d}(a) h^{\otimes d}(x, s_d y) b \\ &= \sigma^{\otimes d}(a) \, \mathrm{Alt}^d(h)(s_d x, s_d y) b \end{aligned}$$

et

$$\begin{aligned}\mathrm{Alt}^d(h)(s_d y, s_d x) &= h^{\otimes d}(y, s_d x)\\ &= \varepsilon^d \sigma^{\otimes d}(h^{\otimes d}(s_d x, y))\\ &= \varepsilon^d \sigma^{\otimes d}(\mathrm{Alt}^d(h)(s_d x, s_d y)).\end{aligned}$$

□

Remarque 2.3.14. Dans la continuité de la remarque 2.3.6, on peut observer que si $V = A$ et $h = \langle 1\rangle_\sigma$, alors l'involution adjointe de $\mathrm{Alt}^d(h)$ est l'involution $\sigma^{\wedge d}$ telle que définie dans [17, 10.20], de sorte que $(\mathrm{Alt}^d(A), \mathrm{Alt}^d(h))$ réalise un isomorphisme dans $\mathbf{Br}_h(K)$ de $(\lambda^d(A), \sigma^{\wedge d})$ vers $(A^{\otimes d}, \sigma^{\otimes d})$.

Remarque 2.3.15. On a construit $\mathrm{Alt}^d(V)$ comme un sous-module de $V^{\otimes d}$, il est donc muni de la restriction de la forme hermitienne $h^{\otimes d}$. On observe facilement que

$$h^{\otimes d}_{|\,\mathrm{Alt}^d(V)} = \langle d!\rangle\,\mathrm{Alt}^d(h)$$

puisque $h^{\otimes d}(s_d x, s_d y) = h^{\otimes d}(x, s_d^2 y)$ et $s_d^2 = d! s_d$. En particulier, en caractéristique non nulle on ne peut pas définir simplement $\mathrm{Alt}^d(h)$ à partir de $h^{\otimes d}$.

On montre alors la compatibilité avec la formule d'addition :

Proposition 2.3.16. *Soient (U, h) et (V, h') deux modules ε-hermitiens sur (A, σ). L'isomorphisme de modules de la proposition 2.3.10 induit une isométrie de*

$$\bigoplus_{k=0}^{d} (\mathrm{Alt}^k(U), \mathrm{Alt}^k(h)) \otimes_K (\mathrm{Alt}^{d-k}(V), \mathrm{Alt}^{d-k}(h'))$$

vers

$$(\mathrm{Alt}^d(U\oplus V), \mathrm{Alt}^d(h\perp h')).$$

Démonstration. Soient $u, u' \in U^{\otimes k}$ et $v, v' \in V^{\otimes d-k}$. Alors

$$\begin{aligned}&\mathrm{Alt}^d(h\perp h')(s_k u\# s_{d-k} v, s_k u\# s_{d-k} v)\\ &= \mathrm{Alt}^d(h\perp h')(s_d(u\otimes v), s_d(u'\otimes v'))\\ &= (h\perp h')^{\otimes d}(s_d(u\otimes v), u'\otimes v')\\ &= \sum_{\pi\in\mathfrak{S}_d} (-1)^\pi (h\perp h')^{\otimes d}(g(\pi)(u\otimes v), u'\otimes v').\end{aligned}$$

On veut montrer que $(h\perp h')^{\otimes d}(g(\pi)(u\otimes v), u'\otimes v')$ est nul si $\pi \notin \mathfrak{S}_{k,d-k}$. Or si $u = x_1\otimes\cdots\otimes x_k$, $u' = y_1\otimes\cdots\otimes y_k$, et $v = x_{k+1}\otimes\cdots\otimes x_d$, $v' = y_{k+1}\otimes\cdots\otimes y_d$, alors

$$\begin{aligned}&(h\perp h')^{\otimes d}(g(\pi)(u\otimes v), u'\otimes v')\\ &= (h\perp h')^{\otimes d}((x_{\pi^{-1}(1)}\otimes\cdots\otimes x_{\pi^{-1}(d)})\cdot g_A(\pi), (y_1\otimes\cdots\otimes y_d))\\ &= \sigma^{\otimes d}(g_A(\pi))\cdot (h\perp h')(x_{\pi^{-1}(1)}, y_1)\otimes\cdots\otimes (h\perp h')(x_{\pi^{-1}(d)}, y_d)\end{aligned}$$

ce qui est en effet nul si $\pi \notin \mathfrak{S}_{k,d-k}$. De là :

$$\begin{aligned}
&\mathrm{Alt}^d(h \perp h')(s_k u \# s_{d-k} v, s_k u \# s_{d-k} v) \\
&= \sum_{\pi \in \mathfrak{S}_{k,d-k}} (-1)^{\pi} (h \perp h')^{\otimes d}(g(\pi)(u \otimes v), u' \otimes v') \\
&= \sum_{\pi_1 \in \mathfrak{S}_k} \sum_{\pi_2 \in \mathfrak{S}_{d-k}} (-1)^{\pi_1 \pi_2} (h \perp h')^{\otimes d}(g(\pi_1) u \otimes g(\pi_2) v), u' \otimes v') \\
&= h(s_k u, u') \otimes h'(s_{d-k} v, v').
\end{aligned}$$

□

2.3.3 Puissances extérieures d'un module ε-hermitien

Dans le cas des espaces vectoriels, $(\mathrm{Alt}^d(V), \mathrm{Alt}^d(h))$ fournissait une définition appropriée pour une opération $\lambda^d : GW(K) \longrightarrow GW(K)$, mais si A n'est pas déployée, on obtient seulement un module ε-hermitien sur $(A^{\otimes d}, \sigma^{\otimes d})$. On va alors utiliser l'isomorphisme $\varphi^{(d)}_{(A,\sigma)}$ dans $\mathbf{Br}_h(K)$.

Définition 2.3.17. Soit (V, h) un module ε-hermitien sur (A, σ). Pour tout $d \in \mathbb{N}$, on définit $(\Lambda^d(V), \lambda^d(h))$ comme la composition (comme morphismes dans $\mathbf{Br}_h(K)$) de $(\mathrm{Alt}^d(V), \mathrm{Alt}^d(h))$ et $\varphi^{(d)}_{(A,\sigma)}$. Il s'agit donc d'un espace bilinéaire symétrique sur K si d est pair, et d'un module ε-hermitien sur (A, σ) si d est impair.

Remarque 2.3.18. Noter que $\Lambda^d(V)$ dépend de σ, bien que le module V soit défini indépendamment. En revanche $\Lambda^d(V)$ ne dépend pas de h. Voir l'exemple ci-dessous.

Exemple 2.3.19. Considérons la forme hermitienne $h = \langle 1 \rangle_\sigma$ (voir exemple 2.2.9), de module sous-jacent $V = A$. Alors si σ est orthogonale $\Lambda^2(A)$ est naturellement identifié à l'espace vectoriel $Skew(A, \sigma)$ des éléments antisymétriques de A, et si σ est symplectique $\Lambda^2(A)$ est naturellement $Sym(A, \sigma)$, l'espace des éléments symétriques. En effet, par construction $\Lambda^2(A)$ est obtenu à partir du $A \otimes_K A$-module à droite $(1-g)(A \otimes_K A)$ (où g est l'élément de Goldman) par l'équivalence de Morita entre $A \otimes_K A$ et K. De là, $\Lambda^2(A)$ est le sous-espace vectoriel $(1-g) \cdot A \subset A$ où l'action à gauche de $A \otimes_K A$ est l'action tordue par σ. Or d'après le lemme 2.2.6, on a $g \cdot a = \varepsilon \sigma(a)$ où $\varepsilon = 1$ si σ est orthogonale et $\varepsilon = -1$ si σ est symplectique, donc $\Lambda^2(A)$ est l'espace des éléments symétrisés ou anti-symétrisés selon le type de σ (et comme la caractéristique est différente de 2, c'est bien équivalent aux éléments symétriques ou anti-symétriques).

De plus, si σ est orthogonale $\lambda^2(h)$ est isométrique à $\langle \frac{1}{2} \rangle T_\sigma^-$, et si σ est symplectique alors $\lambda^2(h)$ est isométrique à $\langle \frac{1}{2} \rangle T_\sigma^+$, où $T_\sigma^\pm$ est la restriction de la forme trace d'involution aux éléments symétriques ou antisymétriques. En effet, T_σ correspond par l'équivalence de Morita ci-dessus à $h \otimes h$, tandis que $\lambda^2(h)$ correspond à $\mathrm{Alt}^2(h)$, et on sait que la restriction de $h \otimes h$ à $\mathrm{Alt}^2(A)$ est $\langle 2\rangle \mathrm{Alt}^2(h)$ (voir la remarque 2.3.15).

Exemple 2.3.20. On prend encore le cas de $h = \langle 1\rangle_\sigma$ pour simplifier, où on suppose σ orthogonale ; alors si $d = \deg(A)$, on a $\lambda^d(h) = \langle \det(\sigma)\rangle$ (discriminant non signé). En effet, on le vérifie facilement après déploiement générique, où c'est une conséquence de la propriété correspondante pour les formes quadratiques, mais le morphismes $K^*/(K^*)^2 \to F^*/(F^*)^2$, où F est un corps de déploiement générique de A, est injectif.

Remarque 2.3.21. En utilisant la remarque 2.3.14, on constate qu'en prenant encore $V = A$ et $h = \langle 1\rangle_\sigma$, $(\lambda^d(V), \lambda^d(h))$ est un isomorphisme dans $\mathbf{Br}_h(K)$ de $(\lambda^d(A), \sigma^{\wedge d})$ vers (A, σ) ou (K, Id) selon la parité de d.

On va montrer que ces opérations vérifient bien les propriétés attendues. On renvoie au premier chapitre pour les définitions nécessaires.

Proposition 2.3.22. *L'association $(V, h) \mapsto (\Lambda^d(V), \lambda^d(h))$ pour (V, h) module ε-hermitien sur (A, σ) ou (K, Id) définit une opération grecque homogène sur $\widetilde{SGW}(A, \sigma)$, qui induit une structure d'anneau grec gradué sur $\widetilde{GW}(A, \sigma)$.*

Démonstration. Pour tout $\gamma \in \Gamma$ et tout $d \in \mathbb{N}$ on a défini $\lambda^d : \widetilde{SGW}(A, \sigma)_\gamma \to \widetilde{SGW}(A, \sigma)_{d\gamma}$, et la proposition 2.3.16 montre que l'application induite $\lambda_t : \widetilde{SGW}(A, \sigma)_\gamma \to G(\widetilde{SGW}(A, \sigma))$ est un morphisme de monoïdes, donc par définition d'une somme directe on obtient de façon naturelle un morphisme $\lambda_t : \widetilde{SGW}(A, \sigma) \to G(\widetilde{SGW}(A, \sigma))$ qui définit une opération grecque graduée.

L'affirmation concernant $\widetilde{GW}(A, \sigma)$ est une simple application du lemme 1.1.25. □

Le théorème 2.2.14 s'étend lui aussi à la structure d'anneau grec :

Proposition 2.3.23. *Le foncteur $(A, \sigma) \mapsto \widetilde{GW}(A, \sigma)$ définit un foncteur de $\mathbf{Br}_h(K)$ dans la catégorie des algèbres* grecques *graduées.*

Démonstration. Il s'agit donc de vérifier que les opérations λ sont respectées par les isomorphismes induits par les équivalences de Morita. Soient donc (B, τ) et (A, σ), et (U, g) qui définit un morphisme $f : (B, \tau) \longrightarrow (A, \sigma)$ dans $\mathbf{Br}_h(K)$, et soit (V, h) un module ε-hermitien sur (B, τ).

Comme $(\Lambda^d(V), \lambda^d(h))$ est obtenu par composition avec $\varphi^{(d)}_{(B,\tau)}$ à partir de $(\mathrm{Alt}^d(V), \mathrm{Alt}^d(h))$ et que la proposition 2.2.13 montre la compatibilité de $\varphi^{(d)}_{(B,\tau)}$ avec les équivalences de Morita, il suffit de vérifier que $f^{\otimes d}$ induit un isomorphisme entre $\mathrm{Alt}^d(h)$ et $\mathrm{Alt}^d(h')$ où $h' = f_*(h)$.

On note $W = V \otimes_B U$, sur lequel est défini h'. Alors on a canoniquement $\mathrm{End}_A(W) \simeq \mathrm{End}_B(V)$ (qu'on notera C), donc

$$\begin{aligned}
\mathrm{Alt}^d(V) \otimes_{B^{\otimes d}} U^{\otimes d} &= s_{d,C} \cdot V^{\otimes d} \otimes_{B^{\otimes d}} U^{\otimes d} \\
&= s_{d,C} \cdot (V \otimes_B U)^{\otimes d} \\
&= s_{d,C} \cdot W^{\otimes d} \\
&= \mathrm{Alt}^d(W).
\end{aligned}$$

Si $x, y \in V^{\otimes d}$ et $u, u' \in U^{\otimes d}$, où $x = x_1 \otimes \cdots \otimes x_d$ et de même pour les autres :

$$\begin{aligned}
&f_*^{\otimes d}(\mathrm{Alt}^d(h))(s_{d,C}x \otimes u, s_{d,C}y \otimes u') \\
&= g^{\otimes d}(u, \mathrm{Alt}^d(h)(s_{d,C}x, s_{d,C}y) \cdot u') \\
&= g^{\otimes d}(u, h^{\otimes d}(x, s_{d,C}y) \cdot u') \\
&= \sum_{\pi \in \mathfrak{S}_d} (-1)^\pi g(u_1, h(x_1, y_{\pi^{-1}(1)})u'_{\pi^{-1}(1)}) \otimes \cdots \otimes g(u_d, h(x_d, y_{\pi^{-1}(d)})u'_{\pi^{-1}(d)}) g_A(\pi) \\
&= \sum_{\pi \in \mathfrak{S}_d} (-1)^\pi h'(x_1 \otimes u_1, y_{\pi^{-1}(1)} \otimes u'_{\pi^{-1}(1)}) \otimes \cdots \otimes h'(x_d \otimes u_d, y_{\pi^{-1}(d)} \otimes u'_{\pi^{-1}(d)}) g_A(\pi) \\
&= \sum_{\pi \in \mathfrak{S}_d} (-1)^\pi (h')^{\otimes d}(x \otimes u, g_C(\pi) y \otimes u') \\
&= h'(x \otimes u, s_{d,C}y \otimes u') \\
&= \mathrm{Alt}^d(h')(s_{d,C}x \otimes u, s_{d,C}y \otimes u').
\end{aligned}$$

□

Exemple 2.3.24. Si h est une forme ε-hermitienne sur (A, σ), alors en combinant les exemples 2.2.15 et 2.3.19, la proposition montre que $\lambda^2(h) = T^+_{\sigma_h}$ si σ_h est symplectique, et $\lambda^2(h) = T^-_{\sigma_h}$ si σ_h est orthogonale.

2.4 Idéal fondamental et filtration

Outre la structure d'anneau grec, l'ingrédient principal pour étendre les méthodes du chapitre précédent aux algèbres à involution est l'existence de la filtration fondamentale de l'anneau de Grothendieck-Witt et son lien avec la cohomologie galoisienne.

2.4.1 Dimension et idéaux

Comme pour l'idéal fondamental de $GW(K)$, l'idéal fondamental de $\widetilde{GW}(A, \sigma)$ est défini par rapport à une application « dimension ».

Définition 2.4.1. Soit V un module à droite sur une algèbre simple centrale A. On appelle *dimension réduite* de V, et on note $\dim(V)$, le degré de l'algèbre $\mathrm{End}_A(V)$ (voir [17, def 1.9]).

Si (V,h) est un module ε-hermitien sur (A,σ), on notera aussi $\dim(h) = \dim(V)$.

Proposition 2.4.2. *L'application $(V,h) \mapsto \dim(V)$ définit un morphisme de semi-anneaux grecs gradués $\widetilde{SGW}(A,\sigma) \longrightarrow \mathbb{N}[\Gamma]$, qui se prolonge de façon unique en un morphisme d'anneaux grecs gradués $\widetilde{GW}(A,\sigma) \longrightarrow \mathbb{Z}[\Gamma]$. On a un diagramme commutatif :*

$$\begin{array}{ccccccc}
GW^{\pm}(K) & \longrightarrow & \widetilde{GW}(A,\sigma) & \xrightarrow{\dim} & \mathbb{Z}[\Gamma] & \xrightarrow{\varepsilon} & \mathbb{Z} \\
\downarrow & & \downarrow & & \downarrow & & \downarrow \\
W(K) & \longrightarrow & \widetilde{W}(A,\sigma) & \xrightarrow{\overline{\dim}} & \mathbb{Z}/2\mathbb{Z}[\Gamma] & \xrightarrow{\varepsilon} & \mathbb{Z}/2\mathbb{Z}
\end{array}$$

où ε est la flèche d'augmentation. Ce diagramme est naturel en (A,σ) (par rapport à la catégorie $\mathbf{Br}_h(K)$), et naturel en K.

Démonstration. La première assertion dit simplement que $\dim(h \cdot g) = \dim(h)\dim(g)$ et $\dim(\lambda^d(h)) = \binom{\dim(h)}{d}$, ce qui découle des constructions. Le diagramme commutatif est clair, de même que la naturalité en K, et la naturalité en (A,σ) dit essentiellement que la dimension est préservée par équivalence de Morita, ce qui résulte du fait d'avoir choisi la dimension réduite. □

On définit $\widetilde{GI}(A,\sigma)$ comme le noyau du morphisme $\widetilde{GW}(A,\sigma) \to \mathbb{Z}$ et $\widetilde{I}(A,\sigma)$ comme le noyau de $\widetilde{W}(A,\sigma) \to \mathbb{Z}/2\mathbb{Z}$ (ou de façon équivalente comme la projection de $\widetilde{GI}(A,\sigma)$ dans $\widetilde{W}(A,\sigma)$). On observe ici une dichotomie importante selon si A est déployée ou non : si A n'est pas déployée, tous les éléments de $GW^{\pm}(A,\sigma)$ sont de dimension paire (et les éléments de $GW^{-}(K)$ sont de dimension paire dans tous les cas), donc $\widetilde{I}(A,\sigma) = I(K) \oplus W^{\pm}(A,\sigma)$ est un idéal homogène.

Si $\gamma = o, s \in \Gamma$, on notera $\widetilde{GI}(A,\sigma)_\gamma$ (resp. $\widetilde{I}(A,\sigma)_\gamma$) l'intersection de $\widetilde{GI}(A,\sigma)$ (resp. $\widetilde{I}(A,\sigma)$) avec $\widetilde{GW}(A,\sigma)_\gamma \subset \widetilde{GW}(A,\sigma)$ (resp. $\widetilde{W}(A,\sigma)_\gamma \subset \widetilde{W}(A,\sigma)$).

Définition 2.4.3. La *filtration fondamentale* de $\widetilde{GW}(A,\sigma)$ (resp. $\widetilde{W}(A,\sigma)$) est $(\widetilde{GI}^n(A,\sigma))_{n\in\mathbb{N}}$ (resp. $(\widetilde{I}^n(A,\sigma))_{n\in\mathbb{N}}$). On note

$$\widetilde{H}^n(A,\sigma) = \widetilde{I}^n(A,\sigma)/\widetilde{I}^{n+1}(A,\sigma)$$

le gradué associé, qu'on qualifiera de *cohomologie mixte* sur (A,σ).

Par définition, $\widetilde{H}^0(A,\sigma) = \mathbb{Z}/2\mathbb{Z}$. Notons que par naturalité du diagramme (2.4.2), $\widetilde{H}^n(A,\sigma)$ ne dépend à isomorphisme (non canonique) près que de la classe de Brauer de A.

2.4.2 Le cas déployé

Comme on vient d'en faire l'observation, le cas où A est déployée est sensiblement différent du cas général. On le traite à part, en se ramenant par équivalence de Morita (non canonique a priori, donc) au cas $(A,\sigma) = (K, \mathrm{Id})$, et on utilise les notations de la partie 2.2.4. On utilise un léger abus de notation en écrivant $\widetilde{GI}(K)$ et $\widetilde{I}(K)$ au lieu de $\widetilde{GI}(K, \mathrm{Id})$ et $\widetilde{I}(K, \mathrm{Id})$. Pour décrire ces idéaux, on pose $GI(K) = \mathrm{Ker}(GW^{\pm}(K) \to \mathbb{Z})$ et $GJ(K) = \mathrm{Ker}(GW^{\pm}(K) \to \mathbb{Z}/2\mathbb{Z})$. On pose également $GJ^{(n)}(K) = GI^{n-1}(K)GJ(K)$ si $n \geqslant 1$ (et $GJ^{(0)}(K) = GW^{\pm}(K)$).

Remarque 2.4.4. On peut montrer que si $n \geqslant 2$, alors $GJ^{(n)}(K) = GJ^n(K) \cap GI(K)$, et que l'inclusion $GI^n(K) \subset GJ^{(n)}(K)$ est en général stricte.

Le fait que les idéaux qui nous intéressent ne soient pas homogènes signifie qu'ils ne se décomposent pas sous la forme $I_1 \oplus I_2 \subset R \oplus R$ à travers l'application Φ. En revanche, on a :

Proposition 2.4.5. *Soit $n \geqslant 1$. Alors (toujours avec les notations de la partie 2.2.4) :*

$$\widetilde{GI}^n(K) = \Psi(GI^n(K) \oplus GJ^{(n-1)}(K)),$$
$$\widetilde{I}^n(K) = \Psi(I^n(K) \oplus I^{n-1}(K)).$$

Démonstration. On procède naturellement par récurrence sur n. Il est clair par définition de Ψ que $\dim(\Psi(x,y)) = \dim(x)$, donc $\widetilde{GI}(K) = \Psi(GI(K) \oplus GW^{\pm}(K))$, et donc $\widetilde{I}(K) = \Psi(I(K) \oplus W(K))$.

Supposons que la propriété tienne jusqu'à $n \in \mathbb{N}^*$. Soient alors $x \in \widetilde{GI}(K)$ et $y \in \widetilde{GI}^n(K)$, qu'on écrit $x = \Psi(x_1, x_2)$ et $y = \Psi(y_1, y_2)$ avec $x_1 \in GI(K)$, $y_1 \in GI^n(K)$ et $y_2 \in GJ^{(n-1)}(K)$. On a d'après la formule (2.2.23) $xy = \Psi(z_1, z_2)$ avec $z_1 = x_1 y_1 \in GI^{n+1}(K)$ et $z_2 = x_1 y_2 + x_2 y_1 + 2x_2 y_2 \in GJ^{(n)}(K)$ (noter que c'est le terme $2x_2y_2$ dans le cas $n = 1$ qui nous oblige à prendre $GJ^{(n)}$ et non GI^n), donc $\widetilde{GI}^{n+1}(K) \subset \Psi(GI^{n+1}(K) \oplus GJ^{(n)}(K))$.

Réciproquement, si $x \in GI^{n+1}(K)$ est de la forme $x = x_1 x_2$ avec $x_1 \in GI(K)$ et $x_2 \in GI^n(K)$, alors $\Psi(x, 0) = \Psi(x_1, 0)\Psi(x_2, 0)$ donc $\Psi(x, 0) \in \widetilde{GI}^{n+1}(K)$, et si $y \in GJ^{(n)}(K)$ est de la forme $y = y_1 y_2$ avec $y_1 \in GI(K)$ et $y_2 \in GJ^{(n-1)}(K)$, alors $\Psi(0, y) = \Psi(y_1, 0)\Psi(0, y_2)$, donc $\Psi(0, y) \in \widetilde{GI}^{n+1}(K)$. Finalement, on a bien $\widetilde{GI}^{n+1}(K) \supset \Psi(GI^{n+1}(K) \oplus GJ^{(n)}(K))$.

L'assertion équivalente dans $\widetilde{W}(K)$ en découle facilement. $\square$

Corollaire 2.4.6. *En particulier, $\widetilde{H}^n(K) \simeq H^n(K, \mu_2) \oplus H^{n-1}(K, \mu_2)$ à travers Ψ.*

Remarque 2.4.7. Si A est déployée, alors dans l'isomorphisme $\widetilde{H}^n(A,\sigma) \simeq H^n(K,\mu_2) \oplus H^{n-1}(K,\mu_2)$, si on note (x_1,x_2) l'image de $x \in \widetilde{H}^n(A,\sigma)$, alors x_2 ne dépend pas du choix de l'équivalence de Morita entre (A,σ) et (K,Id), mais x_1 n'est défini qu'à $x_2 \cup H^1(K,\mu_2)$ près.

2.4.3 Le cas non déployé

Dans le cas où A n'est pas déployée, on a déjà une bonne décomposition homogène $I(A,\sigma) = I(K) \oplus W^{\pm}(A,\sigma)$.

Proposition 2.4.8. *Pour tout $n \geqslant 1$, la décomposition homogène de $\widetilde{I}^n(A,\sigma)$ est donnée par*

$$\widetilde{I}^n(A,\sigma) = I^n(K) \oplus I^n(A,\sigma)_o \oplus I^n(A,\sigma)_s$$

avec $I^n(A,\sigma)_\gamma = I^{n-1}(K)W(A,\sigma)_\gamma$ pour $\gamma = o,s \in \Gamma$.

Démonstration. L'inclusion de la droite vers la gauche est claire. Pour l'autre sens on raisonne par récurrence sur n, le cas $n=1$ étant trivial. On suppose que l'égalité tient jusqu'à $n \geqslant 1$.

Soient $x \in \widetilde{I}(A,\sigma)$ et $y \in \widetilde{I}^n(A,\sigma)$. On peut se ramener à x et y homogènes, et on voit que pour montrer $xy \in I^n(K)$, $I^n(A,\sigma)_o$ ou $I^n(A,\sigma)_s$, il suffit de montrer que $W^\varepsilon(A,\sigma) \cdot W^{\varepsilon'}(A,\sigma) \subset I^2(K)$. Or c'est vrai après déploiement générique puisque tout élément de $W^\varepsilon(A,\sigma)$ est de dimension paire ; mais le fait d'être dans $I^2(K)$ est détecté par le discriminant, qui est préservé par déploiement générique. □

On pose pour $\gamma = o,s \in \Gamma$:

$$H^n(A,\sigma)_\gamma = I^n(A,\sigma)_\gamma / I^{n+1}(A,\sigma)_\gamma. \tag{2.4.9}$$

Corollaire 2.4.10. *On a pour tout $n \geqslant 1$*

$$\widetilde{H}^n(A,\sigma) = H^n(K,\mu_2) \oplus H^n(A,\sigma)_o \oplus H^n(A,\sigma)_s,$$

Notons que d'après la proposition 2.4.8, on peut définir une application naturelle biadditive et surjective

$$H^{n-1}(K,\mu_2) \times W(A,\sigma)_\gamma \longrightarrow H^n(A,\sigma)\gamma,$$

dont il serait intéressant de comprendre le noyau. On note

$$(a_1,\dots,a_{n-1};a)_\sigma$$

l'image de $((a_1,\dots,a_{n-1}),\langle a\rangle_\sigma)$ par cette application ($a_i \in K^*$, $a \in A^*$ symétrique ou anti-symétrique).

Remarque 2.4.11. A priori, si $\gamma = o, s \in \Gamma$, on peut définir $\widetilde{I}^n(A,\sigma)_\gamma$ soit comme la n-ème puissance de $\widetilde{I}(A,\sigma)_\gamma$, soit comme l'intersection de $\widetilde{I}^n(A,\sigma)$ avec $\widetilde{W}(A,\sigma)_\gamma$. La proposition 2.4.8 permet alors de voir que ces deux définitions sont équivalentes quand A n'est pas déployée, donc la notation n'est pas ambiguë.

En revanche, si A est déployée, $\widetilde{I}(A,\sigma)_s = I(K)$, donc sa n-ième puissance est $I^n(K)$, tandis que l'intersection de $\widetilde{I}(A,\sigma)^n$ avec $\widetilde{W}(A,\sigma)_s = W(K)$ est $I^{n-1}(K)$. C'est alors la première définition qu'on emploiera.

2.4.4 Réduction générique d'indice

Un des outils standard dans l'étude des algèbres à involution est le déploiement générique des algèbres en question, ou, de façon un peu plus générale, la réduction générique de l'indice de l'algèbre. Il va de soi qu'on dispose pour toute extension de corps L/K d'un morphisme de restriction $r_{L/K} : \widetilde{H}^n(A,\sigma) \to \widetilde{H}^n(A_L,\sigma_L)$, et dans la mesure où on a une bonne description de $\widetilde{H}^n$ dans le cas déployé, ce type de méthode s'impose de façon assez naturelle dans notre contexte.

Supposons que A ne soit pas déployée. Si A_L n'est pas déployée non plus, alors le morphisme $\widetilde{H}^n(A,\sigma) \to \widetilde{H}^n(A_L,\sigma_L)$ est simplement défini sur chaque composante : $H^n(K,\mu_2) \to H^n(L,\mu_2)$, et $H^n(A,\sigma)_\gamma \to H^n(A_L,\sigma_L)_\gamma$ pour $\gamma = o, s$. Si maintenant A_L est déployée :

Proposition 2.4.12. *Soit (A,σ) non déployée sur K, et soit L/K une extension qui déploie A. Le morphisme de restriction*

$$H^n(K,\mu_2) \oplus H^n(A,\sigma)_o \oplus H^n(A,\sigma)_s \longrightarrow H^n(L,\mu_2) \oplus H^{n-1}(L,\mu_2)$$

est indépendant du choix d'une équivalence de Morita hermitienne entre (A_L,σ_L) et (L,Id). Il est de la forme

$$(x,y,z) \mapsto (x_L + y_L, 0)$$

où $y \mapsto y_L$ est un morphisme $H^n(A,\sigma)_o \to H^n(L,\mu_2)$ également indépendant de tout choix d'équivalence de Morita.

Démonstration. On se fixe un choix d'équivalence de Morita hermitienne entre (A_L,σ_L) et (L,Id). On en déduit un morphisme $W(A,\sigma)_o \to I(L)$ (puisque tout élément de $W(A,\sigma)_o$ est de dimension paire), qu'on note $h \mapsto h_L$, et un choix différent d'équivalence donne un morphisme différent d'une similitude. Soit $(x,y,z) \in \widetilde{H}^n(A,\sigma)$ se relevant en $(q, q'h, q''h') \in \widetilde{I}^n(A,\sigma)$. Son image par le morphisme de restriction

$$I^n(K) \oplus I^{n-1}(K)W(A,\sigma)_o \oplus I^{n-1}(K)W(A,\sigma)_s \longrightarrow I^n(L) \oplus I^{n-1}(L)$$

est donnée par $(q_L + q'_L h_L, -q'_L h_L)$, et donc l'image de (x,y,z) par la restriction est

$$(e_n(q_L) + e_n(q'_L h_L), e_{n-1}(q'_L h_L)) = (x_L + y_L, 0)$$

où $y_L = e_n(q'_L h_L)$ ne dépend que de y. □

Pour tout $r \in \mathbb{N}$, on pose $K_r(A)$ un corps de réduction générique à l'indice 2^r d'une algèbre simple centrale A ; notamment $K_0(A)$ est un corps de déploiement générique de A, et si $2^r \geqslant \operatorname{ind}(A)$ alors $K_r(A) = K$.

Définition 2.4.13. Pour tous $n, r \in \mathbb{N}$, on pose

$$\widetilde{GI}_r^n(A,\sigma) = r_{K_r(A)/K}^{-1}(\widetilde{GI}^n(A_{K_r(A)}, \sigma_{K_r(A)}))$$

où $r_{K_r(A)/K} : \widetilde{GW}(A,\sigma) \longrightarrow \widetilde{GW}(A_{K_r(A)}, \sigma_{K_r(A)})$ est le morphisme de restriction.

On pose de même

$$\widetilde{I}_r^n(A,\sigma) = r_{K_r(A)/K}^{-1}(\widetilde{I}^n(A_{K_r(A)}, \sigma_{K_r(A)})).$$

Notons que $\widetilde{GI}_r^1(A,\sigma) = \widetilde{GI}(A,\sigma)$ pour tout $r \in \mathbb{N}$ puisque la condition sur la dimension est inchangée par extension des scalaires ; de même, $\widetilde{I}_r^1(A,\sigma) = \widetilde{I}(A,\sigma)$. Notons également que la composante symplectique de $\widetilde{GW}(A,\sigma)$ est contenue dans tous les $\widetilde{GI}_0^n(A,\sigma)$ puisqu'après déploiement générique une involution symplectique devient hyperbolique.

On a clairement une croissance par rapport à n et à r :

$$\widetilde{GI}_r^n(A,\sigma) \subset \widetilde{GI}_r^{n+1}(A,\sigma), \quad \widetilde{GI}_{r+1}^n(A,\sigma) \subset \widetilde{GI}_r^n(A,\sigma).$$

Cette hiérarchie permettra de donner des énoncés plus fins concernant les invariants cohomologiques dans le chapitre suivant.

2.4.5 Algèbres de quaternions

On s'attarde ici sur le cas des algèbres de quaternions munies de leur involution canonique, et de leur déploiement générique. Soit donc $(Q, ^-)$ une algèbre de quaternions sur K, munie de son involution canonique.

Dans [26], Quéguiner et Tignol décrivent l'effet du déploiement générique de Q sur $W^\varepsilon(Q, ^-)$. Soit C la variété de Severi-Brauer de Q, qui est une conique, et soit $F = K(C)$ son corps de fonction, qui est donc un corps de déploiement générique de Q. Pour tout point fermé $\mathfrak{p}$ de C, on a une valuation $v_\mathfrak{p}$ discrète de rang 1 sur F, et donc on a les deux application résidus usuelles $\partial_{1,\mathfrak{p}}, \partial_{2,\mathfrak{p}} : W(F) \longrightarrow W(K(\mathfrak{p}))$ (où $\partial_{2,\mathfrak{p}}$ dépend du choix d'une uniformisante locale en $\mathfrak{p}$). Le choix d'un point fermé $a \in C$ de degré 2, qu'on notera en général $a = \infty$, donne en particulier une équivalence de Morita hermitienne entre $(Q_F, ^-)$ et (F, Id) et donc un isomorphisme $W^-(Q_F, ^-) \simeq W(F)$, ce qui donne une application d'extension des scalaires

$$\mathrm{ext}_a : W^-(Q, ^-) \longrightarrow W(F). \tag{2.4.14}$$

Si on choisit un autre point $b \in C$ comme point à l'infini, on dispose alors d'un scalaire $\lambda_{a,b} \in F^*$ tel que le diagamme suivant commute :

$$\begin{tikzcd} & W(F) \arrow[dd, "\cdot\langle\lambda_{a,b}\rangle"] \\ W^-(Q,^-) \arrow[ur, "\mathrm{ext}_a"] \arrow[dr, "\mathrm{ext}_b"'] & \\ & W(F). \end{tikzcd}$$

On pose alors :

$$W_{nr,1,\infty}(F) = \{q \in W(F) \,|\, \partial_{1,\infty}(q) = 0, \, \forall \mathfrak{p} \neq \infty, \partial_{2,\mathfrak{p}}(q) = 0\} \tag{2.4.15}$$

et

$$W_{nr,2}(F) = \{q \in W(F) \,|\, \forall \mathfrak{p}, \partial_{2,\mathfrak{p}}(q) = 0\}. \tag{2.4.16}$$

De plus on peut montrer que $\lambda_{a,b}$ est non ramifié sur tout $c \in C$ sauf en a et b, de sorte que la multiplication par $\lambda_{a,b}$ envoie $W_{nr,1,a}(F)$ sur $W_{nr,1,b}(F)$. Dans [26] il est démontré que ext_∞ induit :

$$W^-(Q,^-) \xrightarrow{\sim} W_{nr,1,\infty}(F) \tag{2.4.17}$$

et

$$0 \longrightarrow n_Q W(K) \longrightarrow W(K) \longrightarrow W_{nr,2}(F) \longrightarrow 0. \tag{2.4.18}$$

En particulier, le noyau de l'application de restriction $\widetilde{W}(Q,^-) \to \widetilde{W}(Q_F,^-)$ est $n_Q W(K) \oplus W^+(Q,^-)$.

Remarque 2.4.19. On pourrait tenter d'utiliser ces résultats pour définir les opérations λ^d pour des formes quaternioniques : si d est impair, on voit facilement que λ^d sur $W(F)$ préserve $W_{nr,1,\infty}(F)$, donc si $h \in W^-(Q,^-)$, on peut définir $\lambda^d(h)$ comme $\mathrm{ext}_\infty^{-1}(\lambda^d(\mathrm{ext}_\infty(h)))$, ce qui ne dépend pas du choix de ∞, puisque λ^d commute avec la multiplication par $\langle\lambda_{a,b}\rangle$ où a et b sont deux choix différents pour ∞. En revanche, si d est pair, on ne peut définir par cette méthode que $\lambda^d(h)$ modulo n_Q : en effet λ^d préserve cette fois $W_{nr,2}(F)$, mais le morphisme de restriction $W(F) \longrightarrow W_{nr,2}(F)$ n'est pas injectif.

En ce qui concerne la cohomologie, on a également des applications de résidu $\partial_\mathfrak{p} : H^d(F,\mu_2) \longrightarrow H^{d-1}(K(\mathfrak{p}),\mu_2)$, et on pose

$$H^d_{nr}(F,\mu_2) = \mathrm{Ker}\left(\bigoplus_{\mathfrak{p}} \partial_\mathfrak{p}\right). \tag{2.4.20}$$

On peut alors noter que si $q \in I^d(F) \cap W_{nr,i}(F)$ pour $i = 1, 2$, alors $e_d(q) \in H^d_{nr}(F, \mu_2)$.

Cela nous permet de définir un morphisme

$$\widetilde{e}_d : \widetilde{I}^d_0(Q, ^-) \longrightarrow H^{d-1}_{nr}(F, \mu_2) \tag{2.4.21}$$

qui est indépendant du choix de ∞. En effet, après déploiement générique, et équivalence de Morita définie par le choix de ∞, un élément de $\widetilde{I}^d_0(Q, ^-)$ est envoyé sur un élément de $\widetilde{I}^d(F)$ tel que la partie paire soit dans $W_{nr,2}(F)$ et la partie impaire dans $W_{nr,1,\infty}(F)$, donc on obtient un élément de $I^{d-1}(F) \cap W_{nr,2}(F)$ (indépendant de ∞) et un élément de $I^{d-1}(F) \cap W_{nr,1,\infty}(F)$ (qui ne dépend de ∞ qu'à similitude près), dont la somme est dans $I^d(F)$, et donc l'invariant e_{d-1} de chacun de ces éléments donne la même classe dans $H^{d-1}_{nr}(F, \mu_2)$ (qui ne dépend donc pas de ∞).

Remarque 2.4.22. On constate qu'on peut définir par ce déploiement générique une classe dans $H^d(F)$ (autre façon de le voir : on peut naturellement définir une classe dans $\widetilde{H}^d(F) = H^d(F) \oplus H^{d-1}(F)$), mais cette classe est en général ramifiée en ∞, et on ne pourra donc pas la redescendre sur K.

On trouve dans [15, prop A.1] une description du noyau et du conoyau de $H^d(K, \mathbb{Q}/\mathbb{Z}(d-1)) \longrightarrow H^d(F, \mathbb{Q}/\mathbb{Z}(d-1)$. En ce qui nous concerne, pour toute algèbre simple centrale A, on définit $M^d_A(K)$ comme étant le sous-groupe de 2-torsion de

$$H^d(K, \mu_4^{\otimes d-1})/[A] \cdot H^{d-2}(K, \mu_2)$$

(qui ne dépend que de la classe de Brauer de A), ainsi que $N^d_A(K) \subset M^d_A(K)$ l'image de l'application naturelle $H^d(K, \mu_2) \longrightarrow M_A(K)$. Le résultat de [15] donne alors un isomorphisme induit par la restriction :

$$M^d_Q(K) \simeq H^d_{nr}(F, \mu_2). \tag{2.4.23}$$

La construction précédente nous donne donc un morphisme

$$\widetilde{e}_d : \widetilde{I}^d_0(Q, ^-) \longrightarrow M^{d-1}_Q(K).$$

. Il s'avère qu'on peut faire un peu mieux.

Proposition 2.4.24. *Pour tout $d \geqslant 1$, le morphisme $\widetilde{e}_d$ ci-dessus est à valeurs dans $N^{d-1}_Q(K)$.*

Pour cela on démontre d'abord le lemme suivant :

Lemme 2.4.25. *Soient $m \in \mathbb{N}$ et $q \in W(K)$ telle que $q_F \in I^m(F)$. Alors il existe $q' \in W(K)$ telle que $q - n_Q q' \in I^m(K)$.*

Démonstration du lemme. Le résultat est clair si $m \leqslant 2$ car alors on a directement $q \in I^m(K)$ (donc on peut prendre $q' = 0$). Pour le cas général on procède par récurrence : supposons que le résultat vale jusqu'à $m \geqslant 2$. Si $q_F \in I^{m+1}(F)$, alors par hypothèse on a $q_1 \in W(K)$ tel que $q - n_Q q_1 \in I^m(K)$. On a alors $e_m(q - n_Q q_1)_F = e_m(q_F) = 0$, donc $e_m(q - n_Q q_1) \in [Q]H^{m-2}(K, \mu_2)$. On pose $q_2 \in I^{m-2}(K)$ tel que $e_m(q - n_Q q_1) = [Q]e_{m-2}(q_2)$, et on définit $q' = q_1 + q_2$. On a bien $e_m(q - n_Q q') = 0$ donc $q - n_Q q' \in I^{m+1}(K)$. $\square$

Démonstration de la proposition. Les cas $d = 1, 2$ sont clairs puisque $N_Q^0(K) = M_Q^0(K) = H^0(K, \mu_2)$ et $N_Q^1(K) = M_Q^1(K) = H^1(K, \mu_2)$. Si $d \geqslant 3$, on prend $q \in W(K)$ la composante quadratique de $x \in \widetilde{I}_0^d(Q, ^-)$, et on choisit q' comme dans le lemme pour que $q - n_Q q' \in I^{d-1}(K)$. Alors $e_{d-1}(q - n_Q q')_F = e_{d-1}(q_F)$ donc $e_{d-1}(q - n_Q q')$ est bien une descente de $\widetilde{e}_d(x)$ dans $H^{d-1}(K, \mu_2)$. $\square$

Remarque 2.4.26. Il y a une dimension « concrète » à cette proposition, contrairement à la définition donnée ci-dessus de $\widetilde{e}_d$, qui utilise le résultat de [15] comme boîte noire (lui-même utilisant des résultats difficiles comme la conjecture de Milnor) et ne permet pas d'avoir des éléments explicites de $M_Q^d(K)$. En effet, il suffit en théorie de suivre le fil de la preuve du lemme, et de trouver à chaque étape une factorisation de $e_m(q - n_Q q_1) \in H^m(K, \mu_2)$ (en reprenant les notations de la preuve) par $[Q]$. On utilise ici seulement le résultat de [15] pour garantir qu'une telle factorisation existe.

Chapitre 3

Invariants d'algèbres à involution

Dans ce chapitre on met en action les différentes techniques développées précédemment pour construire des invariants cohomologiques d'algèbres à involution.

Dans la première partie, on exploite le fait que les invariants $\mathrm{Inv}(I, I^d)$ construits dans le premier chapitre peuvent en réalité s'appliquer dans n'importe quel anneau grec, puisque ce sont des combinaisons d'opérations λ. On peut donc les appliquer dans l'anneau $\widetilde{GW}(A, \sigma)$ défini au deuxième chapitre. L'espoir initial qu'on obtienne ainsi des applications de $\widetilde{GI}(A, \sigma)$ (voir 2.4.3) vers $\widetilde{H}^d(A, \sigma)$ est mis en défaut, mais on obtient tout de même des invariants de degré arbitrairement grands en tenant compte de l'obstruction donnée par l'indice de l'algèbre (voir le corollaire 3.1.3 et la discussion qui suit). On accorde un soin particulier à l'étude des algèbres d'indice 2, pour lesquelles on dispose de formules plus précises (voir la proposition 3.1.8), ainsi que de méthodes de déploiement générique.

La deuxième partie est consacrée à des calculs explicites autour de l'équivalence exceptionnelle entre algèbres de type A_3 et D_3 (voir les théorèmes 3.2.28 et 3.2.37). Ces calculs sont mobilisés dans la partie suivante, qui donne quelques exemples d'applications de nos méthodes (et notamment des méthodes de déploiement générique en indice 2, voir la proposition 3.1.6 adaptée de [4]) pour généraliser certains invariants précédemment connus. Notamment, on étend la définition d'un invariant de degré 4 construit dans [28] (voir la proposition 3.3.4) pour les algèbres de type D_3, et d'un invariant de degré 5 construit dans [9] pour les formes quadratiques de degré 12 dans I^3 (voir la partie 3.3.2).

3.1 Invariants de formes hermitiennes

3.1.1 Opérations π_1^d

Soit (A, σ) une algèbre à involution de première espèce sur K. Comme $\widetilde{GW}(A, \sigma)$ est un anneau grec, on peut y appliquer les opérations π_n^d définies dans le premier chapitre. On dispose de la filtration $\widetilde{GI}^n(A, \sigma)$, qui est l'analogue de la filtration fondamentale de $GW(K)$, et on peut donc espérer que $\pi_n^d(\widetilde{GI}^n(A,\sigma)) \subset \widetilde{GI}^{nd}(A,\sigma)$. Ce résultat est en général faux, mais on obtient quand même (où on note $\lceil x\rceil$ la partie entière *supérieure* d'un réel $x \in \mathbb{R}$) :

Proposition 3.1.1. *Soit $m = \max(2, \mathrm{ind}(A))$. Alors pour tout $d \in \mathbb{N}$, l'opération π_1^d définit une application $\widetilde{GI}(A,\sigma) \to \widetilde{I}^{\lceil d/m\rceil}(A,\sigma)$.*

De plus, en prenant $p = \mathrm{ind}(A)$, π_1^d définit une application $\widetilde{GI}(A,\sigma)_o \to \widetilde{I}^{\lceil d/p\rceil}(A,\sigma)_o$.

Démonstration. On commence par traiter le cas où A n'est pas déployée ; le deuxième énoncé découle alors du premier, et on a $m = \mathrm{ind}(A)$. On peut conclure si on arrive à montrer que $\widetilde{GI}(A,\sigma)$ est additivement engendré par des éléments x tels que la classe de Witt de $\pi_1^d(x)$ est dans $\widetilde{I}^{\lceil d/m\rceil}(A,\sigma)$ pour tout $d \in \mathbb{N}$. En effet, si cette propriété vaut pour x elle vaut aussi pour $-x$: on a $0 = \pi_1^d(x-x)$ donc $\pi_1^d(-x) = -\sum_{k=0}^{d-1} \pi_1^{d-k}(x)\pi_1^k(-x)$, et on peut procéder par récurrence sur d, le cas $d = 0$ étant trivial. Il suffit alors de voir que pour tout $0 \leqslant k \leqslant d-1$, $\lceil (d-k)/m\rceil + \lceil k/m\rceil \geqslant \lceil d/m\rceil$. De même, si x et y vérifient la propriété, on montre que c'est aussi le cas de $x+y$ puisque $\pi_1^d(x+y) = \sum_{k=0}^d \pi_1^k(x)\pi_1^{d-k}(y)$ et on utilise la même inégalité. On peut alors conclure par récurrence sur le nombre de générateurs additifs intervenant dans l'écriture d'un élément.

On rappelle que $\pi_1^d = \sum_{k=1}^d (-1)^{d-k}\binom{d-1}{k-1}\lambda^k$. Or si $x \in \widetilde{GW}(A,\sigma)$, dans $\widetilde{W}(A,\sigma)$ on a $(-1)^k\lambda^k(x) = \langle -1\rangle^k\lambda^k(x) = \lambda^k(\langle -1\rangle x)$, donc :

$$\begin{aligned}
\pi_1^d(x) &= (-1)^d \sum_{k=0}^d \lambda^{d-k}(d-1)(-1)^k\lambda^k(x) \\
&= (-1)^d \sum_{k=0}^d \lambda^{d-k}(d-1)\lambda^k(\langle -1\rangle x) \\
&= (-1)^d\lambda^d(\langle -1\rangle x + (d-1)\langle 1\rangle) \\
&= \lambda^d(x + (d-1)\langle -1\rangle).
\end{aligned}$$

De là, on utilise le fait que $\widetilde{GI}(A,\sigma)$ est additivement engendré par : les éléments de $\hat{I}(K)$ (pour lesquels la propriété voulue est une conséquence des résultats du premier chapitre), et les éléments de la forme $x = y - r\langle -1\rangle$ où y est un élément de dimension minimale r dans $GW^-(K)$ (auquel cas $r = 2$) ou $SGW^\varepsilon(A,\sigma)$ (auquel cas $r = m$). Pour un tel élément x, on a $\pi_1^d(x) = \lambda^d(y + (d-1-r)\langle -1\rangle)$, donc si $d > r$ (et donc en particulier si $d > m$) on a $\pi_1^d(x) = 0$ (en effet pour un élément x de $\widetilde{SGW}(A,\sigma)$, si d est strictement plus grand que la dimension de x, $\lambda^d(x) = 0$).

Supposons maintenant que A soit déployée. Pour le premier énoncé, on a $m = 2$. On peut alors reprendre la même preuve que dans le cas non déployé, en observant que les générateurs de dimension minimale dans les composantes alternée et symplectique sont de dimension $m = 2$ bien que l'indice soit 1. Pour le deuxième énoncé, on a $p = 1$, mais les générateurs de dimension minimale sont bien cette fois de dimension $p = \mathrm{ind}(A) = 1$, puisqu'on n'a plus l'obstruction des plans hyperboliques alternés. □

En utilisant les notations de réducion d'indice de la définition 2.4.13, on obtient :

Corollaire 3.1.2. *Soit $r \geqslant 1$. Alors pour tout $d \in \mathbb{N}$, π_1^d induit des applications $\widetilde{GI}_r(A,\sigma) \to \widetilde{I}_r^{\lceil d/2^r \rceil}(A,\sigma)$, $\widetilde{GI}_0(A,\sigma) \to \widetilde{I}_0^{\lceil d/2 \rceil}(A,\sigma)$, et $\widetilde{GI}_0(A,\sigma)_o \to \widetilde{I}_0^d(A,\sigma)_o$.*

Démonstration. Il suffit d'appliquer les propositions précédentes après une extension des scalaires à $K_r(A)$, le corps de réduction générique à l'indice 2^r. □

3.1.2 Invariants cohomologiques

On peut utiliser les résultats précédents sur les opérations π_1^d pour étendre tous les invariants de Witt de I étudiés dans le premier chapitre.

Corollaire 3.1.3. *Soient $d \in \mathbb{N}$ et $\alpha \in \mathrm{Inv}(I, I^d)$. Pour tout $r \geqslant 1$, l'opération α sur $\widetilde{GW}(A,\sigma)$ induit des applications $\widetilde{GI}_r(A,\sigma) \to \widetilde{I}_r^{\lceil d/2^r \rceil}(A,\sigma)$, $\widetilde{GI}_0(A,\sigma) \to \widetilde{I}_0^{\lceil d/2 \rceil}(A,\sigma)$, et $\widetilde{GI}_0(A,\sigma)_o \to \widetilde{I}_0^d(A,\sigma)_o$.*

Démonstration. On écrit $\alpha = \sum_{n=0}^d a_n \pi_1^n$ avec $a_n \in I^{d-n}(k)$. Alors l'image de $a_n\pi_1^n(\widetilde{GI}(A,\sigma))$ est dans $I^{d-n}(k)\widetilde{I}_r^{\lceil n/2^r \rceil}(A,\sigma)$, et $d - n + \lceil n/2^r \rceil \geqslant \lceil d/2^r \rceil$.

On procède de même pour les cas où $r = 0$. □

On peut alors obtenir des invariants cohomologiques : si $\alpha \in \mathrm{Inv}(I, I^d)$, on obtient une application naturelle

$$\bar{\alpha} : \widetilde{GI}(A,\sigma) \longrightarrow \widetilde{H}^{\lceil d/m \rceil}(A,\sigma)$$

où $m = \max(2, \mathrm{ind}(A))$. Sachant que, par la proposition 2.4.8, $\widetilde{H}^n(A,\sigma)$ a une composante identifiée à $H^n(K,\mu_2)$, on obtient donc également une application naturelle

$$\alpha' : \widetilde{GI}(A,\sigma) \longrightarrow H^{\lceil d/m \rceil}(K,\mu_2)$$

donc un authentique invariant cohomologique. On obtient par ailleurs des invariants à valeurs dans les autres composantes de $\widetilde{H}^n(A,\sigma)$, à savoir $H_o^n(A,\sigma)$ et $H_s^n(A,\sigma)$, mais la nature précise de ces groupes reste à explorer, donc nous nous limiterons ici à la projection sur la composante cohomologique.

Pour obtenir un invariant « de (A,σ) », on peut appliquer une de ces constructions à un élément $h \in \widetilde{GI}(A,\sigma)$ qui « représente » (A,σ) : par exemple $h = \langle 1 \rangle_\sigma - \frac{\deg(A)}{2}\mathcal{H}$ (où $\mathcal{H} \in GW(K)$ est le plan hyperbolique), ou $h = \langle 1 \rangle_\sigma - \deg(A)\langle 1 \rangle$, ou encore si A est de coindice s pair $h = \langle 1 \rangle_\sigma - \frac{s}{2}\mathcal{H}(A,\sigma)$ où $\mathcal{H}(A,\sigma) \in GW(A,\sigma)$ est l'espace hyperbolique hermitien. Tous ces choix ne sont pas fondamentalement différents et correspondent simplement à différentes façon de normaliser l'élément canonique $\langle 1\rangle_\sigma$ pour obtenir un élément de $\widetilde{GI}(A,\sigma)$; précisément, à α fixé ces choix conduisent à des invariants différents, mais en faisant varier α l'ensemble des invariants obtenus ne change pas.

Il est à noter que l'élément de $H^{\lceil d/m\rceil}(K,\mu_2)$ ainsi obtenu ne constitue pas toujours un invariant intéressant en soi : en effet, en général il est nul après déploiement générique, puisque par construction l'élément de $I^{\lceil d/m\rceil}(K)$ dont il est la réduction est en réalité dans I^d après déploiement générique. Il est tout à fait possible que la classe obtenue soit de la forme $x\cup[A]$ où x ne dépend pas de σ (voir l'exemple 3.1.4 ainsi que la remarque 3.1.11), et en particulier les différents α ne donnent a priori pas toujours des invariants distincts dans les cas non déployés (bien qu'ils soient distincts en tant qu'invariants globaux puisqu'ils le sont dans le cas déployé). On peut se faire la représentation imagée suivante : l'élément $\alpha(h)$ (ou disons sa composante dans $W(K)$) possède effectivement de l'information « intéressante » au niveau de $I^d(K)$ comme dans le cas déployé, mais on n'y a pas accès directement parce qu'il y a une obstruction au niveau de $I^{\lceil d/m\rceil}(K)$ (qui disparaît après déploiement), et possiblement à d'autres I^n pour $n<d$.

Une façon possible de remédier à cela dans certains cas favorables est de construire des invariants relatifs : au lieu de considérer la classe de cohomologie de $\alpha(h)$, on peut étudier l'élément $\alpha(h)-\alpha(h')$, qui peut potentiellement se trouver dans une puissance supérieure de I si les « obstructions » évoquées précédemment se compensent. On illustre cette idée dans la partie 3.1.3 en indice 2, ainsi que dans l'exemple suivant.

Exemple 3.1.4. Le discriminant des involutions symplectiques, qui est un invariant de degré 3, peut être défini de la façon suivante (voir [5, thm 4]) : soient σ et σ' deux involutions symplectiques sur A ; alors $T_\sigma^+ - T_{\sigma'}^+\in I^3(K)$ et le discriminant (relatif) $d_\sigma(\sigma')$ est l'invariant e_3 de cette forme. Or dans $\widetilde{GW}(A,\sigma)$, si $h\in GW(A,\sigma)$ a pour adjoint σ', on a $T_\sigma^+ = \langle 2\rangle\lambda^2(\langle 1\rangle_\sigma)$ et $T_{\sigma'}^+ = \langle 2\rangle\lambda^2(h)$ (voir exemple 2.3.19), donc cela correspond à l'idée présentée précédemment, avec $\alpha=\lambda^2$. Dans [5], le fait que la différence soit dans I^3 est justifiée par le fait qu'un groupe symplectique n'a pas d'invariant cohomologique non constant en degré 1 et 2, mais on peut le justifier par un calcul explicite, qui permet de faire certaines remarques.

On pose $q_\sigma = \langle 2\rangle T_\sigma^+ + r\langle -1\rangle$ où $\deg(A)=2r$; c'est une forme quadratique de dimension $2r^2$. Dans [25], Quéguiner montre que $w_1(T_\sigma^+) = w_1(T_\sigma^-) = (2^r)$, ce qui implique que $e_1(q_\sigma)=0$ (voir la proposition 1.2.76 pour le lien entre les invariants de Stiefel-Whitney w_1 et w_2 et les invariants e_1 et e_2, en se rappelant que $e_1 = u_1^{(1)}$ et e_2 est la restriction à I^2 de $u_2^{(1)}$). Elle montre également que

$w_2(T_\sigma^+) = \binom{r}{2}[A] + \binom{r}{2}(-1,-1)$, ce dont on déduit que $w_2(q_\sigma) = \binom{r}{2}[A]$, puis que

$$\begin{aligned} e_2(q_\sigma) &= w_2(q_\sigma) + (r^2-1)(-1) \cup w_1(q_\sigma) + \binom{r^2-2}{2}(-1,-1) \\ &= \binom{r}{2}[A] + \binom{r^2-2}{2}(-1,-1). \end{aligned}$$

On voit donc que, comme $T_\sigma^+ - T_{\sigma'}^+$ est semblable à $q_\sigma - q_{\sigma'}$, $e_2(T_\sigma^+ - T_{\sigma'}^+) = 0$, ce qui justifie la définition de l'invariant (on voit ici un exemple où l'invariant absolu n'est que de degré 2 a priori, mais la partie de degré 2 ne dépend pas de σ donc elle disparaît quand on considère la version relative).

On peut aller plus loin : lorsque r est divisible par 4, $e_2(q_\sigma) = (-1,-1)$, donc on peut poser $\varphi_\sigma = q_\sigma - \langle\langle -1,-1\rangle\rangle$, et définir un invariant absolu par $e_3(\varphi_\sigma)$. Quel que soit r, lorsque l'indice est au plus 2, on peut poser $\varphi_\sigma = q_\sigma - \binom{r}{2}n_Q + \binom{r^2-2}{2}\langle\langle -1,-1\rangle\rangle$, et encore définir un invariant absolu par $e_3(\varphi_\sigma)$. Ces cas couvrent tous ceux où le discriminant symplectique peut être défini de façon absolue (voir [11], qui utilise une preuve très différente). Il ne reste en réalité que le cas où A est d'indice exactement 4 et de coindice impair, car dans ce cas on a $e_2(q_\sigma) = [A] + (-1,-1)$, et on ne dispose pas d'un relevé canonique de $[A]$ dans $I^2(K)$, ce qui nous empêche de faire notre construction.

On constate en tout cas qu'on peut gérer les obstructions évoquées précédemment dans certains cas, soit en considérant des invariants relatifs, soit en éliminant les obstructions quand elles ne dépendent que de la dimension, soit en les éliminant en indice 2 quand elles ne dépendent que de la dimension et de $[Q]$, en utilisant la forme norme comme relevé canonique de cette classe de Brauer.

3.1.3 Invariants en indice 2

Déploiement générique

On présente ici une méthode due à Berhuy dans [4], basée sur l'isomorphisme décrit au chapitre précédent (voir (2.4.23)) entre $M_Q^d(K)$ et $H_{nr}^d(K(Q),\mu_2)$ pour une algèbre de quaternions Q sur K. On présente ici une variation de l'énoncé de Berhuy.

Soit F un sous-foncteur de I ou de Quad, le foncteur de $\mathbf{Field}_{/k}$ vers $\mathbf{Set}$ donné par les classes d'isométries de formes quadratiques. On suppose que F est stable par similitude : pour tout K/k, si $q \in F(K)$ alors $\langle\lambda\rangle q \in F(K)$ pour tout $\lambda \in K^*$; c'est notamment le cas si $F = I^n$. Soit Q une algèbre de quaternions sur k ; à partir de F et de Q, on définit le foncteur F_Q sur $\mathbf{Field}_{/k}$ tel que $F_Q(K)$ soit l'ensemble des classes d'isométrie de formes anti-hermitiennes h relativement à $(Q_K, \bar{\ })$ pour lesquelles, quelle que soit l'extension L/K déployant Q, il existe $q \in F(L)$ tel que $h_L \simeq q$ pour une certaine équivalence de Morita (et par hypothèse sur F s'il existe un tel q, alors tous les autres q tels que $h_L \simeq q$ sont aussi dans $F(L)$).

Soit maintenant $\alpha \in \mathrm{Inv}^d(F, \mu_2)$. On définit le sous-foncteur $F_{\alpha,Q} \subset F_Q$ par la condition que $h \in F_Q(K)$ est dans $F_{\alpha,Q}(K)$ si et seulement si pour tout $q \in F(L)$ tel que $h_L \simeq q$ où L déploie Q, pour tout $\lambda \in L^*$ on a $\alpha(\langle\lambda\rangle q) = \alpha(q)$. Notamment, si α est invariant par similitude, alors $F_{\alpha,Q} = F_Q$.

Remarque 3.1.5. Par construction, si (A, σ) est une algèbre à involution orthogonale d'indice 2 sur K, et si Q_K est l'algèbre de quaternions Brauer-équivalente à A, alors cela a un sens de dire que $\sigma \in F_Q(K)$ ou que $\sigma \in F_{\alpha,Q}(K)$, puisque F_Q et $F_{\alpha,Q}$ sont stables par similitude.

Enfin, on dit que α est non ramifié si pour tout corps K muni d'une k-valuation discrète de rang 1, si $q \in F(K)$ est non ramifiée alors $\alpha(q) \in H^d(K, \mu_2)$ est une classe non ramifiée. On arrive alors à l'énoncé adapté de celui de Berhuy :

Proposition 3.1.6. *Si α est non-ramifié, alors il existe un unique $\hat{\alpha} \in \mathrm{Inv}(F_{\alpha,Q}, M_Q^d)$ tel que pour tout K/k déployant Q, tout $h \in F_{\alpha,Q}(K)$ et tout $q \in F(K)$ tel que $\sigma_h \simeq \sigma_q$ on ait $\hat{\alpha}(h) = \alpha(q)$.*

On notera souvent $\hat{\alpha}$ simplement α puisque par construction ils coïncident dans les cas où ils ont tous les deux un sens.

On peut reprendre la preuve donnée dans [4, prop 9], à ceci près que dans l'énoncé original on n'a pas de condition sur α vis-à-vis des similitudes. Or il est indispensable de rajouter une condition de ce type (éventuellement une variante) pour avoir une compatibilité avec les équivalences de Morita, qui ne permettent de définir une forme quadratique à partir d'une forme anti-hermitienne quaternionique qu'à similitude près. On donnera également une autre justification plus loin.

Remarque 3.1.7. Suivant la démarche de la remarque 3.1.5, on peut aussi bien définir $\hat{\alpha}$ sur des involutions plutôt que des formes anti-hermitiennes : si $(A, \sigma) \in F_{\alpha,Q}(K)$, on peut définir $\hat{\alpha}(A, \sigma) \in M_Q^d(K)$ (simplement en appliquant $\hat{\alpha}$ à n'importe quelle forme anti-hermitienne induisant σ).

L'exemple naturel est $F = I^n$, qui est bien stable par similitude. On sait alors (voir la proposition 1.2.69) que tout $\alpha \in \mathrm{Inv}(I^n, \mu_2)$ est non ramifié. Si $\widetilde{\alpha} = 0$, on peut alors définir $\alpha(A, \sigma)$ pour toute algèbre à involution orthogonale d'indice 2 « génériquement dans I^n ».

On peut même obtenir un peu mieux : si α est quelconque, alors on peut toujours définir $\widetilde{\alpha}(A, \sigma)$ puisque $\widetilde{\alpha}$ est invariant par similitude (voir la remarque 1.2.64), et alors si $\widetilde{\alpha}(A, \sigma) = 0$, on peut définir $\alpha(A, \sigma)$. On peut donc interpréter $\widetilde{\alpha}(A, \sigma)$ comme une obstruction au fait que $\alpha(A, \sigma)$ soit défini. En effet, si $\widetilde{\alpha}(A, \sigma) = 0$, cela signifie que pour toute extension de déploiement L et tout $q \in I^n(L)$ tel que $\sigma_L \simeq \sigma_q$, on a $\widetilde{\alpha}(q) = 0$, donc $\alpha(q)$ ne dépend que de la classe de similitude de q, autrement dit $\sigma \in F_{\alpha,Q}(K)$.

On donne une autre façon de comprendre ce phénomène. On part de $\alpha \in \mathrm{Inv}^d(I^n, \mu_2)$, qu'on relève en un invariant de Witt $\beta \in \mathrm{Inv}(I^n, I^d)$. Soit $h \in GW^-(Q, ^-)$ de dimension $2r$, tel que $\sigma_h = \sigma$. On étend les scalaires de façon à considérer $h_{K(Q)} \in GW^-(Q_{K(Q)}, ^-)$, et on choisit une équivalence de Morita entre $(Q_{K(Q)}, ^-)$ et $(K(Q), \mathrm{Id})$ qui fait correspondre h à un certain $q \in GW(K(Q))$ (qui est donc bien défini seulement à similitude près), dont par hypothèse la classe de Witt est dans $I^n(K(Q))$. On pose $q' = q - r\mathcal{H} \in \hat{I}^n(K(Q))$, et alors $\beta(q') \in \hat{I}^d(K(Q))$. On rappelle (voir la partie 2.4.5) que si l'équivalence de Morita choisie correspond à un certain point fermé $\infty \in C$ où C est la variété de Severi-Brauer de Q, alors $q' \in W_{nr,1,\infty}(K(Q))$. De plus il est facile de voir que pour tout $i \in \mathbb{N}^*$, $\lambda^i(q')$ est dans $W_{nr,1,\infty}(K(Q))$ si i est impair, et dans $W_{nr,1,\infty}(K(Q))$ si i est pair. En particulier, comme $-\widetilde{\beta}$ est la partie impaire de β, et $\beta + \widetilde{\beta}$ est sa partie paire (voir la remarque 1.2.64), on a $\beta(q')$ somme de $-\widetilde{\beta}(q') \in I^{d-1}(K(Q)) \cap W_{nr,1,\infty}(K(Q))$ (qui est bien définie à similitude près) et de $(\beta+\widetilde{\beta})(q') \in I^{d-1}(K(Q)) \cap W_{nr,2,\infty}(K(Q))$ (qui est bien définie). En général, on voit que la somme des deux n'est ni dans $W_{nr,1,\infty}(K(Q))$ ni dans $W_{nr,2,\infty}(K(Q))$, et donc $\alpha(q) = e_d(\beta(q'))$ n'a aucune raison d'être non ramifié. En revanche, lorsque $\widetilde{\beta}(q') \in I^d(K(Q))$, ce qui correspond précisément à l'hypothèse $\widetilde{\alpha}(A,\sigma) = 0$, alors on peut écrire $\alpha(q) = e_d(-\widetilde{\beta}(q')) + e_d((\beta+\widetilde{\beta})(q'))$, et chacune de ces deux classes de cohomologie est non ramifiée qui est bien définie indépendamment de tout choix. On peut alors définir $\alpha(A,\sigma)$ comme l'élément de $M_Q^d(K)$ correspondant.

Méthodes rationnelles

Au lieu d'utiliser le déploiement générique pour se ramener au cas de formes quadratiques, on peut mobiliser les méthodes développées dans la section 3.1, combinées au traitement spécifique qu'on a accordé aux algèbres d'indice 2 dans le chapitre précédent, pour directement travailler au niveau des formes anti-hermitiennes.

Si on reprend les considérations de la partie précédente, et qu'on suppose que $\deg(A)$ est divisible par 4, donc que r est pair, alors q' provient par extension des scalaires de $h' = h - h_0 \in \widetilde{GW}(Q, ^-)$ où $h_0 \in GW^-(Q, ^-)$ est hyperbolique de dimension $2r$. Il faut alors voir q' comme étant dans la composante impaire de $\widetilde{GW}(K(Q)) = GW^{\pm}(K(Q))[\mathbb{Z}/2\mathbb{Z}]$, et alors si on écrit $\beta(h') = x + y$ avec $x \in GW(K)$ et $y \in GW^-(Q, ^-)$, on obtient que $-\widetilde{\beta}(q') = x_{K(Q)}$, et $(\beta + \widetilde{\beta})(q')$ correspond à travers l'équivalence de Morita choisie à $y_{K(Q)}$. En général, on sait par le corollaire 3.1.3 que la classe de Witt de $\beta(h')$ est dans $\widetilde{I}_0^d(Q, ^-)$, donc par la proposition 2.4.24 on obtient un invariant à valeurs dans $N_Q^{d-1}(K) = H^{d-1}(K, \mu_2)/[Q]H^{d-3}(K, \mu_2)$, qui est exactement $\widetilde{\alpha}(A,\sigma)$, mais en restant au niveau du corps de base on a gardé suffisamment de contrôle pour garantir que la classe est dans $N_Q^{d-1}(K)$ et non simplement dans $M_Q^{d-1}(K)$. De plus, si cette classe est nulle alors à nouveau on peut définir $\alpha(A,\sigma)$ à valeurs dans $N_Q^d(K)$ et non simplement dans $M_Q^d(K)$.

Si r n'est pas nécessairement pair, on ne peut pas normaliser h de la sorte, et on prend plutôt $h' = h - r\mathcal{H} \in \widetilde{GI}(Q, ^-)$, où $\mathcal{H}$ désigne le plan hyperbolique dans

$GW(K)$. On a alors encore $\beta(h') \in \widetilde{I}_0^d(Q, ^-)$, donc on en retire un invariant à valeurs dans $N_Q^{d-1}(K)$ (et s'il est nul on peut en déduire un invariant dans $N_Q^d(K)$). En revanche ces invariants ne coïncident plus tout à fait avec ceux obtenus par la méthode de Berhuy à cause du choix de normalisation différent.

On présente un exemple un peu détaillé, le cas de $\beta = g_1^d \in \mathrm{Inv}(I, I^d)$. On part donc de $h = \langle z_1, \ldots, z_r\rangle \in GW^-(Q, ^-)$ et on veut calculer la composante dans $GW(K)$ de $g_1^d(h')$ avec $h' = h - r\mathcal{H}$, ou disons son image dans $W(K)$. Déjà on peut se limiter à d pair, puisque si d est impair $g_1^d(h') \in GW^-(Q, ^-)$. On utilise alors les formules de la proposition 1.2.71, et on est donc amené à calculer

$$q = \sum_{i=0}^{d} \binom{r-i}{d-i} \lambda^{2i}(h),$$

dont on sait a priori qu'il est dans $I^d(K)$, et qu'après extension des scalaires à $K(Q)$ il donne un élément de $I^{2d-1}(K(Q))$.

Proposition 3.1.8. *La composante symétrique de $g_1^{2d}(h - r\mathcal{H}) \in \widetilde{I}^d(Q, ^-)$ est donnée par*

$$\sum_{s=0}^{d} \sum_{i_1<\cdots<i_{2s}} \langle z_{i_1}\rangle \cdots \langle z_{i_{2s}}\rangle \left(\sum_{t=d-2s}^{d-s} \binom{s}{d-s-t} \sum_{\substack{j_1<\cdots<j_t \\ j_i,\ldots,j_t \neq i_1,\ldots i_{2s}}} \langle\langle z_{j_1}^2, \ldots, z_{j_t}^2\rangle\rangle \right)$$

(où la somme entre parenthèses vaut $\binom{s}{d-s}$ si $t = 0$, et est nulle si $t < 0$).

Démonstration. On a dans $W(K)$:

$$\begin{aligned}
&\sum_{i=0}^{d} \binom{r-i}{d-i} \lambda^i(h) \\
&= \sum_{i=0}^{d} \binom{r-i}{d-i} \sum_{s=0}^{i} \sum_{i_1<\cdots<i_{2s}} \sum_{\substack{j_1<\cdots<j_{i-s} \\ j_i,\ldots,j_{i-s} \neq i_1,\ldots i_{2s}}} \langle(-z_{j_1}^2)\cdots(-z_{j_{i-s}}^2)\rangle \langle z_{i_1}\rangle \cdots \langle z_{i_{2s}}\rangle \\
&= \sum_{s=0}^{d} \sum_{i_1<\cdots<i_{2s}} \langle z_{i_1}\rangle \cdots \langle z_{i_{2s}}\rangle \left(\sum_{t=0}^{d-s} (-1)^t \binom{r-s-t}{d-s-t} \lambda^t(\psi_{i_1,\ldots,i_{2s}}) \right)
\end{aligned}$$

où $\psi_{i_1,\ldots,i_{2s}} = \langle z_1^2, \ldots, z_r^2\rangle$ dans laquelle ne figurent pas les $z_{i_1}^2, \ldots, z_{i_{2s}}^2$ (donc $\psi_{i_1,\ldots,i_{2s}}$ est de dimension $r - 2s$). On doit donc montrer que pour une forme de dimension $r - 2s$ on a

$$\sum_{t=0}^{d-s} (-1)^t \binom{r-s-t}{d-s-t} \lambda^t = \sum_{t=d-2s}^{d-s} \binom{s}{d-s-t} P^t.$$

Or (voir 1.2.74) en dimension $r-2s$

$$P^t = \sum_{i=0}^{t} (-1)^i \binom{r-2s-i}{t-i} \lambda^i,$$

donc

$$\begin{aligned}\sum_{t=d-2s}^{d-s} \binom{s}{d-s-t} P^t &= \sum_{t=d-2s}^{d-s} \sum_{i=0}^{t} (-1)^i \binom{r-2s-i}{t-i} \binom{s}{d-s-t} \lambda^i \\ &= \sum_{i=0}^{d-s} (-1)^i \left(\sum_{t=i}^{d-s} \binom{r-2s-i}{t-i} \binom{s}{d-s-t} \right) \lambda^i.\end{aligned}$$

Or $\sum_t \binom{r-2s-i}{t-i}\binom{s}{d-s-t} = \binom{r-s-i}{d-s-i}$ par la formule de Vandermonde, d'où le résultat. $\square$

Remarque 3.1.9. On retrouve sur cette formule le fait que cet élément est dans $I^d(K)$, et aussi qu'il est nul sur $r < 2d$.

On peut également écrire (voir 2.2.24 pour la définition des $\varphi_{z_{a_1},\dots,z_{a_p}}$) :

Corollaire 3.1.10. *Si $d \geqslant 2$, la forme ci-dessus est aussi égale à*

$$\binom{r}{d} \langle\langle -1 \rangle\rangle^{d-2} n_Q + \sum_{p=d}^{2d} \sum_{a_1<\cdots<a_p} \varphi_{z_{a_1},\dots,z_{a_p}} \left(\sum_{s=0}^{\lfloor p/2 \rfloor} \binom{s}{d+s-p} \omega_s(z_{a_1},\dots,z_{a_p}) \right)$$

où $\omega_s(z_1,\dots,z_p) = \sum_{i_1<\cdots<i_{2s}} \langle (-1)^s \operatorname{Trd}_Q(z_{i_1}z_{i_2}) \cdots \operatorname{Trd}_Q(z_{i_{2s-1}}z_{i_{2s}}) \rangle$.

Démonstration. On part de la formule de la proposition, en écrivant

$$\langle z_{i_1} \rangle \cdots \langle z_{i_{2s}} \rangle = \langle (-1)^s \operatorname{Trd}_Q(z_{i_1}z_{i_2}) \cdots \operatorname{Trd}_Q(z_{i_{2s-1}}z_{i_{2s}}) \rangle \varphi_{z_{i_1},\dots,z_{i_{2s}}}.$$

On pose $p = 2s+t$, et $\{a_1,\dots,a_p\} = \{i_1,\dots,i_{2s}\} \cup \{j_1,\dots,j_t\}$. Alors si $s > 0$ on a

$$\langle\langle z_{j_1}^2,\dots,z_{j_t}^2 \rangle\rangle \varphi_{z_{i_1},\dots,z_{i_{2s}}} = \varphi_{z_{a_1},\dots,z_{a_p}},$$

tandis que si $s = 0$ (auquel cas $t = p = d$),

$$\langle\langle z_{j_1}^2,\dots,z_{j_d}^2 \rangle\rangle = \langle\langle -1 \rangle\rangle^{d-2} n_Q + \varphi_{z_{j_1},\dots,z_{j_d}}.$$

Le cas $s = 0$ correspond à $\binom{r}{d}$ termes (donnés par chaque choix des $j_1,\dots,j_d$), ce qui donne le $\binom{r}{d}\langle\langle -1 \rangle\rangle^{d-2} n_Q$. Les autres termes correspondent simplement au regroupement donné en sommant d'abord sur p puis sur s. $\square$

Remarque 3.1.11. On constate que l'invariant e_d de la forme est

$$\binom{r}{d}(-1,\ldots,-1)\cup[Q].$$

En effet, il correspond au terme $\binom{r}{d}\langle\langle -1\rangle\rangle^{d-2}n_Q$, puisque les termes pour $p > d$ sont dans I^p donc ne contribuent pas, et devant chaque $\varphi_{z_{a_1},\ldots,z_{a_d}} \in I^d$ on a $\sum_{s=0}^{\lfloor d/2\rfloor}\omega_s(z_{a_1},\ldots,z_{a_d})$ qui est de dimension $\sum_{s=0}^{\lfloor d/2\rfloor}\binom{d}{2s} = 2^{d-1}$, donc est au moins dans I.

On en déduit que la version relative de cet invariant est au moins à valeur dans I^{d+1}, donc on peut en déduire un invariant relatif de degré au moins $d+1$; de plus, on peut soustraire $\binom{r}{d}\langle\langle -1\rangle\rangle^{d-2}n_Q$ à cette forme, ce qui nous donne un invariant absolu directement à valeurs dans I^{d+1}.

3.2 Autour de l'équivalence entre A_3 et D_3

Dans cette partie on souhaite calculer de façon explicite l'équivalence entre algèbres de type A_3 et D_3. On commence pour cela par expliquer comment on peut définir une involution sur un produit croisé.

3.2.1 Produits croisés à involution

On veut donc décrire à l'aide d'un produit croisé une algèbre à involution. Pour couvrir les cas qui nous intéressent, on doit inclure les involutions unitaires, et donc potentiellement des algèbres qui ne sont pas simples dans le cas où l'extension quadratique centrale est déployée. De plus, on veut autoriser la sous-algèbre galoisienne donnant le produit croisé à être seulement étale et non un corps.

On notera pour cette partie k notre corps de base, et K sera simplement une algèbre étale (généralement quadratique) sur k, et non plus une extension de corps comme dans le reste de la thèse. On rappelle que si K est une k-algèbre étale, on a $K = \prod_{\mathfrak{p}\in\mathrm{Spec}(K)} K_{\mathfrak{p}}$, où $K_{\mathfrak{p}}$ est une extension finie séparable de k.

Algèbres galoisiennes

On commence par quelques rappels sur les algèbres galoisiennes quand l'anneau de base est une algèbre étale sur un corps.

Définition 3.2.1. Soit K une k-algèbre étale. Soient L une K-algèbre étale et G un sous-groupe de $\mathrm{Aut}_K(L)$. On dit que L est G-galoisienne sur K si pour tout $\mathfrak{p} \in \mathrm{Spec}(K)$, $L_{\mathfrak{p}}/K_{\mathfrak{p}}$ est étale de degré $|G|$ et l'action de G sur $L_{\mathfrak{p}}$ est fidèle.

La proposition suivante résume les propriétés élémentaires des algèbres galoisiennes dans ce contexte (voir [8] pour des preuves).

Proposition 3.2.2. *L est G-galoisienne sur K si et seulement s'il existe $K'_\mathfrak{p}/K_\mathfrak{p}$ extension galoisienne de corps de groupe $H_\mathfrak{p} \subset G$ telle que $L_\mathfrak{p} = \mathrm{Ind}_{H_\mathfrak{p}}^G(K'_\mathfrak{p})$, i.e. $L_\mathfrak{p} = (K'_\mathfrak{p})^{[G:H_\mathfrak{p}]}$ en tant que $K_\mathfrak{p}$-algèbre, et G agit sur $L_\mathfrak{p}$ en permutant les copies de $K'_\mathfrak{p}$ selon l'action régulière sur $G/H_\mathfrak{p}$ et en agissant comme $H_\mathfrak{p}$ sur les copies de $K'_\mathfrak{p}$.*

L'application $H \mapsto L^H$ donne une correspondance bijective entre les sous-groupes de G et les sous-algèbres M de L telles que $M_\mathfrak{p}/K_\mathfrak{p}$ est séparable et chaque élément de G agit soit trivialement sur M, soit non-trivialement sur chaque $M_\mathfrak{p}$ (sans forcément les stabiliser).

De plus, si $H \subset G$, L est H-galoisienne sur L^H.

Si pour tout $\mathfrak{p} \in \mathrm{Spec}(K)$, $L_\mathfrak{p}/K_\mathfrak{p}$ est une extension de corps, alors L est G-galoisienne sur K si et seulement si pour tout $\mathfrak{p} \in \mathrm{Spec}(K)$, $L_\mathfrak{p}/K_\mathfrak{p}$ est galoisienne au sens usuel des extensions de corps, de groupe de Galois G, et G agit diagonalement sur L. En particulier dans ce cas G est entièrement déterminé par L/K ; le fait d'être galoisienne est juste une propriété de l'algèbre.

Mais dans le cas général, L/K peut être galoisienne pour différents G non isomorphes, y compris lorsque K est un corps. En effet, si K'/K est une extension galoisienne de corps, alors le théorème montre que pour tout G tel que H soit un sous-groupe d'indice r, l'algèbre $L = (K')^r$ est G-galoisienne avec l'action de permutation de G sur G/H (l'idée étant que $\mathrm{Aut}_K(L)$ est gros : il contient au moins le groupe symétrique S_r).

Une version de Skolem-Noether

L'ingrédient essentiel de la construction des produits croisés est le théorème de Skolem-Noether, qui permet à partir d'un sous-corps galoisien d'une algèbre simple d'obtenir des éléments qui agissent par conjugaison comme le groupe de Galois. Or on sait qu'en général on n'a pas d'équivalent du théorème de Skolem-Noether pour des sous-algèbres semi-simples d'algèbres d'Azumaya (même sur un corps).

Exemple 3.2.3. Les deux plongements $(a,b) \mapsto diag(a,a,b)$ et $(a,b) \mapsto diag(a,b,b)$ de k^2 dans $M_3(k)$ ne sont pas conjugués.

On va donc donner un énoncé un peu plus fin pour travailler avec des sous-algèbres étales (plus fin que ce dont on a strictement besoin, par ailleurs).

Définition 3.2.4. Soit K une k-algèbre étale, et soit E une algèbre d'Azymaya sur K. Soit M une sous-K-algèbre séparable de E. On définit la *signature* du plongement $M \to E$ comme la fonction $\mathrm{Spec}(L) \to \mathbb{N}$ donnée par $\mathfrak{p} \mapsto \deg(C_\mathfrak{p})$ où $L = Z(M)$ et $C_\mathfrak{p} = C_{E_\mathfrak{p}}(M_\mathfrak{p})$.

La signature dépend en général du plongement particulier de M dans E, mais on voit facilement que deux plongements conjugués ont la même signature, ce qui justifie la validité de l'exemple 3.2.3 (les signatures des deux plongements étant respectivement de la forme $(2,1)$ et $(1,2)$). Réciproquement :

Proposition 3.2.5. *Soit K une k-algèbre étale, et soit E une algèbre d'Azumaya sur K. Soit M une K-algèbre séparable, et soient $j_1, j_2 : M \longrightarrow E$ deux K-plongements. S'ils ont la même signature, alors j_1 et j_2 sont conjugués dans E.*

Démonstration. On va imiter la preuve de la version classique (voir par exemple [14, thm 4.9]). On pose $A = M \otimes_K E^{op}$, qui est une algèbre d'Azumaya sur $Z(M)$. On définit alors deux actions de A sur E : $(a \otimes b) \cdot_i x = j_i(a)xb$ pour $i = 1, 2$; on note E_i pour désigner E muni de la structure de A-module correspondante. Alors $\mathrm{End}_A(E_i) = C_A(j_i(A))$ de façon naturelle, et par hypothèse ces deux algèbres sont isomorphes. Or pour une algèbre séparable sur un corps, deux modules ayant des algèbres d'endomorphismes isomorphes sont isomorphes. On a donc un isomorphisme K-linéaire $\varphi : E \to E$ telle que $\varphi(j_1(a)xb) = j_2(a)\varphi(x)b$ pour tous $a \in M$, $x, b \in E$. En prenant $a = 1$, on voit que $\varphi(xb) = \varphi(x)b$ donc $\varphi(x) = ex$ pour $e = \varphi(1) \in E^*$, et en prenant $x = b = 1$ on obtient $ej_1(a) = j_2(a)e$, donc j_1 et j_2 sont conjugués par e. □

Dans la situation de la proposition, si $M = L$ est commutative (donc étale sur K), on dit qu'elle est *strictement maximale* si pour tout $\mathfrak{p} \in \mathrm{Spec}(K)$, $\dim_{K_\mathfrak{p}}(L_\mathfrak{p}) = \deg(E_\mathfrak{p})$ (autrement dit elle est de dimension maximale possible étant donné le degré local de E).

Corollaire 3.2.6. *Soit K une k-algèbre étale, et soit E une algèbre d'Azumaya sur K. Soit $L \subset E$ une sous-K-algèbre étale strictement maximale. Alors tout K-automorphisme de L s'étend en un automorphisme intérieur de E, et l'élément réalisant la conjugaison est unique à multiplication par L^* près.*

Démonstration. Un automorphisme de L définit un deuxième plongement de L dans E en le composant avec l'inclusion naturelle. Or comme L est strictement maximale, on doit avoir $C_E(L) = L$ quel que soit le plongement, donc la signature est nécessairement la même. Ces deux plongements sont donc conjugués dans E, ce qui revient exactement à dire que l'automorphisme de L se prolonge en un automorphisme intérieur. L'élément réalisant la conjugaison est déterminé à un facteur dans $C_E(L)$ près, mais $C_E(L) = L$. □

Produits croisés

On se donne K une algèbre étale sur k, E une algèbre d'Azumaya sur K, et $L \subset E$ une sous-K-algèbre G-galoisienne strictement maximale. On dit alors que E est un produit croisé de L par G.

On peut alors appliquer le corollaire 3.2.6 pour imiter la situation classique et choisir pour tout $g \in G$ un élément $u_g \in E^*$ qui induit par conjugaison l'automorphisme g sur L. On vérifie en regardant la dimension que $E = \bigoplus_{g \in G} L \cdot u_g$.

On a u_g bien défini à multiplication par un élément de L^* près, donc en particulier, comme la conjugaison par $u_g u_h$ induit l'automorphisme gh, on a $\alpha(g, h) \in L^*$ tel que

$$u_g u_h = \alpha(g, h) u_{gh} \qquad (3.2.7)$$

et on vérifie comme dans le cas usuel que l'associativité de E est équivalente au fait que α soit un 2-cocycle de G à valeurs dans L^*, et qu'un choix différent de u_g donne un cocycle cohomologue de la façon naturelle, et ainsi on obtient avec exactement la même preuve la bijection usuelle entre $H^2(G, L^*)$ et les classes d'isomorphismes de produits croisés de L par G (le seul ingrédient supplémentaire est la version du théorème de Skolem-Noether énoncée précédemment).

Notons qu'on prendra toujours $u_1 = 1$, ce qui correspond au fait que le cocycle soit normalisé.

Descente

En gardant les mêmes notations, soit V un E-module à droite, et soit $A = \mathrm{End}_E(V)$. Alors V_L est un A_L-E_L-bimodule simple ; de plus, $E \otimes_K L$ agit à gauche sur E par $(a \otimes \lambda) \cdot x = ax\lambda$, et $A \otimes_K L$ agit à gauche sur V par $(a \otimes \lambda) \cdot v = av\lambda$. Cela donne un triangle commutatif dans $\mathbf{Mor}(K)$ (voir la remarque 2.1.1) :

$$\begin{tikzcd} & E_L \arrow[dl, "V_L"'] \arrow[dr, "E"] & \\ A_L \arrow[rr, "V"] & & L. \end{tikzcd}$$

On a donc une identification canonique $A_L = \mathrm{End}_L(V)$, et on doit pouvoir en déduire une action naturelle de G sur $\mathrm{End}_L(V)$. On pose pour tout $g \in G$

$$\begin{array}{rccc} T_g : & V & \longrightarrow & V \\ & v & \longmapsto & vu_g^{-1} \end{array} \tag{3.2.8}$$

et

$$\begin{array}{rccc} S_g : & \mathrm{End}_L(V) & \longrightarrow & \mathrm{End}_L(V) \\ & f & \longmapsto & T_g \circ f \circ T_g^{-1} \end{array} . \tag{3.2.9}$$

Proposition 3.2.10. *La fonction $g \mapsto S_g$ définit une action semi-linéaire de G sur $\mathrm{End}_L(V)$ qui coïncide avec l'action galoisienne naturelle sur A_L. En particulier, la sous-algèbre des éléments invariants est $A = \mathrm{End}_E(V) \subset \mathrm{End}_L(V)$.*

Démonstration. La composition $S_g S_h$ est la conjugaison par $T_g T_h$, qui est la multiplication à droite par $u_h^{-1} u_g^{-1}$, qui à un élément de L^* près est u_{gh}^{-1}, donc par L-linéarité des éléments de $\mathrm{End}_L(V)$, $S_g S_h = S_{gh}$. De plus, $S_g(f\lambda)(v) = (f(vu_g)\lambda)u_g^{-1} = f(vu_g)u_g^{-1} g(\lambda)$, donc S_g est bien semi-linéaire, d'action g sur L.

Pour montrer que c'est l'action galoisienne naturelle sur A_L, il suffit de montrer que A est bien l'ensemble des points fixes. Or $S_g(f) = f$ est équivalent à $f(vu_g) = f(v)u_g$ pour tout $v \in V$, donc les points fixes sous l'action des S_g sont exactement les f qui commutent avec l'action des u_g, ce qui est équivalent à commuter avec l'action de E puisque E est engendré par les u_g et L. $\square$

Involutions

On décrit maintenant comment définir une involution sur un produit croisé, en conservant les notations précédentes.

Définition 3.2.11. On dit qu'une involution θ sur E est G-centrée sur L si $\theta(L) = L$ et $\theta_{|L} G \theta_{|L} = G$.

Remarque 3.2.12. La dernière hypothèse est automatiquement vérifiée si L est un corps, puisque dans ce cas $G = \mathrm{Aut}_K(L)$, et la restriction de θ à K est un automorphisme d'ordre au plus 2.

On se munit pour la suite d'une involution θ G-centrée sur L. Pour tout $g \in G$, on notera

$$\overline{g} = \theta_{|L} g^{-1} \theta_{|L}, \tag{3.2.13}$$

et

$$\theta_g = g\theta_{|L}, \quad \theta'_g = g^{-1}\theta_{|L}. \tag{3.2.14}$$

Remarque 3.2.15. Les automorphismes θ_g et θ'_g sont chacun involutifs si et seulement si $g = \overline{g}$, ce qui est par exemple le cas pour $g = 1$, auquel cas $\theta_g = \theta'_g = \theta$. Si $\theta_{|L} \in G$ (ce qui arrive notamment lorsque L est un corps et θ est de première espèce), alors on peut prendre $g = \theta_{|L}$ et dans ce cas $\theta_g = \theta'_g = \mathrm{Id}$.

Proposition 3.2.16. *Pour tout $g \in G$, il existe un unique $\mu_g \in L^*$ tel que*

$$\theta(u_g) = \mu_g u_{\overline{g}}, \tag{3.2.17}$$

qui vérifie

$$\mu_{\overline{g}} \theta_g(\mu_g) = 1 \tag{3.2.18}$$

et

$$\mu_h \overline{g}(\mu_g) \alpha(\overline{h}, \overline{g}) = \mu_{gh} \theta_{\overline{gh}}(\alpha(g,h)). \tag{3.2.19}$$

De plus, si on remplace les u_g par $c_g u_g$ avec $c_g \in L^*$, on trouve $\mu'_g = \mu_g \frac{\theta_{\overline{g}}(c_g)}{c_{\overline{g}}}$.

Réciproquement, si $\theta \in \mathrm{Aut}_k(L)$ est un automorphisme d'ordre au plus 2 tel que $\theta G \theta = G$, et si on se donne $(\mu_g)_{g \in G}$ vérifiant les équations (3.2.18) et (3.2.19), alors θ s'étend de façon unique en une involution de E vérifiant (3.2.17).

Démonstration. Soit $\lambda \in L$. Alors $\theta(\theta(\lambda)u_g) = \theta(u_g)\lambda$ mais aussi

$$\begin{aligned} \theta(\theta(\lambda)u_g) &= \theta(u_g(g^{-1}\theta)(\lambda)) \\ &= (\theta g^{-1}\theta)(\lambda)\theta(u_g) \end{aligned}$$

donc $\theta(u_g)$ agit comme $\overline{g}$ sur L, et donc il existe un unique $\mu_g \in L^*$ tel que $\theta(u_g) = \mu_g u_{\overline{g}}$.

On a

$$\begin{aligned}\theta(\theta(u_g)) &= \theta(\mu_g u_{\overline{g}})\\ &= \mu_{\overline{g}} u_g \theta(\mu_g)\\ &= \mu_{\overline{g}}(g\theta)(\mu_g)u_g\end{aligned}$$

d'où la formule (3.2.18). De plus,

$$\begin{aligned}\theta(u_g u_h) &= \theta(\alpha(g,h)u_{gh})\\ \mu_h u_{\overline{h}}\mu_g u_{\overline{g}} &= \mu_{gh}u_{\overline{gh}}\theta(\alpha(g,h))\\ \mu_h\overline{g}(\mu_g)\alpha(\overline{h},\overline{g})u_{\overline{gh}} &= \mu_{gh}\theta_{\overline{gh}}(\alpha(g,h))u_{\overline{gh}}\end{aligned}$$

d'où la formule (3.2.19). Si on remplace u_g par $u'_g = c_g u_g$, alors

$$\begin{aligned}\theta(u'_g) &= \theta(u_g)\theta(c_g)\\ &= \mu_g(\overline{g}\theta)(c_g)u_{\overline{g}}\\ &= \mu_g\frac{\theta_{\overline{g}}(c_g)}{c_{\overline{g}}}u'_{\overline{g}}\end{aligned}$$

d'où la formule de l'énoncé.

Réciproquement, on peut remonter toutes les égalités ci-dessus pour montrer que si on définit θ par les μ_g vérifiant les équations, on obtient bien $\theta(\theta(u_g)) = u_g$ et $\theta(u_g u_h) = \theta(u_h)\theta(u_g)$, et θ définit bien une involution. $\square$

Modules hermitiens et déploiement

Soit (V, h) module ε-hermitien à droite sur (E, θ), et soit $A = \mathrm{End}_E(V)$ munie de $\sigma = \sigma_h$. On est intéressé par la question suivante : comme θ est une involution sur L, on peut considérer l'involution $\sigma \otimes \theta$ sur A_L ; sachant que A_L est déployée, peut-on trouver une forme hermitienne naturelle sur (L, θ) dont c'est l'involution adjointe ?

On va en fait considérer un cadre un peu plus large. On écrit

$$h(x,y) = \sum_{g\in G} u_g h_g(x,y) \tag{3.2.20}$$

avec $h_g : V \times V \longrightarrow L$, uniquement définie par $h_g = \pi_h \circ h$ où

$$\pi_g\left(\sum_t u_t c_t\right) = c_g \tag{3.2.21}$$

(attention, on prend ici la convention d'agir à droite). On pose également f_g : $E \times E \longrightarrow L$ définie par

$$f_g(x,y) = \pi_g(\theta(x)y). \tag{3.2.22}$$

On décrit le comportement général de ces applications :

Lemme 3.2.23. *Soient $g, t \in G$, $x \in E$ et $a, b \in L$. Alors :*

$$\begin{aligned}
\pi_g(axb) &= g^{-1}(a)\pi_g(x)b,\\
\pi_g(\theta(x)) &= g^{-1}(\mu_{\overline{g}})\theta'_g(\pi_{\overline{g}}(x)),\\
\pi_g(u_t x) &= g^{-1}(\alpha(t, t^{-1}g))\pi_{t^{-1}g}(x),\\
\pi_g(xu_t) &= g^{-1}(\alpha(gt^{-1}, t))t^{-1}(\pi_{gt^{-1}}(x)).
\end{aligned}$$

Démonstration. On écrit $x = \sum_g u_g x_g$. Alors $axb = \sum_g a u_g x_g b = \sum_g u_g g^{-1}(a) x_g b$, d'où la première formule. Pour la deuxième :

$$\begin{aligned}
\theta(x) &= \sum_g \theta(x_g)\theta(u_g)\\
&= \sum_g u_{\overline{g}}\overline{g}^{-1}(\mu_g \theta(x_g))\\
&= \sum_g u_g g^{-1}(\mu_{\overline{g}}\theta(x_{\overline{g}})).
\end{aligned}$$

Pour la troisième formule :

$$\begin{aligned}
u_t x &= \sum_g u_t u_g x_g\\
&= \sum_g \alpha(t, g) u_{tg} x_g\\
&= \sum_g \alpha(t, t^{-1}g) u_g x_{t^{-1}g}
\end{aligned}$$

et la quatrième se démontre de façon identique en calculant xu_t. □

Lemme 3.2.24. *Soient $g \in G$, $x, y \in E$ et $a, b \in L$. Alors :*

$$\begin{aligned}
f_g(xa, yb) &= \theta'_g(a) f_g(x, y) b,\\
f_g(y, x) &= g^{-1}(\mu_{\overline{g}})\theta'_g(f_{\overline{g}}(x, y))
\end{aligned}$$

Démonstration. En utilisant la première formule du lemme précédent : $f_g(xa, yb) = \pi_g(\theta(a)\theta(x)yb) = (g^{-1}\theta)(a) f_g(x, y) b$. Puis on applique la deuxième formule du même lemme à $f_g(y, x) = \pi_g(\theta(\theta(x)y))$. □

Lemme 3.2.25. *Soient $g, t \in G$, $x, y \in V$, $a, b \in L$. Alors :*

$$\begin{aligned}
h_g(xa, yb) &= \theta'_g(a) h_g(x, y) b,\\
h_g(y, x) &= \varepsilon g^{-1}(\mu_{\overline{g}})\theta'_g(h_{\overline{g}}(x, y)),\\
h_g(xu_t, y) &= g^{-1}\left(\mu_t \alpha(\overline{t}, \overline{t}^{-1} g)\right) h_{\overline{t}^{-1}g}(x, y),\\
h_g(x, yu_t) &= g^{-1}\left(\alpha(gt^{-1}, t)\right) t^{-1}\left(h_{gt^{-1}}(x, y)\right).
\end{aligned}$$

Démonstration. Sachant que $h_g(x,y) = \pi_g(h(x,y))$, on applique successivement les quatre formules du lemme 3.2.23 aux relations $h(xa,yb) = \theta(a)h(x,y)b$, $h(y,x) = \varepsilon\theta(h(x,y))$, $h(xu_t,y) = \theta(u_t)h(x,y) = \mu_t u_{\bar{t}} h(x,y)$ et $h(x,yu_t) = h(x,y)u_t$. □

On en déduit :

Proposition 3.2.26. *Si $g = \overline{g}$, alors h_g et f_g sont respectivement $\varepsilon\varepsilon_g$-hermitienne et ε_g-hermitienne sur (L,θ'_g), avec $\varepsilon_g = g^{-1}(\mu_g)$. De plus, on a un triangle commutatif dans $\mathbf{Mor}_h(L,\theta'_g)$ (voir la remarque 2.1.10) :*

$$\begin{tikzcd}
 & (E_L, \theta\otimes\theta'_g) \arrow[dr, "f_g"] & \\
(A_L, \sigma\otimes\theta'_g) \arrow[ur, "h_L"] \arrow[rr, "h_g"] & & (L,\theta'_g)
\end{tikzcd}$$

Remarque 3.2.27. Jusqu'ici on a toujours implicitement considéré que les formes étaient ε-hermitiennes avec $\varepsilon = \pm 1$ puisqu'on travaillait avec des involutions de première espèce. Ici si $g \neq \theta$ on a en général θ'_g non triviale sur L, donc une forme peut être ε-hermitienne pour tout ε tel que $\varepsilon\theta'_g(\varepsilon) = 1$.

Démonstration. Si $g = \overline{g}$ alors déjà θ'_g est une involution (voir remarque 3.2.15), et la deuxième formule du lemme 3.2.25 devient

$$h_g(y,x) = \varepsilon g^{-1}(\mu_g)\theta'_g(h_g(x,y))$$

ce qui combiné avec la première formule de ce lemme montre bien que h_g est $\varepsilon\varepsilon_g$-hermitienne relativement à θ'_g.

De même, les deux formules du lemme 3.2.24 montrent que quand $g = \overline{g}$, f_g est ε_g-hermitienne relativement à θ'_g.

On doit alors montrer la relation entre les trois formes hermitiennes. Si on identifie naturellement V à $V_L \otimes_{E_L} E$ par $\Phi : (v\otimes\lambda)\otimes x \mapsto vx\lambda$, on doit alors vérifier que

$$h_g(\Phi((v\otimes\lambda)\otimes x), \Phi((v'\otimes\lambda')\otimes x')) = f_g(x, h_L(v\otimes\lambda, v'\otimes\lambda')x').$$

Or

$$\begin{aligned}
f_g(x, h_L(v\otimes\lambda, v'\otimes\lambda')x') &= \pi_g(\theta(x)h_L(v\otimes\lambda, v'\otimes\lambda')x') \\
&= \pi_g(\theta(x)h(v,v')x'(\theta'_g)(\lambda)\lambda')
\end{aligned}$$

et de l'autre côté

$$\begin{aligned}
h_g(\Phi((v\otimes\lambda)\otimes x), \Phi((v'\otimes\lambda')\otimes x')) &= \pi_g(h(vx\lambda, v'x'\lambda')) \\
&= \pi_g(\theta(\lambda)\theta(x)h(v,v')x'\lambda') \\
&= \theta'_g(\lambda)\pi_g(\theta(x)h(v,v')x'\lambda') \\
&= \pi_g(\theta(x)h(v,v')x'\lambda'(\theta'_g)(\lambda)).
\end{aligned}$$

□

3.2.2 Algèbre de Clifford en indice 2

Soit (A, σ) algèbre à involution orthogonale sur k, qu'on suppose d'indice au plus 2. Soit donc Q l'algèbre de quaternions Brauer-équivalente à A, et on écrit $A = \mathrm{End}_Q(V)$ où V est un Q-module à droite. On a alors $\sigma = \sigma_h$ où h est une forme anti-hermitienne sur $(Q, \bar{\ })$. On choisit une base orthogonale (e_i), qui donne une diagonalisation $h = \langle z_1, \ldots, z_r\rangle$ avec $z_i \in Q$ quaternion pur inversible. On supposera dans la suite que $r \geqslant 2$.

On souhaite décrire explicitement, par générateurs, l'algèbre de Clifford $B = Cl(A, \sigma)$ de (A, σ), munie de son involution canonique τ. La méthode utilisée est tirée de [29], notre apport se situant principalement dans le calcul explicite des relations entre les générateurs. On commence par énoncer le résultat auquel on veut arriver.

Théorème 3.2.28. *On suppose que les z_i donnés par la diagonalisation de h sont k-linéairement indépendants deux à deux. Alors il existe $L \subset B$ sous-k-algèbre étale strictement maximale de la forme $L = k(\xi_1, \ldots, \xi_r)$ avec $\xi_i^2 = z_i^2$, de sorte que $Z(B) = k(\xi)$ où $\xi = \prod_i \xi_i$. L'algèbre L est naturellement G-galoisienne sur k avec $G = (\mathbb{Z}/2\mathbb{Z})^r$, l'involution τ agit comme l'élément $(1, \ldots, 1)$, et $Z(B) = L^H$ où $H \subset G$ est le noyau du morphisme $G \to \mathbb{Z}/2\mathbb{Z}$ donné par la somme des composantes. Le groupe H est engendré par $\tau_{p,q}$ pour tous $p \neq q$, dont les seules composantes non nulles sont en indice p et q. Alors pour tous $p \neq q$ il existe $u_{p,q} \in B$ tels que :*

- *la conjugaison par $u_{p,q}$ induit $\tau_{p,q}$ sur L ;*
- *$\tau(u_{p,q}) = -u_{p,q}$;*
- *si $\{i, j\} \cap \{p, q\} = \emptyset$, $u_{i,j}$ et $u_{p,q}$ commutent ;*
- *$u_{p,q}^2 = Tr_Q(z_p z_q) - 2\xi_p \xi_q$;*
- *si i, p, q sont distincts :*

$$u_{i,p}u_{i,q} = (\lambda_0 - \xi_i + \lambda_p\xi_p - \lambda_q\xi_q - \lambda_{p,q}\xi_p\xi_q)u_{p,q}$$

où $z_i = \lambda_0 + \lambda_p z_p + \lambda_q z_q + \lambda_{p,q} z_p z_q$.

Comme les $\tau_{p,q}$ engendrent H, les $u_{p,q}$ engendrent B avec L, et donc le théorème donne une description complète de la structure de (B, τ). Avant de passer à la preuve proprement dite, on va développer les constructions nécessaires.

Remarque 3.2.29. Si k est infini (ce qu'on peut supposer sans conséquences, puisque sur un corps fini la théorie n'a pas d'intérêt), quitte à changer les e_i, on peut toujours supposer que les z_i sont indépendants deux à deux, et ce sans changer la classe de z_i^2 dans $k^*/(k^*)^2$. En effet, si z_p et z_q sont colinéaires, on remplace e_q par $e_q z$ pour n'importe quel z qui n'est pas dans $k \oplus kz_p$. On peut faire cette modification récursivement sur toutes les paires problématiques, et comme une union finie de plans ne peut pas être égale à Q, on peut toujours trouver un z qui convient.

De plus, quand cette condition est vérifiée, alors $(1, z_p, z_q, z_pz_q)$ forme une k-base de Q pour tous $p \neq q$ donc l'écriture de z_i dans cette base utilisée dans l'énoncé existe toujours et est unique.

Pour prouver le théorème, on va utiliser une méthode de descente. Soit $K \subset Q$ extension quadratique de k (on peut toujours en trouver, sauf si k est quadratiquement clos, auquel cas rien de tout cela n'a d'intérêt), et soit $j \in Q$ un quaternion pur tel que $j\lambda = \overline{\lambda}j$ pour tout $\lambda \in K$. On pose $j^2 = \pi \in k^*$. On a alors $Q = K \oplus jK$. On est donc dans la situation d'un produit croisé à involution (l'algèbre $(Q, ^-)$ munie du sous-corps galoisien K/k de groupe $\mathbb{Z}/2\mathbb{Z}$) et d'un module anti-hermitien (V, h) sur cette algèbre, et on peut appliquer les résultats de la partie précédente.

D'après la proposition 3.2.10, on a donc $A = \mathrm{End}_K(V)^{\mathrm{Gal}(K/k)}$ où si s est l'élément non trivial de $\mathrm{Gal}(K/k)$ on a $s \cdot f = T \circ f \circ T^{-1}$ avec $T(v) = vj^{-1}$. De plus, en appliquant la proposition 3.2.26 à $g = s$ (on est bien ici dans le cas où l'involution se restreint à un élément du groupe de Galois), si on note σ_K l'involution sur $\mathrm{End}_K(V)$ obtenue à partir de $\sigma \otimes \mathrm{Id}$ par identification de A_K et $\mathrm{End}_K(V)$, alors $\sigma_K = \sigma_b$ où $b : V \times V \to K$ est caractérisée par $h(x, y) = a(x, y) + jb(x, y)$.

Lemme 3.2.30. *Pour tous $x, y \in V$, on a*

$$b(T(x), y) = -\frac{1}{\pi}a(x, y) = -\overline{b(x, T(y))}.$$

Démonstration. On applique les deux dernières formules du lemme 3.2.25, avec ici $h_1 = a$, $h_s = b$, et $u_t = u_s = j$. On trouve alors $b(xj, y) = -a(x, y)$ et $b(x, yj) = \overline{a(x, y)}$, et en combinant ces deux formules on trouve le résultat voulu. □

Ainsi, (B, τ) est la descente de $Cl^0(V, b)$ pour l'action galoisienne induite par celle décrite ci-dessus. On décrit cette action :

Proposition 3.2.31. *L'action naturelle de* $\mathrm{Gal}(K/k)$ *sur* $Cl^0(V, b)$ *est donnée pour tous $x, y \in V$ par*

$$s(x \cdot y) = -\pi T(x) \cdot T(y),$$

et $B = Cl^0(V, b)^s$ pour cette action.

Démonstration. On considère l'identification canonique

$$\begin{array}{rccc} \varphi_b : & V \otimes_K V & \longrightarrow & \mathrm{End}_K(V) \\ & x \otimes y & \longmapsto & v \mapsto xb(y, v) \end{array}$$

Alors $s \cdot \varphi_b(x \otimes y) = T \circ \varphi_b(x \otimes y) \circ T^{-1}$ donc

$$\begin{aligned} (s \cdot \varphi_b(x \otimes y))(v) &= xb(y, vj)j^{-1} \\ &= \pi T(x)\overline{b(y, T(v))} \\ &= -\pi T(x)b(T(y), v) \\ &= -\pi \varphi_b(T(x) \otimes T(y))(v). \end{aligned}$$

Donc $s \cdot \varphi_b(x \otimes y)) = \varphi_b(-\pi T(x) \otimes T(y))$, d'où le résultat puisque l'action sur $Cl^0(V,b)$ est caractérisée par l'action sur l'image de φ_b. □

On sait que B est engendrée par l'image du morphisme canonique $\psi : V \otimes_Q ({}^\gamma V) \to Cl(A,\sigma)$. On va décrire de façon explicite ce morphisme :

Proposition 3.2.32. *La composition de ψ avec l'injection canonique $Cl(A,\sigma) \hookrightarrow Cl^0(V,b)$ est donné par*

$$\psi(x \otimes y) = \pi(T(x) \cdot y - x \cdot T(y)).$$

Démonstration. Il s'agit de vérifier que l'application f définie par $f(x \otimes y) = \pi(T(x) \otimes y - x \otimes T(y))$ fait commuter le diagramme

$$\begin{array}{ccc} V \otimes_Q^\gamma V & \xrightarrow{f} & V \otimes_K V \\ \downarrow{\scriptstyle \varphi_h} & & \downarrow{\scriptstyle \varphi_b} \\ \mathrm{End}_Q(V) & \longrightarrow & \mathrm{End}_K(V). \end{array}$$

Or :

$$\begin{aligned} \varphi_b(f(x \otimes y))(v) &= \varphi_b(\pi(T(x) \otimes y - x \otimes T(y)))(v) \\ &= \pi(T(x)b(y,v) - xb(T(y),v)) \\ &= x(jb(y,v) - a(y,v)) \\ &= \varphi_h(x \otimes y)(v) \end{aligned}$$

où on a utilisé les relations du lemme 3.2.30. □

On peut passer à la preuve du théorème :

Démonstration. Pour tous $x, y \in V$, on pose $u(x,y) = \frac{1}{2}\psi(x \otimes y + y \otimes x)$ et $u(x) = \frac{1}{2}\psi(x \otimes x)$. On définit alors les générateurs de l'énoncé comme :

$$\xi_i = u(e_i), \quad u_{p,q} = u(e_p, e_q).$$

Le choix de K n'intervenant pas dans l'énoncé, on peut toujours supposer qu'aucun des z_i n'est dans K. Pour tout $1 \leqslant i \leqslant r$, on écrit $z_i = x_i + jy_i$ avec $x_i, y_i \in K$, et on peut donc supposer $y_i \neq 0$. Si on pose $f_i = e_i z_i$, alors $(e_i, f_i)_i$ est une K-base de V, orthogonale pour b. En effet, la seule chose à vérifier est que $b(e_i, f_i) = 0$, mais $h(e_i, f_i) = h(e_i, e_i) z_i = z_i^2 \in k$. Notons que $b(e_i, e_i) = y_i$, et $b(f_i, f_i) = -z_i^2 y_i$.

On a

$$\xi_i = -\frac{1}{y_i} e_i f_i$$

et

$$u_{p,q} = \frac{1}{y_p y_q}\left((x_q y_p - x_p y_q) e_p e_q - y_p e_p f_q - y_q e_q f_p\right).$$

En effet, on a

$$\begin{aligned} e_i j &= e_i \left[(x_i + j y_i) \frac{1}{y_i} - \frac{x_i}{y_i} \right] \\ &= (-e_i x_i + f_i) \frac{1}{y_i} \end{aligned}$$

ce qu'on peut injecter dans $\xi_i = \frac{1}{2}((e_i j)e_i - e_i(e_i j))$ et $u_{p,q} = \frac{1}{2}((e_p j)e_q - e_p(e_q)j + (e_q j)e_p - e_q(e_p j))$ en tenant compte des relations d'anticommutation dans $Cl(V, b)$.

Toutes les relations résultent alors de calculs explicites dans $Cl(V, b)$ en utilisant la base des e_i et f_i. Notamment, on voit immédiatement par les relations d'orthogonalité que les ξ_i commutent, que $u_{p,q}$ commute avec ξ_i si $i \notin \{p, q\}$, qu'ils anti-commutent si $i \in \{p, q\}$, et que $u_{i,j}$ et $u_{p,q}$ commutent quand $\{i, j\} \cap \{p, q\} = \emptyset$. L'action de l'involution canonique est aussi facile à établir puisque par définition $\tau(x \cdot y) = y \cdot x = -x \cdot y$ si x et y sont orthogonaux.

On a aussi facilement $\xi_i^2 = -\frac{1}{y_i^2} e_i^2 f_i^2 = z_i^2$, et

$$\begin{aligned} u_{p,q}^2 &= \frac{1}{y_p^2 y_q^2} \left(-(x_q y_p - x_p y_q)^2 e_p^2 e_q^2 - y_p^2 e_p^2 f_q^2 - y_q^2 e_q^2 f_p^2 - 2 y_p y_q e_p f_p e_q f_q \right) \\ &= -\frac{1}{y_p y_q} (x_q y_p - x_p y_q)^2 + \frac{1}{y_q} z_q^2 + \frac{1}{y_p} z_p^2 - 2 \frac{1}{y_p y_q} e_p f_p e_q f_q \\ &= (2 x_p x_q + \pi y_p \overline{y_q} + \pi y_q \overline{y_p}) - 2 \xi_p \xi_q \\ &= \mathrm{Trd}_Q(z_p z_q) - 2 \xi_p \xi_q. \end{aligned}$$

La dernière relation est la plus difficile à établir. Écrivons $z_i = \lambda_0 + \lambda_p z_p + \lambda_q z_q + \lambda_{p,q} z_p z_q$. Alors

$$x_i = \lambda_0 + \lambda_p x_p + \lambda_{p,q} x_p x_q + \lambda_{p,q} \pi \overline{y_p} y_q \tag{3.2.33}$$

$$y_i = \lambda_p y_p + \lambda_q y_q + \lambda_{p,q} y_p x_q - \lambda_{p,q} x_p y_q. \tag{3.2.34}$$

Notons que comme z_i est un quaternion pur, $x_i = -\overline{x_i}$ ce qui se traduit par l'équation

$$2\lambda_0 + \lambda_{p,q}(2 x_p x_q + \pi \overline{y_p} y_q + \pi y_p \overline{y_q}) = 0. \tag{3.2.35}$$

On doit comparer d'une part

$$\frac{1}{y_i^2 y_p y_q} \left((x_p y_i - x_i y_p) e_i e_p - y_i e_i f_p - y_p e_p f_i \right) \left((x_q y_i - x_i y_q) e_i e_q - y_i e_i f_q - y_q e_q f_i \right)$$

et d'autre part

$$\begin{aligned} &\frac{1}{y_p y_q} \left(\lambda_0 + \frac{1}{y_i} e_i f_i - \frac{\lambda_p}{y_p} e_p f_p + \frac{\lambda_q}{y_q} e_q f_q - \frac{\lambda_{p,q}}{y_p y_q} e_p f_p e_q f_q \right) \\ &\times \left((x_q y_p - x_p y_q) e_p e_q - y_p e_p f_q - y_q e_q f_p \right). \end{aligned}$$

On peut alors développer et identifier les composantes correspondantes. On trouve des termes non nuls pour les composantes selon e_pe_q, e_pf_q, e_qf_p, f_pf_q, $e_if_ie_pe_q$, $e_if_ie_pf_q$, et $e_if_ie_qf_p$. Les coefficients selon ces trois dernières composantes sont immédiatement égaux après calcul, et ne font pas intervenir les la décomposition de z_i (ils valent respectivement $\frac{x_q}{y_iy_q} - \frac{x_p}{y_iy_p}$, $-\frac{1}{y_iy_q}$ et $-\frac{1}{y_iy_p}$). Les quatre autres coefficients demandent plus de minutie, on est amené à montrer les égalités suivantes :

$$\begin{aligned}
&\lambda_0(x_qy_p - x_py_q) + \lambda_py_qz_p^2 + \lambda_qy_pz_q^2 = -x_px_qy_i + (x_py_q + x_qy_p)x_i + \pi y_py_q\overline{y_i};\\
&\lambda_0y_p + \lambda_q(x_qy_p - x_py_q) + \lambda_{p,q}y_qz_p^2 = x_iy_p - y_ix_p;\\
&\lambda_0y_q + \lambda_p(x_qy_p - x_py_q) + \lambda_{p,q}y_pz_q^2 = y_ix_q - x_iy_q;\\
&\quad\lambda_py_p + \lambda_qy_q + \lambda_{p,q}(x_qy_p - x_py_q) = y_i.
\end{aligned}$$

Pour la deuxième et la quatrième il suffit de remplacer les occurrences de x_i et y_i par les formules (3.2.33), et pour les deux autres il faut en plus utiliser la relation (3.2.35). $\square$

Remarque 3.2.36. Bien que le théorème donne une description complète de la structure de l'algèbre, il ne donne pas directement de formule pour un cocycle associé à la structure de produit croisé associée à L. En effet, on dispose de générateurs canoniques correspondant aux éléments $\tau_{i,j}$ du groupe de Galois, mais il n'y a pas vraiment de choix qui s'impose naturellement pour les autres éléments du groupe. On pourrait par exemple décomposer un $g \in G$ en produit de $\tau_{i,j}$ de support disjoint, en faisant un choix de normalisation (par exemple décomposer en $\tau_{i_1,j_1} \cdots \tau_{i_s,j_s}$ avec $i_1 < j_1 < i_2 < \cdots < j_s$), et décréter que $u_g = u_{i_1,j_1} \cdots u_{i_s,j_s}$. Cela a l'avantage de ne fait intervenir que des générateurs qui commutent entre eux, mais le calcul des produits entre différents u_g devient très pénible car faisant intervenir de façon très lourde la combinatoire de l'ordre sur les coefficients. D'un autre côté, on peut aussi par exemple décomposer g en $\tau_{i_1,r} \cdots \tau_{i_s,r}$ en utilisant l'indice r comme pivot et définir $u_g = u_{i_1,r} \cdots u_{i_s,r}$. On a alors plus de régularité dans le schéma, mais les générateurs en question ne commutent pas, et les calculs restent donc pénibles. Dans tous les cas, bien qu'on puisse en théorie décrire de façon élémentaire un cocycle correspondant à B, la tâche est en réalité assez pénible dès que r n'est pas très petit.

3.2.3 Algèbre discriminante en degré 4

On veut maintenant décrire l'autre sens de l'équivalence entre algèbres de type A_3 et D_3, c'est-à-dire calculer explicitement l'algèbre discriminante d'une algèbre à involution unitaire de degré 4.

Soit donc (B, τ) une telle algèbre sur k, de centre $K = k(\xi)$, avec $\xi^2 = \delta \in k^*$. On suppose qu'on dispose de $L \subset B$ k-algèbre G-galoisienne avec $G = (\mathbb{Z}/2\mathbb{Z})^3$ telle que $\tau(L) = L$, avec $\tau_{|L} \in G$. Comme on sait que (B, τ) est l'algèbre de Clifford d'une certaine algèbre d'indice 2 (précisément son algèbre discriminante), la partie précédente montre qu'une telle sous-algèbre existe toujours.

On pose alors $H \subset G$ tel que $K = L^H$, et on écrit $H = \langle s, t\rangle$. On a $L = K(\xi_1, \xi_2)$ avec $\xi_i^2 = \delta_i \in K^*$ tels que $s(\xi_1) = -\xi_1$, $s(\xi_2) = \xi_2$, $t(\xi_1)\xi_1$ et $t(\xi_2) = -\xi_2$. On choisit u_s, u_t et u_{st} dans B^* qui définissent une structure de produit croisé. En utilisant les formules de la proposition 3.2.16 et la théorème de Hilbert 90, on voit que quitte à changer les u_g on peut supposer $\tau(u_g) = u_g$ pour tout $g \in H$ (quand on fait le calcul en sens inverse on tombe plutôt sur des générateurs vérifiant $\tau(u_g) = -u_g$ mais cela nous permet d'éviter d'avoir à gérer des signes, et il suffit de remplacer u_g par ξu_g pour retrouver l'autre situation).

On pose un certain nombre de notations : pour tout $g \in H$, $a_g = \alpha(g, g) = u_g^2 \in L^*$, $v = \alpha(s, t)$. On peut remarquer que $a_g \in (L^*)^{\langle g,\tau\rangle}$, et on pose $n(a_g) = N_{L^{\langle g,\tau\rangle}/k}(a_g)$ et $tr(a_g) = \mathrm{Tr}_{L^{\langle g,\tau\rangle}/k}(a_g)$ (donc par exemple $n(a_s) = a_s t(a_s)$ et $tr(a_s) = a_s + t(a_s)$). On définit également $N = N_{L/K}(v)$, dont on vérifie sans peine que c'est un élément de k^*. La structure de produit croisé de (B, τ) est entièrement caractérisée par a_s, a_t et v. Pour des raisons techniques, on supposera que les a_g ne sont pas dans k^*, ce qui est toujours possible quitte à changer les u_g. On arrive alors à l'énoncé suivant :

Théorème 3.2.37. *Soit $(A, \sigma) = D(B, \tau)$. Alors $A \simeq M_3(Q)$ où $Q = (\delta\delta_1, n(a_s))$. On note $k' = L^{\langle\tau,t\rangle} = k(\xi\xi_1) \subset Q$, et $j \in Q$ tel que $j^2 = n(a_s)$ et $Q = k' \oplus jk'$. Alors $\sigma \simeq \sigma_h$ où $h = \langle z_1, z_2, z_3\rangle$ avec :*

$$\begin{aligned}
z_1 &= \frac{\delta tr(a_{st})\xi\xi_1}{Nn(a_{st})} + j\frac{2\delta t(v)\xi\xi_1}{Na_s a_{st}\tau(v)}, \\
z_2 &= \delta_2 Nn(a_{st})\xi\xi_1, \\
z_3 &= \frac{-tr(a_s)\xi\xi_1}{n(a_s)} + j\frac{-2\xi\xi_1}{n(a_s)}.
\end{aligned}$$

On va passer le reste de cette partie à montrer ce résultat, et on va procéder par descente. Le plan de la preuve est donc de caractériser $D(B, \tau)$ par un 1-cocyle $G \longrightarrow PGL_6(L)$, noté $g \mapsto [Q_g]$ (où $[Q_g]$ est la classe de $Q_g \in GL_6(L)$), de sorte que $D(B, \tau) \subset M_6(L)$ soit caractérisé comme les points fixes de l'action semi-linéaire de G donnée par $g * A = Q_g g(A) Q_g^{-1}$. Pour ça on commence par décrire B à partir d'un cocycle $H \to PGL_4(L)$, puis on en déduit un cocycle $H \longrightarrow PGL_6(L)$ définissant $\Lambda^2 B$, et on étend ce cocycle à G en donnant l'action de τ, comme décrit dans [17, §10.E]. Il s'agira ensuite de donner un autre 1-cocycle $G \to PGL_6(L)$ (disons $g \mapsto [R_g]$) décrivant $M_3(Q)$, et de montrer que ces deux cocycles sont cohomologues, ce qui établit l'isomorphisme de l'énoncé. Cela revient à trouver $Y \in GL_6(L)$ telle que $[Y^{-1} Q_g g(Y)] = [R_g]$.

En ce qui concerne l'involution σ, il s'agit d'une descente de l'involution adjointe de la forme canonique sur $L^6 \simeq \Lambda^2(L^4)$, et on peut utiliser la matrice explicite Y, ainsi qu'une équivalence de Morita, pour trouver une matrice de la forme hermitienne h à partir d'une matrice pour la forme canonique.

Cocycle définissant B

Soit E un L-module libre de dimension 4, de base (e_i), qu'on utilisera pour identifier $\mathrm{End}_L(E) = M_4(L)$. On définit alors un K-plongement $\varphi : B \to \mathrm{End}_L(E)$ par :

$$\forall \lambda \in L, \varphi(\lambda) = \widetilde{\lambda} = \begin{pmatrix} \lambda & & & \\ & s(\lambda) & & \\ & & t(\lambda) & \\ & & & st(\lambda) \end{pmatrix},$$

$$\varphi(u_s) = \begin{pmatrix} 0 & 1 & & \\ a_s & 0 & & \\ & & 0 & u \\ & & \frac{t(a_s)}{u} & 0 \end{pmatrix},$$

$$\varphi(u_t) = \begin{pmatrix} & & 1 & 0 \\ & & 0 & 1 \\ a_t & 0 & & \\ 0 & s(a_t) & & \end{pmatrix}$$

où on note $u = \frac{v}{st\tau(v)}$, qui vérifie $u_t u_s = u \cdot u_s u_t$, et $N_{L/K}(u) = 1$.

On vérifie qu'on a bien les relations attendues pour que φ définisse un plongement. On en déduit un isomorphisme $\Phi : B_L \xrightarrow{\sim} \mathrm{End}_L(E)$ defini par $\Phi(x \otimes \lambda) = \lambda\varphi(x)$.

On pose alors

$$P_s = \begin{pmatrix} 0 & 1 & & \\ a_s & 0 & & \\ & & 0 & 1 \\ & & a_s & 0 \end{pmatrix}, P_t = \begin{pmatrix} & & 1 & 0 \\ & & 0 & t(u) \\ a_t & 0 & & \\ 0 & \frac{a_t}{u} & & \end{pmatrix}.$$

On vérifie que si on définit $g * A = P_g g(A) P_g^{-1}$ pour $g = s, t$, alors on obtient l'action semi-linéaire de H sur $\mathrm{End}_L(E)$ venant de Φ (bien évidemment P_g est défini à un scalaire de L^* près).

Cela se vérifie par le fait que $g * \varphi(u_h) = \varphi(u_h)$ et $g * \widetilde{\lambda} = \widetilde{g(\lambda)}$ pour $g, h \in \{s, t\}$ et $\lambda \in L$ (bien sûr il suffit de définir l'action de s et t).

Cocycle définissant $\lambda^2 B$

L'isomorphisme Φ induit un isomorphisme $\lambda^2\Phi : \lambda^2 B_L \xrightarrow{\sim} \mathrm{End}_L(\Lambda^2 E)$, qu'on va utiliser pour caractériser $\lambda^2 B$ par descente. On munit $\Lambda^2 E$ de la base naturelle $(e_{12}, e_{34}, e_{13}, e_{24}, e_{14}, e_{23})$ où on écrit $e_{ij} = e_i \wedge e_j$ (l'ordre est choisi pour faciliter les calculs par la suite), et on identifiera alors $\mathrm{End}_L(\Lambda^2 E) = M_6(L)$.

Pour tout $f \in \mathrm{End}_L(E)$, on a par fonctorialité un élément $\Lambda^2(f) \in \mathrm{End}_L(\Lambda^2 E)$ défini par $(\Lambda^2 f)(x \wedge y) = f(x) \wedge f(y)$. On montre alors que l'action semi-linéaire de H sur $\mathrm{End}_L(\Lambda^2 E)$ est donnée par $g * A = Q_g g(A) Q_g^{-1}$ où $Q_g = \Lambda^2 P_g$, soit :

$$Q_s = \begin{pmatrix} -a_s & 0 & & & & \\ 0 & -a_s & & & & \\ & & 0 & 1 & & \\ & & a_s^2 & 0 & & \\ & & & & 0 & a_s \\ & & & & a_s & 0 \end{pmatrix},$$

$$Q_t = \begin{pmatrix} 0 & \frac{a_t}{s(a_t)} & & & & \\ a_t^2 & 0 & & & & \\ & & -a_t u & 0 & & \\ & & 0 & -a_t t(u) & & \\ & & & & 0 & -a_t \\ & & & & \frac{-a_t^2}{s(a_t)} & 0 \end{pmatrix}.$$

Il s'agit de montrer que l'image de $\Lambda^2(\Phi)$ est fixée par cette action. Or si f est dans l'image de Φ alors $\Lambda^2(f)$ est dans l'image de $\Lambda^2(\Phi)$. En effet, si on écrit $\lambda^2 B = \mathrm{End}_{B^{\otimes 2}}(B^{\otimes 2}(1-g))$ avec g l'élément de Goldman, alors pour tout $b \in B$ on peut définir $\lambda^2 b \in \lambda^2 B$ par la multiplication à droite par $b \otimes b$ dans $B^{\otimes 2}(1-g)$ (on a bien $(b \otimes b)(1-g) = (1-g)(b \otimes b)$ donc cette opération est bien définie), et cela correspond dans le cas déployé à la construction $\Lambda^2(f)$, donc par fonctorialité $(\lambda^2 \Phi)(\lambda^2 x) = \Lambda^2(\Phi(x))$. De là, si A est dans l'image de Φ, on a

$$(\Lambda^2 P_g) \cdot g(\Lambda^2 A) \cdot (\Lambda^2 P_g)^{-1} = \Lambda^2(P_g g(A) P_g^{-1}) = \Lambda^2 A$$

et donc l'image de $\Lambda^2(\Phi)$ est bien fixée par cette action.

Cocycle définissant $D(B, \tau)$

Pour définir $A = D(B, \tau)$, il faut encore définir l'action de $\tau \in G$ sur $\mathrm{End}_L(\Lambda^2 E)$. On va montrer qu'elle est donnée par $\tau * A = Q_\tau \tau(A) Q_\tau^{-1}$ avec

$$Q_\tau = \begin{pmatrix} 0 & a_s & & & & \\ a_s n(a_t) & 0 & & & & \\ & & 0 & -a_t & & \\ & & -a_s^2 s(a_t) & 0 & & \\ & & & & 0 & a_s s(a_t) \\ & & & & a_s a_t & 0 \end{pmatrix}.$$

D'après [17, def 10.28], $D(B, \tau)$ est constitué des éléments fixes par l'action de τ sur $\lambda^2 B$, qui agit par $\tau^{\wedge 2} \circ \gamma$ où γ est l'involution canonique, donc l'action de τ

sur $\mathrm{End}_L(\Lambda^2 E)$ est donnée par la composition de $(\lambda^2\Phi)_*(\tau_L^{\wedge 2})$ et $(\lambda^2\Phi)_*(\gamma_L)$ (qui commutent).

Par fonctorialité, $(\lambda^2\Phi)_*(\gamma_L)$ est l'adjointe de la forme canonique

$$\begin{array}{rcl} \Lambda^2 E \times \Lambda^2 E & \longrightarrow & \Lambda^4 E = L \cdot e_{1234} \simeq L \\ (x,y) & \longmapsto & x \wedge y \end{array}$$

qui a pour matrice dans la base choisie de $\Lambda^2 E$:

$$B = \begin{pmatrix} 0 & 1 & & & & \\ 1 & 0 & & & & \\ & & 0 & -1 & & \\ & & -1 & 0 & & \\ & & & & 0 & 1 \\ & & & & 1 & 0 \end{pmatrix}.$$

Quant à $(\lambda^2\Phi)_*(\tau_L^{\wedge 2})$, elle est l'adjointe de la forme hermitienne $h^{\wedge 2}$ où h est une forme hermitienne sur E telle que $\sigma_h = \Phi_*(\tau_L)$. On montre que h a pour matrice dans la base (e_i)

$$M = \begin{pmatrix} a_s a_t & & & \\ & a_t & & \\ & & a_s & \\ & & & \frac{a_t}{s(a_t)} \end{pmatrix}.$$

En effet, on a

$$\sigma_h(A) = M^{-1}\tau({}^tA)M$$

avec $\sigma_h(\widetilde{\lambda}) = \widetilde{\tau(\lambda)}$, donc M commute avec les matrices $\widetilde{\lambda}$. En prenant λ fixe par aucun élément de H, on obtient que M doit être diagonale. De plus, on doit avoir $\sigma_h(\varphi(u_g)) = \varphi(u_g)$ pour $g = s, t$, ce qu'on vérifie par calcul. On a alors comme matrice pour $h^{\wedge 2}$:

$$M' = \Lambda^2 M = \begin{pmatrix} n(a_t) & & & & & \\ & 1 & & & & \\ & & a_s s(a_t) & & & \\ & & & \frac{a_t}{a_s} & & \\ & & & & a_t & \\ & & & & & s(a_t) \end{pmatrix}.$$

On trouve donc $\tau * A = B^{-1t}((M')^{-1}\tau({}^tA)M')B$, et donc $Q_\tau = B^{-1t}M'$, ce qui après calcul donne la matrice annoncée.

Cocycle définissant $M_3(Q)$

On pose donc Q algèbre de quaternions sur k, donnée par la sous-algèbre quadratique $k' = k(\xi\xi_1)$ et le quaternion pur j tel que $j^2 = n(a_s)$ (et j anti-commute avec $\xi\xi_1$). On a $k' = L^D$ avec $D = \langle t, s\tau\rangle \subset G$.

On choisit alors le plongement

$$\begin{array}{rcl} Q & \longrightarrow & M_2(k') \\ x + jy & \longmapsto & \begin{pmatrix} x & n(a_s)s(y) \\ y & s(x) \end{pmatrix} \end{array}$$

où $x, y \in k'$, qui induit un plongement $M_3(Q) \longrightarrow M_6(L)$. On vérifie que le 1-cocycle associé à ce plongement est $g \mapsto [R_g]$ où $R_g = I_6$ si $g \in D$, et $R_g = S$ sinon, où

$$S = \begin{pmatrix} 0 & n(a_s) & & & & \\ 1 & 0 & & & & \\ & & 0 & n(a_s) & & \\ & & 1 & 0 & & \\ & & & & 0 & n(a_s) \\ & & & & 1 & 0 \end{pmatrix}.$$

Cocycles cohomologues

On cherche donc $Y \in GL_6(L)$ telle que $[Y^{-1}Q_g g(Y)] = [R_g]$ dans $PGL_6(L)$, soit

$$Y^{-1}Q_g g(Y) = c_g R_g$$

avec $c_g \in L^*$, et il suffit de le vérifier pour $g = s, t, \tau$.

On vérifie que

$$Y = \begin{pmatrix} Y_1 & & \\ & Y_2 & \\ & & Y_3 \end{pmatrix}$$

convient, où

$$Y_1 = \xi \begin{pmatrix} \frac{1}{s(v)} & \frac{-a_s}{st\tau(v)} \\ \frac{a_t}{\tau(v)} & \frac{-a_s a_t}{t(v)} \end{pmatrix}, Y_2 = \xi_2 \begin{pmatrix} a_s n(a_t)u & 0 \\ 0 & a_s^3 n(a_t)us(u) \end{pmatrix},$$

$$Y_3 = \begin{pmatrix} a_t st(u) & a_s s(a_t)u \\ a_t & a_s s(a_t)ut(u) \end{pmatrix}$$

avec $c_s = \frac{1}{u}$, $c_t = \frac{a_t}{st(u)}$ et $c_\tau = s(a_t)t(u)$.

La preuve est purement calculatoire, on ne reproduira pas le calcul ici par souci de lisibilité. On indique les relations à utiliser entre les différents éléments qui interviennent dans la formule : $\frac{t(a)}{a} = us(u)$, $\frac{b}{s(b)} = ut(u)$, et $N_{L/K}(u) = 1$.

L'existence de Y montre par le mécanisme usuel de la cohomologie que $D(B,\tau) \simeq M_3(Q)$. Mais on a quelque chose de plus concret que cela : si on note $g *_1 A = Q_g g(a) Q_g^{-1}$ la première action considérée, et $g *_2 A = R_q g(a) R_g^{-1}$ la deuxième, alors en posant $\psi(A) = Y^{-1}AY$, qui est un automorphisme de $\mathrm{End}_L(\Lambda^2 E)$, on a précisément $g *_2 (\psi(A)) = \psi(g *_1 A)$. Or $D(B,\tau)$ est constituée des points fixes de l'action $*_1$, et $M_3(Q)$ des points fixes de $*_2$, donc on obtient l'isomorphisme concret suivant : au sein de $\mathrm{End}_L(\Lambda^2 E)$, ψ envoie $D(B,\tau)$ sur $M_3(Q)$.

Descente de la forme quadratique

On a déjà décrit la forme quadratique canonique sur $\mathrm{End}_L(\Lambda^2 E)$, de matrice B. Elle induit une certaine involution sur $\mathrm{End}_L(\Lambda^2 E)$, qui se restreint à $D(B,\tau)$ en son involution canonique. Pour obtenir l'involution correspondante sur $M_3(Q)$, on utilise donc le changement de base donné par Y : l'involution sur $\mathrm{End}_L(\Lambda^2 E)$ correspondant à la forme quadratique de matrice $B' = {}^tYBY$ se restreint en l'involution cherchée sur $M_3(Q)$.

On est donc dans la situation du triangle commutatif suivant dans $\mathbf{Br}_h(K)L$:

$$\begin{tikzcd}
 & (Q_L, {}^-) \simeq (M_2(L), {}^-) \arrow[dr, "\mathcal{H}_{-1}"] & \\
(M_3(Q_L), \sigma_L) \simeq M_6(L) \arrow[ur, "h_L"] \arrow[rr, "b'"] & & (L, \mathrm{Id})
\end{tikzcd}$$

où b' est de matrice B' et $\mathcal{H}_{-1}$ est le plan (hyperbolique) alterné. Par équivalence de Morita on en déduit alors que l'involution σ_L sur $M_6(L) = M_3(M_2(L))$ est adjointe à la forme anti-hermitienne sur $(M_2(L), {}^-)$ de matrice CB', où

$$C = \begin{pmatrix} 0 & -1 & & & & \\ 1 & 0 & & & & \\ & & 0 & -1 & & \\ & & 1 & 0 & & \\ & & & & 0 & -1 \\ & & & & 1 & 0 \end{pmatrix}.$$

Comme une telle matrice n'est définie qu'à un scalaire près, on doit avoir $\lambda \in L^*$ tel que $\lambda CB'$ soit de la forme

$$\begin{pmatrix} x_1 & n(a)s(y_1) & & & & \\ y_1 & s(x_1) & & & & \\ & & x_2 & n(a)s(y_2) & & \\ & & y_2 & s(x_2) & & \\ & & & & x_3 & n(a)s(y_3) \\ & & & & y_3 & s(x_3) \end{pmatrix}$$

avec $x_i, y_i \in k'$, et alors en posant $z_i = x_i + jy_i \in Q$, $\langle z_1, z_2, z_3\rangle$ est une diagonalisation de la forme anti-hermitienne cherchée.

Concrètement, si on choisit $\lambda = \frac{\xi\xi_1}{a_s^2 n(a_t)u}$, on obtient par le calcul les z_i donnés dans l'énoncé du théorème 3.2.37, ce qui achève sa démonstration.

3.3 Quelques invariants en petit degré

On donne ici quelques exemples d'invariants d'algèbres à involution, en utilisant les résultats des parties 3.1 et 3.2.

3.3.1 Invariants a_3 et a_4 en degré 6

Dans cette partie on se donne une algèbre (A,σ) de type D_3 sur k : on a donc A de degré 6 et d'indice au plus 2, et σ est orthogonale. En particulier, on peut appliquer les résultats de la partie 3.1.3 pour construire des invariants cohomologiques : d'après la discussion suivant la proposition 3.1.6, tout invariant $\alpha \in \mathrm{Inv}^d(I,\mu_2)$ définit un invariant $\widetilde{\alpha}(A,\sigma)$ à valeur dans $M_Q^{d-1}(K)$, et si cet invariant est nul on peut définir $\alpha(A,\sigma) \in M_Q^d(K)$. On va montrer que certains de ces invariants se relèvent en des invariants cohomologiques (à valeur dans $H^d(K,\mu_2)$ et non dans $M_Q^d(K)$).

Dans [28, §7], les auteurs considèrent la forme trace d'involution T_τ d'une algèbre (B,τ) de type A_3 telle que $Z(B) = k(\sqrt{-1})$, donc qui correspond à une algèbre (A,σ) de type D_3 dont le discriminant est -1. Ils prouvent que sous cette condition $T_\tau = n_Q + q_4$ où q_4 est une 4-forme de Pfister (donc cette écriture est unique), et posent $a_4(A,\sigma) = e_4(q_4) \in H^4(k,\mu_2)$ (on utilise des notations légèrement différentes). On se propose d'élargir un peu cette construction, en faisant le lien avec nos méthodes.

Précisément, on va établir un lien avec l'invariant $v_4^{(1)} \in \mathrm{Inv}^4(I,\mu_2)$ (voir 1.2.34). Il vérifie $\widetilde{v_4^{(1)}} = v_3^{(1)}$ (voir 1.2.65), donc on peut définir $v_3^{(1)}(A,\sigma) \in M_Q^3(k)$, et lorsque cette classe est nulle on peut définir $v_4^{(1)}(A,\sigma) \in M_Q^4(k)$. En particulier, comme $v_3^{(1)} = (-\delta)\cup u_2^{(1)}$, $v_3^{(1)}$ est toujours nul en discriminant -1, et donc on peut toujours définir $v_4^{(1)}(A,\sigma)$ dans la situation étudiée dans [28]. On va montrer que $a_4(A,\sigma)$ est un relevé de $v_4^{(1)}(A,\sigma)$, y compris dans une situation plus générale où on ne fait pas d'hypothèse sur le discriminant.

Forme trace d'involution

Soit $(B,\tau) = Cl(A,\sigma)$. On rappelle que T_τ est la restriction de la forme trace de B au sous-k-espace des éléments symétriques, et on rappelle également que si d est pair, $\lambda^d(\sigma) \in GW(k)$ est bien définie (par exemple comme étant $\lambda^d(\langle 1\rangle_\sigma) \in GW(k) \subset \widetilde{GW}(A,\sigma)$).

Proposition 3.3.1. *On a l'égalité suivante dans $GW(k)$: $T_\tau = 1 + \lambda^4(\sigma)$.*

On aura besoin au cours de la preuve du lemme suivant :

Lemme 3.3.2. *Soit $z \in Q$. Alors*

$$\operatorname{Trd}_Q(z)^2 - 4\operatorname{Nrd}_Q(z) = 4z_0^2$$

où z_0 est la partie pure de z.

Démonstration. On a $z = x + z_0$ où $2x = \operatorname{Trd}_Q(z)$, et

$$\begin{aligned} N_Q(z) &= (x+z_0)(x-z_0) \\ &= x^2 - z_0^2 \end{aligned}$$

donc $4x^2 - 4N_Q(z) = 4z_0^2$. □

Démonstration. On écrit $\sigma \simeq \sigma_h$ où $h = \langle z_1, z_2, z_3\rangle$ avec $z_i \in Q$ quaternion pur, et Q est l'algèbre de quaternions Brauer-équivalente à A. On supposera que les z_i ne commutent pas deux à deux. On utilise alors les notations du théorème 3.2.28 pour décrire (B, τ). On note $H = \{1, g_1, g_2, g_3\}$ où $g_i(\xi_i) = \xi_i$, donc $g_i = \tau_{p,q}$ où $i \neq p, q$, et $u_i = u_{g_i} = u_{p,q}$.

Soit V l'ensemble des éléments symétriques de (B, τ) ; c'est un k-espace vectoriel de dimension 16. Pour tout $\lambda \in L$, et tout $g \in H$, on a $\tau(u_g) = \varepsilon_g u_g$ avec $\varepsilon_1 = 1$ et $\varepsilon_g = -1$ si $g \neq 1$, donc $\tau(\lambda u_g) = \tau(u_g)\tau(\lambda) = \varepsilon_g (g\tau)(\lambda) u_g$. De là, $\lambda u_g \in V$ si et seulement si $(g\tau)(\lambda) = \varepsilon_g \lambda$. On note L_g l'ensemble des $\lambda \in L$ vérifiant cette condition, et $V_g = L_g u_g \subset V$. Comme $\dim_k(L_g) = 4$, on a $\bigoplus_{g\in H} V_g$ de dimension 16 sur k, donc $V = \bigoplus_{g\in H} V_g$. De plus, cette décomposition est orthogonale pour T_τ puisque les Lu_g sont orthogonaux pour la forme trace (en effet, $\operatorname{Trd}_B(\lambda u_g) = 0$ si $g \neq 1$). On a donc $T_\tau = \sum_g b_g$ où

$$\begin{array}{rccl} b_g : & L_g \times L_g & \longrightarrow & k \\ & (x, y) & \longmapsto & \operatorname{Tr}_{L/K}(x g(y) u_g^2). \end{array}$$

Le k-espace L_1 a pour base $(1, \xi_1\xi_2, \xi_1\xi_3, \xi_2\xi_3)$, qui est une base orthogonale, donc b_1 (qui est isométrique à la forme trace de l'extension L^τ/k) est isométrique à $\langle 1, z_1^2 z_2^2, z_1^2 z_3^2, z_2^2 z_3^2\rangle$. Si on note $\{i, p, q\} = \{1, 2, 3\}$, on a comme k-base de L_{g_i} : $(\xi, \xi_i, \xi_i\xi_p, \xi_i\xi_q)$. Sachant que $u_i^2 = \operatorname{Trd}_Q(z_p z_q) - 2\xi_p\xi_q$, on trouve comme matrice pour b_{g_i} dans cette base :

$$\begin{pmatrix} \delta\operatorname{Trd}_Q(z_p z_q) & -2\delta & & \\ -2\delta & z_i^2\operatorname{Trd}_Q(z_p z_q) & & \\ & & -z_i^2 z_p^2 \operatorname{Trd}_Q(z_p z_q) & 2\delta \\ & & 2\delta & -z_i^2 z_q^2 \operatorname{Trd}_Q(z_p z_q) \end{pmatrix}.$$

Les deux blocs diagonaux ont le même déterminant

$$\Delta = \delta z_i^2(\mathrm{Trd}_Q(z_pz_q)^2 - 4z_p^2z_q^2),$$

qui d'après le lemme 3.3.2 vaut

$$\Delta = 4\delta z_i^2(z_pz_q)_0^2 \equiv z_p^2z_q^2(z_pz_q)_0^2 \bmod (k^*)^2.$$

On en déduit :

$$\begin{aligned}
b_{g_i} &= \langle \delta\,\mathrm{Trd}_Q(z_pz_q)\rangle\langle 1, z_p^2z_q^2(z_pz_q)_0^2\rangle + \langle -z_i^2z_p^2\,\mathrm{Trd}_Q(z_pz_q)\rangle\langle 1, z_p^2z_q^2(z_pz_q)_0^2\rangle \\
&= \langle \delta\,\mathrm{Trd}_Q(z_pz_q)\rangle\langle 1, -z_q^2\rangle\langle 1, z_p^2z_q^2(z_pz_q)_0^2\rangle \\
&= \langle \delta\,\mathrm{Trd}_Q(z_pz_q)\rangle\langle\langle z_q^2, -z_p^2z_q^2(z_pz_q)_0^2\rangle\rangle.
\end{aligned}$$

Or

$$\begin{aligned}
(z_q^2, -z_p^2z_q^2(z_pz_q)_0^2) &= (z_q^2, z_p^2) + (z_q^2, (z_pz_q)_0^2) \\
&= (z_p^2, z_q^2) + [Q]
\end{aligned}$$

(on rappelle que z_q et $(z_pz_q)_0$ anti-commutent). De là, $\langle\langle z_q^2, -z_p^2z_q^2(z_pz_q)_0^2\rangle\rangle = \varphi_{z_p,z_q}$ (d'après la proposition 2.2.24) et finalement $b_{g_i} = \langle -\delta\rangle\langle z_p\rangle\langle z_q\rangle$ (d'après la proposition 2.2.26). Donc en combinant les calculs de b_1 et des b_{g_i} :

$$T_\tau = \langle 1, z_1^2z_2^3, z_1^2z_3^2, z_2^2z_3^2\rangle + \sum_{p<q}\langle -\delta\rangle\langle z_p\rangle\langle z_q\rangle. \tag{3.3.3}$$

D'autre part,

$$\begin{aligned}
1 + \lambda^4(h) &= 1 + \sum_{p<q}\lambda^2(\langle z_p\rangle)\lambda^2(\langle z_q\rangle) + \sum_{p<q}\lambda^2(\langle z_i\rangle)\langle z_p\rangle\langle z_q\rangle \\
&= \langle 1, z_1^2z_2^3, z_1^2z_3^2, z_2^2z_3^2\rangle + \sum_{p<q}\langle -z_i^2\rangle\langle z_p\rangle\langle z_q\rangle
\end{aligned}$$

et on conclut par le fait que $z_p^2z_q^2$ est représenté par φ_{z_p,z_q} (en effet, $-z_p^2$ et $-z_q^2$ sont tous les deux représentés) donc $\langle -\delta\rangle\langle z_p\rangle\langle z_q\rangle = \langle -z_i^2\rangle\langle z_p\rangle\langle z_q\rangle$. □

Invariants a_3 et a_4

En utilisant la formule (3.3.3), on voit que

$$\begin{aligned}
e_2(T_\tau) &= (-z_1^2z_2^2, -z_1^2z_3^2) + \sum_{i<j}[Q] + (z_i^2, z_j^2) \\
&= (-1, -\delta) + \sum_{i<j}(z_i^2, z_j^2) + [Q] + \sum_{i<j}(z_i^2, z_j^2) \\
&= (-1, -\delta) + [Q]
\end{aligned}$$

donc on peut poser

$$q_\tau = T_\tau - \langle\langle -1, -\delta\rangle\rangle - n_Q \in I^3(k).$$

On définit alors $a_3(A,\sigma) = e_3(q_\tau)$ et si $a_3(A,\sigma) = 0$ on pose $a_4(A,\sigma) = e_4(q_\tau)$ (ce qui coïncide bien avec la définition précédente lorsque $\delta = -1$).

Proposition 3.3.4. *La classe de $a_3(A,\sigma)$ dans $M_Q^3(k)$ est $v_3^{(1)}(A,\sigma)$, et si $a_3(A,\sigma) = 0$ alors la classe de $a_4(A,\sigma)$ dans $M_Q^4(k)$ est $v_4^{(1)}(A,\sigma)$.*

Démonstration. Par construction des invariants dans M_Q^d, il suffit de prouver le résultat quand A est déployée. Soit donc q de dimension 6 telle que $\sigma = \sigma_q$. On écrit $q = q_1 + q_2$ avec $q_i = \langle a_i, b_i, c_i\rangle$. D'après la proposition précédente, $q_\tau = 1 + \lambda^4(q) - \langle\langle -1, -\delta\rangle\rangle$. On a

$$\begin{aligned}
1 + \lambda^4(q) &= 1 + \lambda^3(q_1)q_2 + \lambda^2(q_1)\lambda^2(q_2) + q_1\lambda^3(q_2) \\
&= 1 + \lambda^3(q_1)\lambda^3(q_2)\lambda^2(q_2) + \lambda^2(q_1)\lambda^2(q_2) + \lambda^3(q_1)\lambda^2(q_1)\lambda^3(q_2) \\
&= (1 + \langle -\delta\rangle\lambda^2(q_1))(1 + \langle -\delta\rangle\lambda^2(q_2))
\end{aligned}$$

car $q_i = \lambda^3(q_i)\lambda^2(q_i)$, et $-\delta = \lambda^3(q_1)\lambda^3(q_2)$. Or

$$\begin{aligned}
1 + \langle -\delta\rangle\lambda^2(q_i) &= 1 + \langle -\delta\rangle\langle a_ib_i, a_ic_i, b_ic_i\rangle \\
&= (1 - \langle -\delta\rangle) + \langle -\delta\rangle\langle 1, a_ib_i, a_ic_i, b_ic_i\rangle.
\end{aligned}$$

On a donc

$$\begin{aligned}
1 + \lambda^4(q) &= (\langle\langle -\delta\rangle\rangle + \langle -\delta\rangle\langle\langle -a_1b_1, -a_1c_1\rangle\rangle)(\langle\langle -\delta\rangle\rangle + \langle -\delta\rangle\langle\langle -a_2b_2, -a_2c_2\rangle\rangle) \\
&= \langle\langle -1, -\delta\rangle\rangle - \langle\langle -\delta\rangle\rangle(\langle\langle -a_1b_1, -a_1c_1\rangle\rangle + \langle\langle -a_2b_2, -a_2c_2\rangle\rangle) \\
&+ \langle\langle -a_1b_1, -a_1c_1, -a_2b_2, -a_2c_2\rangle\rangle
\end{aligned}$$

donc

$$q_\tau = -\langle\langle -\delta\rangle\rangle(\langle\langle -a_1b_1, -a_1c_1\rangle\rangle + \langle\langle -a_2b_2, -a_2c_2\rangle\rangle) + \langle\langle -a_1b_1, -a_1c_1, -a_2b_2, -a_2c_2\rangle\rangle.$$

En particulier, comme on vérifie que $(-a_ib_i, -a_ic_i) = w_2(q_i) + (-1) \cup w_1(q_i) + (-1,-1)$, on trouve

$$\begin{aligned}
a_3(q) &= w_1(q) \cup ((-1) \cup w_1(q) + w_2(q_1) + w_2(q_2)) \\
&= (-1,-1) \cup w_1(q) + (w_1(q_1) + w_1(q_2)) \cup (w_2(q_1) + w_2(q_2)) \\
&= (-1,-1) \cup w_1(q) + w_3(q_1) + w_3(q_2) + w_1(q_1) \cup w_2(q_2) + w_1(q_2) \cup w_2(q_1) \\
&= (-1,-1) \cup w_1(q) + w_3(q).
\end{aligned}$$

Or d'après la proposition 1.2.76 on a justement $v_3^{(1)}(q) = w_3(q) + (-1,-1) \cup w_1(q)$, donc on a bien $v_3^{(1)}(q) = a_3(q)$ dans le cas déployé.

Supposons $a_3(q) = 0$. Alors $\langle\langle -\delta\rangle\rangle(\langle\langle -a_1b_1, -a_1c_1\rangle\rangle + \langle\langle -a_2b_2, -a_2c_2\rangle\rangle)$ est dans $I^4(k)$, et donc $\langle\langle -\delta, -a_1b_1, -a_1c_1\rangle\rangle = \langle\langle -\delta, -a_2b_2, -a_2c_2\rangle\rangle$, ce qui implique que

$$q_\tau = -\langle\langle -1, -\delta, -a_1b_1, -a_1c_1\rangle\rangle + \langle\langle -a_1b_1, -a_1c_1, -a_2b_2, -a_2c_2\rangle\rangle$$

et donc

$$\begin{aligned} a_4(q) &= ((-1,-1) + (-1)\cup w_1(q_1) + w_2(q_1)) \\ &\quad \cup ((-1)\cup w_1(q) + (-1,-1) + (-1)\cup w_1(q_2) + w_2(q_2)) \\ &= (-1)^{\cup 4} + (-1,-1)\cup w_2(q_1) + (-1,-1)\cup w_2(q_2) + w_2(q_1)\cup w_2(q_2) \\ &\quad + (-1)^{\cup 3}\cup w_1(q_1) + (-1)\cup w_1(q_1)\cup w_2(q_2) + (-1)\cup w_3(q_1). \end{aligned}$$

D'autre part, d'après la proposition 1.2.76 on a

$$\begin{aligned} v_4^{(1)}(q) &= a_3(q) + (-1)^{\cup 4} + (-1,-1)\cup w_2(q) + w_4(q) \\ &= (-1)^{\cup 4} + (-1,-1)\cup w_2(q_1) + (-1,-1)\cup w_2(q_2) + w_2(q_1)\cup w_2(q_2) \\ &\quad + (-1,-1)\cup w_1(q_1)\cup w_1(q_2) + w_1(q_1)\cup w_3(q_2) + w_3(q_1)\cup w_1(q_2) \end{aligned}$$

donc

$$\begin{aligned} a_4(q) - v_4^{(1)}(q) &= (-1)^{\cup 3}\cup w_1(q_1) + (-1)\cup w_1(q_1)\cup w_2(q_2) \\ &\quad + (-1)\cup w_3(q_1) + (-1,-1)\cup w_1(q_1)\cup w_1(q_2) \\ &\quad + w_1(q_1)\cup w_3(q_2) + w_3(q_1)\cup w_1(q_2). \end{aligned}$$

On conclut en montrant que cette classe est égale à $w_1(q_1)\cup a_3(q)$, qui vaut 0 par hypothèse. En effet, en utilisant le fait que $w_1(q_1)\cup w_1(q_1) = (-1)\cup w_1(q_1)$, $w_1(q_1)\cup w_2(q_1) = w_3(q_1)$ et $w_1(q_1)\cup w_3(q_1) = (-1)\cup w_3(q_1)$, on trouve :

$$\begin{aligned} w_1(q_1)\cup a_3(q) &= w_1(q_1)\cup ((-1,-1)\cup w_1(q) + w_3(q)) \\ &= w_1(q_1)\cup ((-1,-1)\cup w_1(q_1) + (-1,-1)\cup w_1(q_2) + w_3(q_1) \\ &\quad + w_2(q_1)\cup w_1(q_2) + w_1(q_1)\cup w_2(q_2) + w_3(q_2)) \\ &= (-1)^{\cup 3}\cup w_1(q_1) + (-1,-1)\cup w_1(q_1)\cup w_1(q_2) \\ &\quad + (-1)\cup w_3(q_1) + w_3(q_1)\cup w_1(q_2) \\ &\quad + (-1)\cup w_1(q_1)\cup w_2(q_2) + w_1(q_1)\cup w_3(q_2). \end{aligned}$$

□

3.3.2 Invariant a_5 en degré 12

Dans le premier chapitre, on a décrit les invariants cohomologiques des foncteurs I^n, mais également des $I^{n,1}$, dont les éléments sont de la forme $\langle\langle c\rangle\rangle q$ où q est dans I^{n-1}. Ces invariants sont du type $\Delta^{n,1}(\alpha) : \langle\langle c\rangle\rangle q \mapsto (c)\cup\alpha(q)$ où α est un invariant quelconque de I^{n-1} (voir la proposition 1.2.85). On veut étendre ces invariants à certains types d'algèbres à involution, et en particulier on étend l'invariant a_5 défini dans [9, def 20.8] (voir aussi [27, §9]) aux algèbres d'indice 2.

Précisément, soit (A, σ) une algèbre à involution orthogonale de degré 12 telle que σ soit « génériquement dans I^3 », c'est-à-dire que sur tout corps de déploiement L, σ_L est adjointe à une forme $q \in I^3(L)$ (ou encore, c'est équivalent au fait que $\langle 1\rangle_\sigma \in \widetilde{I}_0^3(A, \sigma)$). Alors, comme d'après [24] toute forme quadratique de degré 12 dans I^3 est en réalité dans $I^{3,1}$, σ est génériquement dans $I^{3,1}$. On suppose maintenant que A est d'indice 2. Pour tout invariant cohomologique $\alpha \in \mathrm{Inv}^d(I^2, \mu_2)$, on peut donc appliquer $\Delta^{3,1}(\widetilde{\alpha})$ à (A, σ) pour obtenir un élément de $M_Q^d(K)$, et si cet invariant est nul on peut définir $\Delta^{3,1}(\alpha)(A, \sigma) \in M_Q^{d+1}(K)$.

Proposition 3.3.5. *Soit (A, σ) une algèbre à involution orthogonale de degré 12 telle que σ soit adjointe à une forme dans $I^3(L)$ pour tout corps de déploiement L de A. Alors si $(-1) \cup e_3(A, \sigma) = 0$, on peut définir un invariant $a_5(A, \sigma) \in M_A^5(K)$ qui dans le cas déployé correspond à l'invariant a_5 de [9].*

Démonstration. Par construction, l'invariant a_5 est égal (avec nos notations) à $\Delta^{3,1}(u_4^{(2)})$, donc la discussion du paragraphe précédent s'applique avec $\alpha = u_4^{(2)} \in \mathrm{Inv}^4(I^2, \mu_2)$. On a alors $\widetilde{\alpha} = (-1) \cup u_2^{(2)} = (-1) \cup e_2$, donc $\Delta^{3,1}(\widetilde{\alpha}) = (-1) \cup e_3$. On définit donc, lorsque $(-1) \cup e_3(A, \sigma) = 0$, $a_5(A, \sigma) \in M_Q^5(K)$ comme $\Delta^{3,1}(u_4^{(2)})(A, \sigma)$. $\square$

On peut par ailleurs remarquer que la condition de l'énoncé est toujours vérifiée lorsque -1 est un carré dans K.

Index des notations

Général

k	corps de caractéristique $\neq 2$	
K	extension de k	
L	extension de K	
(K, v)	corps K muni d'une valuation discrète de rang 1	
$\mathbf{Field}_{/k}$	catégorie des extensions de corps de k	
$\mathbf{Set}$	catégorie des ensembles	
$\mathbf{Set}_*$	catégorie des ensembles pointés	
$(a_1, \ldots, a_r)$	symbole galoisien dans $H^n(K, \mu_2)$	
$\binom{n}{a_1,\ldots,a_r}$	coefficient multinomial	
$\lceil x \rceil$	partie entière supérieure de x	
$\lfloor x \rfloor$	partie entière inférieure de x	
$s \vee t$	*OU* logique appliqué aux bits de s et t	(1.2.48)
$s \wedge t$	*ET* logique appliqué aux bits de s et t	(1.2.48)
$\mathfrak{S}_{p,q}$	sous-groupe de Young de $\mathfrak{S}_d$	p.82
$Sh(p, q)$	ensemble des (p, q)-mélanges de $\mathfrak{S}_d$	p.82
$R[G]$	algèbre de groupe de G sur R	
R_g	composante de degré $g \in G$ de R, anneau G-gradué	
Φ	isomorphisme tautologique $R \oplus R \to R[\mathbb{Z}/2\mathbb{Z}]$	(2.2.19)
$x_{(0)}$	$\Phi(x, 0)$	(2.2.19)
$x_{(1)}$	$\Phi(0, x)$	(2.2.19)
Δ	plongement diagonal $R \to R[\mathbb{Z}/2\mathbb{Z}]$	(2.2.20)
Ψ	isomorphisme modifié $R \oplus R \to R[\mathbb{Z}/2\mathbb{Z}]$	(2.2.21)

Formes quadratiques

$\langle a_1, \ldots, a_r \rangle$	forme quadratique diagonalisée
$C(q)$	algèbre de Clifford de q
$C_0(q)$	algèbre de Clifford paire de q
$\mathrm{disc}(q)$	discriminant (signé) de q

$\mathcal{H}$	plan hyperbolique symétrique	
$\mathcal{H}_{-1}$	plan hyperbolique alterné	
$SGW(K)$	semi-anneau des formes quadratiques sur K	(2.2.1)
$GW(K)$	anneau de Grothendieck-Witt de K	
$W(K)$	anneau de Witt de K	
$SGW^-(K)$	monoïde des formes alternées sur K	(2.2.1)
$GW^-(K)$	groupe de Grothendieck-Witt des formes alternées sur K	
$SGW^{\pm}(K)$	$SGW(K) \oplus SGW^-(K)$	
$GW^{\pm}(K)$	$GW(K) \oplus GW^-(K)$	
$\hat{I}(K)$	idéal des formes de dimension nulle de $GW(K)$	p.19
$I(K)$	idéal fondamental de $W(K)$	p.19
$\langle\langle a \rangle\rangle$	forme de Pfister $\langle 1 \rangle - \langle a \rangle \in \hat{I}(K)$	p.19
$\langle\langle a_1, \ldots, a_r \rangle\rangle$	r-forme de Pfister $\langle\langle a_1 \rangle\rangle \cdots \langle\langle a_r \rangle\rangle \in \hat{I}^r(K)$	p.19
Quad_{2r}	foncteur des formes quadratiques de dim $2r$	
Quad'_{2r}	sous-foncteur de Quad_{2r} des formes de discriminant trivial	p.56
$\hat{\lambda}^d(q)$	opération λ vue à travers $I \simeq \hat{I}$	(1.2.70)
$P^d(q)$	opération $\langle a_1, \ldots, a_n \rangle \mapsto \sum_{i_1 < \cdots < i_d} \langle\langle a_{i_1}, \ldots, a_{i_d} \rangle\rangle$	(1.2.74)
$I^{n,r}(K)$	formes semi-factorisées dans $I^n(K)$	(1.2.84)

Invariants

$\mathrm{Inv}(F, H)$	invariants de F à valeurs dans H	p.13
$\mathrm{Inv}_{norm}(F, H)$	invariants normalisés de F à valeurs dans H	p.13
$\mathrm{Inv}(F, \mu_2)$	inv. cohom. de F à valeurs dans μ_2	p.13
$\mathrm{Inv}^d(F, \mu_2)$	inv. cohom. de degré d de F à valeurs dans μ_2	p.13
$\mathrm{Inv}(F, W)$	invariants de Witt de F	p.13
w_i	invariant de Stiefel-Whitney	(0.0.2)
e_n	invariant de la conjecture de Milnor	(0.0.3)
$A(K)$	généralement $H^*(K, \mu_2)$ ou $W(K)$	p.32
$A^d(K)$	composante de degré d de $A(K)$	p.32
$\delta(A) = \delta$	élément de $A(k)$ (généralement 0 ou 1)	(1.2.51)
f_n	morphisme $I^n(K) \to A^n(K)$	p.33
$\{a_1, \ldots, a_r\}$	$f_n(\langle\langle a_1, \ldots, a_r \rangle\rangle)$	p.33
M	$\mathrm{Inv}(I^n, A)$	p.35
M^d	$\mathrm{Inv}(I^n, A^d)$	p.35
f_n^d	$(f_{nd} \circ \pi_n^d) \in \mathrm{Inv}^{nd}(I^n, A)$	(1.2.7)
g_n^d	invariant dans $\mathrm{Inv}^{nd}(I^n, A)$	(1.2.32)
$u_{nd}^{(n)}$	f_n^d si $A(K) = H^*(K, \mu_2)$	(1.2.8)
$v_{nd}^{(n)}$	g_n^d quand $A(K) = H^*(K, \mu_2)$	(1.2.34)
Φ^{ε}	opérateur $M \to M$ $(\varepsilon = \pm 1)$	(1.2.16)
Φ	opérateur de décalage Φ^+	(1.2.16)

α^ε	$\Phi^\varepsilon(\alpha)$ $(\varepsilon = \pm 1)$	(1.2.16)
$\alpha^{s+,t-}$	$(\Phi^+)^s \circ (\Phi^-)^t(\alpha)$	(1.2.20)
$\alpha_{\|I^{n+1}}$	restriction de $\alpha \in \mathrm{Inv}(I^n, A)$ à I^{n+1}	p.46
Ψ	opérateur $M \to M$	(1.2.59)
$\widetilde{\alpha}$	$\Psi(\alpha)$	(1.2.59)
$h^d(q)$	$P^d(q)$ ou $w_d(q)$	p.55
$\Delta^{n,r}$	opérateur $\mathrm{Inv}_{norm}(I^{n,r}, A) \to \mathrm{Inv}_{norm}(I^{n-r}, A)$	(1.2.85)
$\alpha^{(r)}$	$\Delta^{n,r}(\alpha)$	(1.2.85)

Anneaux grecs

$G(R)$	$1 + tR[[t]] \subset R[[t]]$	(1.1.4)
α_t	opération grecque $R \to G(R)$	(1.1.6)
α^d	d-ième composante d'une opération grecque	(1.1.1)
$\Gamma(R)$	ensembe des opérations grecques de R	(1.1.1)
$+_G$	addition de $G(R)$ (produit des séries)	(1.1.29)
$\times_G$	produit de $G(R)$	(1.1.29)
ε_R	morphisme naturel $G(R) \to R$	(1.1.5)
$L(R)$	lettres grecques de R	(1.1.7)
Λ_R	application naturelle $\Gamma(R) \longrightarrow L(R)$	(1.1.8)
$A(R)$	automorphismes de $G(R)$ commutant avec ε_R	(1.1.9)
π_n^d	$d$ième composante de l'opération grecque π_n	(1.1.41)

Algèbres et involutions

(A, σ)	algèbre à involution de première espèce sur K	
(A_L, σ_L)	extension de (A, σ) au corps L	
$Sym(A, \sigma)$	éléments symétriques de $(A\sigma)$	
$Skew(A, \sigma)$	éléments anti-symétriques de (A, σ)	
$C_A(B)$	centralisateur de B dans A	
$Z(A)$	centre de A	
A^{op}	algèbre opposée de A	
Trd_A	trace réduite de A	
T_σ	forme trace d'involution de (A, σ)	(2.1.7)
T_σ^+	restriction de T_σ à $Sym(A, \sigma)$	
T_σ^-	restriction de T_σ à $Skew(A, \sigma)$	
$T_{\sigma,a}$	forme trace d'involution tordue par a	(2.2.9)
Nrd_A	norme réduite de A	
σ_b	involution adjointe de b	
σ_q	involution adjointe de q	

$Cl(A,\sigma)$	algèbre de Clifford (paire) de (A,σ)	
$K(A)$	corps de déploiement générique de A	
$K_r(A)$	corps de réduction générique à l'indice 2^r de A	p.94
$\mathrm{Br}(K)$	groupe de Brauer de K	
$[A]$	classe de Brauer de A	
$A \sim B$	A et B sont Brauer-équivalente	
$\mathbf{Br}(K)$	2-groupe de Brauer de K	partie 2.1.1
$\mathbf{Mor}(R)$	catégorie de Morita d'un anneau commutatif R	(2.1.1)
$B \xrightarrow{V} A$	V est un B-A-bimodule simple	partie 2.1.1
$\dim(V)$	dimension réduite d'un A-module	(2.4.1)
U^*	dual du B-A-bimodule U	(2.1.2)
${}^\sigma U^\tau$	bimodule dual vu à travers les involutions σ et τ	(2.1.8)
g_A	élément de Goldman de A	p.83
$g_A(\pi)$	élément de $A^{\otimes d}$ correspondant à $\pi \in \mathfrak{S}_d$	p.83
$s_{d,A} = s_d$	élément anti-symétrisant de $A^{\otimes d}$	(2.3.4)
$\mathrm{Alt}^d(V)$	puissance alternée d'un A-module	(2.3.5)
$\lambda^d(A)$	$d$ième puissance extérieure de l'algèbre A	(2.3.6)
$sh_{p,q}$	application de mélange de $V^{\otimes d}$	(2.3.8)
$x\#y$	produit de mélange de x et y	(2.3.7)
$\sigma^{\wedge d}$	puissance extérieure d'une involution	(2.3.14)

Formes hermitiennes

σ_h	involution adjointe de h	
$h \perp h'$	somme orthogonale de deux formes ε-herm.	
$\langle a\rangle_\sigma$	forme diagonale sur (A,σ)	(2.2.9)
$\mathcal{H}(A,\sigma)$	espace hyperbolique hermitien sur (A,σ)	
$\mathbf{Br}_h(K)$	2-groupe de Brauer hermitien de K	partie 2.1.2
$(B,\tau) \xrightarrow{(V,h)} (A,\sigma)$	(V,h) est un bimodule ε-hermitien	partie 2.1.2
h_A	identité de (A,σ) dans $\mathbf{Br}_h(K)$	(2.1.4)
h^*	dual de la forme ε-hermitienne h	(2.1.9)
$\varphi^{(d)}_{(A,\sigma)}$	isom. $(A,\sigma)^{\otimes d} \to (A,\sigma)$ ou (K,Id)	(2.2.7)
$\mathbf{Mor}_h(R,\iota)$	catégorie de Morita hermitienne de (R,ι)	(2.1.1)
$f \oplus f'$	somme orthogonale de morphismes dans $\mathbf{Br}_h(K)$	
$SGW^\varepsilon(A,\sigma)$	monoïde des formes ε-hermitiennes sur (A,σ)	(2.2.1)
$GW^\varepsilon(A,\sigma)$	gpe de Grothendieck-Witt des formes ε-herm.	
$W^\varepsilon(A,\sigma)$	groupe de Witt des formes ε-hermitiennes	
$SGW^\pm(A,\sigma)$	$SGW(A,\sigma) \oplus SGW^-(A,\sigma)$	(2.2.1)
$GW^\pm(A,\sigma)$	$GW(A,\sigma) \oplus GW^-(A,\sigma)$	
$W^\pm(A,\sigma)$	$W(A,\sigma) \oplus W^-(A,\sigma)$	
$\widetilde{SGW}(A,\sigma)$	semi-anneau de Grothendieck-Witt mixte de (A,σ)	(2.2.1)

$\widetilde{GW}(A,\sigma)$	anneau de Grothendieck-Witt mixte de (A,σ)	(2.2.1)
$\widetilde{W}(A,\sigma)$	anneau de Witt mixte de (A,σ)	(2.2.11)
Γ	groupe de graduation $\{+,-,o,s\}$	(2.2.2)
$\widetilde{SGW}(A,\sigma)_+$	$SGW(K)$	p.70
$\widetilde{GW}(A,\sigma)_+$	$GW(K)$	p.70
$\widetilde{W}(A,\sigma)_+$	$W(K)$	p.75
$\widetilde{SGW}(A,\sigma)_-$	$SGW^-(K)$	p.70
$\widetilde{GW}(A,\sigma)_-$	$GW^-(K)$	p.70
$\widetilde{W}(A,\sigma)_-$	0	p.75
$\widetilde{SGW}(A,\sigma)_o$	composante orthogonale de $\widetilde{SGW}(A,\sigma)$	p.70
$\widetilde{GW}(A,\sigma)_o$	composante orthogonale de $\widetilde{GW}(A,\sigma)$	p.70
$\widetilde{W}(A,\sigma)_o$	composante orthogonale de $\widetilde{W}(A,\sigma)$	p.75
$\widetilde{SGW}(A,\sigma)_s$	composante symplectique de $\widetilde{SGW}(A,\sigma)$	p.70
$\widetilde{GW}(A,\sigma)_s$	composante symplectique de $\widetilde{GW}(A,\sigma)$	p.70
$\widetilde{W}(A,\sigma)_s$	composante symplectique de $\widetilde{W}(A,\sigma)$	p.75
$\widetilde{GW}(K)$	$\widetilde{GW}(K,\mathrm{Id})$	(2.2.17)
$\widetilde{W}(K)$	$\widetilde{W}(K,\mathrm{Id})$	(2.2.18)
$\mathrm{Alt}^d(h)$	puissance alternée d'une forme ε-herm.	(2.3.12)
$\Lambda^d(V)$	puissance extérieure d'un A-module	(2.3.17)
$\lambda^d(h)$	puissance extérieure d'une forme ε-herm.	(2.3.17)
$\dim(h)$	dimension réduite d'une forme ε-herm.	(2.4.1)
$\widetilde{GI}(A,\sigma)$	idéal fondamental de $\widetilde{GW}(A,\sigma)$	p.90
$\widetilde{I}(A,\sigma)$	idéal fondamental de $\widetilde{W}(A,\sigma)$	p.90
$\widetilde{GI}(A,\sigma)_o$	$\widetilde{GI}(A,\sigma)\cap\widetilde{GW}(A,\sigma)_o$	p.90
$\widetilde{I}(A,\sigma)_o$	$\widetilde{I}(A,\sigma)\cap\widetilde{W}(A,\sigma)_o$	p.90
$\widetilde{GI}(A,\sigma)_s$	$\widetilde{GI}(A,\sigma)\cap\widetilde{GW}(A,\sigma)_s$	p.90
$\widetilde{I}(A,\sigma)_s$	$\widetilde{I}(A,\sigma)\cap\widetilde{W}(A,\sigma)_s$	p.90
$\widetilde{H}^n(A,\sigma)$	cohomologie mixte	2.4.3
$\widetilde{GI}(K)$	$\widetilde{GI}(K,\mathrm{Id})$	p.91
$\widetilde{I}(K)$	$\widetilde{I}(K,\mathrm{Id})$	p.91
$GI(K)$	$\mathrm{Ker}(GW^{\pm}(K)\to\mathbb{Z})$	p.91
$GJ(K)$	$\mathrm{Ker}(GW^{\pm}(K)\to\mathbb{Z}/2\mathbb{Z})$	p.91
$GJ^{(n)}(K)$	$GI^{n-1}(K)GJ(K)$ $(n\geqslant 1)$	p.91
$\widetilde{H}^n(K)$	$\widetilde{H}^d(K,\mathrm{Id})$	(2.4.6)
$I^n(A,\sigma)_o$	$I^{n-1}(K)W(A,\sigma)_o$	(2.4.8)
$H^n(A,\sigma)_o$	$I^n(A,\sigma)_o/I^{n+1}(A,\sigma)_o$	(2.4.9)
$I^n(A,\sigma)_s$	$I^{n-1}(K)W(A,\sigma)_s$	(2.4.8)

$H^n(A,\sigma)_s$	$I^n(A,\sigma)_s/I^{n+1}(A,\sigma)_s$	(2.4.9)
$\widetilde{GI}_r^n(A,\sigma)$	élém. dans $\widetilde{GI}^n(A,\sigma)$ sur $K_r(A)$	(2.4.13)
$\widetilde{I}_r^n(A,\sigma)$	élém. dans $\widetilde{I}^n(A,\sigma)$ sur $K_r(A)$	(2.4.13)

Quaternions

$(Q,^-)$	algèbre de quaternions munie de son involution canonique	
n_Q	forme norme d'une algèbre de quaternions Q	
$\varphi_{z_1,\ldots,z_r}$	r-forme de Pfister $\langle\langle z_1^2,\ldots,z_r^2\rangle\rangle - \langle\langle -1\rangle\rangle^{r-2}n_Q$	(2.2.24)
$\mathfrak{p}$	point fermé de la variété de Severi-Brauer	p.94
$v_{\mathfrak{p}}$	valuation induite par $\mathfrak{p}$	p.94
$\partial_{1,\mathfrak{p}}$	premier résidu $W(F)\to W(K(\mathfrak{p}))$	p.94
$\partial_{2,\mathfrak{p}}$	deuxième résidu $W(F)\to W(K(\mathfrak{p}))$	p.94
ext_∞	extension des scalaires $W^-(Q,^-)\to W(F)$	(2.4.14)
$W_{nr,1,\infty}(F)$	premier groupe de Witt non ramifié	(2.4.15)
$W_{nr,2,\infty}(F)$	deuxième groupe de Witt non ramifié	(2.4.16)
$\partial_{\mathfrak{p}}$	résidu $H^d(F,\mu_2)\to H^{d-1}(K(\mathfrak{p}),\mu_2)$	p.95
$H^d_{nr}(F,\mu_2)$	cohomologie non ramifiée	(2.4.20)
$\widetilde{e}_d$	invariant $\widetilde{I}_0^d(Q,^-)\to H^{d-1}_{nr}(F,\mu_2)$	(2.4.21)
$M^d_A(K)$	2-torsion de $H^d(K,\mu_4^{\otimes d-1})/[A]\cdot H^{d-2}(K,\mu_2)$	(2.4.23)
$N^d_A(K)$	$H^d(K,\mu_2)/[A]\cdot H^{d-2}(K,\mu_2)$	p.96
F_Q	formes anti-herm. sur Q compatibles avec F	p.103
$F_{\alpha,Q}$	sous-foncteur de F_Q des formes compatibles avec α	p.103
$\hat{\alpha}$	invariant dans $\mathrm{Inv}(F_{\alpha,Q},M^d_Q)$ induit par α	(3.1.6)

Produits croisés

K	k-algèbre étale	p.108
$K_{\mathfrak{p}}$	composante de K correspondant à $\mathfrak{p}$ß $\mathrm{Spec}(K)$	p.108
u_g	générateur d'un produit croisé	p.110
$\alpha(g,h)$	2-cocycle décrivant un produit croisé	(3.2.7)
T_g	opération semi-linéaire sur V	(3.2.8)
S_g	opération semi-linéaire sur $\mathrm{End}_L(V)$	(3.2.9)
$\overline{g}$	$\theta_{\|L}g^{-1}\theta_{\|L}$	(3.2.13)
θ_g	$g\theta_{\|L}$	(3.2.14)
θ'_g	$g^{-1}\theta_{\|L}$	(3.2.14)
μ_g	élément de L^* décrivant l'involution sur un produit croisé	(3.2.16)
π_g	projection $E\to L$ liée à g	(3.2.21)
$h_g(x,y)$	$\pi_g(h(x,y))$	(3.2.20)
$f_g(x,y)$	$\pi_g(\theta(x)y)$	(3.2.22)

$\varepsilon_g \quad g^{-1}(\mu_g)$ (3.2.26)

Algèbre de Clifford

Q	algèbre de quaternion équivalente à A
B	$Cl(A,\sigma)$
(e_i)	base orthogonale de V
$\langle z_1,\dots,z_r\rangle$	diagonalisation de h
L	sous-algèbre étale de B
G	$\mathrm{Gal}(L/k)$
H	$\mathrm{Gal}(L/Z(B))$
$\tau_{p,q}$	élément de G
K	sous-corps quadratique de Q
j	quaternion pur, $Q = K \oplus jK$
π	j^2
s	élément non trivial de $\mathrm{Gal}(K/k)$
b	forme bilinéaire, $\sigma_K \simeq \sigma_b$
φ_b	identification $V \otimes_K V \to \mathrm{End}_K(V)$
ψ	morphisme canonique $V \otimes_Q ({}^{\gamma}V) \to Cl(A,\sigma)$
$u(x,y)$	$\frac{1}{2}\psi(x\otimes y + y\otimes x)$
$u(x)$	$\frac{1}{2}\psi(x\otimes x)$
ξ_i	$u(e_i)$
ξ	$\prod_i \xi_i$
$u_{p,q}$	$u(e_p,e_q)$

Bibliographie

[1] Adrian Albert. Involutorial simple algebras and real riemann matrices. *Ann. of Math.*, 1935.

[2] Jon K. Arason. Cohomologische invarianten quadratischer formen. *Journal of algebra*, 1975.

[3] John Baez and Aaron Lauda. Higher-dimensional algebra v : 2-groups. *Theory and Applications of Categories*, 2003.

[4] Grégory Berhuy. Cohomological invariants of quaternionic skew-hermitian modules. 2006.

[5] Grégory Berhuy, Marina Monsurro, and Jean-Pierre Tignol. The discriminant of a symplectic involution. *Pacific J. Math.*

[6] Ingrid Dejaiffe. Somme orthogonale d'algèbres à involution et algèbre de clifford. *Communications in algebra*, 1998.

[7] Richard Elman, Nikita Karpenko, and Alexander Merkurjev. *The algebraic and geometric theory of quadratic forms.* AMS.

[8] Miguel Ferrero and Antonio Paques. Galois theory of commutative rings revisited. *Contributions to algebra and geometry*, 1997.

[9] Skip Garibaldi. *Cohomological invariants, exceptional groups and Spin groups.* AMS, 2009.

[10] Skip Garibaldi, Alexander Merkurjev, and Jean-Pierre Serre. *Cohomological invariants in Galois theory.* AMS.

[11] Skip Garibaldi, Parimala, and Jean-Pierre Tignol. Discriminant of symplectic involutions. *Pure and applied mathematics*, 2009.

[12] Philippe Gille and Tamàs Szamuely. *Central simple algebras and Galois cohomology.* Cambridge, 2006.

[13] Bill Jacob and Markus Rost. Degree four cohomological invariants for quadratic forms. *Invent. Math.*, 1989.

[14] Nathan Jacobson. *Basic Algebra II.* Dover, 2009.

[15] Bruno Kahn, Markus Rost, and R. Sujatha. Unramified cohomology of quadrics i. *American Journal of Mathematics*, 1998.

[16] Max-Albert Knus. *Quadratic and hermitian forms over rings.* Springer-Verlag, 1991.

[17] Max-Albert Knus, Alexander Merkurjev, Markus Rost, and Jean-Pierre Tignol. *The Book of Involutions.* AMS, 1998.

[18] Max-Albert Knus, Parimala, and Srinivas. Azumaya algebras with involution. *Journal of algebra*, 1990.

[19] T.Y. Lam. *Quadratic forms over fields.* AMS, 2004.

[20] David Lewis. A product of hermitian forms over quaternion division algebras. *J. London Math. Soc.*, 1980.

[21] Alexander Merkurjev. Degree three cohomological invariants of semisimple groups. *JEMS*, 2016.

[22] Alexander Merkurjev. Unramified degree three invariants of reductive groups. *Adv. Math.*, 2016.

[23] James Milnor. Algebraic k-theory and quadratic forms. *Invent. Math.*, 1970.

[24] Albrecht Pfister. Quadratische formen in beliebigen körpen. *Invent. Math.*, 1966.

[25] Anne Quéguiner. Cohomological invariants of algebras with involution. *Journal of algebra*, 1997.

[26] Anne Quéguiner and Jean-Pierre Tignol. Quaternionic skew-hermitian forms and function fields of conics. prépublication.

[27] Markus Rost. On the galois cohomology of spin(14). non publié.

[28] Markus Rost, Jean-Pierre Serre, and Jean-Pierre Tignol. La forme trace d'une algèbre simple centrale de degré 4. *C.R. Acad. Sci. Paris*, 2005.

[29] Elizabeth Seip-Hornix. Clifford algebras of quadratic quaternion forms. *Indagationes Mathematicae*, 1965.

[30] Jean-Pierre Serre. *Cohomologie galoisienne.* Springer, 5 edition, 1994.

[31] Jean-Pierre Tignol. *Quadratic forms, linear algebraic groups and cohomology*, chapter Cohomological invariants of algebras with involution. Springer, 2010.

[32] Charles Vial. Operations in milnor k-theory.

[33] Vladimir Voevodsky. Motivic cohomology with $\mathbf{Z}/2$ coefficients. *Publ. Math. IHES*, 2003.

[34] André Weil. Algebras with involutions and the classical groups. *J. Indian Math. Soc.*, 1960.

[35] Donald Yau. *Lambda-Rings.* World Scientific, 2010.

[36] Élie Cartan. *Sur la structure des groupes de transformations finis et continus.* PhD thesis, ENS, 1894.

Thèse de mathématiques

Mots-clés : invariant cohomologique, algèbre à involution, opération lambda, anneau de Witt, filtration fondamentale, équivalence de Morita hermitienne.

Résumé : Afin d'étudier certains types d'objets algébriques, et notamment les groupes algébriques, Serre a introduit la notion d'invariants, en particulier d'invariants cohomologiques. La construction d'invariants cohomologiques non triviaux de groupes algébriques est un domaine actif de la recherche actuelle, et très peu d'invariants sont connus en degré strictement supérieur à 3.

Dans le premier chapitre, on donne une description complète des invariants de Witt et des invariants cohomologiques des foncteurs I^n comme combinaison d'invariants fondamentaux se comportant comme des puissances divisées, dont la construction repose de façon cruciale sur les opérations lambda dans l'anneau de Grothendieck-Witt. On étudie également le comportement des ces invariants vis-à-vis de diverses opérations comme le produit ou les similitudes.

Le deuxième chapitre est consacré à la construction d'un anneau de Witt « mixte » associé à une algèbre à involution : l'idée fondamentale est de définir le produit de deux formes *eps*-hermitiennes à l'aide d'une équivalence de Morita canonique donnée par la forme trace d'involution associée à l'algèbre. On définit également des opérations lambda sur l'anneau de Grothendieck-Witt mixte, ainsi qu'une filtration fondamentale imitant le cas déployé. Une attention particulière est portée aux calculs explicites dans le cas des algèbres d'indice 2.

On mobilise ces outils dans le troisième chapitre pour imiter les constructions du chapitre 1 dans le cadre des formes hermitiennes, et on construit ainsi des invariants cohomologiques d'algèbres à involution, avec des résultats plus détaillés en indice 2. L'intérêt principal est de pouvoir en principe construire des invariants non triviaux de degré arbitrairement grand, bien que l'indice de l'algèbre constitue une forme d'obstruction.

Title : Cohomological invariants of algebraic groups and algebras with involution

Abstract : In order to study certain algebraic objects, and notably algebraic groups, Serre introduced the notion on invariants, in particular cohomological invariants. The construction of non-trivial cohomological invariants of algebraic groups is an active area of modern research, and very few invariants are known in degree greater than 3.

In the first chapter, we give a complete description of Witt and cohomological invariants of the functors I^n as combinations of fundamental invariants behaving like divided powers, whose construction relies crucially on lambda operations in the Grothendieck-Witt ring. We also study the behaviour of these invariants with respect to various operations such as products or similitudes.

The second chapter is dedicated to the construction of a "mixed" Witt ring associated to an algebra with involution : the fundamental idea is to define the product of two ε-hermitian forms using a Morita equivalence given by the involution trace form of the algebra. We also define lambda operations on the mixed Grothendieck-Witt ring, as well as a fundamental filtration imitating the split case. A particular attention is given to explicit calculations in the case of algebras of index 2.

We use those tools in the third chapter to mimic the constructions of chapter 1 in the framework of hermitian forms, and thus construct cohomological invariants of algebras with involution, with more detailed results in index 2. The main interest is to be in principle able to define non-trivial invariants of arbitrarily high degree, although the index constitues a form of obstruction.

Thèse préparée au LAGA (UMR 7539) - Institut Galilée
99 avenue Jean Baptiste clément
93430 Villetaneuse