N° d'ordre : 2267

THESE

présentée à

L'UNIVERSITÉ BORDEAUX I

ÉCOLE DOCTORALE DE MATHÉMATIQUES ET INFORMATIQUE

PAR **Jean-Yves DEGOS**

POUR OBTENIR LE GRADE DE

DOCTEUR

SPÉCIALITÉ : MATHÉMATIQUES PURES

Classes caractéristiques de représentations galoisiennes et invariants d'algèbres étales sur un corps de caractéristique 2

Soutenue le 9 octobre 2000.

Après avis de :

M. B. KAHN, Directeur de Recherches	Université Paris VII	Rapporteurs
M. M. OJANGUREN, Professeur	Université de Lausanne	

Devant la commission d'examen formée de :

M. J. BARGE, Professeur	Ecole Polytechnique	
M. P. CASSOU-NOGUÈS, Professeur	Université Bordeaux I	
M. B. EREZ, Professeur	Université Bordeaux I	Directeur de thèse
M. M. OJANGUREN, Professeur	Université de Lausanne	

– 2000 –

Remerciements

J'ai pu établir un premier contact favorable avec Boas Erez à l'occasion de travaux dirigés de Géométrie Algébrique en Maîtrise, puis d'un travail sur les démonstrations de la loi réciprocité quadratique effectué en D. E. A.. Ayant une prédilection pour l'algèbre et préférant les enchaînements d'idées aux calculs, c'est tout naturellement que je l'ai sollicité en 1997 pour diriger mes recherches. Au cours de ces années, j'ai pu apprécier son humanité, sa générosité et sa conception horizontale des mathématiques. Je le remercie d'avoir accepté de m'encadrer lors de ce travail.

J'ai pu voir exposer Bruno Kahn à plusieurs reprises sur des thèmes en relations directes avec les questions abordées dans cette thèse. Je lui suis reconnaissant d'avoir accepté d'être rapporteur.

Manuel Ojanguren a également bien voulu examiner ma thèse, et je le remercie de l'avoir fait avec beaucoup de précisions.

Jean Barge, avec lequel j'ai pu avoir des échanges fructueux en 1998 lors d'un colloque autour des formes quadratiques à Paris, et Philippe Cassou-Noguès, dont j'apprécie toujours les qualités d'exposant, ont accepté de faire partie du jury ; je les en remercie vivement.

Sur le plan mathématique, je voudrais remercier Ian J. Leary, Victor P. Snaith, et Andrzej Kozlowski pour l'intérêt qu'ils ont manifesté pour mon travail, ainsi que Karl Gruenberg, Martin J. Taylor, et Peter Kropholler pour les cours qu'ils ont donnés à Edimbourg en 1998 concernant certains aspects de l'Algèbre Homologique que l'on retrouve mis en oeuvre dans le premier chapitre : cohomologie des groupes, cohomologie galoisienne et cohomologie singulière.

En cette période où la place des Mathématiques dans l'enseignement s'est trouvée récemment contestée, j'ai également plaisir à exprimer ma gratitude aux professeurs de Mathématiques dont j'ai été l'élève puis l'étudiant depuis la sixième : sans leur participation, je n'aurais pas été conduit à vouloir entreprendre ce travail.

Sur le plan matériel, je voudrais mentionner les structures grâce auxquelles j'ai pu bénéficier d'excellentes conditions de travail : le Laboratoire de Mathématiques Pures, l'Ecole doctorale de Mathématiques et Informatique, ainsi que l'Institut de Mathématiques de Bordeaux.

Je remercie tous les doctorants bordelais que j'ai cotoyés, pour leur convivialité et leur sens de l'humour, en particulier Eric Edo et Stanislav Kupin, mes collègues de bureau.

Les encouragements de Nicolas Brisebarre, le soutien d'Emmanuelle Alonso, et les moments partagés avec Gilles Rémus et Claire Jacquemart m'ont beaucoup apporté.

Enfin, le dernier mot sera pour mes parents, qui ont su créer autour de moi une atmosphère favorable aux études.

Table des matières

Introduction **7**

1 Classes caractéristiques de représentations galoisiennes **13**
1.1 Le problème d'Atiyah et le théorème de Fulton-MacPherson . . . 13
1.1.1 Revêtements auxiliaires 14
1.1.2 Le transfert d'Evens 16
1.1.3 Le théorème de Fulton-MacPherson 18
1.2 La conjecture de Segal et le théorème de Kozlowski 19
1.2.1 Introduction 19
1.2.2 Le transfert de Kozlowski 21
1.2.3 Le transfert d'Evens normalisé 22
1.2.4 Egalité des transferts sur les classes de Stiefel-Whitney . . 25
1.3 Relation avec le théorème de Kahn 27
1.3.1 Les idées 28
1.3.2 Des extensions aux revêtements et des représentations aux fibrés vectoriels via les espaces classifiants 29
1.3.3 L'égalité des transferts en cohomologie galoisienne 36
1.4 Conclusion et problèmes ouverts 42

2 Invariants d'algèbres étales sur un corps de caractéristique 2 **43**
2.1 Invariants dans le groupe $H^1(G_F, \mathbb{Z}/2\mathbb{Z})$ 43
2.1.1 L'invariant $\epsilon(e_{E/F})$ d'une algèbre étale E/F 43
2.1.2 Sur l'invariant de Arf d'un espace quadratique 44
2.1.3 Sur l'invariant de Dickson d'un automorphisme orthogonal 47
2.1.4 Forme $\widetilde{T}_{E/F}$ et invariant $d^+(E/F)$ d'une algèbre étale . . . 51
2.1.5 L'égalité $j(d^+(E/F)) = \epsilon(e_{E/F})$ 54
2.2 Calculs de discriminants additifs d'extensions 59
2.2.1 Méthode des relèvements 59
2.2.2 Méthode des polynômes symétriques 61
2.2.3 Méthode s_2 64
2.3 Invariants dans le groupe $H^1(G_F, F_s^*/F_s^{*2})$ 65
2.3.1 L'invariant de Clifford 65
2.3.2 Un critère de trivialité 66

2.3.3 La norme spinorielle 67
2.4 Conclusion et questions ouvertes 70

A Le théorème de Cartan-Dieudonné en caractéristique 2 **73**

B Fonctions Maple utilisées **79**

C Discriminants additifs obtenus avec Maple **83**
C.1 Notations 83
C.2 Résultats 83

D A propos du pfaffien **87**
D.1 Introduction 87
D.2 Formule de développement 89
D.3 Application : coefficients de la comatrice alternée 90

Bibliographie du chapitre 1 **93**

Bibliographie du chapitre 2 **97**

Introduction

Cette thèse s'organise en deux chapitres dont le dénominateur commun est une formule publiée par J.-P. Serre en 1984, exprimant une relation entre invariants quadratiques que l'on peut attacher à une algèbre étale E de rang n sur un corps F de caractéristique différente de 2 (c'est-à-dire une algèbre isomorphe à un produit d'extensions finies séparables sur F).

A une telle algèbre, sont associés plusieurs invariants dans les groupes de cohomologie galoisienne $H^1(G_F, \mathbb{Z}/2\mathbb{Z}) \simeq F^*/F^{*2}$ et $H^2(G_F, \mathbb{Z}/2\mathbb{Z}) \simeq \mathrm{Br}_2(F)$, par deux voies différentes.

La première voie consiste à utiliser la théorie des formes quadratiques, plus précisément, à utiliser la forme quadratique $Q_E : x \mapsto Tr_{E/F}(x^2)$ qui est non dégénérée de rang n. Un invariant dans $H^1(G_F, \mathbb{Z}/2\mathbb{Z})$ est obtenu par le biais du discriminant $(d_{E/F}) = w_1(Q_E)$ de Q_E. Un invariant dans $H^2(G_F, \mathbb{Z}/2\mathbb{Z})$ est obtenu en considérant l'invariant de Hasse-Witt de Q_E, noté $w_2(Q_E)$.

La seconde voie consiste à utiliser la théorie de Galois, plus précisément, en notant $\mathfrak{S}_n$ le groupe symétrique d'ordre n, à utiliser un élément $e_{E/F} \in H^1(G_F, \mathfrak{S}_n)$ bien défini à conjugaison près qui caractérise E à isomorphisme près. Un invariant dans $H^1(G_F, \mathbb{Z}/2\mathbb{Z})$ est obtenu en composant $e_{E/F}$ avec la signature $\epsilon : \mathfrak{S}_n \to \mathbb{Z}/2\mathbb{Z}$. Un invariant dans $H^2(G_F, \mathbb{Z}/2\mathbb{Z})$, à l'aide de l'élément $s_n \in H^2(\mathfrak{S}_n, \mathbb{Z}/2\mathbb{Z}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ correspondant à l'extension

$$1 \to \{1, \omega\} \to \tilde{\mathfrak{S}}_n \to \mathfrak{S}_n \to 1\,, \tag{1}$$

est construit en considérant $e^*_{E/F} s_n \in H^2(G_F, \mathbb{Z}/2\mathbb{Z})$. L'extension (1) est obtenue par image inverse de l'extension $\mathrm{Pin}_n \to O_n$.

La clé pour la comparaison des invariants obtenus par les deux voies différentes se trouve dans les faits suivants. Si $O_n(F_s)$ désigne le groupe orthogonal de la forme $(x_1, \ldots, x_n) \mapsto \sum_{i=1}^n x_i^2$ sur F_s^n, alors l'ensemble de cohomologie $H^1(G_F, O_n(F_s))$ classe les formes quadratiques non dégénérées de rang n définies sur F, et l'image d'un élément de $e_{E/F} \in H^1(G_F, \mathfrak{S}_n)$ définissant l'algèbre E/F par l'application

$$H^1(G_F, \mathfrak{S}_n) \to H^1(G_F, O_n(F_s))$$

déduite du plongement naturel de $\mathfrak{S}_n$ dans $O_n(F_s)$ (groupe orthogonal de la somme de carrés), correspond précisément à la classe de l'espace quadratique $(E, x \mapsto Tr_{E/F}(x^2))$.

Les invariants dans $H^1(G_F,\mathbb{Z}/2\mathbb{Z})$ mentionnés ci-dessus *coïncident*. Cela provient du fait que le déterminant d'une matrice de permutation est égal à la signature de cette permutation. La "formule de Serre" ([Se2], Théorème 1, page 65) exprime qu'il y a cependant une relation non triviale entre les invariants dans $H^2(G_F,\mathbb{Z}/2\mathbb{Z})$ évoqués ci-dessus. Plus précisément, on a :

$$w_2(Q_E) = e^*_{E/F}s_n + (2, d_{E/F})\,. \tag{2}$$

Si F est un corps de caractéristique différente de 2, E/F une extension finie séparable, $\rho : G_E \to Gl(V)$ une représentation galoisienne réelle de degré $r \geq 1$, il est possible d'attacher à ρ des classes (de Stiefel-Whitney) $w_i(\rho) \in H^i(G_E,\mathbb{Z}/2\mathbb{Z})$, et on désigne alors par $w(\rho)$ la classe totale $w(\rho) := \sum_{i\geq 0} w_i(\rho) \in H^*(G_E,\mathbb{Z}/2\mathbb{Z})$ avec $w_0(\rho) = 1$ par convention.

La formule de Serre apparaît comme un argument essentiel dans la preuve du résultat suivant établi par B. Kahn en 1984 ([Ka1], Théorème 1, page 224) : dans $H^*(G_F,\mathbb{Z}/2\mathbb{Z})$,

$$w(\mathrm{Ind}_{G_E}^{G_F}\rho) = w(\mathrm{Ind}_{G_E}^{G_F}\mathbf{1}_{G_E})^r\mathcal{N}_{E/F}(w(\rho))\,, \tag{3}$$

où $\mathcal{N}_{E/F} : H^{**}(G_E,\mathbb{Z}/2\mathbb{Z}) \to H^{**}(G_F,\mathbb{Z}/2\mathbb{Z})$ est le transfert multiplicatif et $\mathbf{1}_{G_E}$ la représentation triviale de degré 1 de G_E.

Cet énoncé apporte une solution, dans un cas particulier, à un problème posé par M. Atiyah (voir [Ati] page 63), qui demandait que l'on trouve une expression générale pour les classes caractéristiques de la représentation $\mathrm{Ind}(\rho)$ induite d'une représentation ρ en termes des classes de ρ.

En 1984, W. Fulton et R. MacPherson ont donné ([FM2], Formule 5.5, page 20, annoncée dans [FM1]) une formule — que nous énonçons ci-après dans un cas particulier — dans un contexte où $f : X \to Y$ est un revêtement de degré n de CW-complexes, et R un fibré vectoriel de rang $r \geq 1$ sur X, et l'on a alors

$$w(f_*R) = w(f_*\mathbf{1}_X)^r\left(\mathcal{N}_f(w(R)) + \sum_\lambda f_{\lambda *}\left((w(V_\lambda)^{-1} - 1).\chi_\lambda(w(R))\right)\right)\,, \tag{4}$$

égalité qui a lieu dans l'algèbre $H^*(Y,\mathbb{Z}/2\mathbb{Z})$ de cohomologie singulière modulo 2 de l'espace Y. Le sens des notations intervenant dans la formule ci-dessus sera précisé ultérieurement. Ce qu'il faut observer à ce stade est que la forme du second membre ci-dessus suggère que l'on puisse déduire la formule de Kahn (3) de celle de Fulton et MacPherson, et ces derniers ont posé la question de savoir comment l'on pouvait y parvenir.

Le *premier chapitre* de cette thèse répond à cette question. On y démontre

Théorème 1 (Théorème 1.3.1, page 27) *La formule de Kahn (3) s'obtient à partir de la formule de Fulton-MacPherson (4) par inflation à la cohomologie galoisienne.*

Ce théorème est démontré dans la section 1.3. Dans la section 1.1, on revient sur les classes de Stiefel-Whitney, le problème d'Atiyah et sur les notations intervenant dans l'énoncé de la formule (4), en particulier sur le transfert d'Evens $\mathcal{N}_f$. Ce transfert se comporte en général mal avec les classes de Stiefel-Whitney, ce qui a conduit A. Kozlowski, en relation avec une conjecture de G. Segal (sur laquelle nous reviendrons dans la section 1.2), à construire un transfert $\mathcal{N}_f^w$ qui se comporte bien avec elles, ainsi qu'à définir un transfert d'Evens normalisé $\widetilde{\mathcal{N}}_f$.

C'est un problème ouvert que de montrer l'égalité $\mathcal{N}_f^w = \widetilde{\mathcal{N}}_f$. Cette égalité résulterait d'une propriété de transitivité concernant le transfert d'Evens normalisé, à savoir $\widetilde{\mathcal{N}}_{g\circ f} = \widetilde{\mathcal{N}}_g \circ \widetilde{\mathcal{N}}_f$. Dans cette perspective, nous démontrons

Théorème 2 (Th. 1.2.8, Th. 1.2.9 pages 16-17) *Si $x \in H^{**}(X, \mathbb{Z}/2\mathbb{Z})$ est une classe de Stiefel-Whitney totale de fibré vectoriel ou un élément homogène, alors*

$$\widetilde{\mathcal{N}}_{g\circ f}(x) = \widetilde{\mathcal{N}}_g(\widetilde{\mathcal{N}}_f(x))\,.$$

Le point clé pour la comparaison des énoncés de Kahn et Fulton-MacPherson, est que, en cohomologie galoisienne, on a l'égalité $\mathcal{N}_{E/F}^w = \widetilde{\mathcal{N}}_{E/F}$, qui repose au minimum sur le fait que les classes de Stiefel-Whitney totales de représentations galoisiennes sont décomposables (i. e. sommes de cup-produits de termes de degré 1) établi par Kahn ([Ka1], Théorème 4 page 247), que l'on peut également justifier par le théorème de Voevodsky (toute classe de cohomologie galoisienne est décomposable).

Le *second chapitre* de cette thèse s'intéresse au cas où le corps de base F est maintenant de *caractéristique* 2. On a de bons analogues pour les invariants définis par les deux voies indiquées au début de l'introduction, qui sont à valeurs dans le groupe $H^1(G_F, \mathbb{Z}/2\mathbb{Z})$.

Le cobord de la suite longue de cohomologie associée à la suite exacte d'Artin-Schreier

$$0 \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow F_s \xrightarrow{\wp : x \mapsto x^2 + x} F_s \longrightarrow 0$$

permet d'obtenir un isomorphisme

$$j : F/\wp(F) \xrightarrow{\simeq} H^1(G_F, \mathbb{Z}/2\mathbb{Z})\,.$$

A toute algèbre étale E/F de rang n on associe son discriminant additif $d^+(E/F)$ à valeurs dans $F/\wp(F)$, défini par

$$d^+(E/F) = \mathrm{Arf}\,(\widetilde{T}_{E'/F}) + \varepsilon(n')\,.$$

Dans cet énoncé, $E' = E$ (resp. $E' = E \times F$) si n est pair (resp. impair) et pour $k \in \mathbb{Z}$, $\varepsilon(k) = 0$ (resp. $\varepsilon(k) = 1$) si $k \bmod 8 \in \{0, 1, 2, 7\}$ (resp. si $k \bmod 8 \in \{3, 4, 5, 6\}$). Enfin, $\mathrm{Arf}\,(\widetilde{T}_{E'/F})$ est l'invariant de Arf de la forme quadratique non dégénérée $\widetilde{T}_{E'/F}$ associée à E' : si $x \in E'$, $\widetilde{T}_{E'/F}(x)$ est le coefficient en degré $n'-2$ du polynôme caractéristique de la multiplication par x sur le F-espace vectoriel E'.

D'autre part, l'algèbre étale E/F correspond à isomorphisme près à un élément $e_{E/F} \in H^1(G_F, \mathfrak{S}_n)$ comme plus haut. La signature

$$\epsilon : \mathfrak{S}_n \longrightarrow \mathbb{Z}/2\mathbb{Z}$$

notée additivement induit une application

$$\begin{array}{rcl} H^1(G_F, \mathfrak{S}_n) & \longrightarrow & H^1(G_F, \mathbb{Z}/2\mathbb{Z}) \\ e & \longmapsto & \big(\gamma \mapsto \epsilon(e(\gamma))\big) \end{array}$$

qui permet d'associer à E/F un invariant dans $H^1(G_F, \mathbb{Z}/2\mathbb{Z})$, à savoir

$$\epsilon(e_{E/F}),$$

où $\epsilon(e_{E/F})$ est une notation abusive pour l'élément $\gamma \mapsto \epsilon(e_{E/F}(\gamma))$.

Dans [BM], A.-M. Bergé et J. Martinet ont démontré le résultat suivant.

Théorème 3 (Théorème 2.1.21, page 54) *Soit E/F une algèbre étale de rang n, et $e_{E/F} \in H^1(G_F, \mathfrak{S}_n)$ défini à conjugaison près, caractérisant E à isomorphisme près. Alors, on a dans $H^1(G_F, \mathbb{Z}/2\mathbb{Z})$,*

$$j(d^+(E/F)) = \epsilon(e_{E/F}),$$

où $j : F/\wp(F) \xrightarrow{\simeq} H^1(G_F, \mathbb{Z}/2\mathbb{Z})$ est l'isomorphisme donné par la théorie d'Artin-Schreier, $d^+(E/F)$ est le discriminant additif, et

$$\epsilon : H^1(G_F, \mathfrak{S}_n) \to H^1(G_F, \mathbb{Z}/2\mathbb{Z})$$

est l'application induite par la signature.

Le résultat principal de ce chapitre est une redémonstration de ce théorème.

Il faut mentionner que quatre démonstrations (voir [KMRT], Notes, page 321) de ce théorème sont disponibles dans la littérature.

Tout d'abord celle de Bergé-Martinet ([BM], Théorème 2.6), qui définissent l'invariant $d^+(E/F)$ en ayant recours à des relèvements à des anneaux de valuation discrète de caractéristique 0. Le langage cohomologique, en particulier la torsion galoisienne au moyen d'un élément $e_{E/F} \in H^1(G_F, \mathfrak{S}_n)$, n'apparaît pas explicitement.

Ensuite, celle de A. Wadsworth ([Wad], Théorème 1.16 page 245), qui prouve la relation entre l'invariant de Berlekamp d'une extension E/F et l'invariant de Revoy (dont la définition dans le cas où E/F est de degré impair diffère légèrement de celle de l'invariant $d^+(E/F)$) qui avait été conjecturée par P. Revoy ([Rev], Conjecture (C) page 233), et présente essentiellement les mêmes caractéristiques que la précédente.

En se plaçant dans le cadre de la théorie de la descente, W. C. Waterhouse a proposé une définition naturelle du "discriminant". Dans ce cadre, il montre que les définitions choisies par Revoy sans cette approche systématique sont les bonnes, et montre trois formules qui rendent compte des situations en toutes caractéristiques (voir à ce sujet la Remarque 2.1.25 page 58 qui explicite le passage de son résultat à celui du Théorème 3). La démonstration de ces formules, qui sont la conclusion de l'article [Wat], utilise clairement les méthodes cohomologiques, ne fait pas appel à des rélèvements en caractéristique 0, mais utilise des résultats concernant les groupes algébriques.

Enfin plus récemment, M. A. Knus, A. Merkuriev, M. Rost et J.-P. Tignol ont donné une preuve encore différente ([KMRT], Proposition (18.24) page 293) d'un énoncé équivalent au Théorème 3. La torsion galoisienne de la forme triangulaire

$$(x_1, \ldots , x_n) \mapsto \sum_{1\leq i<j\leq n} x_i x_j \, ,$$

au moyen d'un élément $e_{E/F} \in H^1(G_F, \mathfrak{S}_n)$ est présente en filigrane, et le matériel utilisé est plus élémentaire que dans [Wat].

La preuve que nous donnons dans ce chapitre est l'objet de la section 2.1 ; elle présente des points communs avec celle de [KMRT] en ce qui concerne la stratégie générale, que nous allons essayer d'esquisser. Pour n pair, le groupe symétrique $\mathfrak{S}_n$ se plonge dans le groupe orthogonal $O_n(F_s, T)$ de la forme triangulaire ci-dessus. On en déduit une application

$$\phi : H^1(G_F, \mathfrak{S}_n) \longrightarrow H^1(G_F, O_n(F_s, T)) \, .$$

Ce dernier groupe est en bijection avec les classes d'isomorphismes de formes quadratiques non dégénérées sur F. On montre alors que si E/F est de degré pair $n = 2m$, la forme $\widetilde{T}_{E/F}$ est la tordue de la forme triangulaire ci-dessus au moyen d'un élément $e_{E/F} \in H^1(G_F, \mathfrak{S}_n)$ défini à conjugaison près (Théorème 2.1.20 page 53), et caractérisant E/F à isomorphisme près, ce qui signifie que

$$\widetilde{T}_{E/F} = \phi(e_{E/F}) \, .$$

Ce point est détaillé dans la sous-section 2.1.4. Or on dispose de l'invariant de Dickson, qui est un homomorphisme $\Delta : O_n(F_s, T) \to \mathbb{Z}/2\mathbb{Z}$ (voir sous-section 2.1.3). Comme cela est précisé dans la sous-section 2.1.5, on peut donc essayer de relier l'invariant de Arf de la forme $\widetilde{T}_{E/F}$ avec l'invariant de Dickson des éléments $e_{E/F}(\gamma) \in \mathfrak{S}_n \hookrightarrow O_n(F_s, T)$, $\gamma \in G_F$, et c'est en cela que notre preuve se distingue de celle que l'on trouve dans [KMRT].

Un autre aspect de ce chapitre est l'aspect algorithmique : étant donné $f \in F[X]$ irréductible séparable et $E \simeq F[X]/(f)$, comment calculer $d^+(E/F)$? Dans la section 2.2, on décrit trois méthodes pour y parvenir au moyen du système de calcul Maple (voir Appendices B et C). Nous avons ainsi pu refaire les calculs qui avaient été effectués par Bergé et Martinet en fin d'article, et pû confirmer la plupart des résultats qu'ils avaient donnés, sauf lorsque le polynôme f est de degré 5 (voir Remarque 2.2.6 page 63).

La section 2.3 fait le point sur l'existence éventuelle d'invariants dans le groupe $H^1(G_F, F_s^*/F_s^{*2})$. On y dégage l'argument intrinsèque qui a permis à Bergé et Martinet de montrer que l'invariant de Clifford de l'espace quadratique $(E', \widetilde{T}_{E'/F})$ est trivial (Proposition 2.3.6 page 67).

L'Appendice A est l'occasion de mettre en relief la structure de la démonstration du Théorème de Cartan-Dieudonné concernant les générateurs du groupe orthogonal en caractéristique 2, peu souvent reprise dans la littérature.

Enfin, en marge de ce travail, nous avons, au cours de l'étude de [BM], été amené à nous intéresser au pfaffien d'une matrice alternée. En relation avec cette notion, dans l'Appendice D, nous établissons une preuve du résultat suivant, dont on trouve un énoncé erroné dans la littérature.

Théorème 4 (Proposition D.1.2, page 88) *La formule de développement du pfaffien par rapport à une ligne est la suivante.*

$$\textit{Pour } 1 \leq i \leq n,\ P_f(Y) = \sum_{j=1}^{n} (-1)^{i+j-1} \epsilon(i,j) P_f(Y_{i;j}) Y_{i,j}\ ,\ \textit{avec}$$

$$\epsilon(i,j) = \begin{cases} 1 & si \quad i < j\,, \\ -1 & si \quad i > j\,, \\ 0 & si \quad i = j\,. \end{cases}$$

Chapitre 1

Classes caractéristiques de représentations galoisiennes

1.1 Le problème d'Atiyah et le théorème de Fulton-MacPherson

M. F. Atiyah a attaché des classes de Chern (resp. des classes de Stiefel-Whitney) aux représentations linéaires complexes (resp. réelles) de groupes finis ([Ati], Proposition 1.1, et Proposition 1.2 page 26) qui sont caractérisées par des propriétés formelles que nous rappellerons dans la sous-section 1.3.2. Il a mentionné que toutes ces classes de Chern pouvaient être calculées dès lors que l'on savait calculer celles de représentations induites.

L. Evens a défini un transfert "multiplicatif" en cohomologie des groupes dans ([Ev1], §5). Il l'utilise pour calculer les classes de Chern d'induites de représentations de *degré 1* ([Ev2], Théorème 4 page 188). Avec D. S. Kahn, il traite le cas d'induites de représentations par rapport à un sous-groupe normal d'indice premier ([EK], Théorème III page 317).

Fulton et MacPherson apportent une réponse au problème d'Atiyah, en le plaçant dans un cadre géométrique plus général, qui comprend trois situations : deux situations topologiques, et une situation algébrique. La première situation topologique concerne les classes de Stiefel-Whitney de fibrés vectoriels réels à valeurs dans la cohomologie singulière modulo 2. La deuxième situation topologique concerne les classes de Chern de fibrés vectoriels complexes à valeurs dans la cohomologie singulière entière paire. Enfin la situation algébrique concerne les classes de Chern de fibrés vectoriels algébriques, à valeurs dans l'anneau de Chow. Ils font la démonstration dans la situation algébrique, où l'on bénéficie de la théorie de l'intersection sur l'anneau de Chow et une construction du transfert multiplicatif au niveau des cycles. D'après ce qu'on a pu comprendre, sans vérifier tous les détails, ils donnent ensuite une construction du transfert multiplicatif, et invoquent la théorie des cocycles géometriques de Goresky ([Gor], Theorem 4.7 page 182) pour dire que leur démonstration demeure valide dans les situations topologiques.

Toutefois, dans la sous-section 1.1.3, nous énoncerons le théorème de Fulton-MacPherson en nous restreignant à la première situation topologique (dans le cas restreint plus particulier où le revêtement est un revêtement de degré fini de CW-complexes), qui est celle qui nous concerne en vue de la démonstration du théorème de Kahn.

Dans leur travail, ils montrent que leur transfert multiplicatif peut être identifié au transfert d'Evens, c'est pourquoi nous avons décidé de privilégier ici la terminologie de transfert d'Evens, dont nous rappelons, dans la sous-section 1.1.2, les propriétés qui sont nécessaires à la lecture de la section 1.3.

1.1.1 Revêtements auxiliaires

Soit $f : X \to Y$ un revêtement de degré n ([God], §2 pages 106 et suivantes) de CW-complexes. A partir de f et d'un foncteur F de la catégorie $\mathcal{S}_n$ des ensembles finis à n éléments dans la catégorie $\mathcal{S}_m$ des ensembles finis à m éléments (les morphismes étant les bijections), on construit un revêtement auxiliaire $f_F : X_F \to Y$, de la façon suivante.

Comme f est un revêtement de degré n, on a un recouvrement ouvert $(V_i)_{i\in I}$ de Y avec pour chaque $i \in I$ un ensemble fini S_i et un homéomorphisme (appelé trivialisation) $\phi_i : f^{-1}(V_i) \to V_i \times S_i$, ainsi que pour $i \neq j$ tels que $V_i \cap V_j \neq \emptyset$, des applications continues localement constantes

$$g_{j,i} : V_i \cap V_j \to \mathrm{Mor}(S_i, S_j)$$

telles que

$$\phi_j \phi_i^{-1}(x, s) = (x, g_{j,i}(x)(s)) \text{ pour } (x, s) \in (V_i \cap V_j) \times S_i\,,$$

et satisfaisant donc

$$g_{k,j}(x) \circ g_{j,i}(x) = g_{k,i}(x) \text{ pour } x \in V_i \cap V_j \cap V_k\,.$$

Maintenant, comme F est un foncteur, on en déduit des applications localement constantes

$$\begin{array}{rcl} g_{F\,j,i} : V_i \cap V_j & \to & \mathrm{Mor}(F(S_i), F(S_j)) \\ x & \mapsto & F\big(g_{j,i}(x)\big) \end{array}$$

telles que

$$g_{F\,k,j}(x) \circ g_{F\,j,i}(x) = g_{F\,k,i}(x) \text{ pour } x \in V_i \cap V_j \cap V_k\,.$$

Grâce à ([God], Théorème 5.1 page 115), cela assure l'existence d'un revêtement $f_F : X_F \to Y$, unique à isomorphisme près, ayant pour $i \in I$ des trivialisations

$$\phi_{F\,i} : {f_F}^{-1}(V_i) \to V_i \times F(S_i)$$

telles que

$$\phi_{Fj}\phi_{Fi}^{-1}(x,s) = (x, g_{Fj,i}(x)(s)) \text{ pour } (x,s) \in (V_i \cap V_j) \times F(S_i)\,.$$

Dans la suite, on va considérer deux foncteurs particuliers.

Le foncteur F_λ

Une *suite* $\lambda = (\lambda_1, \ldots, \lambda_n)$ est une suite finie d'entiers satisfaisant

$$\lambda_1 \geq \ldots \geq \lambda_n \geq 0\,.$$

Un *zéro-cycle de type λ sur* l'ensemble S (à n éléments) est une somme formelle

$$\sum_{s \in S} a_s \cdot s\,,$$

où l'ensemble $\{a_s, s \in S\}$ est en bijection avec l'ensemble $\{\lambda_i, 1 \leq i \leq n\}$. On peut ensuite définir le foncteur

$$\begin{array}{rcl} F_\lambda : \mathcal{S}_n & \to & \mathcal{S}_m \\ S & \mapsto & F_\lambda(S) = \{\text{zéro-cycles de type } \lambda \text{ sur } S\} \end{array},$$

où $m = \mathrm{Card}(F_\lambda(S))$ (qui ne dépend pas de S).

On note $f_\lambda : X_\lambda \to Y$ le revêtement associé.

Le foncteur $F_{\lambda,a}$

Ensuite, on écrit $a \in \lambda$ s'il existe $1 \leq i \leq n$ avec $\lambda_i = a$, et pour $a \in \lambda$, on peut définir le foncteur

$$\begin{array}{rcl} F_{\lambda,a} : \mathcal{S}_n & \to & \mathcal{S}_{m'} \\ S & \mapsto & F_{\lambda,a}(S) = \{(z = \sum_{s \in S} a_s.s, s_0),\ \text{avec} \\ & & z \text{ zéro-cycle de type } \lambda \text{ sur } S \text{ et } a_{s_0} = a\} \end{array},$$

où $m' = \mathrm{Card}(F_{\lambda,a}(S))$ (indépendant de S).

On note $f_{\lambda,a} : X_{\lambda,a} \to Y$ le revêtement associé.

Un diagramme

Pour chaque suite λ et chaque $a \in \lambda$, on a un diagramme commutatif de revêtements

$$\begin{tikzcd} X_{\lambda,a} \arrow[r, "\rho_{\lambda,a}"] \arrow[d, "\pi_{\lambda,a}"'] \arrow[dr, "f_{\lambda,a}"] & X \arrow[d, "f"] \\ X_\lambda \arrow[r, "f_\lambda"] & Y \end{tikzcd},$$

où la flèche $\rho_{\lambda,a}$ (resp. la flèche $\pi_{\lambda,a}$) est définie en considérant la transformation naturelle du foncteur F_λ dans le foncteur identité (resp. du foncteur $F_{\lambda,a}$ dans le foncteur F_λ) qui correspond à l'oubli du zéro-cycle (resp. à l'oubli du point distingué).

Il résulte de cela que $\pi_{X_{\lambda,a}}$ est un revêtement de degré $m_a(\lambda)$: le nombre d'occurrences de a dans la suite λ.

On est souvent amené, lors de démonstrations par dévissages (dont le principe est formalisé dans [FM2], Proposition 12.1 page 50), à considérer les constructions précédentes dans le cas où le revêtement f est de degré 2.

Exemple fondamental

Si $f : X \to Y$ est de degré 2, une suite λ est la donnée de deux entiers $\lambda_1 \geq \lambda_2 \geq 0$.

Si $\lambda_1 = \lambda_2$, il n'y a qu'un zéro-cycle de type λ, donc $f_\lambda : X_\lambda \to Y$ est simplement une identification, et si $a = \lambda_1 = \lambda_2$, $f_{\lambda,a} : X_\lambda \to Y$ est isomorphe à $f : X \to Y$.

Si $\lambda_1 \neq \lambda_2$, il y a deux zéro-cycles de type λ, et comme $m_{\lambda_i}(\lambda) = 1$ pour $i \in \{1, 2\}$, les revêtements π_{λ_i} pour $i \in \{1, 2\}$ sont triviaux.

1.1.2 Le transfert d'Evens

Rappelons d'abord que l'on note

$$H^*(X) := \bigoplus_{i \geq 0} H^i(X, \mathbb{Z}/2\mathbb{Z})$$

la somme directe des groupes de cohomologie singulière modulo 2 d'un espace X.

Pour un revêtement de degré fini $f : X \to Y$ de CW-complexes, Fulton et MacPherson ont construit un transfert multiplicatif en cohomologie singulière modulo 2 :

$$\mathcal{N}_f : H^*(X) \to H^*(Y)\,,$$

qui est une généralisation du transfert d'Evens.

Nous énumérons ci-après les propriétés de l'application $\mathcal{N}_f$ qui nous seront utiles.

Propriété 1.1.1 (MULTIPLICATIVITÉ, [FM2], Prop. 7.1 p. 30) *Soient $f : X \to Y$ un revêtement de degré n de CW-complexes, et $(x, y) \in H^*(X) \times H^*(X)$. Alors, dans $H^*(Y)$,*

$$\mathcal{N}_f(x \cdot y) = \mathcal{N}_f(x) \cdot \mathcal{N}_f(y)\,.$$

Propriété 1.1.2 (FONCTORIALITÉ, [FM2], Prop. 7.3 p. 30) *Soit $f : X \to Y$ et $g : Y' \to Y$ deux revêtements de degré fini n de CW-complexes tels que le diagramme*

$$\begin{tikzcd} X' \arrow[r, "g'"] \arrow[d, "f'"'] & X \arrow[d, "f"] \\ Y' \arrow[r, "g"'] & Y \end{tikzcd}$$

soit un carré fibré. Alors, pour $x \in H^*(X)$, on a

$$g^*(\mathcal{N}_f(x)) = \mathcal{N}_{f'}({g'}^*(x)) .$$

Propriété 1.1.3 (IDENTITÉ, [FM2], Prop. 7.4 p. 31) *Si f est l'identité, $\mathcal{N}_f$ est l'identité.*

Propriété 1.1.4 (UNION DISJOINTE, [FM2], Prop. 7.5 p. 31) *Soit $f : X \to Y$ un revêtement de degré fini de CW-complexes, où $X = \coprod_{k=1}^m X_k$ est réunion disjointe de CW-complexes. Pour $1 \le k \le m$, on note $i_k : X_k \to X$ l'inclusion, et $f_k : X_k \to Y$ la restriction de f à X_k. Alors pour $x \in H^*(X)$,*

$$\mathcal{N}_f(x) = \prod_{k=1}^m \mathcal{N}_{f_k}(i_k^*(x)) .$$

Propriété 1.1.5 (TRANSITIVITÉ, [FM2], Prop. 7.8 p. 33) *Soient $f : X \to Y$ et $g : Y \to Z$ deux revêtements de degrés finis de CW-complexes et $x \in H^*(X)$. Alors*

$$\mathcal{N}_{g\circ f}(x) = \mathcal{N}_g(\mathcal{N}_f(x)) .$$

Propriété 1.1.6 (FORMULE D'ADDITION, [FM2], Cor. 8.2 p. 34) *Soient $f : X \to Y$ un revêtement de degré n de CW-complexes et $r+1$ éléments de $H^*(X)$ notés $x, x_1, \ldots, x_r$ tels que $x = x_1 + \cdots + x_r$. Alors*

$$\mathcal{N}_f(x) = \sum_\lambda f_{\lambda *}(\chi_\lambda(x)) \text{ où } \chi_\lambda(x) := \prod_{a\in\lambda} \mathcal{N}_{\pi_{\lambda,a}}(\rho_{\lambda,a}^*(x_a)) ,$$

où, dans la somme ci-dessus, λ parcourt toutes les suites à n termes.

Ces propriétés ne caractérisent pas exactement le transfert $\mathcal{N}_f$. Pour obtenir une caractérisation axiomatique, il faut travailler en cohomologie relative (voir [FM2], Théorème 9.4 page 40), mais nous ne rentrerons pas ici dans ces détails.

Signalons également qu'une preuve algébrique de la formule d'addition a été ensuite donnée par D. Tambara ([Tam2], Proposition 4.1 page 1402).

1.1.3 Le théorème de Fulton-MacPherson

Dans la suite, $f : X \to Y$ désigne un revêtement de degré n de CW-complexes.

Si R est un fibré vectoriel *réel* sur X de rang r, pour $i \geq 0$, on note $w_i(R)$ les classes de Stiefel-Whitney de R, éléments de $H^i(X, \mathbb{Z}/2\mathbb{Z})$. On note

$$w(R) := \sum_{i \geq 0} w_i(R) \in H^*(X)\,,$$

la classe de Stiefel-Whitney totale de R. Les classes de Stiefel-Whitney jouissent des propriétés suivantes, qui les caractérisent de manière unique.

(i) Si R est un fibré vectoriel de rang r sur X, on a

$$w_i(R) = 0 \text{ pour } i > r \text{ et } w_0(R) = 1\,.$$

(ii) Si R est un fibré vectoriel sur X et $f : X' \to X$ une application continue, alors on a

$$w_i(f^*R) = f^*(w_i(R)) \text{ pour } i \geq 0\,.$$

(iii) Si R et R' sont des fibrés vectoriels sur X, alors on a

$$w(R \oplus R') = w(R) \cdot w(R')\,,$$

(iv) Si R est le fibré en droites canonique sur $\mathbb{RP}^1$, alors $w_1(R)$ est non nul.

Pour plus de détails, on peut consulter par exemple ([MiSt], §4 p. 37).

On note ensuite $f_*(R)$ l'*image directe* de R par f, c'est-à-dire le fibré vectoriel de rang nr dont les fibres sont définies par

$$\forall y \in Y,\ f_*R(y) := \bigoplus_{x \in f^{-1}(y)} R(x)\,.$$

Pour tout espace X, on note $\mathbf{1}_X^{\oplus r}$ le fibré vectoriel trivial de rang r sur X. On note $V := f_*(\mathbf{1}_X)$ et on définit aussi pour chaque suite λ :

$$V_\lambda := \bigoplus_{a \in \lambda} \pi_{\lambda,a_*}\left(\mathbf{1}_{X_{\lambda,a}}^{\oplus a}\right)\,.$$

On est maintenant en mesure d'énoncer le théorème.

Théorème 1.1.7 ([FM2], Théorème 5.1 et Formule 5.5) *Soient $f : X \to Y$ un revêtement de degré n de CW-complexes, et R un fibré vectoriel de rang r sur X. Alors on a (voir Propriété 1.1.6) :*

$$w(f_*R) = w(f_*\mathbf{1}_X)^r \left(\sum_\lambda f_{\lambda*}\left(w(V_\lambda)^{-1}.\chi_\lambda(w(R))\right)\right)\,, \tag{1.1}$$

ou de manière équivalente,

$$w(f_*R) = w(f_*\mathbf{1}_X)^r \left(\mathcal{N}_f(w(R)) + \sum_\lambda f_{\lambda *}\left((w(V_\lambda)^{-1} - 1).\chi_\lambda(w(R)) \right) \right) . \quad (1.2)$$

Dans la somme ci-dessus, λ parcourt l'ensemble

$$\{(\lambda_1, \ldots, \lambda_n) \in \mathbb{N}^n \,|\, r \geq \lambda_1 \geq \ldots \geq \lambda_n \geq 0\} .$$

Vue la formulation (1.2) du Théorème 1.1.7, on peut se demander ([FM2], Remarque 5.10 page 22) si l'on peut en déduire le théorème de Kahn (voir (3) page 8).

C'est la formule d'addition (Propriété 1.1.6) qui permet de passer de l'énoncé (1.1) à l'énoncé (1.2) dans le Théorème 1.1.7.

Remarque 1.1.8 *Dans ([Tam1], Théorème 2.4 page 10), D. Tambara a utilisé le Théorème 1.1.7 (dans la situation algébrique) pour calculer la classe de Chern totale de l'image directe multiplicative $\mathcal{N}_f(R)$ d'un fibré vectoriel R, qui est définie par la propriété que sa fibre en tout point $y \in Y$ est donnée par*

$$\mathcal{N}_f(R)(y) = \bigotimes_{x \in f^{-1}(y)} R(x) .$$

1.2 La conjecture de Segal et le théorème de Kozlowski

1.2.1 Introduction

En 1972, G. Segal (voir [Seg2]) s'est intéressé aux théories cohomologiques généralisées. Ce sont des théories cohomologiques qui satisfont à tous les axiomes de Eilenberg-Steenrod (voir [Bens] §2.5), excepté celui de la dimension. Ainsi à tout espace X est associée une collection $\{G^i(X, A_i), i \geq 0\}$ de groupes abéliens. Il a également montré que le groupe $G(X)$ des unités de l'anneau $H^{**}(X) = \prod_{i\geq 0} H^i(X, \mathbb{Z}/2\mathbb{Z})$ est le terme de degré 0 d'une théorie cohomologique généralisée ([Seg3], Proposition 1.1 page 289). Il en est de même de $\widetilde{KO}(X)$, la K-théorie réduite de X (construite sur les classes d'isomorphismes de fibrés vectoriels réels sur X). Segal avait posé la question suivante (voir [Seg3], (b) page 293).

La classe de Stiefel-Whitney totale $w : \widetilde{KO}(X) \to G(X)$ s'étend-elle en une transformation de théories cohomologiques généralisées?

D. S. Kahn et S. B. Priddy ont associé à chaque théorie cohomologique généralisée un transfert ([KP], Définition 1.4 page 982), et une transformation entre théories cohomologiques généralisées doit commuter aux transferts de ces dernières (voir [KP]). Or le transfert de la théorie cohomologique généralisée dont le terme de degré 0 est $\widetilde{KO}(X)$ (resp. est $G(X)$) n'est autre que l'image directe (resp. le transfert d'Evens) ([KP], Proposition 2.4 page 984 et [Bens], §4.1, Remarque, page 124), et l'on sait que le transfert d'Evens ne commute pas à la classe de Stiefel-Whitney totale. Segal demanda donc à A. Kozlowski de construire pour chaque revêtement de degré fini $f : X \to Y$ un transfert $\mathcal{N}_f^w : G(X) \to G(Y)$ qui commute à la classe de Stiefel-Whitney totale. C'est l'aboutissement de la série d'articles ([Koz1], [Koz2], [Koz3], [Koz4]), où il a aussi proposé d'introduire un transfert d'Evens *normalisé* (noté $\widetilde{\mathcal{N}}_f$), et a conjecturé l'égalité

$$\mathcal{N}_f^w \stackrel{?}{=} \widetilde{\mathcal{N}}_f \,. \tag{1.3}$$

La motivation pour introduire $\widetilde{\mathcal{N}}_f$, est qu'il permet d'obtenir un énoncé plus compact de la formule de Fulton-MacPherson (voir Théorème 1.2.5). Dans la suite, nous rappelons les caractéristiques du transfert de Kozlowski, nous apportons des précisions concernant la définition du transfert d'Evens normalisé, et nous démontrons enfin :

Théorème 1.2.1 *Soit $f : X \to Y$ un revêtement de CW-complexes de degré n, et R un fibré vectoriel sur X. Alors*

$$\widetilde{\mathcal{N}}_f(w(R)) = \mathcal{N}_f^w(w(R))\,.$$

Il faut préciser que la famille des $w(R)$, où R parcourt les classes d'isomorphismes de fibrés vectoriels réels sur X de rang fini, n'engendre pas $G(X)$ en général, comme on peut le constater dans ([GKT], §2) dans le cas où $X = BG$ est espace classifiant d'un groupe fini G.

Pour démontrer l'égalité (1.3) conjecturée par Kozlowski, il faut vérifier, pour le transfert $\widetilde{\mathcal{N}}_f$, les cinq propriétés axiomatiques qui caractérisent le transfert $\mathcal{N}_f^w$, qui sont données par le Théorème 1.2.2 que nous énonçons dans la sous-section 1.2.2. Les propriétés (i), (ii) (iv), et (v) résultent du travail de Fulton et MacPherson. Kozlowski mentionne que la propriété (iii) est plus difficile à établir. Dans la sous-section 1.2.3, nous l'avons fait dans deux cas particuliers (voir Théorème 1.2.8 et Théorème 1.2.9), et cela suffit pour établir le Théorème 1.2.1, par dévissages, ce que nous faisons dans la sous-section 1.2.4.

Nous tenons enfin à mentionner un bon guide traitant d'une partie des notions de topologie algébrique que nous avons mentionnées ci-dessus (et dans le détail desquelles nous ne sommes pas toujours rentré) : la "brève histoire de la topologie" de J. Dieudonné ([Die]), et tout particulièrement le paragraphe 18.

1.2.2 Le transfert de Kozlowski

Kozlowski démontre le théorème suivant.

Théorème 1.2.2 ([Koz4], Théorème 1.1 page 61) *Pour tout revêtement de degré fini de CW-complexes $f : X \to Y$, il existe un transfert $\mathcal{N}_f^w : G(X) \to G(Y)$ tel que le diagramme*

$$\begin{tikzcd} \widetilde{KO}(X) \arrow[r, "w"] \arrow[d, "f_*"'] & G(X) \arrow[d, "\mathcal{N}_f^w"] \\ \widetilde{KO}(Y) \arrow[r, "w"] & G(Y) \end{tikzcd}$$

soit commutatif (f_* désignant le transfert en K-théorie réduite). Ce transfert est caractérisé de manière unique par les propriétés suivantes.
(i) Si

$$\begin{tikzcd} X' \arrow[r, "g'"] \arrow[d, "f'"'] & X \arrow[d, "f"] \\ Y' \arrow[r, "g"] & Y \end{tikzcd}$$

est un carré fibré à homotopie près où g et g' sont des revêtements de degrés finis, on a

$$\mathcal{N}_{f'}^w \circ g'^* = g^* \circ \mathcal{N}_f^w \,.$$

(ii) Si $f = Id : X \to X$, $\mathcal{N}_f^w = Id : G(X) \to G(X)$.
(iii) Si $X \xrightarrow{f} Y \xrightarrow{g} Z$ est une composition de revêtements de degrés finis, alors

$$\mathcal{N}_{g \circ f}^w = \mathcal{N}_g^w \circ \mathcal{N}_f^w \,.$$

(iv) Si $f : X \to Y$ est une union disjointe de revêtements $X = X_1 \coprod X_2$, et si $x \in G(X)$, alors

$$\mathcal{N}_f^w(x) = \mathcal{N}_{f_1}^w(i_1^* x) \cdot \mathcal{N}_{f_2}^w(i_2^* x)$$

où $i_k : X_k \to X$ est l'inclusion, et f_k est la restriction de f à X_k pour $k \in \{1, 2\}$.
(v) Soit $f : X \to Y$ un revêtement de degré 2. Alors, en notant $t = w_1(f_*(\mathbf{1}_X))$,

$$\mathcal{N}_f^w \left(\sum_{i \geq 0} x_i \right) = \mathcal{N}_f \left(\sum_{i \geq 0} x_i \right) + \sum_{i \geq 0} \mathcal{N}_f(x_i)((1+t)^{-i} + 1) \,.$$

Il construit ainsi un transfert qui se comporte bien avec les classes de Stiefel-Whitney (voir le premier diagramme du Théorème 1.2.2).

1.2.3 Le transfert d'Evens normalisé

Nous apportons ci-après des précisions concernant la définition du transfert d'Evens normalisé telle qu'elle a été suggérée par les commentaires faisant suite à la Proposition 4.1 page 70 de [Koz4].

Définition 1.2.3 *Pour tout revêtement de degré fini $f : X \to Y$ de CW-complexes, il existe une unique application (appelée* TRANSFERT D'EVENS NORMALISÉ*)*

$$\widetilde{\mathcal{N}}_f : H^{**}(X) \longrightarrow H^{**}(Y)\,,$$

caractérisée par les deux axiomes suivants :
(i) Pour tout revêtement $g : X \to Y$ de CW-complexes de degré fini, et tout entier $i \geq 0$:

$$\forall x \in H^i(X),\ \widetilde{\mathcal{N}}_g(x) := w(g_*(\mathbf{1}_X))^{-i}\mathcal{N}_g(x)\,.$$

(ii) Pour $x = \sum_{i\geq 0} x_i$, avec $x_i \in H^i(X)$ pour tout entier $i \geq 0$,

$$\widetilde{\mathcal{N}}_f(x) = \sum_{\lambda} f_{\lambda *}\left(\prod_{a\in\lambda}\widetilde{\mathcal{N}}_{\pi_{\lambda,a}}(\rho^*_{\lambda,a}(x_a))\right)\,,$$

où la somme porte sur toutes les suites λ formées de n entiers tels que $\lambda_1 \geq \cdots \geq \lambda_n \geq 0$.

Remarque 1.2.4 *(i) Les notations de (ii) ci-dessus sont celles de la sous-section 1.1.3. Remarquons que la définition est bien fondée, car on somme une famille de séries sommables.*
(ii) Le transfert $\widetilde{\mathcal{N}}_f$ est donc défini sur $H^{**}(X)$, et bien que la comparaison avec le transfert $\mathcal{N}^w_f$ soit un problème qui se pose uniquement sur $G(X)$, l'étude de la propriété (iii) pour $\widetilde{\mathcal{N}}_f$ peut donc être faite sur $H^{**}(X)$.

La motivation pour introduire cette définition est qu'elle permet d'obtenir la reformulation suivante du théorème de Fulton-MacPherson (cf. [Koz4], Théorème 4.2 page 70), qui la rapproche de celle du théorème de Kahn.

Théorème 1.2.5 *Soit $f : X \to Y$ un revêtement de degré fini de CW-complexes. Soit R un fibré vectoriel réel de rang r. Alors*

$$w(f_*(R)) = w(f_*(\mathbf{1}_X))^r\widetilde{\mathcal{N}}_f(w(R))\,.$$

PREUVE : Puisque pour toute suite λ, on a

$$\begin{aligned} w(V_\lambda)^{-1}(w(R)) &= \left(\prod_{a\in\lambda} w(\pi_{\lambda,a_*}(\mathbf{1}^{\oplus a}_{X_{\lambda,a}}))\right)^{-1}\prod_{a\in\lambda}\mathcal{N}_{\pi_{\lambda,a}}(\rho^*_{\lambda,a}(w_a(R)))\,,\\ &= \prod_{a\in\lambda} w(\pi_{\lambda,a_*}(\mathbf{1}_{X_{\lambda,a}}))^{-a}\mathcal{N}_{\pi_{\lambda,a}}(\rho^*_{\lambda,a}(w_a(R)))\,,\\ &= \prod_{a\in\lambda}\widetilde{\mathcal{N}}_{\pi_{\lambda,a}}(\rho^*_{\lambda,a}(w_a(R))))\,,\end{aligned}$$

c'est une simple réécriture du Théorème de Fulton-MacPherson. ■

Nous allons donner quelques propriétés de l'application $\widetilde{\mathcal{N}}_f$. Pour cela, il est commode d'introduire une valuation sur l'anneau $H^{**}(X)$.

Définition 1.2.6 *L'anneau $H^{**}(X)$ est muni d'une valuation :*

$$\begin{array}{rcl} v : H^{**}(X) & \to & \mathbb{N} \cup \{\infty\} \\ x = \sum_{i \geq 0} x_i & \mapsto & \min\{i \geq 0 \,|\, x_i \neq 0\} \end{array} .$$

Cette valuation sert à justifier que certains énoncés de l'article de Fulton-MacPherson, qui sont vrais pour des éléments de $H^*(X) := H^*(X, \mathbb{Z}/2\mathbb{Z})$ (somme directe des groupes de cohomologies), le sont pour les éléments de $H^{**}(X)$ (produit direct des groupes de cohomologies), par passage à la limite pour la topologie définie pour v.

Lemme 1.2.7 *Soit $f : X \to Y$ un revêtement de degré fini n de CW-complexes. Alors $\widetilde{\mathcal{N}}_f$ est multiplicatif, c'est-à-dire :*

$$\forall (x, y) \in H^{**}(X) \times H^{**}(X),\ \widetilde{\mathcal{N}}_f(xy) = \widetilde{\mathcal{N}}_f(x)\widetilde{\mathcal{N}}_f(y) .$$

Preuve : Écrivons $x = \sum_{i \geq 0} x_i$ et $y = \sum_{i \geq 0} y_i$ avec $(x_i, y_i) \in H^i(X) \times H^i(X)$ pour tout entier $i \geq 0$. En imitant Fulton et MacPherson ([FM2], Définition 15.2, page 56), définissons

$$\begin{array}{rcl} f_\Delta : H^{**}(X) & \to & H^{**}(Y) \\ x = \sum_{i \geq 0} x_i & \mapsto & \sum_\lambda f_{\lambda *}\left(w(V_\lambda)^{-1} \chi_\lambda(x)\right) \end{array} .$$

En notant $|\lambda| := \lambda_1 + \cdots + \lambda_n$, on a $\chi_\lambda(x) \in H^{|\lambda|}(X_\lambda)$ pour toute suite λ et tout $x \in H^{**}(X)$. On en déduit facilement que

$$v(f_\Delta(x) - f_\Delta(y)) \geq v(x - y) \text{ pour tous } (x, y) \in H^{**}(X) \times H^{**}(X) .$$

Il suit de cela que f_Δ est continue sur $H^{**}(X)$. Elle est donc multiplicative, d'après ([FM2], Proposition 15.3 page 56). Or $\widetilde{\mathcal{N}}_f(x) = f_\Delta(x)$, donc le lemme est prouvé. ■

Les deux théorèmes suivants sont liés à l'étude de la propriété (iii) pour le transfert d'Evens normalisé.

Théorème 1.2.8 *Si $X \xrightarrow{f} Y \xrightarrow{g} Z$ est une composition de revêtements de degrés finis de CW-complexes, on a pour tout $i \geq 0$,*

$$\forall\, x \in H^i(X),\ \widetilde{\mathcal{N}}_{g \circ f}(x) = \widetilde{\mathcal{N}}_g(\widetilde{\mathcal{N}}_f(x)) .$$

Preuve : Comme $x \in H^i(X)$, on a par définition

$$\widetilde{\mathcal{N}}_{g\circ f}(x) = w((g\circ f)_*(\mathbf{1}_X))^{-i}\mathcal{N}_{g\circ f}(x)\,,$$

$$\widetilde{\mathcal{N}}_{g\circ f}(x) = w((g\circ f)_*(\mathbf{1}_X))^{-i}\mathcal{N}_g(\mathcal{N}_f(x)) \text{ par multiplicativité de } \mathcal{N}_f\,. \tag{1.4}$$

Comme $\mathcal{N}_f(x) \in H^{in}(Y)$ (on note n le degré du revêtement f), on a aussi

$$\widetilde{\mathcal{N}}_g(\mathcal{N}_f(x)) = w(g_*(\mathbf{1}_Y))^{-in}\mathcal{N}_g(\mathcal{N}_f(x))\,,$$

et on en tire

$$\mathcal{N}_g(\mathcal{N}_f(x)) = w(g_*(\mathbf{1}_Y))^{in}\widetilde{\mathcal{N}}_g(\mathcal{N}_f(x))\,. \tag{1.5}$$

On porte maintenant (1.5) dans (1.4), ce qui donne

$$\widetilde{\mathcal{N}}_{g\circ f}(x) = w((g\circ f)_*(\mathbf{1}_X))^{-i}w(g_*\mathbf{1}_Y)^{ni}\widetilde{\mathcal{N}}_g(\mathcal{N}_f(x))\,. \tag{1.6}$$

On applique alors la formule de Fulton-MacPherson au fibré $f_*\mathbf{1}_X$ de rang n sur Y et au revêtement $g : Y \to Z$, pour écrire

$$w(g_*(f_*\mathbf{1}_X)) = w(g_*\mathbf{1}_Y)^n\widetilde{\mathcal{N}}_g(w(f_*\mathbf{1}_X))\,. \tag{1.7}$$

On reporte (1.7) dans (1.6), ce qui donne

$$\begin{aligned}\widetilde{\mathcal{N}}_{g\circ f}(x) &= w(g_*\mathbf{1}_Y)^{-ni}\widetilde{\mathcal{N}}_g(w(f_*\mathbf{1}_X))^{-i}w(g_*\mathbf{1}_Y)^{ni}\widetilde{\mathcal{N}}_g(\mathcal{N}_f(x))\\ &= \widetilde{\mathcal{N}}_g(w(f_*\mathbf{1}_X))^{-i}\widetilde{\mathcal{N}}_g(\mathcal{N}_f(x))\,,\end{aligned}$$

et la multiplicativité de $\widetilde{\mathcal{N}}_g$, résultant de la Proposition 15.3 de [FM2] permet d'obtenir la formule souhaitée. ■

Une méthode sensiblement identique permet d'obtenir :

Théorème 1.2.9 *Soit $f : X \to Y$ un revêtement de degré n de CW-complexes, $g : Y \to Z$ un revêtement de degré m de CW-complexes, et R un fibré vectoriel de rang r sur X. Alors*

$$\widetilde{\mathcal{N}}_g(\widetilde{\mathcal{N}}_f(w(R))) = \widetilde{\mathcal{N}}_{g\circ f}(w(R))\,.$$

Preuve : On applique une première fois la formule de Fulton-MacPherson au fibré f_*R et au revêtement g, pour obtenir

$$w(g_*(f_*R)) = w(g_*\mathbf{1}_Y)^{rn}\widetilde{\mathcal{N}}_g(w(f_*R))\,. \tag{1.8}$$

On applique une seconde fois la formule de Fulton-MacPherson au fibré R et au revêtement $g \circ f$, pour obtenir

$$w((g \circ f)_* R) = w((g \circ f)_* \mathbf{1}_X)^r \widetilde{\mathcal{N}}_{g\circ f}(w(R)) \,. \tag{1.9}$$

En utilisant le fait que $(g \circ f)_* R \simeq g_*(f_* R)$, on peut égaler les deux membres de (1.8) et (1.9), d'où

$$w(g_* \mathbf{1}_Y)^{rn} \widetilde{\mathcal{N}}_g(w(f_* R)) = w((g \circ f)_* \mathbf{1}_X)^r \widetilde{\mathcal{N}}_{g\circ f}(w(R)) \,. \tag{1.10}$$

Maintenant, on applique une troisième fois la formule de Fulton-MacPherson au fibré R et au revêtement f, pour obtenir

$$w(f_* R) = w(f_* \mathbf{1}_X)^r \widetilde{\mathcal{N}}_f(w(R)) \,.$$

On porte cette dernière expression dans (1.10), et en utilisant la multiplicativité de $\widetilde{\mathcal{N}}_g$, on obtient

$$w(g_* \mathbf{1}_Y)^{rn} \widetilde{\mathcal{N}}_g(w(f_* \mathbf{1}_X))^r \widetilde{\mathcal{N}}_g(\widetilde{\mathcal{N}}_f(w(R))) = w(g_*(f_* \mathbf{1}_X))^r \widetilde{\mathcal{N}}_{g\circ f}(w(R)) \,. \tag{1.11}$$

Or, en appliquant une quatrième fois la formule de Fulton-MacPherson au fibré $f_* \mathbf{1}_X$ et au revêtement g, on obtient

$$w(g_*(f_* \mathbf{1}_X)) = w(g_* \mathbf{1}_Y)^n \widetilde{\mathcal{N}}_g(w(f_* \mathbf{1}_X)) \,.$$

En portant ceci dans (1.11) et en simplifiant, on obtient :

$$\widetilde{\mathcal{N}}_g(\widetilde{\mathcal{N}}_f(w(R))) = \widetilde{\mathcal{N}}_{g\circ f}(w(R)) \,,$$

ce qu'on voulait. ■

1.2.4 Egalité des transferts sur les classes de Stiefel-Whitney

Comme annoncé antérieurement, nous démontrons maintenant le Théorème 1.2.1 par dévissages.

Lemme 1.2.10 *Soit $f : X \to Y$ un revêtement de CW-complexes de degré 2. Alors pour tout $x \in H^{**}(X)$,*

$$\mathcal{N}_f^w(x) = \widetilde{\mathcal{N}}_f(x) \,.$$

Preuve : Puisque le revêtement f est de degré 2, pour les suites $\lambda = (\lambda_1, \lambda_2)$ telles que $\lambda_1 = \lambda_2 = i$ pour $i \geq 0$ (Exemple fondamental, page 16), on sait que pour $a \in \lambda$, on a $X_\lambda = Y$, $f_\lambda = Id_Y$, $X_{\lambda,a} = X$, $\rho_{\lambda,a} = Id_X$, et $\pi_{\lambda,a} = f$. Pour les autres, les revêtements $\pi_{\lambda,a}$ sont triviaux. Il suit de ces remarques que :

$$\widetilde{\mathcal{N}}_f(x) \;=\; \sum_{i=0}^{+\infty}(1+t)^{-i}\mathcal{N}_f(x_i) + \sum_{\lambda_1>\lambda_2} f_{\lambda *}(\chi_\lambda(x)) \,,$$

où $t := w_1(f_*(\mathbf{1}_X))$. D'autre part (Théorème 1.2.2, (v)) :

$$\mathcal{N}_f^w(\sum_{i=0}^{\infty} x_i) = \mathcal{N}_f(\sum_{i=0}^{\infty} x_i) + \sum_{i=0}^{\infty}\mathcal{N}_f(x_i)((1+t)^{-i}+1)\,.$$

Il s'agit donc de justifier que

$$\mathcal{N}_f(\sum_{i=0}^{\infty} x_i) = \sum_{i=0}^{+\infty}\mathcal{N}_f(x_i) + \sum_{\lambda_1>\lambda_2} f_{\lambda *}(\chi_\lambda(x))\,.$$

Cela se fait en appliquant, pour tout entier $r \geq 1$, la formule d'addition

$$\mathcal{N}_f(\sum_{i=0}^{r} x_i) = \sum_{i=0}^{r}\mathcal{N}_f(x_i) + \sum_{r\geq\lambda_1>\lambda_2} f_{\lambda *}(\chi_\lambda(x))\,,$$

et en passant à la limite sur r. ■

Lemme 1.2.11 *Soit $m \geq 1$ un entier, et*

$$X_1 \xrightarrow{f_1} X_2 \xrightarrow{f_2} \cdots \longrightarrow X_i \xrightarrow{f_i} X_{i+1} \xrightarrow{f_{i+1}} \cdots \longrightarrow X_m \xrightarrow{f_m} Y$$

une suite de revêtements de CW-complexes de degré 2. Alors pour tout fibré vectoriel R de rang r sur X_1,

$$\widetilde{\mathcal{N}}_{f_m\circ\cdots\circ f_1}(w(R)) = \mathcal{N}^w_{f_m\circ\cdots\circ f_1}(w(R))\,.$$

Preuve : On raisonne par récurrence sur m. Si $m = 1$, on utilise le lemme précédent. Sinon, on pose $f := f_{m-1}\circ\cdots\circ f_1$, et l'on a alors

$$\begin{aligned}\widetilde{\mathcal{N}}_{f_m\circ f}(w(R)) &= \widetilde{\mathcal{N}}_{f_m}(\widetilde{\mathcal{N}}_f(w(R))) \text{ (Théorème 1.2.9)}\,,\\ &= \mathcal{N}^w_{f_m}(\mathcal{N}^w_f(w(R))) \text{ (lemme précédent et récurrence)}\,,\\ &= \mathcal{N}^w_{f_m\circ f}(w(R))\end{aligned}$$

grâce la transivité du transfert de Kozlowski, ce qui achève la preuve. ■

Lemme 1.2.12 *Soient $f : X \to Y$ un revêtement de CW-complexes, où $X = \coprod_{k=1}^m X_k$ est réunion disjointe de CW-complexes. Pour $1 \leq k \leq m$, on note $i_k : X_k \to X$ l'inclusion, et $f_k : X_k \to Y$ la restriction de f à X_k. Alors, pour tout fibré vectoriel R de rang r sur X,*

$$\widetilde{\mathcal{N}}_f(w(R)) = \prod_{k=1}^{m}\widetilde{\mathcal{N}}_{f_k}(i_k^*(w(R)))\,.$$

Preuve : La formule de Fulton-MacPherson donne les égalités

$$w(f_*(R)) = w(f_*(\mathbf{1}_X))^r \widetilde{\mathcal{N}}_f(w(R)) \text{ et}$$

$$w(f_{k*}(i_k^*(R))) = w(f_{k*}(\mathbf{1}_{X_k}))^r \widetilde{\mathcal{N}}_{f_k}(w(i_k^*(R))) \text{ pour } 1 \leq k \leq m\,.$$

En utilisant l'isomorphisme $f_*R \simeq \oplus_{k=1}^m f_{k*}(i_k^*(R))$ pour tout fibré vectoriel R sur X, on obtient

$$w(f_*(R)) = \prod_{k=1}^m w(f_{k*}(i_k^*(R))) \text{ et } w(f_*(\mathbf{1}_X))^r = \prod_{k=1}^m w(f_{k*}(\mathbf{1}_{X_k}))^r\,,$$

de sorte que

$$\widetilde{\mathcal{N}}_f(w(R)) = \prod_{k=1}^m \widetilde{\mathcal{N}}_{f_k}(i_k^*(w(R)))\,,$$

ce qu'on voulait, puisque i_k^* commute avec w. ■

On peut maintenant prouver le Théorème 1.2.1, à l'aide de dévissages. Explicitement, il existe ([FM2], §12) un changement de base $g : Y' \to Y$ avec $g^* : H^{**}(Y) \to H^{**}(X)$ injectif tel que le carré

$$\begin{array}{ccc} X' & \xrightarrow{g'} & X \\ {\scriptstyle f'}\downarrow & & \downarrow{\scriptstyle f} \\ Y' & \xrightarrow{g} & Y\,, \end{array}$$

soit un carré fibré, avec la propriété que $f' : X' \to Y'$ soit union disjointe de revêtements qui sont des homéomorphismes ou des compositions de revêtements de degré 2. Dans ces conditions, grâce au Lemme 1.2.11 et au Lemme 1.2.12, on peut écrire :

$$\begin{aligned} g^*(\widetilde{\mathcal{N}}_f(w(R))) = \widetilde{\mathcal{N}}_{f'}(g'^*(w(R))) &= \\ \widetilde{\mathcal{N}}_{f'}(w(g'^*(R))) &= \mathcal{N}_{f'}^w(w(g'^*(R))) = \mathcal{N}_{f'}^w(g'^*(w(R)))\,. \end{aligned}$$

D'après (Théorème 1.2.2, (i)), on a $\mathcal{N}_f^w(g'^*(w(R))) = g^*(\mathcal{N}_f^w(w(R)))$. L'injectivité de g^* permet enfin de conclure $\widetilde{\mathcal{N}}_f(w(R)) = \mathcal{N}_f^w(w(R))$. ■

1.3 Relation avec le théorème de Kahn

Nous utilisons maintenant tout le travail accompli ci-dessus pour mettre en relation les deux formules mentionnées dans l'introduction (voir page 8).

Théorème 1.3.1 *La formule de Kahn (3) s'obtient à partir de la formule de Fulton-MacPherson (4) par inflation à la cohomologie galoisienne.*

1.3.1 Les idées

Nous commençons, par donner un aperçu de l'enchaînement d'idées qui permettent le relier le théorème de Kahn au théorème de Fulton-MacPherson, puis nous serons plus précis dans les sections suivantes.

Etape 1 : Inflation de la formule de Fulton-MacPherson

Soit E/F une extension finie séparable de corps commutatifs de caractéristique différente de 2, G_E le groupe de Galois absolu de F et $\rho : G_E \to Gl(V)$ une représentation galoisienne réelle de degré r.
On choisit une extension galoisienne finie L/F telle que $E \subset L$ et ρ se factorise à travers $\rho_L : \mathrm{Gal}(L/E) \to Gl(V)$, représentation qui correspond à un fibré vectoriel réel $\xi_L(\rho)$ sur l'espace classifiant $B\,\mathrm{Gal}(L/E)$. On a alors

$$w(\rho) = \inf_{\mathrm{Gal}(L/E),G_E}(w(\xi_L(\rho)))\,.$$

On applique la formule de Fulton-MacPherson au fibré $\xi_L(\rho)$ et au revêtement de CW-complexes $f_L : X \overset{not}{=} B\,\mathrm{Gal}(L/E) \to B\,\mathrm{Gal}(L/F)$. On obtient alors

$$w(f_{L*}(\xi_L(\rho))) = w(f_{L*}(\mathbf{1}_X))^r \sum_\lambda f_{\lambda *}\left(w([f_{L*}(\mathbf{1}_X)]_\lambda)^{-1}.\chi_\lambda(w(\xi_L(\rho)))\right)\,,$$

La difficulté est de calculer l'image par $\inf_{\mathrm{Gal}(L/F),G_F}$ de la somme ci-dessus et de voir qu'elle vaut $\mathcal{N}_{E/F}(w(\rho))$.

Etape 2 : Utilisation du transfert de Kozlowski

La formule de Fulton-MacPherson exprime que le transfert d'Evens $\mathcal{N}_f$ se comporte mal avec les classes de Stiefel-Whitney. Mais le transfert de Kozlowski $\mathcal{N}_f^w$ se comporte bien avec elles (premier diagramme du Théorème 1.2.2). On peut alors écrire

$$w(f_{L*}(\xi_L(\rho))) = w(f_{L*}(\mathbf{1}_X))^r \mathcal{N}_{f_L}^w(w(\xi_L(\rho)))\,.$$

Comme les classes de Stiefel-Whitney totales sont inversibles dans $H^{**}(Y)$, en notant $Y = B\,\mathrm{Gal}\,(L/F)$, cette égalité jointe à la précédente dit que

$$\sum_\lambda f_{\lambda *}\left(w([f_{L*}(\mathbf{1}_X)]_\lambda)^{-1}.\chi_\lambda(w(\xi_L(\rho)))\right) = \mathcal{N}_{f_L}^w(w(\xi_L(\rho)))\,,$$

terme dont on sait qu'il s'inflate sur $\mathcal{N}_{E/F}^w(w(\rho))$ (voir [Sn], Chap. 4, §2).

Etape 3 : Les transferts $\mathcal{N}_{E/F}^w$ et $\mathcal{N}_{E/F}$ coïncident sur les unités de $H^{**}(G_F)$

Comme observé par Kozlowski ([Koz5], §2) cela résulte de la conjecture de Milnor (cf. [Ka2], [Mor]), démontrée par Voevodsky ou du fait que les classes de

Stiefel-Whitney totales de représentations galoisiennes sont décomposables (i. e. sommes de cup-produits de termes de degré 1) résultat établi par Kahn ([Ka1], Théorème 4 page 247), argument auquel il faut joindre une formule explicite ([Ka1], Proposition II.1.4) pour calculer $\mathcal{N}_{E/F}(a)$, avec E/F quadratique et $a \in H^1(G_E)$, dont la preuve utilise la formule de Serre qui a été mentionnée dans l'introduction.

Nous revenons maintenant sur les étapes ci-dessus.

1.3.2 Des extensions aux revêtements et des représentations aux fibrés vectoriels via les espaces classifiants

A propos des espaces classifiants

Etant donné un groupe topologique G, on peut se poser le problème de classer les G-fibrés principaux sur une base X ayant certaines propriétés, et on obtient un espace, noté BG, appelé espace classifiant du groupe G, qui n'est défini qu'à homotopie près, et on fait alors le choix d'un modèle pour un tel espace. En 1968, Segal a donné ([Seg1]) une construction très générale utilisant les techniques simpliciales, que nous allons décrire ici. Pour cela, on rappelle d'abord quelques définitions classiques.

Définition 1.3.2 *Un* OBJET SIMPLICIAL D'UNE CATÉGORIE $\mathbf{C}$ *un foncteur contravariant $A : Ord \to \mathbf{C}$, où Ord est la catégorie dont les objets sont les ensembles finis totalement ordonnés, dont les morphismes sont les applications croissantes.*

Définition 1.3.3 *La* RÉALISATION GÉOMÉTRIQUE D'UN ENSEMBLE SIMPLICIAL *A est un espace topologique $\Delta(A)$ ainsi construit. Pour un ensemble fini S, on note $\Delta(S)$ le simplexe standard dont S est l'ensemble des sommets. Alors*

$$\Delta(A) := \frac{\coprod_{S \in \mathrm{Ob}(Ord)} \Delta(S) \times A(S)}{\sim},$$

où $\sim$ est la relation d'équivalence engendrée par les relations

$$\big(x, A(\theta)(a)\big) \sim \big(\Delta(\theta)(x), a\big), \text{ pour } x \in \Delta(S), a \in \Delta(T), \text{ et } \theta : S \to T\,.$$

Définition 1.3.4 *La* CATÉGORIE ASSOCIÉ À UN OBJET S DE Ord *est la catégorie, encore notée S, qui a pour objets les éléments de S, et qui est telle que pour $(x, y) \in S^2$, $\mathrm{Mor}(x, y)$ est réduit à un élément lorsque $x \leq y$ et vide sinon.*

Définition 1.3.5 *Le* NERF D'UNE CATÉGORIE $\mathbf{C}$ *est l'ensemble simplicial, noté $N(\mathbf{C})$, et défini par*

$$N(\mathbf{C})(S) := Func(S, \mathbf{C})\,,$$

où $Func(S, \mathbf{C})$ désigne l'ensemble des foncteurs contravariants de S dans $\mathbf{C}$.

Définition 1.3.6 *Une catégorie* $\mathbf{C}$ *est une* CATÉGORIE TOPOLOGIQUE *si les collections* $\mathrm{Ob}(\mathbf{C})$ *et* $\mathrm{Mor}(\mathbf{C})$ *des objets et des morphismes de* $\mathbf{C}$ *sont des ensembles, qui sont munis de topologies telles que les quatre applications*

$$\begin{array}{rccc} \textit{Source}: & \mathrm{Mor}(\mathbf{C}) & \to & \mathrm{Ob}(\mathbf{C}) \\ \textit{But}: & \mathrm{Mor}(\mathbf{C}) & \to & \mathrm{Ob}(\mathbf{C}) \\ \textit{Identité}: & \mathrm{Ob}(\mathbf{C}) & \to & \mathrm{Mor}(\mathbf{C}) \\ \textit{Composition}: & \mathrm{Mor}(\mathbf{C}) \times_{\mathrm{Ob}(\mathbf{C})} \mathrm{Mor}(\mathbf{C}) & \to & \mathrm{Mor}(\mathbf{C}) \end{array}$$

soient continues.

Définition 1.3.7 *La* CATÉGORIE $\overline{\mathbf{G}}$ *d'un groupe topologique* G *est la catégorie qui a pour objets les éléments de* G*, et dans laquelle il y a un isomorphisme unique entre chaque paire d'éléments de* G*.*

Définition 1.3.8 *La* CATÉGORIE $\mathbf{G}$ *d'un groupe topologique* G *est la catégorie qui a un seul objet, dont les isomorphismes se composent comme les éléments de* G*.*

Définition 1.3.9 *Le* FONCTEUR $\overline{\mathbf{G}} \to \mathbf{G}$ *envoie le morphisme* (g_1, g_2) *de* $\overline{\mathbf{G}}$ *sur le morphisme* $g_1^{-1}g_2$ *de* $\mathbf{G}$*.*

Cela dit, on peut maintenant définir (le modèle simplicial de) l'espace classifiant d'un groupe.

Définition 1.3.10 *L'espace classifiant d'une catégorie* $\mathbf{C}$ *est la realisation géométrique de l'ensemble simplicial* $N\mathbf{C}$ *; l'espace classifiant d'un groupe topologique* G *est l'espace classifiant de la catégorie* $\mathbf{G}$*. On le note* BG*.*

Proposition 1.3.11 *Le modèle simplicial de l'espace classifiant fournit un foncteur* B *de la catégorie des groupes topologiques dans la catégorie des espaces topologiques et applications continues.*

Proposition 1.3.12 *Si* G *est un groupe fini, alors*
(i) Les espaces $B\overline{\mathbf{G}}$ *et* BG *sont des CW-complexes,*
(ii) Il y a une fibration $B\overline{\mathbf{G}} \to BG$ *localement triviale,*
(iii) L'espace $B\overline{\mathbf{G}}$ *est contractile.*

PREUVE : (i) En effet pour tout objet S de Ord, les ensembles $N\overline{\mathbf{G}}(S)$ et $N\mathbf{G}(S)$ sont finis donc discrets, donc les réalisations géométriques des ensembles simpliciaux $N\overline{\mathbf{G}}$ et $N\mathbf{G}$ sont des CW-complexes, d'après ([LuWe], Théorème 4.6 page 91).
(ii) On a en effet une application continue régulière (i. e. qui envoie une cellule dans une cellule) et cellulaire (i. e. qui envoie les squelettes dans les squelettes) (voir [LuWe], III, Théorèmes 4.7 et 4.8 page 92) $B\overline{\mathbf{G}} \to BG$ induite par le foncteur

$\overline{\mathbf{G}} \to \mathbf{G}$ qui envoie le morphisme (g_1, g_2) de $\overline{\mathbf{G}}$ sur le morphisme $g_1^{-1}g_2$ de $\mathbf{G}$. Le groupe G est étant fini, muni de la topologie discrète, c'est un CW-complexe fini, donc un rétracte absolu de voisinage ([Bre], Corollaire E.8 page 540), et cela suffit pour conclure, d'après [Seg1].
(iii) En effet, la catégorie $\overline{\mathbf{G}}$ est équivalente à la catégorie à un objet et un morphisme, donc les espaces classifiants de ces deux catégories sont homotopes d'après ([Seg1], Proposition 2.1 page 106). ∎

Notation 1.3.13 *Si G est un groupe fini, on note $EG := B\overline{\mathbf{G}}$.*

Proposition 1.3.14 *Si G est un groupe fini, alors*
(i) Les espaces EG/G et BG sont homéomorphes,
(ii) L'espace EG est localement compact.

Preuve : (i) L'action de G sur lui-même par translations induit une structure de G-ensemble simplicial sur le nerf $N\overline{\mathbf{G}}$, et comme ensembles simpliciaux, $N\overline{\mathbf{G}}/G \simeq N\mathbf{G}$. Plus précisément, pour tout $S \in \mathrm{Ob}(Ord)$, on a une action de G sur $N\overline{\mathbf{G}}$ définie par

$$\begin{array}{ccccc} G & \times & N\overline{\mathbf{G}} & \to & N\overline{\mathbf{G}} \\ (g & , & F) & \mapsto & gF : \left\{ \begin{array}{l} (gF)(s) = gF(s) \text{ pour } s \in \mathrm{Ob}(S)\,, \\ (gF)(s \mapsto s') = \big(gF(s), gF(s')\big)\,. \end{array} \right. \end{array}$$

Cela permet de définir une application

$$\begin{array}{rcl} \overline{\alpha}(S) : N\overline{\mathbf{G}} & \to & N\mathbf{G} \\ F & \mapsto & \overline{\alpha}(S)(F) : (s \mapsto s') \mapsto F(s)^{-1}F(s')\,, \end{array}$$

qui se factorise en une application $\alpha(S) : N\overline{\mathbf{G}}(S)/G \to N\mathbf{G}(S)$, laquelle définit une transformation naturelle $\alpha : N\overline{\mathbf{G}}/G \to N\mathbf{G}$ qui est un isomorphisme, car on peut définir une transformation naturelle inverse β, en considérant pour tout $S \in \mathrm{Ob}(Ord)$ l'application qui suit (s_0 et le minimum de S)

$$\begin{array}{rcl} \beta(S) : N\mathbf{G}(S) & \to & N\overline{\mathbf{G}}(S)/G \\ F & \mapsto & \beta(S)(F) : \left\{ \begin{array}{l} \beta(S)(F)(s) = F(s_0 \mapsto s) \text{ pour } s \in S\,, \\ \beta(S)(F)(s \mapsto s') = \big(F(s_0 \mapsto s), F(s_0 \mapsto s')\big) \end{array} \right. \end{array}$$

Ainsi $BG = \Delta(N\mathbf{G})$ est homéomorphe à $\Delta(N\overline{\mathbf{G}}/G)$. Comme la réalisation géométrique commute au quotient par G ([LuWe], III, Prop. 5.6 page 98), l'espace $\Delta(N\overline{\mathbf{G}}/G)$ est homéomorphe à $\Delta(N\overline{\mathbf{G}})/G = EG/G$.

(ii) Chaque classe c de EG est représenté modulo $\sim$ par un élément de $(x_S, a_S) \in \Delta(S) \times N\overline{\mathbf{G}}(S)$ avec S ensemble fini totalement ordonné. Si n est le cardinal de S, et $[n] := \{i \in \mathbb{N}, 0 \le i \le n\}$, alors S est isomorphe à $[n-1]$ dans Ord donc (x_S, a_S) est équivalent à unique élément $(x_{[n-1]}, a_{[n-1]}) \in \Delta([n-1]) \times N\overline{\mathbf{G}}([n-1])$, lui-même equivalent à un point $(x_{[k]}, a_{[k]}) \in \Delta([k]) \times N\overline{\mathbf{G}}([k])$

unique avec $x_{[k]}$ point intérieur de $\Delta([k])$ et $a_{[k]}$ simplexe non dégénéré ([LuWe], Lemme 4.1 page 89). L'image dans EG de $\Delta([k]) \times \{x_{[k]}\}$ est un compact, qui contient l'image de $\mathrm{Int}(\Delta([k])) \times \{x_{[k]}\}$ qui est un ouvert qui contient c. ■

Proposition 1.3.15 *Soit G un groupe fini, et H un sous-groupe d'indice n. Si $i : H \to G$ est l'inclusion, alors l'application $Bi : BH \to BG$ est homotope à un revêtement de degré n.*

PREUVE : On a en effet le diagramme suivant :

$$\begin{tikzcd} & EG/H \arrow[dr] & \\ EH/H \arrow[ur] \arrow[rr] \arrow[d] & & EG/G \arrow[d] \\ BH \arrow[rr, "Bi"'] & & BG \end{tikzcd},$$

où les flèches verticales sont des homéomorphismes. La flèche $EG/H \to EG/G$ est un revêtement de degré n, car puisque EG est un CW-complexe, il est localement connexe, et les deux quotients sont séparés. C'est suffisant d'après ([God], Proposition 3.4 page 111), car puisque le groupe G est fini, il opère proprement EG (dans le sens où, pour tout compact K de EG, l'ensemble des éléments de G tels que $gK \cap K \neq \emptyset$ est relativement compact dans G) et librement sur EG (pour tout point $x \in EG$, le stabilisateur de x sous G est trivial). ■

Théorème 1.3.16 *Soit G un groupe fini, il y a alors des isomorphismes naturels*

$$\begin{array}{rcl} H_*(G, \mathbb{Z}/2\mathbb{Z}) & \xrightarrow{\simeq} & H_*(BG, \mathbb{Z}/2\mathbb{Z}), \\ H^*(G, \mathbb{Z}/2\mathbb{Z}) & \xrightarrow{\simeq} & H^*(BG, \mathbb{Z}/2\mathbb{Z}), \end{array}$$

les membres de gauche désignant la (co)homologie modulo 2 du groupe G et les membres de droite désignant la (co)homologie singulière modulo 2 de l'espace BG.

PREUVE : On s'inspire de ([Ros], Prop. 5.1.27, p. 263) et ([Wei], Th. 6.10.5 p. 204). La preuve de la Proposition 5.1.27 de [Ros] utilise le complexe des chaînes cellulaires, cependant que celle du Théorème 6.10.5 de [Wei] utilise le complexe des chaînes singulières de EG, en commençant par montrer le Lemme 1.3.17 ci-après, et les égalités

$$\begin{array}{rcl} \mathrm{Hom}_{\mathbb{Z}/2\mathbb{Z}G}(S_*(EG), \mathbb{Z}/2\mathbb{Z}) & = & \mathrm{Hom}_{\mathbf{Ab}}(S_*(EG)_G, \mathbb{Z}/2\mathbb{Z}) \\ & = & \mathrm{Hom}_{\mathbf{Ab}}(S_*(BG), \mathbb{Z}/2\mathbb{Z}), \end{array}$$

dont le théorème résulte. Pour pouvoir appliquer le Lemme 1.3.17, il faut observer que puisque EG est localement compact, le groupe G, fini, opère proprement sur EG ([God], Proposition 6.9 page 29) au sens donné dans le Lemme 1.3.17. ■

Lemme 1.3.17 *Si G opère proprement sur X (dans le sens où pour tout point de $x \in X$, il existe un ouvert U de X contenant x tel que les translatés gU soient disjoints de U dès que $g \neq 1$), et si $S_*(X)$ désigne le complexe des $\mathbb{Z}/2\mathbb{Z}$-modules libres sur les simplexes singuliers de X, alors $S_*(X)$ est un complexe de chaînes de $\mathbb{Z}/2\mathbb{Z}[G]$-modules libres, et $S_*(X)_G = S_*(X) \otimes_{\mathbb{Z}/2\mathbb{Z}[G]} \mathbb{Z}/2\mathbb{Z}$ est le complexe singulier de X/G.*

Preuve : On copie la preuve ([Wei], Lemme 6.10.2 page 204) en remplaçant $\mathbb{Z}$ par $\mathbb{Z}/2\mathbb{Z}$. Explicitement, notons $\mathcal{B}_n$ l'ensemble des applications continues $\sigma : \Delta_n \to X$. Le groupe G agit sur $\mathcal{B}_n$, l'action étant définie en associant à $(g, \sigma) \in G \times \mathcal{B}_n$ l'élément $g\sigma$ désignant la composition de σ et de la translation par g. Comme $S_n(X)$ est le $\mathbb{Z}/2\mathbb{Z}$-module libre de base $\mathcal{B}_n$, $S_n(X)$ est un $\mathbb{Z}/2\mathbb{Z}[G]$-module. Comme la translation par g envoie les faces de σ sur les faces de $g\sigma$, l'opérateur de bord $d : S_n(X) \to S_{n-1}(X)$ est un homomorphisme de $\mathbb{Z}/2\mathbb{Z}G$-modules, donc $S_*(X)$ est un complexe de $\mathbb{Z}/2\mathbb{Z}[G]$-modules.

Soit $\mathcal{B}'_n$ l'ensemble des applications continues $\sigma' : \Delta_n \to X/G$. La propriété du relèvement unique des chemins pour un revêtement montre que chaque $\sigma' : \Delta_n \to X/G$ se relève en une application $\sigma : \Delta_n \to X$, et tout autre relèvement est de la forme $g\sigma$ pour $g \in G$. Comme les $g\sigma$ sont distincts, cela prouve que $\mathcal{B}_n \simeq G \times \mathcal{B}'_n$ comme G-ensemble. En choisissant un relèvement pour chaque σ', on obtient une application $\mathcal{B}'_n \to \mathcal{B}_n$, puis une base de $S_n(X)$ comme $\mathbb{Z}/2\mathbb{Z}[G]$-module. Cela prouve que l'application naturelle $S_n(X) \to S_n(X/G)$ induit un isomorphisme $S_n(X)_G \simeq S_n(X/G)$. ■

Proposition 1.3.18 *Soient N un sous-groupe fermé normal d'un groupe fini G, et $i : G \to G/N$ la surjection canonique. Notons $Bi : BG \to B(G/N)$ l'application continue associée. Alors l'application d'inflation en cohomologie des groupes*

$$\inf_{G/N,G} : H^*(G/N, \mathbb{Z}/2\mathbb{Z}) \to H^*(G, \mathbb{Z}/2\mathbb{Z})$$

s'identifie à l'image inverse $(Bi)^*$ en cohomologie singulière

$$(Bi)^* : H^*(B(G/N), \mathbb{Z}/2\mathbb{Z}) \to H^*(BG, \mathbb{Z}/2\mathbb{Z})\,.$$

Preuve : Cela résulte de la fonctorialité de la construction $G \to BG$. ■

Représentations de groupes finis et fibrés vectoriels

A une représentation réelle de degré r du groupe fini G

$$\phi : G \to Gl(V)\,,$$

on souhaite associer un fibré vectoriel réel de rang r

$$R_\phi \to BG\,.$$

Définition 1.3.19 *Si $\phi : G \to Gl(V)$ est une représentation réelle de degré r, on définit R_ϕ comme le quotient de $EG \times V$ par l'action diagonale de G (agissant sur V via ϕ), de sorte que l'on a un diagramme commutatif*

$$\begin{tikzcd} EG \times V \arrow[r, "p_1"] \arrow[d, "\tilde{\pi}"'] & EG \arrow[d, "\pi"] \\ R_\phi \arrow[r, "\tilde{p}_1"] & BG \end{tikzcd},$$

où p_1 est la projection sur la première composante, et π est l'application surjective $EG = B\overline{\mathbf{G}} \to BG$ (voir Proposition 1.3.12, (ii)).

C'est le choix fait par B. Kahn ([Ka1], §4.1 page 238) ; cette construction remonte d'ailleurs à Borel ([Bor]). Le résultat suivant, qui n'est pas mentionné dans ce dernier article, est implicitement nécessaire pour attacher des classes de Stiefel-Whitney aux représentations galoisiennes réelles.

Lemme 1.3.20 *Soient G un groupe profini et $K \supset K'$ deux sous-groupes ouverts normaux. On note $f_{K,K'} : G/K' \to G/K$ l'homomorphisme canonique et $Bf_{K,K'} : B(G/K') \to B(G/K)$ l'application continue associée (voir Proposition 1.3.11). Soient $\rho_{K'} : G/K' \to Gl(V)$ et $\rho_K : G/K \to Gl(V)$ deux représentations telles que $\rho_K \circ f_{K,K'} = \rho_{K'}$. Alors on a un isomorphisme de fibrés vectoriels sur $B(G/K')$*

$$R_{\rho_{K'}} \simeq (Bf_{K,K'})^* R_{\rho_K} .$$

PREUVE : Il suffit de considérer le cube suivant

$$\begin{tikzcd} & E(G/K) \times V \arrow[rr] \arrow[dd] & & E(G/K) \arrow[dd] \\ E(G/K') \times V \arrow[ur] \arrow[rr] \arrow[dd] & & E(G/K') \arrow[ur] \arrow[dd] & \\ & R_{\rho_K} \arrow[rr] & & B(G/K) \\ R_{\rho'_K} \arrow[ur] \arrow[rr] & & B(G/K') \arrow[ur] & \end{tikzcd}$$

où les faces avant et arrière sont commutatives par définition des fibrés R_{ρ_K} et $R_{\rho_{K'}}$, les faces supérieure et droite sont commutatives par fonctorialité de E et B, et la face gauche est commutative à cause de la relation entre ρ_K et $\rho_{K'}$. Il en résulte que la face inférieure est commutative. ∎

Voyons maintenant comment on attache des classes de Stiefel-Whitney aux représentations galoisiennes.

Application à la définition des classes de Stiefel-Whitney de représentations galoisiennes

Pour attacher des classes de Stiefel-Whitney à une représentation galoisienne réelle, on commence par la factoriser à travers un groupe fini. On obtient une représentation de groupe fini, laquelle correspond à un fibré vectoriel réel sur l'espace classifiant de ce groupe fini. On sait qu'alors ce fibré vectoriel possède des classes de Stiefel-Whitney (voir sous-section 1.1.3 page 18). Les classes de Stiefel-Whitney de la représentation galoisienne initiale s'obtiennent par inflation de ces dernières. Pour voir que la définition est bien fondée, il faut s'assurer qu'elle ne dépend pas du groupe fini à travers lequel on factorise la représentation galoisienne réelle initiale.

Dorénavant, on fixe F un corps commutatif de caractéristique différente de 2, on note F_s une clôture séparable de F, et $G_F = \mathrm{Gal}\,(F_s/F)$ son groupe de Galois, muni de la topologie de Krull.

Définition 1.3.21 *Une* REPRÉSENTATION GALOISIENNE RÉELLE *est un homomorphisme continu $\rho : G_E \to Gl(V)$, du groupe de Galois $G_E = \mathrm{Gal}\,(F_s/E)$, où E/F est une extension finie séparable de F contenue dans F_s, dans le groupe $Gl(V)$ des automorphismes d'un espace vectoriel V de dimension finie, muni de la topologie discrète.*

L'espace d'arrivée étant muni de la topologie discrète, l'hypothèse de continuité sur ρ *équivaut* à l'existence d'un sous-groupe ouvert normal de H de G_E tel que ρ se factorise à travers G_E/H. On note $\rho_H : G_E/H \to Gl(V)$ la représentation factorisée. On peut lui associer un fibré vectoriel R_{ρ_H} par la construction précédente (Définition 1.3.19).

Définition 1.3.22 *Pour $q \geq 1$, on note $w_q(\rho_H)$ la q-ième classe de Stiefel-Whitney du fibré vectoriel R_{ρ_H}.*

Proposition-Définition 1.3.23 *Pour $q \geq 1$,*

$$\inf_{G_E/H,G_E}(w_q(\rho_H)) \in H^*(G_E)$$

ne dépend pas du groupe H. On pose donc

$$w(\rho) := \inf_{G_E/H,G_E}(w_q(\rho_H))\,.$$

Preuve : Soient H et H' deux sous-groupes ouverts normaux de G_E. On note $\rho_H : G_E/H \to Gl(V)$ et $\rho_{H'} : G_E/H' \to Gl(V)$ les représentations factorisées associées, déduites de ρ. Il s'agit de voir que :

$$\inf_{G_E/H,G_E}(w(\rho_H)) = \inf_{G_E/H',G_E}(w(\rho_{H'}))\,,$$

où $w(\rho_H)$ (resp. $w(\rho_{H'})$) est la classe de Stiefel-Whitney totale de ρ_H (resp. de $\rho_{H'}$) dans $H^*(B(G_E/H))$ (resp. dans $H^*(B(G_E/H'))$. Si pour tous sous-groupes ouverts normaux K et K' de G_E tels que $K \supset K'$ on note

$$f_{K,K'} : G_E/K' \longrightarrow G_E/K$$

l'homomorphisme induit, pour tout entier $q \geq 0$, on peut écrire par définition de la cohomologie galoisienne de G_E le diagramme commutatif :

$$\begin{tikzcd} H^q(G_E/H) \arrow[r, "f^*_{H,H\cap H'}"] \arrow[dr, "f^*_H"'] & H^q(G_E/(H\cap H')) \arrow[d, "f^*_{H\cap H'}"] & H^q(G_E/H') \arrow[l, "f^*_{H',H\cap H'}"'] \arrow[dl, "f^*_{H'}"] \\ & H^q(G_E) & \end{tikzcd},$$

où $f^*_H = \inf_{G_E/H,G_E}$ et $f^*_{H'} = \inf_{G_E/H',G_E}$. Maintenant, les isomorphismes

$$(Bf_{H,H\cap H'})^* R_{\rho_H} \simeq R_{\rho_{H\cap H'}} \text{ et } (Bf_{H',H\cap H'})^* R_{\rho_{H'}} \simeq R_{\rho_{H\cap H'}} \,,$$

(résultant du Lemme 1.3.20), ainsi que la fonctorialité des classes de Stiefel-Whitney et la commutativité du diagramme ci-dessus donnent pour $q \geq 1$:

$$f^*_{H,H\cap H'}(w_q(\rho_{H\cap H'})) = w_q(\rho_H) \text{ et } f^*_{H',H\cap H'}(w_q(\rho_{H\cap H'})) = w_q(\rho'_H)\,, \text{ d'où}$$

$$\inf_{G_E/H,G_E}(w_q(\rho_H)) = \inf_{G_E/(H\cap H'),G_E}(w_q(\rho_{H\cap H'})) = \inf_{G_E/H',G_E}(w_q(\rho_{H'}))\,,$$

ce qu'il fallait démontrer. ■

Remarque 1.3.24 *B. Kahn mentionne qu'il n'est pas pratique ([Ka1], §1.2 page 240) de "considérer l'espace classifiant du groupe profini" G_E. On peut observer que la cohomologie singulière modulo 2 de cet espace classifiant n'est pas la cohomologie galoisienne (courrier électronique de J.-F. Jardine). Curieusement, c'est ainsi que Kozlowski définit les classes de Stiefel-Whitney pour les représentations galoisiennes ([Koz5], page 517).*

1.3.3 L'égalité des transferts en cohomologie galoisienne

Les résultats de la sous-section précédente permettent de définir le transfert d'Evens $\mathcal{N}_{E/F}$ et le transfert de Kozlowski $\mathcal{N}^w_{E/F}$ pour une extension finie séparable E/F de corps commutatifs de caractéristique différente de 2.

Définition 1.3.25 *Si E/F est une extension finie séparable de corps, on définit deux applications*

$$\mathcal{N}_{E/F} : H^{**}(G_E) \to H^{**}(G_F) \text{ et } \mathcal{N}^w_{E/F} : G(G_E) \to G(G_F)$$

en posant :

$$\mathcal{N}_{E/F} = \varinjlim_{L} \mathcal{N}_{f_{L/E,L/F}} \text{ et } \mathcal{N}^w_{E/F} = \varinjlim_{L} \mathcal{N}^w_{f_{L/E,L/F}},$$

où L parcourt les sous-extensions galoisiennes finies de F contenues dans F_s et contenant E et

$$f_{L/E,L/F} : B\,\mathrm{Gal}\,(L/E) \to B\,\mathrm{Gal}\,(L/F),$$

est l'application déduite par fonctorialité de B de $\mathrm{Gal}\,(L/E) \subset \mathrm{Gal}\,(L/F)$.

Cette définition est celle que l'on trouve dans [Sn] (voir [Sn], Chap 4, 2, (2.4) page 145), mais en ce qui concerne $\mathcal{N}_{E/F}$, elle coïncide avec celle qu'a donnée B. Kahn. Cela résulte de la confrontation des Proposition I.2.4 page 231, §I.4.1, §I.4.2 page 238, et §II.1.2 page 240 de [Ka1]. Elle permet d'établir le résultat suivant.

Lemme 1.3.26 *Soient E/F une extension finie séparable, L/F une extension galoisienne finie contenant E, et $f_{L/E,L/F} : B\,\mathrm{Gal}\,(L/E) \to B\,\mathrm{Gal}\,(L/F)$ comme ci-dessus. Alors*

$$\inf_{\mathrm{Gal}\,(L/F),G_F} \circ \mathcal{N}_{f_{L/E,L/F}} = \mathcal{N}_{E/F} \circ \inf_{\mathrm{Gal}\,(L/E),G_E} \text{ et}$$

$$\inf_{\mathrm{Gal}\,(L/F),G_F} \circ \mathcal{N}^w_{f_{L/E,L/F}} = \mathcal{N}^w_{E/F} \circ \inf_{\mathrm{Gal}\,(L/E),G_E}.$$

Preuve : Cela résulte de la Définition 1.3.25. Plus précisément, on a deux systèmes inductifs $(H^*(B\,\mathrm{Gal}\,(L/E)), \phi^E_{L,L'})$ et $(H^*(B\,\mathrm{Gal}\,(L/F)), \phi^F_{L,L'})$. Pour $L \leq L'$ (c'est-à-dire $L \subset L'$), le diagramme

$$\begin{tikzcd} H^*(B\,\mathrm{Gal}\,(L/E)) \arrow[r, "\phi^E_{L,L'}"] \arrow[d, "\mathcal{N}_{f_{L/E,L/F}}"'] & H^*(B\,\mathrm{Gal}\,(L'/E)) \arrow[d, "\mathcal{N}_{f_{L'/E,L'/F}}"] \\ H^*(B\,\mathrm{Gal}\,(L/F)) \arrow[r, "\phi^F_{L,L'}"] & H^*(B\,\mathrm{Gal}\,(L'/F)) \end{tikzcd}$$

est commutatif, donc d'après les propriétés élémentaires des limites inductives, il existe une application (voir [Sha], §2 page 295)

$$\mathcal{N}_{E/F} := \varinjlim_{L} \mathcal{N}_{f_{L/E,L/F}} : \varinjlim_{L} H^*(B\,\mathrm{Gal}\,(L/E)) \to \varinjlim_{L} H^*(B\,\mathrm{Gal}\,(L/F))$$

telle que pour tout L, on ait

$$\mathcal{N}_{E/F} \circ \phi^E_L = \phi^F_L \circ \mathcal{N}_{f_{L/E,L/F}},$$

où

$$\phi^E_L : H^*(B\,\mathrm{Gal}\,(L/E)) \to \varinjlim_{L} H^*(B\,\mathrm{Gal}\,(L/E))$$

et

$$\phi_L^F : H^*(B\,\mathrm{Gal}\,(L/F)) \to \varinjlim_L H^*(B\,\mathrm{Gal}\,(L/F))$$

sont les surjections canoniques, et s'identifient aux inflations

$$\inf_{\mathrm{Gal}\,(L/E),G_E} : H^*(\mathrm{Gal}\,(L/E)) \to H^*(G_E)$$

et

$$\inf_{\mathrm{Gal}\,(L/F),G_F} : H^*(\mathrm{Gal}\,(L/F)) \to H^*(G_F)\,,$$

ce qui permet d'obtenir la première formule du lemme. La seconde s'obtient de façon analogue. ■

Nous allons maintenant pouvoir démontrer :

Théorème 1.3.27 *Les applications $\mathcal{N}_{E/F}$ et $\mathcal{N}^w_{E/F}$, vues comme applications de $G(G_E) \to G(G_F)$, coïncident.*

On va se ramener par réductions successives au cas où l'extension E/F est quadratique. La première réduction repose sur le résultat classique suivant.

Lemme 1.3.28 *Soit K/F une extension finie séparable de degré impair, alors l'application de restriction*

$$\mathrm{Res}_{K/F} : H^{**}(G_K, \mathbb{Z}/2\mathbb{Z}) \longrightarrow H^{**}(G_F, \mathbb{Z}/2\mathbb{Z})$$

est injective.

PREUVE : ([Se3], I, §2, Corollaire à la Proposition 9 page 10). ■

On étudie donc la différence entre $\mathrm{Res}_{K/F}\mathcal{N}_{E/F}$ et $\mathrm{Res}_{K/F}\mathcal{N}^w_{E/F}$ pour une extension K/F bien choisie.

Lemme 1.3.29 *Soit E/F une extension finie séparable de degré n. On peut donc choisir $\theta \in E$ tel que $E = F(\theta)$. Soit L/F une extension galoisienne contenant E. On considère K le sous-corps de L fixé par un 2-Sylow S de $\mathrm{Gal}\,(L/F)$. Alors $\mathrm{Gal}\,(L/E)$ et $\mathrm{Gal}\,(L/K)$ sont deux sous-groupes d'indices finis de $\mathrm{Gal}\,(L/F)$. On peut écrire*

$$\mathrm{Gal}\,(L/F) = \coprod_{i=1}^{r} \mathrm{Gal}\,(L/K)\tau_i\,\mathrm{Gal}\,(L/E)\,.$$

Si $E_i := K(\tau_i(\theta))$ pour $1 \leq i \leq r$, on a

$$E \otimes_F K \simeq \prod_{i=1}^{r} E_i \text{ et } \mathrm{Gal}\,(L/E_i) = \tau_i\,\mathrm{Gal}\,(L/E)\tau_i^{-1} \cap \mathrm{Gal}\,(L/K) \text{ pour } 1 \leq i \leq r\,.$$

Les extensions E_i/K pour $1 \leq i \leq r$ sont finies séparables, chacune contenue dans L/K, de groupe de Galois un 2-groupe, et l'extension K/F est de degré impair. Si on note $c_{\tau_i,L}$ l'application provenant par fonctorialité de B de l'homomorphisme

$$\begin{array}{rcl} \tau_i \operatorname{Gal}(L/E){\tau_i}^{-1} & \to & \operatorname{Gal}(L/E) \\ s & \mapsto & {\tau_i}^{-1} s \tau_i\,, \end{array}$$

on a alors :

$$\begin{array}{rcl} {f_{L/K,L/F}}^* \circ \mathcal{N}_{f_{L/E,L/F}} & = & \displaystyle\prod_{i=1}^{r} \mathcal{N}_{f_{L/E_i,L/K}} \circ \operatorname{Res}_{\tau_i \operatorname{Gal}(L/E){\tau_i}^{-1}, \operatorname{Gal}(L/E_i)} \circ c^*_{\tau_i,L}\,, \\ {f_{L/K,L/F}}^* \circ \mathcal{N}^w_{f_{L/E,L/F}} & = & \displaystyle\prod_{i=1}^{r} \mathcal{N}_{f_{L/E_i,L/K}} \circ \operatorname{Res}_{\tau_i \operatorname{Gal}(L/E){\tau_i}^{-1}, \operatorname{Gal}(L/E_i)} \circ c^*_{\tau_i,L}\,. \end{array}$$

Preuve : Avec les notations ci-dessus, on peut écrire le diagramme suivant

$$\begin{tikzcd} \coprod_{i=1}^{r} B\operatorname{Gal}(L/E_i) \arrow[r, "(g_{L/E_i,L/E})_i"] \arrow[d, "(f_{L/E_i,L/K})_i"'] & B\operatorname{Gal}(L/E) \arrow[d, "f_{L/E,L/F}"] \\ B\operatorname{Gal}(L/K) \arrow[r, "f_{L/K,L/F}"] & B\operatorname{Gal}(L/F) \end{tikzcd}\,,$$

où les flèches $g_{L/E_i,L/E}$ pour $1 \leq i \leq r$ proviennent par fonctorialité de B des homomorphismes définis par

$$\begin{array}{rcl} \operatorname{Gal}(L/E_i) & \to & \operatorname{Gal}(L/E) \\ s & \mapsto & {\tau_i}^{-1} s \tau_i \end{array}\,,$$

et la flèche $f_{L/E,L/F}$, la flèche $f_{L/K,L/F}$, ainsi que les flèches $f_{L/E_i,L/K}$ pour $1 \leq i \leq r$ proviennent par fonctorialité de B d'inclusions. On observe que $g_{L/E_i,L/E}$ est la composée de $B\operatorname{Gal}(L/E_i) \to B(\tau_i \operatorname{Gal}(L/E){\tau_i}^{-1})$, application qui induit la restriction $\operatorname{Res}_{\tau_i \operatorname{Gal}(L/E){\tau_i}^{-1}, \operatorname{Gal}(L/E_i)}$ en cohomologie, et de $c_{\tau_i,L}$. Le diagramme ci-dessus est, d'après ([Str], Lemme 7.3 page 130), homotope à un diagramme de pullback, ce qui permet d'écrire, en utilisant les propriétés de fonctorialité et d'union disjointe des transferts,

$$\begin{array}{rcl} {f_{L/K,L/F}}^* \circ \mathcal{N}_{f_{L/E,L/F}} & = & \displaystyle\prod_{i=1}^{r} \mathcal{N}_{f_{L/E_i,L/K}} \circ g^*_{L/E_i,L/E}\,, \\ & = & \displaystyle\prod_{i=1}^{r} \mathcal{N}_{f_{L/E_i,L/K}} \circ \operatorname{Res}_{\tau_i \operatorname{Gal}(L/E){\tau_i}^{-1}, \operatorname{Gal}(L/E_i)} \circ c^*_{\tau_i,L} \end{array}$$

$$\begin{array}{rcl} {f_{L/K,L/F}}^* \circ \mathcal{N}^w_{f_{L/E,L/F}} & = & \displaystyle\prod_{i=1}^{r} \mathcal{N}^w_{f_{L/E_i,L/K}} \circ g^*_{L/E_i,L/E}\,, \\ & = & \displaystyle\prod_{i=1}^{r} \mathcal{N}_{f_{L/E_i,L/K}} \circ \operatorname{Res}_{\tau_i \operatorname{Gal}(L/E){\tau_i}^{-1}, \operatorname{Gal}(L/E_i)} \circ c^*_{\tau_i,L}\,, \end{array}$$

comme annoncé. ∎

Le résultat précédent montre qu'il suffit de montrer l'égalité $\mathcal{N}_{E/F} = \mathcal{N}^w_{E/F}$ sur $G(G_E)$ pour toute extension finie séparable E/F contenue dans une extension galoisienne de groupe de Galois un 2-groupe, qui est filtrée par une tour d'extensions quadratiques.

En effet, pour $x \in G(G_E)$, il existe une extension galoisienne finie L/F avec $L \supset E$ et un élément $x_L \in G(B(\mathrm{Gal}\,(L/E)))$ tel que $x = \inf_{\mathrm{Gal}\,(L/E),G_E}(x_L)$. Alors, en faisant la construction du lemme précédent,

$$\begin{aligned}
\mathrm{Res}_{K/F}\big(\mathcal{N}_{E/F}(x)\big) &= \mathrm{Res}_{K/F}\Big(\mathcal{N}_{E/F}\big(\inf_{\mathrm{Gal}\,(L/E),G_E}(x_L)\big)\Big)\\
&= \mathrm{Res}_{K/F}\Big(\inf_{\mathrm{Gal}\,(L/F),G_F}\big(\mathcal{N}_{f_{L/E,L/F}}(x_L)\big)\Big)\\
&= \inf_{\mathrm{Gal}\,(L/K),G_K}\Big(f^*_{L/E,L/F}\big(\mathcal{N}_{f_{L/E,L/F}}(x_L)\big)\Big)\\
&= \inf_{\mathrm{Gal}\,(L/K),G_K}\Big(\prod_{i=1}^{r}\mathcal{N}_{f_{L/E_i,L/K}}\big(g^*_{L/E_i,L/E}(x_L)\big)\Big)\\
&= \prod_{i=1}^{r}\inf_{\mathrm{Gal}\,(L/K),G_K}\Big(\mathcal{N}_{f_{L/E_i,L/K}}\big(g^*_{L/E_i,L/E}(x_L)\big)\Big)\\
&= \prod_{i=1}^{r}\mathcal{N}_{E_i/K}\Big(\inf_{\mathrm{Gal}\,(L/E_i),G_{E_i}}\big(g^*_{L/E_i,L/E}(x_L)\big)\Big)\,,
\end{aligned}$$

et pour la même raison :

$$\mathrm{Res}_{K/F}\big(\mathcal{N}^w_{E/F}(x)\big) = \prod_{i=1}^{r}\mathcal{N}^w_{E_i/K}\Big(\inf_{\mathrm{Gal}\,(L/E_i),G_{E_i}}\big(g^*_{L/E_i,L/E}(x_L)\big)\Big)\,.$$

L'énoncé suivant ramène maintenant à traiter le cas où E/F est quadratique.

Lemme 1.3.30 *Soit E/F une extension finie séparable contenue dans une extension galoisienne L de groupe de Galois un 2-groupe. Alors il existe des sous-extensions $(E_i)_{1\leq i\leq t}$ avec*

$$E = E_1 \supset E_2 \supset \cdots \supset E_t = F \ \textit{et}\ [E_{i+1} : E_i] = 2 \ \textit{pour}\ 1 \leq i \leq t\,,$$

et on en déduit que

$$\mathcal{N}_{E/F} = \mathcal{N}_{E_1/E_2} \circ \mathcal{N}_{E_2/E_3} \circ \cdots \circ \mathcal{N}_{E_{t-1}/E_t}\,,$$

$$\mathcal{N}^w_{E/F} = \mathcal{N}^w_{E_1/E_2} \circ \mathcal{N}^w_{E_2/E_3} \circ \cdots \circ \mathcal{N}^w_{E_{t-1}/E_t}\,,$$

Preuve : On montre la première partie du lemme par récurrence sur le degré de E/F. Si E/F est quadratique c'est vrai ; on suppose que c'est vrai pour toute extension E/F avec $[E:F] \leq 2^k$ où $k \leq n$. Si E/F est de degré 2^{n+1}, soit H un sous-groupe de $G = \mathrm{Gal}\,(L/F)$ tel que $E = L^H$. Si H est normal dans G, l'extension E/F est *galoisienne* : on prend $\sigma \in \mathrm{Gal}\,(E/F)$ un élément d'ordre 2, et on applique l'hypothèse de récurrence à $E_1 = L^{<\sigma>}$. Si H n'est pas normal dans G, le normalisateur $N_G(H)$ de H dans G satisfait $H \subsetneq N_G(H) \subsetneq G$, d'après ([Rob], Chap 5, 5.2.4 page 121). Si $E' := L^{N_G(H)}$, on peut appliquer l'hypothèse de récurrence à E/E' et E'/F dont les degrés sont inférieurs à 2^n.

Les deux égalités s'obtiennent en considérant la suite de composition

$$B\,\mathrm{Gal}\,(L/E_1) \longrightarrow B\,\mathrm{Gal}\,(L/E_2) \longrightarrow \cdots \longrightarrow B\,\mathrm{Gal}\,(L/E_t)\,,$$

en utilisant les propriétés de transitivité des transferts d'Evens et de Kozlowski (Propriété 1.1.5 et (iii) du Théorème 1.2.2), et en passant à la limite sur L. ∎

On traite maintenant le cas où E/F est une extension quadratique.

Théorème 1.3.31 *Si E/F est une extension quadratique, et si $\sum_{i\geq 0} x_i$ est un élément de $G(G_E)$, alors*

$$\mathcal{N}^w_{E/F}\left(\sum_{i\geq 0} x_i\right) = \mathcal{N}_{E/F}\left(\sum_{i\geq 0} x_i\right)\,.$$

Preuve : En inflatant la formule (v) du Théorème 1.2.2, on obtient

$$\mathcal{N}^w_{E/F}\left(\sum_{i\geq 0} x_i\right) = \mathcal{N}_{E/F}\left(\sum_{i\geq 0} x_i\right) + \sum_{i\geq 0} \mathcal{N}_{E/F}(x_i)((1+t)^{-i}+1)\,, \qquad (1.12)$$

avec $t = \inf_{\mathrm{Gal}\,(L/F),G_F}(w_1(f_{L/E,L/F_*}(\mathbf{1}_{B\,\mathrm{Gal}\,(L/E)}))) = (d_{E/F})$ (Lemme 1.3.32 ci-dessous), pour toute extension galoisienne finie L/F contenant E. Pour montrer le lemme, il suffit de constater que la somme intervenant dans le membre de droite de la formule (1.12) est une somme de termes ayant un facteur $(d_{E/F})^k \cdot \mathcal{N}_{E/F}(x_i)$ pour $k \geq 1$ et $i \geq 1$, qui sont tous nuls : ceci est *spécifique à la cohomologie galoisienne* et résultera du Lemme 1.3.33 ci-dessous. ∎

Lemme 1.3.32 *Soit E/F une extension quadratique de discriminant $d_{E/F}$ dans $F^*/F^{*2} \simeq H^1(G_F, \mathbb{Z}/2\mathbb{Z})$, et L/F une extension galoisienne finie contenant E. Alors*

$$\inf_{\mathrm{Gal}\,(L/F),G_F}(w_1(f_{L/E,L/F_*}(\mathbf{1}_{B\,\mathrm{Gal}\,(L/E)}))) = (d_{E/F})\,.$$

Preuve : Le membre de droite désigne l'élément de $H^1(G_F, \mathbb{Z}/2\mathbb{Z}) = \mathrm{Hom}_{cont}(G_F, \mathbb{Z}/2\mathbb{Z})$ dont un représentant est $\gamma \mapsto \gamma(\sqrt{d_{E/F}})$. Dans le membre de gauche, le fibré $f_{L/E,L/F_*}(\mathbf{1}_{B\,\mathrm{Gal}\,(L/E)})$ correspond à l'induite à $\mathrm{Gal}\,(L/F)$ de la représentation triviale de $\mathrm{Gal}\,(L/E)$, qui est, d'après ([Se4], 3.3, exemple 1 page 43), la représentation ρ de permutation de $\mathrm{Gal}\,(L/E)$ associée à G_F/G_E. D'autre part, l'élément $w_1(f_{L/E,L/F_*}(\mathbf{1}_{B\,\mathrm{Gal}\,(L/E)})) \in H^1(B\,\mathrm{Gal}\,(L/F), \mathbb{Z}/2\mathbb{Z})$ correspond, d'après (axiome SW3 de [GKT] page 327) à l'élément $\gamma \mapsto \det(\rho(\gamma))$, compte tenu de l'isomorphisme $H^1(B\,\mathrm{Gal}\,(L/F), \mathbb{Z}/2\mathbb{Z}) \simeq \mathrm{Hom}_{cont}(\mathrm{Gal}\,(L/F), \mathbb{Z}/2\mathbb{Z})$, et l'on peut vérifier qu'en composant cet élément avec l'homomorphisme canonique $G_F \to \mathrm{Gal}\,(L/F)$, on trouve $(d_{E/F})$. ■

Lemme 1.3.33 *Soit E/F une extension quadratique de discriminant $d_{E/F}$ dans F^*/F^{*2}. Alors pour tout $i \geq 1$, et tout $x \in H^i(G_E)$, on a*

$$(d_{E/F}) \cdot \mathcal{N}_{E/F}(x) = 0\,.$$

PREUVE : Il résulte de la Proposition II.1.4 et du Lemme II.2.1 pages 240-241 de [Ka1] que l'assertion du lemme ci-dessus est vraie pour les éléments de $H^i(G_E)$ qui sont sommes de cup-produits de termes de degré 1 (donc *décomposables*). La conjecture de Milnor ([Mil2] ou [Se3], Annexe, 2.3, page 164) mentionnée par Kahn ([Ka1]) et Kozlowski ([Koz5]) a été démontrée par Voevodsky ([Mor], Théorème 2.2 page 124). Cela implique que tout élément de $H^i(G_E)$, $i \geq 1$ est décomposable. ■

Remarque 1.3.34 *(i) La décomposabilité des classes de Stiefel-Whitney totales de représentations galoisiennes, établie par Kahn ([Ka1], Théorème 4 page 247) suffit pour établir que $\mathcal{N}_{E/F}(x) = \mathcal{N}^w_{E/F}(x)$ si x est une classe de Stiefel-Whitney totale de représentations galoisiennes, ce qui suffit pour montrer la formule (3) de l'introduction, bien qu'on montre plus ici.*
(ii) Pour tout complément concernant la conjecture de Milnor et le théorème de Voevodsky, on peut consulter [Ka2] et [Mor].

1.4 Conclusion et problèmes ouverts

Au cours de ce chapitre, via les travaux de Kozlowski, nous avons explicité le lien qui existe entre la formule de Fulton-MacPherson ((4), page 8) et celle de Kahn ((3), page 8), et qui donne une vision plus "intrinsèque" de la démonstration de cette dernière.

Nous avons également apporté une contribution à la résolution de la conjecture de Kozlowski, qui demeure néanmoins ouverte.

En revanche, il faut signaler que la conjecture de Segal que nous avons énoncée dans la section 1.2 a été résolue par C. P. Boyer, H. B. Lawson, P. Lima-Filho, B. M. Mann, M.-L. Michelsohn ([BLLMM], Théorème B page 376).

On ne sait pas si le transfert de Kozlowski provient d'une théorie cohomologique généralisée, ni si le transfert introduit par les cinq auteurs ci-dessus coïncide avec celui de Kozlowski.

Chapitre 2

Invariants d'algèbres étales sur un corps de caractéristique 2

2.1 Invariants dans le groupe $H^1(G_F, \mathbb{Z}/2\mathbb{Z})$

Cette section s'organise comme suit : dans la sous-section 2.1.1, on définit l'invariant $\epsilon(e_{E/F})$, à valeurs dans $H^1(G_F, \mathbb{Z}/2\mathbb{Z})$, associé à une algèbre étale E/F de rang n. Dans la sous-section 2.1.2, on compare deux définitions, l'une géométrique, l'autre matricielle, de l'invariant de Arf d'un espace quadratique non dégénéré sur un corps de caractéristique 2.

La sous-section 2.1.3 est consacrée à l'invariant de Dickson d'un automorphisme orthogonal : on donne là aussi deux définitions que l'on compare.

L'invariant $d^+(E/F)$ est défini dans la sous-section 2.1.4, et dans la sous-section 2.1.5, on montre l'égalité $j(d^+(E/F)) = \epsilon(e_{E/F})$.

2.1.1 L'invariant $\epsilon(e_{E/F})$ d'une algèbre étale E/F

Dans la suite, F est un corps de caractéristique 2, F_s une clôture séparable de F de groupe de Galois G_F. La suite exacte d'Artin-Schreier

$$0 \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow F_s \xrightarrow{\wp : x \mapsto x^2 + x} F_s \longrightarrow 0$$

permet d'obtenir un isomorphisme

$$j : F/\wp(F) \xrightarrow{\simeq} H^1(G_F, \mathbb{Z}/2\mathbb{Z}) \,,$$

défini ainsi : un élément $a \in F$ représentant une classe de $F/\wp(F)$ a pour image l'homomorphisme continu

$$\begin{array}{rcl} G_F & \longrightarrow & \mathbb{Z}/2\mathbb{Z} \\ \gamma & \longmapsto & \gamma(x) - x \text{ où } x^2 + x = a, x \in F_s \,. \end{array}$$

La signature

$$\epsilon : \mathfrak{S}_n \longrightarrow \mathbb{Z}/2\mathbb{Z}$$

notée additivement induit une application

$$\begin{array}{rcl} H^1(G_F, \mathfrak{S}_n) & \longrightarrow & H^1(G_F, \mathbb{Z}/2\mathbb{Z}) \\ e & \longmapsto & \big(\gamma \mapsto \epsilon(e(\gamma))\big) \end{array}$$

qui permet d'associer à E/F un invariant dans $H^1(G_F, \mathbb{Z}/2\mathbb{Z})$, à savoir

$$\epsilon(e_{E/F}),$$

où $\epsilon(e_{E/F})$ est une notation abusive pour l'élément $\gamma \mapsto \epsilon(e_{E/F}(\gamma))$.

2.1.2 Sur l'invariant de Arf d'un espace quadratique

Le corps F est toujours de caractéristique 2.

Sur la définition géométrique de l'invariant de Arf

Définition 2.1.1 *Un* ESPACE QUADRATIQUE (V, q) *est la donnée d'un espace vectoriel* V *de dimension finie, muni d'une* FORME QUADRATIQUE, *c'est-à-dire une application* $q : V \to F$ *telle que*
(i) $\forall (a, x) \in F \times V, q(ax) = a^2 q(x)$,
(ii) L'application

$$\begin{array}{rcl} b_q : V \times V & \longrightarrow & F \\ (x, y) & \longmapsto & q(x + y) - q(x) - q(y) \end{array}$$

est F*-bilinéaire.*

Définition 2.1.2 *Un espace quadratique* (V, q) *est* NON DÉGÉNÉRÉ *si la forme* b_q *définit un isomorphisme de* V *sur* $V^* = \mathrm{Hom}_F(V, F)$.

Un espace quadratique non dégénéré est alors de dimension paire.

Définition 2.1.3 *Soit* (V, q) *un espace quadratique non dégénéré. Une base* $(e_1, f_1, \ldots, e_m, f_m)$ *de* V *est* SYMPLECTIQUE *pour* q *si* $b_q(e_i, f_i) = 1$ *pour* $1 \leq i \leq m$, $b_q(e_i, e_j) = b_q(f_i, f_j) = 0$ *pour* $1 \leq i, j \leq m$.

Définition 2.1.4 *Soit* (V, q) *un espace quadratique non dégénéré. L'*INVARIANT DE ARF *de* (V, q), *que l'on note* $\mathrm{Arf}(V, q)$, *est la classe modulo le groupe additif* $\wp(F) := \{x^2 + x, x \in F\}$ *de l'élément*

$$\mathrm{Arf}_{\mathcal{B}}(q) := \sum_{i=1}^{m} q(e_i) q(f_i),$$

où $\mathcal{B} = (e_1, f_1, \ldots, e_m, f_m)$ *est une base symplectique de* V *pour* q.

Sur la définition matricielle de l'invariant de Arf

La définition de l'invariant de Arf $\mathrm{Arf}(V, q)$ d'un espace quadratique non dégénéré (V, q) de dimension paire qu'on a donnée ci-dessus est "géométrique". Le Lemme 2.1.6 et le Corollaire 2.1.7 qui suivent, et qui seront utilisés dans la preuve du Théorème 3, visent à en donner une définition "matricielle" (i. e. la formule (2.4) dudit Corollaire) qui facilite son calcul (on n'a plus besoin de connaître une base symplectique).

Notation 2.1.5 *Pour tout entier $n \geq 2$ et toute matrice $M \in M_n(F)$, on note $s_1(M)$ (resp. $s_2(M)$) le coefficient en degré X^{n-1} (resp. X^{n-2}) du polynôme caractéristique de M.*

Lemme 2.1.6 *Soit M et N deux matrices de $M_n(F)$ telles que $W = {}^tM + M$ est inversible. Alors*

$$s_2(W^{-1}(M + {}^tN + N)) = s_2(W^{-1}M) + s_1(W^{-1}N) + (s_1(W^{-1}N))^2 .$$

Preuve : C'est le Lemme (0.5) page xx de [KMRT]. On développe le membre de gauche à l'aide de

$$s_2(W^{-1}M + W^{-1}(N + {}^tN)) =$$

$$s_2(W^{-1}M) + s_2(W^{-1}(N + {}^tN)) + s_1(W^{-1}M)s_1(W^{-1}(N + {}^tN)) +$$
$$s_1(W^{-1}MW^{-1}(N + {}^tN)) .$$

Pour montrer le lemme, on procède par étapes en montrant

$$s_2(W^{-1}(N + {}^tN)) = (s_1(W^{-1}N))^2 , \tag{2.1}$$

$$s_1(W^{-1}M)s_1(W^{-1}(N + {}^tN)) = 0 , \tag{2.2}$$

$$s_1(W^{-1}MW^{-1}(N + {}^tN)) = s_1(W^{-1}N) . \tag{2.3}$$

Comme une matrice et sa transposée ont le même polynôme caractéristique, les traces de $W^{-1}N$ et de ${}^t(W^{-1}N) = {}^tW^{-1}$ sont égales, donc

$$s_1((W^{-1})^tN) = s_1({}^tW^{-1}) = s_1(W^{-1}N) .$$

Donc $s_1(W^{-1}(N + {}^tN)) = 0$ et la formule (2.2) est montrée.

De même, on a

$$s_1(W^{-1}M(W^{-1})^tN) = s_1(N(W^{-1})^tMW^{-1}) = s_1((W^{-1})^tMW^{-1}N) ,$$

donc le membre gauche de (2.3) est

$$s_1(W^{-1}M(W^{-1})N) + s_1((W^{-1})^t MW^{-1}N) = s_1(W^{-1}(M + {}^tM)W^{-1}N)\,.$$

Comme $M + {}^tM = W$, cela prouve (2.3).

Enfin, le membre de gauche de (2.1) est

$$s_2(W^{-1}N) + s_2((W^{-1})^t N) + s_1(W^{-1}N)s_1((W^{-1})^t N) + s_1(W^{-1}N(W^{-1})^t N)\,.$$

Comme $W^{-1}N$ et $(W^{-1})^t N = (W^{-1})^t (W^{-1}N)W$ ont le même polynôme caractéristique, on a $s_i(W^{-1}N) = s_i((W^{-1})^t N)$ pour $i \in \{1, 2\}$. On déduit de cela que les deux premiers termes s'annulent, et que le troisième vaut $(s_1(W^{-1}N))^2$. Donc pour prouver (2.1), il suffit de voir que

$$s_1(W^{-1}N(W^{-1})({}^tN)) = 0\,.$$

Comme $W = {}^tM + M$, on a $W^{-1} = (W^{-1})^t MW^{-1} + W^{-1}MW^{-1}$, d'où

$$\begin{aligned} s_1(W^{-1}N(W^{-1})({}^tN)) &= s_1(W^{-1}MW^{-1}N(W^{-1}))({}^tN)) \\ &+ s_1((W^{-1})^t MW^{-1}N(W^{-1})({}^tN))\,, \end{aligned}$$

et (2.1) si l'on montre que les deux termes du membre de droite sont égaux. Comme ${}^tW = W$, on a ${}^t(W^{-1}MW^{-1}N(W^{-1})) = N(W^{-1})^t N(W^{-1})^t MW^{-1}$, d'où

$$\begin{aligned} s_1(W^{-1}MW^{-1}N(W^{-1})) &= s_1((N(W^{-1})^t N)((W^{-1})^t MW^{-1})) \\ &= s_1((W^{-1})^t MW^{-1}N(W^{-1})({}^tN))\,, \end{aligned}$$

et la preuve du lemme est achevée. ■

Corollaire 2.1.7 *Soit (V, q) un espace quadratique non dégénéré de dimension $n = 2m$, et M une matrice de q dans une base symplectique. Alors, dans $F/\wp(F)$*

$$\mathrm{Arf}\,(V, q) = s_2((M + {}^tM)^{-1}M) + \frac{m(m-1)}{2}\,, \tag{2.4}$$

où Arf (V, q) *est l'invariant de Arf de (V, q).*

PREUVE : Si M est une matrice de q dans une base $(e_1, \ldots, e_n)$ de V, cela signifie que $q(x) = {}^tXMX$ lorsque $X = {}^t(x_1, \ldots, x_n)$ avec $x = \sum_{i=1}^n x_i e_i$. D'après le Lemme 2.1.6, le membre de droite ne dépend donc ni de la base symplectique $\mathcal{B} = (e_1, f_1, \ldots, e_m, f_m)$ choisie, ni de la matrice M, qu'on peut donc supposer être constituée de m blocs diagonaux de la forme

$$\begin{pmatrix} \alpha_i & 1 \\ 0 & \beta_i \end{pmatrix}, \text{ avec } \alpha_i = q(e_i) \text{ et } \beta_i = q(f_i) \text{ pour } 1 \le i \le m\,.$$

Ainsi, Arf $(V, q) = \sum_{i=1}^m \alpha_i\beta_i = s_2((M + {}^tM)^{-1}M) + \frac{m(m-1)}{2}$ modulo $\wp(F)$. ■

2.1.3 Sur l'invariant de Dickson d'un automorphisme orthogonal

Dans cette section, on va comparer deux définitions de l'invariant de Dickson $\Delta(u)$ (à valeurs dans le groupe $\mathbb{Z}/2\mathbb{Z}$) d'un élément u du groupe orthogonal $O(V, q)$ d'un espace quadratique non dégénéré. La première ("géométrique", voir Définition 2.1.12), repose sur l'algèbre de Clifford de (V, q)) et est pratique pour montrer que l'invariant de Dickson d'une transvection orthogonale de vecteur anisotrope est 1 (Lemme 2.1.13). La seconde ("matricielle", voir Proposition 2.1.14) est pratique pour montrer que l'invariant de Dickson définit un homomorphisme (Proposition 2.1.16). Le Corollaire 2.1.15 vise à rapprocher ces deux définitions. Ces résultats seront utilisés dans la preuve du Théorème 3.

Sur la définition géométrique de l'invariant de Dickson.

Définition 2.1.8 *Soit (V, q) un espace quadratique non dégénéré. On appelle* Algèbre de Clifford *de (V, q), et on note $C(V, q)$ la F-algèbre*

$$T(V)/I \text{ avec } T(V) = \bigoplus_{m \geq 0} V^{\otimes m} \text{ et } I = \{v \otimes v - q(v), v \in V\}T(V)\,.$$

Lemme 2.1.9 *Soit $(e_1, f_1, \dots, e_m, f_m)$ une base symplectique d'un espace quadratique non dégénéré (V, q) de dimension $n = 2m$. Alors*
(i) Les éléments

$$e_1^{k_1} f_1^{l_1} \dots e_m^{k_m} f_m^{l_m} \text{ avec } 0 \leq k_i, l_i \leq 1 \text{ pour } 1 \leq i \leq m$$

forment une base de $C(V, q)$.
(ii) On a les relations

$$e_i e_i = q(e_i)\,, f_i f_i = q(f_i)\,,$$
$$e_i e_j = e_j e_i\,, f_i f_j = f_j f_i, \text{ et } e_i f_j + f_j e_i = \delta_{i,j}$$

pour $1 \leq i, j \leq m$.
(iii) On a l'isomorphisme

$$C(V, q) \simeq \bigotimes_{i=1}^{m} C(F \times F, q(e_i)x^2 + xy + q(f_i)y^2)\,.$$

Preuve : Voir ([Di2], II, §7 page 53) puis ([Di2], II, §10 page 63), et aussi ([Sch], page 343). ■

Définition 2.1.10 *Soit (V, q) un espace quadratique non dégénéré de dimension $n = 2m$. L'algèbre de Clifford paire de (V, q), notée $C^+(V, q)$, est la sous-algèbre de $C(V, q)$ engendrée par les éléments $e_1^{k_1} f_1^{l_1} \dots e_m^{k_m} f_m^{l_m}$ avec $0 \leq k_i, l_i \leq 1$ pour $1 \leq i \leq m$ (où $\mathcal{B} = (e_1, f_1, \dots e_m, f_m)$ est une base symplectique de V pour q), avec parmi les entiers $\{k_1, l_1, \dots, k_m, l_m\}$, un nombre pair d'entre eux égaux à 1.*

Lemme 2.1.11 *Soit (V, q) un espace quadratique non dégénéré de dimension $n = 2m$ et $\mathcal{B} = (e_1, f_1, \ldots e_m, f_m)$ une base de V symplectique pour q. Alors*
(i) Le centre de $C(V, q)$ est F.
(ii) Le centre de $Z(C^+(V, q))$ de $C^+(V, q)$ est $F(\zeta)$ où

$$\zeta = e_1 f_1 + \cdots + e_m f_m \,.$$

PREUVE : Voir ([Sch], chap. 9, §4, 4.8 page 343). ■

Pour $u \in O(V, q)$, l'isomorphisme u du F-espace vectoriel V se prolonge en un automorphisme de l'algèbre $C(V, q)$, qui se restreint en un automorphisme de l'algèbre $C^+(V, q)$, puis de son centre $Z(C^+(V, q))$, encore noté u.

Définition 2.1.12 *Pour $u \in O(V, q)$, on appelle* INVARIANT DE DICKSON *de u, et on note $\Delta(u)$ l'élément défini par*

$$\Delta(u) = \begin{cases} 0 & si \quad u_{|Z(C^+(V,q))} = Id_{Z(C^+(V,q))} \,, \\ 1 & si \quad u_{|Z(C^+(V,q))} \neq Id_{Z(C^+(V,q))} \,, \end{cases}$$

où $Z(C^+(V, q))$ désigne le centre de l'algebre de Clifford paire de l'espace quadratique non dégénéré (V, q) de dimension $n = 2m$.

Lemme 2.1.13 *Si $\tau_v \in O(V, q)$ est la transvection orthogonale de vecteur anisotrope $v \in V$, alors $\Delta(\tau_v) = 1$.*

PREUVE : Rappelons que pour $x \in V$, $\tau_v(x) = x + \frac{b_q(x,v)}{q(v)}$. Il suffit alors de compléter $e_1 := v$ en une base symplectique $(e_1, f_1, \ldots, e_m, f_m)$ de V pour q ($n = \dim V = 2m$) et de vérifier que $\tau_v(\zeta) \neq \zeta$ pour $\zeta = e_1 f_1 + \cdots + e_m f_m$. ■

Sur la définition matricielle de l'invariant de Dickson.

Proposition 2.1.14 *Soit (V, q) un espace quadratique non dégénéré de dimension $n = 2m$, et $u \in O(V, q)$. Soit $\mathcal{B}$ une base de V, M une matrice de q dans $\mathcal{B}$, et $W = {}^tM + M$, puis soit U la matrice de u dans $\mathcal{B}$. Alors*
(i) Il existe une matrice $R \in M_n(F)$ avec ${}^tUMU = M + R - {}^tR$.
(ii) L'élément $Tr(W^{-1}R)$ de F, qui ne dépend que de u, vaut 0 ou 1.

PREUVE : On adapte ([KMRT], Proposition (12.7) page 156). Le point (i) résulte de ce que $u \in O(V, q)$. Montrons donc (ii). Si on change de base pour V, la matrice U est remplacée par $U' = P^{-1}UP$, où $P \in Gl_n(F)$, et la matrice M est remplacée par la matrice $M' = {}^tPMP + N - {}^tN$ avec $N \in M_n(F)$ convenable. La matrice $W' = {}^tM' + M'$ est alors reliée à W par $W' = {}^tPWP$. Supposons que R et R' sont des matrices telles que

$${}^tUMU - M = R - {}^tR \text{ et } {}^tU'M'U' - M' = R' - {}^tR' \,.$$

En ajoutant à chaque membre sa transposée, on en déduit que

$$ {}^tUWU = W \text{ et } {}^tU'W'U' = W' . $$

Pour prouver que $Tr(W^{-1}R)$ ne dépend que de u, il faut montrer que $Tr(W'^{-1}R')$ est égal à $Tr(W^{-1}R)$. En substituant à M' son expression en termes de M, on obtient que $R' - {}^tR' = R'' - {}^tR''$ avec

$$ R'' = {}^tPRP + {}^tP^tU^t(P^{-1})^tNP^{-1}UP - U $$

donc $R' = R'' + S$ où S est une matrice symétrique de $M_n(F)$. Puisque $W'^{-1} = W'^{-1}M'W'^{-1} + {}^t(W'^{-1}M'W'^{-1})$, on en déduit que W' est alternée, et il en résulte que $Tr(W'^{-1}S) = 0$. Ainsi $Tr(W'^{-1}R') = Tr(W'^{-1}R'')$. On déduit de cela que

$$ \begin{aligned} Tr(W'^{-1}R'') &= Tr(P^{-1}W^{-1}RP) + Tr(P^{-1}W^{-1t}U^t(P^{-1})NP^{-1}UP) \qquad (2.5)\\ &+ Tr(P^{-1}(W^{-1})^t(P^{-1})N) . \end{aligned} $$

Mais comme $(W^{-1})^tU = U^{-1}W^{-1}$, le second terme du membre de droite de l'égalité (2.5) vaut

$$ Tr(P^{-1}U^{-1}(W^{-1})^t(P^{-1})NP^{-1}UP) = Tr((W^{-1})^t(P^{-1})NP^{-1}) . $$

Ainsi, les deux derniers termes du second membre de (2.5) se neutralisent, et on obtient

$$ Tr(W'^{-1}R') = Tr(W'^{-1}R'') = Tr(W^{-1}R) , $$

qui ne dépend donc que de u. Pour montrer que cet élément vaut 0 ou 1, on calcule $s_2(W^{-1}M)$, le coefficient en X^{n-2} dans le polynôme caractéristique de $W^{-1}M$. Puisque $U^{-1}W^{-1} = (W^{-1})^tU$, on a $U^{-1}W^{-1}MU = (W^{-1})^tUMU$, donc

$$ s_2(W^{-1}M) = s_2((W^{-1})^tUMU) . $$

En subsituant dans le second membre ci-dessus l'égalité ${}^tUMU = M + R - {}^tR$, on obtient

$$ s_2(W^{-1}M) = s_2(W^{-1}M + W^{-1}R - (W^{-1})^tR) , $$

et comme $W^{-1} = {}^t(W^{-1})$, on peut appliquer le Lemme 2.1.6 pour obtenir

$$ s_2(W^{-1}M) = s_2(W^{-1}M) + Tr(W^{-1}R) + (Tr(W^{-1}R))^2 , $$

et on conclut que $Tr(W^{-1}R) + (Tr(W^{-1}R))^2 = 0$, donc $Tr(W^{-1}R) \in \{0, 1\}$. ■

Corollaire 2.1.15 *Soit (V, q) un espace quadratique non dégénéré de dimension $n = 2m$, et $u \in O(V, q)$. Soit $\mathcal{B}$ une base de V, M une matrice de q dans $\mathcal{B}$, et $W = {}^tM + M$, puis soit U la matrice de u dans $\mathcal{B}$, et $R \in M_n(F)$ avec ${}^tUMU = M + R - {}^tR$. Alors l'élément $Tr(W^{-1}R)$ est l'invariant de Dickson $\Delta(u)$ de u (Définition 2.1.12).*

PREUVE : En utilisant la définition "géométrique", J. Dieudonné donne dans [Di1], une formule pour calculer l'invariant de Dickson $\Delta(u)$ d'un élément $u \in O(V,q)$ à partir des coefficients de sa matrice dans une base $\mathcal{B} = (e_1, \dots, e_m, e_{m+1}, \dots, e_{2m})$ de V symplectique pour q (au sens de la Définition 2.1.3 page 44, avec $f_i = e_{m+i}$ avec $1 \leq i \leq m$). Explicitement, si

$$u(e_i) = \sum_{j=1}^{m} a_{i,j} e_j + \sum_{j=1}^{m} b_{i,j} e_{m+j} \text{ et } u(e_{m+i}) = \sum_{j=1}^{m} c_{i,j} e_j + \sum_{j=1}^{m} d_{i,j} e_{m+j}$$

pour $1 \leq j \leq m$, alors

$$\Delta(u) = \sum_{1 \leq i,j \leq m} \alpha_j a_{i,j} c_{i,j} + \beta_j b_{i,j} d_{i,j} + b_{i,j} c_{i,j} \, ,$$

avec $\alpha_i = q(e_i)$ et $\beta_i = q(e_{m+i})$ pour $1 \leq i \leq m$. Pour comparer ceci à l'élément $Tr(W^{-1}R)$ (R étant à déterminer), on introduit les six matrices

$$\begin{array}{lll} A = (a_{j,i})_{1 \leq i,j \leq m} \, , & B = (b_{j,i})_{1 \leq i,j \leq m} \, , & \underline{\alpha} = \mathrm{Diag}(\alpha_i, 1 \leq i \leq m) \, , \\ C = (c_{j,i})_{1 \leq i,j \leq m} \, , & D = (d_{j,i})_{1 \leq i,j \leq m} \, , & \underline{\beta} = \mathrm{Diag}(\beta_i, 1 \leq i \leq m) \, , \end{array}$$

de sorte que si U est la matrice de u dans la base $\mathcal{B}$ et si M est la matrice de q dans la base $\mathcal{B}$ sous la forme d'un tableau diagonal de matrices $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, on a

$$U = \begin{pmatrix} A & C \\ B & D \end{pmatrix} \text{ et } M = \begin{pmatrix} \underline{\alpha} & Id \\ 0 & \underline{\beta} \end{pmatrix} .$$

En utilisant la relation ${}^tUWU = W$, on voit que ${}^tAD = {}^tBC + Id$. Il en résulte que si on pose

$$R_0 := {}^tB\underline{\beta}D + {}^tA\underline{\alpha}C + {}^tBC \, ,$$

on peut écrire

$${}^tUMU = \begin{pmatrix} \underline{\alpha} + R_1 - {}^tR_1 & R_0 + Id \\ {}^tR_0 & \underline{\beta} + R_2 - {}^tR_2 \end{pmatrix} = M + R - {}^tR$$

avec

$$R := \begin{pmatrix} R_1 & R_0 \\ 0 & R_2 \end{pmatrix} .$$

On en déduit que $Tr(W^{-1}R) = Tr(R_0) = \Delta(u)$, ce qu'il fallait démontrer. ■

Avec la définition "matricielle", il est facile de voir que l'invariant de Dickson définit un homomorphisme, comme le précise la proposition suivante.

Proposition 2.1.16 *Soit (V, q) un espace quadratique non dégénéré de dimension $n = 2m$. L'application*

$$\begin{array}{rcl} \Delta : O(V, q) & \longrightarrow & \mathbb{Z}/2\mathbb{Z} \\ u & \longmapsto & \Delta(u) \end{array}$$

est un homomorphisme de groupes.

Preuve : On choisit $\mathcal{B}$ une base de V, et on appelle M une matrice de q dans $\mathcal{B}$, U la matrice de u dans $\mathcal{B}$ et V la matrice de v dans $\mathcal{B}$. On a alors

$$^tUMU = M + R_U - {}^tR_U \text{ avec } R_U \in M_n(F)\,, \tag{2.6}$$

$$^tVMV = M + R_V - {}^tR_V \text{ avec } R_V \in M_n(F)\,. \tag{2.7}$$

On déduit de cela que

$$\begin{array}{rcl} ^t(UV)MUV & = & ^tV^tUMUV \\ & = & ^tV(M + R_U - {}^tR_U)V \text{ d'après (2.6)} \\ & = & M + R_V - {}^tR_V + {}^tVR_UV - {}^tV^tR_UV \text{ d'après (2.7)} \\ & = & M + R_{UV} - {}^tR_{UV}\,, \end{array}$$

en posant $R_{UV} := R_V + {}^tVR_UV$, de sorte que

$$\begin{array}{rcl} \Delta(u \circ v) & = & Tr(W^{-1}R_{UV}) \\ & = & Tr(W^{-1}R_V) + Tr((W^{-1})^tVR_UV) \\ & = & \Delta(v) + Tr((W^{-1})^tVR_UV)\,. \end{array}$$

Mais d'après (2.7), on a $^tVWV = W$, donc

$$\begin{array}{rcl} Tr((W^{-1})^tVR_UV) & = & Tr(V^{-1}W^{-1}(^tV)^{-1t}VR_UV) \\ & = & Tr(V^{-1}W^{-1}R_UV) \\ & = & Tr(W^{-1}R_U) \\ & = & \Delta(u)\,, \end{array}$$

ce qui montre que $\Delta(u \circ v) = \Delta(u) + \Delta(v)$, et que Δ est un homomorphisme. ■

2.1.4 Forme $\widetilde{T}_{E/F}$ et invariant $d^+(E/F)$ d'une algèbre étale

Définition 2.1.17 *Soit E/F une algèbre étale de rang n (i. e. isomorphe à un produit fini d'extensions finies séparables de F). Pour $x \in E$, on note $\widetilde{T}_{E/F}(x)$ le coefficient en degré $n-2$ du polynôme caractéristique de la multiplication par x sur le F-espace vectoriel E. On a donc*

$$\widetilde{T}_{E/F}(x) = \sum_{1 \le i < j \le n} \gamma_i(x)\gamma_j(x)\,,$$

si $\mathrm{Hom}_F(E, F_s) = \{\gamma_i, 1 \le i \le n\}$.

La forme $\widetilde{T}_{E/F}$, souvent notée $T_{2,E/F}$ a été étudiée par de nombreux auteurs : voir [Rev], [Wad], [BM], [Wat], et [KMRT].

On montre facilement qu'elle est *non dégénérée* si n est pair. Dans le cas où n est impair, il y a deux façons d'attacher un espace quadratique non dégénéré à E/F ; prendre $(\mathrm{Ker}(Tr_{E/F}), \widetilde{T}_{E/F})$ — c'est le choix de Revoy, qui est repris par Wadsworth, Waterhouse, et Knus-Merkuriev-Rost-Tignol. On peut aussi prendre $(E', \widetilde{T}_{E'/F})$ avec $E' = E \times F$ — c'est le choix fait par Bergé-Martinet. Plus précisément, on a la définition suivante.

Définition 2.1.18 ([BM], Définition 2.3 page 66) *Le* SIGNE ADDITIF *est défini par*

$$\begin{array}{rcl} \varepsilon : \mathbb{Z} & \longrightarrow & \mathbb{Z}/2\mathbb{Z} \\ k & \longmapsto & 0 \textit{ si } k \textit{ mod } 8 \in \{0,1,2,7\}\,, \\ k & \longmapsto & 1 \textit{ si } k \textit{ mod } 8 \in \{3,4,5,6\}\,, \end{array}$$

et le DISCRIMINANT ADDITIF DE L'ALGÈBRE E/F *est l'élément de* $F/\wp(F)$ *défini par :*

$$d^+(E/F) \overset{def}{=} \mathrm{Arf}\,(\widetilde{T}_{E'/F}) + \varepsilon(n')\,, \ \textit{avec}$$

$$E' = \begin{cases} E & \textit{si} \quad n \textit{ est pair,} \\ E \times F & \textit{si} \quad n \textit{ est impair,} \end{cases} \quad \textit{et } n' = [E' : F]\,.$$

J.-P. Serre voyait en [BM] (qui n'a pas recours aux outils cohomologiques), un analogue (pour les invariants en degré 1) de son article sur l'invariant de Witt ([Se2]). La suite de cette sous-section a pour but de préciser ce point de vue.

Le corps F est toujours de caractéristique 2. Si n est un entier pair, la forme quadratique

$$(x_1, \ldots, x_n) \mapsto T = \sum_{1 \le i < j \le n} x_i x_j$$

est non dégénérée sur F_s^n, et invariante sous l'action évidente du groupe symétrique $\mathfrak{S}_n$ qui consiste à permuter les variables. On a donc un plongement

$$\mathfrak{S}_n \hookrightarrow O_n(F_s, T)$$

du groupe symétrique $\mathfrak{S}_n$ dans le groupe orthogonal $O_n(F_s, T)$ de l'espace (F_s^n, T), qui à $\sigma \in \mathfrak{S}_n$ associe l'automorphisme de F_s^n qui permute la base canonique à l'aide de σ, qu'on notera encore abusivement σ. On notera également

$$T = \begin{pmatrix} 0 & 1 & \ldots & \ldots & 1 \\ 0 & 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \ddots & \ddots & 0 & 1 \\ 0 & \ldots & \ldots & 0 & 0 \end{pmatrix} \in M_n(F)\,,$$

qui est une matrice de la forme T ci-desssus dans la base canonique de F_s^n. Rappelons le résultat suivant, ainsi qu'un schéma de preuve.

Proposition 2.1.19 *Pour n pair, le groupe $H^1(G_F, O_n(F_s, T))$ classe les formes quadratiques non dégénérées de rang n sur F.*

Preuve : (i) Si on se donne un élément $e \in H^1(G_F, O_n(F_s, T))$, c'est en particulier un élément de $H^1(G_F, Gl_n(F_s))$. Or $H^1(G_F, Gl_n(F_s)) = \{1\}$ ([Se1], X, §1, Prop. 3 p. 159), donc e est un cobord. Cela signifie qu'il existe une matrice $M \in Gl_n(F_s)$ telle que pour tout $\gamma \in G_F, e(\gamma) = \gamma(M)M^{-1}$. En écrivant que $e(\gamma) \in O_n(F_s, T)$, on en déduit que que la matrice

$$^tMTM$$

est stable sous l'action de G_F (agissant par évalutation des coefficients), à une matrice alternée près. Elle définit donc la classe d'isomorphisme de la forme quadratique non dégénérée de rang n sur F dont une matrice est ^tMTM.

(ii) Réciproquement, toute classe d'isomorphisme de formes quadratiques non dégénérées sur F de rang n s'obtient par la construction précédente. ■

La forme quadratique non dégénérée qu'on définit (à isomorphisme près) au moyen de l'élément e selon la construction exposée dans le point (i) de la preuve ci-dessus s'appelle la “tordue” de la forme triangulaire T au moyen de e.

Le théorème suivant exprime que si E/F est une algèbre étale de rang n pair, la forme $\widetilde{T}_{E/F}$ est la tordue de la forme triangulaire T au moyen de $e_{E/F}$. C'est une étape essentielle dans la preuve du Théorème 3.

Théorème 2.1.20 *Soit E/F une algèbre étale de degré pair $n = 2m$, et $e_{E/F} \in H^1(G_F, \mathfrak{S}_n)$ qui caractérise E à isomorphisme près. On considère l'application d'ensemble pointés*

$$\phi : H^1(G_F, \mathfrak{S}_n) \longrightarrow H^1(G_F, O_n(F_s, T)),$$

où T est la forme quadratique définie par $(x_1, \dots, x_n) \mapsto \sum_{1\leq i<j\leq n} x_i x_j$. Alors

$$\phi(e_{E/F}) = \widetilde{T}_{E/F}.$$

Preuve : On numérote les éléments de $\mathrm{Hom}_F(E, F_s) = \{\gamma_i, 1 \leq i \leq n\}$ de sorte que

$$e_{E/F}(\gamma)(i) = \gamma \circ \gamma_i \text{ pour } \gamma \in G_F \text{ et } 1 \leq i \leq n.$$

On identifie $e_{E/F}(\gamma) \in \mathfrak{S}_n$ avec son image dans $O_n(F_s, T)$. La preuve de la Proposition 2.1.19 montre que pour établir le présent théorème, il suffit de trouver une matrice $M \in Gl_n(F_s)$ telle que

$$\begin{cases} e_{E/F}(\gamma) = \gamma(M)M^{-1} \text{ pour tout } \gamma \in G_F, \\ ^tMTM \text{ est une matrice de } \widetilde{T}_{E/F}. \end{cases}$$

Or, si $\mathcal{B} = (e_1, \ldots, e_n)$ est une base symplectique pour $\widetilde{T}_{E/F}$, il suffit de prendre

$$M = (\gamma_i(e_j))_{1\le i,j\le n}\,.$$

On obtient alors, en utilisant le fait que $\gamma(M)M^{-1} \in O_n(F_s, T)$, le fait que

$$C := {}^tMTM = D + {}^tB + B\,,$$

où D est une matrice (fixe sous l'action de G_F) de $\widetilde{T}_{E/F}$ dans la base $\mathcal{B}$, et $B \in M_n(F_s)$. Plus précisément, on a

$$C = \left(\sum_{1\le k<l\le n} \gamma_k(e_i)\gamma_l(e_j)\right)_{1\le i,j\le n} \in M_n(F_s)\,,$$

$B = (b_{i,j})_{1\le i,j\le n}$ avec

$$b_{i,j} = \begin{cases} \sum_{1\le k<l\le n} \gamma_k(e_i)\gamma_l(e_j) & \text{si } i > j\,, \\ 0 & \text{si } i \le j\,, \end{cases}$$

et enfin $D = (d_{i,j})_{1\le i,j\le n}$, où

$$d_{i,j} = \begin{cases} 0 & \text{si } i > j\,, \\ \sum_{1\le k<l\le n} \gamma_k(e_i)\gamma_l(e_i) = \widetilde{T}_{E/F}(e_i) & \text{si } i = j\,, \\ \sum_{1\le k<l\le n} (\gamma_k(e_i)\gamma_l(e_j) + \gamma_k(e_j)\gamma_l(e_i)) = b_{\widetilde{T}_{E/F}}(e_i, e_j) & \text{si } i < j\,. \end{cases}$$

Le théorème est donc prouvé. ■

Nous avons défini tous les éléments intervenant dans la preuve du Théorème 3.

2.1.5 L'égalité $j(d^+(E/F)) = \epsilon(e_{E/F})$

Le but ici est de démontrer le Théorème 3 annoncé dans l'introduction, qui compare deux invariants que l'on peut associer à une algèbre étale E/F : l'invariant $d^+(E/F)$ défini via les formes quadratiques (voir sous-section 2.1.4) et l'invariant $\epsilon(e_{E/F})$ via la théorie de Galois (voir sous-section 2.1.1). Nous donnons l'énoncé, puis la preuve du théorème, qui utilise trois lemmes techniques placés ensuite, joints aux résultats de la sous-section 2.1.4. On termine par quelques commentaires sur la preuve qu'on donne et celles qui existent par ailleurs dans la littérature.

Théorème 2.1.21 *Soit E/F une algèbre étale de rang n, et $e_{E/F} \in H^1(G_F, \mathfrak{S}_n)$ caractérisant E à isomorphisme près. Alors, on a dans $H^1(G_F, \mathbb{Z}/2\mathbb{Z})$,*

$$j(d^+(E/F)) = \epsilon(e_{E/F})\,,$$

où $j : F/\wp(F) \overset{\simeq}{\to} H^1(G_F, \mathbb{Z}/2\mathbb{Z})$ est l'isomorphisme donné par la théorie d'Artin-Schreier, $d^+(E/F)$ est le discriminant additif, et

$$\epsilon : H^1(G_F, \mathfrak{S}_n) \to H^1(G_F, \mathbb{Z}/2\mathbb{Z})$$

est l'application induite par la signature.

Preuve : (i) *Cas 1 :* Lorsque $n = 2m$ est pair, on a $\frac{m(m-1)}{2} \equiv \varepsilon(n')$ modulo 2. Il suffit donc de montrer que

$$j\left(\mathrm{Arf}\,(\widetilde{T}_{E/F}) + \frac{m(m-1)}{2}\right) = \epsilon(e_{E/F})\,, \tag{2.8}$$

ce que nous allons faire maintenant. Pour cela, reprenons les notations de la preuve du Théorème 2.1.20. L'égalité

$$D = C + {}^tB + B$$

permet d'écrire, grâce au Lemme 2.1.6,

$$s_2(A^{-1}D) = s_2(A^{-1}C) + \wp(Tr(A^{-1}B))\,, \tag{2.9}$$

où A est la matrice constituée de m blocs diagonaux de la forme $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. D'après le Corollaire 2.1.7, l'image par j du membre de gauche de l'égalité (2.9) est égal au membre de gauche de l'affirmation (2.8). Il s'agit donc de montrer que l'image par j du membre de droite de l'égalité (2.9) est égal au membre de droite de l'affirmation (2.8). Pour cela, il suffit d'établir les faits suivants :

1. Pour tout $\gamma \in G_F$, $\gamma(Tr(A^{-1}B)) - Tr(A^{-1}B)$ est l'invariant de Dickson $\Delta(\gamma(M)M^{-1})$ de l'élément $\gamma(M)M^{-1} \in O_n(F_s, T)$ (Lemme 2.1.22),
2. Pour tout $\gamma \in G_F$, l'invariant de Dickson $\Delta(\gamma(M)M^{-1})$ est la signature $\epsilon(e_{E/F}(\gamma))$ de l'élément $e_{E/F}(\gamma)$ (Lemme 2.1.22),
3. $s_2(A^{-1}C) = 0$ (Lemme 2.1.24),

car il résulte de ceux-ci que dans $F/\wp(F)$, on a

$$j(\wp(Tr(A^{-1}B))) = \epsilon(e_{E/F})\,.$$

En effet, d'après ([Se1], X, §3, a)), l'isomorphisme j est défini par

$$\begin{array}{rcl} j : F/\wp(F) & \longrightarrow & H^1(G_F, \mathbb{Z}/2\mathbb{Z}) \\ a & \longmapsto & (\gamma \mapsto \gamma(x) - x) \text{ avec } x^2 + x = a\,. \end{array}$$

Or on déduit des points 1 et 2 que

$$j(\wp(Tr(A^{-1}B))) = \epsilon(e_{E/F})\,.$$

(ii) *Cas 2 :* L'égalité (2.8) appliquée à $E \times F$ donne

$$j\left(\operatorname{Arf}(\widetilde{T}_{E\times F/F}) + \frac{(m+1)m}{2}\right) = \epsilon(e_{E\times F/F})\,.$$

Or $\epsilon(e_{E\times F/F})) = \epsilon(e_{E/F})$, et $\frac{(m+1)m}{2} \equiv \varepsilon(n')$ modulo 2. On a donc

$$j\left(\operatorname{Arf}(\widetilde{T}_{E'/F}) + \varepsilon(n')\right) = \epsilon(e_{E/F})\,,$$

et le théorème est montré. ■

Lemme 2.1.22 *Si $\Delta(.)$ désigne l'invariant de Dickson, on a*

$$\gamma(Tr(A^{-1}B)) - Tr(A^{-1}B) = \Delta(\gamma(M)M^{-1}) \text{ pour tout } \gamma \in G_F\,.$$

PREUVE : Les notations sont celles de la preuve du Théorème 2.1.20. On a alors

$$\begin{aligned}
{}^t(\gamma(M)M^{-1})T\gamma(M)M^{-1} &= {}^t(M^{-1}){}^t(\gamma(M))T\gamma(M)M^{-1}\\
&= {}^t(M^{-1})\gamma({}^tMTM)M^{-1}\\
&= {}^t(M^{-1})\gamma(D + {}^tB + B)M^{-1}\\
&= {}^t(M^{-1})DM^{-1} + {}^t(M^{-1}){}^t(\gamma(B))M^{-1}\\
&\quad + {}^t(M^{-1})(\gamma(B))M^{-1}\\
&= T + R(\gamma) + {}^t(R(\gamma))\,,
\end{aligned}$$

avec $R(\gamma) = {}^t(M^{-1})(\gamma(B) - B)M^{-1}$. Il suit alors de la Proposition 2.1.14, que

$$\begin{aligned}
\Delta(\gamma(M)M^{-1}) &= Tr((T + {}^tT)^{-1t}(M^{-1})(\gamma(B) - B)M^{-1})\\
&= Tr(M(A^{-1}){}^t(M){}^t(M^{-1})(\gamma(B) - B)M^{-1})\\
&= \gamma(Tr(A^{-1}B)) - Tr(A^{-1}B)\,.
\end{aligned}$$

Pour le passage de la première égalité à la seconde, on utilise le fait que $A = {}^tM({}^tT + T)M$. ■

Lemme 2.1.23 *Avec les notations de la preuve du Théorème 2.1.21, on a dans le groupe $\mathbb{Z}/2\mathbb{Z}$:*

$$\Delta(\gamma(M)M^{-1}) = \epsilon(e_{E/F}(\gamma)) \text{ pour tout } \gamma \in G_F\,,$$

où $\Delta(.)$ est l'invariant de Dickson, et $\epsilon(.)$ est la signature, notée additivement.

PREUVE : C'est essentiellement tautologique car l'égalité

$$\gamma(M)M^{-1} = \epsilon(e_{E/F}(\gamma)) \text{ pour tout } \gamma \in G_F$$

signifie que pour tout $\gamma \in G_F$, la matrice $\gamma(M)M^{-1}$ est la matrice de l'automorphisme orthogonal, noté abusivement $e_{E/F}(\gamma)$, qui permute les vecteurs de la base canonique $(\epsilon_i)_{1\le i\le n}$ de F_s^n à l'aide de la permutation $e_{E/F}(\gamma)$. Cet élément a pour invariant de Dickson $\epsilon(e_{E/F}(\gamma))$, car si $\epsilon(e_{E/F}(\gamma))$ vu comme une permutation, est produit de r transpositions $(i_1, j_1)\cdots(i_r, j_r)$, alors $\epsilon(e_{E/F}(\gamma))$ vu comme automorphisme orthogonal pour T, est le produit $\tau_1\cdots\tau_r$ où τ_k est la transvection orthogonale de vecteur anisotrope $\epsilon_{i_k}+\epsilon_{j_k}$ pour $1\le k\le r$. Or $\Delta(\tau_k)=1$ pour tout $1\le k\le r$ (Lemme 2.1.13) et Δ est un homomorphisme (Lemme 2.1.16), d'où le lemme. ∎

Lemme 2.1.24 *Avec les notations de la preuve du Théorème 2.1.20, on a*

$$s_2(A^{-1}C)=0\,.$$

Preuve : On a $C={}^tM\cdot T\cdot M$, donc $A=C+{}^tC={}^tM(T+{}^tT)M$, d'où

$$s_2(A^{-1}C)=s_2((T+{}^tT)^{-1}T)\,.$$

On observe alors que $(T+{}^tT+Id)^2=0$, donc $T+{}^tT=(T+{}^tT)^{-1}$. On en déduit que

$$s_2((T+{}^tT)^{-1}T)=s_2((T+{}^tT)T)=s_2((T+{}^tT+Id)T+T)\,.$$

D'autre part, on a la relation suivante entre coefficients des polynômes caractéristiques :

$$s_2((T+{}^tT+Id)T+T)-s_2(T)-s_2((T+{}^tT+Id)T)=$$

$$s_1((T+{}^tT+Id)T)s_1(T)-s_1((T+{}^tT+Id)T^2)\,.$$

Comme $T+{}^tT+Id$ est de rang 1, on a $s_2((T+{}^tT+Id)T)=0$. Comme T est nilpotente, $s_1(T)=s_2(T)=0$. Un calcul montre que $s_1((T+{}^tT+Id)T^2)=0$, et donc $s_2(A^{-1}C)=s_2((T+{}^tT)^{-1}T)=s_2((T+{}^tT+Id)T+T)=0$. ∎

L'originalité de cette preuve du Théorème 2.1.21 (et qui la distingue de celle que l'on trouve dans [KMRT]) se trouve dans la façon dont on établit le fait que pout tout $\gamma\in G_F$, $\gamma(Tr(A^{-1}B))-Tr(A^{-1}B)$ est la signature de la permutation $e_{E/F}(\gamma)$: on montre le Lemme 2.1.22. Dans [KMRT] (Proposition (18.24) page 293), les auteurs établissent que pour $1\le r\le n-1$, lorsque $e_{E/F}(\gamma)$ est la transposition $(r, r+1)$, on a $\gamma(Tr(A^{-1}B))=Tr(A^{-1}B)+1$. Ils utilisent pour cela "l'idempotent de séparabilité" de E ([KMRT], Définition (18.9) page 285), c'est-à-dire l'élément de $E\otimes_F E$ qui correspondant à la fonction caractéristique de la diagonale de $\mathrm{Hom}_F(E, F_s)\times\mathrm{Hom}_F(E, F_s)$ sous l'isomorphisme

$$E\otimes_F E\simeq \mathrm{Map}\big(\mathrm{Hom}_F(E, F_s)\times\mathrm{Hom}_F(E, F_s), F_s\big)^{G_F}\,.$$

Il doivent supposer que dans la base $\mathcal{B}$ qui intervient dans la preuve du Théorème 2.1.20, on a $e_1=1$ pour l'argument fonctionne.

La formule (2.8) de la preuve du Théorème 2.1.21 rend compte de la différence qu'il existe entre le discriminant additif (noté $d^+(E/F)$) d'une algèbre étale E/F et son invariant de Arf $\mathrm{Arf}\,(E/F)$, tels qu'ils ont été définis par A.-M. Bergé et J. Martinet. Elle explique la nécessité qu'il y a à introduire le signe additif (qui, d'ailleurs, n'est pas additif, puisque $\varepsilon(3) + \varepsilon(3) \neq \varepsilon(6)$).

La preuve du Théorème 2.1.21 permet de ne pas avoir recours aux relèvements en caractéristique 0, comme c'était le cas dans [BM] et [Wad] ; elle permet aussi de raisonner directement au niveau des algèbres (sans traiter d'abord le cas des extensions), et d'obtenir l'additivité de $d^+(E/F)$ directement à partir de celle du second membre.

L'invariant de Arf tel qu'il était défini par Revoy est, dans le cas du degré impair, l'invariant de Arf de l'espace quadratique $(\mathrm{Ker}(Tr_{E/F}), \widetilde{T}_{E/F})$; il coïncide avec l'invariant de Arf de $(E', \widetilde{T}_{E'/F})$, puisque ces deux espaces diffèrent d'un plan hyperbolique.

Nous terminons par une remarque qui fait la traduction entre ce que nous venons de faire et le Théorème 10 de [Wat] page 219, sans trop rentrer dans le détail des objets mis en jeu.

Remarque 2.1.25 *Si $R = F$ est un corps de caractéristique 2, et $S = F[X]/(f)$ est une algèbre étale donnée par un polynôme séparable. Alors*
(i) l'élément $d(S/R)$ est l'invariant de Berlekamp (voir [Wat] page 215, deuxième paragraphe), i.e. c'est la R-algèbre étale définie par $d^+(f)$ (voir Définition 2.2.1).
(ii) Lorsque n est pair *(donc $n = 2m$), $n - 1$ est inversible dans R donc la formule b) du Théorème 10 de [Wat] s'applique, à savoir :*

$$d(Q_2(\{S\}) = d(S/R)d(Q_2/R) \ \textit{dans}\ H^1(R, \mathfrak{S}_2)\,.$$

Dans cette formule, $d(Q_2\{S\}/R)$ est l'invariant de Arf de la forme trace seconde $\widetilde{T}_{S/R}$ ([Wat], Théorème 9, page 217) et l'élément $d(Q_2/R)$ est une algèbre quadratique qui est décomposée en même temps que $m(m-1)/2$ est pair ([Wat], Exemple 2 page 218). Ceci est à comparer avec la formule (2.8).
(iii) Lorsque n est impair *(donc $n = 2m + 1$), n est inversible dans R, donc la formule c) du Théorème 10 de [Wat], à savoir :*

$$d(Q_2^0(\{S\}) = d(S/R)d(Q_2^0/R) \ \textit{dans}\ H^1(R, \mathfrak{S}_2)\,.$$

Dans cette formule, $d(Q_2\{S\}/R)$ est l'invariant de Arf ([Wat], Théorème 9, page 217) de la forme trace seconde $\widetilde{T}_{S/R}$ restreinte au noyau de la forme trace $Tr_{S/R}$ (qui est l'invariant de Arf de la forme $\widetilde{T}_{S\times R/R}$), et l'élément $d(Q_2/R)$ est une algèbre quadratique qui est décomposée en même temps que $m(m+1)/2$ est pair ([Wat], Exemple 2 page 218). Ceci est à comparer avec la formule du Théorème 2.1.21 dans le cas impair.

La section suivante donne des exemples de calculs de discriminants additifs.

2.2 Calculs de discriminants additifs d'extensions

Il y a trois méthodes au moins pour calculer le discriminant additif d'une extension, mais avant de les détailler, commençons par rappeler une définition et donner un résultat.

Définition 2.2.1 *Soient F un corps de caractéristique 2, $f(X) \in F[X]$ un polynôme irréductible unitaire séparable de degré $n \geq 1$, et $\gamma_1, \dots, \gamma_n$ une liste de ses racines dans une clôture algébrique de F. On appelle* DISCRIMINANT ADDITIF DU POLYNÔME f, *et on note $d^+(f)$, la quantité :*

$$d^+(f) := \sum_{1 \leq i < j \leq n} \frac{\gamma_i \gamma_j}{(\gamma_i + \gamma_j)^2} = \delta^+(f)^2 + \delta^+(f) \text{ où } \delta^+(f) := \sum_{1 \leq i < j \leq n} \frac{\gamma_i}{\gamma_i + \gamma_j}.$$

La quantité $d^+(f)$ a été introduite par E. R. Berlekamp ([Be], où il note $\beta(f)$ l'élément noté ici $\delta^+(f)$). Elle a été reprise par R. Baeza ([B1], où il note $\alpha(f)$ l'élément noté ici $\delta^+(f)$), par P. Revoy ([Rev]) et A. Wadsworth ([Wad]) sous la terminologie d'*Invariant de Berlekamp*. La terminologie de "discriminant additif" est justifiée par le résultat suivant.

Théorème 2.2.2 *Soit E/F une extension finie séparable degré n de corps de caractéristique 2, et $f \in F[X]$ un polynôme irréductible séparable tel que $E \simeq F[X]/(f)$. Alors on a dans $F/\mathcal{P}(F)$:*

$$d^+(E/F) = d^+(f).$$

PREUVE : Soit $e_{E/F} \in H^1(G_F, \mathfrak{S}_n)$ correspondant à E. On vérifie que pour tout $\gamma \in G_F$ on a $\gamma(\delta^+(f)) = \delta^+(f) + \epsilon(e_{E/F}(\gamma))$, et on peut alors appliquer le Théorème 2.1.21, qui permet d'obtenir $j(d^+(E/F)) = j(d^+(f))$ dans $H^1(G_F, \mathbb{Z}/2\mathbb{Z})$. ■

Les trois méthodes de calcul de $d^+(E/F)$ sont alors les suivantes :
– la méthode des relèvements,
– la méthode des polynômes symétriques,
– la méthode s_2.

Nous rentrons maintenant un peu plus dans les détails.

2.2.1 Méthode des relèvements

Elle consiste à calculer un représentant de $d^+(f)$ en se servant de l'énoncé suivant (cf. ([Wad], Lemme 1.6 et Proposition 1.7 pages 239-240), ainsi que ([BM], Théorème 2.6 page 68)) que nous donnons sans démonstration.

Proposition 2.2.3 *Soit E/F une extension étale de corps de caractéristique 2, et $f \in F[X]$ un polynôme irréductible séparable. On relève F en un anneau A de valuation discrète complet de caractéristique 0, de maximal $2A$, et E en la clôture intégrale B de A dans L, extension non ramifiée de K, obtenue comme corps de rupture de $\hat{f} \in K[X]$, relèvement unitaire de f à $A[X]$. Alors*

$$disc(\hat{f}) = \hat{u}^2 + 4\hat{v} \text{ avec } (\hat{u}, \hat{v}) \in A^* \times A \Rightarrow v/u^2 \text{ représente } d^+(f)\,.$$

On est ainsi ramené à calculer un discriminant en caractéristique différente de 2, ce que l'on sait faire rapidement grâce à l'algèbre linéaire. En utilisant les calculs de discriminants génériques effectués par T. Sasaki, Y. Kanada, et S. Watanabe ([SKW]), A.-M. Bergé et J. Martinet ([BM], page 76) ont employé cette méthode pour trouver les valeurs suivantes pour les discriminants additifs.

$f(X)$	$X + a$
$d^+_{BM}(f)$	$0\,[\wp(F)]$

$f(X)$	$X^2 + aX + b$
$d^+_{BM}(f)$	$\dfrac{b}{a^2}\,[\wp(F)]$

$f(X)$	$X^3 + aX^2 + bX + c$
$d^+_{BM}(f)$	$\dfrac{a^3c + b^3 + c^2}{(c + ab)^2}\,[\wp(F)]$

$f(X)$	$X^4 + aX^3 + bX^2 + cX + d$
$d^+_{BM}(f)$	$\dfrac{a^3c^3 + b^3c^2 + c^4 + a^2b^3d + a^4d^2}{(a^2d + abc + c^2)^2}\,[\wp(F)]$

$f(X)$	$X^5 + bX^3 + cX^2 + dX + e$
$d^+_{BM}(f)$	$\dfrac{b^3c^2d^2 + c^4d^2 + c^5e + bc^3de + b^5e^2 + b^3de^2 + e^4}{(c^2d + bce + e^2)^2}\,[\wp(F)]$

Afin de vérifier ces calculs, nous avons calculé le discriminant additif la méthode suivante.

2.2.2 Méthode des polynômes symétriques

Dans cette méthode, c'est encore $d^+(f)$ que l'on va calculer. On commence par faire la remarque suivante.

Remarque 2.2.4 *Avec les notations de la Définition* 2.2.1*, l'élément* $d^+(f)$ *vaut* $R(\gamma_1, \dots, \gamma_n)$*, où* R *est la fraction rationnelle*

$$R(X_1, \dots, X_n) = \sum_{1 \leq i < j \leq n} \frac{X_i X_j}{(X_i + X_j)^2} = \frac{N(X_1, \dots, X_n)}{D(X_1, \dots, X_n)^2}$$

où $D(X_1, \dots, X_n) = \prod_{1 \leq i < j \leq n} (X_i + X_j)$ *et* $N(X_1, \dots, X_n) \in F[X_1, \dots, X_n]$*. Les polynômes* N *et* D *sont symétriques donc s'expriment comme polynômes en* $s_1, \dots, s_n$ *à coefficients dans* F*, disons* N_1 *et* D_1*.*

La méthode des polynômes symétriques consiste alors à chercher l'expression des polynômes N_1 et D_1 de la Remarque 2.2.4, en termes des polynômes symétriques élémentaires, puis de les évaluer modulo 2 en les coefficients du polynôme f.

Donc si $n \geq 1$ un entier, et A est un anneau commutatif unitaire, et si

$$P(X_1, \dots, X_n) \in A[X_1, \dots, X_n]$$

est un polynôme symétrique, on veut trouver son expression comme polynôme en les polynômes symétriques élémentaires

$$s_k = \sum_{1 \leq i_1 < \cdots < i_k \leq n} X_{i_1} \dots X_{i_k}\,, \text{ pour } 1 \leq k \leq n.$$

Pour cela, on implémente l'algorithme classique décrit dans la preuve du Théorème 6.1 de [La] page 191, ce qui donne lieu aux deux fonctions Maple `se` et `sym` dont on trouvera les définitions en Appendice B.

La fonction `se` prend en entrée un entier n suivi d'un entier k (inférieur à n) et renvoie le polynôme s_k.

La fonction `sym` prend en entrée un entier n suivi d'un polynôme symétrique homogène en $x[1], \dots, x[n]$ et l'exprime en fonction de $s[1], \dots, s[n]$.

Par exemple, on peut exprimer $P(X_1, X_2, X_3) = (X_1 + X_2 + X_3)X_1X_2X_3$ en termes des polynômes symétriques élémentaires grâce à l'instruction :

```
> sym(3, (x[1]+x[2]+x[3])*x[1]*x[2]*x[3]);
```

On obtient comme attendu :

```
s[3] s[1]
```

Maintenant que l'on sait écrire les polynômes symétriques (homogènes) en fonction des polynômes symétriques élémentaires, on calcule de façon générique le polynôme D (dont le carré est, modulo 2, le discriminant usuel de f) et le polynôme N qui interviennent dans la Remarque 2.2.4, au moyen des fonctions `sqrtdendiscadd` et `numdiscadd`, dont les définitions sont données dans l'Appendice B.

On exprime ensuite N et D comme polynômes en les polynômes symétriques élémentaires, au moyen de la fonction `sym`. Cela permet d'obtenir les polynômes N_1 et D_1.

Il reste à calculer le quotient N_1/D_1^2 de l'évaluation modulo 2 de ces polynômes en les coefficients de f.

En procédant ainsi, nous avons pu trouver les valeurs suivantes pour les valeurs des discriminants additifs.

$f(X)$	$X+a$
$d^+(f)$	$0\,[\wp(F)]$

$f(X)$	X^2+aX+b
$d^+(f)$	$\dfrac{b}{a^2}\,[\wp(F)]$

$f(X)$	X^3+aX^2+bX+c
$d^+(f)$	$\dfrac{a^3c+b^3+c^2+abc}{(c+ab)^2}\,[\wp(F)]$

$f(X)$	$X^4+aX^3+bX^2+cX+d$
$d^+(f)$	$\dfrac{a^3c^3+b^3c^2+c^4+a^2b^3d+a^4d^2+abc^3+a^3bcd}{(a^2d+abc+c^2)^2}\,[\wp(F)]$

$f(X)$	$X^5+bX^3+cX^2+dX+e$
$d^+(f)$	$\dfrac{b^3c^2d^2+c^4d^2+c^5e+bc^3de+b^5e^2+b^3de^2+e^4+bce^3}{(c^2d+bce+e^2)^2}\,[\wp(F)]$

On peut vérifier si les valeurs qu'on a calculées pour les discriminants additifs $d^+(f)$ sont compatibles avec les valeurs de $d^+_{BM}(f)$, qu'on a rappelées auparavant. C'est ce que l'on fait dans le lemme suivant.

Lemme 2.2.5 *On a les faits suivants :*
(i) si le degré de f est inférieur ou égal à 4, on a $d^+(f) - d^+_{BM}(f) \in \mathcal{P}(F)$,
(ii) si le degré de f est 5, on a $d^+(f) - d^+_{BM}(f) \notin \mathcal{P}(F)$ en général.

PREUVE : Montrons d'abord (i). Dans le cas des *degrés* 1 *et* 2, l'affirmation est évidente. Dans le cas du *degré* 3, il faut vérifier que $x := d^+(f) - d^+_{BM}(f) \in \mathcal{P}(F)$. Or on a

$$x := \frac{abc}{c^2 + a^2b^2} = \frac{t(u+t)}{u^2} \text{ avec } t = c \text{ et } u = c + ab\,.$$

Dans le cas du *degré* 4, il faut vérifier que $x := d^+(f) - d^+_{BM}(f) \in \mathcal{P}(F)$. Or on a

$$x := \frac{abc^3 + a^3bcd}{(abc + da^2 + c^2)^2} = \frac{t(u+t)}{u^2} \text{ avec } t = abc \text{ et } u = abc + c^2 + a^2d\,.$$

Montrons maintenant le point (ii). La différence $x := d^+(f) - d^+_{BM}(f)$ vaut

$$x := \frac{bce^3}{(e^2 + bce + c^2d)^2}\,.$$

En général, $x \notin \wp(F)$. En effet, $x \in \mathcal{P}(F)$ si et seulement si le polynôme $X^2 + (e^2 + bce + c^2d)X + bce^3$ a une racine dans F ; mais si F est le corps à deux éléments, et si $b = c = d = e = 1$, ce dernier polynôme est irréductible sur l'anneau $F[X]$. ■

Le point (ii) du lemme ci-dessus s'explique par la remarque suivante.

Remarque 2.2.6 *Dans la valeur de $d^+_{BM}(f)$ en degré 5, le terme bc^3de a été oublié.*

En effet, le discriminant générique du polynôme $X^5 + bX^3 + cX^2 + dX + e$ s'écrit, modulo 8, $\hat{u}^2 + 4\hat{v}$, avec

$$\hat{u} = e^2 + bce + c^2d \text{ et } \hat{v} = b^3de^2 + b^3c^2d^2 + c^4d^2 + c^5e + e^4 + b^5e^2\,,$$

donc la différence entre v/u^2 et la valeur de $d^+(f)$ que nous trouvons est

$$\frac{bc^3de + bce^3}{(e^2 + bce + c^2d)^2} = \frac{bce(c^2d + e^2)}{(e^2 + bce + c^2d)^2} \in \wp(F)\,.$$

Nous passer maintenant à la méthode s_2.

2.2.3 Méthode s_2

La preuve du Théorème 2.1.21 montre que pour calculer le discriminant additif $d^+(E/F)$, il suffit de calculer la classe modulo $\wp(F)$ de $s_2((M + {}^tM)^{-1}M)$, où M est une matrice de la forme $\widetilde{T}_{E'/F}$. Dans le cas d'une extension E définie par un polynôme séparable $f(X) = X^n + \sum_{i=0}^{n-1} a_i X^i$, l'algorithme de calcul est le suivant, que nous détaillons de façon à rendre plus lisibles les définitions des trois fonctions Maple `formettilde, formebinttilde, matttilde` et `ds2` (voir Appendice B) qui en constituent une partie de l'implémentation.

1) En notant θ une racine de f telle que $E = F(\theta)$, tout élément u de E' s'écrit

$$\begin{array}{lll} \sum_{i=0}^{n-1} u_i\theta^i & \text{si} & n \text{ est pair,} \\ \\ (\sum_{i=0}^{n-1} u_i\theta^i, u_n) & \text{si} & n \text{ est impair,} \end{array}$$

avec $(u_0, \ldots, u_n) \in F^{n+1}$. On calcule la forme $\widetilde{T}_{E'/F}$ évaluée en $u \in E'$. C'est ce que fait la fonction `formettilde(f,x,u)` (voir Appendice B).

2) Avec les mêmes notations, on calcule la forme bilinéaire associée $b_{\widetilde{T}_{E'/F}}$ en $(u, v) \in E' \times E'$. C'est ce que fait la fonction `formebinttilde(f,x,u,v)` (voir Appendice B).

3) On peut, en subsituant à u et v dans les expressions trouvées en 1) et 2) les valeurs adéquates, construire une matrice M de la forme $\widetilde{T}_{E'/F}$ dans la base

$$\mathcal{B}' = \left\{ \begin{array}{rll} (1, \theta, \ldots, \theta^{n-1}) & \text{si} & n \text{ est pair,} \\ ((1, 0), (\theta, 0), \ldots, (\theta^{n-1}, 0), (0, 1)) & \text{si} & n \text{ est impair.} \end{array} \right.$$

C'est ce que fait la fonction `matttilde(f,x)` (voir Appendice B).

4) Maple dispose alors de toutes les fonctions nécessaires pour nous permettre de calculer $s_2((M + {}^tM)^{-1}M)$. La fonction `ds2(m)` (voir Appendice B) effectue ce calcul.

5) On peut vérifier que la valeur trouvée pour $s_2((M + {}^tM)^{-1}M)$ est la même, modulo $\wp(F)$, que celle trouvée pour $d^+(f)$ par la méthode des polynômes symétriques. Pour cela, désignons par x la différence entre les deux quantités. On écrit $x = p/q^2$, où p et q sont des polynômes en les coefficients de f, à coefficients dans $\mathbb{F}_2$. La propriété $x \in \wp(F)$ est alors équivalente à celle, pour le polynôme $T^2 + qT + p$, de se factoriser en deux polynômes de degré 1 en T. L'instruction Maple `Factors(t^2+q*t+p) mod 2` permet de tester cette propriété.

Cela dit, on trouvera en Appendice C, les résultats qui montrent que les calculs effectués par les deux dernières méthodes sont cohérents. Il faut mentionner que la méthode des relèvements est la meilleure. Pourtant c'est la méthode de polynômes symétriques qui nous a incité à implémenter la fonction `sym`, chose qui n'est pas inutile, puisque cette fonction n'est pas prédéfinie dans les versions courantes de Maple. Mentionnons aussi que c'est le travail sur la méthode s_2

qui nous a fait découvrir une erreur concernant la formule de développement du pfaffien (voir Appendice D).

2.3 Invariants dans le groupe $H^1(G_F, F_s^*/F_s^{*2})$

Le second invariant que l'on associe habituellement à une algèbre étale E/F sur un corps F *de caractéristique différente de* 2 est son invariant de Witt, c'est-à-dire l'invariant de Witt de la forme $x \mapsto Tr_{E/F}(x^2)$, à valeurs dans le sous-groupe $\mathrm{Br}_2(F)$ des éléments du groupe de Brauer $\mathrm{Br}(F)$ dont l'ordre divise 2, qui s'identifie au groupe $H^2(G_F, \mathbb{Z}/2\mathbb{Z})$. Cet invariant de Witt s'interprète en termes d'algèbre de Clifford.

Par analogie, l'invariant que l'on peut "spontanément" associer à une algèbre étale E/F sur un corps F *de caractéristique* 2 est son invariant de Clifford, c'est-à-dire l'invariant de Clifford (voir sous-section 2.3.1) de l'espace quadratique non dégénéré $(E', \widetilde{T}_{E'/F})$, à valeurs dans le sous-groupe $\mathrm{Br}_2(F)$ des éléments du groupe de Brauer $\mathrm{Br}(F)$ dont l'ordre divise 2, qui s'identifie cette fois au groupe $H^1(G_F, F_s^*/F_s^{*2})$ (voir par exemple [Ara], page 256), toujours à cause de la suite exacte longue de cohomologie galoisienne associée à la suite d'Artin-Schreier.

Malheureusement cet invariant est trivial (voir [BM], Théorème 3.5 et Corollaire 3.6 pages 70-71). On le retrouve ici en exhibant l'argument intrinsèque : la forme $\widetilde{T}_{E'/F}$ préserve les carrés (voir Proposition 2.3.6). Dans la sous-section 2.3.3, on se sert de la norme spinorielle pour tenter de construire un autre invariant (Théorème 2.3.11).

2.3.1 L'invariant de Clifford

Le Lemme 2.3.1 (déjà donné dans la sous-section 2.1.3) et le Lemme 2.3.1 qui suivent justifient la Définition de l'invariant de Clifford $c(V, q)$ d'un espace quadratique non dégénéré (Définition 2.3.3), puis d'une algèbre étale (Définition 2.3.4).

Lemme 2.3.1 *Soit $(e_1, f_1, \dots, e_m, f_m)$ une base symplectique d'un espace quadratique non dégénéré (V, q) de dimension $n = 2m$. Alors*
(i) Les éléments

$$e_1^{k_1} f_1^{l_1} \dots e_m^{k_m} f_m^{l_m} \text{ avec } 0 \leq k_i, l_i \leq 1 \text{ pour } 1 \leq i \leq m$$

forment une base de $C(V, q)$.
(ii) On a les relations

$$e_i e_i = q(e_i)\,, f_i f_i = q(f_i)\,,$$

$$e_i e_j = e_j e_i\,, f_i f_j = f_j f_i, \text{ et } e_i f_j + f_j e_i = \delta_{i,j}$$

pour $1 \leq i, j \leq m$.

(iii) On a l'isomorphisme

$$C(V,q) \simeq \bigotimes_{i=1}^{m} C(F \times F, q(e_i)x^2 + xy + q(f_i)y^2)\,.$$

Lemme 2.3.2 *Si (V,q) est un espace quadratique non dégénéré de dimension 2, de base symplectique (e,f), et si $a = q(e)$ et $b = q(f)$. Alors l'algèbre $C(V,q)$ est isomorphe à l'algèbre de quaternions $[\Delta, a)$ où $\Delta = ab$.*

PREUVE : Dans $C(V,q)$, on a $e^2 = a$, $f^2 = b$ et $ef + fe = 1$. Il suffit donc de poser poser $x = ef$ et $y = e$ pour voir $C(V,q)$ est isomorphe à l'algèbre de rang 4 dont une base sur F est $\{1, x, y, xy\}$ avec les relations : $x^2 + x = \Delta$, $y^2 = a$ et $xy + yx = y$. C'est, par définition, l'algèbre de quaternions notée $[\Delta, a)$. ■

En mettant bout à bout les deux lemmes précédents, on voit que $C(V,q)$ est isomorphe à un produit tensoriel d'algèbres de quaternions, d'où la définiton suivante.

Définition 2.3.3 *D'après le Lemme 2.3.1 et le Lemme 2.3.2, l'algèbre $C(V,q)$ est une algèbre centrale simple sur F. On appelle* INVARIANT DE CLIFFORD *et on note $c(V,q)$ la classe de $C(V,q)$ dans la 2-torsion du groupe de Brauer $\mathrm{Br}_2(F)$.*

Définition 2.3.4 *Soit E/F une algèbre étale de rang n. On pose*

$$E' := \begin{cases} E & \text{si} \quad n \text{ est pair,} \\ E \times F & \text{si} \quad n \text{ est impair.} \end{cases}$$

*L'*INVARIANT DE CLIFFORD *de E/F est*

$$c(E/F) := c(E', \widetilde{T}_{E'/F})\,,$$

où pour $x \in E'$, $\widetilde{T}_{E'/F}(x)$ est le coefficient en degré $[E' : F] - 1$ du polynôme caractéristique de la multiplication par x sur E'.

2.3.2 Un critère de trivialité

On dégage un critère de trivialité de l'invariant de Clifford (Proposition 2.3.6) ; c'est l'argument intrinsèque implicitement utilisé par A.-M. Bergé et J. Martinet ([BM]) pour montrer la trivialité de l'invariant de Clifford d'une algèbre étale (voir Théorème 2.3.7).

Proposition 2.3.5 *Soit (V,q) un espace quadratique non dégénéré de dimension 2. Alors*

$$c(V,q) = 0 \Leftrightarrow \exists v \in V \mid q(v) = 1\,.$$

Preuve : On sait que la classe de l'algèbre $[\Delta, a)$ est triviale si et seulement si l'invariant de Arf de (V, q) est nul, ou si a est norme de l'extension $F(x)/F$ avec $x^2 + x = \Delta$. Mais si Arf (V, q) est nul, la forme q représente 1 sur V puisqu'elle est hyperbolique, et si a est norme de l'extension $F(x)/F$ avec $x^2 + x = \Delta$, alors il existe $(\lambda, \mu) \in F \times F$ tels que $a = \lambda^2 + \lambda\mu + ab\mu^2$, donc

$$\begin{aligned} q(\frac{\lambda}{a}e + \mu f) &= a\left(\frac{\lambda}{a}\right)^2 + \frac{\lambda}{a}\mu + b\mu^2 \\ &= \frac{\lambda^2 + \lambda\mu + ab\mu^2}{a} \\ &= 1\,, \end{aligned}$$

ce qui prouve le lemme. ■

Proposition 2.3.6 *Soit E/F une algèbre de rang $2m$, munie d'une forme quadratique $q : E \to F$ non dégénérée satisfaisant*

$$q(x^2) = q(x)^2 \text{ pour tout } x \in E.$$

Alors l'invariant de Clifford de (E, q) est nul.

Preuve : Soit $(e_1, f_1, \ldots, e_m, f_m)$ une base du F-espace vectoriel E, symplectique pour q. Puisque la forme q est non dégénérée, elle représente un élément non nul de F sur chaque plan $P_i := Fe_i \oplus Ff_i$ pour $1 \leq i \leq m$, en un point qu'on notera x_i. Maintenant, pour $1 \leq i \leq m$, on complète le vecteur x_i de P_i en une base (x_i, y_i) de P_i. Comme q préserve les carrés, les plans (x_i^2, y_i^2) sont deux-à-deux orthogonaux pour q, et l'on a $q(q(x_i)^{-1}x_i^2) = 1$. Il suit alors de ce qui précède que $c(V, q) = 0$. ■

Théorème 2.3.7 *Soit E/F une algèbre étale de rang n. L'invariant de Clifford $c(E/F)$ est trivial.*

Preuve : La forme $\widetilde{T}_{E'/F}$ préserve les carrés, donc la Proposition 2.3.6 s'applique. ■

2.3.3 La norme spinorielle

On est donc amené à rechercher pour l'algèbre étale E/F, d'autres invariants dans le groupe $H^1(G_F, F_s^*/F_s^{*2})$. Une tentative naturelle consiste à utiliser la norme spinorielle dont nous rappelons la définition ci-après, mais à nouveau, celle-ci est infructueuse (Théorème 2.3.11).

C'est le théorème suivant qui nous sert à définir la norme spinorielle.

Théorème 2.3.8 *Soit (V, q) un espace quadratique non dégénéré tel que le groupe $O(V, q)$ soit engendré par les transvections orthogonales (cf. Appendice A). Alors (i) Pour $u \in O(V, q)$, il existe un unique $s_u \in C(V, q)$ (resp. $s_u \in C^+(V, q)$ inversible), déterminé à un scalaire près, tel que*

$$u(x) = s_u x {s_u}^{-1} \text{ pour tout } x \in V .$$

(ii) Pour tout élément inversible $s \in C(V, q)$ (resp. $s \in C^+(V, q)$) tel que $sVs^{-1} = V$, l'application $x \mapsto sxs^{-1}$ définit un élément de $O(V, q)$ (resp. de $O^+(V, q)$).

PREUVE : (i) Supposons que u soit une transvection orthogonale, c'est-à-dire qu'il existe $v \in V$ anisotrope, tel que

$$u(x) = x + \frac{b_q(x, v)}{q(v)} v \text{ pour } x \in V .$$

Alors $u(x) = x + (xv + vx)v^{-2}v = vxv^{-1}$ et $s = v$ convient. En général, lorsque u est produit de p transvections orthogonales $\tau_{v_1}, \dots, \tau_{v_p}$ par rapport à des vecteurs non isotropes $v_1, \dots, v_p$, on peut prendre $s = v_1 \cdots v_p$. Comme $u \in O^+(V, q)$ si et seulement si p est pair, $u \in O^+(V, q)$ si et seulement si $s_u \in C^+(V, q)$. Si s et s' sont tels que $sxs^{-1} = s'xs'^{-1}$ pour tout $x \in V$, on voit que $s'^{-1}s$ appartient au centre de $C(V, q)$ et à celui de $C^+(V, q)$, donc est dans F^*. (ii) On a $q(sxs^{-1}) = sxs^{-1}sxs^{-1} = sxxs^{-1} = sq(x)s^{-1} = q(x)ss^{-1} = q(x)$ donc $u \in O(V, q)$. Si $s \in C^+(V, q)$ et si $u \notin O^+(V, q)$, il existe, d'après (i), $r \in C(V, q) \setminus C^+(V, q)$ tel que $sxs^{-1} = rxr^{-1}$ pour tout $x \in V$; mais alors s et r sont proportionnels, ils doivent donc appartenir à $C^+(V, q)$ en même temps : contradiction! ■

Définition 2.3.9 *Soit (V, q) un espace quadratique non dégénéré, tel que le groupe $O(V, q)$ soit engendré par les transvections orthogonales (voir Appendice A). L'homomorphisme*

$$\begin{array}{rcl} \overline{\theta} : O(V, q) & \longrightarrow & F^*/F^{*2} . \\ u & \longmapsto & s_u(s_u)^J = q(v_1) \cdots q(v_{2p}) \end{array}$$

(où s_u est l'élément associé à u dans le théorème précédent, et J est l'anti-involution canonique de $C(V, q)$) s'appelle la NORME SPINORIELLE.

Lemme 2.3.10 ([Di2], §10, 6),8) pages 66-67) *Dans les énoncés suivants, on note θ la restriction de $\overline{\theta}$ à $O^+(V, q)$,*
(i) Le noyau $\operatorname{Ker} \theta$ contient le sous-groupe $D(O^+(V, q))$ des commutateurs de $O^+(V, q)$.
(ii) L'image $\operatorname{Im} \theta$ est le sous-groupe de F^*/F^{*2} des classes des éléments de la forme $q(v)q(v')$ avec $(v, v') \in V \times V$ anisotropes pour q.
(iii) Si $n \geq 2$ et si l'indice de (V, q) (dimension commune des sous-espaces totalement isotropes maximaux) est supérieur à 1, on a une suite exacte

$$1 \longrightarrow D(O^+(V, q)) \longrightarrow O^+(V, q) \xrightarrow{\theta} F^*/F^{*2} \longrightarrow 1 .$$

Preuve : Le point (i) résulte de ce que $D(O^+(V,q))$ est abélien.

Pour (ii), tout élément de l'image est un produit de telles classes. Pour la réciproque, noter que $q(v)q(v') = \theta(t_v t_{v'})$.

Pour (iii), l'hypothèse sur l'indice signifie qu'il existe un plan $P = (e_1, f_1)$ hyperbolique, que l'on complète en une base $\mathcal{B}$ symplectique pour q. Si $\lambda \in F^*$, on note u l'élément de $O(V,q)$ tel que $u(e_1) = \lambda e_1$, $u(f_1) = \lambda^{-1} f_1$, et u induit l'identité sur l'orthogonal de (e_1, f_1). On vérifie alors que $u = \tau_{\lambda e_1 + f_1} \tau_{e_1 + f_1}$ d'où $\theta(u) = \lambda$ modulo F^{*2}, donc θ est *surjective*. Pour obtenir l'*injectivité*, on procède ainsi : V contient le plan hyperbolique P, on montre que d'une part $D(O^+(V, q_{|P})) = \operatorname{Ker} \theta_{|O^+(V, q_{|P})}$, et que d'autre part $q(P) = q(V)$ (égal à F) et $D(O^+(V, q_{|P})) = \operatorname{Ker} \theta_{|O^+(V, q_{|P})}$ entraînent $D(O^+(V,q)) = \operatorname{Ker} \theta$ ([O'M], §55 page 137). ■

Pour trouver un invariant $H^1(G_F, F_s^*/F_s^{*2})$ pour les algèbres étales de rang n, on peut essayer d'abord de construire une application $\mathfrak{S}_n$ dans F_s^*/F_s^{*2}, mais cela ne donne rien, comme le montre le théorème suivant.

Théorème 2.3.11 *On considère l'homomorphisme*

$$f : \mathfrak{S}_n \longrightarrow F_s/F_s^{*2}$$

où pour $\sigma \in \mathfrak{S}_n$, $f(\sigma)$ désigne la norme spinorielle de la rotation $r(\sigma)$ du groupe orthogonal $O_{2n}(F_s)$ définie par :

$$r(\sigma)(e_{2i-1}) = e_{2\sigma(i)-1} \text{ et } r(\sigma)(e_{2i}) = e_{2\sigma(i)} \text{ pour } 1 \leq i \leq n\,.$$

Alors, pour tout $\sigma \in \mathfrak{S}_n$ on a $f(\sigma) = 1$.

Preuve : Il suffit de prouver le résultat pour les transpositions, ce qui permet de supposer que $n = 2$. Si σ est la transposition $(1, 2)$, la matrice de $r(\sigma)$ dans la base $\mathcal{B} = (e_1 + e_3, e_2 + e_4, e_1, e_4)$ est (avec un abus de notation)

$$\sigma = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

On définit pour $\lambda \in F_s^*$, les matrices

$$\sigma_\lambda = \begin{pmatrix} 1 & 0 & \lambda & 0 \\ 0 & 1 & 0 & \lambda \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \text{ et } t_\lambda = \begin{pmatrix} \lambda & 0 & 0 & 0 \\ 0 & \lambda & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

et on montre les formules

$$t_\lambda \sigma {t_\lambda}^{-1} = \sigma_\lambda \text{ et } \sigma_{\lambda+\mu} = \sigma_\lambda \sigma_\mu \text{ pour } (\lambda, \mu) \in F_s^*\,.$$

On en déduit que si $j \in F_s^*$ est tel que $j^2 + j = 1$, alors $\sigma_{j^2} = \sigma_j \sigma$, puis $\sigma_{j^2} = t_{j^2} t_j{}^{-1} \sigma_j t_j t_{j^2}{}^{-1}$, soit $\sigma_{j^2} = t_{j^2}{}^2 \sigma_j t_{j^2}{}^{-2}$. De cela on conclut que

$$\sigma = \sigma_j t_{j^2}{}^2 \sigma_j{}^{-1} t_{j^2}{}^{-2}$$

est un commutateur, donc sa norme spinorielle est triviale. ■

2.4 Conclusion et questions ouvertes

Dans ce chapitre nous avons étudié deux invariants dans le groupe $H^1(G_F, \mathbb{Z}/2\mathbb{Z})$ que l'on peut associer à une algèbre étale E/F de rang n sur un corps F de caractéristique 2 : l'image $j(d^+(E/F))$, par le cobord j de la suite exacte d'Artin-Schreier de son discriminant additif $d^+(E/F) \in F/\wp(F)$ défini en utilisant les formes quadratiques ; l'image $\epsilon(e_{E/F})$ par la signature d'un homomorphisme continu $e_{E/F} : G_F \to \mathfrak{S}_n$. Ces deux invariants coïncident (Théorème 2.1.21).

On ne sait toujours pas si l'on peut attacher E/F un invariant non trivial dans $H^1(G_F, F_s^*/F_s^{*2})$.

Pour tout entier $r \geq 0$, on note $\bigwedge^r M$ le quotient de $\bigotimes^r M$ par le sous-module engendré par les tenseurs décomposés possédant deux composantes identiques.

On note $x_1 \wedge \cdots \wedge x_r$ l'image de $x_1 \otimes \cdots \otimes x_r$.

Lorsque M est libre de rang n, alors $\bigwedge^r M$ est réduit à $\{0\}$ si $r > n$ et est de rang $\binom{n}{r}$ pour $0 < r \leq n$. De plus si M est muni d'une forme bilinéaire $(x, y) \mapsto f(x, y)$, on peut montrer ([Bo2], §2, Proposition 6) qu'il existe sur $\bigwedge^r M$ une unique forme bilinéaire vérifiant l'identité

$$\bigwedge^r f(x_1 \wedge \cdots \wedge x_r, y_1 \wedge \cdots \wedge y_r) = \det\left(f(x_i, y_j)\right)_{1 \leq i,j \leq r}.$$

Ceci s'applique en particulier au cas où $M = E$ est une algèbre étale de rang n sur un corps F de caractéristique *différente* de 2, muni de la forme bilinéaire $(x, y) \mapsto Tr_{E/F}(xy)$, et J.-P. Serre démontre alors le théorème suivant, qui m'a été communiqué par G. Berhuy.

Théorème 2.4.1 ([BF], §1,Théorème 1) *Soit F un corps de caractéristique* différente *de 2, et $E \mapsto q_E$ un invariant quadratique d'algèbres étales de rang n sur F. Alors*

$$q_E \simeq \sum_{i=0}^{m} \lambda_i \bigwedge^i Tr_{E/F},$$

où m est la partie entière de $n/2$ et $\lambda_1, \ldots, \lambda_m$ sont des formes quadratiques sur F.

On ignore si le résultat analogue en caractéristique 2 où on remplacerait la forme bilinéaire $(x, y) \mapsto Tr_{E/F}(xy)$ par la forme bilinéaire $(x, y) \mapsto \widetilde{T}_{E/F}$ peut être établi.

En tout cas, si le corps de base F n'est pas parfait, le groupe $H^1(G_F, F_s^*/F_s^{*2})$ n'est pas trivial a priori, et l'utilisation des méthodes qu'a developpées K. Kato dans [Kat] (reprises dans [CT]) pour démontrer un analogue de la conjecture de Milnor en caractéristique 2 semble être indispensable pour exhiber un invariant dans $H^1(G_F, F_s^*/F_s^{*2})$ pour les algèbres étales qui serait non trivial.

Appendice A

Le théorème de Cartan-Dieudonné en caractéristique 2

Le théorème suivant, dû à E. Cartan et J. Dieudonné, donne des générateurs simples pour le groupe orthogonal d'un espace quadratique non dégénéré sur un corps de caractéristique 2.

Théorème A.0.2 *Soit* (V, q) *un espace quadratique non dégénéré. Rappelons que la transvection orthogonale* t_x *de vecteur anisotrope* v *est définie par la formule*

$$t_v(x) = x + \frac{b_q(x, v)}{q(v)} v \text{ pour } x \in V ,$$

et notons $T(V, q)$ *le sous-groupe de* $O(V, q)$ *engendré par ces transvections. Alors*
(i) $O(V, q) = T(V, q)$ *sauf si* $\dim V = 4$, $F = \mathbb{F}_2$ *et* (V, q) *est hyperbolique ;*
(ii) $[O(V, q) : T(V, q)] = 2$ *si* $\dim V = 4$, $F = \mathbb{F}_2$ *et* (V, q) *est hyperbolique.*

Une preuve se trouve dans ([Che], chapitre 1, pages 14-21). Nous la reproduisons ici, de façon à bien mettre en relief sa structure, et le niveau où intervient la discussion qui mène au cas exceptionnel (ii) ci-dessus.

Définition A.0.3 *Soit* (V, q) *un espace quadratique non dégénéré.*
(i) Un sous-espace W *de* V *est* TOTALEMENT ISOTROPE *si* $W \subset W^\perp$ *;*
(ii) Un sous-espace W *de* V *est* TOTALEMENT SINGULIER *si il est totalement isotrope et si* q *s'annule sur* W.
(ii) Un élément $u \in O(V, q)$ *est* SINGULIER *si l'image de l'application*

$$\begin{array}{rcl} \phi_u : V & \longrightarrow & V \\ x & \longmapsto & u(x) - x \end{array}$$

est un sous-espace totalement singulier.

Lemme A.0.4 *Soit (V, q) un espace quadratique non dégénéré, et $u \in O(V, q)$. Alors*

$$\phi_u(V) = (\operatorname{Ker} \phi_u)^\perp .$$

PREUVE : Soit $y \in \phi_u(V)$ et $x \in \operatorname{Ker} \phi_u$. Alors il existe $v \in V$ tel que $y = u(v) - v$ et

$$\begin{aligned} b_q(y, x) &= b_q(u(v) - v, x)\,, \\ &= b_q(u(v), x) - b_q(v, x)\,, \\ &= b_q(u(v), u(x)) - b_q(v, x)\,, \\ &= 0\,, \end{aligned}$$

Ainsi $\phi_u(V) \subset \operatorname{Ker} \phi_u{}^\perp$, avec égalité puisque $\dim \phi_u(V) = \dim V - \dim \operatorname{Ker} \phi_u = \dim(\operatorname{Ker} \phi_u)^\perp$. ■

Proposition A.0.5 *Soit $u \in O(V, q)$. Alors il existe $t \in T(V, q)$ tel que $t \circ u$ soit singulier.*

PREUVE : Si u n'est pas singulier, il existe $z \in V$ non singulier tel que $z = u(x) - x$. Soit t_z la transvection orthogonale de vecteur z. Alors on vérifie $q(z) = b_q(z, x)$ et $t_z(u(x)) = x$, donc $x \in \operatorname{Ker} \phi_{t_z u}$.

Notons $H = (Fz)^\perp$. On a $z \in \phi_u(V)$ donc $\phi_u(V)^\perp \subset (Fz)^\perp$, et par le lemme précédent, $\phi_u(V)^\perp = \operatorname{Ker} \phi_u$, donc $\operatorname{Ker} \phi_u \subset H$.

Ainsi on a $\dim \operatorname{Ker} \phi_{t_z u} > \dim \operatorname{Ker} \phi_u$ puisque $\operatorname{Ker} \phi_u + Fx \subset \operatorname{Ker} \phi_{t_z u}$.

En répétant ce procédé, on obtient un élément $t \in T(V, q)$ tel que $\dim \operatorname{Ker} \phi_{tu}$ est maximale donc $\phi_{tu}(V)$ est totalement singulier, et $t \circ u$ est singulier, ce qu'il fallait démontrer. ■

Proposition A.0.6 *Soit (V, q) un espace quadratique non dégénéré. Alors étant donnés deux sous-espaces totalement singuliers N et N', il existe un élément $u \in T(V, q)$ tel que $u(N') = N$.*

PREUVE : On peut supposer que $l := \dim_F(N \cap N') < \dim_F N$ (sinon on a $N = N'$ et $u = \mathrm{Id}$ convient).

On commence par montrer qu'il existe hyperplan H tel que $H^\perp$ contient un vecteur z non isotrope tel que $\dim_F(t_z(N') \cap N) > l$. En effet, puisque $\dim(N + N') > \dim N'$, le sous-espace $N + N'$ n'est pas totalement singulier, et il existe alors un vecteur $z = x + x'$ avec $x \in N$, $x' \in N'$. Puisque $q(z) = b_q(x, x') \neq 0$, on a $x \notin N'$. Soit $H := (Fz)^\perp$. Alors

$$t_z(x') = x' - b_q(x, x')^{-1} b_q(x, x') z = -x \in N\,.$$

D'autre part, si $x'' \in N \cap N'$, on a

$$b_q(x, x'') = b_q(x', x'') = b_q(z, x'') = 0\,,$$

et on déduit de cela que $x'' = t_z(x'') \in t_z(N')$, puis que $Fx + N \cap N' \subset N \cap t_z(N')$.

Maintenant, le sous-espace $t_z(N')$ est totalement singulier maximal.

Si $\dim(t_z(N') \cap N) = \dim N$, on a donc terminé.

Sinon, c'est qu'on a $\dim(t_z(N') \cap N) < \dim N$, et en itérant le procédé, on trouve u, produit de transvections orthogonales, tel que $\dim(u(N') \cap N) = \dim N$. Puisque que $u(N') \cap N$ et N sont des sous-espaces totalement singuliers maximaux, cela entraîne que $u(N') = N$. ■

Proposition A.0.7 *Soit (V, q) un espace quadratique non dégénéré, N un sous-espace totalement singulier maximal, et P un sous-espace totalement singulier maximal tel que $P \oplus N = V$. On définit H par*

$$H = \{s \in O(V, q) \mid s(x) = x \text{ pour tout } x \in N\}.$$

Alors, on a les faits suivants.
(i) Pour $s \in H$ et $x \in V$, on a $s(x) - x \in N$.
(ii) L'application

$$\begin{array}{rcl} H & \xrightarrow{\alpha} & \mathrm{Alt}(P \times P) \\ s & \longmapsto & [(y, y') \mapsto b_q(y, s(y'))] \end{array}$$

est un isomorphisme de groupe de H sur le groupe additif $\mathrm{Alt}(P \times P)$ des formes alternées sur $P \times P$.
(iii) Pour tout $s \in H$, le rang de $\alpha(s)$ est égal à la dimension $\dim(s - \mathrm{Id})(V)$.
(iv) Si les images de $(s, s') \in H \times H$ par α ont des rangs égaux, alors il existe $t \in O(V, q)$ tel que $s' = tst^{-1}$.

PREUVE : Montrons (i). Pour $x \in V$, on a $s(x) - x \in \mathrm{Im}(\phi_s(V)) = (\mathrm{Ker}\,\phi_s)^\perp$ par le Lemme A.0.4. Comme $N \subset \mathrm{Ker}\,\phi_s$, on a $(\mathrm{Ker}\,\phi_s)^\perp \supset N^\perp = N$, puisque N est totalement singulier.

Montrons (ii). Pour $s \in H$, l'application $\alpha(s)$ est bilinéaire ; elle est *alternée*, car si $y \in P$, qui est un sous-espace singulier, on a $q(y) = 0$ puis $q(s(y)) = 0$ donc on en déduit

$$\alpha(s)(y, y) = b_q(y, s(y)) = q(s(y) - y) = 0,$$

car $s(y) - y \in N$.

Le fait que α est un *homomorphisme* résulte des égalités

$$\begin{array}{rcl} (ss')(y') - y' & = & s(s'(y') - y') - s(y') - y' \\ & = & s'(y') - y' + s(y') - y' \text{ (par (i))}, \end{array}$$

ainsi que du fait que $b_q(y, y') = 0$.

Montrons que α est *injectif* : si $\alpha(s) = 0$ alors $b_q(y, s(y')) = 0$ pour tous $(y, y') \in P \times P$, donc $b_q(y, s(y') - y') = 0$ donc $s(y') - y' \in P^\perp = P$. Mais $s(y') - y' \in N$, donc $s(y') - y' = 0$, ceci pour tout $y' \in P$. Alors s fixe N et P donc c'est l'identité de V.

Montrons que α est *surjectif.* Soit $a \in \mathrm{Alt}(P \times P)$. L'application $x \mapsto (y \mapsto b_q(x, y)$ définit un isomorphisme de N sur le dual de P. Donc pour tout $y' \in P$, il existe un unique $u(y') \in N$ tel que

$$b_q(y, u(y')) = a(y, y') \text{ pour tout } y \in P\,.$$

La formule $y' \mapsto u(y')$ définit alors une application linéaire de P dans N, que l'on prolonge en un automorphisme s de V par

$$s(x + y) = x + y + u(y)\,,\ x \in N,\ y \in P,$$

qui est dans H et satisfait $a = \alpha(s)$, donc α est surjectif.

On montre (iii) et et (iv) simultanément. Etant donné $s \in H$, on note $2r$ le rang de $\alpha(s)$. Il existe une base $(y_i)_{1\leq i\leq m}$ de P telle que

$$\alpha(s)(y_i, y_j) = \begin{cases} 1 & \text{si } \{i, j\} = \{2k - 1, 2k\} \text{ pour } 1 \leq k \leq r \\ 0 & \text{sinon.} \end{cases}$$

On définit alors $(y_i)_{1\leq i\leq m}$ par la propriété, pour $k \leq r$, que

$$\begin{array}{rcl} x_{2k-1} & = & u(y_{2k})\,, \\ x_{2k-1} & = & u(y_{2k-1})\,. \end{array}$$

On vérifie alors que $b_q(x_i, y_j) = \delta_{i,j}$ pour $1 \leq i, j \leq 2r$.

On complète $(x_1, \dots, x_{2r})$ en une base $(x_i)_{1\leq i\leq m}$ de N telle que

$$b_q(x_i, y_j) = \delta_{i,j} \text{ pour } 1 \leq i, j \leq m\,.$$

Les bases $(x_i)_{1\leq i\leq m}$ et $(y_i)_{1\leq i\leq m}$ satisfont alors

$$\left\{\begin{array}{rcl} s(y_{2k-1}) & = & y_{2k-1} + x_{2k} \text{ pour } k \leq r\,, \\ s(y_{2k}) & = & y_{2k} + x_{2k-1} \text{ pour } k \leq r\,, \\ s(y_i) & = & y_i \text{ pour } i > r\,, \end{array}\right.$$

ce qui prouve le point (iii). Pour obtenir (iv), on construit, pour $s' \in H$ tel que le rang de $\alpha(s')$ soit $2r$, des éléments $(x'_1, \dots, x'_m)$ et $(y'_1, \dots, y'_m)$ qui jouent vis-à-vis de s' le même rôle de que $(x_1, \dots, x_m)$ et $(y_1, \dots, y_m)$ vis-à-vis de s, et t l'isomorphisme de V tel que

$$t(x_i) = x'_i \text{ et } t(y_i) = y'_i \text{ pour } 1 \leq i \leq m\,.$$

C'est un élément de $O(V, q)$ qui satisfait $tst^{-1} = s'$, d'où (iv). ■

Proposition A.0.8 *Il existe un sous-espace totalement singulier maximal W tel que si*

$$H_W \overset{def}{=} \{\sigma \in O(V, q) \,|\, \sigma(x) = x \text{ pour tout } x \in W^{\perp}\}\,,$$

alors :
(i) Tout $s \in O(V, q)$ singulier est dans H_W, à conjugaison près par un élément de $T(V, q)$,
(ii) On a $O(V, q) = H_W \cdot T(V, q)$ et $T(V, q)$ est normal dans $O(V, q)$.

PREUVE : On montre (i) en deux étapes. *Première étape* : construction de W. Fixons s un élément singulier de $O(V,q)$. Le sous-espace $\phi_s(V)$ est contenu dans un sous-espace totalement singulier maximal, qu'on notera W. On peut, d'après ([Che], Proposition I.3.2 page 13) construire un sous-espace P, totalement singulier maximal, avec $W \cap P = \{0\}$ et $W + P$ non isotrope. Si

$$R \stackrel{def}{=} (W \oplus P)^{\perp},$$

on vérifie que $W^{\perp} = W \oplus R$, de sorte que si

$$N \stackrel{def}{=} W \oplus R,$$

on a $V = N \oplus P$, et la Proposition A.0.7 peut s'appliquer : le groupe H qu'elle définit n'est autre que le groupe H_W.

Deuxième étape : si $s' \in O(V,q)$ est un autre élément singulier, soient W' un sous-espace totalement singulier maximal contenant $\phi_{s'}(V)$ et $r \in T(V,q)$ tel que $r(W') = W$ (Proposition A.0.6). Comme s' fixe les éléments de $W'^{\perp}$, l'élément $rs'r^{-1}$ est dans H_W.

Maintenant, le point (ii) résulte de la Proposition A.0.5. ■

La proposition suivante constitue la dernière étape de la preuve du Théorème A.0.2, qui sera alors achevée.

Proposition A.0.9 *Soit* (V,q) *un espace quadratique non dégénéré de dimension* n*. On note* ν *l'indice de* q*. Alors, avec les notations de la Proposition A.0.8,*
(i) Si $\operatorname{Card} F \geq 3$*, tout élément singulier de* H_W *est contenu dans* $T(V,q)$*.*
(ii) Si $\operatorname{Card} F = 2$*, et si* $\nu \in \{0,1\}$*, le groupe* H_W *est trivial.*
(iii) Si $\operatorname{Card} F = 2$*, et si* $\nu > 2$ *(donc* $n > 4$*), le groupe* H_W *est trivial.*
(iv) Si $\operatorname{Card} F = 2$*, et si* $\nu = 2$ *(donc* $n = 4$*), le groupe* H_W *est d'ordre* 2*.*

PREUVE : Montrons (i). Dans ce cas, étant donné $u \in H_W$ singulier, on peut choisir $\mu \in F \setminus \{0,-1\}$ de sorte que les formes alternées $\alpha(u)$, $\mu\alpha(u)$ et $(1+\mu)\alpha(u)$ aient même rang. Alors la Proposition A.0.7 et la Proposition A.0.8 permettent de conclure que ces trois formes correspondent à des éléments de H_W, à savoir respectivement u et, disons, u_μ et $u_{\mu+1}$ qui sont conjugués par des éléments de $O(V,q)$. Leurs classes modulo $T(V,q)$ sont donc égales à un même élément $c \in O(V,q)/T(V,q)$, tel que $c^2 = c$ (puisque $u = u_\mu u_{\mu+1}$) donc $c = 1$ et $u \in T(V,q)$.

Le point (ii) résulte du fait que sur un espace de dimension 0 ou 1, toute forme alternée est nulle.

Pour (iii), il suffit de voir que pour $s \in O(V,q)$ singulier avec $\dim \phi_s(V) = n-2$, on a $s \in T(V,q)$, car toute forme alternée est somme de formes de rang 2.

Pour cela, on prend deux vecteurs $(w_1, w_2) \in W \times W$ linéairement indépendants, et deux vecteurs $(p_1, p_2) \in P \times P$ linéairement indépendants tels que

$$\left\{ \begin{array}{rcl} s(p_1) & = & p_1 - w_2 \\ s(p_2) & = & p_2 + w_1 \end{array} \right. .$$

Le sous-espace engendré par les vecteurs w_1, w_2, p_1, p_2 est donc non isotrope, et son orthogonal (fixé par s), contient donc un vecteur z anisotrope. On vérifie alors que

$$s = t_{z+w_1} \circ t_{z+w_2} \circ t_{z+w_1+w_2} \circ t_z \, .$$

Dans le cas (iv), l'espace (V, q) est donc isomorphe à l'espace $\mathbb{F}_2^4$ muni de la forme dont l'expression dans la base canonique $(e_1, \ldots, e_4)$ est $(x_1, x_2, x_3, x_4) \mapsto x_1x_2 + x_3x_4$. Le sous-espace W de la Proposition A.0.8 est de dimension 2 donc H_W est isomorphe au groupe additif des formes alternées sur l'espace $P \times P$ avec P sous-espace totalement singulier maximal de V : il est clair qu'il n'y a que deux telles formes. ■

Appendice B

Fonctions Maple utilisées

```
formettilde:=proc(p,x,u)
local n1,n,liste,i,j,element,matcar,forme;
n:=degree(p,x):
if modp(n,2)=1 then n1:=n+1 else n1:=n: fi:
element:=sum(u[i]*x^i,i=0..n-1):
liste:=seq(rem(element*x^j,p,x),j=0..n-1):
matcar:=array(1..n1,1..n1):
for i from 1 to n do
for j from 1 to n do
matcar[i,j]:=coeff(liste[i],x,j-1):
od:
od:
if n1<>n then for i from 1 to n do matcar[i,n1]:=0:
matcar[n1,i]:=0: od: matcar[n1,n1]:=u[n]: fi:
forme:=modp(coeff(collect(
linalg[charpoly](matcar,x),x),x,n1-2),2):
end:

ordb:=proc(bol:boolean)
if bol then 1 else 0 fi:
end:

formebinttilde:=proc(p,x,u,v)
local n,n1,liste,i,j,element,matcar,forme,t;
n:=degree(p,x):
if modp(n,2)=1 then n1:=n+1 else n1:=n: fi:
forme:=formettilde(p,x,t):
forme:=subs({seq(t[i]=u[i]+v[i],i=0..n1-1)},forme)-
subs({seq(t[i]=u[i],i=0..n1-1)},forme)-
subs({seq(t[i]=v[i],i=0..n1-1)},forme):
```

```
modp(expand(forme),2):
end:

matttilde:=proc(p,x)
local n,liste,i,j,k,element,matr,forme,u,v,t,formebin,n1;
n:=degree(p,x):
if modp(n,2)=1 then n1:=n+1 else n1:=n: fi:
forme:=formettilde(p,x,t):
formebin:=formebinttilde(p,x,u,v):
matr:=array(1..n1,1..n1):
for i from 1 to n1 do
for j from 1 to n1 do
if i=j then matr[i,j]:=subs({seq(t[k-1]=ordb(i=k),k=1..n1)}
                            ,forme)
else
if i<j then
matr[i,j]:=subs({seq(u[k-1]=ordb(i=k),k=1..n1)},
                {seq(v[k-1]=ordb(j=k),k=1..n1)},formebin)
else: matr[i,j]:=0:
fi: fi:
od: od:
evalm(matr):
end:

se:=proc(n:nonnegint,k:nonnegint)
if k=1
   then
       if n=1
         then x[1];
         else se(n-1,1)+x[n];
       fi;
   else
       if n=k
         then se(n-1,n-1)*x[n];
         else se(n-1,k)+x[n]*se(n-1,k-1);
       fi;
fi:
end:

sym:=proc(n:nonnegint,p) # n : nombre de variables
                         # p : polynome en x[1], ..., x[n]
                         # sortie : polynome en s[i], 1<=i<=n
local q,k,h,i,p0,h0;
```

```
q:=expand(p):
k:=0:
if n=1
 then subs(x[1]=s[1],q)
 else
  while subs(x[n]=0,q)=0
    do k:=k+1: q:=simplify(q/product(x[i],i=1..n)): od:
  p0:=sym(n-1,subs(x[n]=0,q)):
  h:=expand(subs({seq(s[i]=se(n,i),i=1..n)},(q-p0)/s[n])):
  if whattype(h)=integer
    then s[n]^k*(p0+s[n]*h):
    else s[n]^k*(p0+s[n]*sym(n,h)):
  fi:
fi:
end:

sqrtdendiscadd:=proc(n)
local termes,i,j,fin;
termes:=seq(seq(x[i]+x[j],j=i+1..n),i=1..n):
fin:=n*(n-1)/2:
product('termes[i]','i'=1..fin):
end:

numdiscadd:=proc(n)
local termes,i,j,fin;
termes:=seq(seq(x[i]*x[j]/(x[i]^2+x[j]^2),j=i+1..n),i=1..n):
fin:=n*(n-1)/2:
if fin=1
  then numer(termes):
  else numer(sum('termes[i]','i'=1..fin)):
fi
end:

ds2:=proc(m)
local w,h,n;
n:=coldim(m):
w:=map(x->modp(x,2),evalm(m+transpose(m))):
h:=map(x->modp(x,2),evalm(inverse(w) &*m)):
factor(
  coeff(
    collect(
      map(x->modp(x,2),expand(charpoly(h,t)))
    ,t)
```

```
      ,t,n-2)
    ) mod 2:
    end:
```

Appendice C

Discriminants additifs obtenus avec Maple

C.1 Notations

Chacune des entrées de la section suivante contient

- Un polynôme $f \in F[X]$, supposé irréductible et séparable, le corps F étant de caractéristique 2.
- La matrice M triangulaire supérieure de la forme $\tilde{T}_{E'/F}$ de l'algèbre E' associée à l'extension E définie par $F[X]/(f)$ dans la base $\mathcal{B}'$ (voir 3) page 64).
- La valeur D_1 du représentant de $d^+(E/F)$ trouvé par la méthode des polynômes symétriques (voir page 61).
- La valeur D_2 du représentant de $d^+(E/F)$ trouvé par la méthode s_2 (voir page 64), à savoir $s_2((M + {}^tM)^{-1}M)$.
- Des éléments p et q tels que $D_1 - D_2 = p/q^2$.
- Des éléments t_1 et t_2 tels que $T^2 + qT + p = (T - t_1)(T - t_2)$.

C.2 Résultats

Degré 2

$$f(X) = X^2 + aX + b\,,$$

$$M = \begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix}\,,$$

$$D_1 = \frac{b}{a^2}\,,$$

$$D_2 = \frac{b}{a^2}\,,$$

$$p = 0\,,$$

$$q = 1\,,$$

$$t_1 = 0\,,$$

$$t_2 = 1\,.$$

Degré 3

$$f(X) = X^3 + aX^2 + bX + c\,,$$

$$M = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & b & c+ab & a \\ 0 & 0 & b^2 & a^2 \\ 0 & 0 & 0 & 0 \end{pmatrix}\,,$$

$$D_1 = \frac{a^3c + b^3 + c^2 + abc}{(c+ab)^2}\,,$$

$$D_2 = \frac{a^3c + b^3 + c^2}{(c+ab)^2}\,,$$

$$p = abc\,,$$

$$q = c + ab\,,$$

$$t_1 = c\,,$$

$$t_2 = ab\,.$$

Degré 4

$$f(X) = X^4 + aX^3 + bX^2 + cX + d\,,$$

$$M = \begin{pmatrix} 0 & a & a^2 & a^3+ab+c \\ 0 & b & c+ab & a^2b+ac \\ 0 & 0 & b^2 & ab^2+bc+ad \\ 0 & 0 & 0 & b^3+abc+c^2+a^2d+bd \end{pmatrix},$$

$$D_1 = \frac{a^3c^3+b^3c^2+c^4+a^2b^3d+a^4d^2+abc^3+a^3bcd}{(a^2d+abc+c^2)^2},$$

$$\begin{aligned} D_2 &= (a^{10}d^5c^2+a^{12}b^4d^4+c^{10}a^2d+a^{11}d^4c^3+a^4c^6b^7+a^7b^4c^7+a^6b^6c^6 \\ &\quad +a^3b^3c^9+a^{12}d^5b^2+a^7b^7c^5+a^2c^{10}b^2+a^8b^8c^4+a^{10}d^5b^3+a^4d^2c^8 \\ &\quad +a^8d^4c^4+a^5b^5c^7+ac^{11}b+c^{10}b^3+c^{11}a^3+c^{12}+a^8b^6c^4d+a^6b^4c^6d \\ &\quad +a^8b^4c^4d^2+a^6b^7c^4d+a^4b^2dc^8+a^{10}d^4b^2c^2+a^{11}d^4b^3c+a^9d^4bc^3 \\ &\quad +a^8d^4b^3c^2+b^3c^8a^2d+a^{12}d^6)/(c^4+a^2b^2c^2+a^4d^2)^3, \end{aligned}$$

$$\begin{aligned} p &= a(a^{13}d^7c^2+a^{15}b^4d^6+c^{14}ad+c^{10}a^5d^3+a^6b^7c^9+a^4b^5c^{11}+a^2b^3c^{13} \\ &\quad +a^{15}d^7b^2+a^8b^9c^7+ac^{14}b^2+a^9b^{10}c^6+a^9d^5c^6+a^{14}d^7bc+a^7b^2d^3c^8 \\ &\quad +a^{10}d^4b^3c^5+a^9b^4c^6d^3+a^{10}b^5c^5d^3+a^{11}b^6c^4d^3+a^7b^4c^8d^2+a^4b^3c^{11}d \\ &\quad +a^9b^6c^6d^2+a^6b^3c^9d^2+a^8b^7c^7d+a^{13}b^4d^5c^2+a^{12}b^5d^4c^3+a^{13}b^6d^4c^2 \\ &\quad +a^{10}d^5c^5b+c^{13}a^2db+a^{14}d^6b^3c+a^{13}d^6b^2c^2+a^9b^8c^6d+a^{10}b^7c^5d^2 \\ &\quad +a^5c^{10}b^2d^2+a^6b^5c^9d+a^6d^3c^9b+a^9d^4c^6b^2+a^{11}b^8c^4d^2+a^{12}d^5b^3c^3), \end{aligned}$$

$$q = a^4b^4c^4+a^8d^4+c^8,$$

$$\begin{aligned} t_1 &= a^8b^2d^3+a^7b^3cd^2+a^6b^4c^2d+a^5b^5c^3+a^7bcd^3+a^5b^3c^3d \\ &\quad +a^6c^2d^3+a^3b^3c^5+a^4c^4d^2+a^3bc^5d+a^2b^2c^6+a^2c^6d+c^8, \end{aligned}$$

$$\begin{aligned} t_2 &= a^2c^6d+a^7bcd^3+a^3bc^5d+a^8d^4+a^6c^2d^3+a^4c^4d^2+a^5b^3c^3d \\ &\quad +a^7b^3cd^2+a^3b^3c^5+a^8b^2d^3+a^2b^2c^6+a^6b^4c^2d+a^4b^4c^4+a^5b^5c^3. \end{aligned}$$

Degré 5

$$f(X) = X^5+cX^2+dX+e,$$

$$M = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & c & 0 & e & 0 \\ 0 & 0 & 0 & e & c^2 & 0 \\ 0 & 0 & 0 & c^2 & cd & c \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix},$$

$$D_1 = \frac{c^4d^2 + c^5e + e^4}{(c^2d + e^2)^2},$$

$$D_2 = \frac{ec^5 + c^4d^2 + de^2c^2 + e^4}{(c^2d + e^2)^2},$$

$$p = de^2c^2,$$

$$q = c^2d + e^2,$$

$$t_1 = e^2,$$

$$t_2 = c^2d.$$

Appendice D

A propos du pfaffien

D.1 Introduction

Soit $p \geq 1$ un entier, et posons $n = 2p$. On considère la matrice alternée générique $Y = (Y_{i,j})_{1 \leq i,j \leq n}$ telle que pour $1 \leq i, j \leq n$,

$$Y_{i,j} = \begin{cases} X_{i,j} & \text{si} \quad i < j\,, \\ 0 & \text{si} \quad i = j\,, \\ -X_{j,i} & \text{si} \quad i > j\,, \end{cases}$$

où $\{X_{i,j}\}_{1 \leq i < j \leq n}$ sont des indéterminées (sur $\mathbb{Z}$). Soit A l'anneau de polynômes $\mathbb{Z}[\{X_{i,j}\}_{1 \leq i < j \leq n}]$.

Définition D.1.1 *Le* pfaffien *de la matrice Y ci-dessus (noté $P_f(Y)$) est l'unique polynôme $P \in A$ tel que*

$$\omega^p = p! P e_1 \wedge \cdots \wedge e_{2p}\,, \quad \textit{où}$$

$$\omega = \sum_{1 \leq i < j \leq 2p} Y_{i,j} e_i \wedge e_j\,.$$

Pour $1 \leq i, j \leq n$ éventuellement égaux, on note $Y_{i;j}$ la matrice (d'ordre $n-1$ si $i = j$ et $n-2$ si $i \neq j$) déduite de Y en supprimant les lignes et les colonnes i et j ; en particulier, il convient d'observer que $P_f(Y_{i;j}) = P_f(Y_{j;i})$. On convient enfin que le pfaffien d'une matrice sans coefficient (cas où $n = 0$) vaut 1.

Dans [Bo2], §5, exercice 5, page 86, on affirme le résultat suivant, qui donnerait le développement du pfaffien suivant une ligne :

$$\forall\, 1 \leq i \leq n,\ \ P_f(Y) = \sum_{j=1}^{n} (-1)^{i+j-1} P_f(Y_{i;j}) Y_{i,j}\,. \tag{D.1}$$

Or la formule (D.1) est fausse, comme le montre l'exemple suivant.

Exemple

Considérons en effet le cas où $p = 2$ et $i = 2$. On a d'une part

$$P_f(X) = X_{1,2}X_{3,4} - X_{1,3}X_{2,4} + X_{1,4}X_{2,3}\,,$$

et d'autre part le membre de droite de (D.1) vaut :

$$P_f(Y_{2;1})Y_{2,1} - P_f(Y_{2;2})Y_{2,2} + P_f(Y_{2;3})Y_{2,3} - P_f(Y_{2;4})Y_{2,4} =$$
$$= -X_{3,4}X_{1,2} + X_{1,4}X_{2,3} - X_{1,3}X_{2,4} \neq P_f(Y)\,.$$

Nous nous proposons d'établir ici la formule correcte (Proposition D.1.2 ci-après) qu'il faut substituer à (D.1). Précisons que le facteur correcteur introduit n'affecte pas les résultats de [BM]. Nous l'utiliserons ensuite pour obtenir une propriété de divisibilité des coefficients de la matrice des cofacteurs d'une matrice alternée par son pfaffien (Corollaire D.1.3 ci-après), en nous inspirant de [Kow], § 61-62, pp. 129 et suivantes.

Proposition D.1.2 *La formule de développement du pfaffien par rapport à une ligne est*

$$\textit{Pour } 1 \le i \le n,\ \ P_f(Y) = \sum_{j=1}^{n} (-1)^{i+j-1}\epsilon(i,j)P_f(Y_{i;j})Y_{i,j}\,,\ \ \textit{avec}$$

$$\epsilon(i,j) = \begin{cases} 1 & si \quad i < j\,, \\ -1 & si \quad i > j\,, \\ 0 & si \quad i = j\,. \end{cases}$$

Corollaire D.1.3 *Soit $\tilde{Y} = (\tilde{Y}_{i,j})_{1\le i,j\le n}$ la matrice des cofacteurs de Y. Alors, pour $1 \le i,j \le n$,*

$$\tilde{Y}_{i,j} = P_f(Y)U_{i,j}\,, \tag{D.2}$$

$$\textit{avec } U_{i,j} = (-1)^{i+j-1}\epsilon(i,j)P_f(Y_{i;j})\,.$$

Ce corollaire fournit une raison supplémentaire pour laquelle la formule (D.1) est fausse : sans le coefficient correcteur que nous introduisons, la matrice des cofacteurs de Y serait symétrique, cependant que Y est anti-symétrique. Dans les sous-sections qui suivent, nous démontrons la Proposition, puis le Corollaire.

D.2 Formule de développement

Considérons donc
$$\omega = \sum_{1 \leq k < l \leq 2p} Y_{k,l} e_k \wedge e_l \,.$$

Par définition, on sait que $\omega^p = P_f(Y)p!e_1 \wedge \cdots \wedge e_{2p}$. On écrit alors pour $1 \leq i < j \leq 2p$, $\omega = \omega_1 + \omega_2 + \omega_3 + \omega_4$, où

$$\begin{aligned}
\omega_1 &:= Y_{i,j} e_i \wedge e_j \,, \\
\omega_2 &:= e_i \wedge \alpha \text{ avec } \alpha = \sum_{l \neq i} Y_{i,l} e_l \,, \\
\omega_3 &:= e_j \wedge \beta \text{ avec } \beta = \sum_{l \neq j} Y_{j,l} e_l \,, \\
\omega_4 &:= \omega_{i,j} \text{ avec } \omega_{i,j} = \sum_{\substack{1 \leq k < l \leq 2p \\ \{k,l\} \cap \{i,j\} = \emptyset}} Y_{k,l} e_k \wedge e_l \,,
\end{aligned}$$

de sorte que si on note $I = \{(r_1, \ldots, r_p) \,|\, 1 \leq r_s \leq 4 \text{ pour } 1 \leq s \leq p\}$, on a
$$\omega^p = \sum_{(r_1,\ldots,r_p) \in I} \omega_{r_1} \wedge \cdots \wedge \omega_{r_p} \,.$$

Supposons alors qu'il existe un entier s avec $1 \leq s \leq p$ et $r_s = 1$. Sous cette hypothèse, on aura $\omega_{r_1} \wedge \cdots \wedge \omega_{r_p} = 0$ sauf peut-être si $r_t = 4$ pour tout $1 \leq t \leq p$ avec $t \neq s$, ce qu'on supposera par la suite. Dans ce cas

$$\begin{aligned}
\omega_{r_1} \wedge \cdots \wedge \omega_{r_p} &= Y_{i,j} \omega_{i,j}^{s-1} \wedge e_i \wedge e_j \wedge \omega_{i,j}^{p-s} \,, \\
&= Y_{i,j} e_i \wedge \omega_{i,j}^{s-1} \wedge e_j \wedge \omega_{i,j}^{p-s} \,, \\
&= Y_{i,j} e_i \wedge e_j \wedge \omega_{i,j}^{p-1} \,.
\end{aligned}$$

Donc, si on note $J = \{(r_1, \ldots, r_p) \,|\, \exists s, 1 \leq s \leq p, r_s = 1\}$, on a

$$\begin{aligned}
\omega^p &= \sum_{(r_1,\ldots,r_p) \in J} \omega_{r_1} \wedge \cdots \wedge \omega_{r_p} + \sum_{(r_1,\ldots,r_p) \in I \setminus J} \omega_{r_1} \wedge \cdots \wedge \omega_{r_p} \,, \\
&= pY_{i,j} e_i \wedge e_j \wedge (p-1)! P_f(Y_{i;j}) e_1 \wedge \cdots \wedge \hat{e}_i \wedge \cdots \wedge \hat{e}_j \wedge \cdots \wedge e_{2p} + \\
&\quad \sum_{(r_1,\ldots,r_p) \in I \setminus J} \omega_{r_1} \wedge \cdots \wedge \omega_{r_p} \,, \\
&= (p! Y_{i,j} (-1)^{i+j-1} + p! R_{i,j}) e_1 \wedge \cdots \wedge e_{2p} \,,
\end{aligned}$$

où $R_{i,j}$ est un polynôme de A, de degré 0 en $Y_{i,j}$.

Si maintenant on suppose $1 \leq j < i \leq 2p$, le même calcul montre que
$$\omega^p = (p! Y_{j,i} (-1)^{i+j-1} + p! R_{j,i}) e_1 \wedge \cdots \wedge e_{2p} \,.$$

Ainsi, dans tous les cas, si $1 \leq i, j \leq 2p$ et $i \neq j$, on a

$$P_f(Y) = (-1)^{i+j-1}\epsilon(i,j)P_f(Y_{i;j})Y_{i,j} + R_{i,j}\,,$$

où $R_{i,j}$ est un polynôme de A, de degré 0 en $Y_{i,j}$.

D'autre part, il est clair d'après la Définition D.1.1, que si l'on fixe $1 \leq i \leq 2p$, il existe des polynômes $Q_{i,j}$ de A, de degré 0 en $Y_{i,j}$ pour $1 \leq j \leq 2p$, $j \neq i$ tels que

$$P_f(Y) = \sum_{j=1}^{n} Y_{i,j}Q_{i,j} \text{ avec la convention } Q_{i,i} = 0\,.$$

On conclut en invoquant l'unicité du quotient dans la division euclidienne de $P_f(Y)$ par $Y_{i,j}$, que $Q_{i,j} = (-1)^{i+j-1}Y_{i,j}\epsilon(i,j)P_f(Y_{i;j})$ pour $j \neq i$. On a donc bien prouvé la Proposition.

D.3 Application : coefficients de la comatrice alternée

On s'inspire de [Kow], § 61-62, pp. 129 et suivantes ; l'idée est d'utiliser les deux séries d'identités :

$$\left(\sum_{j=1}^{n} \tilde{Y}_{l,j}Y_{k,j} = \delta_{k,l}P_f(Y)^2,\ (1 \leq k,l \leq n)\right),$$

et

$$\left(\sum_{j=1}^{n} U_{l,j}Y_{k,j} = \delta_{k,l}P_f(Y),\ (1 \leq k,l \leq n)\right).$$

Le Corollaire D.1.3 résulte de l'unicité de la solution du système linéaire

$$\left(\sum_{j=1}^{n} y_{l,j}Y_{k,j} = \delta_{k,l}P_f(Y), (1 \leq k,l \leq n)\right)$$

en les inconnues $(y_{i,j})_{1\leq i,j\leq n}$.

La première série d'identités est bien connue : c'est la formule $Y{}^t\tilde{Y} = {}^t\tilde{Y}Y = I$. Voyons comment on obtient la seconde. Pour $k = l$, ce n'est autre que la Proposition D.1.2. Si maintenant $k \neq l$, on forme deux matrices auxiliaires Y' et Y'' définies par

$$Y'_{i,j} = \begin{cases} Y_{k,j} & \text{pour} \quad 1 \leq j \leq n, i = l\,, \\ Y_{i,j} & \text{pour} \quad 1 \leq j \leq n, i \neq l\,, \end{cases}$$

et

$$Y''_{i,j} = \begin{cases} Y'_{i,k} & \text{pour} \quad 1 \leq j \leq n, i = l\,, \\ Y'_{i,j} & \text{pour} \quad 1 \leq j \leq n, i \neq l\,. \end{cases}$$

La matrice Y'' est alternée et donc justiciable de la Proposition D.1.2, qu'on écrit pour $i = l$. Cela donne

$$P_f(Y'') = \sum_{j=1}^{n} Y''_{l,j}(-1)^{l+j-1}\epsilon(l,j)P_f(Y''_{l;j})\,,$$

ou encore

$$P_f(Y'') = \sum_{j=1}^{n} Y_{k,j}(-1)^{l+j-1}\epsilon(l,j)P_f(Y_{l;j})\,.$$

Or Y'' a deux colonnes (et deux lignes) nulles, donc son déterminant est nul, de même que son pfaffien. Ceci achève la preuve du Corollaire D.1.3. ■

Bibliographie du chapitre 1

[AdMi] Adem A., Milgram R. J. – Cohomology of finite groups, *Grund. der math. Wiss.* #309, Springer-Verlag, Berlin, Heidelberg, New-York (1994).

[Ati] Atiyah M. F. – Characters and cohomology of finite groups, *Publ. math. I. H. E. S.* **9** (1961) 23-64.

[Bens] Benson D. J. – Representation and cohomology I, Cambridge studies in adv. math. #30, Cambridge University Press (1991).

[Bens] Benson D. J. – Representation and cohomology II, Cambridge studies in adv. math. #31, Cambridge University Press (1991).

[Bor] Borel A., Hirzebruch F. – Characteristic classes and homogeneous spaces I, *Amer. J. Math.* **80** (1958) 458-538.

[BLLMM] Boyer C. P., Lawson H. B., Lima-Filho P., Mann B. M., Michelsohn M.-L. – Algebraic cycles and infinite loop spaces, *Inv. Math.* **113** (1993) 373-388.

[Bre] Bredon G. E. – Geometry and Topology, *Graduate Texts in Mathematics* #139, Springer-Verlag, Berlin, Heidelberg, New-York (1993).

[Die] Dieudonné J. – Une brève histoire de la Topologie, *Development of mathematics 1900-1950*, Birkhäuser, 1994, 35-153.

[DoLa] Dold A., Lashof R. – Principal quasifibrations and fibre homotopy equivalence of bundles, *Illinois J. Math.* **3** (1959) 285-305.

[Ev1] Evens L. – A generalization of the transfer map in the cohomology of groups, *Trans. Amer. Math. Soc.* **108** (1963) 54-65.

[Ev2] Evens L. – On the Chern classes of representations of finite groups, *Trans. Amer. Math. Soc.* **115** (1965) 180-193.

[EK] Evens L., Kahn D. S. – Chern classes of certain representations of finite groups, *Trans. Amer. Math. Soc.* **245** (1978) 309-330.

[FM1] Fulton W., MacPherson R. – Classes caractéristiques des images directes des fibrés vectoriels pour les revêtements, *C. R. Acad. Sci. Paris*, Série I, **299** (1984) 379-382.

[FM2] Fulton W., MacPherson R. – Characteristic classes of direct images bundles for coverings maps, *Ann. of Math.* **125** (1987) 1-92.

[GKT] Gunarwardena J., Kahn B., Thomas C. – Stiefel-Whitney classes of real representations of finite groups, *J. Algebra* **126** (1989) 327-347.

[God] Godbillon C. – Eléments de topologie algébrique, Hermann, 1971.

[Gor] Goresky R. M. – Whitney Stratified chains and cochains, *Trans A. M. S.* **267** (1981) 175-196.

[Hu] Husemöller D. – Fibre bundles, McGraw-Hill series in higher math., McGraw-Hill book company (1966).

[Ka1] Kahn B. – Classes de Stiefel-Whitney de formes quadratiques et représentations galoisiennes réelles, *Inv. Math.* **78** (1984) 223-256.

[Ka2] Kahn B. – La conjecture de Milnor, d'après V. Voevodsky, *Sém. Bourbaki*, 49ème année **834** Juin (1996).

[Koz1] Kozlowski A. – The transfer in Segal's cohomology, *Illinois J. Math.* **27** *(4)* (1983) 614-623.

[Koz2] Kozlowski A. – Operations in Segal's cohomology, *Math. Proc. Camb. Phi. Soc.* **95** (1984) 437-441.

[Koz3] Kozlowski A. – The Evens-Kahn formula for the total Stiefel-Whitney class *Proc. Amer. Math. Soc.* **91** (1984) 309-313.

[Koz4] Kozlowski A. – Transfers in the group of multiplicative units of the classical cohomology ring and Stiefel-Whitney classes, *Publ. RIMS, Kyoto Univ.* **25** (1989) 59-74.

[Koz5] Kozlowski A. – Characteristic classes of Galois representations, *Math. Proc. Camb. Phi. Soc.*, **108** (1990) 517-522.

[KP] Kahn D., Priddy S. B. – Applications of the tranfer to stable homotopy theory, *Bull. Amer. Math. Soc.*, **78** (1972) 981-987.

[LuWe] Lundell A. T., Weingram S. – The topology of CW-complexes, The University series in Higher Mathematics, Van Nostrand Reinhold Company, London, 1969.

[MaMi] Madsen I., Milgram R. J. – The classifying spaces for surgery and cobordism of manifolds, Annals of mathematics studies **92**, Princeton University Press, 1979.

[Mer] Merkuriev A. S. – On the norm residue symbol of degree 2, *Soviet. Math. Dokl.* **24** (1981) 546-551.

[Milg] Milgram R. J. – The bar construction and abelian H-spaces, *Illinois J. Math.* **11** (3) (1967) 242-250.

[Mil1] Milnor J. W. – Construction of universal bundles II, *Ann. of Math.* **63** (3) (1956) 431-436.

[Mil2] Milnor J. W. – Algebraic K-theory and quadratic forms, *Inv. Math* **9** (1970) 318-344.

[MiSt] Milnor J. W., Stasheff J. D. – Characteristic classes, *Ann. of math. studies* #76, Princeton University Press (1974).

[Mor] Morel F. – Voevodsky's proof of Milnor's conjecture, *Bull. Amer. Math. Soc. (N.S.)* **35** (1998), no. 2, 123–143.

[Rob] Robinson D. J. S. – A course in the theory of groups, *Graduate Texts in Mathematics* #80, Springer-Verlag, Berlin, New York, Heidelberg, seconde édition, 1996.

[Ros] Rosenberg J. – Algebraic K-theory and its applications, *Graduate Texts in Mathematics* #147, Springer-Verlag, Berlin, New York, Heidelberg, 1994.

[Se1] Serre J. P. – Conducteurs d'Artin des caractères réels, *Inv. Math.* **14** (1971) 173-183.

[Se2] Serre J. P. – L'invariant de Witt de la forme $\mathrm{Tr}(x^2)$, *Comm. Math. Helv.* **59** (1984) 651-676.

[Se3] Serre J. P. – Cohomologie galoisienne, *Lect. Notes in Math.* **5**, Springer-Verlag, Berlin, Heidelberg, New-York, cinquième édition, (1991).

[Se4] Serre J. P. – Représentations linéaires des groupes finis, 5ème édition, Hermann, Paris, 1998.

[Seg1] Segal G. – Classifying spaces and spectral sequences, *Publ. Math. I. H. E. S.* **34** (1968) 105-112.

[Seg2] Segal G. – Categories and cohomology theories, *Topology* **13** (1974) 293-312.

[Seg3] Segal G. – The multiplicative group of classical cohomology, *Quart. J. Math.* **26** (1975) 289-293.

[Sha] Shapiro J. M. — A Riemann-Roch type theorem for the Witt and Milnor rings of a field, *J. Pure and Applied Alg.* **15** (1979) 293-304.

[Sn] Snaith V. P. – Topological Methods in Galois Representation Theory, John Wiley and Sons, New-York (1989).

[St] Steenrod N. – Topology of fibre bundles, Princeton University Press, 1951.

[Str] Steiner R. — Multiplicative transfers in ordinary cohomology, *Proc. Edinburgh Math. Soc. (2)* **25** (1982) *2* 113-131.

[Tam1] Tambara D. – Chern classes of multiplicative direct image of vector bundles, *J. Algebra* **139** (4) (1991) 1-26.

[Tam2] Tambara D. – On multiplicative transfer, *Comm. Algebra* **21** (4) (1993) 1393-1420.

[Wei] Weibel C. A. – An introduction to homological algebra, Cambridge studies in adv. math. #38, Cambridge University Press (1994).

Bibliographie du chapitre 2

[Ara] Arason J. K. — Wittring und Galoiscohomologie bei Characteristik 2, *J. reine angew. Math* **307/308** (1979) 247-256.

[Arf] Arf. C. — Untersuchungen über quadratische Fromen in Körpern der Characteristik 2, *J. reine angew. Math* **183** (1941) 146-167.

[B1] Baeza R. — Discriminants of polynomials and of quadratic forms, *J. Algebra* **72** (1981) 17-28.

[B2] Baeza R. — On the Arf invariant of quadratic forms and knots, *Linear and Multilinear Algebra* **16** (1984) 247-252.

[BF] Berhuy G., Frings C. — On the second trace form of central simple algebras in characteristic two, *Preprint*, 2000.

[BM] Bergé A.-M., Martinet J. — Formes quadratiques et extensions en caractéristique 2, *Ann. Inst. Fourier (Grenoble)* **35** *2* (1985) 57-77 ; aussi *Séminaire de Théorie des Nombres de Bordeaux*, Exposé 35, Année 1982-1983.

[Be] Berlekamp E. R. — An analog to the discriminant over fields of characteristic two, *J. Algebra* **38** (1976) 315-317.

[Bo1] Bourbaki — Algèbre / Chapitres IV à VII, Masson, Paris (1981).

[Bo2] Bourbaki — Algèbre / Chapitre IX, Hermann, Paris (1959).

[Che] Chevalley C. — The algebraic theory of spinors, Columbia University Press, 1954.

[CT] Colliot-Thélène J.-L. — Cohomologie galoisienne des corps valués discrets henseliens, d'après K. Kato et S. Bloch., *Algebraic K-theory and its applications* (Trieste, 1997), 120-163, *World Sci. Publishing, River Edge, NJ, 1999.*

[Di1] Dieudonné J. — Pseudo-discriminant and Dickson invariant, *Pacific J. Math.* **5** (1955) 907-910.

[Di2] Dieudonné J. — La géométrie des groupes classiques, *Erg. der Math. und ihrer Gren. neue Folge* **5**, 2ème édition, Springer-Verlag, 1963.

[Dye] Dye R. H. — On the Arf invariant, *J. Algebra* **53** (1978) 36-39.

[Kat] Kato K. — Symmetric bilinear forms, quadratic forms and Milnor K in characteristic 2, *Inv. Math.* **66** (1982) 493-510.

[KMRT] Knus M. A., Merkuriev A., Rost. M., Tignol J.-P. — The book of involutions, American Mathematical Society Colloquium publications, Volume 44, 1998.

[Kow] Kowalewski G. — Determinantentheorie, Chelsea publishing company, New-York, 1948.

[La] Lang S. — Algebra, 3ème édition, Addison-Wesley, New-York (1993).

[McD] MacDonald I. G. — Symmetric functions and Hall polynomials, 2nd edition, Oxford Science Publications (1995).

[O'M] O'Meara O. T. — Introduction to quadratic forms, *Grund. der math. Wiss.* **117**, Springer-Verlag, Berlin, Heidelberg, New-York, 1971.

[Per] Perlis R. — On the analytic determination of the trace form, *Canad. Math. Bull.* **24** *4* (1985) 422-430.

[Pfi] Pfister A. — On the Milnor Conjectures : History, Influence, Applications, *Johannes Gutenberg-Universität Mainz Preprint-Reihe des Fachbereichs Mathematik*, 1999.

[Rev] Revoy P. — Remarques sur la forme trace, *Linear and Multilinear Algebra* (1989) **10** 223-233.

[Sch] Scharlau W. — Quadratic and hermitian forms, *Grund. der Math. Wiss.* **270**, Springer-Verlag, Berlin, Heidelberg, New-York (1985).

[SKW] Sasaki T., Kanada Y., Watanabe S. — Calculations of discriminants of high degree equations, *Tokyo J. Math.* **4** (1981) 493-499.

[Se1] Serre J.-P. — Corps locaux, Hermann, Paris, 1968.

[Se2] Serre J.-P. — L'invariant de Witt de la forme $\mathrm{Tr}(x^2)$, *Comm. Math. Helv.* **59** (1984) 651-676.

[Wad] Wadsworth A. R. — Discriminants in characteristic two, *Linear and Multilinear Algebra*, **17** (1985) 235-263.

[Wat] Waterhouse W. C. — Discriminants of étale and algebras and related structures, *J. reine angew. Math.* **379** (1987) 209-220.

[Zas] Zassenhaus H. — On the spinor norm, *Arch. Math.* **13** (1962) 434-451.