Invariants cohomologiques des groupes de Coxeter finis

Jerôme Ducoat

UNIVERSITÉ DE GRENOBLE

THÈSE

Pour obtenir le grade de

DOCTEUR DE L'UNIVERSITÉ DE GRENOBLE

Spécialité : **Mathématiques**

Arrêté ministériel : 7 août 2006

Présentée par

Jérôme DUCOAT

Thèse dirigée par **Grégory BERHUY**

préparée au sein **Institut Fourier**
et de **l'Ecole Doctorale Mathématiques, Sciences et Technologies de l'Information, Informatique (MSTII)**

Cohomological invariants of finite Coxeter groups

Invariants cohomologiques des groupes de Coxeter finis

Thèse soutenue publiquement le **le 22 octobre 2012**,
devant le jury composé de :

M. Grégory BERHUY
Professeur, Université Grenoble 1, Directeur de thèse
M. Philippe GILLE
DR CNRS, Ecole Normale Supérieure de Paris, Examinateur
M. Bruno KAHN
DR CNRS, Institut Mathématique de Jussieu, Examinateur
M. Alexander MERKURJEV
Professor, University of California, Los Angeles, Rapporteur
M. Emmanuel PEYRE
Professeur, Université Grenoble 1, Examinateur
M. Jean-Pierre TIGNOL
Professeur, Université Catholique de Louvain, Rapporteur

À Émilie,

Remerciements

Mes premiers remerciements vont à mon directeur de thèse Grégory Berhuy pour m'avoir proposé un sujet de thèse dans un domaine extrêmement intéressant, pour m'avoir accordé sa confiance en me laissant une grande liberté de recherche et pour m'avoir épaulé tout au long de ces trois années et quelques.

Je remercie profondément Alexander Merkurjev et Jean-Pierre Tignol de m'avoir fait l'honneur d'être rapporteurs de ma thèse tout comme je remercie sincèrement Philippe Gille, Bruno Kahn et Emmanuel Peyre d'avoir accepté d'être membres du jury.

Je souhaite également remercier Eva Bayer, Skip Garibaldi, Max-Albert Knus et Mark MacDonald pour l'intérêt qu'ils ont porté à mon travail et pour nos enrichissantes discussions lors des différentes occasions où nous nous sommes rencontrés.

De même, je remercie chaleureusement José Bertin, Laurent Manivel et Emmanuel Peyre notamment au sein de l'institut Fourier pour m'avoir écouté, soutenu et pour leurs conseils toujours judicieux. Je remercie d'ailleurs plus généralement les membres de l'institut pour les conditions de travail de qualité qu'ils offrent aux doctorants.

Je remercie aussi Frédérique Oggier de m'accorder sa confiance et de me donner l'opportunité de me tourner vers un nouvel horizon de recherches.

J'ai une pensée particulière pour Maksim, Charles, Aléna, Demba _entre autres_ pour les bons moments passés en conférence, ainsi que pour mes collègues doctorants de l'institut Fourier (dans le désordre) Damien et Guillaume mes cobureaux quand je suis arrivé et Thomas, Aurélien, Bashar, Mathieu, Hassan, Jean-Matthieu et tous les autres.

Je remercie aussi mes amis Thibault, Charlotte, Adrien, Alice, Richard, Laurent, Damien et le gang des Lyonnais Simon, Céline, Xavier, Lisa, Christopher, Rémy,

François, Thomas _et j'en oublie beaucoup !_ parmi lesquels de nombreux thésards, compagnons de galère.

Comment ne pas évidemment penser à mes parents toujours à l'écoute et prêts à me soutenir, à Didier et Sylvie, qui m'avez accueilli si généreusement et qui me témoignez tant d'affection, à mes soeurs Sandra et Aline, à mes beaux-frères les deux Sébastien, Yann et au petit Raphaël mon petit neveu préféré (le seul, pour le moment...). J'ai aussi une tendre pensée pour ma grand-mère Marcelle, pour Rolande et pour mes grand-parents aujourd'hui disparus, ainsi que pour le reste de la famille.

Et enfin et surtout, bien sûr, Émilie, ton soutien inconditionnel, ta présence, ton sourire au quotidien me permettent de surmonter bien des épreuves et des tracas, que je ne m'imagine pas vivre sans toi et je souhaite te dire un énorme merci, qui signifie bien plus pour moi que ce simple mot.

Contents

Introduction (version française)

Un problème général en mathématiques est de classifier des objets, à isomorphisme près. Notons Obj l'ensemble des objets considérés. Quand ceux-ci sont trop compliqués à comprendre directement, on cherche des invariants, c'est-à-dire des applications de l'ensemble des classes d'isomorphisme de ces objets vers un ensemble d'objets mieux connus et on espère obtenir des invariants assez d'information pour permettre la classification. Dans le cas de structures algébriques (comme les algèbres, les formes quadratiques, les variétés algébriques, etc), elles sont souvent définies sur un corps et stables par extension des scalaires. Fixons un corps de base k_0. Il est naturel de considérer le foncteur $\mathsf{Obj} : k/k_0 \mapsto \mathsf{Iso}_k(\mathsf{Obj})$, où, pour toute extension de corps k/k_0, $\mathsf{Iso}_k(\mathsf{Obj})$ désigne l'ensemble des classes d'isomorphisme des objets définis sur k.

Pour commencer, considérons comme foncteur des objets, le foncteur $\mathbf{Quad}^n_{k_0}$ des classes d'isométrie des formes quadratiques non dégénérées, de rang fixé $n \geq 1$ sur une extension de corps quelconque k/k_0. Alors, pour les formes quadratiques, le discriminant, l'algèbre de Clifford (ou l'algèbre de Clifford paire, selon que l'une ou l'autre est centrale simple sur le corps de base), l'invariant de Hasse-Witt ou la signature (si $k_0 \subset \mathbb{R}$) sont invariants par isométrie (cf. [12] ou [10] pour les définitions). Quand $k_0 = \mathbb{Q}$, les formes quadratiques non dégénérées sur $\mathbb{Q}$ sont classifiées à isométrie près par le rang, le discriminant, l'invariant de Hasse-Witt et la signature (cf. par exemple [21]). Cependant, cette classification n'est pas vraie pour un corps arbitraire (cf. [9]). On peut alors se demander s'il existe d'autres invariants qui permettraient d'obtenir une classification complète.

Remarquons d'abord que le discriminant, l'algèbre de Clifford (paire) et l'invariant de Hasse-Witt induisent des transformations naturelles du foncteur $\mathbf{Quad}^n_{k_0}$ vers un foncteur de cohomologie galoisienne $H^i(k, \mathbb{Z}/2\mathbb{Z})$. En effet, le groupe de cohomologie galoisienne $H^1(k, \mathbb{Z}/2\mathbb{Z})$ est isomorphe au groupe des classes de carrés de k et le groupe de cohomologie galoisienne $H^2(k, \mathbb{Z}/2\mathbb{Z})$ est isomorphe au sous-groupe des éléments de 2-torsion dans le groupe de Brauer de k, qui classifie les algèbres centrales simples d'indice une puissance de 2 sur k à équivalence de Brauer près (cf. [10]; remarquons aussi que Merkurjev a prouvé que ce groupe est engendré par les classes de produits tensoriels d'algèbres de quaternions sur k, cf. [27] pour

une preuve). On peut alors se demander s'il y a d'autres invariants à valeurs dans de tels groupes de cohomologie. Avant de donner la réponse pour les formes quadratiques, considérons la situation plus générale suivante.

Soit G un schéma en groupes algébrique lisse sur k_0. Si k/k_0 est une extension de corps, le premier ensemble de cohomologie galoisienne $H^1(k, G)$ est en bijection avec l'ensemble des classes d'isomorphisme de G-torseurs sur k. Dans de nombreux cas particuliers, ces ensembles classifient aussi d'autres structures algébriques intéressantes. On en présente ici quelques exemples (on remarque que le mot "classifie" ci-dessous signifie "est en bijection avec l'ensemble des classes d'isomorphisme de") :

(a) quand le schéma en groupes G est fini et constant, pour toute extension k/k_0, l'ensemble $H^1(k, G)$ classifie les G-algèbres galoisiennes sur k;

(b) quand $G = \mathbf{O}_n$ est le schéma en groupes orthogonal sur k_0 (i.e. associé au groupe orthogonal de la forme quadratique unité $\langle 1, ..., 1\rangle$ de rang n sur k), l'ensemble $H^1(k, G)$ classifie les formes quadratiques non dégénérées de rang n sur k;

(c) quand $G = \mathfrak{S}_n$ est le groupe symétrique sur n éléments, l'ensemble $H^1(k, G)$ classifie les algèbres étales de rang n sur k.

Soit Γ_{k_0} le groupe de Galois absolu sur k_0 et soit C un Γ_{k_0}-module fini. On introduit le foncteur de cohomologie galoisienne abélienne

$$H^*(./k_0, C) : k/k_0 \mapsto H^*(k, C) = \bigoplus_{i\in\mathbb{N}} H^i(k, C)$$

de la catégorie des extensions de corps de k_0 à la catégorie des ensembles (plus précisément, ce foncteur est à valeurs dans la catégorie des groupes abéliens et on compose ici par le foncteur d'oubli). On considère alors les morphismes de foncteurs de Obj vers $H^*(./k_0, C)$. On les appelle invariants cohomologiques des objets sur k_0 à coefficients dans C. Dans la suite, on utilise principalement comme foncteur d'objets le foncteur de cohomologie galoisienne

$$H^1(./k_0, G) : k/k_0 \mapsto H^1(k, G)$$

de la catégorie des extensions de corps de k_0 vers la catégorie des ensembles et on note $\mathsf{Inv}_{k_0}(G, C)$ l'ensemble des invariants cohomologiques de G sur k_0 à coefficients dans C.

Revenons maintenant au foncteur $\mathbf{Quad}^n_{k_0}$. Pour toute extension k/k_0 et toute forme quadratique non dégénérée diagonale $q = \langle \alpha_1, \ldots, \alpha_n\rangle$, avec $\alpha_1, \ldots, \alpha_n$ des

classes de carrés dans k, on pose

$$w_i(q) = \sum_{1 \leq j_1 < \ldots < j_i \leq n} (\alpha_{j_1}) \cdot \cdots \cdot (\alpha_{j_i}).$$

On remarque d'abord que cette définition n'est pas restrictive puisque toute classe d'isométrie de formes quadratiques (non dégénérées) contient (au moins) une forme diagonale. De plus, $w_i(q)$ est bien définie (si deux formes quadratiques diagonales sont isométriques, leurs images par w_i sont égales). Cela induit donc des invariants cohomologiques $w_i \in \mathsf{Inv}_{k_0}(\mathbf{O}_n, \mathbb{Z}/2\mathbb{Z})$ appelés invariants de Stiefel-Whitney. Dans [24], Serre a décrit la structure du groupe $\mathsf{Inv}_{k_0}(\mathbf{O}_n, \mathbb{Z}/2\mathbb{Z})$: il est muni d'une structure de $H^*(k_0, \mathbb{Z}/2\mathbb{Z})$-module libre, dont une base est donnée par les invariants de Stiefel-Whitney w_i pour $0 \leq i \leq n$. Néanmoins, les formes quadratiques non dégénérées ne sont pas classifiées, à isométrie près, par leurs invariants cohomologiques à coefficients dans $\mathbb{Z}/2\mathbb{Z}$. Dans [19], Scharlau a donné des exemples de corps k et de formes quadratiques q et q' qui ne sont pas isométriques et pour lesquelles pour tout $0 \leq i \leq n$, $w_i(q) = w_i(q')$.

Soit $n \geq 1$. Serre a montré dans [24] que le groupe des invariants cohomologiques des n-formes de Pfister à coefficients dans $\mathbb{Z}/2\mathbb{Z}$ est un $H^*(k_0, \mathbb{Z}/2\mathbb{Z})$-module libre avec une base donnée par $\{1, e_n\}$, où

$$e_n(\langle\langle \alpha_1, ..., \alpha_n \rangle\rangle) = (\alpha_1) \cdot \cdots \cdot (\alpha_n).$$

De plus, Serre a donné la description du groupe des invariants cohomologiques des algèbres d'octonions, des formes hermitiennes ou des algèbres d'Albert (cf. [24], 18.4, 21.6 or 22.5).

Plus récemment, dans [14] et dans [15], MacDonald a déterminé une base du groupe des invariants cohomologiques du schéma en groupes des automorphismes d'une algèbre de Jordan centrale simple scindée de degré impair.

Remarquons aussi qu'une classification complète est connue pour les formes quadratiques sur un corps quelconque (à isométrie près). Grâce à la conjecture de Milnor prouvée par Voevodsky (cf. [16] pour l'énoncé et [26] et [18] pour la preuve), les invariants e_n (définis ci-dessus pour les formes de Pfister) classifient complètement les formes quadratiques sur un corps de base quelconque. En effet, deux formes quadratiques q_1 et q_2 sont isométriques si et seulement si $q_1 - q_2$ est hyperbolique et si les classes de cohomologie $e_n(q_1 - q_2)$ s'annulent pour tout $n \geq 0$. Remarquons que ces invariants e_n ne sont pas définis pour toute forme quadratique et ne peuvent pas définir des invariants cohomologiques dans $\mathsf{Inv}_{k_0}(\mathbf{O}_n, \mathbb{Z}/2\mathbb{Z})$ (sauf pour $n = 0$ et $n = 1$).

Revenons à la situation où G est un schéma en groupes algébrique lisse sur k_0. Pour les groupes algébriques connexes simplement connexes absolument simples,

Rost a montré que le groupe des invariants normalisés cohomologiques de G de degré 3 à coefficients dans $\mathbb{Q}/\mathbb{Z}(2)$ est fini cyclique et engendré par un invariant canonique R_G appelé invariant de Rost (voir la contribution de Merkurjev de [24]).

On considère à présent le cas où G est un groupe fini. Les invariants cohomologiques de certains groupes finis peuvent être utiles pour résoudre le problème de Noether. On rappelle qu'on dit que le problème de Noether est vrai pour le groupe G sur le corps k_0 s'il existe un plongement $\rho : G \to \mathsf{GL}_n(k_0)$ tel que, si K_ρ est le sous-corps de $k_0(X_1, ..., X_n)$ fixé par G, alors K_ρ est k_0-rational. Serre a démontré dans [24], 33.10, que s'il existe un invariant cohomologique de G sur k_0 qui est à la fois non ramifié et non constant, alors le problème de Noether est faux pour G sur k_0. En utilisant cette propriété, Serre a prouvé que le problème de Noether est faux pour tout groupe ayant un 2-sous-groupe de Sylow cyclique d'ordre ≥ 8 sur $\mathbb{Q}$ (cf. [24], 33.16).

Cependant, on ne connaît actuellement que très peu de résultats sur les invariants cohomologiques des groupes finis. Dans [24], Serre a décrit les invariants cohomologiques des groupes 2-élémentaires et du groupe symétrique. Le but de cette thèse est de généraliser le travail de Serre sur les invariants cohomologiques du groupe symétrique aux groupes de Coxeter finis.

Dans le chapitre 1, on rappelle les résultats classiques de cohomologie galoisienne, dans les cas non-abélien et abélien, en y ajoutant les résultats principaux sur les applications résidu; on expose ensuite les principaux outils sur les invariants cohomologiques décrits dans [24].

Dans le chapitre 2, on donne des exemples explicites d'invariants cohomologiques, en rappelant d'abord les résultats de Serre sur les invariants cohomologiques des groupes 2-élémentaires, du groupe orthogonal et du groupe symétrique. En particulier, on donne la description de Serre des invariants cohomologiques de $\mathfrak{S}_n$, où $n \geq 1$. Soit $n \geq 1$. On pose, pour tout $0 \leq i \leq n$,

$$\begin{aligned} w_i : H^1(./k_0, \mathfrak{S}_n) &\to H^*(./k_0, \mathbb{Z}/2\mathbb{Z}) \\ (L) &\mapsto w_i(\mathsf{Tr}_L(x^2)) \end{aligned} .$$

Cet invariant w_i est appelé le i^e invariant de Stiefel-Whitney. Dans [24], 25.13, Serre a montré que, pour tout corps k_0 de caractéristique différente de 2 et pour tout $n \geq 2$, le $H^*(k_0, \mathbb{Z}/2\mathbb{Z})$-module $\mathsf{Inv}_{k_0}(\mathfrak{S}_n, \mathbb{Z}/2\mathbb{Z})$ est libre et une base est donnée par la famille $\{w_i\}_{0 \leq i \leq [\frac{n}{2}]}$.

On établit ensuite quelques résultats sur les invariants cohomologiques de certains groupes de réflection simples, comme le groupe de Weyl de type G_2, le groupe de Coxeter de type H_3 et les groupes diédraux $\mathbb{D}_n$ avec n qui n'est pas divisible par

4 ainsi que le groupe diédral $\mathbb{D}_4$.

L'objectif du chapitre 3 est d'établir un principe général d'annulation pour les invariants cohomologiques des groupes de Coxeter finis en caractéristique zéro. On remarque d'abord que, pour décrire les invariants cohomologiques du groupe symétrique, Serre a énoncé le principe de déploiement suivant (cf. [24], 24.9).

Théorème (Serre, 2003)**.** *Soit k_0 un corps tel que $\mathsf{char}(k_0)$ ne divise pas l'ordre de C et soit $n \geq 2$. Soit aussi $a \in \mathsf{Inv}_{k_0}(\mathfrak{S}_n, \mathbb{Z}/2\mathbb{Z})$. Supposons que, pour toute extension k/k_0, $a_k(E) = 0$ dès que E est une k-algèbre étale isomorphe à un produit direct de k-algèbres étales de rang ≤ 2. Alors $a = 0$.*

Passons maintenant à la généralisation de ce résultat aux groupes de Coxeter finis en caractéristique zéro. On rappelle qu'un groupe de Coxeter fini W est un groupe de réflection réel, c'est-à-dire qu'il existe une représentation linéaire fidèle $\rho : W \hookrightarrow GL(V)$ dans un espace vectoriel réel V de dimension finie, tel que W est engendré par des réflections de V. Remarquons que réflection signifie ici un endomorphisme r de V tel que le rang de $r - \mathsf{id}_V$ est égal à 1 et que $r^2 = \mathsf{id}_V$.

Soit G un groupe fini et $H \subset G$ un sous-groupe. Si $a \in \mathsf{Inv}_{k_0}(G, C)$, le composé $H^1(./k_0, H) \longrightarrow H^1(./k_0, G) \xrightarrow{a} H^*(./k_0, C)$ définit un invariant de H, appelé la restriction de a à H.

Dans [24] 25.15, Serre a énoncé un principe d'annulation pour les invariants cohomologiques des groupes de Weyl. On prouve dans cette thèse une généralisation de ce principe aux groupes de Coxeter finis.

Théorème (Serre, 2003)**.** *Soit W un groupe de Coxeter fini et soit k_0 un corps de caractéristique zéro contenant un sous-corps sur lequel la représentation réelle de W comme groupe de réflection est réalisable. Soit C un Γ_{k_0}-module fini et $a \in \mathsf{Inv}_{k_0}(W, C)$. Supposons que toute restriction de a à un sous-groupe abélien de W engendré par des réflections est nul. Alors $a = 0$.*

On remarque que cette hypothèse sur le corps de base k_0 est automatiquement satisfaite pour les groupes de Weyl puisque toute représentation irréductible réelle d'un groupe de Weyl est réalisable sur le corps des rationnels $\mathbb{Q}$. Cependant, pour d'autres groupes de Coxeter, ce n'est pas le cas (par exemple, si $W = \mathbb{D}_n$ est le groupe diédral d'ordre $2n$, la représentation géométrique réelle standard $\rho : W \to \mathsf{GL}_2(\mathbb{R})$ est réalisable sur $\mathbb{Q}(\cos(\frac{2\pi}{n}))$ mais pas sur $\mathbb{Q}$).

On note enfin qu'on retrouve exactement le principe de déploiement à partir du principe d'annulation dans le cas des groupes de Weyl de type A_n.

Dans le chapitre 4, on s'intéresse aux groupes de Weyl de type B_n ou C_n. Soit $n \geq 2$ W un groupe de Weyl de type B_n (on note qu'un groupe de Weyl de type

C_n est isomorphe à W). Soit k un corps de caractéristique différente de 2. Alors $H^1(k, W)$ est en bijection avec l'ensemble des classes d'isomorphisme des paires (L, α), où L est une k-algèbre étale et α une classe de carrés dans L. On pose, pour tout $0 \leq i \leq n$,

$$\begin{array}{c} w_i : H^1(./k_0, \mathfrak{S}_n) \to H^*(./k_0, \mathbb{Z}/2\mathbb{Z}) \\ (L, \alpha) \mapsto w_i(\mathsf{Tr}_L(x^2)) \end{array} .$$

De plus, on remarque que, pour toute paire $(L, \alpha) \in H^1(k, W)$, la classe d'isomorphisme de la forme quadratique $\mathsf{Tr}_L(\alpha x^2)$ ne dépend pas du choix d'un représentant dans la classe de carrés de α. Posons alors

$$\begin{array}{c} \widetilde{w_i} : H^1(./k_0, \mathfrak{S}_n) \to H^*(./k_0, \mathbb{Z}/2\mathbb{Z}) \\ (L, \alpha) \mapsto w_i(\mathsf{Tr}_L(\alpha x^2)) \end{array} .$$

Ces invariants sont aussi appelés invariants de Stiefel-Whitney de W.

Théorème. *Soit k_0 un corps de caractéristique zéro, tel que -1 et 2 sont des carrés dans k_0. Soit $n \geq 2$ et W un groupe de Weyl de type B_n. Alors le $H^*(k_0, \mathbb{Z}/2\mathbb{Z})$-module $\mathsf{Inv}_{k_0}(W, \mathbb{Z}/2\mathbb{Z})$ est libre avec une base donnée par la famille*

$$\{w_i \cdot \widetilde{w_j}\}_{0 \leq i \leq [\frac{n}{2}], 0 \leq j \leq 2([\frac{n}{2}]-i)}.$$

Dans le chapitre 5, on s'intéresse aux groupes de Weyl de type D. Soit W un groupe de Weyl de type D_n ($n \geq 4$). On a la suite exacte

$$1 \longrightarrow W \longrightarrow W' \xrightarrow{p} \mathbb{Z}/2\mathbb{Z} \longrightarrow 1 \ ,$$

où W' est un groupe de Weyl de type B_n et $p : (\epsilon_1, ..., \epsilon_n, \sigma) \mapsto \prod_{i=1}^{n} \epsilon_i$.

Soit k_0 un corps de caractéristique différente de 2. Si $a \in \mathsf{Inv}_{k_0}(W', \mathbb{Z}/2\mathbb{Z})$, alors $\mathsf{Res}^W_{W'}(a)$ est un invariant cohomologique de W. Ainsi, pour $0 \leq i \leq n$, $\mathsf{Res}^W_{W'}(w_i)$ est un invariant de W est encore noté w_i. De même, pour $0 \leq i \leq n$, $\mathsf{Res}^W_{W'}(\widetilde{w_i})$ est un invariant de W et est encore noté $\widetilde{w_i}$.

Théorème. *Soit k_0 un corps de caractéristique zéro. Soit $n \geq 4$ et W un groupe de Weyl de type D_n. Alors le $H^*(k_0, \mathbb{Z}/2\mathbb{Z})$-module $\mathsf{Inv}_{k_0}(W, \mathbb{Z}/2\mathbb{Z})$ est libre de base*

$$\{w_i \cdot \widetilde{w_j}\}_{0 \leq i \leq [\frac{n}{2}], 0 \leq j \leq 2([\frac{n}{2}]-i) \text{ et } j \text{ pair}} .$$

Introduction

A general problem in mathematics is to classify objects, up to isomorphism. Let us denote by Obj the set of the objects. When it is too complicated, we look for invariants, i.e. maps from the set of isomorphism classes of the objects to a set of well-understood objects and we hope to get from invariants enough information to allow classification. Concerning algebraic structures (such as algebras, quadratic forms, algebraic varieties, etc) they are often defined over a field and stable by scalar extension. Let k_0 be a base field. It is natural to consider the functor $\mathsf{Obj} : k/k_0 \mapsto \mathsf{Iso}_k(\mathsf{Obj})$, where, for any k/k_0, $\mathsf{Iso}_k(\mathsf{Obj})$ denotes the set of isomorphism classes of the objects defined over k.

Let us first consider the functor $\mathbf{Quad}^n_{k_0}$ of the isometry classes of the non-degenerate quadratic forms of fixed rank $n \geq 1$ over an arbitrary extension field k/k_0 as the functor of the objects. Then, for quadratic forms, the discriminant, the Clifford algebra (or the even Clifford algebra, depending on which is central simple over the base field), the Hasse-Witt invariant or the signature (if $k_0 \subset \mathbb{R}$) are invariant under isometry (see [12] or [10] for definitions). When $k_0 = \mathbb{Q}$, the non-degenerate quadratic forms over $\mathbb{Q}$ are classified by the rank, the discriminant, the Hasse-Witt invariant and the signature up to isometry (see for instance [21]). However, this classification does not hold for an arbitrary field (see [9]). We then may wonder whether there are other invariants so that a complete classification would be obtained.

Let us first note that the discriminant, the (even) Clifford algebra and the Hasse-Witt invariant yield some natural transformations from the functor $\mathbf{Quad}^n_{k_0}$ to some Galois cohomology functor $H^i(k, \mathbb{Z}/2\mathbb{Z})$. Indeed, the Galois cohomology group $H^1(k, \mathbb{Z}/2\mathbb{Z})$ is isomorphic to the group of the square-classes in k and the Galois cohomology group $H^2(k, \mathbb{Z}/2\mathbb{Z})$ is isomorphic to the 2-torsion part of the Brauer group of k, which classifies the central simple algebras of index a power of 2 over k up to Brauer equivalence (see [10]; note also that Merkurjev proved that this group is generated by the classes of tensor products of quaternion algebras over k, see [27] for a proof). We then may wonder whether there should be some other invariants with values in such cohomological groups. Before giving the answer for quadratic forms, let us look at a more general situation.

Let G be a smooth algebraic group scheme over k_0. If k/k_0 is a field extension over k_0, the first Galois cohomology set $H^1(k, G)$ is in bijection with the set of the isomorphism classes of G-torsors over k. In many particular cases, these sets also classify many other interesting algebraic structures. Here are a few examples (note that the word "classifies" below means "is in bijection with the set of isomorphism classes of") :

(a) when the group scheme G is finite constant, for any k/k_0, the set $H^1(k, G)$ classifies Galois G-algebras over k;

(b) when $G = \mathbf{O}_n$ is the orthogonal group scheme over k_0 (i.e. associated with the orthogonal group of the unit quadratic form $\langle 1, ..., 1\rangle$ of rank n over k), the set $H^1(k, G)$ classifies non-degenerate quadratic forms of rank n over k;

(c) when $G = \mathfrak{S}_n$ is the symmetric group on n letters, the set $H^1(k, G)$ classifies étale algebras of rank n over k.

Let Γ_{k_0} denote the absolute Galois group over k_0 and let C be a finite Γ_{k_0}-module. Let us introduce the abelian Galois cohomology functor

$$H^*(./k_0, C) : k/k_0 \mapsto H^*(k, C) = \bigoplus_{i\in\mathbb{N}} H^i(k, C)$$

from the category of the field extensions over k_0 to the sets category (to be precise, this functor has values in the abelian groups category and we compose here by the forgetful functor). We then consider morphisms of functors from Obj to $H^*(./k_0, C)$. Such morphisms are called cohomological invariants of the objects over k_0 with coefficients in C. In the sequel, we mainly use the Galois cohomology functor

$$H^1(./k_0, G) : k/k_0 \mapsto H^1(k, G)$$

from the category of field extensions over k_0 to the category of sets as the functor of objects and we denote by $\mathsf{Inv}_{k_0}(G, C)$ the set of the cohomological invariants of G over k_0 with coefficients in C.

Let us come back to the functor $\mathbf{Quad}^n_{k_0}$. For any k/k_0, for any non-degenerate diagonalized quadratic form $q = \langle\alpha_1, \ldots, \alpha_n\rangle$, with $\alpha_1, \ldots, \alpha_n \in k^\times/k^{\times 2}$, we set

$$w_i(q) = \sum_{1\leq j_1<\ldots<j_i\leq n} (\alpha_{j_1}) \cdot \cdots \cdot (\alpha_{j_i}).$$

Note first that this definition is not restrictive since any isometry class of non-degenerate quadratic forms contains (at least) a diagonalized form. Note also that $w_i(q)$ is well-defined (if two diagonalized quadratic forms are isometric, their image

by w_i are equal). It yields some cohomological invariants $w_i \in \mathsf{Inv}_{k_0}(\mathbf{O}_n, \mathbb{Z}/2\mathbb{Z})$ called Stiefel-Whitney invariants. In [24], Serre described the structure of the group $\mathsf{Inv}_{k_0}(\mathbf{O}_n, \mathbb{Z}/2\mathbb{Z})$: it carries a structure of free $H^*(k_0, \mathbb{Z}/2\mathbb{Z})$-module, with a basis given by the Stiefel-Whitney invariants w_i for $0 \leq i \leq n$. Nevertheless, the non-degenerate quadratic forms are not classified by their cohomological invariants with coefficients in $\mathbb{Z}/2\mathbb{Z}$. In [19], Scharlau gave examples of fields k and of quadratic forms q and q' which are non isometric and such that for any $0 \leq i \leq n$, $w_i(q) = w_i(q')$.

Let $n \geq 1$. Serre proved in [24] that the group of the cohomological invariants of the n-fold Pfister forms with coefficients in $\mathbb{Z}/2\mathbb{Z}$ is a free $H^*(k_0, \mathbb{Z}/2\mathbb{Z})$-module with a basis $\{1, e_n\}$, where

$$e_n(\langle\langle \alpha_1, ..., \alpha_n \rangle\rangle) = (\alpha_1) \cdot \cdots \cdot (\alpha_n).$$

Note also that Serre gave the description of the group of cohomological invariants of the octonion algebras, of hermitian forms or of Albert algebras (see [24], 18.4, 21.6 or 22.5).

More recently, in [14] and in [15], MacDonald determined a basis for the cohomological invariants of the automorphism group scheme of a split central simple Jordan algebra of odd degree.

Let us also note that a complete classification is known for quadratic forms over an arbitrary field (up to isometry). Thanks to Milnor's conjecture proved by Voevodsky (see [16] for the statement and [26] and [18] for the proof) the invariants e_n (defined above for Pfister forms) completely classify quadratic forms over an arbitrary base field. Indeed, two quadratic forms q_1 and q_2 are isometric if and only if $q_1 - q_2$ is hyperbolic and the cohomology classes $e_n(q_1 - q_2)$ all vanish for any $n \geq 0$. Note that these invariants e_n are not defined for any quadratic form and then can not yield cohomological invariants in $\mathsf{Inv}_{k_0}(\mathbf{O}_n, \mathbb{Z}/2\mathbb{Z})$ (unless $n = 0$ and $n = 1$).

Let us come back to the situation where G is a smooth algebraic group scheme over k_0. For absolutely simple simply connected algebraic groups, Rost proved the group of the normalized cohomological invariants of G of degree 3 with coefficients in $\mathbb{Q}/\mathbb{Z}(2)$ is finite cyclic and generated by a canonical invariant R_G called the Rost invariant (see Merkurjev's part of [24]).

Let us now consider the case where G is a finite group. The cohomological invariants of finite groups may be useful to solve Noether's problem. Let us recall that we say that Noether's problem is true for the group G over the field k_0 if there exists an embedding $\rho : G \to \mathsf{GL}_n(k_0)$ such that, if K_ρ is the subfield of $k_0(X_1, ..., X_n)$ fixed by G, then K_ρ is k_0-rational. Serre proved in [24], 33.10, that

if there exists a cohomological invariant of G over k_0 which is unramified and non constant, then Noether's problem is false for G over k_0. Using this property, Serre proved that Noether's problem is false for any group with a cyclic 2-Sylow subgroup of order ≥ 8 over $\mathbb{Q}$ (see [24], 33.16).

However, very few is known about cohomological invariants of finite groups. In [24], Serre described the cohomological invariants of 2-elementary groups and of symmetric groups. The aim of this thesis is to generalize the work from Serre about cohomological invariants of symmetric groups to finite Coxeter groups.

In Chapter 1, we recall the background on Galois cohomology in both non-abelian and abelian cases, including the framework of residue maps; then we state the main tools on cohomological invariants described in [24].

In Chapter 2, we provide examples of cohomological invariants, first recalling results of Serre on cohomological invariants of 2-elementary groups, of the orthogonal group and of the symmetric group. In particular, we recall Serre's description of the cohomological invariants of $\mathfrak{S}_n$, where $n \geq 1$. Let $n \geq 1$. Set, for any $0 \leq i \leq n$,

$$\begin{array}{rcl} w_i : H^1(./k_0, \mathfrak{S}_n) & \to & H^*(./k_0, \mathbb{Z}/2\mathbb{Z}) \\ (L) & \mapsto & w_i(\mathsf{Tr}_L(x^2)) \end{array}.$$

This invariant w_i is called the i^{th}-Stiefel-Whitney invariant. In [24], 25.13, Serre proved that, for any field k_0 of characteristic different from 2 and for any $n \geq 2$, the $H^*(k_0, \mathbb{Z}/2\mathbb{Z})$-module $\mathsf{Inv}_{k_0}(\mathfrak{S}_n, \mathbb{Z}/2\mathbb{Z})$ is free with basis $\{w_i\}_{0 \leq i \leq [\frac{n}{2}]}$.

We then provide some computations to describe the cohomological invariants of some simple reflection groups, such as the Weyl group of type G_2, the Coxeter group of type H_3 and the dihedral groups $\mathbb{D}_n$ for n not divisible by 4 and for $n = 4$.

The aim of Chapter 3 is to state a general vanishing principle for the cohomological invariants of the finite Coxeter groups in characteristic zero. Note first that, to describe the cohomological invariants of the symmetric groups, Serre stated the following splitting principle (see [24], 24.9).

Theorem (Serre, 2003)**.** *Let k_0 be a field such that $\mathsf{char}(k_0)$ does not divide the order of C and let $n \geq 2$. Let also $a \in \mathsf{Inv}_{k_0}(\mathfrak{S}_n, \mathbb{Z}/2\mathbb{Z})$. Assume that, for every extension k/k_0, $a_k(E) = 0$ whenever E is an étale k-algebra isomorphic to a direct product of étale k-algebras of rank ≤ 2. Then $a = 0$.*

Let us now state the generalization of this result to finite Coxeter groups in characteristic zero. Let us recall that a finite Coxeter group W is a finite real reflection group, i.e. there exists a faithful linear representation $\rho : W \hookrightarrow GL(V)$ in a finite dimensional real vector space V, such that W is generated by reflections of V.

Note that by reflection, we mean an endomorphism r of V such that the rank of $r - \mathsf{id}_V$ is equal to 1 and that $r^2 = \mathsf{id}_V$.

Let G be a finite group and let $H \subset G$ be a subgroup. If $a \in \mathsf{Inv}_{k_0}(G, C)$, the compositum $H^1(./k_0, H) \longrightarrow H^1(./k_0, G) \xrightarrow{a} H^*(./k_0, C)$ defines an invariant of H, called the restriction of a to H.

In [24] 25.15, Serre stated a vanishing principle for the cohomological invariants of the Weyl groups. We prove in this thesis a generalization of this principle to finite Coxeter groups.

Theorem (Serre, 2003)**.** *Let W be a finite Coxeter group and let k_0 be a field of characteristic zero containing a subfield on which the real representation of W as a reflection group is realizable. Let C be a finite Γ_{k_0}-module and let $a \in \mathsf{Inv}_{k_0}(W, C)$. Assume that every restriction of a to an abelian subgroup of W generated by reflections is zero. Then $a = 0$.*

Note also that this assumption on the base field k_0 is automatically satisfied for Weyl groups since any irreducible real representation of a Weyl group is realizable over the field of rationals $\mathbb{Q}$. However, for other Coxeter groups, this is not the case (for instance, if $W = \mathbb{D}_n$ is the dihedral group of order $2n$, the standard geometric real representation $\rho : W \to \mathsf{GL}_2(\mathbb{R})$ is realizable over $\mathbb{Q}(\cos(\frac{2\pi}{n}))$ but not over $\mathbb{Q}$).

Note finally that we recover exactly Theorem from Theorem 3.1 in case of Weyl groups of type A_n.

In Chapter 4, we deal with Weyl groups of type B_n or C_n. Let now $n \geq 2$ and let W be a Weyl group of type B_n (note that the Weyl group of type C_n is isomorphic to W). Let k be a field of characteristic different from 2. Then $H^1(k, W)$ is in bijection with the set of the isomorphism classes of the pairs (L, α) up to isomorphism, where L is an étale k-algebra and α a square class in L. Set, for any $0 \leq i \leq n$,

$$\begin{array}{rcl} w_i : H^1(./k_0, \mathfrak{S}_n) & \to & H^*(./k_0, \mathbb{Z}/2\mathbb{Z}) \\ (L, \alpha) & \mapsto & w_i(\mathsf{Tr}_L(x^2)) \end{array}.$$

Moreover, note that, for any $(L, \alpha) \in H^1(k, W)$, the isomorphism class of the quadratic form $\mathsf{Tr}_L(\alpha x^2)$ does not depend on the choice of a representative in the square class α. Now set

$$\begin{array}{rcl} \widetilde{w_i} : H^1(./k_0, \mathfrak{S}_n) & \to & H^*(./k_0, \mathbb{Z}/2\mathbb{Z}) \\ (L, \alpha) & \mapsto & w_i(\mathsf{Tr}_L(\alpha x^2)) \end{array}.$$

These invariants are also called Stiefel-Whitney invariants of W.

Theorem. *Let k_0 be a field of characteristic zero, such that -1 and 2 are squares in k_0. Let $n \geq 2$ and let W be a Weyl group of type B_n. Then the $H^*(k_0, \mathbb{Z}/2\mathbb{Z})$-module $\mathsf{Inv}_{k_0}(W, \mathbb{Z}/2\mathbb{Z})$ is free with basis*

$$\{w_i \cdot \widetilde{w_j}\}_{0 \leq i \leq [\frac{n}{2}], 0 \leq j \leq 2([\frac{n}{2}]-i)}.$$

In Chapter 5, we deal with Weyl groups of type D. Let now W be a Weyl group of type D_n ($n \geq 4$). We have the exact sequence

$$1 \longrightarrow W \longrightarrow W' \xrightarrow{p} \mathbb{Z}/2\mathbb{Z} \longrightarrow 1 \ ,$$

where W' is a Weyl group of type B_n and $p : (\epsilon_1, ..., \epsilon_n, \sigma) \mapsto \prod_{i=1}^{n} \epsilon_i$.

Let k_0 be a field of characteristic different from 2. If $a \in \mathsf{Inv}_{k_0}(W', \mathbb{Z}/2\mathbb{Z})$, then $\mathsf{Res}^W_{W'}(a)$ is a cohomological invariant of W. Thus, for $0 \leq i \leq n$, $\mathsf{Res}^W_{W'}(w_i)$ is an invariant of W and is still denoted by w_i. Likewise, for $0 \leq i \leq n$, $\mathsf{Res}^W_{W'}(\widetilde{w_i})$ is an invariant of W and is still denoted by $\widetilde{w_i}$.

Theorem. *Let k_0 be a field of characteristic zero. Let $n \geq 4$ and let W be a Weyl group of type D_n. Then the $H^*(k_0, \mathbb{Z}/2\mathbb{Z})$-module $\mathsf{Inv}_{k_0}(W, \mathbb{Z}/2\mathbb{Z})$ is free with basis*

$$\{w_i \cdot \widetilde{w_j}\}_{0 \leq i \leq [\frac{n}{2}], 0 \leq j \leq 2([\frac{n}{2}]-i) \text{ and } j \text{ even}} \cdot$$

Chapter 1

Galois cohomology

RÉSUMÉ

Dans ce chapitre, on commence par définir le premier ensemble de cohomologie galoisienne d'un groupe et on rappelle que ces ensembles classifient diverses structures algébriques, notamment les algèbres étales, les algèbres étales pointées, les torseurs ou les algèbres galoisiennes. Dans une deuxième partie, on introduit les groupes de cohomologie galoisienne dans le cas abélien munis notamment de l'opération cup-produit, puis on donne les principales propriétés d'applications nommées résidus, qui joueront un rôle crucial tout au long de cette thèse. Dans une troisième et dernière partie, on définit les invariants cohomologiques et on expose les principaux outils décrits dans [24], tels que, par exemple, les torseurs versels.

1.1 Non abelian Galois cohomology

1.1.1 Cohomology of profinite groups

In this section, let us recall the basic results without proof. For further details, we let the reader see [1], Chapter II.

For all this section, let Γ be a profinite group. Recall that it is a topological group which is isomorphic to the inverse limit of an inverse system of finite groups (endowed with the product topology).

Definition 1.1. *Let A be a set endowed with the discrete topology. A left action of Γ on A is called continuous if the stabilizer of each element $a \in A$*

$$\mathsf{Stab}_\Gamma(a) = \{\gamma \in \Gamma \mid \gamma.a = a\}$$

is an open subgroup in Γ.

We call Γ-set any set A endowed with a continuous left action of Γ. We call Γ-group any group A which is a Γ-set and such that Γ acts by group morphisms on A. A morphism of Γ-sets (resp. Γ-groups) $f : A \to B$ is a map (resp. a group morphism) such that, for any $\gamma \in \Gamma$ and any $a \in A$, $f(\gamma.a) = \gamma.f(a)$.

Definition 1.2. *Let A be a Γ-group A. We call 0^{th} cohomology set of Γ with coefficients (or with values) in A the set A^Γ consisting of the Γ-invariant elements of A. We sometimes denote it by $H^0(\Gamma, A)$.*

Definition 1.3. *Let A be a Γ-group. A 1-cocycle or simply a cocycle of Γ with values in A is a continuous map*

$$\begin{aligned} \alpha : \Gamma &\to A \\ \gamma &\mapsto \alpha_\gamma \end{aligned}$$

such that, for all $\gamma, \gamma' \in \Gamma$, $\alpha_{\gamma\gamma'} = \alpha_\gamma \gamma.\alpha_{\gamma'}$. We denote by $Z^1(\Gamma, A)$ the set of the cocycles of Γ with values in A. The constant map $\gamma \mapsto 1$ is called the trivial cocycle.

Remark. If Γ trivially acts on A, then a cocycle is just a group homomorphism from Γ to A.

Lemma 1.1. *Let A be a Γ-group and let $\alpha : \Gamma \to A$ be a cocycle. For any $a \in A$, the map*

$$\begin{aligned} \alpha_a : \Gamma &\to A \\ \gamma &\mapsto a\alpha_\gamma \gamma.a^{-1} \end{aligned}$$

is also a cocycle.

Definition 1.4. *Two cocycles α, α' are cohomologous (denoted by $\alpha \sim \alpha'$) if there exists $a \in A$ such that $\alpha' = \alpha_a$.*

It is easily seen that $\sim$ is an equivalence relation on $Z^1(\Gamma, A)$.

Definition 1.5. *We denote by $H^1(\Gamma, A)$ the set of equivalence classes $Z^1(\Gamma, A)/\sim$ and we call it the first cohomology set of Γ with coefficients in A.*

The set $H^1(\Gamma, A)$ is a pointed set (i.e. a set with a distinguished element called base point, here the cohomology class of the trivial cocycle $\mathbf{1}$).

Proposition 1.1. *Let A and B be two Γ-groups and let $f : A \to B$ be a morphism of Γ-groups. Then, for any cocycle $\alpha \in Z^1(\Gamma, A)$, the map*

$$\begin{aligned} \beta : \Gamma &\to B \\ \gamma &\mapsto f(\alpha_\gamma) \end{aligned}$$

is a cocycle with values in B and the cohomology class of β only depends on the cohomology class of α, which yields a map

$$f_* : H^1(\Gamma, A) \to H^1(\Gamma, B).$$

Let B be a Γ-group and let $A \subset B$ be a Γ-subgroup. Let B/A denote the set of the right cosets of B modulo A. Then B/A is a Γ-set and the natural projection $B \to B/A$ yields by restriction a map $B^\Gamma \to (B/A)^\Gamma$. Let us define a map $(B/A)^\Gamma \to H^1(\Gamma, A)$. Let $b.A \in (B/A)^\Gamma$. Since $b.A$ is invariant by Γ, then for any $\gamma \in \Gamma$, $(\gamma b).A = b.A$ and we have $(b^{-1}\gamma.b).A = b^{-1}.(\gamma b.A) = b^{-1}.(b.A) = A$, thus $\alpha : \gamma \mapsto b^{-1}\gamma.b$ is a map from Γ to A.

Lemma 1.2. *This map is a cocycle with values in A and its cohomology class does not depend on the choice of b in the coset $b.A$.*

Before going further, let us define a morphism of pointed sets : let (E, e), (F, f) be some pointed sets. A morphism of pointed sets $\Phi : (E, e) \to (F, f)$ is a map $\Phi : E \to F$ such that $\Phi(e) = f$. We call kernel of Φ the preimage of the base point f and we denote it by $\mathsf{Ker}(\Phi)$. Note that $\mathsf{Ker}(\Phi) = 1$ does not imply that the map Φ is injective ! Finally, we say that a sequence of morphisms of pointed sets

$$(E, e) \xrightarrow{\Phi} (F, f) \xrightarrow{\Psi} (G, g)$$

is exact if $\mathsf{Ker}(\Psi) = \mathsf{Im}(\Phi)$.

Corollary 1.1. *The induced map $(B/A)^\Gamma \to H^1(\Gamma, A)$ given by the previous construction is a morphism of pointed-sets. We denote it by δ^0 and we call it 0^{th} connecting map.*

Proposition 1.2. *Let B be a Γ-group and let $A \subset B$ be a Γ-subgroup. Then the following sequence of pointed Γ-sets is exact*

$$1 \longrightarrow A^\Gamma \xrightarrow{f_*} B^\Gamma \xrightarrow{g_*} (B/A)^\Gamma \xrightarrow{\delta^0} H^1(\Gamma, A) \xrightarrow{f_*} H^1(\Gamma, B) \ .$$

Corollary 1.2. *There is a bijection between the kernel $\mathsf{ker}(H^1(\Gamma, A) \to H^1(\Gamma, B))$ and the orbit of the group B^Γ in $(B/A)^\Gamma$ (where B^Γ acts by multiplication on the left on $(B/A)^\Gamma$).*

Definition 1.6. *If k is a field, the absolute Galois group $\Gamma_k = \mathsf{Gal}(k_{sep}/k)$ (where k_{sep} denotes a separable closure of k) is a profinite group. The i^{th} Galois cohomology set is the group $H^i(\Gamma_k, A)$ and is denoted by $H^i(k, A)$ for $i = 0, 1$.*

Note that we will define at section 1.2 some cohomology sets of any higher degree when the Γ-group is abelian.

1.1.2 Galois cohomology of algebraic group schemes

This section and the following directly follows the approach of [12], VII,29. We assume that the reader knows the scheme language (at least over a field). Unless stated otherwise, all the schemes considered here are affine and we will not precise it in general. Let us recall the definition of an algebraic group scheme : if k is a field, let Alg_k denote the category of the associative commutative unital k-algebras.

Definition 1.7. *Let k be a field and let $G : \mathsf{Alg}_k \to \mathsf{AbGrps}$ be a covariant functor with values in the category of abelian groups. Then G is an (affine) algebraic group scheme if it is representable as a functor $\mathsf{Alg}_k \to \mathsf{Sets}$ by a k-algebra of finite type.*

Let G be an algebraic group scheme over k. Then the absolute Galois group Γ_k of k continuously acts on $G(k_{\mathsf{sep}})$. Hence, the cohomology sets $H^0(k, G(k_{\mathsf{sep}}))$ and $H^1(k, G(k_{\mathsf{sep}}))$ are well-defined. Let us denote by

$$H^i(k, G) = H^i(k, G(k_{\mathsf{sep}})) \text{ for } i = 0, 1.$$

Note that, in particular, $H^0(k, G) = G(k_{\mathsf{sep}})^{\Gamma_k} = G(k)$.

Any algebraic group scheme homomorphism $f : G \to H$ (which is nothing but a morphism of functors) between two algebraic group schemes G and H, yields by functoriality a Γ_k-homomorphism of $G(k_{\mathsf{sep}})$ in $H(k_{\mathsf{sep}})$ and so a group homomorphism $H^0(k, G) \to H^0(k, H)$ and a morphism of pointed sets

$$H^1(k, G) \to H^1(k, H).$$

Let us now give an important example of algebraic group schemes : the general linear group.

Example 1.1. Let V be a finite dimensional k-vector space. We define the algebraic group scheme $\mathsf{GL}(V)$ to be the functor sending a k-algebra L to the group of the invertible elements of the algebra $\mathsf{End}_k(V) \otimes_k L$ (where $\mathsf{End}_k(V)$ denotes the k-algebra of endomorphisms of V). Thus, we get that, for any k-algebra L,

$$\mathsf{GL}(V)(L) = \mathsf{GL}(V_L)$$

where $V_L = V \otimes_k L$.

Let G be an algebraic group scheme over k and let $\rho : G \to \mathsf{GL}(V)$ be a linear representation of G (i.e. an algebraic group scheme homomorphism : for any k-algebra L, we denote by $\rho(L)$ the linear representation $G(L) \to \mathsf{GL}(V_L)$ given by ρ). Let us fix $v \in V$ and let us identify V with a k-subspace of $V_{\mathsf{sep}} = V \otimes_k k_{\mathsf{sep}}$.

Definition 1.8. *An element $v' \in V_{sep}$ is called a twisted ρ-form of v if*

$$v' = \rho_{sep}(g)(v)$$

for some $g \in G(k_{sep})$, with $\rho_{sep} = \rho(k_{sep})$.

Let us now consider the category $\widetilde{A}(\rho, v)$ whose objects are the twisted ρ-forms of v and whose arrows $v' \to v''$ are the elements $g \in G(k_{\mathsf{sep}})$ such that $\rho_{\mathsf{sep}}(g)(v') = v''$. This category is a connected groupoid (i.e. every arrow has an inverse and there exists at least one arrow between any two objects). Let us denote by $A(\rho, v)$ the groupoid whose objects are the twisted ρ-forms v' of v that belong to V (seen as a k-subspace of V_{sep}) and whose arrows $v' \to v''$ are the elements $g \in G(k)$ such that $\rho(g)(v') = v''$. Hence, if X denotes the Γ_k-set of the objects of $\widetilde{A}(\rho, v)$, X^{Γ_k} is the set of the objects of $A(\rho, v)$. Moreover, the set of the orbits of $G(k)$ in X^{Γ_k} is the set $\mathsf{Isom}(A(\rho, v))$ of the isomorphism classes of $A(\rho, v)$. It is a pointed set with base point the isomorphism class of v.

Let us denote by $\mathsf{Aut}_G(v)$ the stabilizer of v. It is a subgroup of the algebraic group scheme G. Since $G(k_{\mathsf{sep}})$ transitively acts on X, the Γ_k-set X is identified with the set of the cosets of $G(k_{\mathsf{sep}})$ modulo $\mathsf{Aut}_G(v)(k_{\mathsf{sep}})$. By Corollary 1.2, we get a natural bijection between the kernel of $H^1(k, \mathsf{Aut}_G(v)) \to H^1(k, G)$ and the orbit $X^{\Gamma_k}/G(k)$. Thus, we get the following proposition.

Proposition 1.3. *If $H^1(k, G)$ is trivial, there is a natural bijection of pointed sets*

$$\mathsf{Isom}(A(\rho, v)) \widetilde{\to} H^1(k, \mathsf{Aut}_G(v))$$

1.1.3 Classification of algebraic structures and first cohomology sets

Let us recall Hilbert's 90^{th} Theorem (see [12], Theorem 29.2). Recall that a separable algebra over a field k is a k-algebra which is isomorphic to a direct product of finite dimensional simple (i.e. containing no non-trivial two-sided ideal) k-algebras.

Theorem 1.1. *For any associative separable k-algebra A, the first cohomology set $H^1(k, \mathsf{GL}_1(A))$ is trivial.*

Let A be a finite dimensional k-algebra. The multiplication in A yields a linear map $v : A \otimes_k A \to A$. Let V denote the k-vector space $\mathsf{Hom}_k(A \otimes_k A, A)$ and let $G = \mathsf{GL}(A)$ be the linear group of A, seen as a k-vector space. Let us consider the representation $\rho : G \to GL(V)$ given by

$$\rho(g)(v')(x \otimes y) = g \circ v'(g^{-1}(x) \otimes g^{-1}(y))$$

for any $g \in G$, any $v' \in V$ and any $x, y \in A$. A linear map $g \in G$ is an algebra automorphism of A if and only if $\rho(g)(v) = v$. Therefore, the algebraic group schemes $\mathsf{Aut}_{\mathsf{alg}}(A)$ and $\mathsf{Aut}_G(v)$ are equal. A twisted ρ-form of v is a k-algebra A', which is equal as a k-vector space to A (but not necessarily as a k-algebra), such that the k_{sep}-algebras $A'_{\mathsf{sep}} = A' \otimes_k k_{\mathsf{sep}}$ et $A_{\mathsf{sep}} = A \otimes_k k_{\mathsf{sep}}$ are isomorphic. Hence, by Proposition 1.3 and by Hilbert's 90^{th} Theorem, since $\mathsf{GL}_1(\mathsf{End}(V)) = GL(V)$, we get the following result (see [12], 29.8).

Proposition 1.4. *The Galois cohomology set $H^1(k, \mathsf{Aut}_{\mathsf{alg}}(A))$ is in bijection with the set of the isomorphism classes of the k-algebras $A' \in \mathsf{Alg}_k$ such that*

$$A'_{sep} \simeq_{k_{sep}} A_{sep}.$$

Let us explicit the bijection : if $\beta : A_{\mathsf{sep}} \widetilde{\to} A'_{\mathsf{sep}}$ is a k_{sep}-isomorphism, the corresponding cohomology class is represented by the cocycle

$$\alpha_\gamma = \beta^{-1} \circ (\mathsf{Id} \otimes \gamma) \circ \beta \circ (\mathsf{Id} \otimes \gamma^{-1})$$

for all $\gamma \in \Gamma_k$. Conversely, a cohomology class represented by a cocycle α in $Z^1(k, \mathsf{Aut}_{\mathsf{alg}}(A))$ corresponds to the isomorphism class of

$$A' = \{x \in A_{\mathsf{sep}} \mid \alpha_\gamma \circ (\mathsf{Id} \otimes \gamma)(x) = x, \forall \gamma \in \Gamma_k\}.$$

Let us state the following corollary of Hilbert's 90^{th} Theorem ([12], 29.5).

Corollary 1.3. *Let k be a field and let $\mathcal{K} : V = V_0 \supset V_1 \supset \cdots \supset V_k$ be a flag of finite dimensional k-vector spaces. Let also G be its algebraic group scheme of automorphisms over k. Then $H^1(k, G) = 1$.*

Let k be a field and let us consider pairs (A, L) consisting of a k-algebra A and a subalgebra $L \subset A$. An isomorphism of pairs $(A', L') \simeq (A, L)$ is a k-algebra isomorphism $A' \simeq A$ which restricts to an isomorphism $L' \simeq L$. Let G be the group scheme of automorphisms of the flag of vector spaces $A \supset L$. The group G acts on the space $\mathsf{Hom}_k(A \otimes_k A, A)$ as in Proposition 1.4 and, if $m : A \otimes_k A \to A$ is the multiplication map, the group scheme $\mathsf{Aut}_G(m)$ coincides with the group scheme $\mathsf{Aut}_{\mathsf{alg}}(A, L)$ of automorphisms of the pair (A, L). Since $H^1(k, G) = 1$ by Corollary 1.3, Proposition 1.3 yields the following result (see [12], 29.12).

Proposition 1.5. *The Galois cohomology set $H^1(k, \mathsf{Aut}_{\mathsf{alg}}(A, L))$ is in bijection with the set of the isomorphism classes of the pairs (A', L') defined above such that*

$$(A', L')_{sep} \simeq_{k_{sep}} (A, L)_{sep}.$$

Étale algebras

Let us recall the definition of an étale algebra (see [2], V.34 Théorème 4, V.29 Corollaire, V.47 Proposition 1 and V.36 Proposition 3 for proofs and further details).

Proposition 1.6. *Let L be a finite dimensional commutative k-algebra. The following assertions are equivalent :*

(i) $L \simeq K_1 \times \cdots \times K_r$ where, for $i = 1...r$, K_i/k is a finite separable field extension of k.

(ii) $L_{k_{sep}} \simeq k_{sep} \times \cdots \times k_{sep}$

(iii) *the quadratic form*

$$\begin{aligned} q_L : L &\to k \\ x &\mapsto Tr_{L/k}(x^2) \end{aligned}$$

is non-degenerate.

(iv) *the order of the set* $X(L) = \mathsf{Hom}_k(L, k_{sep})$ *is exactly* $\mathsf{dim}_k(L)$.

If moreover the field k *is assumed to be infinite, conditions* (i) *to* (iv) *are equivalent to :*

(v) $L \simeq k[X]/(f)$, *where* f *is a polynomial with coefficients in* k *with only simple roots in an algebraic closure of* k.

Definition 1.9. *We say that a* k*-algebra* L *is étale if it satisfies one of the equivalent assertions of Proposition 1.6 and the integer* $\mathsf{dim}_k(L)$ *is called the degree or the rank of* L .

Note that it directly follows from Proposition 1.6 that étale algebras remain étale after scalar extension.

Proposition 1.7. *The Galois cohomology set* $H^1(k, \mathfrak{S}_n)$ *is in bijection with the set of the isomorphism classes of étale* k*-algebras of degree* n. *Moreover, the cohomology class of the trivial cocycle is sent on the isomorphism class of the split* k*-algebra* k^n.

Note that we consider $\mathfrak{S}_n$ as a constant algebraic group scheme here with a trivial action of the absolute Galois group on $\mathfrak{S}_n(k_{\mathsf{sep}}) = \mathfrak{S}_n$. We let the reader refer to [12], 29.9 for another proof.

Proof. Let $n \geq 1$ and let $A = k \times \cdots \times k = k^n$. The k-algebra A is clearly étale with degree n and $A_{\mathsf{sep}} = k_{\mathsf{sep}}^n$, so the k-algebras A', such that the k_{sep}-algebras $A' \otimes_k k_{\mathsf{sep}}$ and k_{sep}^n are isomorphic, are exactly the étale k-algebras. By Proposition 1.4, we have to compute the k_{sep}-points of the algebraic group scheme $\mathsf{Aut}_{\mathsf{alg}}(k^n)$. Any k_{sep}-algebra automorphism of k_{sep}^n sends an idempotent (i.e. an element e of k_{sep}^n such that $e^2 = e$) to an idempotent. Yet any idempotent of k_{sep}^n may be written $e_I = \sum_{i \in I} e_i$, where I belongs to the subsets of $\{1, ..., n\}$ and where $\{e_i\}_{i \in I}$ denotes the canonical basis of k_{sep}^n (as a k_{sep}-vector space). Since the formula $e_I.e_J = e_{I \cap J}$ is obvious, it is now clear that to determine a k_{sep}-algebra automorphism of k_{sep}^n is the same as to determine the images of the e_i, $i = 1...n$. Let f be a k_{sep}-point of $\mathsf{Aut}_{\mathsf{alg}}(k^n)$. Then $f(e_i) = e_{I_i}$ for some $I_i \subset \{1, ..., n\}$. Since f is injective and $f(0) = 0$, for all $i = 1...n$, $f(e_i) \neq (0, ..., 0)$, which proves that I_i

is non-empty. Furthermore, if $i \neq j \in \{1,...,n\}$, $0 = f(e_i.e_j) = e_{I_i}.e_{I_j} = e_{I_i \cap I_j}$, so $I_i \cap I_j = \emptyset$. Eventually, we get that $\underset{i \in I}{\cup} I_i = \{1,...,n\}$ since

$$(1,...,1) = f(1,...,1) = f(\sum_{i=1}^{n} e_i) = \sum_{i=1}^{n} f(e_i) = \sum_{i=1}^{n} e_{I_i} = e_{\cup_{i=1}^{n} I_i}$$

(we used the obvious formula $e_I + e_J = e_{I \cup J}$). Hence, $(I_1,...,I_n)$ is a partition of the set $\{1,...,n\}$ with no empty term. Thus, each I_i is a singleton and f permutes the e_i for $i = 1...n$. Therefore, the set of the k_{sep}-points of $\mathsf{Aut}_{\mathsf{alg}}(k^n)$ injects into $\mathfrak{S}_n$. Moreover, if $\sigma \in \mathfrak{S}_n$, the algebra homomorphism $e_i \mapsto e_{\sigma(i)}$ is an automorphism. It then shows that the group of the k_{sep}-points of $\mathsf{Aut}_{\mathsf{alg}}(k^n)$ is isomorphic to $\mathfrak{S}_n$. This concludes the proof of Proposition 1.7.■

Pointed étale algebras

Let k be a field of characteristic different from 2. We call pointed étale k-algebra of rank n any couple (L, α) with L an étale k-algebra of rank n and α a square-class in $L^\times$. Let L, L' be étale k-algebras of rank n and let α, α' be square-classes respectively in $L^\times$ and in $L'^\times$. A morphism of pointed étale algebras $(L, \alpha) \to (L', \alpha')$ is a homomorphism $f : L[\sqrt{\alpha}] \to L'[\sqrt{\alpha'}]$ of k-algebras such that $f(L) \subset L'$ and $f(\sqrt{\alpha}) = \lambda\sqrt{\alpha'}$ for some $\lambda \in L'$ (note that by $L[\sqrt{\alpha}]$, we mean the k-algebra $k[X]/(X^2 - \alpha)$). Note that you can find a proof of the following result in [22].

Proposition 1.8. *Let k be any field of characteristic different from 2. The set of the isomorphism classes of the pointed étale k-algebras of rank n is in bijection with the set $H^1(k, W)$, where W is a Weyl group of type B_n (see Appendix A). Moreover the cohomology class of the trivial cocycle is mapped onto the isomorphism class of the pair $(k^n, 1)$.*

Proof. By Proposition 1.5, as the pairs (L, α) are exactly the twisted k-forms of $(k^n, 1)$ up to isomorphism, we just have to see that the automorphism group of $(k^n, 1)$ is W. Note that $k^n[\sqrt{1}] = k^{2n}$ and that $\mathsf{Aut}_k(k^{2n}) = \mathfrak{S}_{2n}$. Let us call $1, 2, ..., 2n$ the $2n$ factors of k^{2n} and let us consider the elements of $\mathsf{Aut}_k(k^n, 1)$ as permutations of $\{1, ..., 2n\}$. We have the morphism

$$\begin{aligned} \Phi : \mathsf{Aut}_k(k^n, 1) &\to \mathsf{Aut}_k k^n \\ f &\mapsto f_{|k^n}. \end{aligned}$$

Then it is easily seen that $\mathsf{Ker}(\Phi)$ consists of the permutations fixing the subsets $\{1, 2\}, \{3, 4\}, ..., \{2n-1, 2n\}$. Thus $\mathsf{Ker}(\Phi)$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^n$. It yields the exact sequence

$$1 \longrightarrow (\mathbb{Z}/2\mathbb{Z})^n \longrightarrow \mathsf{Aut}_k(k^n, 1) \xrightarrow{\Phi} \mathfrak{S}_n \longrightarrow 1\ .$$

Moreover, the inclusion $\mathfrak{S}_n = \mathsf{Aut}_k(k^n) \hookrightarrow W$ splits this exact sequence and $\mathfrak{S}_n$ acts on $\mathsf{Ker}(\Phi)$ by permuting the subsets $\{1,2\},\{3,4\},...,\{2n-1,2n\}$. Therefore $\mathsf{Aut}_k(k^n,1) \simeq W$. ■

More explicitely, the isomorphism class of (L,α) is represented, as a cohomology class, by the cocycle

$$\varphi_{L,\alpha} : \begin{array}{l} \Gamma_k \to W \\ \gamma \mapsto \big((\epsilon_1(\gamma),...,\epsilon_n(\gamma)),\sigma_\gamma\big) \end{array}$$

where, for any $\gamma \in \Gamma_k$:

σ_γ is the permutation induced by the action of γ on $X(L) = \mathsf{Hom}(L, k_{\mathsf{sep}})$

$\epsilon_i(\gamma) = 1$ if γ does not exchange factors $2i-1$ and $2i$ in $L[\sqrt{\alpha}] \otimes_k k_{\mathsf{sep}} \simeq k_{\mathsf{sep}}^{2n}$,
$\epsilon_i(\gamma) = -1$ otherwise.

Interpretation of $H^1(k,W)$ when W is a Weyl group of type D_n

Let $n \geq 4$, let W be a Weyl group of type D_n (see Appendix A). We associate to W its root system

$$S = \{\pm e_i \pm e_j \mid 1 \leq i < j \leq n\}.$$

Let us denote by W' the Weyl group of type B_n corresponding to the root system

$$S' = \{\pm e_i, \pm(e_i \pm e_j) \mid, 1 \leq i \leq n, 1 \leq j \neq i \leq n\}.$$

We clearly have an inclusion $W \subset W'$. More precisely, W is the kernel of the map

$$\begin{array}{rl} p : & W' \to \mathbb{Z}/2\mathbb{Z} \\ & \big((\epsilon_1,...,\epsilon_n),\sigma\big) \mapsto \prod_{i=1}^{n} \epsilon_i. \end{array}$$

Let k be a field of characteristic different from 2. As we saw in the case of a Weyl group of type B_n (see Proposition 1.8), the pointed set $H^1(k,W')$ classifies pairs (L,α) up to isomorphism where L is étale of rank n and α a square-class in $L^\times$.

Proposition 1.9. *The image of the map $H^1(k,W) \to H^1(k,W')$ corresponds to the pairs (L,α) such that any representative of α has norm 1 in L over k. Moreover, the image of the cohomology class of the trivial cocycle corresponds to the isomorphism class of the pair $(k^n,1)$.*

Proof. By Proposition 1.2, we have the following long exact sequence :

$$\cdots \to \mathbb{Z}/2\mathbb{Z} \to H^1(k,W) \to H^1(k,W') \to H^1(k,\mathbb{Z}/2\mathbb{Z}).$$

The image of $H^1(k,W) \to H^1(k,W')$ is then equal to the kernel (i.e. to the preimage of 1) of $H^1(k,W') \to H^1(k,\mathbb{Z}/2\mathbb{Z})$. Let us write $H^1(k,W') \to H^1(k,\mathbb{Z}/2\mathbb{Z})$ in terms of pointed étale algebras. Let us recall that the bijection

$$k^\times/k^{\times 2} \simeq H^1(k,\mathbb{Z}/2\mathbb{Z})$$

is given by : for any $b \in k^\times$, the square-class of b maps to the cohomology class of the cocycle φ_b, where

$$\varphi_b : \Gamma_k \to \mathbb{Z}/2\mathbb{Z}$$
$$\gamma \mapsto \frac{\gamma(\sqrt{b})}{\sqrt{b}}.$$

Let $(L,\alpha) \in H^1(k,W')$. We want to find $\beta \in k^\times/k^{\times 2}$ such that, if $b \in k^\times$ denotes a representative of β, for every $\gamma \in \Gamma_k$,

$$\frac{\gamma(\sqrt{b})}{\sqrt{b}} = \prod_{i=1}^{n} \epsilon_i(\gamma).$$

Note that this quantity does not depend on the choice of such a representative in the square-class β.

Let $a \in L^\times$ be any representative of α. Let us show that $b = N_{L/k}(a)$ agrees. Then $N_{L/k}(a) = \prod_{i=1}^{n} a_i$ where the a_i are the images of a by the different morphisms from L to k_{sep}. Let $\gamma \in \Gamma_k$. We have : $\frac{\gamma(\sqrt{b})}{\sqrt{b}} = \prod_{i=1}^{n} \frac{\gamma(\sqrt{a_i})}{\sqrt{a_i)}}$ and, as $\sqrt{a}$ generates $E = L[\sqrt{\alpha}]$ over L,

$$E \otimes_k k_{\mathsf{sep}} \simeq k_{\mathsf{sep}}(\sqrt{a_1}) \times \cdots \times k_{\mathsf{sep}}(\sqrt{a_n}),$$

so $\frac{\gamma(\sqrt{a_i})}{\sqrt{a_i}}$ is equal to 1 if γ does not exchange the two factors of $k_{\mathsf{sep}}(\sqrt{a_i}) \simeq k_{\mathsf{sep}}^2$, -1 otherwise. Therefore, it is equal to $\epsilon_i(\gamma)$.

To conclude, the cocycle image of (L,α) (with values in $\mathbb{Z}/2\mathbb{Z}$) corresponds to the square-class of $N_{L/k}(a)$ and then the kernel of the map $H^1(k,W') \to H^1(k,\mathbb{Z}/2\mathbb{Z})$ consists of the pairs (L,α) such that the square-class of $N_{L/k}(a)$ is trivial (where a denotes any representative of α in $L^\times$). ■

In the sequel, we will denote by $N_{L/k}(\alpha)$ the square-class of $N_{L/k}(a)$ where a is a representative of α in $L^\times$. Note that triples $(L,\alpha,\partial_{L,\alpha})$ (where L is an étale k-algebra, α a square-class such that $N_{L/k}(\alpha) = 1$ and $\partial_{L,\alpha} : k(\sqrt{N_{L/k}(\alpha)}) \to k^2$ an isomorphism of k-algebras) are classified by the cohomology set $H^1(k,W)$, up to a good notion of isomorphisms on these triples (see [13]).

1.1.4 Torsors and Galois algebras

This section is directly inspired from [12], 18.B and 28.D.

G-torsors and $H^1(k, G)$

Definition 1.10. *Let k be a field and let G be a Γ_k-group. A G-torsor T over k is a non-empty Γ_k-set endowed with a simply transitive right action of G, compatible with the action of Γ_k, i.e. for any $\gamma \in \Gamma_k$, any $g \in G$ and any $t \in T$,*

$$\gamma.(x^g) = (\gamma.x)^g.$$

Let us denote by $G - \mathsf{Tors}_{\Gamma_k}$ the set of the G-torsors over k. A morphism of G-torsors is a map which is G-equivariant and Γ_k-equivariant.

Example 1.2. If $\alpha \in Z^1(k, G)$ is a cocycle, let us endow the set $T_\alpha = G$ with the following Γ_k and G-actions : for any $\gamma \in \Gamma_k$ and any $x, g \in G$, $\gamma \star_\alpha x = \alpha_\gamma \gamma.x$ and $x^g = xg$. Then T_α is a G-torsor over k.

In fact, every G-torsor is isomorphic to a torsor T_α :

Proposition 1.10. *The map $\alpha \mapsto T_\alpha$ yields the following bijection :*

$$H^1(k, G) \widetilde{\to} \mathsf{Isom}(G - \mathsf{Tors}_{\Gamma_k}).$$

Galois algebras

In this paragraph, G is a finite group considered here as a constant algebraic group scheme. We consider étale k-algebras L endowed with an action of G by k-automorphisms. Such algebras are called G-algebras over k. Let us denote by L^G the subalgebra of the G-invariant elements

$$L^G = \{x \in L \mid \forall g \in G, g(x) = x\}.$$

Let L be a G-algebra over k and set $X(L) = \mathsf{Hom}_k(L, k_{\mathsf{sep}})$. Then $X(L)$ is a Γ_k-set and the map

$$\begin{aligned} \mathsf{Aut}_k(L) &\to \mathsf{Aut}_k(X(L)) \\ \alpha &\mapsto (\xi \mapsto \xi \circ \alpha) \end{aligned}$$

is a group isomorphism, with $\mathsf{Aut}_k(X(L))$ the set of the bijections of $X(L)$ compatible with the Γ_k action.

Proposition 1.11. *Let L be a G-algebra over k. Then $L^G = k$ if and only if G acts transitively on $X(L)$.*

Definition 1.11. *Let L be a G-algebra over k such that $\mid G \mid = \mathsf{dim}_k(L)$. We say that L is a Galois G-algebra if $L^G = k$.*

By Proposition 1.11, a G-algebra L over k is Galois if and only if $\mid G \mid = \mathsf{dim}_k(L)$ and the G-action on $X(L)$ is simply transitive, which is equivalent to the fact that $X(L)$ is a G-torsor over k.

Example 1.3. Let L be a Galois G-algebra over k. If L is a field, we get that $G = \mathsf{Aut}_{\mathsf{Alg}_k}(L)$. Therefore, we have a Galois G-algebra structure on a field L if and only if L/k is a Galois field extension isomorphic to G. The G-algebra structure is then given by an isomorphism $G \simeq \mathsf{Gal}(L/k)$.

Furthermore, we have the following correspondence.

Proposition 1.12. *Let G be a finite group. The categories of Galois G-algebras and G-torsors are anti-equivalent. In particular, for any field k, the set $H^1(k, G)$ classifies Galois G-algebras up to isomorphism.*

1.2 Abelian Galois cohomology

Let us recall the construction of the higher Galois cohomology groups in the abelian case. For further details, we let the reader refer to [1], Chapter II and [20].

1.2.1 Higher profinite cohomology groups

Let Γ be a profinite group.

Definition 1.12. *We call Γ-module any abelian Γ-group.*

Let A be a Γ-module. Note that the set $Z^1(\Gamma, A)$ of the 1-cocycles of Γ with coefficients in A is an abelian group with the pointwise multiplication of maps. Since this operation is compatible with the cohomology equivalence relation, the set $H^1(\Gamma, A)$ inherits of an abelian group structure.
Let $n \geq 0$ and let denote by $C^n(\Gamma, A)$ the set of continuous maps from Γ^n to A (note that by convention $C^0(\Gamma, A) = A$). Let us define a map

$$d_n : C^n(\Gamma, A) \to C^{n+1}(\Gamma, A)$$

by induction by : for any $a \in A$,

$$d_0(a) : \gamma \mapsto \gamma.a - a,$$

for any $f \in C^n(\Gamma, A)$,

$$d_n(f) : (\gamma_1, ..., \gamma_{n+1}) \mapsto \gamma_1.f_{\gamma_2,...,\gamma_{n+1}} + \sum_{i=1}^{n} (-1)^i f_{\gamma_1,...,\gamma_i\gamma_{i+1},...,\gamma_{n+1}} + (-1)^{n+1} f_{\gamma_1,...,\gamma_n}.$$

Definition 1.13. *A n-cocycle of Γ with values in A is a continuous map α in $C^n(\Gamma, A)$ such that $d_n(\alpha) = 0$ and $\alpha_{\gamma_1,...,\gamma_n} = 0$ whenever $\gamma_i = 1$ for some $i \in \{1, ..., n\}$.*
A map $\alpha \in C^n(\Gamma, A)$ is a n-coboundary of Γ with values in A if there exists $\beta \in C^{n-1}(\Gamma, A)$ such that $\alpha = d_{n-1}(\beta)$ and $\beta_{\gamma_1,...,\gamma_n} = 0$ whenever $\gamma_i = 1$ for some $i \in \{1, ..., n\}$.

Note that, for $n = 1$, the notion of 1-cocycle is exactly the notion of cocycle, defined in Section 1.1. Note also that by convention, a 1-coboundary is a continuous map in the image of $d_0 : A \to C^1(\Gamma, A)$.

We denote the set of n-cocycles by $Z^n(\Gamma, A)$ and the set of n-coboundaries by $B^n(\Gamma, A)$. It is easily checked that $Z^n(\Gamma, A)$ is an abelian subgroup of $C^n(\Gamma, A)$ and that $B^n(\Gamma, A)$ is a subgroup of $Z^n(\Gamma, A)$ (we have $d_n d_{n-1} = 0$).

Definition 1.14. *The quotient group $Z^n(\Gamma, A)/B^n(\Gamma, A)$ is denoted by $H^n(\Gamma, A)$ and called the n^{th} cohomology group of Γ with coefficients in A. Moreover, two n-cocycles are cohomologous if they have same image in $H^n(\Gamma, A)$.*

The constant map

$$\begin{aligned} \Gamma^n &\to A \\ (\gamma_1, ..., \gamma_n) &\mapsto 1 \end{aligned}$$

is a n-cocycle and is called the trivial n-cocycle.

Proposition 1.13. *Let A, B be Γ-modules and let $f : A \to B$ be a group morphism compatible with the Γ-actions and let $n \geq 0$. For any n-cocycle $\alpha \in Z^n(\Gamma, A)$, the map $f_\star(\alpha) = f \circ \alpha$ is a n-cocycle and the map*

$$\begin{aligned} f_\star : H^n(\Gamma, A) &\to H^n(\Gamma, B) \\ [\alpha] &\mapsto [f_\star(\alpha)] \end{aligned}$$

is a well-defined group morphism.

Proposition 1.14. *For any short exact sequence of Γ-modules*

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0 \,,$$

there are some group morphisms $\delta^n : H^n(\Gamma, C) \to H^n(\Gamma, A)$ called connecting maps such that the following long sequence starting from $n = 0$ is exact.

$$0 \longrightarrow \cdots \longrightarrow H^n(\Gamma, A) \xrightarrow{f_\star} H^n(\Gamma, B) \xrightarrow{g_\star} H^n(\Gamma, C) \xrightarrow{\delta^n} H^{n+1}(\Gamma, A) \longrightarrow \cdots$$

Relations to subgroups

Let Γ be a group, let Γ' be a subgroup of Γ and let A be a Γ-module. Let us denote by $\iota : \Gamma' \to \Gamma$ the inclusion map. Then A also is a Γ'-module, Γ' acting on A by restricting the action of Γ. For any n-cocycle $\alpha \in Z^n(\Gamma, A)$, it is easily seen that the map $\widetilde{\alpha} : (\gamma'_1, ..., \gamma'_n) \mapsto \alpha_{\gamma'_1,...,\gamma'_n}$ belongs to $Z^n(\Gamma', A)$. Furthermore, the following proposition holds.

Proposition 1.15. *Keeping notation above, for any integer $n \geq 0$, the map $\alpha \mapsto \widetilde{\alpha}$ yields a map $H^n(\Gamma, A) \to H^n(\Gamma', A)$, called restriction map and denoted by $\mathsf{Res}_{\Gamma}^{\Gamma'}$.*

Note that when $n = 0$, the restriction map is the inclusion map $A^{\Gamma} \hookrightarrow A^{\Gamma'}$.

Let now Γ' be an open subgroup of Γ of finite index m in Γ and let A be a Γ-module. Then, for any $n \geq 0$, we can construct maps $H^n(\Gamma', A) \to H^n(\Gamma, A)$ called corestriction map and denoted by $\mathsf{Cor}_{\Gamma}^{\Gamma'}$ via the cocycles. We just give here the construction in degree 0 (the reader may refer to [8] for the general construction). Let $\{\gamma_1, ..., \gamma_m\}$ be a system of representatives of the cosets of Γ modulo Γ'. In degree 0, the map is given by

$$\begin{aligned} A^{\Gamma'} &\to A^{\Gamma} \\ a' &\mapsto \sum_{j=1}^{m} \gamma_j.m \end{aligned}$$

Proposition 1.16. *Let Γ be a profinite group, let Γ' be an open subgroup of Γ that has finite index m in Γ and let A be a Γ-module. Then the map*

$$\mathsf{Cor} \circ \mathsf{Res} : H^n(\Gamma, A) \to H^n(\Gamma, A)$$

is the multiplication by m for any $n \geq 0$.

Cup-products

Let Γ be a profinite group and let A and B be Γ-modules. We endow the tensor product $A \otimes_{\mathbb{Z}} B$ of the following Γ-module structure : for any $a \in A$, for any $b \in B$ and for any $\gamma \in \Gamma$, $\gamma.(a \otimes b) = (\gamma.a) \otimes (\gamma.b)$.

Proposition 1.17. *Let $i, j \geq 1$, let $\alpha \in Z^i(\Gamma, A)$ and $\beta \in Z^j(\Gamma, B)$ be two cocycles. The map*

$$\begin{aligned} \Gamma^{i+j} &\to A \otimes_{\mathbb{Z}} B \\ (\gamma_1, ..., \gamma_{i+j}) &\mapsto \alpha_{\gamma_1,...,\gamma_i} \otimes \gamma_1 \cdots \gamma_i.\beta_{\gamma_{i+1},...,\gamma_{i+j}} \end{aligned}$$

is a $(i+j)^{th}$ cocycle and its cohomology class only depends on the cohomology classes of α and β. Moreover, the induced map

$$\cdot : H^i(\Gamma, A) \times H^j(\Gamma, B) \to H^{i+j}(\Gamma, A \otimes_{\mathbb{Z}} B)$$

is $\mathbb{Z}$-bilinear.

Definition 1.15. *This map $\cdot$ is called the cup-product.*

Note that for $i = j = 0$, the cup-product is the natural map $A^\Gamma \times B^\Gamma \to (A \otimes B)^\Gamma$.

The cup-product satisfies the following functorial properties : for any $i, j \geq 0$ and any morphism of Γ-modules $A \to A'$, the following diagram commutes

$$\begin{array}{ccc} H^i(\Gamma, A) \times H^j(\Gamma, B) & \longrightarrow & H^{i+j}(\Gamma, A \otimes B) \\ \downarrow & & \downarrow \\ H^i(\Gamma, A') \times H^j(\Gamma, B) & \longrightarrow & H^{i+j}(\Gamma, A' \otimes B) \end{array} .$$

Note that similar diagrams commute in the second variable.

Proposition 1.18. *The cup-product is an associative, anti-commutative, $\mathbb{Z}$-bilinear and graded operation (note that by anti-commutative, we mean $a \cdot b = (-1)^{ij}(b \cdot a)$ where we identify $A \otimes B$ with $B \otimes A$).*

More generally, given three Γ-modules A, B, C and a Γ-homomorphism $A \times B \to C$, we also call cup-product the pairings

$$H^i(\Gamma, A) \times H^j(\Gamma, B) \to H^{i+j}(\Gamma, C)$$

(by composing the cup-product defined above with $H^{i+j}(\Gamma, A \otimes B) \to H^{i+j}(\Gamma, C)$).

Abelian Galois cohomology

To end this paragraph, let us apply these cohomological constructions to Galois groups. Let k be a field. Recall that Γ_k denotes its absolute Galois group. As already said in Section 1.1, Γ_k is a profinite group. Let also C be a Γ_k-module. For any integer $n \geq 0$, we denote by $H^n(k, C)$ the cohomology group $H^n(\Gamma_k, C)$. For any $n \geq 0$ and any separable field extension K/k (resp. finite separable field extension), we also denote by $\mathsf{Res}_{K/k}$ (resp. by $\mathsf{Cor}_{K/k}$) the restriction map (resp. corestriction map) of K/k.

1.2.2 Galois cohomology modulo 2

Let k be a field of characteristic different from 2. By definition, if $[\alpha]$ and $[\beta]$ are in $H^n(k, \mathbb{Z}/2\mathbb{Z})$, then $[\alpha] + [\beta] = [\alpha\beta]$. In particular, $2[\alpha] = 0$. Let us identify the first cohomology group $H^1(k, \mathbb{Z}/2\mathbb{Z})$ (see for instance [1]).

Proposition 1.19. *The cohomology group $H^1(k, \mathbb{Z}/2\mathbb{Z})$ is isomorphic to $k^\times/k^{\times 2}$.*

More precisely, for any $a \in k^\times$, let us denote by $x_a \in k_{\mathsf{sep}}^\times$ satisfying $x_a^2 = a$. For any $\gamma \in \Gamma_k$, there exists a unique $\epsilon_\gamma \in \mathbb{Z}/2\mathbb{Z}$ such that

$$\frac{\gamma(x_a)}{x_a} = (-1)^{\epsilon_\gamma}.$$

Then the abelian group homomorphism

$$\begin{aligned} k^\times &\to H^1(k, \mathbb{Z}/2\mathbb{Z}) \\ a &\mapsto \big(\gamma \mapsto \epsilon_\gamma\big) \end{aligned}$$

is surjective and has kernel $k^{\times 2}$.

If $a \in k^\times$, we denote by (a) the cohomology class in $H^1(k, \mathbb{Z}/2\mathbb{Z})$ in correspondence with square-class of a in $k^\times$ (via the previous identification). Therefore, we have the equality $(ab) = (a) + (b)$ for any $a, b \in k^\times$.

Moreover, the map

$$\begin{aligned} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} &\to \mathbb{Z}/2\mathbb{Z} \\ (\epsilon_1, \epsilon_2) &\mapsto \epsilon_1\epsilon_2 \end{aligned}$$

is $\mathbb{Z}$-bilinear so we will consider in the sequel the cup-product

$$\cdot : H^i(k, \mathbb{Z}/2\mathbb{Z}) \times H^i(k, \mathbb{Z}/2\mathbb{Z}) \to H^{i+j}(k, \mathbb{Z}/2\mathbb{Z}).$$

Let us end this section by giving useful formulae for the cup-products of cohomology classes in $H^1(k, \mathbb{Z}/2\mathbb{Z})$.

Proposition 1.20. *For all $a, b \in k^\times$, the following properties hold :*

(i) $(a) \cdot (b) = (b) \cdot (a)$.

(ii) $(a) \cdot (b) = 0$ *if and only if b is a norm of $k(\sqrt{a})/k$ (where $k(\sqrt{a})/k = k$ if a is a square in $k^\times$).*

(iii) $(a) \cdot (1 - a) = 0$

(iv) $(a) \cdot (-a) = 0$

(v) $(a) \cdot (a) = (a) \cdot (-1)$.

1.2.3 Residue maps

We let the reader refer to [10], Chapter 6 for the general construction of the residue maps in Galois cohomology. This section follows the approach of [24], Chapters II and III.

Residue map for the Galois cohomology of a local field: the complete case

Let K be a field endowed with a discrete valuation v. Let us denote by k the residue field with respect to v. We set $\Gamma_K = \mathsf{Gal}(K_{\mathsf{sep}}/K)$ and $\Gamma_k = \mathsf{Gal}(k_{\mathsf{sep}}/k)$. Assume that K is complete. The valuation v extends uniquely to K_{sep} and the residue field of K_{sep} is an algebraic closure of k. This yields a surjection $\Gamma_K \to \Gamma_k$. Let us denote by I_K its kernel, and let us call it the inertia group of (K, v). Then the exact sequence

$$1 \longrightarrow I_K \longrightarrow \Gamma_K \longrightarrow \Gamma_k \longrightarrow 1$$

is split.

For the end of this section, let C be a finite Γ_k-module whose order is non-divisible by the residue characteristic. Then C is also a Γ_K-module with trivial action of I.

Theorem 1.2. *For any integer $i \geq 0$, there exists a map*

$$r_i : H^i(K, C) \to H^{i-1}(k, \mathsf{Hom}(I_K, C))$$

such that the sequence

$$0 \longrightarrow H^i(k, C) \xrightarrow{\pi} H^i(K, C) \xrightarrow{r_i} H^{i-1}(k, \mathsf{Hom}(I_K, C)) \longrightarrow 0 \qquad (1.1)$$

is exact.

Let n be an integer not divisible by the characteristic of the residue field k and such that $nC = 0$. We set $C(-1) = \mathsf{Hom}(\mu_n, C)$ where Hom denotes here the continuous homomorphisms. This Γ_k-module is called the -1^{th}-Tate's twist of C. Note that this definition does not depend on the choice of n. We may show that

$$C(-1) \simeq \mathsf{Hom}(I_K, C).$$

We can then write the exact sequence (1.1)

$$0 \longrightarrow H^i(k, C) \xrightarrow{\pi} H^i(K, C) \xrightarrow{r_i} H^{i-1}(k, C(-1)) \longrightarrow 0\,. \qquad (1.2)$$

For any $\alpha \in H^i(K, C)$, the element $r_i(\alpha)$ is called the residue of α. For $x \in K^\times$, we denote by $(x)_n$ the class of x in $K^\times / K^{\times n} = H^1(K, \mu_n)$. We then get the following decomposition

Proposition 1.21. *Let π be a uniformizing element of K. Every $\alpha \in H^i(K, C)$ may be uniquely written as*

$$\alpha = \alpha_0 + (\pi)_n \cdot \alpha_1,$$

with $\alpha_0 \in H^i(k, C)$ and $\alpha_1 \in H^{i-1}(k, C(-1))$. Moreover, $r_i(\alpha) = \alpha_1$.

Residue map for the Galois cohomology of a local field: the non-complete case

Let us consider now a more general situation : we do not assume anymore that K is complete. Keeping the previous notation, we choose an extension $\widetilde{v}$ of the valuation v from K to K_{sep} (it is not unique but two such extensions are conjugate). Let us denote by $\mathsf{Dec}_{\widetilde{v}}$ the corresponding decomposition group $\{\gamma \in \Gamma_K \mid \gamma.\widetilde{v} = \widetilde{v}\}$. Let us denote by K_v the completion of K for the valuation v and by $K_{\mathsf{sep},\widetilde{v}}$ the completion of K_{sep} with respect to $\widetilde{v}$. The subfield $K_{\mathsf{sep}}.K_v$ is the biggest algebraic subextension of K_v in $K_{\mathsf{sep},\widetilde{v}}$. By Krasner's Lemma, $K_{\mathsf{sep}}.K_v$ is separably closed. We then identify it with $(K_v)_{\mathsf{sep}}$. We have

$$\mathsf{Dec}_{\widetilde{v}} = \mathsf{Gal}(K_{\mathsf{sep}}.K_v/K_v) = \mathsf{Gal}((K_v)_{\mathsf{sep}}/K_v) = \Gamma_{K_v}.$$

Let C be a finite Γ_K-module whose order is non-divisible by the characteristic of k. Assume that C is "unramified" at v, i.e. that the inertia group of $\mathsf{Dec}_{\widetilde{v}}$ trivially acts on C. Let $\alpha \in H^i(K, C)$ and let us denote by α_v its image in $H^i(K_v, C) = H^i(\mathsf{Dec}_{\widetilde{v}}, C)$. We define the residue $r_v(\alpha)$ of α to be the residue of α_v in $H^{i-1}(k, C(-1))$ (note that K and K_v have the same residue field k).

Definition 1.16. *If $r_v(\alpha) \neq 0$, we say that α is ramified at v. If $r_v(\alpha) = 0$, we say that α is unramified at v. In the latter case, α_v may be identified with an element of $H^i(k, C)$, denoted by $\alpha(v)$ and called the value of α at v.*

Hence, we get two canonical maps which link the Galois cohomology of K to the Galois cohomology of its residue field k, with respect to the valuation v :

$$r_v : H^i(K, C) \to H^{i-1}(k, C(-1))$$

the residue at v and

$$\mathsf{ker}(r_v) \to H^i(k, C)$$

the value at v. When K is complete, the exact sequence (1.2) implies that the residue map is surjective and that the value map is an isomorphism.

Residue maps and restriction maps

Let us now state a functoriality property for the residue maps. Let (K, v) be a field endowed with a discrete valuation. Let us denote by k its residue field. We do not assume K to be complete for v. Let C be a finite Γ_K-module with order prime to the residue characteristic which is not ramified at v. Let K'/K be a field extension and let v' be an extension of v to K', with ramification index e and residue field k'. We have the residue maps $r_v : H^i(K, C) \to H^{i-1}(k, C(-1))$ and $r'_v : H^i(K', C) \to H^{i-1}(k', C(-1))$.

Proposition 1.22. *Residue maps are compatible with restriction maps:*

(i) the following diagram commutes

$$\begin{array}{ccc} H^i(K, C) & \xrightarrow{r_v} & H^{i-1}(k, C(-1)) \\ \downarrow & & \downarrow e. \\ H^i(K', C) & \xrightarrow{r_{v'}} & H^{i-1}(k', C(-1)) \end{array}$$

where the right vertical map is given by the multiplication by e of the natural map $H^{i-1}(k, C(-1)) \to H^{i-1}(k', C(-1))$.

(ii) The following diagram commutes

$$\begin{array}{ccc} \mathsf{ker}(r_v) & \longrightarrow & H^i(k, C) \\ \downarrow & & \downarrow \\ \mathsf{ker}(r_{v'}) & \longrightarrow & H^i(k', C) \end{array}$$

Residue map for the Galois cohomology of a rational field

Let k be a field. Let us first consider the Galois cohomology of $k(t)$, where t is an indeterminate over k. Let $\mathbb{P}_1 = \mathbb{P}_1(k)$. The function field of $\mathbb{P}_1$ is $K = k(t)$. A closed point P of $\mathbb{P}_1$ identifies with a discrete valuation v on K, which is trivial on k given by

$$\begin{aligned} v : K &\to \mathbb{Z} \\ f &\mapsto \mathsf{ord}_P(f). \end{aligned}$$

Let V be the set of these valuations. Assume that C is a finite Γ_k-module whose order n is not divisible by the characteristic of k. Let us denote, for any $v \in V$, by K_v the completion of K at v. It is a local field and its residue field $k(v)$ is a finite extension of k. We then have a residue map $r_v : H^i(K, C) \to H^{i-1}(k(v), C(-1))$.

Lemma 1.3. *Let $\alpha \in H^i(K, C)$. The set of the valuations where α is ramified is finite.*

Therefore, the following map is well-defined :

$$\oplus r_v : H^i(K,C) \to \underset{v\in V}{\oplus} H^{i-1}(k(v), C(-1))$$
$$\alpha \mapsto (r_v(\alpha))_{v\in V}.$$

Theorem 1.3. *The following sequence is exact*

$$0 \longrightarrow H^i(k,C) \xrightarrow{\pi} H^i(K,C) \xrightarrow{\oplus r_v} \bigoplus_{v\in V} H^{i-1}(k(v), C(-1))$$
$$\xrightarrow{c} H^{i-1}(k, C(-1)) \longrightarrow 0,$$

where c denotes the direct sum of the corestriction maps

$$\mathsf{Cor} : H^{i-1}(k(v), C(-1)) \to H^{i-1}(k, C(-1)).$$

Definition 1.17. *An element of $H^i(K,C)$ is constant if it lies in the image of $H^i(k,C) \to H^i(K,C)$. The equation $c \circ (\oplus r_v) = 0$ is called the residue formula.*

The point at the infinity of $\mathbb{P}_1$ defines a place denoted by ∞, with residue field $k(\infty) = k$. The corresponding corestriction map is then the identity. Hence, we get from Theorem 1.3:

Corollary 1.4. *The following sequence is exact*

$$0 \longrightarrow H^i(k,C) \xrightarrow{\pi} H^i(K,C) \xrightarrow{\underset{v\in V\setminus\{\infty\}}{\oplus} r_v} \bigoplus_{v\in V\setminus\{\infty\}} H^{i-1}(k(v), C(-1)) \longrightarrow 0\,.$$

Definition 1.18. *An element $\alpha \in H^i(K,C)$ is unramified (resp. unramified outside $0,\infty$) if its residue at any $v \in V$ (resp. at any $v \in V \setminus \{0,\infty\}$) is zero.*

By the residue formula, $\alpha \in H^i(K,C)$ is unramified if its residues over the affine line are all zero. We denote by $H^i_{\mathsf{unr}}(K,C)$ (resp. by $H^i_{\mathsf{unr,\ outside}\{0,\infty\}}(K,C)$) the corresponding group. Corollary 1.4 shows that any unramified element α belongs to $H^i(k,C)$, which means that $H^i_{\mathsf{unr}}(K,C) = H^i(k,C)$.

If $\alpha \in H^i_{\mathsf{unr,\ outside}\{0,\infty\}}(K,C)$ has residue $\alpha_1 \in H^{i-1}(k, C(-1))$ at 0, then the cohomology class $\alpha - (t)_n.\alpha_1$ is unramified.

Corollary 1.5. *Let $\alpha \in H^i_{\mathit{unr,\ outside}\{0,\infty\}}(K,C)$. Then α may be uniquely written $\alpha_0 + (t)_n.\alpha_1$, with $\alpha_0 \in H^i(k,C)$ and $\alpha_1 \in H^{i-1}(k, C(-1))$. Moreover, we have $r_{v_0}(\alpha) = \alpha_1$.*

To end this section, let us generalize these results to the Galois cohomology of $k(t_1, ..., t_n)$. Recall that C is a finite Γ_k-module with order prime to the characteristic of the residue field.

Theorem 1.4. *Let $n \geq 1$ and let $K = k(t_1, ..., t_n)$ be a rational field with n indeterminates.*

(i) The natural map $H^i(k, C) \to H^i(K, C)$ is injective.

(ii) Let $\alpha \in H^i(K, C)$ be an element whose residues are zero at any discrete valuations of K, which are trivial on k (they correspond to the irreducible hypersurfaces of the affine space Aff^n of dimension n). Then α is constant (i.e. lies in the image of the map $H^i(k, C) \to H^i(K, C)$).

1.3 Cohomological invariants

Let us now introduce the notion of cohomological invariants (we still follow here the approach of [24], Chapter I). Let k_0 be a field and let G be a smooth algebraic group scheme over k_0. We consider the functor $H^1(./k_0, G)$ from the category of the field extensions of k_0 to the category of the sets, given by

$$H^1(./k_0, G) : k/k_0 \mapsto H^1(k, G).$$

Let now C be a finite Γ_{k_0}-module whose order is not divisible by the characteristic of k_0. We denote by $H^*(./k_0, C)$ the functor from the category of the field extensions of k_0 to the category of the abelian groups, given by

$$H^*(./k_0, C) : k/k_0 \mapsto H^*(k, C) = \bigoplus_{i \geq 0} H^i(k, C).$$

Since we have seen in the previous section that the functor H is quite well understood, we want to understand the functor A thanks to the functor H.

Definition 1.19. *A cohomological invariant of G over k_0 with coefficients in C is a morphism of functors from $H^1(./k_0, G)$ to $H^*(./k_0, C)$ is called a cohomological invariant of G over k_0 with coefficients in C. The group of all these cohomological invariants is denoted by $\mathsf{Inv}_{k_0}(G, C)$.*

Note that we consider the functor $H^*(./k_0, C)$ with values in the category of sets. Rephrasing Definition 1.19, $a \in \mathsf{Inv}_{k_0}(G, C)$ if and only if, for any extension k/k_0, there is a map $a_k : H^1(k, G) \to H^*(k, C)$ and if for any extensions k/k_0 and k'/k, the following diagrams commute

$$\begin{array}{ccc} H^1(k, G) & \xrightarrow{a_k} & H^*(k, C) \\ \downarrow & & \downarrow \\ H^1(k', G) & \xrightarrow{a_{k'}} & H^*(k', C) \end{array} .$$

Definition 1.20. *Let $\alpha \in H^*(k_0, C)$. For any extension k/k_0, let $(a^\alpha)_k$ be the constant map with value the image of α by the restriction map $H^*(k_0, C) \to H^*(k, C)$. These maps clearly define an invariant a_α called a constant invariant.*

It then yields a natural embedding $H^*(k_0, C) \hookrightarrow \mathsf{Inv}_{k_0}(G, C)$.

Definition 1.21. *An element $a \in \mathsf{Inv}_{k_0}(G, C)$ is normalized if $a_{k_0}([1]) = 0$, where $[1]$ denotes the cohomology class of the trivial cocycle in $H^1(k_0, G)$.*

Proposition 1.23. *Every cohomological invariant $a \in \mathsf{Inv}_{k_0}(G, C)$ may be written in a unique way as the sum of a constant invariant and a normalized invariant.*

1.3.1 Cohomological invariants and ramification

Before going further, let us give the more general definition of a torsor over a smooth variety.

Definition 1.22. *Let G be a smooth algebraic group scheme over k_0 and let X be a smooth variety over k_0. A G-torsor over X is a locally flat scheme T of finite type over X such that G acts freely (at right) on T and such that the map*

$$\begin{aligned} G \times_X T &\to T \times_X T \\ (g, t) &\mapsto (t, t^g) \end{aligned}$$

is an isomorphism.

Let K/k_0 be a field extension with a discrete valuation v on K. Let us denote by R its valuation ring and by k its residue field. Assume that R contains k_0; thus, R, K and k are k_0-algebras (for k, via the compositum $k_0 \hookrightarrow R \to k$). Assume moreover that K is complete for v.

Let T_k be a G-torsor over k. Then there is a G-torsor over R denoted by T_R whose special fiber is T_k and this torsor is unique up to isomorphism (see [7], p.401, Prop. 8.1). Furthermore, since every G-torsor over R yields by basis extension a G-torsor over K, this defines a map $i : H^1(k, G) \to H^1(K, G)$. We then state Rost's compatibility theorem (see [24], 11.1).

Theorem 1.5. *If $a \in \mathsf{Inv}_{k_0}(G, C)$, the following diagram commutes :*

$$\begin{array}{ccc} H^1(k, G) & \xrightarrow{i} & H^1(K, G) \\ {\scriptstyle a_k}\downarrow & & \downarrow{\scriptstyle a_K} \\ H(k, C) & \xrightarrow{j} & H(K, C) \end{array},$$

where j denotes the natural map induced by the quotient map $\Gamma_K \to \Gamma_k$.

We do not assume anymore that K is complete. It is still true that every G-torsor T over R yields a G-torsor T_k over k and a G-torsor T_K over K. We have the following result (see [24], 11.7).

Theorem 1.6. *For any $a \in \mathsf{Inv}_{k_0}(G, C)$, if α denotes $a(T_K)$, then*

(i) the residue of α at v is zero.

(ii) the value of α at v is $a(T_k)$.

1.3.2 Cohomological invariants and versal torsors

Let us define the notion of versal torsor (see [24], 5.1).

Definition 1.23. *Let k_0 be a field and let G be a smooth algebraic group scheme over k_0. A versal G-torsor is a G-torsor P over an extension field K/k_0 such that there exist a smooth irreducible variety X over k_0 with function field K and a G-torsor $Q \to X$ with basis X satisfying the two following properties :*

(i) the fiber of Q at the generic point of X is P;

(ii) for any field extension k/k_0 with k infinite, for any G-torsor T over k and for any open non-empty subvariety U of X, there exists $x \in U(k)$ whose fiber Q_x is isomorphic to T (i.e. the set $\{x \in X(k) \mid Q_x \simeq T\}$ is dense in X).

Then a cohomological invariant is uniquely determined by its value on a versal torsor (see [24], 12.3).

Theorem 1.7. *Let k_0 be a field, let G be a smooth algebraic group scheme over k_0 and let $P \in H^1(K, G)$ be a versal torsor over k_0. Let a, b be two cohomological invariants in $\mathsf{Inv}_{k_0}(G, C)$. If $a(P) = b(P)$ in $H^*(K, C)$, then $a = b$.*

Note that Theorem 1.7 shows that the map

$$\begin{aligned} \mathsf{Inv}(G, C) &\to H^*(K, C) \\ a &\mapsto a(P) \end{aligned}$$

is injective. Hence, we may see the set $\mathsf{Inv}_{k_0}(G, C)$ as a subgroup of $H^*(K, C)$.

Chapter 2

Examples

RÉSUMÉ

Dans ce chapitre, on fournit des exemples explicites d'invariants cohomologiques, en rappelant d'abord les résultats de Serre sur les invariants cohomologiques des groupes 2-élémentaires, du groupe orthogonal et du groupe symétrique. En particulier, on définit les invariants de Stiefel-Whitney pour les formes quadratiques ainsi que pour le groupe symétrique et qui forment une base du module des invariants cohomologiques de ces groupes. Ensuite, on calcule explicitement les invariants cohomologiques du groupe alterné $\mathfrak{A}_5$ et du groupe de Coxeter exceptionnel de type H_3, puis des groupes diédraux $\mathbb{D}_n$ où n n'est pas divisible par 4 et enfin du groupe diédral $\mathbb{D}_4$, isomorphe au groupe de Weyl de type B_2.

2.1 Cohomological invariants of 2-elementary abelian groups

This section follows the approach of [24], 16. We only consider here invariants with coefficients in $\mathbb{Z}/p\mathbb{Z}$, where p is a prime number different from the characteristic of the base field k_0 (most of time, we will take $p = 2$). In this situation, the cup-product endows the group $\mathsf{Inv}_{k_0}(G, \mathbb{Z}/p\mathbb{Z})$ with the structure of a $H^*(k_0, \mathbb{Z}/p\mathbb{Z})$-module. In the sequel, we describe this module structure in several cases.

2.1.1 Cohomological invariants of $\mathbb{Z}/2\mathbb{Z}$

In this paragraph, all the fields considered have characteristic different from 2. Recall that, for any field k (of characteristic different from 2),

$$H^1(k, \mathbb{Z}/2\mathbb{Z}) \simeq k^\times/k^{\times 2}$$

(see Section 1.2.2). Let k_0 be a field. It is easily seen that, for any field extension k/k_0, the maps

$$\begin{aligned} H^1(k, \mathbb{Z}/2\mathbb{Z}) &\to H^0(k, \mathbb{Z}/2\mathbb{Z}), \\ \varphi &\mapsto 1 \end{aligned}$$

yield a cohomological invariant of $\mathbb{Z}/2\mathbb{Z}$, denoted by $\underline{1}$. Likewise, for any extension k/k_0 the identity maps

$$\mathsf{id} : H^1(k, \mathbb{Z}/2\mathbb{Z}) \to H^1(k, \mathbb{Z}/2\mathbb{Z})$$

also yield a cohomological invariant of $\mathbb{Z}/2\mathbb{Z}$, denoted by $\underline{\mathsf{id}}$.

We then have the following result (see [24], 16.2)

Proposition 2.1. *The $H^*(k_0, \mathbb{Z}/2\mathbb{Z})$-module $\mathit{Inv}_{k_0}(\mathbb{Z}/2\mathbb{Z}), \mathbb{Z}/2\mathbb{Z})$ is free with basis $\{\underline{1}, \underline{id}\}$.*

2.1.2 Cohomological invariants of a direct product of groups

Let G and G' be smooth algebraic group schemes over k_0 and let p be a prime number different from $\mathsf{char}(k_0)$. We set $C = \mathbb{Z}/p\mathbb{Z}$ here. Then we have the following statement (see [24], Exercise 16.5).

Proposition 2.2. *Let us assume that there exists a family $(a_j)_{j\in J}$ of elements of $\mathit{Inv}_{k_0}(G, \mathbb{Z}/p\mathbb{Z})$ such that, for every field extension k/k_0, the images of the a_j $(j \in J)$ in $\mathit{Inv}_k(G, \mathbb{Z}/p\mathbb{Z})$ form an $H^*(k, \mathbb{Z}/p\mathbb{Z})$-basis of $\mathit{Inv}_k(G, \mathbb{Z}/p\mathbb{Z})$. Then there is an $H^*(k_0, \mathbb{Z}/p\mathbb{Z})$-linear automorphism*

$$\mathit{Inv}_{k_0}(G, \mathbb{Z}/p\mathbb{Z}) \otimes_{H^*(k_0, \mathbb{Z}/p\mathbb{Z})} \mathit{Inv}_{k_0}(G', \mathbb{Z}/p\mathbb{Z}) \simeq \mathit{Inv}_{k_0}(G \times G', \mathbb{Z}/p\mathbb{Z}).$$

Proof. Since, for any extension k/k_0, $H^1(k, G \times G') \simeq H^1(k, G) \times H^1(k, G')$, we denote the elements of $H^1(k, G \times G')$ by pairs of cohomology classes (α, α') with $\alpha \in H^1(k, G)$ and $\alpha' \in H^1(k, G')$.

If $a \in \mathsf{Inv}_{k_0}(G, \mathbb{Z}/p\mathbb{Z})$ and $a' \in \mathsf{Inv}_{k_0}(G', \mathbb{Z}/p\mathbb{Z})$, we can define a cohomological invariant $a \cdot a'$ of $\mathsf{Inv}_{k_0}(G \times G', \mathbb{Z}/p\mathbb{Z})$ via the maps

$$\begin{aligned} a_k \cdot a'_k : H^1(k, G \times G') &\to H^*(k, \mathbb{Z}/p\mathbb{Z}) \\ (\alpha, \alpha') &\mapsto a_k(\alpha) \cdot a'_k(\alpha') \end{aligned}$$

where k runs through all field extensions over k_0. This yields a map Θ from $\mathsf{Inv}_{k_0}(G,\mathbb{Z}/p\mathbb{Z}) \times \mathsf{Inv}_{k_0}(G',\mathbb{Z}/p\mathbb{Z})$ to $\mathsf{Inv}_{k_0}(G\times G',\mathbb{Z}/p\mathbb{Z})$. Since the cup-product endows the groups $\mathsf{Inv}_{k_0}(G,\mathbb{Z}/p\mathbb{Z})$ and $\mathsf{Inv}_{k_0}(G',\mathbb{Z}/p\mathbb{Z})$ with the structure of an $H^*(k_0,\mathbb{Z}/p\mathbb{Z})$-$H^*(k_0,\mathbb{Z}/p\mathbb{Z})$-bimodule, then the cup-product endows the tensor product $\mathsf{Inv}_{k_0}(G,\mathbb{Z}/p\mathbb{Z}) \otimes_{H^*(k_0,\mathbb{Z}/p\mathbb{Z})} \mathsf{Inv}_{k_0}(G',\mathbb{Z}/p\mathbb{Z})$ with the structure of a module over $H^*(k_0,\mathbb{Z}/p\mathbb{Z})$. Moreover, since the cup-product is $\mathbb{Z}$-bilinear and associative, the map Θ is $H^*(k_0,\mathbb{Z}/p\mathbb{Z})$-bilinear. We then get from Θ a map

$$c_{G,G'} : \mathsf{Inv}_{k_0}(G,\mathbb{Z}/p\mathbb{Z}) \otimes_{H^*(k_0,\mathbb{Z}/p\mathbb{Z})} \mathsf{Inv}_{k_0}(G',\mathbb{Z}/p\mathbb{Z}) \to \mathsf{Inv}_{k_0}(G\times G',\mathbb{Z}/p\mathbb{Z}),$$

which is $H^*(k_0,\mathbb{Z}/p\mathbb{Z})$-linear. Let us show that $c_{G,G'}$ is an isomorphism. Let us prove, for instance, the surjectivity of this map (the proof of the injectivity being left to the reader since it may be proved similarly to the surjectivity).

Let $a \in \mathsf{Inv}_{k_0}(G\times G',\mathbb{Z}/p\mathbb{Z})$. Let k/k_0 be a field extension and let $\alpha' \in H^1(k,G')$. Then, for any field extension k'/k, the maps

$$\begin{aligned}(a^{k,\alpha'})_{k'} : H^1(k',G) &\to H^*(k',\mathbb{Z}/p\mathbb{Z})\\ \alpha &\mapsto a_{k'}(\alpha, \mathsf{Res}_{k'/k}(\alpha'))\end{aligned}$$

clearly define a cohomological invariant $a^{k,\alpha'} \in \mathsf{Inv}_k(G,\mathbb{Z}/p\mathbb{Z})$. By assumption, the images of the elements of the family $(a_j)_{j\in J}$ (that we still denote by a_j, $j\in J$) form a basis of $\mathsf{Inv}_k(G,\mathbb{Z}/p\mathbb{Z})$. Therefore, there are some uniquely determined coefficients $c_j^{k,\alpha'} \in H^*(k,\mathbb{Z}/p\mathbb{Z})$ (for $j\in J$) such that $a^{k,\alpha'} = \sum_{j\in J} c_j^{k,\alpha'} \cdot a_j$. Now set $j\in J$ and let us show that the maps

$$\begin{aligned}(c_j)_k : H^1(k,G') &\to H^*(k,\mathbb{Z}/p\mathbb{Z})\\ \alpha' &\mapsto c_j^{k,\alpha'}\end{aligned}$$

define a cohomological invariant of G' over k_0, when k runs through all field extensions over k_0.

Let k be an extension of k_0 and let k' be an extension of k. We then have to show the commutativity of the diagram

$$\begin{array}{ccc} H^1(k,G') & \xrightarrow{(c_j)_k} & H^*(k,\mathbb{Z}/p\mathbb{Z}) \\ \Big\downarrow{\scriptstyle \mathsf{Res}_{k'/k}} & & \Big\downarrow{\scriptstyle \mathsf{Res}_{k'/k}} \\ H^1(k',G') & \xrightarrow[(c_j)_{k'}]{} & H^*(k',\mathbb{Z}/p\mathbb{Z}) \end{array}$$

i.e. for any cohomology class $\alpha' \in H^1(k,G')$, $\mathsf{Res}_{k'/k}(c_j^{k,\alpha'}) = c_j^{k',\mathsf{Res}_{k'/k}(\alpha')}$.

Let $\alpha' \in H^1(k, G')$. We have

$$a^{(k', \mathsf{Res}_{k'/k}(\alpha'))} = \sum_{j \in J} c_j^{k', \mathsf{Res}_{k'/k}(\alpha')} \cdot a_j$$

We also have, for any extension k''/k,

$$\begin{aligned} \mathsf{Res}_{k'k''/k''} \circ (a^{(k,\alpha')})_{k''} &= \mathsf{Res}_{k'k''/k''}\big(\sum_{j \in J} c_j^{k,\alpha'} \cdot (a_j)_{k''}\big) \\ &= \sum_{j \in J} \mathsf{Res}_{k'/k}(c_j^{k,\alpha'}) \cdot (a_j)_{k'k''} \circ \mathsf{Res}_{k'k''/k''} \end{aligned}$$

since the a_j $(j \in J)$ are cohomological invariants over k.

Note first that $\mathsf{Res}_{k'/.} \circ (a^{k,\alpha'})_.$ is a cohomological invariant of G over k'. Indeed, if k''/k' is an extension, $\mathsf{Res}_{k'k''/k''} \circ (a^{k,\alpha'})_{k''} = (a^{k,\alpha'})_{k''}$ and we are done since $a^{k,\alpha'}$ is a cohomological invariant of G.

Let us show that the cohomological invariants $a^{k', \mathsf{Res}_{k'/k}(\alpha')}$ and $\mathsf{Res}_{k'/.} \circ (a^{k,\alpha'})_.$ of G over k' are equal. Let k''/k' be a field extension and let $\alpha \in H^1(k'', G)$. We have

$$\mathsf{Res}_{k'k''/k''} \circ (a^{k,\alpha'})_{k''}(\alpha) = a_{k''}^{k,\alpha'}(\alpha) = a''_k(\alpha, \mathsf{Res}_{k''/k}(\alpha'))$$

and

$$(a^{k', \mathsf{Res}_{k'/k}(\alpha')})_{k''}(\alpha) = a_{k''}\big(\alpha, \mathsf{Res}_{k''/k'}(\mathsf{Res}_{k'/k}(\alpha'))\big).$$

Yet it is well-known (see for example [1], p.93) that as $k''/k'/k$ is a tower of extensions,

$$\mathsf{Res}_{k''/k} = \mathsf{Res}_{k''/k'} \circ \mathsf{Res}_{k'/k},$$

which proves the equalities between the two considered invariants.

Therefore, we get that

$$\begin{aligned} \sum_{j \in J} c_j^{k', \mathsf{Res}_{k'/k}(\alpha')} \cdot a_j = a^{k', \mathsf{Res}_{k'/k}(\alpha')} &= \mathsf{Res}_{k'/.} \circ (a^{k,\alpha'})_. \\ &= \sum_{j \in J} \mathsf{Res}_{k'/k}(c_j^{k,\alpha'}) \cdot a_j \end{aligned}$$

Thus, as the family $(a_j)_{j \in J}$ makes up an $H^*(k', \mathbb{Z}/p\mathbb{Z})$-basis of $\mathsf{Inv}_{k'}(G, \mathbb{Z}/p\mathbb{Z})$, it is in particular a free family, so we obtain that, for any $j \in J$,

$$c_j^{k', \mathsf{Res}_{k'/k}(\alpha')} = \mathsf{Res}_{k'/k}(c_j^{k,\alpha'}).$$

Therefore, for any $j \in J$, c_j is a cohomological invariant of G' over k_0 with coefficients in $\mathbb{Z}/p\mathbb{Z}$. We then can conclude that $a = \sum_{j \in J} c_j \cdot a_j$, which is a cohomological

invariant in $\mathsf{Inv}_{k_0}(G \times G', \mathbb{Z}/p\mathbb{Z})$ and it obviously lies in the image of $c_{G,G'}$ (a preimage is $\sum_{j \in J} a_j \otimes c_j$, up to a sign coming from the anti-commutativity of the cup-product). ■

Let us apply Proposition 2.2 to 2-elementary abelian groups. Let $G = (\mathbb{Z}/2\mathbb{Z})^n$. Recall that

$$H^1(k, G) \simeq H^1(k, \mathbb{Z}/2\mathbb{Z}) \times \cdots \times H^1(k, \mathbb{Z}/2\mathbb{Z}) \text{ and that } H^1(k, \mathbb{Z}/2\mathbb{Z}) \simeq k^\times / k^{\times 2}.$$

Let $I \subset \{1, ..., n\}$. For any k/k_0, let us define

$$\begin{aligned} (a_I)_k : H^1(k, G) &\to H^i(k, \mathbb{Z}/2\mathbb{Z}) \\ (x_1, ..., x_n) &\mapsto (x_I) \end{aligned}$$

where i denotes the cardinality of I and (x_I) denotes the cup product of the (x_i)'s, $i \in I$. It is clear that these maps define a cohomological invariant of G.

Actually, these invariants form a basis of $\mathsf{Inv}_{k_0}(G, \mathbb{Z}/2\mathbb{Z})$ ([24], Theorem 16.4), which can easily be proved by induction from Proposition 2.1 and Proposition 2.2.

Corollary 2.1. *Let $n \geq 1$ and $G = (\mathbb{Z}/2\mathbb{Z})^n$. Then the $H^*(k_0, \mathbb{Z}/2\mathbb{Z})$-module $\mathsf{Inv}_{k_0}(G, \mathbb{Z}/2\mathbb{Z})$ is free with basis $(a_I)_{I \subset \{1,...,n\}}$.*

2.2 Restriction to subgroups

This section is directly inspired from [24], Chapter V. We recall here some tools to determine the cohomological invariants of an algebraic group scheme G thanks to the invariants of some subgroups.

Let k_0 be a field, let G be a smooth algebraic group scheme over k_0 and let C be a finite Γ_{k_0}-module whose order is not divisible by $\mathsf{char}(k_0)$. Let us define the restriction of invariants.

Definition 2.1. *If $a \in \mathsf{Inv}_{k_0}(G, C)$ and if H is a subgroup of G, the restriction $\mathsf{Res}^H_G(a)$ of a to H is the compositum of the two following morphisms of functors :*

$$H^1(./k_0, H) \longrightarrow H^1(./k_0, G) \xrightarrow{a} H^*(./k_0, C) \ .$$

Let us study the image of the restriction map. Let us denote by N the normalizer of H in G. For any $g \in N(k_0)$, the inner map

$$\begin{aligned} i_g : H &\to H \\ h &\mapsto ghg^{-1} \end{aligned}$$

is an automorphism of H. Thus $N(k_0)$ acts on $\mathsf{Inv}_{k_0}(H,C)$: if $a \in \mathsf{Inv}_{k_0}(G,C)$ and $g \in N(k_0)$, we set, for any extension k/k_0,

$$\begin{aligned} g.a : H^1(k,G) &\to H^*(k,C). \\ [\varphi] &\mapsto a_k([i_g \circ \varphi]) \end{aligned}$$

Note that in order to lighten the notation, we have made the confusion between $g \in N(k_0)$ and its image in $N(k)$. We then have the following proposition (see [24], 13.2).

Proposition 2.3. *The following properties hold :*

1. *The action of $N(k_0)$ factors through $N(k_0)/H(k_0)$.*
2. *If $a \in \mathsf{Inv}_{k_0}(H,C)$ lies in the image of the restriction map Res_G^H, then a is fixed by $N(k_0)/H(k_0)$.*

This proposition leads us to look for subgroups H of G with injective restriction map Res_G^H and/or such that the image of the restriction map is exactly the set of the H-invariants fixed by $N(k_0)/H(k_0)$.

For the rest of this section, let G be a finite group (viewed as a constant algebraic group scheme). Let H be a subgroup of G. Recall that C has finite order. Let us state the following important result (see [24], Corollary 15.4).

Proposition 2.4. *If the index $[G : H]$ is prime to the order of C, then the restriction map $\mathsf{Res}_G^H : \mathsf{Inv}_{k_0}(G,H) \to \mathsf{Inv}_{k_0}(H,C)$ is injective.*

This applies in particular when H is a p-Sylow subgroup of G and C is a p-group. Let us look at a special case where the image of the restriction map is exactly the invariants fixed by the normalizer (see [24], Example 15.7).

Proposition 2.5. *Let G be a finite group, let H be a p-Sylow subgroup of G and let C be a p-group. Assume that H is abelian. Then an invariant $a \in \mathsf{Inv}_{k_0}(H,C)$ lies in the image of the restriction map Res_G^H if and only if a is fixed under the action of N/H.*

Let us end this section by giving an example of such submodules fixed under the action of a normalizer.

Example 2.1. Let $n \geq 2$ and let W be a Weyl group of type B_n (see A). Its associated root system is $S = \{\pm e_i, \pm e_i \pm e_j, 1 \leq i \neq j \leq n\}$. Set $S_0 = \{\pm e_1, ..., \pm e_n\}$. The subgroup H_0 of W generated by the reflections corresponding to the roots in S_0 is clearly isomorphic to $(\mathbb{Z}/2\mathbb{Z})^n$. By Corollary 2.1, the family of invariants

$\{a_I\}_{I\subset\{1,\dots,n\}}$ is a basis of the $H^*(k_0,\mathbb{Z}/2\mathbb{Z})$-module $\mathsf{Inv}_{k_0}(H_0,\mathbb{Z}/2\mathbb{Z})$. Let us identify the invariants fixed by the normalizer N_0 of H_0. Since W permutes the lines $\mathbb{R}e_i$ $(1\leq i\leq n)$, we have $N_0=W$. Moreover, we have the exact split sequence

$$1\longrightarrow H_0\longrightarrow W\longrightarrow \mathfrak{S}_n\longrightarrow 1\ .$$

Thus, $N_0/H_0\simeq\mathfrak{S}_n$ and acts on H_0 by permuting the coordinates. Proposition 2.6 then follows easily.

Proposition 2.6. *For $0\leq i\leq n$, the cohomological invariants*

$$a_i^{(0)}=\sum_{I\subset\{1,\dots,n\};|I|=i} a_I$$

form a basis of the submodule $\mathsf{Inv}_{k_0}(H_0,\mathbb{Z}/2\mathbb{Z})^{N_0/H_0}$.

2.3 Cohomological invariants of $\mathbf{O}_n$

Let k be a field of characteristic different from 2 and let $n\geq 1$. Let us recall that $H^1(k,\mathbf{O}_n)$ classifies, up to isomorphism, the non-degenerate quadratic forms of rank n over k. Recall also that any quadratic form q of rank n over k is isomorphic to a diagonal quadratic form $q\simeq\langle\alpha_1,\dots,\alpha_n\rangle$ for $\alpha_i\in k^\times$ (see e.g. [21]). For any $0\leq i\leq n$, if $q\simeq\langle\alpha_1,\dots,\alpha_n\rangle$, set

$$w_i(q)=\sum_{1\leq j_1<\dots<j_i\leq n}(\alpha_{j_1})\cdot\dots\cdot(\alpha_{j_i})$$

One may show (see [6]) that, for $0\leq i\leq n$, $w_i(q)$ is well-defined and only depends on the isomorphism class of q. It then yields cohomological invariants of the orthogonal group $\mathbf{O}_n$ of the unit quadratic form of rank n, called Stiefel-Whitney invariants. Then Serre described completely the cohomological invariants of the quadratic forms in term of these Stiefel-Whitney invariants (see [24], 17.3).

Theorem 2.1 (Serre, 2003)**.** *Let k_0 be a field of characteristic different from 2. Then the Stiefel-Whitney invariants w_i for $0\leq i\leq n$ form a basis of the $H^*(k_0,\mathbb{Z}/2\mathbb{Z})$-module $\mathsf{Inv}_{k_0}(\mathbf{O}_n,\mathbb{Z}/2\mathbb{Z})$.*

2.4 Cohomological invariants of $\mathfrak{S}_n$

Let k_0 be a field of characteristic different from 2 and let $n\geq 2$. Let us recall that, for any field extension k/k_0, the set $H^1(k,\mathfrak{S}_n)$ classifies étale k-algebras of rank n, up to isomorphism (see Proposition 1.7).

Definition 2.2. *For every extension k/k_0, we will call multiquadratic étale k-algebra any étale k-algebra which is isomorphic to a direct product of étale k-algebras of rank ≤ 2.*

In [24], 24.9, Serre gave a splitting principle for cohomological invariants of the symmetric group $\mathfrak{S}_n$.

Theorem 2.2. *Let k_0 be a field of characteristic different from 2 and let $n \geq 2$. Let also C be any finite Γ_{k_0}-module whose order is not divisible by $\mathsf{char}(k_0)$. Let $a \in \mathsf{Inv}_{k_0}(\mathfrak{S}_n, C)$. Then $a = 0$ if and only if $a_k(E) = 0$ for every multiquadratic étale algebra E of rank n over any field extension k/k_0.*

In other words, the values of an invariant on the multiquadratic étale algebras completely determines this invariant. The proof essentially relies on the existence of a versal $\mathfrak{S}_n$-torsor with rational base field over k_0.

We may also reformulate the splitting principle as follows. Let

$$H = \langle (12), (34), ..., (2[\frac{n}{2}] - 1, 2[\frac{n}{2}]) \rangle.$$

Then, for any k/k_0, the image of the map $H^1(k, H) \to H^1(k, \mathfrak{S}_n)$ exactly coincides with the set of isomorphism classes of multiquadratic étale k-algebras. Therefore, Theorem 2.2 states that the map

$$\mathsf{Res}^H_{\mathfrak{S}_n} : \mathsf{Inv}_{k_0}(\mathfrak{S}_n, C) \to \mathsf{Inv}_{k_0}(H, C)$$

is injective.

The following corollary is an immediate consequence of Theorem 2.2 (see [24], 24.12).

Corollary 2.2. *For any normalized invariant $a \in \mathsf{Inv}_{k_0}(\mathfrak{S}_n, C)$, we have $2a = 0$.*

The determination of the cohomological invariants of $\mathfrak{S}_n$ with coefficients in a Γ_{k_0}-module C of odd order then follows.

Corollary 2.3. *Let C be a finite Γ_{k_0}-module of odd order. Any cohomological invariant of $\mathfrak{S}_n$ over k_0 with coefficients in C is constant.*

Proof. Let m be the order of C. Thanks to Proposition 1.23, we just have to check that the only normalized invariant is the zero invariant. Let $a \in \mathsf{Inv}_{k_0}(\mathfrak{S}_n, C)$ be normalized. By Corollary 2.2, $2a = 0$. Moreover, for any $i \geq 0$ and any extension k/k_0, $H^i(k, C)$ is a m-torsion group (it is easily checked for instance on the cocycles). Thus, $m.a = 0$. Since m is odd and $2a = 0$, we get that $a = 0$. ■

This allows us to consider only Γ_{k_0}-modules with even order. Let us take the simplest one: $C = \mathbb{Z}/2\mathbb{Z}$. Let us define some cohomological invariants of $\mathfrak{S}_n$. Recall that étale algebras are characterized by their trace form (see Proposition 1.6): for any field k of characteristic different from 2, a k-algebra E of rank n is étale if and only if the trace form $q_E : x \mapsto \mathsf{Tr}_{E/k}(x^2)$ is a non-degenerate quadratic form. Now set, for any $0 \leq i \leq n$,

$$\begin{array}{c} w_i : H^1(./k_0, \mathfrak{S}_n) \to H^*(./k_0, \mathbb{Z}/2\mathbb{Z}) \\ (E) \mapsto w_i(q_E) \end{array}.$$

This invariant w_i is called the i^{th} Stiefel-Whitney invariant of $\mathfrak{S}_n$. Then Serre proved that a basis of the module $\mathsf{Inv}_{k_0}(\mathfrak{S}_n, \mathbb{Z}/2\mathbb{Z})$ is given by some Stiefel-Whitney invariants (see [24], 25.13).

Theorem 2.3 (Serre, 2003)**.** *Let k_0 be a field of characteristic different from 2 and let $n \geq 2$. Then the $H^*(k_0, \mathbb{Z}/2\mathbb{Z})$-module $\mathsf{Inv}_{k_0}(\mathfrak{S}_n, \mathbb{Z}/2\mathbb{Z})$ is free with basis $\{w_i\}_{0 \leq i \leq [\frac{n}{2}]}$.*

Let us sketch the proof of Serre. Thanks to the splitting principle, we are now able to completely describe the set $\mathsf{Inv}_{k_0}(\mathfrak{S}_n, \mathbb{Z}/2\mathbb{Z})$. By Proposition 2.3, the image of the map $\mathsf{Res}^H_{\mathfrak{S}_n}$ is contained in $\mathsf{Inv}_{k_0}(\mathfrak{S}_n, \mathbb{Z}/2\mathbb{Z})^{N/H}$, where N denotes the normalizer of H in $\mathfrak{S}_n$. Let us note that $N/H \simeq \mathfrak{S}_{[\frac{n}{2}]}$. By Theorem 2.2, we already know that this map is injective. Then, to completely determine the cohomological invariants of $\mathfrak{S}_n$ with coefficients in $\mathbb{Z}/2\mathbb{Z}$, it is enough to show that the image of the restriction map $\mathsf{Res}^H_{\mathfrak{S}_n}$ is exactly $\mathsf{Inv}_{k_0}(\mathfrak{S}_n, \mathbb{Z}/2\mathbb{Z})^{\mathfrak{S}_{[\frac{n}{2}]}}$. Yet, a direct computation shows that the restrictions of the Stiefel-Whitney invariants to H generate the $H^*(k_0, \mathbb{Z}/2\mathbb{Z})$-module $\mathsf{Inv}_{k_0}(\mathfrak{S}_n, \mathbb{Z}/2\mathbb{Z})^{\mathfrak{S}_{[\frac{n}{2}]}}$.

2.5 Cohomological invariants of $\mathfrak{A}_5$ and of the Coxeter group of type H_3

Let $G = \mathfrak{A}_5$ be the alternating group on 5 letters, let k_0 be a field of characteristic different from 2 and let $C = \mathbb{Z}/2\mathbb{Z}$. Note that any 2-Sylow subgroup of $\mathfrak{A}_5$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2$. Let us denote by H the 2-Sylow subgroup of $\mathfrak{A}_5$ generated by the double transpositions (12)(34) and (13)(24). By Proposition 2.4 and Proposition 2.5, we get an isomorphism

$$\mathsf{Inv}_{k_0}(\mathfrak{A}_5, \mathbb{Z}/2\mathbb{Z}) \simeq \mathsf{Inv}_{k_0}(H, \mathbb{Z}/2\mathbb{Z})^{N/H},$$

where N denotes here the normalizer of H in $\mathfrak{A}_5$. An easy computation shows that $N = \mathfrak{A}_4$ the alternating group over the set $\{1, 2, 3, 4\}$. Therefore, N/H is isomorphic to $\mathbb{Z}/3\mathbb{Z}$: $N/H = \{H, (123).H, (132).H\}$. Thus, the module of the

cohomological invariants of $\mathfrak{A}_5$ is the submodule of the cohomological invariants of $(\mathbb{Z}/2\mathbb{Z})^2$, fixed under the action of (123) and (132) (see the beginning of Section 2.2).

Corollary 2.1 states that the cohomological invariants of $(\mathbb{Z}/2\mathbb{Z})^2$ form a free $H^*(k_0, \mathbb{Z}/2\mathbb{Z})$-module with basis 1, $a_{\{1\}}$, $a_{\{2\}}$ and $a_{\{1,2\}}$, where $a_{\{1\}}$ is the first projection, $a_{\{2\}}$ the second projection and $a_{\{1,2\}} = a_{\{1\}} \cdot a_{\{2\}}$. More precisely, for any extension k/k_0,

$$\begin{aligned} a_{\{1\}} &: (x_1, x_2) \mapsto (x_1) \\ a_{\{2\}} &: (x_1, x_2) \mapsto (x_2) \\ \text{and } a_{\{1,2\}} &: (x_1, x_2) \mapsto (x_1) \cdot (x_2). \end{aligned}$$

Since $H = \langle (12)(34), (13)(24) \rangle$, via the bijection $k^\times/k^{\times 2} \to H^1(k, \mathbb{Z}/2\mathbb{Z})$, we identify the square-class x_1 with a cocycle $\varphi_1 : \gamma \mapsto ((12)(34))^{\epsilon_1(\gamma)}$ (where ϵ_1 is a cocycle with values in $\mathbb{Z}/2\mathbb{Z}$). Likewise, we identify the square-class x_2 with a cocycle $\varphi_2 : \gamma \mapsto ((13)(24))^{\epsilon_2(\gamma)}$ (where ϵ_2 is also a cocycle with values in $\mathbb{Z}/2\mathbb{Z}$). Let us study the action of (123) and (132) on $a_{\{1\}}$. Let k/k_0 be a field extension and let $\varphi : \gamma \to ((12)(34))^{\epsilon_1(\gamma)}.((13)(24))^{\epsilon_2(\gamma)}$ be any cocycle with values in H.
Since

$$(123)(12)(34)(132) = (14)(23) = (12)(34).(13)(24)$$

and

$$(123)(13)(24)(132) = (12)(34),$$

the cocycle $(123).\varphi$ writes

$$(123).\varphi : \gamma \mapsto ((12)(34))^{\epsilon_1(\gamma)+\epsilon_2(\gamma)}.((13)(24))^{\epsilon_1(\gamma)}.$$

Likewise, $(132).\varphi$ may be written as

$$(132).\varphi : \gamma \mapsto ((12)(34))^{\epsilon_2(\gamma)}.((13)(24))^{\epsilon_1(\gamma)+\epsilon_2(\gamma)}.$$

Hence,

$$\begin{aligned} (123).a_{\{1\}} &= (x_1, x_2) \mapsto (x_1 x_2), \\ (132).a_{\{1\}} &= (x_1, x_2) \mapsto (x_2), \end{aligned}$$

so

$$a_{\{1\}} + (123).a_{\{1\}} + (132).a_{\{1\}} = 0.$$

Likewise,

$$\begin{aligned} a_{\{2\}} + (123)a_{\{2\}} + (132)a_{\{2\}} = 0 \text{ and} \\ a_{\{1,2\}} + (123)a_{\{1,2\}} + (132)a_{\{1,2\}} = a_{\{1,2\}} + (-1) \cdot (a_{\{1\}} + a_{\{2\}}). \end{aligned}$$

Moreover, it is easily checked that the invariants 1, $a_{\{1\}} + (123).a_{\{1\}} + (132).a_{\{1\}}$, $a_{\{2\}} + (123).a_{\{2\}} + (132).a_{\{2\}}$ and $a_{\{1,2\}} + (123).a_{\{1,2\}} + (132).a_{\{1,2\}}$ generate the

submodule $\mathsf{Inv}_{k_0}(H,\mathbb{Z}/2\mathbb{Z})^{N/H}$. It then follows that $\mathsf{Inv}_{k_0}(H,\mathbb{Z}/2\mathbb{Z})^{N/H}$ is free with basis

$$1, \quad a_{\{1,2\}} + (-1)\cdot(a_{\{1\}} + a_{\{2\}}).$$

Moreover, taking the restriction of the invariants of $\mathfrak{S}_5$ yield cohomological invariants of $\mathfrak{A}_5$. Let us take the restriction of the Stiefel-Whitney invariant w_2. We have to identify its restriction to H. It follows from the definition of the restriction (see Definition 2.1) that $\mathsf{Res}^H_{\mathfrak{A}_5}(\mathsf{Res}^{\mathfrak{A}_5}_{\mathfrak{S}_5}(w_2)) = \mathsf{Res}^H_{\mathfrak{S}_5}(w_2)$.

Lemma 2.1. *The map $H^1(k,H) \to H^1(k,\mathfrak{S}_5)$ is given by $(a,b) \mapsto k(\sqrt{a},\sqrt{b})\times k$.*

Proof. Take any k-algebra $L = k(\sqrt{a},\sqrt{b})$. Then $\sqrt{a}+\sqrt{b}$ is a primitive element of L and the automorphism group is

$$\begin{aligned}\mathsf{Aut}_k(L) = \{\mathsf{id}, \varphi_{+,-} : \sqrt{a}+\sqrt{b} \mapsto \sqrt{a}-\sqrt{b}, &\varphi_{-,+} : \sqrt{a}+\sqrt{b} \mapsto -\sqrt{a}+\sqrt{b},\\ &\varphi_{-,-} : \sqrt{a}+\sqrt{b} \mapsto -\sqrt{a}-\sqrt{b}\}.\end{aligned}$$

Extending scalars to a separable closure k_{sep} of k, we get

$$\begin{aligned}L \otimes_k k_{\mathsf{sep}} &\simeq k[X]/(X-(\sqrt{a}+\sqrt{b}))\times k[X]/(X-(\sqrt{a}-\sqrt{b}))\\ &\qquad \times k[X]/(X-(-\sqrt{a}+\sqrt{b}))\times k[X]/(X-(-\sqrt{a}-\sqrt{b}))\\ &\simeq k_{\mathsf{sep}}^4.\end{aligned}$$

Thus, $\mathsf{Aut}_k(L)$ can easily be identified with the subgroup H, as a subgroup of $\mathsf{Aut}_{k_{\mathsf{sep}}}(k^4_{\mathsf{sep}}) = \mathfrak{S}_4$. ■

Furthermore, it is easily checked that the trace form of a biquadratic k-algebra $k(\sqrt{a},\sqrt{b})$ is $\langle 1,a,b,ab\rangle$. Therefore, for any $a,b,\in k^\times/k^{\times 2}$,

$$\begin{aligned}w_2(k(\sqrt{a},\sqrt{b})\times k) &= w_2(\langle 1,a,b,ab,1\rangle)\\ &= w_2(\langle a,b,ab\rangle)\\ &= (a)\cdot(b)+(a)\cdot(ab)+(b)\cdot(ab)\\ &= (a)\cdot(b)+(-1)\cdot(ab).\end{aligned}$$

Thus, we have

$$\mathsf{Res}^H_{\mathfrak{A}_5}(\mathsf{Res}^{\mathfrak{A}_5}_{\mathfrak{S}_5}(w_2)) = a_{\{1,2\}} + (-1)\cdot(a_{\{1\}}+a_{\{2\}}).$$

In conclusion,

Proposition 2.7. *Let k_0 be a field of characteristic different from 2. Then the cohomological invariants 1, $\mathsf{Res}^{\mathfrak{A}_5}_{\mathfrak{S}_5}(w_2)$ form a basis of the $H^*(k_0,\mathbb{Z}/2\mathbb{Z})$-module $\mathsf{Inv}_{k_0}(\mathfrak{A}_5,\mathbb{Z}/2\mathbb{Z})$.*

Let now W be the Coxeter group associated to the root system H_3 (see Appendix A). Then $W \simeq \mathfrak{A}_5 \times \mathbb{Z}/2\mathbb{Z}$. The description of $\mathsf{Inv}_{k_0}(W, \mathbb{Z}/2\mathbb{Z})$ then follows from Proposition 2.2.

Proposition 2.8. *The $H^*(k_0, \mathbb{Z}/2\mathbb{Z})$-module $\mathsf{Inv}_{k_0}(W, \mathbb{Z}/2\mathbb{Z})$ is free of rank 4 with a basis given by the invariants*

$$1,\ \mathsf{Res}^{\mathfrak{A}_5}_{\mathfrak{S}_5}(w_2),\ \underline{id}^{\mathbb{Z}/2\mathbb{Z}} \text{ and } \mathsf{Res}^{\mathfrak{A}_5}_{\mathfrak{S}_5}(w_2) \cdot \underline{id}^{\mathbb{Z}/2\mathbb{Z}},$$

defined via the isomorphism $W \simeq \mathfrak{A}_5 \times \mathbb{Z}/2\mathbb{Z}$.

2.6 Cohomological invariants of some dihedral groups

2.6.1 Cohomological invariants of $\mathbb{D}_n$, with n odd

Let n be an odd integer and let k_0 be a field of characteristic different from 2. Let us recall the standard geometric presentation of $\mathbb{D}_n$ (see Apendix A): $\mathbb{D}_n$ is the group of linear automorphisms of the real plane with canonical basis (e_1, e_2), generated by the rotation σ of angle $\frac{2\pi}{n}$ and by the reflection τ with respect to the line $\mathbb{R}e_1$. It is obvious that every 2-Sylow subgroup of $\mathbb{D}_n$ is isomorphic to $\mathbb{Z}/2\mathbb{Z}$. Let us denote by H the 2-Sylow subgroup of $\mathbb{D}_n$ generated by τ. By Proposition 2.4 and Proposition 2.5, we get the isomorphism $\mathsf{Inv}_{k_0}(\mathbb{D}_n, \mathbb{Z}/2\mathbb{Z}) \simeq \mathsf{Inv}_{k_0}(H, \mathbb{Z}/2\mathbb{Z})^{N/H}$, where N denotes the normalizer of H in $\mathbb{D}_n$. An easy computation shows that this normalizer N is equal to H.

Proposition 2.9. *Let k_0 be a field of characteristic different from 2 and let $n \geq 2$ be an odd integer. The $H^*(k_0, \mathbb{Z}/2\mathbb{Z})$-module $\mathsf{Inv}_{k_0}(\mathbb{D}_n, \mathbb{Z}/2\mathbb{Z})$ is free of rank 2.*

2.6.2 Cohomological invariants of $\mathbb{D}_n$, with $n \equiv 2 \mod 4$

Let $n \geq 6$ such that $n \equiv 2 \mod 4$. Then $\mathbb{D}_n \simeq \mathbb{D}_{\frac{n}{2}} \times \mathbb{Z}/2\mathbb{Z}$. By Proposition 2.2, we get that:

Proposition 2.10. *Let k_0 be a field of characteristic different from 2 and let $n \geq 6$ such that $n \equiv 2 \mod 4$. The $H^*(k_0, \mathbb{Z}/2\mathbb{Z})$-module $\mathsf{Inv}_{k_0}(\mathbb{D}_n, \mathbb{Z}/2\mathbb{Z})$ is free of rank 4.*

Note that, when $n = 6$, the dihedral group $\mathbb{D}_6$ is isomorphic to the Weyl group of type G_2 (see Appendix A). In this particular case, we can say a little more : $\mathbb{D}_6 \simeq \mathbb{D}_3 \times \mathbb{Z}/2\mathbb{Z}$ and $\mathbb{D}_3 \simeq \mathfrak{S}_3$. Therefore, combining Theorem 2.3 with $n = 3$ and Proposition 2.1, we obtain that :

Proposition 2.11. *Let k_0 be a field of characteristic different from 2. Then the $H^*(k_0, \mathbb{Z}/2\mathbb{Z}$-module $\mathsf{Inv}_{k_0}(\mathbb{D}_6, \mathbb{Z}/2\mathbb{Z})$ is free with basis*

$$1,\ w_1^{\mathfrak{S}_3},\ \mathit{id}^{\mathbb{Z}/2\mathbb{Z}} \text{ and } w_1^{\mathfrak{S}_3}\cdot \mathit{id}^{\mathbb{Z}/2\mathbb{Z}},$$

via the isomorphism $\mathbb{D}_6 \simeq \mathfrak{S}_3 \times \mathbb{Z}/2\mathbb{Z}$.

It remains to determine the case $n \equiv 0 \mod 4$. We only consider here the case $n = 4$.

2.6.3 Cohomological invariants of $\mathbb{D}_4$

The results of this section were presented by Serre in his minicourse at the Ascona conference in 2007 in a different way.

Contrary to what we have done all along this chapter, we will not exhibit an injective restriction map, but we will determine the cohomological invariants of $\mathbb{D}_4$, by computing residues in $H^*(./k_0, \mathbb{Z}/2\mathbb{Z})$ on a versal torsor.

If $k = k_0(c_1, ..., c_r)$ is a rational field extension over k_0 with transcendance degree r and if P is an irreducible polynomial (in the variables $c_1, ..., c_r$ over k_0), let us denote by D_P the irreducible divisor in $\mathsf{Spec}(k_0[c_1, ..., c_r])$ associated with P. Let us also denote by v_P the valuation v_{D_P} corresponding to the divisor D_P and by r_P the residue map r_{v_P}.

Let us first state a technical lemma.

Lemma 2.2. *Let $l \geq 0$ and let $k = k_0(t, u, v_1, ..., v_l)$ be a rational field extension over k_0 with transcendence degree $l + 2$. If $\alpha \in H^*(k, \mathbb{Z}/2\mathbb{Z})$ is not ramified at any k_0-valuation on k, except maybe at the valuations v_t and v_u, then there exist $c_0, c_1, c_2, c_3 \in H^*(k_0, \mathbb{Z}/2\mathbb{Z})$ such that*

$$\alpha = c_0 + c_1 \cdot (t) + c_2 \cdot (u) + c_3 \cdot (u) \cdot (t).$$

Proof. Set $k' = k_0(t, u)$. If $l \geq 1$, for any effective divisor D of $\mathsf{Spec}(k'[v_1, ..., v_l])$, α is not ramified at v_D. By Theorem 1.4, $\alpha \in H^*(k', \mathbb{Z}/2\mathbb{Z})$. If now D is an irreducible divisor of $\mathsf{Spec}(k_0(t)[u])$, different from D_u, then α is not ramified at v_D by assumption. By Corollary 1.5, there exist some $\alpha_0, \alpha_1 \in H^*(k_0(t), \mathbb{Z}/2\mathbb{Z})$ such that

$$\alpha = \alpha_0 + \alpha_1 \cdot (u). \tag{2.1}$$

Let now D be an irreducible divisor of $\mathsf{Spec}(k_0[t])$ different from D_t. Then $D \times \mathbb{A}^1$ is an irreducible divisor of $\mathsf{Spec}(k_0[u, t])$ different from D_t and D_u, and we have the commutative diagram (see Proposition 1.22)

$$\begin{array}{ccc} H^*(k_0(t), \mathbb{Z}/2\mathbb{Z}) & \xrightarrow{r_{v_D}} & H^*(\kappa(D), \mathbb{Z}/2\mathbb{Z}) \\ \Big\downarrow{\scriptstyle \mathsf{Res}_{k_0(t,u)/k_0(t)}} & & \Big\downarrow{\scriptstyle \mathsf{Res}_{\kappa(D)(u)/\kappa(D)}} \\ H^*(k_0(t, u), \mathbb{Z}/2\mathbb{Z}) & \xrightarrow[r_{v_{D\times\mathbb{A}^1}}]{} & H^*(\kappa(D)(u), \mathbb{Z}/2\mathbb{Z}), \end{array}$$

which implies

$$0 = r_{v_{D\times\mathbb{A}^1}}(\alpha) = \mathsf{Res}_{\kappa(D)(u)/\kappa(D)}(r_{v_D}(\alpha_0)) + \mathsf{Res}_{\kappa(D)(u)/\kappa(D)}(r_{v_D}(\alpha_1)) \cdot (u).$$

Since $\kappa(D)(u)/\kappa(D)$ is purely transcendental, the map $\mathsf{Res}_{\kappa(D)(u)/\kappa(D)}$ is injective, so

$$0 = r_D(\alpha_0) + r_D(\alpha_1) \cdot (u),$$

and since u is an indeterminate over $\kappa(D)$,

$$r_D(\alpha_0) = r_D(\alpha_1) = 0$$

(it is an immediate consequence of Corollary 1.5).

Therefore, α_0 and α_1 are not ramified at any k_0-valuation on $k_0(t)$ except maybe at v_t, so, by Corollary 1.5, there exist some $c_0, c_1, c_2, c_3 \in H^*(k_0, \mathbb{Z}/2\mathbb{Z})$ such that

$$\alpha_0 = c_0 + c_1 \cdot (t) \text{ and } \alpha_1 = c_2 + c_3 \cdot (t),$$

and Equation (2.1) allows us to conclude. ■

Note that the dihedral group $\mathbb{D}_4$ is isomorphic to the Weyl group of type B_2 (see Appendix A). Let k be a field of characteristic different from 2. We will thus use in the sequel the interpretation for the first cohomology set $H^1(k, \mathbb{D}_4)$ in terms of pointed étale algebras (see Proposition 1.8). The cohomology classes of $H^1(k, \mathbb{D}_4)$ identify with the pointed étale algebras (L, α), where L is an étale k-algebra of rank 2 and α a square-class in $L^\times$. In Chapter 4, we will define some cohomological invariants for the Weyl groups of type B_n and then describe them all. Let us define them for the group $\mathbb{D}_4$. As we have seen in Section 2.4 for étale algebras, for any pointed étale k-algebra (L, α), the trace form of L

$$q_{L,\alpha} : x \mapsto \mathsf{Tr}_{L/k}(\alpha x^2)$$

define Stiefel-Whitney invariants (for $0 \leq i \leq 2$)

$$\begin{aligned} w_i : H^1(./k_0, \mathbb{D}_4) &\to H^*(./k_0, \mathbb{Z}/2\mathbb{Z}) \\ (L, \alpha) &\mapsto w_i(q_L). \end{aligned}$$

With pointed étale algebras (L, α), we may associate another trace form, twisted by α

$$q_{L,\alpha} : x \mapsto \mathsf{Tr}_{L/k}(\alpha x^2)$$

which is also non-degenerate. It then defines another family of Stiefel-Whitney invariants (for $0 \leq i \leq 2$)

$$\begin{aligned} \widetilde{w}_i : H^1(./k_0, \mathbb{D}_4) &\to H^*(./k_0, \mathbb{Z}/2\mathbb{Z}) \\ (L, \alpha) &\mapsto w_i(q_{L,\alpha}) \end{aligned}.$$

Theorem 2.4. *Let k_0 be a field of characteristic different from 2. Then the set $\mathsf{Inv}_{k_0}(\mathbb{D}_4, \mathbb{Z}/2\mathbb{Z})$ is a free $H^*(k_0, \mathbb{Z}/2\mathbb{Z})$-module with basis $\{1, w_1, \widetilde{w}_1, \widetilde{w}_2\}$.*

Proof. Let $K = k_0(t, u, v)$, where t, u, v are independent indeterminates. We consider the $\mathbb{D}_4$-torsor $\big(K(\sqrt{t}), u + v\sqrt{t}\big)$ over K. This torsor is versal over k_0 for $\mathbb{D}_4$ (see Definition 1.23). Recall that every cohomological invariant is completely determined by its value on a versal torsor (see Theorem 1.7). Moreover, we have the following formulae :

$$\begin{aligned}
&w_1(K(\sqrt{t}), u + v\sqrt{t}) = (2.2t) = (t),\\
&\widetilde{w}_1(K(\sqrt{t}), u + v\sqrt{t}) = (2u.2ut(u^2 - v^2t)) = (t(u^2 - v^2t)) \text{ and}\\
&\widetilde{w}_2(K(\sqrt{t}), u + v\sqrt{t}) = (2u) \cdot (2ut(u^2 - v^2t)) = (2u) \cdot (-t(u^2 - v^2t)).
\end{aligned}$$

It then remains to prove the following two facts :

(i) the family $\{1, (t), (t(u^2 - v^2t)), (2u) \cdot (-t(u^2 - v^2t))\}$ is free in the module $H^*(K, \mathbb{Z}/2\mathbb{Z})$ over $H^*(k_0, \mathbb{Z}/2\mathbb{Z})$;

(ii) if $a \in \mathsf{Inv}_{k_0}(\mathbb{D}_4, \mathbb{Z}/2\mathbb{Z})$, there exist $d_0, d_1, \widetilde{d_1}, \widetilde{d_2} \in H^*(k_0, \mathbb{Z}/2\mathbb{Z})$ such that

$$a_K(K(\sqrt{t}), u+v\sqrt{t}) = d_0+d_1\cdot(t)+\widetilde{d_1}\cdot(t(u^2-v^2t))+\widetilde{d_2}\cdot(2u)\cdot(-t(u^2-v^2t)).$$

Let us first show (i). Let $\lambda_0, \lambda_1, \lambda_2, \lambda_3 \in H^*(k_0, \mathbb{Z}/2\mathbb{Z})$ such that

$$0 = \lambda_0 + \lambda_1 \cdot (t) + \lambda_2 \cdot (t(u^2 - v^2t)) + \lambda_3 \cdot (2u) \cdot (-t(u^2 - v^2t)).$$

Let us take the residue at the valuation corresponding to $(u^2 - v^2t)$. Then,

$$0 = \lambda_2 + \lambda_3 \cdot (2u) = (\lambda_2 + \lambda_3 \cdot (2)) + \lambda_3 \cdot (u).$$

Taking now the residue at v_u, it is easily seen that $\lambda_3 = 0$, which implies that $\lambda_2 = 0$. We then obtain that $0 = \lambda_0 + \lambda_1 \cdot (t)$, so taking the residue at v_t, we get that $\lambda_1 = 0$. Thus, $\lambda_0 = 0$ and this proves (i).

Let us prove (ii). Let a be a cohomological invariant of $\mathbb{D}_4$ over k_0 and set

$$\beta = a_K(K(\sqrt{t}), u + v\sqrt{t})$$

and

$$\beta_1 = \mathsf{Res}_{K(\sqrt{t})/K}(\beta) = a_{K(\sqrt{t})}\big(K(\sqrt{t})^2, (u + v\sqrt{t}, u - v\sqrt{t})\big).$$

Let us consider $H_0 \subset \mathbb{D}_4$ (viewed as the Weyl group of type B_2) the subgroup defined in Example 2.1. It is easily seen that the image of the map

$$\iota : H^1(K(\sqrt{t}), H_0) \to H^1(K(\sqrt{t}), \mathbb{D}_4)$$

is the set of the pointed étale algebras $(K(\sqrt{t})^2, (\alpha_0, \alpha_1))$, with α_0, α_1 some square-classes in $K(\sqrt{t})^\times$ (see Chapter 4, Proposition 4.1 for a proof). Since the cohomology class associated with the pointed algebra $\big(K(\sqrt{t})^2, (u+v\sqrt{t}, u-v\sqrt{t})\big)$ lies in the image of ι, we get

$$\beta_1 = \mathsf{Res}_W^{H_0}(a)_{K(\sqrt{t})}\big(u + v\sqrt{t}, u - v\sqrt{t}\big).$$

Therefore, since $\mathsf{Res}_W^{H_0}(a)$ is a cohomological invariant of $H_0 \simeq \big(\mathbb{Z}/2\mathbb{Z}\big)^2$, by Example 2.1, there are some $b_0, b_1, b_2 \in H^*(k_0, \mathbb{Z}/2\mathbb{Z})$ such that, for any field extension k/k_0 and for any $(\alpha_1, \alpha_2) \in H^1(k, H_0)$, we have :

$$(\mathsf{Res}_W^{H_0}(a))_k(\alpha_1, \alpha_2) = b_0 + b_1 \cdot (\alpha_1\alpha_2) + b_2 \cdot (\alpha_1) \cdot (\alpha_2).$$

Hence, we get that

$$\beta_1 = b_0 + b_1 \cdot (u^2 - v^2 t) + b_2 \cdot (u + v\sqrt{t}) \cdot (u - v\sqrt{t}).$$

Since the extension $K(\sqrt{t})/K$ is not ramified at the valuation corresponding to $(u^2 - v^2 t)$, we have the commutative diagram (see Proposition 1.22)

$$\begin{array}{ccc} H^*(K, \mathbb{Z}/2\mathbb{Z}) & \xrightarrow{r_{u^2-v^2t}} & H^*(k_0(u,v), \mathbb{Z}/2\mathbb{Z}) \ . \\ \Big\downarrow{\scriptstyle \mathsf{Res}_{K(\sqrt{t})/K}} & & \Big\downarrow{\scriptstyle \mathsf{id}} \\ H^*(K(\sqrt{t}), \mathbb{Z}/2\mathbb{Z}) & \xrightarrow[r_{u+v\sqrt{t}}]{} & H^*(k_0(u,v), \mathbb{Z}/2\mathbb{Z}) \end{array}$$

In the residue field associated with $r_{u+v\sqrt{t}}$ over $K(\sqrt{t})$, we have $\overline{2u} = \overline{u - v\sqrt{t}}$, since $u + v\sqrt{t} + u - v\sqrt{t} = 2u$. The previous commutative diagram yields that

$$r_{u^2-v^2t}(\beta) = r_{u+v\sqrt{t}}(\beta_1) = b_1 + b_2 \cdot (2u).$$

In particular, $r_{u^2-v^2t}(\beta)$ is not ramified, except maybe at v_u. Now set

$$\beta' = \beta + r_{u^2-v^2t}(\beta) \cdot (u^2 - v^2 t).$$

Let us show that the cohomology class β' is not ramified except maybe at v_t and at v_u. Let D be an irreducible divisor of $\mathsf{Spec}(k_0[t, u, v])$ different from D_t, D_u and $D_{u^2-v^2t}$. The cohomology class of the pointed algebra $(K(\sqrt{t}), u+v\sqrt{t})$ is not ramified (i.e. lies in the image of the map $H^1(\kappa(D), \mathbb{D}_4) \to H^1(K(\sqrt{t}), \mathbb{D}_4)$, see Definition 3.1 in Chapter 3), except maybe at the valuations corresponding to the irreducible divisors of the discriminant of the algebra $K(\sqrt{t})\big(\sqrt{u + v\sqrt{t}}\big)/K$, i.e. at v_t and at $v_{u^2-v^2t}$. Since $D \neq D_t, D_{u^2-v^2t}$, the cohomology class of the pointed algebra $(K(\sqrt{t}), u + v\sqrt{t})$ is not ramified at v_D, thus $r_{v_D}(\beta) = 0$. Hence,

$$r_{v_D}(\beta') = r_{v_D}(\beta) + r_{v_D}((b_1 + b_2 \cdot (2u)) \cdot (u^2 - v^2 t)) = 0.$$

Furthermore,

$$r_{u^2-v^2t}(\beta') = r_{u^2-v^2t}(\beta) + r_{u^2-v^2t}\big(r_{u^2-v^2t}(\beta)\cdot(u^2-v^2t)\big) = 2r_{u^2-v^2t}(\beta) = 0.$$

Hence β' is not ramified, except maybe at v_t and v_u. By Lemma 2.2, there exist $c_0, c_1, c_2, c_3 \in H^*(k_0, \mathbb{Z}/2\mathbb{Z})$, such that

$$\beta' = c_0 + c_1\cdot(t) + c_2\cdot(u) + c_3\cdot(u)\cdot(t),$$

so

$$\beta = c_0 + c_1\cdot(t) + c_2\cdot(u) + c_3\cdot(u)\cdot(t) + (b_1 + b_2\cdot(2u))\cdot(u^2-v^2t).$$

Yet we know that $r_u(\beta) = 0$, hence

$$0 = c_2 + c_3\cdot(t) + b_2\cdot(\overline{u^2-v^2t}) = c_2 + c_3\cdot(t) + b_2\cdot(-t).$$

It yields

$$0 = c_2 + b_2\cdot(-1) + (c_3+b_2)\cdot(t).$$

As the family $\{1,(t)\}$ is free in the $H^*(k_0,\mathbb{Z}/2\mathbb{Z})$-module $H^*(k_0(t),\mathbb{Z}/2\mathbb{Z})$, we get that $c_2 = b_2\cdot(-1)$ and $c_3 = b_2$. Eventually,

$$\begin{aligned}\beta &= c_0 + c_1\cdot(t) + b_1\cdot(u^2-v^2t) + b_2\cdot(2)\cdot(u^2-v^2t) + b_2\cdot(u)\cdot(-t(u^2-v^2t))\\ &= c_0 + (c_1 + b_2\cdot(2))\cdot(t) + b_1\cdot(u^2-v^2t) + b_2\cdot(2u)\cdot(-t(u^2-v^2t)).\end{aligned}$$

Therefore,

$$\beta = c_0 + (c_1 + b_1 + b_2\cdot(2))\cdot(t) + b_1\cdot(t(u^2-v^2t)) + b_2\cdot(2u)\cdot(-t(u^2-v^2t)),$$

This proves (ii). ■

Let us end this section by giving relations between some cohomological invariants of $\mathbb{D}_4$ that we will use below :

Proposition 2.12. *We have the following equalities :*

$$w_2 = (2)\cdot w_1,\ w_1\cdot\widetilde{w}_1 = (-1)\cdot w_1 \text{ and } w_1\cdot\widetilde{w}_2 = 0.$$

Proof. By [24], Theorem 12.3, we just have to check the equalities on the versal $\mathbb{D}_4$-torsor $T = (K(\sqrt{t}), u+v\sqrt{t})$. Let us prove for instance the first one. We have

$$w_2(T) = w_2(\langle 2, 2t\rangle) = (2)\cdot(2t) = (2)\cdot(t) = (2)\cdot w_1(\langle 2, 2t\rangle).$$

The other equalities are left to the reader. ■

Chapter 3

Vanishing principle for finite Coxeter groups

RÉSUMÉ

Dans ce chapitre, on énonce et prouve un principe d'annulation pour les invariants cohomologiques d'un groupe de Coxeter fini sur un corps de caractéristique zéro suffisamment grand. Ce principe généralise le principe de déploiement de Serre pour les invariants cohomologiques du groupe symétrique énoncé au chapitre 2 (théorème 2.2). On notera que ce principe d'annulation était connu de Serre dans le cas des groupes de Weyl (cf. [24], 25.15). En fin de chapitre, on prouve que, lorsque le principe d'annulation est vrai, de la même manière que pour le groupe symétrique, tout invariant cohomologique d'un groupe de Coxeter fini est tué par 2. On termine ce chapitre en appliquant le principe d'annulation à la cohomologie négligeable.

In this chapter, we state and prove a general vanishing principle for the cohomological invariants of a finite Coxeter group. This principle generalizes Serre's splitting principle for the cohomological invariants of the symmetric group (Theorem 2.2). Note also that the vanishing principle was known to Serre for Weyl groups (see [24], 25.15).

3.1 The vanishing principle

Theorem 3.1. *Let W be a finite Coxeter group and let k_0 be a field of characteristic zero containing a subfield on which the real representation of W as a reflection*

group is realizable. Let C be a finite Γ_{k_0}-module. Let also $a \in \mathsf{Inv}_{k_0}(W, C)$. Assume that every restriction of a to an abelian subgroup of W generated by reflections is zero. Then $a = 0$.

We use the strategy suggested by Serre in [24], 25.15. Recall first that a cohomology class in $H^1(k, W)$ corresponds to an isomorphism class of a W-torsor over k. By Theorem 1.7, a cohomological invariant of W is completely determined by its value on a versal torsor. Thanks to a Chevalley's theorem, we construct a versal W-torsor T^{vers} with rational base field $K = k_0(c_1, ..., c_n)$. We then show that, if a cohomological invariant a of W satisfies the hypothesis of Theorem 3.1, the cohomology class $a(T^{\mathsf{vers}})$ is unramified at any place coming from an irreducible divisor of the affine space $\mathsf{Spec}(k_0[c_1, ..., c_n])$. By Theorem 1.4, the cohomology class $a(T^{\mathsf{vers}})$ is constant. Since a vanishes on the trivial torsor, we get that $a = 0$.

From now on, in Section 3.1, let W and let k_0 be as in Theorem 3.1.

3.1.1 Ramification of cohomology classes of W

Let us recall what ramification means for cohomology classes in $H^1(k, W)$. Let R be a discrete valuation ring of valuation v, let K be its fraction field and let k be its residue field. Assume that K is complete for the valuation v. Let us also recall that we denote by Γ_K (resp. by Γ_k) the absolute Galois group of K (resp. the absolute Galois group of k). Finally, let us denote by I_K the inertia group of K and by $\pi : \Gamma_K \to \Gamma_k$ the quotient morphism.

Proposition 3.1. *Let $\alpha \in H^1(K, W)$. If φ is a cocycle representing α, then the following assertions are equivalent :*

(i) $\varphi(I_K) = \{1_W\}$*;*

(ii) there is a unique group homomorphism $\overline{\varphi} : \Gamma_k \to W$ such that the following diagram is commutative :

$$\begin{array}{ccc} \Gamma_K & \xrightarrow{\varphi} & W \\ {\scriptstyle\pi}\downarrow & \nearrow_{\overline{\varphi}} & \\ \Gamma_k & & \end{array}$$

(iii) α belongs to the image of the natural application $H^1(k, W) \to H^1(K, W)$.

Note that this statement only depends on the cohomology class α.

Proof.

(i)⇒ (ii) Assume that $\varphi(I_K) = \{1_W\}$. Then φ factors through $\overline{\varphi} : \Gamma_K/I_K \to W$; yet $\Gamma_k = \Gamma_K/I_K$, so $\overline{\varphi}$ is the required morphism.

(ii)⇒ (iii) The homomorphism π yields the map $\pi^* : H^1(k, W) \to H^1(K, W)$, given by $[\psi] \in H^1(k, W) \mapsto [\psi \circ \pi] \in H^1(K, W)$ (where [.] denotes the cohomology class associated to the cocycle). Moreover, by *(ii)*, since $\varphi = \overline{\varphi} \circ \pi$, $[\overline{\varphi}]$ is a preimage of α by π^*.

(iii)⇒ (i) Assume that α admits a preimage $\beta \in H^1(k, W)$ by π^*. Then there is a cocycle ψ representing β such that $\varphi = \psi \circ \pi$, so the image of I_K by φ is trivial. ■

Definition 3.1. *We say that the cohomology class $\alpha \in H^1(K, W)$ is unramified if α satisfies one of the three equivalent properties of Proposition 3.1.*

3.1.2 A versal W-torsor with rational base field

We let the reader refer to Definition 1.23 for a definition of a versal torsor.

As elements of W are automorphisms of a vector space $V \simeq k_0^n$ for some $n > 0$ (since the representation ρ is realizable over a subfield of k_0 and then extends to k_0), W naturally acts on the dual V^* and on the associated symmetric algebra $\mathsf{Sym}(V^*)$. Note that this k_0-algebra is isomorphic to a polynomial algebra $k_0[x_1, ..., x_n]$ with n indeterminates. We then consider the underlying action of W on $k_0[x_1, ..., x_n]$ and the invariant subalgebra $k_0[x_1, ..., x_n]^W$. By a theorem of Chevalley (see Appendix A, Theorem A.1), $k_0[x_1, ..., x_n]^W$ is a polynomial k_0-algebra of transcendence degree n. In other words, $k_0[x_1, ..., x_n]^W \simeq k_0[c_1, ..., c_n]$ for some independent indeterminates $c_1, ..., c_n$ over k_0.

Let us translate this situation into scheme language. Set $Q = \mathsf{Spec}(k_0[x_1, ..., x_n])$ and $X = \mathsf{Spec}(k_0[c_1, ..., c_n])$. We have a morphism $f : Q \to X$ which is exactly the quotient morphism $\mathsf{Aff}^n_x \to \mathsf{Aff}^n_x/W = \mathsf{Aff}^n_c$. Let y be an element of $k_0[x_1, ..., x_n]$ whose orbit by W has maximal order. We then localize f at the locus $\Delta_c = f(\Delta_x)$, where $\Delta_x = \{w.y - w'.y \mid w \neq w', w, w' \in W\}$. We then get from f a morphism $Q_{\Delta_x} \to X_{\Delta_c}$ that we still denote by f. With this localization, W acts without fixed points on Q_{Δ_x} and we still have $Q_{\Delta_x}/W = X_{\Delta_c}$. Hence, Q_{Δ_x} is a W-torsor with base X_{Δ_c}.

We denote by $K = k_0(c_1, ..., c_n)$ the function field of X (which is also the function field of X_{Δ_c}) and by $L = k_0(x_1, ..., x_n)$ the function field of Q. Since X_{Δ_c} is an irreducible variety, let us denote by T^{vers} the fiber of f at the unique generic point of X_{Δ_c}. Thus, T^{vers} is a W-torsor over K, corresponding to the field extension L/K which is Galois, with Galois group W.

Proposition 3.2. *Keeping the notation above, T^{vers} is a versal torsor for W over k_0.*

Proof. Let k/k_0 be a field extension. Let T be a W-torsor over k. Then T corresponds to a Galois W-algebra over k and we choose a generator $(a_1, ..., a_n)$. We localize Q_{Δ_x} at the ideal $(x_1 - a_1, ..., x_n - a_n)$ of $k[x_1, ..., x_n]_{\Delta_x}$. The image $x = f(x_1 - a_1, ..., x_n - a_n)$ is a k-point of X_{Δ_c} and the fiber of f in x is a W-torsor over k isomorphic to T. Since k is infinite (k_0 has characteristic zero), the set of the generators of the Galois W-algebra is dense with respect to the Zariski topology on Aff^n_x, so condition *2.* in Definition 1.23 is satisfied. ■

Note that the isomorphism class of T^{vers} corresponds to the cohomology class of the natural projection

$$\begin{aligned} \varphi^{\mathsf{vers}} : \Gamma_K &\to W. \\ \gamma &\mapsto \gamma_{|L} \end{aligned}$$

3.1.3 Ramification of the versal torsor T^{vers}

In this section, we want to study the ramification of the isomorphism class of the versal torsor T^{vers} at the different valuations on K which are trivial on k_0. These valuations are determined by the irreducible divisors of Aff^n_c. Let D be such a divisor. Let us denote by v_D the discrete valuation on K associated to D, K_D the completion of K with respect to this valuation and $k_0(D)$ the residue field of K for v_D, which identifies with the function field of D over k_0. We denote by T^{vers}_D the image of T^{vers} under the application

$$\begin{aligned} H^1(K, W) &\to H^1(K_D, W) \\ [\varphi] &\mapsto [\varphi \circ i_D] \end{aligned}$$

where $i_D : \Gamma_{K_D} \to \Gamma_K$ is the natural inclusion.

The aim of this paragraph is to study the ramification of the cohomology class of T^{vers}_D. We denote by $\varphi^{\mathsf{vers}}_D$ the morphism $\Gamma_{K_D} \xrightarrow{i_D} \Gamma_K \xrightarrow{\varphi^{\mathsf{vers}}} W$; it represents the cohomology class of T^{vers}_D. Thus, by Proposition 3.1, we have to study the subgroup $\varphi^{\mathsf{vers}}_D(I_{K_D})$.

Since $[\varphi^{\mathsf{vers}}]$ is represented by the Galois extension L/K, $[\varphi^{\mathsf{vers}}_D]$ is represented by the Galois W-algebra $L \otimes_K K_D$ over K_D. Moreover, there is an isomorphism of K_D-algebras

$$L \otimes_K K_D \simeq \prod_{\widetilde{v}|v_D} L_{\widetilde{v}}$$

where $L_{\widetilde{v}}$ denotes the completion of L with respect to the extension $\widetilde{v}$ of v_D (see for example [17] II.8).

Let $\widetilde{v}_D$ be an extension of the valuation v_D to L. We denote by $\widetilde{L}_D$ the completion of L with respect to this valuation. Then $\widetilde{L}_D$ is a Galois extension of K_D,

with Galois group $\widetilde{W} = \{w \in W, \widetilde{v}_D \circ w = \widetilde{v}_D\}$, which is of course a subgroup of W.

Set $e = (0, ..., 0, 1, 0, ..., 0)$ in the product $\prod_{\widetilde{v}|v_D} L_{\widetilde{v}}$, where $1 \in \widetilde{L}_D$. Then e is a primitive idempotent of $L \otimes_K K_D$ and by [12], Proposition 18.18, $\widetilde{L}_D = e.(L \otimes_K K_D)$ is a Galois $\widetilde{W}$-algebra (and a field) and we have the isomorphism of W-algebras

$$L \otimes_K K_D \simeq \mathsf{Ind}_{\widetilde{W}}^{W}(\widetilde{L}_D).$$

Thus, since the induced algebra (for the Galois algebras) corresponds to the inclusion for the cocycles, $\varphi_D^{\mathsf{vers}}$ factors through $\widetilde{W}$:

$$\begin{array}{ccc} \Gamma_{K_D} & \xrightarrow{\varphi_D^{\mathsf{vers}}} & W \ , \\ {\scriptstyle\psi}\downarrow & \nearrow & \\ \widetilde{W} & & \end{array}$$

where ψ is a cocycle representing the cohomology class corresponding to $\widetilde{L}_D/K_D$. It yields that $\varphi_D^{\mathsf{vers}}(I_{K_D}) = \psi(I_{K_D})$. Therefore the ramification of T_D^{vers} is $\psi(I_{K_D})$.

Let us denote by $l(\widetilde{v}_D)$ the residue field associated with $\widetilde{L}_D$ and if $w \in \widetilde{W}$, let us denote by $\overline{w}$ the induced $k_0(D)$-automorphism (as w respects the valuation $\widetilde{v}_D$, w restricts to $w : \mathcal{O}_{\widetilde{v}_D} \to \mathcal{O}_{\widetilde{v}_D}$, where $\mathcal{O}_{\widetilde{v}_D}$ denotes the valuation ring of $\widetilde{v}_D$ in L and sends the maximal ideal of $\mathcal{O}_{\widetilde{v}_D}$ into itself, so going to quotients, we get an automorphism $\overline{w}$ of $l(\widetilde{v}_D)$). We then introduce the inertia subgroup $\widetilde{I} = \{w \in \widetilde{W} \mid \overline{w} = \mathsf{id}_{l(\widetilde{v}_D)}\}$ of $\widetilde{W}$.

Lemma 3.1. *Keeping the notation above, $\psi(I_{K_D}) \subset \widetilde{I}$.*

Proof. Let us denote by $\overline{k_0(D)}$ an algebraic closure of $k_0(D)$. Recall that $(K_D)_{\mathsf{sep}}$ has residue field $\overline{k_0(D)}$ and that $(k_0(D))_{\mathsf{sep}}$ is the residue field corresponding to the biggest subextension of $(K_D)_{\mathsf{sep}}$ fixed by the inertia group I_{K_D}. Let $\gamma \in I_{K_D}$. Then the $k_0(D)$-automorphism $\overline{\gamma}$ is trivial over $k_0(D)_{\mathsf{sep}}$. In other words, the image of γ by the group homomorphism $\Gamma_{K_D} \to \Gamma_{k_0(D)}$ is the identity and we have the commutative diagram

$$\begin{array}{ccc} \Gamma_{K_D} & \longrightarrow & \Gamma_{k_0(D)} \\ {\scriptstyle\psi}\downarrow & & \downarrow{\scriptstyle\mathsf{res}} \\ \widetilde{W} & \longrightarrow & \mathsf{Gal}(l(\widetilde{v}_D)/k_0(D)) \end{array}$$

where horizontal maps are induced by going to quotients (by valuation theory, the sequence

$$0 \longrightarrow \widetilde{I} \longrightarrow \widetilde{W} \longrightarrow \mathsf{Gal}(l(\widetilde{v}_D)/k_0(D))) \longrightarrow 0$$

is exact). Then the $k_0(D)$-automorphism of $l(\widetilde{v}_D)$ induced by $\psi(\gamma)$ is equal to the identity, which proves that $\psi(\gamma)$ belongs to $\widetilde{I}$. ■

Let us now study the inertia group $\widetilde{I}$ and let us introduce the discriminant $\mathsf{Discr}(L/K)$ of L/K. Let us recall that the isomorphism class of the versal torsor T^{vers} may be identified with the isomorphism class of the Galois algebra L/K, i.e. with the set of K-embeddings of L in K_{sep}. Yet, these embeddings are completely determined by the image of a primitive element y of L over K. Therefore, this discriminant may be written as:

$$\mathsf{Discr}(L/K) = \prod_{t \neq t'} (t(y) - t'(y)),$$

where $t, t' : L \hookrightarrow K_{\mathsf{sep}}$.

Moreover, one can choose, as a primitive element, a polynomial in $k_0[x_1, ..., x_n]$ with total degree 1 : since k_0 is infinite, there exists $y = a_1x_1 + ... + a_nx_n$ (where $a_i \in k_0$ for $i = 1, ..., n$) such that, for all $w \neq w' \in W$, $w(y) \neq w'(y)$. Indeed, as W is a group, it is enough to check that there exist $a_1, ..., a_n \in k_0$ such that $y = a_1x_1 + ... + a_nx_n$ and that, for all $w \in W$, $w(y) \neq y$, which is satisfied as soon as the vector $\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}$ is not an eigenvector of any matrix representing a non-trivial element of W in the basis $(x_1, ..., x_n)$ of the dual space $V^* \simeq k_0^n$.

From now on, y will denote a primitive element of L/K, which is a polynomial of total degree 1 in $x_1, ..., x_n$. Let us now compute the ramification of T_D^{vers}.

Lemma 3.2. *Assume that D is an irreducible divisor which does not divide the ideal $\left(\mathsf{Discr}_{L/K}\right)$. Then the isomorphism class of T_D^{vers} is unramified.*

Proof. Since we have shown above that the ramification is contained in $\widetilde{I}$, it is enough to prove that $\widetilde{I}$ is trivial. Yet the sequence

$$0 \longrightarrow \widetilde{I} \longrightarrow \widetilde{W} \longrightarrow \mathsf{Gal}(l(\widetilde{v}_D)/k_0(D))) \longrightarrow 0$$

is exact. Since D does not divide the discriminant, the extension $\widetilde{L}_D/K_D$ is unramified, which shows that $[\widetilde{L}_D : K_D] = [l(\widetilde{v}_D) : k_0(D)]$, so $\widetilde{W} \simeq \mathsf{Gal}(l(\widetilde{v}_D)/k_0(D)))$. Therefore, $\widetilde{I}$ is trivial. ■

Lemma 3.3. *Assume now that D is an irreducible divisor of $\mathsf{Spec}(k_0[c_1, ..., c_n])$ which divides the discriminant ideal $\left(\mathsf{Discr}_{L/K}\right)$. Then $\widetilde{I} = \langle r \rangle$, where r is a reflection of W.*

Proof. Since D divides the discriminant ideal, the extension $\widetilde{L}_D/K_D$ is ramified, so its inertia group $\widetilde{I}$ is not trivial. Let us compute it. Since $\widetilde{v}_D$ is a valuation on $L = k_0(x_1, ..., x_n)$, which is trivial on k_0 (because it extends v_D which is itself trivial on k_0), $\widetilde{v}_D$ is a valuation associated with an irreducible divisor $\widetilde{D}$ of $\mathsf{Spec}(k_0[x_1, ..., x_n])$; furthermore, since $\widetilde{v}_D$ extends v_D, the divisor $\widetilde{D}$ is above D, so $\widetilde{D}$ is generated by an irreducible factor of $\mathsf{Discr}(L/K)$ decomposed in $k_0[x_1, ..., x_n]$. Then there are two distinct elements $t_1, t_2 \in T^{\mathsf{vers}}$ such that $\widetilde{D} = (t_1(y) - t_2(y))$ (we identify the image of L in K_{sep} with L itself; that is why we consider $t_1(y)$ and $t_2(y)$ as polynomials in $x_1, ..., x_n$). Therefore, the valuation $\widetilde{v}_D$ is described as follows : for any $f \in L$, $\widetilde{v}_D(f)$ is equal to the order of $(t_1(y) - t_2(y))$ as zero or pole in the rational fraction f.

Let $w \in \widetilde{I}$. Then $\overline{w} = \mathsf{id}_{l(\widetilde{v}_D)}$. Let $f \in \mathcal{O}_{\widetilde{v}_D}$ (i.e. which has not $t_1(y) - t_2(y)$ as a pole). As $l(\widetilde{v}_D) = \mathcal{O}_{\widetilde{v}_D}/\mathcal{M}_{\widetilde{v}_D}$, there is a $g \in \mathcal{O}_{\widetilde{v}_D}$ such that :

$$w(f) = f + g.(t_1(y) - t_2(y))$$

If we now write $g = \frac{g_0}{g_1}$, with $g_0, g_1 \in k_0[x_1, ..., x_n]$ and $t_1(y) - t_2(y)$ not dividing g_1, we get that

$$g_1.(w(f) - f) = g_0.(t_1(y) - t_2(y)).$$

Consider the particular case where f is a polynomial in $k_0[x_1, ..., x_n]$. Then the equality now reads in $k_0[x_1, ..., x_n]$ (because W acts on $k_0[x_1, ..., x_n]$) and since $t_1(y) - t_2(y)$ does not divide g_1, $t_1(y) - t_2(y)$ divides $w(f) - f$. Therefore, there is a polynomial g_2 in $k_0[x_1, ..., x_n]$ such that

$$w(f) - f = g_2.(t_1(y) - t_2(y)) \tag{3.1}$$

Assume now that f is a polynomial of total degree 1. Then f identifies with a linear form on V and as w is an automorphism of V, $w(f) = f \circ w^{-1}$ is still a linear form on V, so via the identification $\mathsf{Sym}(V^*) \simeq k_0[x_1, ..., x_n]$, $w(f)$ is still a polynomial of total degree 1.

Let us now show that the total degree of $t_1(y) - t_2(y)$ is equal to 1. First note that, since $t_1(y) - t_2(y)$ is an irreducible factor of $\mathsf{Discr}_{L/K}$ in $k_0[x_1, ..., x_n]$, it has total degree ≥ 1. Assume that $w \neq \mathsf{id}$. Then there is a $f_0 \in V^*$ such that $w(f_0) \neq f_0$. Thus, $w(f_0) - f_0$ is a polynomial of total degree 0 or 1. Taking total degree in Equation (3.1), we get that $t_1(y) - t_2(y)$ has exactly total degree 1. Therefore, g_2 has total degree at most 0. Thus, for any $f \in V^*$, there exists $a \in k_0$ such that

$$w(f) - f = a.(t_1(y) - t_2(y)).$$

We then get that w is a pseudo-reflection of V^* (i.e. an endomorphism such that the rank of $w - \mathsf{id}_{V^*}$ is equal to 1). Yet, since W is a reflection group over $\mathbb{R}$, the only pseudo-reflections in W are reflections. Therefore, the non-trivial elements

of $\widetilde{I}$ are reflections.

By [23] IV.2, Corollary 2 of Proposition 7, we get that $\widetilde{I}$ is cyclic (note that the residue field of $l(\widetilde{v}_D)$ is an extension of k_0, then has characteristic zero). Then $\widetilde{I}$ is of order 2 (recall that it can not be trivial). Finally $\widetilde{I} = \{1, r\}$ (where r is a reflection of W). ■

Let us recall that we have $\varphi_D^{\mathsf{vers}}(I_{K_D}) = \psi(I_{K_D}) \subset \widetilde{I} = \{1, r\}$. Then

$$\varphi_D^{\mathsf{vers}}(I_{K_D}) = \{1\} \text{ or } \varphi_D^{\mathsf{vers}}(I_{K_D}) = \{1, r\}.$$

In the first case, T^{vers} is unramified at D. In the second case, we state the key lemma for our inductive proof of Theorem 3.1.

Lemma 3.4. *Assume that $\varphi_D^{\mathsf{vers}}(I_{K_D}) = \langle r \rangle$. Then there is a subgroup W_0 of W generated by reflections, such that $\varphi_D^{\mathsf{vers}}(\Gamma_{K_D}) \subset W_0 \times \langle r \rangle \subset W$.*

Proof. Since the sequence

$$1 \longrightarrow I_{K_D} \longrightarrow \Gamma_{K_D} \longrightarrow \Gamma_{k_0(D)} \longrightarrow 1$$

is exact, $\varphi_D^{\mathsf{vers}}(I_{K_D})$ is normal in $\varphi_D^{\mathsf{vers}}(\Gamma_{K_D})$. Therefore, r is in the center of $\varphi_D^{\mathsf{vers}}(\Gamma_{K_D})$, that is to say that $\varphi_D^{\mathsf{vers}}(\Gamma_{K_D})$ is contained in the centralizer $C(r)$ of r in W.

By assumption on k_0, the real representation $\rho : W \hookrightarrow GL(V)$ of W as a reflection group over $\mathbb{R}$ yields a representation $W \hookrightarrow GL(V_{k_0})$ of W as a reflection group over k_0.

Let now e be a non-zero vector of $\mathsf{Im}(r - \mathsf{id}_V)$ and let H be the hyperplane of the fixed points of r in V. Let also $w \in W$. Then w and r commute if and only if $\mathbb{R}e$ and H are stable by w (see Appendix A, Proposition A.1). Assume that w and r commute. Then, $w(H) \subset H$ and $w(e) = b.e$ for some $b \in \mathbb{R}$. As W is finite, b is a root of the unity in $\mathbb{R}$, so $b = \pm 1$.

Let $W_0 = \{w \in W \mid w(e) = e\}$. As an isotropy subgroup of W, W_0 is a reflection group over $\mathbb{R}$ (see Appendix A, Proposition A.2) and hence is a reflection group over k_0.

It remains to prove that $C(r) \simeq W_0 \times \langle r \rangle$. Let us first note that, since W acts by isometries on the euclidean space $V_{\mathbb{R}}$, $W_0 = \{w \in W \mid w(H) \subset H \text{ and } w(e) = e\}$. One can show easily that W_0 and $\langle r \rangle$ are normal in $C(r)$, that the intersection $W_0 \cap \langle r \rangle$ is trivial and that $W_0.\langle r \rangle = C(r)$. Therefore, $C(r)$ is the direct product of W and $\langle r \rangle$. ■

3.1.4 Proof of Theorem 3.1

Let us begin with a key lemma for our proof by induction.

Lemma 3.5. *Let W be a finite Coxeter group and let k_0 be a field satisfying the hypothesis of Theorem 3.1. Let W' be a proper subgroup of W which is also generated by reflections. Let us assume that there is a reflection r of W which is not in W' and which commutes with any reflection of W'. If Theorem 3.1 is true for W', then Theorem 3.1 is also true for $W' \times \langle r \rangle$.*

Proof. Let $a \in \mathsf{Inv}_{k_0}(W' \times \langle r \rangle, C)$ such that every restriction to an abelian subgroup generated by reflections is zero. Let k/k_0 be a field extension. We have the isomorphism $H^1(k, W' \times \langle r \rangle) \simeq H^1(k, W') \times H^1(k, \langle r \rangle)$. Then, in the sequel of the proof, we denote the elements of $H^1(k, W' \times \langle r \rangle)$ by pairs (α, ϵ), where α is a cohomology class in $H^1(k, W')$ and ϵ a square-class in $H^1(k, \langle r \rangle)$.

Let $(\alpha_0, \epsilon_0) \in H^1(k, W' \times \langle r \rangle)$ be such an element. For any extension k'/k, we set

$$\begin{array}{rl} (\widetilde{a}_{\epsilon_0,k})_{k'} : H^1(k', W') & \to H^*(k', C) \\ \alpha & \mapsto a_{k'}(\alpha, \epsilon_0) \end{array}.$$

It is easily seen that these maps define a cohomological invariant $\widetilde{a}_{\epsilon_0,k}$ of W' over k. Let k'/k be a field extension and assume that $\alpha \in H^1(k', W')$ lies in the image of a map $H^1(k', H') \to H^1(k', W')$, where H' is an abelian subgroup of W' generated by reflections. Then (α, ϵ_0) is in the image of $H^1(k', H' \times \langle r \rangle) \to H^1(k', W' \times \langle r \rangle)$ and since $H' \times \langle r \rangle$ is an abelian subgroup of $W' \times \langle r \rangle$ generated by reflections, by assumption on a, $a_{k'}(\alpha, \epsilon_0) = 0$. Hence, $(\widetilde{a}_{\epsilon_0,k})_{k'}(\alpha) = 0$. Therefore, $\widetilde{a}_{\epsilon_0,k}$ satisfies the assumption of Theorem 3.1. As Theorem 3.1 is true for W' (by the hypothesis on W'), we get that $\widetilde{a}_{\epsilon_0,k} = 0$. It then yields that $a_k(\alpha_0, \epsilon_0) = 0$. Finally, $a = 0$. ■

We can now give the proof of Theorem 3.1.

Proof. For convenience, we say that $a \in \mathsf{Inv}_{k_0}(W, C)$ satisfies (P) if every restriction of a to an abelian subgroup generated by reflections is zero. We show Theorem 3.1 by induction on the order m of W : if $m = 1$ or $m = 2$, it is trivial. Let $m \geq 3$. Assume that, for every integer l with $1 \leq l < m$, every cohomological invariant of a Coxeter group which satisfies the assumption of Theorem 3.1 over k_0 of order l satisfying (P) is zero.

Let $a \in \mathsf{Inv}_{k_0}(W, C)$ satisfying (P). We will prove that, for any irreducible divisor D of Aff_c^n, the residue $r_{v_D}(a_K(\varphi^{\mathsf{vers}}))$, at the valuation v_D corresponding to the divisor D, is zero. Then, by Theorem 1.4, $a_K(\varphi^{\mathsf{vers}})$ will be constant and since φ^{vers} corresponds to the versal torsor T^{vers} for W over k_0, a will be constant by Theorem 1.7. Thus, since the restrictions of a to any abelian subgroup generated

by reflections are zero, a will vanish on the trivial torsor and we will get that $a = 0$.

Let D be an irreducible divisor in $\mathsf{Spec}(k_0[c_1, ..., c_n])$. Let us prove that the residue $r_{v_D}(a_K(\varphi^{\mathsf{vers}}))$ is zero. We know by Lemma 3.2 and Lemma 3.3 that $\varphi_D^{\mathsf{vers}}(I_{K_D}) = \{1\}$ or $\varphi_D^{\mathsf{vers}}(I_{K_D}) = \langle r \rangle$ for some reflection $r \in W$. In the first case, $\varphi_D^{\mathsf{vers}}$ is not ramified so, by Theorem 1.6, $r_{v_D}(a_K(\varphi^{\mathsf{vers}})) = r_{v_D}(a_{K_D}(\varphi_D^{\mathsf{vers}})) = 0$.

Assume now that $\varphi_D^{\mathsf{vers}}(I_{K_D}) = \langle r \rangle$. By Lemma 3.4, $\varphi_D^{\mathsf{vers}}(\Gamma_{K_D}) \subset W_0 \times \langle r \rangle$. Since W_0 is a proper subgroup of W and a reflection group over k_0, it satisfies the assumptions of Theorem 3.1 so by the induction hypothesis, Theorem 3.1 is true for W_0. By Lemma 3.5, Theorem 3.1 is also true for the group $W_0 \times \langle r \rangle$.

Since a satisfies (P), $\mathsf{Res}_W^{W_0 \times \langle r \rangle}(a)$ also satisfies (P), so $\mathsf{Res}_W^{W_0 \times \langle r \rangle}(a) = 0$. Thus, as $[\varphi_D^{\mathsf{vers}}]$ lies in the image of the map $H^1(K_D, W_0 \times \langle r \rangle) \to H^1(K_D, W)$, we get that $a_{K_D}(\varphi_D^{\mathsf{vers}}) = 0$. Hence, its residue $r_{v_D}(a_{K_D}(\varphi_D^{\mathsf{vers}}))$ is also zero.

We then have shown that, for every irreducible divisor of $\mathsf{Spec}(k_0[c_1, ..., c_n])$, $r_{v_D}(a_{K_D}(\varphi_D^{\mathsf{vers}})) = 0$. This concludes the proof. ■

3.2 Applications

The following two applications directly generalize similar results of Serre for the symmetric groups and were already known to Serre (see [24] 25.15).

3.2.1 Invariants are killed by 2

Recall that W is a finite Coxeter group, k_0 is a field of characteristic zero containing a subfield on which the representation of W, as a reflection group is realizable. Recall also that C is a finite Γ_{k_0}-module.

Let us state a first consequence of Theorem 3.1 (generalizing [24], 24.12).

Corollary 3.1. *For every normalized cohomological invariant $a \in \mathsf{Inv}_{k_0}(W, C)$, $2a = 0$. In particular, if C has odd order, W has no non-trivial normalized invariant.*

Proof. Let $a \in \mathsf{Inv}_{k_0}(W, C)$ be a normalized cohomological invariant. By Theorem 3.1, it is enough to prove that, for any abelian subgroup H of W generated by reflections, $2\mathsf{Res}_W^H(a) = 0$. We prove it by induction on the order m of W. For $m = 1$ or 2, it is trivial.

Let $m \geq 3$. Let us denote by S a root system corresponding to W (see Appendix A). Let H be an abelian subgroup of W generated by reflections. Then $H \simeq$

$\langle r_1\rangle \times \cdots \times \langle r_s\rangle$ for some $s \geq 1$ and for some pairwise commuting reflections $r_1, ..., r_s$ in W. Let e_1 be the root in S corresponding to r_1 and let W' be the group generated by reflections given by the root subsystem $S' = S \cap \{e_1\}^{\perp}$. Then W' is a proper subgroup of W and a reflection group over k_0. Using the induction hypothesis with W' and with the normalized invariant $\mathsf{Res}_W^{W'}(a)$, we get that

$$2(\mathsf{Res}_W^{W'}(a)) = 0.$$

Let $H' = \langle r_2\rangle \times \cdots \times \langle r_s\rangle$. Since $H' \subset W'$,

$$2\mathsf{Res}_W^{H'}(a) = 2\mathsf{Res}_{W'}^{H'}(\mathsf{Res}_W^{W'}(a)) = 0.$$

Let k be an extension of k_0 and let $T \in H^1(k, H)$. Then $T = T_1 \times T_2$, where $T_1 \in H^1(k, \langle r_1\rangle)$ and $T_2 \in H^1(k, H')$. Thus,

$$2\mathsf{Res}_W^{H'}(a)_k(T_2) = 0.$$

Now set $T' = T_1' \times T_2$ the H-torsor , where T_1' is the trivial torsor in $H^1(k, \langle r\rangle)$. Since $T' = T_1' \times T_2 = i^*(T_2)$ with $i : H' \hookrightarrow H$ and $i^* : H^1(k, H') \to H^1(k, H)$ the induced map, the definition of the restriction map yields

$$(\mathsf{Res}_W^H(a))_k(T') = \mathsf{Res}_H^{H'}(\mathsf{Res}_W^H(a))_k(T_2).$$

Therefore,

$$2\mathsf{Res}_W^H(a)_k(T') = 0.$$

Moreover, there is an extension k'/k of degree at most 2 such that T_1 and T_1' are isomorphic over k'. Then T' and T are also isomorphic over k'. Hence,

$$\mathsf{Res}_W^H(a)_{k'}(\mathsf{Res}_{k'/k}(T)) = \mathsf{Res}_W^H(a)_{k'}(\mathsf{Res}_{k'/k}(T')),$$

so

$$\mathsf{Res}_{k'/k}(\mathsf{Res}_W^H(a)_k(T)) = \mathsf{Res}_{k'/k}(\mathsf{Res}_W^H(a)_k(T'))$$

and applying the corestriction map $\mathsf{Cor}_{k'/k}$, we get that

$$[k' : k].\mathsf{Res}_W^H(a)_k(T) = [k' : k].\mathsf{Res}_W^H(a)_k(T')$$

which proves that

$$2\mathsf{Res}_W^H(a)_k(T) = 2\mathsf{Res}_W^H(a)_k(T') = 0.$$

We conclude by using Theorem 3.1 to $2a$.

The second part of Corollary 3.1 directly follows from the first part and from the fact that in the ring $H^*(k_0, C)$, $\#C.1 = 0$. ■

Corollary 3.1 allows us to restrict to Γ_{k_0}-modules C of even order. The most elementary one is of course $\mathbb{Z}/2\mathbb{Z}$ endowed with the trivial action of Γ_{k_0} and we will take $C = \mathbb{Z}/2\mathbb{Z}$ in most of our examples.

3.2.2 Application to negligible cohomology

Let G be a finite group and let M a finite G-module, with trivial action. Let k be a field and $x \in H^*(G, M)$. We have a natural map

$$\begin{aligned}(a_x)_k : H^1(k, G) &\to H^*(k, M)\\ [\varphi] &\mapsto [\varphi^*(x)]\end{aligned}$$

Since G acts trivially on M, for any extension k'/k, the maps $(a_x)_{k'}$ define a cohomological invariant of G over k with coefficients in M.

This gives us a family of cohomological invariants of G. We want to determine the cohomology classes $x \in H^*(G, M)$ for which these invariants are zero.

Definition 3.2. *Let G be a finite group and let M be a G-module. Then a cohomology class $x \in H^*(G, M)$ is negligible if, for any field k and any (continuous) homomorphism $\varphi : \Gamma_k \to G$, we have $\varphi^*(x) = 0$ in $H^*(k, M)$. We denote by $H^*_{negl}(G, M)$ the subset of $H^*(G, M)$ consisting of the negligible cohomology classes.*

In fact, as stated in the following proposition, it is enough to consider only fields of characteristic zero (see [24], 26.1).

Proposition 3.3. *An element $x \in H^*(G, M)$ is negligible if $\varphi^*(x) = 0$ for any field k of characteristic zero and any $\varphi : \Gamma_k \to G$.*

For any $x \in H^*(G, M)$, let us denote by a_x the cohomological invariant over $\mathbb{Q}$ induced by x. Then Proposition 3.3 exactly says that

$$H^*_{\mathsf{negl}}(G, M) = \{x \in H^*(G, M) \mid a_x = 0\}.$$

As a first example, let us give a negligibility criterion for 2-elementary groups (see [24], Lemma 26.4).

Example 3.1. Let G be a 2-elementary group and let $x \in H^i(G, \mathbb{Z}/2\mathbb{Z})$. Then x is negligible if and only if the restriction of x to every subgroup of G of order ≤ 2 is zero.

The following result is clear and its proof is left to the reader.

Lemma 3.6. *Let $i \geq 0$ and let $x \in H^i(G, M)$. For any subgroup H of G,*

$$\mathsf{Res}^H_G(a_x) = a_{\mathsf{Res}^H_G(x)}.$$

The next result is the natural generalization of a result of Serre on negligible cohomology classes of $\mathfrak{S}_n$ (see [24], 26.3) to Weyl groups.

Theorem 3.2. *Let W be a Weyl group and let M be a finite W-module, with trivial action. Let $i \geq 0$. We have the following assertions :*

(1) $x \in H^i(W, M)$ is negligible if and only if its restrictions to the abelian subgroups generated by reflections are negligible.

(2) for any $i > 0$, for any $x \in H^i(W, M)$, the cohomology class $2x$ is negligible.

(3) An element $x \in H^i(W, \mathbb{Z}/2\mathbb{Z})$ is negligible if and only if its restrictions to the subgroups of order ≤ 2 of W are zero.

Proof. *(1)* Let $x \in H^i(W, M)$. By Proposition 3.3, the kernel of the natural map

$$H^i(W, M) \to \mathsf{Inv}_{\mathbb{Q}}(W, M)$$
$$x \mapsto a_x$$

is exactly $H^i_{\mathsf{negl}}(W, M)$. Furthermore, since W is a reflection group over $\mathbb{Q}$ (see Appendix A, Theorem A.2), Theorem 3.1 yields that $a_x = 0$ if and only if $\mathsf{Res}^H_W(a_x) = 0$ for any abelian subgroup H of W generated by reflections. Thus, by Lemma 3.6, x is negligible if and only if for any abelian subgroup H of W generated by reflections, the restriction $\mathsf{Res}^H_W(x)$ is negligible.

(2) Let $i > 0$ and $x \in H^i(W, M)$. Let us show that $a_{2x} = 2a_x$. For any field k of characteristic zero and any $[\varphi] \in H^1(k, W)$, $(a_{2x})_k([\varphi])$ is represented by $(\gamma_1, ..., \gamma_i) \mapsto 2x(\varphi(\gamma_1), ..., \varphi(\gamma_i))$. Hence, $a_{2x} = 2a_x$. We conclude the proof by using Corollary 3.1.

(3) By *(1)*, $x \in H^i(W, \mathbb{Z}/2\mathbb{Z})$ is negligible if and only if for any abelian subgroup H of W generated by reflections, $\mathsf{Res}^H_W(x)$ is negligible. Then, Example 3.1 allows us to conclude. ■

Chapter 4

Cohomological invariants of the Weyl group of type B or C

RÉSUMÉ

Dans ce chapitre, on s'intéresse aux groupes de Weyl de type B (ou C, ce sont les mêmes). A l'aide de l'interprétation en termes d'algèbres étales pointées donnée dans le premier chapitre, on peut définir deux familles d'invariants de Stiefel-Whitney, ceux associés à la forme quadratique trace et ceux associés à la forme quadratique trace tordue. L'objectif de ce chapitre est de prouver à l'aide du principe d'annulation établi au chapitre 3 que tout invariant cohomologique d'un groupe de Weyl de type B s'écrit comme combinaison linéaire de cup-produits d'invariants de Stiefel-Whitney.

Let k_0 be a field of characteristic different from 2 and let W be a Weyl group. Then the cup-product endows the abelian group $\mathsf{Inv}_{k_0}(W, \mathbb{Z}/2\mathbb{Z})$ with an $H^*(k_0, \mathbb{Z}/2\mathbb{Z})$-module structure.

Let $n \geq 2$, let $(e_1, ..., e_n)$ be the canonical basis of $\mathbb{R}^n$ and let S be the root system of type B_n : $S = \{\pm e_i, \pm e_i \pm e_j, 1 \leq i \neq j \leq n\}$. Let us denote by W its Weyl group. By the classification given in Appendix A, W is isomorphic to the semi-direct product $\left(\mathbb{Z}/2\mathbb{Z}\right)^n \rtimes \mathfrak{S}_n$, where $\mathfrak{S}_n$ acts on $\left(\mathbb{Z}/2\mathbb{Z}\right)^n$ by permuting coordinates. Note that the Weyl group of type C_n is isomorphic to W, so both cases B and C are the same.

The purpose of this chapter is to prove the following structure theorem for the

$H^*(k_0, \mathbb{Z}/2\mathbb{Z})$-module $\mathsf{Inv}_{k_0}(W, \mathbb{Z}/2\mathbb{Z})$.

Theorem 4.1. *Let k_0 be a field of characteristic zero, such that -1 and 2 are squares in k_0, let $n \geq 2$ and let W be a Weyl group of type B_n. Then the $H^*(k_0, \mathbb{Z}/2\mathbb{Z})$-module $\mathsf{Inv}_{k_0}(W, \mathbb{Z}/2\mathbb{Z})$ is free with basis*

$$\{w_i \cdot \widetilde{w}_j\}_{0 \leq i \leq [\frac{n}{2}], 0 \leq j \leq 2([\frac{n}{2}]-i)}.$$

4.1 The vanishing principle for Weyl groups of type B_n

Let us start with restating the vanishing principle (Theorem 3.1) in the case of a Weyl group of type B_n, especially in terms of pointed étale algebras (see Proposition 1.8).

For any integer q such that $0 \leq q \leq [\frac{n}{2}]$, let H_q be the subgroup of W associated with the root subsystem of S :

$$S_q = \{\pm e_1 \pm e_2, \pm e_3 \pm e_4, ..., \pm e_{2q-1} \pm e_{2q}, \pm e_{2q+1}, ..., \pm e_n\}.$$

Then it is easily seen that the set $\{H_q \mid 0 \leq q \leq [\frac{n}{2}]\}$ forms a system of representatives modulo conjugation of the maximal abelian subgroups of W generated by reflections.

Proposition 4.1. *Assume that n is even (the case n odd is similar), and let k/k_0 be an extension. Let $0 \leq q \leq \frac{n}{2}$ and let $u_1, ..., u_{n/2}, v_1, ..., v_{n/2}$ be square-classes in $k^\times$. The image of $(u_1, v_1, u_2, v_2, ..., u_{n/2}, v_{n/2})$ by the map $H^1(k, H_q) \to H^1(k, W)$ is*

$$T_q = (k(\sqrt{u_1 v_1}) \times \cdots \times k(\sqrt{u_q v_q}) \times k^{n-2q}, (u_1, u_2, ..., u_q, u_{q+1}, v_{q+1}, ..., u_{n/2}, v_{n/2})).$$

Proof. For any $0 \leq q' \leq q$, set $\varphi_{q'} : \gamma \mapsto \frac{\gamma(\sqrt{u_{q'}})}{\sqrt{u_{q'}}}$ and $\psi_{q'} : \gamma \mapsto \frac{\gamma(\sqrt{v_{q'}})}{\sqrt{v_{q'}}}$. For $2q+1 \leq q' \leq \frac{n}{2}$, set $\eta_{q'} : \gamma \mapsto \begin{cases} \frac{\gamma\left(\sqrt{u_{[\frac{q'}{2}]}}\right)}{\sqrt{u_{[\frac{q'}{2}]}}} \text{ if } q' \text{ is odd} \\ \frac{\gamma\left(\sqrt{v_{[\frac{q'}{2}]}}\right)}{\sqrt{v_{[\frac{q'}{2}]}}} \text{ if } q' \text{ is even} \end{cases}$. To be precise, we then compose these morphisms $\varphi_{q'}$, $\psi_{q'}$ and $\eta_{q'}$ by the group isomorphism $\{\pm 1\} \xrightarrow{\sim} \mathbb{Z}/2\mathbb{Z}$, so that we get cocycles with values in $\mathbb{Z}/2\mathbb{Z}$. Note that we still call $\varphi_{q'}$, $\psi_{q'}$ and $\eta_{q'}$ these cocycles.

Now set

$$\Phi : \gamma \mapsto (r_{e_1+e_2})^{\varphi_1(\gamma)} \cdot (r_{e_1-e_2})^{\psi_1(\gamma)} \cdot (r_{e_3+e_4})^{\varphi_2(\gamma)} \cdot (r_{e_3-e_4})^{\psi_2(\gamma)} \cdots (r_{e_{2q-1}+e_{2q}})^{\varphi_q(\gamma)} \cdot (r_{e_{2q-1}-e_{2q}})^{\psi_q(\gamma)} \cdot (r_{e_{2q+1}})^{\eta_{2q+1}(\gamma)} \cdot (r_{e_{2q+2}})^{\eta_{2q+2}(\gamma)} \cdots (r_{e_n})^{\eta_n(\gamma)}.$$

For any $0 \leq q' \leq q$, the maps $\varphi_{q'}$ and $\psi_{q'}$ are cocycles with values in $\mathbb{Z}/2\mathbb{Z}$ and any two r_e and $r_{e'}$ in H_q commute. Therefore, Φ is a cocycle of W over k, representing the cohomology class image of $(u_1, v_1, u_2, v_2, ..., u_{n/2}, v_{n/2})$ by the map $H^1(k, H_q) \to H^1(k, W)$. Let us show that Φ represents the cohomology class T_q. Indeed, if we take the first two factors $\gamma \mapsto (r_{e_1+e_2})^{\varphi_1(\gamma)} \cdot (r_{e_1-e_2})^{\psi_1(\gamma)}$, it corresponds to a cocycle $\Phi_1 : \gamma \mapsto ((\epsilon_1(\gamma), \epsilon_2(\gamma)), \sigma_1(\gamma))$ with values in $\mathbb{D}_4$ (see Proposition 1.8). For any $\gamma \in \Gamma_k$,

$$\begin{aligned} r_{e_1-e_2}(e_1) &= e_2, \\ r_{e_1+e_2}(e_1) &= -e_2, \\ r_{e_1+e_2} \circ r_{e_1-e_2}(e_1) &= -e_1. \end{aligned}$$

Hence,

$$\begin{aligned} \sigma_1(\gamma) &= (12)^{\varphi_1(\gamma)+\psi_1(\gamma)} \\ \epsilon_1(\gamma) &= \varphi_1(\gamma) \\ \epsilon_2(\gamma) &= \varphi_1(\gamma). \end{aligned}$$

It is now easily seen that Φ_1 represents the cohomology class $(k(\sqrt{u_1 v_1}), u_1)$. We then can do the same for the other factors. It then follows that Φ represents the cohomology class T_q. ■

We may now reformulate Theorem 3.1 for Weyl groups of type B_n, $n \geq 2$.

Corollary 4.1. *Let k_0 be a field of characteristic zero, let C be a finite Γ_{k_0}-module and let $a \in \mathit{Inv}_{k_0}(W, C)$. Then $a = 0$ if and only if for any $0 \leq q \leq [\frac{n}{2}]$, $\mathit{Res}_W^{H_q}(a) = 0$. In other words, $a = 0$ if and only if a vanishes on the pairs*

$$(k(\sqrt{t_1}) \times \cdots \times k(\sqrt{t_q}) \times k^{n-2q}, (\alpha_1, ..., \alpha_{n-q}))$$

(for $0 \leq q \leq [\frac{n}{2}]$), where the square-class α_i has a representative in $k^\times$ for any $0 \leq i \leq n - q$.

Proof. Since Γ_k acts trivially on W, the images of the maps $H^1(k, H) \to H^1(k, W)$ and $H^1(k, H') \to H^1(k, W)$ are the same if H and H' are two conjugate subgroups of W. Then the result directly follows from Theorem 3.1. ■

4.2 Proof of Theorem 4.1 for n even : a generating family

For all this section, let us assume that n is even and set $m = \frac{n}{2}$.

Let us explain the strategy of the proof. We will show that the family of Stiefel-Whitney invariants

$$\{w_i \cdot \widetilde{w}_j\}_{0 \leq i \leq [\frac{n}{2}], 0 \leq j \leq 2([\frac{n}{2}]-i)}$$

generates the module $\mathsf{Inv}_{k_0}(W, \mathbb{Z}/2\mathbb{Z})$ by induction on $m \geq 1$. If $m = 1$, $W \simeq \mathbb{D}_4$ and Theorem 2.4 gives the answer. Let $m \geq 2$ and let $a \in \mathsf{Inv}_{k_0}(W, \mathbb{Z}/2\mathbb{Z})$. Then we show, as a consequence of Corollary 4.1 that, if we consider a particular subgroup W_0 of W isomorphic to $\mathbb{D}_4 \times W'$, where W' is a Weyl group of type B_{2m-2}, then a is completely determined by $\mathsf{Res}_W^{W_0}(a)$. Since we know the invariants of $\mathbb{D}_4$ and of W', we can write $\mathsf{Res}_W^{W_0}(a)$ in terms of invariants of W_0, that we can describe from invariants of $\mathbb{D}_4$ and W'. Then, by a second induction on $0 \leq q \leq m$, we study the restrictions to H_q in order to identify $\mathsf{Res}_W^{W_0}(a)$ with a linear combination of the restrictions of the required Stiefel-Whitney invariants.

From now on, let k_0 be any field of characteristic zero such that -1 and 2 are squares in k_0. However, much (but not all) of what follows is true, without this assumption.

We now prove the following result by induction on $m \geq 1$.

Proposition 4.2. *For any $m \geq 1$, if W is a Weyl group of type B_{2m}, the family $\{w_i \cdot \widetilde{w}_j\}_{0 \leq i \leq m, 0 \leq j \leq 2(m-i)}$ generates $\mathsf{Inv}_{k_0}(W, \mathbb{Z}/2\mathbb{Z})$ as an $H^*(k_0, \mathbb{Z}/2\mathbb{Z})$-module.*

If $m = 1$, $W \simeq \mathbb{D}_4$ and Theorem 2.4 allows us to conclude.

Let $m \geq 2$ and let W be a Weyl group of type B_{2m}. Let us assume that any Weyl group W' of type $B_{2(m-1)}$ satisfies the induction hypothesis, i.e. the family $\{w_i^{W'} \cdot \widetilde{w}_j^{W'}\}_{0 \leq i \leq m-1, 0 \leq j \leq 2(m-1-i)}$ generates the module $\mathsf{Inv}_{k_0}(W', \mathbb{Z}/2\mathbb{Z})$ over $H^*(k_0, \mathbb{Z}/2\mathbb{Z})$.

Let W be a Weyl group of type B_{2m}. It corresponds to a root system

$$S = \{\pm e_i, \pm e_i \pm e_j, 1 \leq i \leq 2m, 1 \leq j \neq i \leq 2m\}$$

Let us denote by W' the subgroup of W corresponding to the root subsystem

$$S' = \{\pm e_i, \pm e_i \pm e_j, 3 \leq i \leq 2m, 3 \leq j \neq i \leq 2m\}.$$

It is a Weyl group of type B_{2m-2}. Let us also denote by W_0 the non-irreducible Weyl group corresponding to the root subsystem $\{\pm e_1, \pm e_2, \pm e_1 \pm e_2\} \sqcup S'$. Then W_0 is a subgroup of W isomorphic to $\mathbb{D}_4 \times W'$.

Lemma 4.1. *Any cohomological invariant of W over k_0 with coefficients in $\mathbb{Z}/2\mathbb{Z}$ is completely determined by its restriction to W_0.*

Proof. By Corollary 4.1, any invariant of W is completely determined by its restrictions to the subgroups H_q for $0 \leq q \leq m$. Let $0 \leq q \leq m$. The root system S_q defined in Section 4.1 corresponding to H_q is clearly a subset of

$$\{\pm e_1, \pm e_2, \pm e_1 \pm e_2\} \sqcup S'.$$

Hence, $H_q \subset W_0$. It implies that, if k/k_0 is an extension and if T_q is a W-torsor over k which lies in the image of $H^1(k, H_q) \to H^1(k, W)$, then T_q also lies in the image of $H^1(k, W_0) \to H^1(k, W)$. ■

4.2.1 Restrictions of the Stiefel-Whitney invariants to W_0 and to the subgroups H_q

The aim of this section is to give formulae for restrictions of Stiefel-Whitney invariants to the subgroups W_0 and H_q, $q = 0, ..., m$. Note that $w_0 = 1 = \widetilde{w}_0$. Let us first compute the restrictions of Stiefel-Whitney invariants to W_0.

Proposition 4.3. *We have the following formulae :*

(i) for $1 \leq j \leq 2m$, $\mathsf{Res}_W^{W_0}(\widetilde{w}_j) = \widetilde{w}_2^{\mathbb{D}_4} \cdot \widetilde{w}_{j-2}^{W'} + \widetilde{w}_1^{\mathbb{D}_4} \cdot \widetilde{w}_{j-1}^{W'} + \widetilde{w}_j^{W'}$;

(ii) for $1 \leq i \leq m$, $\mathsf{Res}_W^{W_0}(w_i) = w_i^{W'} + w_1^{\mathbb{D}_4} \cdot w_{i-1}^{W'}$;

(iii) for $1 \leq i \leq m$ *and* $1 \leq j \leq 2(m-i)$,

$$\mathsf{Res}_W^{W_0}(w_i \cdot \widetilde{w}_j) = \widetilde{w}_2^{\mathbb{D}_4} \cdot w_i^{W'} \cdot \widetilde{w}_{j-2}^{W'} + \widetilde{w}_1^{\mathbb{D}_4} \cdot w_i^{W'} \cdot \widetilde{w}_{j-1}^{W'} + w_1^{\mathbb{D}_4} \cdot w_{i-1}^{W'} \cdot \widetilde{w}_j^{W'} + w_i^{W'} \cdot \widetilde{w}_j^{W'}.$$

Proof. Let k/k_0 be a field extension. Let $(L, \alpha) \in H^1(k, W_0)$. Then $L = L_1 \times L_2$ with L_1 an étale k-algebra of rank 2 and $\alpha = (\alpha_1, \alpha_2)$. Thus, the quadratic form $q_{L,\alpha} : x \mapsto \mathsf{Tr}_L(\alpha x^2)$ decomposes into $q_{L,\alpha} = q_{L_1,\alpha_1} \oplus q_{L_2,\alpha_2}$. Hence, for $0 \leq j \leq 2m$,

$$w_j(q_{L,\alpha}) = \sum_{0 \leq i \leq j} w_i(q_{L_1,\alpha_1}) \cdot w_{j-i}(q_{L_2,\alpha_2}).$$

Since $w_i(q_{L_1,\alpha_1}) = 0$ as soon as $i > 2$, we get that

$$w_j(q_{L,\alpha}) = w_2(q_{L_1,\alpha_1}) \cdot w_{j-2}(q_{L_2,\alpha_2}) + w_1(q_{L_1,\alpha_1}) \cdot w_{j-1}(q_{L_2,\alpha_2}) + w_j(q_{L_2,\alpha_2})$$

which gives us *(i)*. Likewise, with the quadratic form $q_L : x \mapsto \mathsf{Tr}_L(x^2)$, we get that, for $0 \leq i \leq m$,

$$w_i(q_L) = w_2(q_{L_1}) \cdot w_{i-2}(q_{L_2}) + w_1(q_{L_1}) \cdot w_{i-1}(q_{L_2}) + w_i(q_{L_2})$$

Thus, *(ii)* follows from Proposition 2.12 using the assumption that -1 and 2 are squares in $k_0^\times$. Since the cup-product commutes with the restriction map, Formula *(iii)* follows from *(i)*, *(ii)* and from Proposition 2.12. ■

Let us now consider the restrictions of Stiefel-Whitney invariants to the subgroups H_q, for $0 \leq q \leq m$. We do not need here the exhaustive list of all the restrictions, so we only give those that will be useful in the sequel.

Lemma 4.2. *Let $q \in \{0, ..., m-1\}$. For all $q+1 \leq i \leq m$ and all $0 \leq j \leq 2(m-i)$,*

$$\mathsf{Res}_W^{H_q}(w_i \cdot \widetilde{w}_j) = 0.$$

Proof. If k is an extension of k_0 and if

$$T_q = (k(\sqrt{t_1}) \times ... \times k(\sqrt{t_q}) \times k^{2(m-q)}, (u_1, ..., u_q, u_{q+1}, v_{q+1}, ..., u_m, v_m))$$

is a W-torsor over k lying in the image of $H^1(k, H_q) \to H^1(k, W)$, then

$$\begin{aligned} w_i(T_q) &= w_i(\langle 2, 2t_1, 2, 2t_2, ..., 2, 2t_q \rangle) \\ &= w_i(\langle 1, t_1, ..., 1, t_q \rangle) \\ &= w_i(\langle t_1, ..., t_q \rangle) \end{aligned}$$

which is 0 since $i \geq q+1$. ■

Let us go further for the case $q = 0$. Recall that, for any $I \subset \{1, ..., 2m\}$, a_I denotes the invariant of H_0 given by $(x_1, ..., x_{2m}) \mapsto (x)_I$, where $(x)_I$ is the cup-product of the (x_i) for $i \in I$ (see Corollary 2.1). Recall also that $a_j^{(0)}$ denotes the invariant $\sum_{I \subset \{1,...,2m\}; |I| = j} a_I$, for $0 \leq j \leq 2m$ (see Proposition 2.6).

Lemma 4.3. *For any $0 \leq j \leq 2m$, $\mathsf{Res}_W^{H_0}(\widetilde{w}_j) = a_j^{(0)}$. In particular, the family $\{\mathsf{Res}_W^{H_0}(\widetilde{w}_j)\}_{0 \leq j \leq 2m}$ is free over $H^*(k_0, \mathbb{Z}/2\mathbb{Z})$.*

Proof. If k/k_0 is an extension and $T_0 = (k^{2m}, (u_1, v_1, ..., u_m, v_m))$ is a W-torsor over k lying in the image of $H^1(k, H_0) \to H^1(k, W)$, we have

$$\widetilde{w}_j(T_0) = w_j(\langle u_1, v_1, ..., u_m, v_m \rangle) = a_j^{(0)}(u_1, v_1, ..., u_m, v_m).$$

Moreover, by Proposition 2.6, the invariants $a_j^{(0)}$ form a basis of the submodule $\mathsf{Inv}_{k_0}(H_0, \mathbb{Z}/2\mathbb{Z})^{N_0/H_0}$ and this gives the freedom of $\{\mathsf{Res}_W^{H_0}(\widetilde{w}_j)\}_{0 \leq j \leq 2m}$. ■

Lemma 4.4. *Let $0 \leq i \leq m$. Then, for any $j > 2(m-i)$, $w_i \cdot \widetilde{w}_j = 0$.*

Proof. Let $j > 2(m-i)$. By Corollary 4.1, it is enough to show that the restriction of $w_i \cdot \widetilde{w}_j$ to any subgroup H_q of W $(0 \leq q \leq m)$ is zero. Let $0 \leq q \leq m$, let k/k_0 be a field extension and let

$$T_q = (k(\sqrt{t_1}) \times ... \times k(\sqrt{t_q}) \times k^{2(m-q)}, (u_1, ..., u_q, u_{q+1}, v_{q+1}, ..., u_m, v_m))$$

be a W-torsor over k lying in the image of $H^1(k, H_q) \to H^1(k, W)$. We then have to show that $w_i(T_q) \cdot \widetilde{w}_j(T_q) = 0$. By Lemma 4.2, $w_i(T_q) = 0$ if $q < i$. Let us

assume that $q \geq i$. We have :

$$\begin{aligned} w_i(T_q) \cdot \widetilde{w}_j(T_q) &= w_i(\langle t_1, ..., t_q \rangle) \cdot w_j(\langle u_1, u_1t_1, ..., u_q, u_qt_q, u_{q+1}, v_{q+1}, ..., u_m, v_m \rangle) \\ &= \sum_{1 \leq j_1 < ... < j_i \leq q} (t_{j_1}) \cdot \ldots \cdot (t_{j_i}) \cdot \big[\sum_{j'=0}^{j} w_{j'}(\langle u_1, u_1t_1, ..., u_q, u_qt_q \rangle) \\ &\qquad \cdot w_{j-j'}(\langle u_{q+1}, v_{q+1}, ..., u_m, v_m \rangle) \big]. \end{aligned}$$

Since the quadratic form $\langle u_{q+1}, v_{q+1}, ..., u_m, v_m \rangle$ has rank $2(m-q)$, we have $w_{j-j'}(\langle u_{q+1}, v_{q+1}, ..., u_m, v_m \rangle) = 0$ if $j - j' > 2(m-q)$. So we get :

$$\begin{aligned} w_i(T_q) \cdot \widetilde{w}_j(T_q) = &\sum_{1 \leq j_1 < ... < j_i \leq q} (t_{j_1}) \cdot \ldots \cdot (t_{j_i}) \\ &\cdot \big[\sum_{j'=j-2(m-q)}^{j} w_{j'}(\langle u_1, u_1t_1, ..., u_q, u_qt_q \rangle) \\ &\qquad \cdot w_{j-j'}(\langle u_{q+1}, v_{q+1}, ..., u_m, v_m \rangle) \big]. \end{aligned}$$

Since $j > 2(m-i)$, then $j - 2(m-q) > 2(q-i)$, which gives us :

$$\begin{aligned} w_i(T_q) \cdot \widetilde{w}_j(T_q) = &\sum_{1 \leq j_1 < ... < j_i \leq q} (t_{j_1}) \cdot \ldots \cdot (t_{j_i}) \\ &\cdot \big[\sum_{j'=2(q-i)+1}^{j} w_{j'}(\langle u_1, u_1t_1, ..., u_q, u_qt_q \rangle) \\ &\qquad \cdot w_{j-j'}(\langle u_{q+1}, v_{q+1}, ..., u_m, v_m \rangle) \big]. \end{aligned} \tag{4.1}$$

Let us show that, for any $0 \leq j \leq q$ and any $2(q-i) < j' \leq j$,

$$\begin{aligned} &(t_j) \cdot w_{j'}(\langle u_1, u_1t_1, ..., u_q, u_qt_q \rangle) \\ &\quad = (t_j) \cdot w_{j'}(\langle u_1, u_1t_1, ..., u_{j-1}, u_{j-1}t_{j-1}, u_{j+1}, u_{j+1}t_{j+1}, ..., u_q, u_qt_q \rangle). \end{aligned} \tag{4.2}$$

Let $2(q-i) < j' \leq j$. For sake of simplicity, let us assume that $j = 1$. We have

$$\begin{aligned} w_{j'}(\langle u_1, u_1t_1, ..., u_q, u_qt_q \rangle) = &(u_1) \cdot (u_1t_1) \cdot w_{j'-2}(\langle u_2, u_2t_2, ..., u_q, u_qt_q \rangle) \\ &+ (u_1) \cdot w_{j'-1}(\langle u_2, u_2t_2, ..., u_q, u_qt_q \rangle) \\ &+ (u_1t_1) \cdot w_{j'-1}(\langle u_1, u_1t_1, ..., u_q, u_qt_q \rangle) \\ &+ w_{j'}(\langle u_2, u_2t_2, ..., u_q, u_qt_q \rangle), \end{aligned}$$

so

$$\begin{aligned} w_{j'}(\langle u_1, u_1t_1, ..., u_q, u_qt_q \rangle) = &(u_1) \cdot (u_1t_1) \cdot w_{j'-2}(\langle u_2, u_2t_2, ..., u_q, u_qt_q \rangle) \\ &+ (t_1) \cdot w_{j'-1}(\langle u_2, u_2t_2, ..., u_q, u_qt_q \rangle) \\ &+ w_{j'}(\langle u_2, u_2t_2, ..., u_q, u_qt_q \rangle). \end{aligned}$$

Hence,

$$\begin{aligned}(t_1)\cdot w_{j'}(\langle u_1, u_1t_1, ..., u_q, u_qt_q\rangle)&\\ = (t_1)\cdot(u_1)\cdot(u_1t_1)\cdot w_{j'-2}(\langle u_2, u_2t_2, ..., u_q, u_qt_q\rangle)&\\ + (t_1)\cdot(t_1)\cdot w_{j'-1}(\langle u_2, u_2t_2, ..., u_q, u_qt_q\rangle)&\\ + (t_1)\cdot w_{j'}(\langle u_2, u_2t_2, ..., u_q, u_qt_q\rangle).&\end{aligned}$$

Since $(t_1)\cdot(u_1)\cdot(u_1t_1) = 0$ and $(t_1)\cdot(t_1) = (t_1)\cdot(-1) = 0$, we get that

$$(t_1)\cdot w_{j'}(\langle u_1, u_1t_1, ..., u_q, u_qt_q\rangle) = (t_1)\cdot w_{j'}(\langle u_2, u_2t_2, ..., u_q, u_qt_q\rangle).$$

This proves (4.2). An obvious induction shows that, for any $0 \leq j_1 < ... < j_i \leq q$,

$$\begin{aligned}(t_{j_1})\cdot....\cdot(t_{j_i})\cdot w_{j'}(\langle u_1, u_1t_1, ..., u_q, u_qt_q\rangle)&\\ = (t_{j_1})\cdot....\cdot(t_{j_i})\cdot w_{j'}(\langle u_{j'_1}, u_{j'_1}t_{j'_1}, ..., u_{j'_{q-i}}, u_{j'_{q-i}}t_{j'_{q-i}}\rangle)&\end{aligned}$$

where $\{j'_1, ..., j'_{q-i}\}$ is the complementary of $\{j_1, ...j_i\}$ in $\{1, ..., q\}$. Since the quadratic form $Q = \langle u_{j'_1}, u_{j'_1}t_{j'_1}, ..., u_{j'_{q-i}}, u_{j'_{q-i}}t_{j'_{q-i}}\rangle$ has rank $2(q-i)$, we get, for any $j' > 2(q-i)$, that $w_{j'}(Q) = 0$. Using this in Equation (4.1), we can conclude that $w_i(T_q)\cdot\widetilde{w}_j(T_q) = 0$. ■

Remark. This lemma does not hold anymore if we do not assume that -1 or 2 are squares in k_0.

Let us state the last lemma of this section.

Lemma 4.5. *Let $0 \leq q \leq m$. The family $\{\mathsf{Res}^{H_q}_W(w_q\cdot\widetilde{w}_j)\}_{0\leq j\leq 2(m-q)}$ is free over $H^*(k_0, \mathbb{Z}/2\mathbb{Z})$.*

Proof. To show that this family of invariants is free, it is enough to prove that the value of the invariants on a versal H_q-torsor over k_0 form a free family (see Theorem 1.7). Let $t_1, ..., t_q, u_1, ..., u_m, v_{q+1}, ..., v_m$ be independent indeterminates over k_0 and set $K = k_0(t_1, ..., t_q, u_1, ..., u_m, v_{q+1}, ..., v_m)$. Let us denote by T_q the image of the versal H_q-torsor

$$(u_1, u_1t_1, ..., u_q, u_qt_q, u_{q+1}, v_{q+1}, ..., u_m, v_m)$$

by $H^1(K, H_q) \to H^1(K, W)$. We have to show that the cohomology classes $w_q(T_q)\cdot\widetilde{w}_j(T_q)$ where $0 \leq j \leq 2(m-q)$ form a free family over $H^*(k_0, \mathbb{Z}/2\mathbb{Z})$.

Let $0 \leq j \leq 2(m-q)$. We have $w_q(T_q) = w_q(\langle t_1, ..., t_q\rangle) = (t_1)\cdot....\cdot(t_q)$ and

$$\begin{aligned}\widetilde{w}_j(T_q) &= w_j(\langle 2u_1, 2u_1t_1, ..., 2u_q, 2u_qt_q, u_{q+1}, v_{q+1}, ..., u_m, v_m\rangle)\\ &= w_j(\langle u_1, u_1t_1, ..., u_q, u_qt_q, u_{q+1}, v_{q+1}, ..., u_m, v_m\rangle)\\ &= \sum_{0\leq j'\leq j} w_{j'}(\langle u_1, u_1t_1, ..., u_q, u_qt_q\rangle)\cdot w_{j-j'}(\langle u_{q+1}, v_{q+1}, ..., u_m, v_m\rangle).\end{aligned}$$

As shown in the proof of Lemma 4.4, for any $1 \leq j' \leq j$,

$$(t_1) \cdot w_{j'}(\langle u_1, u_1t_1, ..., u_q, u_qt_q\rangle) = (t_1) \cdot w_{j'}(\langle u_2, u_2t_2, ..., u_q, u_qt_q\rangle).$$

Thus an easy induction shows that $(t_1) \cdot \ldots \cdot (t_q) \cdot w_{j'}(\langle u_1, u_1t_1, ..., u_q, u_qt_q\rangle) = 0$. Hence,

$$w_q(T_q) \cdot \widetilde{w}_j(T_q) = (t_1) \cdot \ldots \cdot (t_q) \cdot w_j(\langle u_{q+1}, v_{q+1}, ..., u_m, v_m\rangle).$$

Furthermore, since the monomials in $(t_1), ..., (t_q), (u_1), ..., (u_m), (v_{q+1}), ..., (v_m)$ form a free family over $H^*(k_0, \mathbb{Z}/2\mathbb{Z})$, it is easily seen that the invariants $w_q(T_q) \cdot \widetilde{w}_j(T_q)$, for $0 \leq j \leq 2(m-q)$, also form a free family over $H^*(k_0, \mathbb{Z}/2\mathbb{Z})$. ■

Remark. This lemma, contrary to Lemma 4.4, is still true if we do not assume anymore that -1 or 2 are squares in k_0.

4.2.2 Cohomological invariants of W_0

The subgroup W_0 of W is isomorphic to the direct product $W(B_2) \times W(B_{n-2})$. Therefore, since we know a basis of the module of the cohomological invariants of $\mathbb{D}_4$ (see Theorem 2.4), then by Proposition 2.2 and by the induction hypothesis, we get the description of the cohomological invariants of W_0.

Corollary 4.2. *The module* $\mathsf{Inv}_{k_0}(W_0, \mathbb{Z}/2\mathbb{Z})$ *is free with basis*

$$\{w_l^{\mathbb{D}_4} \cdot w_i^{W'} \cdot \widetilde{w}_j^{W'}\}_{l \in \{0,1,\widetilde{1},\widetilde{2}\}, 0 \leq i \leq m-1, 0 \leq j \leq 2(m-1-i)}.$$

Note that we do not need to make the assumption here that the family

$$\{w_i^{W'} \cdot \widetilde{w}_j^{W'}\}_{0 \leq i \leq m-1, 0 \leq j \leq 2(m-1-i)}$$

is free over $H^*(k_0, \mathbb{Z}/2\mathbb{Z})$. Note also that we used (and we still do it later on) the notation $w_{\widetilde{1}}^{\mathbb{D}_4} = \widetilde{w}_1^{\mathbb{D}_4}$ and $w_{\widetilde{2}}^{\mathbb{D}_4} = \widetilde{w}_2^{\mathbb{D}_4}$ in order to simplify the expressions.

Let us summarize what we got. Let $a \in \mathsf{Inv}_{k_0}(W, \mathbb{Z}/2\mathbb{Z})$. By Corollary 4.1, the invariant a is completely determined by its values on the W-torsors that lie in the image of a map $H^1(k, H_q) \to H^1(k, W)$ (for $0 \leq q \leq m$). In fact, Lemma 4.1 yields that a is completely determined by its restriction to the subgroup W_0 and so by its values on the W-torsors that are the image of a W_0-torsor. For any extension k/k_0, such a torsor is a W-torsor over k of the form $T_1 \times T_2$, where T_1 is a $\mathbb{D}_4$-torsor over k and T_2 a W'-torsor over k. In the sequel, we will then work with these W-torsors of the form $T_1 \times T_2$ over any extension k/k_0.

By Corollary 4.2, there exist some $b_{l,i,j} \in H^*(k_0, \mathbb{Z}/2\mathbb{Z})$, for any $l \in \{0, 1, \widetilde{1}, \widetilde{2}\}$, any $0 \leq i \leq m-1$ and any $0 \leq j \leq 2(m-1-i)$ such that

$$\mathsf{Res}_W^{W_0}(a) = \sum_{l \in \{0,1,\widetilde{1},\widetilde{2}\}, 0 \leq i \leq m-1, 0 \leq j \leq 2(m-1-i)} b_{l,i,j} \cdot w_l^{\mathbb{D}_4} \cdot w_i^{W'} \cdot \widetilde{w}_j^{W'}. \tag{4.3}$$

4.2.3 Restrictions of $\mathsf{Res}_W^{W_0}(a)$ to H_q, for $0 \leq q \leq m$

We now show the following proposition by induction on $q \in \{0, ..., m-1\}$.

Proposition 4.4. *There are some coefficients $C_{i,j} \in H^*(k_0, \mathbb{Z}/2\mathbb{Z})$ such that, for any $0 \leq q \leq m-1$,*

$$\mathsf{Res}_W^{W_0}(a) = \sum_{0 \leq i \leq q, 0 \leq j \leq 2(m-i)} C_{i,j} \cdot \mathsf{Res}_W^{W_0}(w_i \cdot \widetilde{w}_j) + a_{q+1}$$

where

$$a_{q+1} = \sum_{l \in \{0,\widetilde{1},\widetilde{2}\}, q+1 \leq i \leq m-1, 0 \leq j \leq 2(m-1-i)} b_{l,i,j} \cdot w_l^{\mathbb{D}_4} \cdot w_i^{W'} \cdot \widetilde{w}_j^{W'} + \sum_{q \leq i < m-1, 0 \leq j \leq 2(m-1-i)} b_{1,i,j} \cdot w_1^{\mathbb{D}_4} \cdot w_i^{W'} \cdot \widetilde{w}_j^{W'}.$$

In other words, at each step q of our induction, we identify parts of the sums with a linear combination of the invariants $w_q \cdot \widetilde{w}_j$ for $0 \leq j \leq 2(m-q)$ by considering the restriction to the subgroup H_q, where we have a lot of information about torsors, Stiefel-Whitney invariants, etc. It then reduces the extra term a_{q+1}. We finally show that at rank m of the induction, the extra term has completely disappeared.

Proof. Before starting with the proof, let us sketch the main idea of the proof. Let k/k_0 be a field extension. Then $H^1(k, W_0) \simeq H^1(k, \mathbb{D}_4) \times H^1(k, W')$, so any W_0-torsor over k writes (T_1, T_2) with $T_1 \in H^1(k, \mathbb{D}_4)$ and $T_2 \in H^1(k, W')$. If moreover $T_2 = T_1' \times T_3$ with $T_1' \in H^1(k, \mathbb{D}_4)$, the images of the two W_0-torsors $(T_1, T_1' \times T_3)$ and $(T_1', T_1 \times T_3)$ by the map $H^1(k, W_0) \to H^1(k, W)$ are obviously the same. Therefore, $\mathsf{Res}_W^{W_0}(a)$ lies in the submodule of the invariants c of W_0 satisfiyng the equalities $c_k(T_1, T_1' \times T_3) = c_k(T_1', T_1 \times T_3)$ for any such torsors T_1, T_1' and T_3. We then show that the restrictions of the Stiefel-Whitney invariants to W_0 generate this submodule.

Let us prove Proposition 4.4 by induction on q. Let us check the case $q = 0$ first : let us consider the restriction $\mathsf{Res}_W^{H_0}(a)$. Let k/k_0 be an extension, let $T_1 = (k^2, (u_1, v_1))$ be a $\mathbb{D}_4$-torsor over k and let $T' = (k^{2m-2}, (u_2, v_2, ..., u_m, v_m))$

be a W'-torsor over k so that the cohomology class associated with $T_1 \times T'$ lies in the image of $H^1(k, H_0) \to H^1(k, W)$. Hence,

$$a_k(T_1 \times T') = \sum_{\substack{l \in \{0,1,\widetilde{1},\widetilde{2}\},\\ 0 \leq i \leq m-1, 0 \leq j \leq 2(m-1-i)}} b_{l,i,j} \cdot w_l^{\mathbb{D}_4}(T_1) \cdot w_i^{W'}(T') \cdot \widetilde{w}_j^{W'}(T').$$

For any $1 \leq i \leq m-1$, $w_i^{W'}(T') = 0$ and $w_1^{\mathbb{D}_4}(T_1) = 0$, so we have :

$$a_k(T_1 \times T') = \sum_{l \in \{0,\widetilde{1},\widetilde{2}\}, 0 \leq j \leq 2(m-1)} b_{l,0,j} \cdot w_l^{\mathbb{D}_4}(T_1) \cdot \widetilde{w}_j^{W'}(T').$$

Let us embed H_0 in $W_0 = \mathbb{D}_4 \times W'$. Then H_0 decomposes in this product in two factors, the left one being isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2$ and denoted by $H_0^{\mathbb{D}_4}$ and the right factor being an abelian subgroup of W' generated by reflections. We denote it by H_0'. Note that H_0' is for W' exactly what H_0 is for W. Lemma 4.3 applies here for W' and H_0' :

$$\mathsf{Res}_{W'}^{H_0'}(\widetilde{w}_j^{W'}) = a_j^{(0)} = \sum_{J \subset \{3,\ldots,2m\}, |J|=j} a_J.$$

For any $0 \leq j \leq 2(m-1)$, we have

$$\begin{aligned}\mathsf{Res}_{\mathbb{D}_4}^{H_0^{\mathbb{D}_4}}(\widetilde{w}_1^{\mathbb{D}_4}) \cdot \mathsf{Res}_{W'}^{H_0'}(\widetilde{w}_j^{W'}) &= \big(a_{\{1\}} + a_{\{2\}}\big) \cdot \Big(\sum_{J \subset \{3,\ldots,2m\}, |J|=j} a_J\Big) \\ &= \sum_{J \subset \{3,\ldots,2m\}, |J|=j} \big(a_{\{1\}\cdot J} + a_{\{2\}\cdot J}\big)\end{aligned}$$

and

$$\begin{aligned}\mathsf{Res}_{\mathbb{D}_4}^{H_0^{\mathbb{D}_4}}(\widetilde{w}_2^{\mathbb{D}_4}) \cdot \mathsf{Res}_{W'}^{H_0'}(\widetilde{w}_j^{W'}) &= a_{\{1,2\}} \cdot \Big(\sum_{J \subset \{3,\ldots,2m\}, |J|=j} a_J\Big) \\ &= \sum_{J \subset \{3,\ldots,2m\}, |J|=j} a_{\{1,2\}\cdot J}.\end{aligned}$$

Let us come back to $\mathsf{Res}_W^{H_0}(a)$. We get that

$$\begin{aligned}\mathsf{Res}_W^{H_0}(a) = \sum_{0 \leq j \leq 2(m-1)} \Big[& b_{0,0,j} \cdot \Big(\sum_{J \subset \{3,\ldots,2m\}, |J|=j} a_J\Big) \\ & + b_{\widetilde{1},0,j} \cdot \Big(\sum_{J \subset \{3,\ldots,2m\}, |J|=j} (a_{J\cdot\{1\}} + a_{J\cdot\{2\}})\Big) \\ & + b_{\widetilde{2},0,j} \cdot \Big(\sum_{J \subset \{3,\ldots,2m\}, |J|=j} a_{J\cdot\{1,2\}}\Big)\Big].\end{aligned}$$

Moreover, $\mathsf{Res}_W^{H_0}(a)$ belongs to the submodule of the cohomological invariants of H_0 fixed by the group N_0/H_0. By Proposition 2.6, for any $i = 0, ..., 2m$, there exists $b_i \in H^*(k_0, \mathbb{Z}/2\mathbb{Z})$ such that

$$\mathsf{Res}_W^{H_0}(a) = \sum_{i=0}^{2m} b_i \cdot a_i^{(0)},$$

where, for $i = 0, ..., 2m$, $a_i^{(0)} = \sum_{I \subset \{1,...,2m\}, |I|=i} a_I$.

Furthermore, the family $(a_I)_{I\subset\{1,...,2m\}}$ is free in $\mathsf{Inv}_{k_0}(H_0, \mathbb{Z}/2\mathbb{Z})$ (see Proposition 2.1), so we get the following relations : for any $0 \leq j \leq 2(m-1)$,

$$b_{0,0,j} = b_j,\ b_{\widetilde{1},0,j} = b_{j+1} \text{ and } b_{\widetilde{2},0,j} = b_{j+2}.$$

We can now say that

$$\begin{aligned} b_{0,0,1} &= b_{\widetilde{1},0,0}, \\ \text{for any } j \geq 2, b_{0,0,j} &= b_{\widetilde{1},0,j-1} = b_{\widetilde{2},0,j-2} \text{ and} \\ b_{\widetilde{1},0,2m-2} &= b_{\widetilde{2},0,2m-3}. \end{aligned} \tag{4.4}$$

If we set $a_0' = \mathsf{Res}_W^{W_0}(a) + a_1$ (it is a cohomological invariant of W_0), then

$$\begin{aligned} a_0' &= \sum_{l\in\{0,\widetilde{1},\widetilde{2}\}, 0\leq j\leq 2(m-1)} b_{l,0,j} \cdot w_l^{\mathbb{D}_4} \cdot \widetilde{w}_j^{W'} \\ &= b_{0,0,0} + b_{0,0,1} \cdot \widetilde{w}_1^{W'} + b_{\widetilde{1},0,0} \cdot \widetilde{w}_1^{\mathbb{D}_4} \\ &\quad + \sum_{j=2}^{2m-2} \left(b_{0,0,j} \cdot \widetilde{w}_j^{W'} + b_{\widetilde{1},0,j-1} \cdot \widetilde{w}_1^{\mathbb{D}_4} \cdot \widetilde{w}_{j-1}^{W'} + b_{\widetilde{2},0,j} \cdot \widetilde{w}_2^{\mathbb{D}_4} \cdot \widetilde{w}_{j-2}^{W'} \right) \\ &\quad + b_{\widetilde{1},0,2m-2} \cdot \widetilde{w}_1^{\mathbb{D}_4} \cdot \widetilde{w}_{2m-2}^{W'} + b_{\widetilde{2},0,2m-3} \cdot \widetilde{w}_2^{\mathbb{D}_4} \cdot \widetilde{w}_{2m-3}^{W'} \\ &\quad + b_{\widetilde{2},0,2m-2} \cdot \widetilde{w}_2^{\mathbb{D}_4} \cdot \widetilde{w}_{2m-2}^{W'}. \end{aligned}$$

Therefore, using Relations (4.4), we get :

$$\begin{aligned} a_0' =& b_{0,0,0} + b_{0,0,1} \cdot \left(\widetilde{w}_1^{W'} + \widetilde{w}_1^{\mathbb{D}_4} \right) \\ &+ \sum_{j=2}^{2m-2} b_{0,0,j} \cdot \left(\widetilde{w}_j^{W'} + \widetilde{w}_1^{\mathbb{D}_4} \cdot \widetilde{w}_{j-1}^{W'} + \widetilde{w}_2^{\mathbb{D}_4} \cdot \widetilde{w}_{j-2}^{W'} \right) \\ &+ b_{\widetilde{1},0,2m-2} \cdot \left(\widetilde{w}_1^{\mathbb{D}_4} \cdot \widetilde{w}_{2m-2}^{W'} + \widetilde{w}_2^{\mathbb{D}_4} \cdot \widetilde{w}_{2m-3}^{W'} \right) \\ &+ b_{\widetilde{2},0,2m-2} \cdot \widetilde{w}_2^{\mathbb{D}_4} \cdot \widetilde{w}_{2m-2}^{W'}. \end{aligned}$$

By Lemma 4.3, for $0 \leq j \leq 2m$,

$$\mathsf{Res}_W^{W_0}(\widetilde{w}_j) = \widetilde{w}_2^{\mathbb{D}_4} \cdot \widetilde{w}_{j-2}^{W'} + \widetilde{w}_1^{\mathbb{D}_4} \cdot \widetilde{w}_{j-1}^{W'} + \widetilde{w}_j^{W'},$$

thus :

$$\begin{aligned} a_0' =& b_{0,0,0} \cdot \mathsf{Res}_W^{W_0}(\widetilde{w}_0) + b_{0,0,1} \cdot \mathsf{Res}_W^{W_0}(\widetilde{w}_1) + \sum_{j=2}^{2m-2} b_{0,0,j} \cdot \mathsf{Res}_W^{W_0}(\widetilde{w}_j) \\ &+ b_{\widetilde{1},0,2m-2} \cdot \mathsf{Res}_W^{W_0}(\widetilde{w}_{2m-1}) + b_{\widetilde{2},0,2m-2} \cdot \mathsf{Res}_W^{W_0}(\widetilde{w}_{2m}) \\ =& \sum_{j=0}^{2m-2} b_{0,0,j} \cdot \mathsf{Res}_W^{W_0}(\widetilde{w}_j) + b_{\widetilde{1},0,2m-2} \cdot \mathsf{Res}_W^{W_0}(\widetilde{w}_{2m-1}) \\ &+ b_{\widetilde{2},0,2m-2} \cdot \mathsf{Res}_W^{W_0}(\widetilde{w}_{2m}). \end{aligned}$$

This concludes the case $q = 0$.

Assume now that $1 \leq q \leq m-1$ and that the induction hypothesis is true for the rank $q-1$. By induction hypothesis (see Proposition 4.4), we want to study the extra term a_q. Note that a_q is a cohomological invariant of W_0. Recall that

$$\begin{aligned} a_q = & \sum_{l \in \{0,\widetilde{1},\widetilde{2}\}, q \leq i \leq m-1, 0 \leq j \leq 2(m-1-i)} b_{l,i,j} \cdot w_l^{\mathbb{D}_4} \cdot w_i^{W'} \cdot \widetilde{w}_j^{W'} \\ & + \sum_{q-1 \leq i \leq m-1, 0 \leq j \leq 2(m-1-i)} b_{1,i,j} \cdot w_1^{\mathbb{D}_4} \cdot w_i^{W'} \cdot \widetilde{w}_j^{W'}. \end{aligned}$$

We then have to show that

$$a_q = \sum_{0 \leq j \leq 2(m-q)} C_{q,j} \cdot \mathsf{Res}_W^{W_0}(w_q \cdot \widetilde{w}_j) + a_{q+1},$$

where $C_{q,j} \in H^*(k_0, \mathbb{Z}/2\mathbb{Z})$ for $0 \leq j \leq 2(m-q)$. Let k/k_0 be an extension, let $T_1 = (k^2, (u_1, v_1))$ be a $\mathbb{D}_4$-torsor over k, let $T_2 = (k(\sqrt{t_2}), u_2))$ and let

$$T_3 = (k(\sqrt{t_3}) \times ... \times k(\sqrt{t}_{q+1}) \times k^{2(m-q-1)}, (u_3, ..., u_{q+1}, u_{q+2}, v_{q+2}, ..., u_m, v_m))$$

so that $T_2 \times T_3$ is a W'-torsor over k. Then $T_1 \times (T_2 \times T_3)$ is a W_0-torsor which lies in the image of $H^1(k, H_q) \to H^1(k, W)$. Since $w_i^{W'}(T_2 \times T_3) = w_i(\langle t_2, ..., t_{q+1} \rangle)$, we get that $w_i^{W'}(T_2 \times T_3) = 0$ if $i \geq q+1$. On the other hand, $w_1^{\mathbb{D}_4}(T_1) = 0$. Therefore, we obtain that

$$(a_q)_k(T_1 \times (T_2 \times T_3)) = \sum_{\substack{l \in \{0,\widetilde{1},\widetilde{2}\}, \\ 0 \leq j \leq 2(m-1-q)}} b_{l,q,j} \cdot w_l^{\mathbb{D}_4}(T_1) \cdot w_q^{W'}(T_2 \times T_3) \cdot \widetilde{w}_j^{W'}(T_2 \times T_3). \tag{4.5}$$

Let us now consider the $\mathbb{D}_4$-torsor $T_2 = (k(\sqrt{t_2}), u_2)$ and the W'-torsor

$$T_1 \times T_3 = \big(k^2 \times k(\sqrt{t_3}) \times ... \times k(\sqrt{t}_{q+1}) \times k^{2(m-q-1)}, \\ (u_1, v_1, u_3, ..., u_{q+1}, u_{q+2}, v_{q+2}, ..., u_m, v_m)\big).$$

Then $w_i^{W'}(T_1 \times T_3) = w_i(\langle t_3, ..., t_{q+1}\rangle)$, so if $i \geq q$, $w_i^{W'}(T_1 \times T_3) = 0$. Hence,

$$(a_q)_k(T_2 \times (T_1 \times T_3)) = \sum_{0 \leq j \leq 2(m-q)} b_{1,q-1,j} \cdot w_1^{\mathbb{D}_4}(T_2) \cdot w_{q-1}^{W'}(T_1 \times T_3) \cdot \widetilde{w}_j^{W'}(T_1 \times T_3). \tag{4.6}$$

Since the two W_0-torsors $T_1 \times (T_2 \times T_3)$ and $T_2 \times (T_1 \times T_3)$ are isomorphic, it follows from (4.5) and (4.6) that

$$\begin{aligned} &\sum_{l \in \{0,\widetilde{1},\widetilde{2}\} 0 \leq j \leq 2(m-1-q)} b_{l,q,j} \cdot w_l^{\mathbb{D}_4}(T_1) \cdot w_q^{W'}(T_2 \times T_3) \cdot \widetilde{w}_j^{W'}(T_2 \times T_3) \\ &\quad = \sum_{0 \leq j \leq 2(m-q)} b_{1,q-1,j} \cdot w_1^{\mathbb{D}_4}(T_2) \cdot w_{q-1}^{W'}(T_1 \times T_3) \cdot \widetilde{w}_j^{W'}(T_1 \times T_3). \end{aligned} \tag{4.7}$$

Now set $k_1 = k_0(u_2, ..., u_m, t_2, ..., t_{q+1}, v_{q+2}, ..., v_m)$ and assume that u_1 and v_1 are independent indeterminates over k_1. Then the family $\{1, \widetilde{w}_1^{\mathbb{D}_4}(T_1), \widetilde{w}_2^{\mathbb{D}_4}(T_1)\}$ is free over $H^*(k_1, \mathbb{Z}/2\mathbb{Z})$. We then have to collect classes $w_l^{\mathbb{D}_4}(T_1)$ in (4.7). Denoting in an analogous way to $W' \subset W$, by W'' the "same" subgroup of W',then by Proposition 4.3 and since $w_1^{\mathbb{D}_4}(T_1) = 0$, we get, for any $0 \leq j \leq 2(m-q)$:

$$\begin{aligned} w_{q-1}^{W'}(T_1 \times T_3) \cdot \widetilde{w}_j^{W'}(T_1 \times T_3) = &\widetilde{w}_2^{\mathbb{D}_4}(T_1) \cdot w_{q-1}^{W''}(T_3) \cdot \widetilde{w}_{j-2}^{W''}(T_3) \\ &+ \widetilde{w}_1^{\mathbb{D}_4}(T_1) \cdot w_{q-1}^{W''}(T_3) \cdot \widetilde{w}_{j-1}^{W''}(T_3) \\ &+ w_{q-1}^{W''}(T_3) \cdot \widetilde{w}_j^{W''}(T_3). \end{aligned}$$

Since the family $\{1, \widetilde{w}_1^{\mathbb{D}_4}(T_1), \widetilde{w}_2^{\mathbb{D}_4}(T_1)\}$ is free, we obtain from (4.7) the following equalities : for any $l \in \{0, \widetilde{1}, \widetilde{2}\}$,

$$\begin{aligned} &\sum_{0 \leq j \leq 2(m-1-q)} b_{l,q,j} \cdot w_q^{W'}(T_2 \times T_3) \cdot \widetilde{w}_j^{W'}(T_2 \times T_3) \\ &\quad = \sum_{0 \leq j \leq 2(m-q)} b_{1,q-1,j} \cdot w_1^{\mathbb{D}_4}(T_2) \cdot w_{q-1}^{W''}(T_3) \cdot \widetilde{w}_{j-l}^{W''}(T_3). \end{aligned} \tag{4.8}$$

Now set $k_2 = k_0(u_3, ..., u_m, t_3, ..., t_{q+1}, v_{q+2}, ..., v_m)$ and let t_2, u_2 be independent indeterminates over k_2. Then the family $\{1, \widetilde{w}_1^{\mathbb{D}_4}(T_2), \widetilde{w}_2^{\mathbb{D}_4}(T_2)\}$ is free in $H^*(k_2, \mathbb{Z}/2\mathbb{Z})$ (and $w_1^{\mathbb{D}_4}(T_2) = \widetilde{w}_1^{\mathbb{D}_4}(T_2)$). We then have to collect these terms : since $w_q^{W'}(T_3) = 0$, by Proposition 4.3, for any $0 \leq j \leq 2(m-1-q)$, we have

$$w_q^{W'}(T_2 \times T_3) \cdot \widetilde{w}_j^{W'}(T_2 \times T_3) = w_1^{\mathbb{D}_4}(T_2) \cdot w_{q-1}^{W''}(T_3) \cdot \widetilde{w}_j^{W''}(T_3).$$

Hence, for any $l \in \{0, \widetilde{1}, \widetilde{2}\}$, we get from (4.8) that

$$\begin{aligned} &\sum_{0 \leq j \leq 2(m-1-q)} b_{l,q,j} \cdot w_{q-1}^{W''}(T_3) \cdot \widetilde{w}_j^{W''}(T_3) \\ &\qquad = \sum_{0 \leq j \leq 2(m-q)} b_{1,q-1,j} \cdot w_{q-1}^{W''}(T_3) \cdot \widetilde{w}_{j-l}^{W''}(T_3). \end{aligned}$$

We have the three following equalities:
for $l = 0$:

$$\begin{aligned} 0 = & \sum_{0\leq j\leq 2(m-1-q)} \left(b_{0,q,j} + b_{1,q-1,j}\right) \cdot w_{q-1}^{W''}(T_3) \cdot \widetilde{w}_j^{W''}(T_3) \\ & + b_{0,q-1,2(m-q)-1} \cdot w_{q-1}^{W''}(T_3) \cdot \widetilde{w}_{2(m-q)-1}^{W''}(T_3) \\ & + b_{0,q-1,2(m-q)} \cdot w_{q-1}^{W''}(T_3) \cdot \widetilde{w}_{2(m-q)}^{W''}(T_3); \end{aligned} \tag{4.9}$$

for $l = \widetilde{1}$:

$$\begin{aligned} 0 = & \sum_{0\leq j\leq 2(m-1-q)} \left(b_{\widetilde{1},q,j} + b_{1,q-1,j+1}\right) \cdot w_{q-1}^{W''}(T_3) \cdot \widetilde{w}_j^{W''}(T_3) \\ & + b_{1,q-1,2(m-q)} \cdot w_{q-1}^{W''}(T_3) \cdot \widetilde{w}_{2(m-q)-1}^{W''}(T_3); \end{aligned} \tag{4.10}$$

for $l = \widetilde{2}$:

$$0 = \sum_{0\leq j\leq 2(m-1-q)} \left(b_{\widetilde{2},q,j} + b_{1,q-1,j+2}\right) \cdot w_{q-1}^{W''}(T_3) \cdot \widetilde{w}_j^{W''}(T_3). \tag{4.11}$$

We now apply Lemma 4.4 replacing W by W'' and q by $q-1$:

$$w_{q-1}^{W''} \cdot \widetilde{w}_j^{W''} = 0 \text{ if } j > 2(m-2-(q-1)) = 2(m-q)-2.$$

Therefore,

$$w_{q-1}^{W''}(T_3) \cdot \widetilde{w}_{2(m-q)-1}^{W''}(T_3) = 0 = w_{q-1}^{W''}(T_3) \cdot \widetilde{w}_{2(m-q)}^{W''}(T_3).$$

Thus Relations (4.9), (4.10) and (4.11) become :
for $l = 0$:

$$\sum_{0\leq j\leq 2(m-1-q)} \left(b_{0,q,j} + b_{1,q-1,j}\right) \cdot w_{q-1}^{W''}(T_3) \cdot \widetilde{w}_j^{W''}(T_3) = 0; \tag{4.12}$$

for $l = \widetilde{1}$:

$$\sum_{0\leq j\leq 2(m-1-q)} \left(b_{\widetilde{1},q,j} + b_{1,q-1,j+1}\right) \cdot w_{q-1}^{W''}(T_3) \cdot \widetilde{w}_j^{W''}(T_3) = 0; \tag{4.13}$$

for $l = \widetilde{2}$:

$$\sum_{0\leq j\leq 2(m-1-q)} \left(b_{\widetilde{2},q,j} + b_{1,q-1,j+2}\right) \cdot w_{q-1}^{W''}(T_3) \cdot \widetilde{w}_j^{W''}(T_3) = 0. \tag{4.14}$$

Assume now that $t_3, ..., t_{q+1}, u_3, ..., u_m, v_{q+2}, ..., v_m$ are independent indeterminates over k_0. Let us denote by H_q'' the subgroup of W'', defined likely to $H_q \subset W$.

Then, replacing W by W'' and q by $q-1$, Lemma 4.5 implies that the invariants $\mathsf{Res}^{H''_q}_{W''}(w^{W''}_{q-1}\cdot\widetilde{w}^{W''}_j)$ (with $0\leq j\leq 2(m-1-q)$) form a free family over $H^*(k_0,\mathbb{Z}/2\mathbb{Z})$. Since T_3 is clearly the image of a versal torsor of H''_q, we get as a direct consequence of Theorem 1.7 that, for $0\leq j\leq 2(m-1-q)$, the invariants $w^{W''}_{q-1}(T_3)\cdot\widetilde{w}^{W''}_j(T_3)$ form a free family over $H^*(k_0,\mathbb{Z}/2\mathbb{Z})$. It then follows from (4.12), (4.13) and (4.14) that, for any $l\in\{0,1,2\}$ and any $j\in\{0,...,2(m-1-q)\}$,

$$b_{\widetilde{l},q,j}+b_{1,q-1,j+l}=0. \tag{4.15}$$

Reordering equalities (4.15), we get that, for any $2\leq j\leq 2(m-1-q)$:

$$\begin{aligned}
b_{0,q,0} =& b_{1,q-1,0},\\
b_{0,q,1} =& b_{\widetilde{1},q,0}=b_{1,q-1,1},\\
b_{\widetilde{2},q,j-2}=b_{\widetilde{1},q,j-1} =& b_{0,q,j}=b_{1,q-1,j},\\
b_{\widetilde{2},q,2(m-1-q)-1} =& b_{\widetilde{1},q,2(m-1-q)}=b_{1,q-1,2(m-q)-1},\\
b_{\widetilde{2},q,2(m-1-q)} =& b_{1,q-1,2(m-q)-1}.
\end{aligned} \tag{4.16}$$

Let us now come back to a_q :

$$\begin{aligned}
a_q = &\sum_{l\in\{0,\widetilde{1},\widetilde{2}\},q\leq i\leq m-1,0\leq j\leq 2(m-1-i)} b_{l,i,j}\cdot w_l^{\mathbb{D}_4}\cdot w_i^{W'}\cdot\widetilde{w}_j^{W'}\\
&+\sum_{q-1\leq i\leq m-1,0\leq j\leq 2(m-1-i)} b_{1,i,j}\cdot w_1^{\mathbb{D}_4}\cdot w_i^{W'}\cdot\widetilde{w}_j^{W'},
\end{aligned}$$

so :

$$\begin{aligned}
a_q = &\sum_{l\in\{0,\widetilde{1},\widetilde{2}\},0\leq j\leq 2(m-1-q)} b_{l,q,j}\cdot w_l^{\mathbb{D}_4}\cdot w_q^{W'}\cdot\widetilde{w}_j^{W'}\\
&+\sum_{0\leq j\leq 2(m-q)} b_{1,q-1,j}\cdot w_1^{\mathbb{D}_4}\cdot w_{q-1}^{W'}\cdot\widetilde{w}_j^{W'} \qquad +a_{q+1}.
\end{aligned}$$

Set $a'_q=a_q+a_{q+1}$. Using relations (4.16), we have :

$$\begin{aligned}
a'_q = & b_{1,q-1,0}\cdot\left(w_q^{W'}+w_1^{\mathbb{D}_4}\cdot w_{q-1}^{W'}\right)\\
&+b_{1,q-1,1}\cdot\left(\widetilde{w}_1^{\mathbb{D}_4}\cdot w_q^{W'}+w_1^{\mathbb{D}_4}\cdot w_{q-1}^{W'}\cdot\widetilde{w}_1^{W'}+w_q^{W'}\cdot\widetilde{w}_1^{W'}\right)\\
&+\sum_{2\leq j\leq 2(m-1-q)} b_{1,q-1,j}\cdot\left(\widetilde{w}_2^{\mathbb{D}_4}\cdot w_q^{W'}\cdot\widetilde{w}_{j-2}^{W'}+\widetilde{w}_1^{\mathbb{D}_4}\cdot w_q^{W'}\cdot\widetilde{w}_{j-1}^{W'}\right.\\
&\qquad\qquad\left.+w_1^{\mathbb{D}_4}\cdot w_{q-1}^{W'}\cdot\widetilde{w}_j^{W'}+w_q^{W'}\cdot\widetilde{w}_j^{W'}\right)\\
&+b_{1,q-1,2(m-q)-1}\cdot\left(\widetilde{w}_2^{\mathbb{D}_4}\cdot w_q^{W'}\cdot\widetilde{w}_{2(m-1-q)-1}^{W'}+\right.\\
&\qquad\left.\widetilde{w}_1^{\mathbb{D}_4}\cdot w_q^{W'}\cdot\widetilde{w}_{2(m-1-q)}^{W'}+w_1^{\mathbb{D}_4}\cdot w_{q-1}^{W'}\cdot\widetilde{w}_{2(m-q)-1}^{W'}\right)\\
&+b_{1,q-1,2(m-q)}\cdot\left(\widetilde{w}_2^{\mathbb{D}_4}\cdot w_q^{W'}\cdot\widetilde{w}_{2(m-1-q)}^{W'}+w_1^{\mathbb{D}_4}\cdot w_{q-1}^{W'}\cdot\widetilde{w}_{2(m-q)}^{W'}\right).
\end{aligned} \tag{4.17}$$

Recall now the formulae of Proposition 4.3. For any $2 \leq j \leq 2(m-1-q)$,

$$w_q = w_q^{W'} + w_1^{\mathbb{D}_4} \cdot w_{q-1}^{W'}, \tag{4.18}$$

$$w_q \cdot \widetilde{w}_1 = \widetilde{w}_1^{\mathbb{D}_4} \cdot w_q^{W'} + w_1^{\mathbb{D}_4} \cdot w_{q-1}^{W'} \cdot \widetilde{w}_1^{W'} + w_q^{W'} \cdot \widetilde{w}_1^{W'}, \tag{4.19}$$

$$\begin{aligned} w_q \cdot \widetilde{w}_j =& \widetilde{w}_2^{\mathbb{D}_4} \cdot w_q^{W'} \cdot \widetilde{w}_{j-2}^{W'} + \widetilde{w}_1^{\mathbb{D}_4} \cdot w_q^{W'} \cdot \widetilde{w}_{j-1}^{W'} + w_1^{\mathbb{D}_4} \cdot w_{q-1}^{W'} \cdot \widetilde{w}_j^{W'} \\ &+ w_q^{W'} \cdot \widetilde{w}_j^{W'}, \end{aligned} \tag{4.20}$$

$$\begin{aligned} w_q \cdot \widetilde{w}_{2(m-q)-1} =& \widetilde{w}_2^{\mathbb{D}_4} \cdot w_q^{W'} \cdot \widetilde{w}_{2(m-1-q)-1}^{W'} + \widetilde{w}_1^{\mathbb{D}_4} \cdot w_q^{W'} \cdot \widetilde{w}_{2(m-1-q)}^{W'} \\ &+ w_1^{\mathbb{D}_4} \cdot w_{q-1}^{W'} \cdot \widetilde{w}_{2(m-q)}^{W'} \end{aligned} \tag{4.21}$$

and

$$w_q \cdot \widetilde{w}_{2(m-q)} = \widetilde{w}_2^{\mathbb{D}_4} \cdot w_q^{W'} \cdot \widetilde{w}_{2(m-1-q)}^{W'} + w_1^{\mathbb{D}_4} \cdot w_{q-1}^{W'} \cdot \widetilde{w}_j^{W'}. \tag{4.22}$$

Note that we used Lemma 4.4 : $w_q^{W'} \cdot \widetilde{w}_{2(m-q)-1}^{W'} = 0$ and $w_q^{W'} \cdot \widetilde{w}_{2(m-q)}^{W'} = 0$. Therefore, using relations (4.18) to (4.22) in relation (4.17), we get that

$$\begin{aligned} a'_q = & \, b_{1,q-1,0} \cdot \mathsf{Res}_W^{W_0}(w_q) + b_{1,q-1,1} \cdot \mathsf{Res}_W^{W_0}(w_q \cdot \widetilde{w}_1) \\ &+ \sum_{2 \leq j \leq 2(m-1-q)} b_{1,q-1,j} \cdot \mathsf{Res}_W^{W_0}(w_q \cdot \widetilde{w}_j) \\ &+ b_{1,q-1,2(m-q)-1} \cdot \mathsf{Res}_W^{W_0}(w_q \cdot \widetilde{w}_{2(m-q)-1}) \\ &+ b_{1,q-1,2(m-q)} \cdot \mathsf{Res}_W^{W_0}(w_q \cdot \widetilde{w}_{2(m-q)}), \end{aligned} \tag{4.23}$$

which yields :

$$a'_q = \sum_{0 \leq j \leq 2(m-q)} b_{1,q-1,j} \cdot \mathsf{Res}_W^{W_0}(w_q \cdot \widetilde{w}_j). \tag{4.24}$$

This ends the induction and the proof of Proposition 4.4. ■

We eventually get that there exist some coefficients $C_{i,j} \in H^*(k_0, \mathbb{Z}/2\mathbb{Z})$ such that

$$\mathsf{Res}_W^{W_0}(a) = \sum_{0 \leq i \leq m-1, 0 \leq j \leq 2(m-i)} C_{i,j} \cdot \mathsf{Res}_W^{W_0}(w_i \cdot \widetilde{w}_j) + a_m$$

where

$$a_m = \sum_{m-1 \leq i \leq m-1, 0 \leq j \leq 2(m-1-i)} b_{1,i,j} \cdot w_1^{\mathbb{D}_4} \cdot w_i^{W'} \cdot \widetilde{w}_j^{W'} = b_{1,m-1,0} \cdot w_1^{\mathbb{D}_4} \cdot w_{m-1}^{W'}.$$

By Proposition 4.3, $\mathsf{Res}_W^{W_0}(w_m) = w_m^{W'} + w_1^{\mathbb{D}_4} \cdot w_{m-1}^{W'}$ and $w_m^{W'} = 0$. Hence, $\mathsf{Res}_W^{W_0}(a)$ is a linear combination of the invariants $\mathsf{Res}_W^{W_0}(w_i \cdot \widetilde{w}_j)$ of W_0, for $0 \leq i \leq m$ and

$0 \leq j \leq 2(m-i)$. Since the restriction to W_0 completely determines the invariant a, we get that a is a linear combination of the invariants $w_i \cdot \widetilde{w}_j$ of W, $0 \leq i \leq m$, $0 \leq j \leq 2(m-i)$. Therefore, for $0 \leq i \leq m, 0 \leq j \leq 2(m-i)$, the invariants $w_i \cdot \widetilde{w}_j$ of W generate the module $\mathsf{Inv}_{k_0}(W, \mathbb{Z}/2\mathbb{Z})$. This ends the proof of Proposition 4.2.

4.2.4 A basis of $\mathsf{Inv}_{k_0}(W, \mathbb{Z}/2\mathbb{Z})$

Note that any result of this section is still true if we do not assume that $-1, 2 \in k_0^{\times 2}$.

Theorem 4.2. *The family $\{w_i \cdot \widetilde{w}_j\}_{0 \leq i \leq m, 0 \leq j \leq 2(m-i)}$ is free over $H^*(k_0, \mathbb{Z}/2\mathbb{Z})$.*

Proof. Let $\{\lambda_{i,j}\}_{0 \leq i \leq m, 0 \leq j \leq 2(m-i)}$ be a family of coefficients of $H^*(k_0, \mathbb{Z}/2\mathbb{Z})$ such that

$$a = \sum_{0 \leq i \leq m, 0 \leq j \leq 2(m-i)} \lambda_{i,j} \cdot w_i \cdot \widetilde{w}_j = 0.$$

Let us show by induction on $q \in \{0, ..., m\}$, that, for any $q \in \{0, ..., m\}$, $\lambda_{q,j} = 0$ for any $j \in \{0, ..., 2(m-i)\}$.

Assume first that $q = 0$. Let us consider the restriction of a to H_0. We have to show that, for any $0 \leq j \leq 2m$, $\lambda_{0,j} = 0$. By Lemma 4.2, for any extension k/k_0, for any W-torsor T_0 over k lying in the image of the map $H^1(k, H_0) \to H^1(k, W)$ and for any $i > 0$, we have $w_i(T_0) = 0$. Thus,

$$a_k(T_0) = \sum_{0 \leq j \leq 2m} \lambda_{0,j} \cdot \widetilde{w}_j(T_0).$$

By Lemma 4.3, the family $\{\mathsf{Res}^{H_0}_W(\widetilde{w}_j)\}_{0 \leq j \leq 2m}$ is free in the $H^*(k_0, \mathbb{Z}/2\mathbb{Z})$-module of the invariants of H_0 modulo 2. Therefore, we get that $\lambda_{0,j} = 0$ for any $0 \leq j \leq 2m$.

Let now $0 < q \leq m$. Let us assume that, for any $0 \leq i < q$, $\lambda_{i,j} = 0$ for any $0 \leq j \leq 2(m-i)$. Hence,

$$a = \sum_{q \leq i \leq m, 0 \leq j \leq 2(m-i)} \lambda_{i,j} \cdot w_i \cdot \widetilde{w}_j.$$

Let us now consider the restriction $\mathsf{Res}^{H_q}_W(a)$ of a to H_q. Let k/k_0 be an extension and let $T_q = (k(\sqrt{t_1}) \times ... \times k(\sqrt{t_q}) \times k^{2(m-q)}, (u_1, ..., u_q, u_{q+1}, v_{q+1}, ..., u_m, v_m))$ be a W-torsor over k lying in the image of $H^1(k, H_q) \to H^1(k, W)$. By Lemma 4.2, if $i \geq q+1$, $w_i(T_q) = 0$. Thus,

$$a_k(T_q) = \sum_{0 \leq j \leq 2(m-q)} \lambda_{q,j} \cdot w_q(T_q) \cdot \widetilde{w}_j(T_q).$$

Therefore, $\mathsf{Res}_W^{H_q}(a) = \sum_{0\leq j\leq 2(m-q)} \lambda_{q,j} \cdot \mathsf{Res}_W^{H_q}(w_q \cdot \widetilde{w}_j)$. By Lemma 4.5, the family $\{\mathsf{Res}_W^{H_q}(w_q \cdot \widetilde{w}_j)\}_{0\leq j\leq 2(m-q)}$ is free over $H^*(k_0, \mathbb{Z}/2\mathbb{Z})$. We can conclude that $\lambda_{q,j} = 0$ for every $0 \leq j \leq 2(m-q)$. This ends the induction. ■

4.3 Proof of Theorem 4.1 : the case n odd

In this section we just sketch the proof of Theorem 4.1 with n odd. Let us recall the statement.

Theorem. *Let k_0 be a field of characteristic zero, such that -1 and 2 are squares in k_0. Let $m \geq 1$ and let W be a Weyl group of type B_{2m+1}. Then the module $\mathsf{Inv}_{k_0}(W, \mathbb{Z}/2\mathbb{Z})$ is free over $H^*(k_0, \mathbb{Z}/2\mathbb{Z})$, with basis*

$$\{w_i \cdot \widetilde{w}_j\}_{0\leq i\leq m, 0\leq j\leq 2(m-i)}.$$

Let W be a Weyl group of type B_{2m+1}. Let

$$S = \{\pm e_i, \pm e_i \pm e_j, 1 \leq i \leq 2m+1, 1 \leq j \neq i \leq 2m+1\}$$

be the root system corresponding to W. Let

$$S_0 = \{\pm e_i, \pm e_i \pm e_j, 1 \leq i \leq 2m, 1 \leq j \neq i \leq 2m\} \sqcup \{\pm e_{2m+1}\}.$$

Then the reflections associated with S_0 generate a subgroup W_0 of W, isomorphic to $W' \times \langle r_{e_{2m+1}} \rangle$, where W' is a Weyl group of type B_{2m}. Let $a \in \mathsf{Inv}_{k_0}(W, \mathbb{Z}/2\mathbb{Z})$. Mimicking the proof of the case B_{2m}, we may show that $\mathsf{Res}_W^{W_0}(a)$ completely determines a. Then we write $\mathsf{Res}_W^{W_0}(a)$ as cup-products of invariants of W' and of $\mathbb{Z}/2\mathbb{Z}$. Looking at the restrictions to the subgroups H_q as in the case B_{2m}, we finally get the result. Note that computations are much easier here because of the factor $\mathbb{Z}/2\mathbb{Z}$ instead of $\mathbb{D}_4$.

Chapter 5

Cohomological invariants of the Weyl group of type D_n, $n \geq 4$

RÉSUMÉ

Dans ce chapitre, on s'intéresse aux groupes de Weyl de type D. Un tel groupe se réalisant comme sous-groupe d'un groupe de Weyl de type B, on peut définir par restriction les deux familles d'invariants de Stiefel-Whitney. L'objectif de ce chapitre est d'établir et de prouver à l'aide du principe d'annulation du chapitre 3 un résultat analogue à celui du chapitre précédent afin de déterminer complètement les invariants cohomologiques des groupes de Weyl de type D.

Let $n \geq 4$, W be a Weyl group of type D_n. We associate to W its root system $S = \{\pm e_i \pm e_j \mid 1 \leq i < j \leq n\}$ (see Appendix A for more details).

Let us denote W' the Weyl group of type B_n corresponding to the root system

$$S' = \{\pm e_i, \pm(e_i \pm e_j) \mid, 1 \leq i \leq n, 1 \leq j \neq i \leq n\}.$$

We clearly have an inclusion $W \subset W'$.

Let k be a field of characteristic zero. As we saw in Proposition 1.8, the pointed set $H^1(k, W')$ is in bijection with the set of isomorphism classes of pairs (L, α) where L is étale of rank n and α a class of squares in L^*. Furthermore, Proposition 1.9 states that the image of the map $H^1(k, W) \to H^1(k, W')$ corresponds to pairs (L, α) such that α has norm 1 in L.

Moreover, we can easily construct some Stiefel-Whitney invariants, from Stiefel-Whitney invariants of W' simply by taking the restriction. We then set for any $0 \leq i \leq [\frac{n}{2}]$, $w_i = \mathsf{Res}^W_{W'}(w_i)$ and for any $0 \leq i \leq n$, $\widetilde{w}_i = \mathsf{Res}^W_{W'}(\widetilde{w}_i)$.

Let us now state the structure theorem for cohomological invariants of W.

Theorem 5.1. *The $H^*(k_0, \mathbb{Z}/2\mathbb{Z})$-module $\mathsf{Inv}_{k_0}(W, \mathbb{Z}/2\mathbb{Z})$ is free with basis given by $w_i \cdot \widetilde{w}_j$, where $0 \leq i \leq [\frac{n}{2}]$, $0 \leq j \leq 2([\frac{n}{2}] - i)$ and j even.*

5.1 The vanishing principle

Consider now $S_0 = \{\pm e_{2i-1} \pm e_{2i} \mid 1 \leq i \leq [\frac{n}{2}]\}$. It is a root subsystem of S. The associated reflections generate a subgroup H of W.

Note that any maximal abelian subgroup of W generated by reflections is conjugated with H. The vanishing theorem for cohomological invariants of Coxeter groups may be written in the following form.

Theorem 5.2. *Let k_0 be any field of characteristic zero. The restriction map $\mathsf{Res}^H_W : \mathsf{Inv}_{k_0}(W, C) \to \mathsf{Inv}_{k_0}(H, \mathbb{Z}/2\mathbb{Z})$ is injective.*

Moreover, the image of this map is contained in $\mathsf{Inv}_{k_0}(H, C)^{N_H/H}$, where N_H denotes the normalizer of H in W (see Proposition 2.3). Let us define some cohomological invariants of H belonging to this submodule. For any field k of characteristic zero and any square-classes $x_1, ..., x_n \in k^*/k^{*2}$, we set

$$a_{r,s}(x_1, ..., x_n) = \sum_{1 \leq m_1 < ... < m_r \leq n-1 \text{ odd numbers}} (x_{m_1}) \cdot (x_{m_1+1}) \cdot \dots \cdot (x_{m_r}) \cdot (x_{m_r+1}) \cdot \Big(\sum_{\mathbf{l} \in I_s \atop \mathbf{l} \cap \{m_1, m_1+1, ..., m_r, m_r+1\} = \emptyset} (x)_{\mathbf{l}} \Big)$$

where

$$I_s = \{\{l_1, ..., l_s\} \in \mathbb{N}^s \mid 1 \leq l_1 < ... < l_s \leq n \text{ and } \forall 0 \leq m \leq \frac{n}{2}, \{2m-1, 2m\} \not\subset \{l_1, ..., l_s\}\}.$$

Recall that we used the notation $(x)_{\mathbf{l}} = (x_{l_1}) \cdot \dots \cdot (x_{l_s})$, with $\mathbf{l} = \{l_1, ..., l_s\}$.

This definition yields some cohomological invariants $a_{r,s} \in \mathsf{Inv}_{k_0}(H, \mathbb{Z}/2\mathbb{Z})$ for any $0 \leq r, s$ and $r + s \leq \frac{n}{2}$.

Lemma 5.1. *The $H^*(k_0, \mathbb{Z}/2\mathbb{Z})$-module $\mathsf{Inv}_{k_0}(H, \mathbb{Z}/2\mathbb{Z})^{N_H/H}$ is free with basis given by the invariants $a_{r,s}$, for $0, \leq r, s$ and $r + s \leq \frac{n}{2}$.*

Proof. If n is even, then $H \subset W(D_n) \subset W(D_{n+1})$ and the normalizers $N_H(W(D_n))$ and $N_H(W(D_{n+1}))$ are equal. We then may assume n even. Let us first prove that the family $\{a_{r,s}\}_{0 \leq r,s; r+s \leq \frac{n}{2}}$ is free over $H^*(k_0, \mathbb{Z}/2\mathbb{Z})$. Note that, for any $0 \leq r, s$ such that $r + s \leq \frac{n}{2}$,

$$a_{r,s} = \sum_{\substack{I \subset \{1,\dots,n\} \\ |I| = 2r+s \\ I \text{ contains exactly } r \text{ pairs } \{2m-1, 2m\}}} a_I.$$

For any $0 \leq r, s$ such that $r + s \leq \frac{n}{2}$, let $c_{r,s} \in H^*(k_0, \mathbb{Z}/2\mathbb{Z})$ such that

$$\sum_{r,s} c_{r,s} \cdot a_{r,s} = 0.$$

Then,

$$\sum_{r,s} c_{r,s} \cdot \big(\sum_I a_I\big) = 0.$$

Since each subset I appearing in the decomposition of some $a_{r,s}$ does not appear in the decomposition of another $a_{r',s'}$ and since the family $\{a_I\}_{I \subset \{1,\dots,n\}}$ is free (see Proposition 2.1), we get that $c_{r,s} = 0$ for any $0 \leq r, s$ such that $r + s \leq \frac{n}{2}$. Therefore, the family $\{a_{r,s}\}_{0 \leq r,s; r+s \leq \frac{n}{2}}$ is free over $H^*(k_0, \mathbb{Z}/2\mathbb{Z})$.

Let us now prove that, for any $r, s \geq 0$ such that $r + s \leq \frac{n}{2}$, $a_{r,s}$ belongs to $M = \mathsf{Inv}_{k_0}(H, \mathbb{Z}/2\mathbb{Z})^{N_H/H}$ and that the family $\{a_{r,s}\}_{0 \leq r,s; r+s \leq \frac{n}{2}}$ generates the $H^*(k_0, \mathbb{Z}/2\mathbb{Z})$-module M. For sake of simplicity, let us show it for $n = 4$. In this case, the subgroup H is associated with the root subsystem $\{\pm e_1 \pm e_2, \pm e_3 \pm e_4\}$.

Set

$$\begin{aligned}
w_{(12)} &: e_1 + e_2 \mapsto e_1 - e_2; \quad e_1 - e_2 \mapsto e_1 + e_2; \quad e_3 + e_4 \mapsto e_3 + e_4; \\
&\quad e_3 - e_4 \mapsto e_3 - e_4; \\
w_{(34)} &: e_1 + e_2 \mapsto e_1 + e_2; \quad e_1 - e_2 \mapsto e_1 - e_2; \quad e_3 + e_4 \mapsto e_3 - e_4; \\
&\quad e_3 - e_4 \mapsto e_3 + e_4 \\
w_{(12)(34)} &: e_1 + e_2 \mapsto e_1 - e_2; \quad e_1 - e_2 \mapsto e_1 + e_2; \quad e_3 + e_4 \mapsto e_3 - e_4; \\
&\quad e_3 - e_4 \mapsto e_3 + e_4 \\
w^{\leftrightarrow} &: e_1 + e_2 \mapsto e_3 + e_4; \quad e_1 - e_2 \mapsto e_3 - e_4; \quad e_3 + e_4 \mapsto e_1 + e_2; \\
&\quad e_3 - e_4 \mapsto e_1 - e_2 \\
w^{\leftrightarrow}_{(12)} &: e_1 + e_2 \mapsto e_3 - e_4; \quad e_1 - e_2 \mapsto e_3 + e_4; \quad e_3 + e_4 \mapsto e_1 + e_2; \\
&\quad e_3 - e_4 \mapsto e_1 - e_2
\end{aligned}$$

$$
\begin{aligned}
w_{(34)}^{\leftrightarrow} :& e_1 + e_2 \mapsto e_3 + e_4; \quad e_1 - e_2 \mapsto e_3 - e_4; \quad e_3 + e_4 \mapsto e_1 - e_2; \\
& e_3 - e_4 \mapsto e_1 + e_2 \\
w_{(12)(34)}^{\leftrightarrow} :& e_1 + e_2 \mapsto e_3 - e_4; \quad e_1 - e_2 \mapsto e_3 + e_4; \quad e_3 + e_4 \mapsto e_1 - e_2; \\
& e_3 - e_4 \mapsto e_1 + e_2.
\end{aligned}
$$

Then

$$N_H/H = \{H, w_{(12)}H, w_{(34)}H, w_{(12)(34)}H, w^{\leftrightarrow}H, w_{(12)}^{\leftrightarrow}H, w_{(34)}^{\leftrightarrow}H, w_{(12)(34)}^{\leftrightarrow}H\}.$$

First note that, for any $0 \leq r, s$ such that $r + s \leq 2$, $a_{r,s}$ belongs to M. Indeed, for instance,

$$
\begin{aligned}
a_{0,1} :& (x_1, x_2, x_3, x_4) \mapsto (x_1) + (x_2) + (x_3) + (x_4) \\
w_{(12)}.a_{0,1} :& (x_1, x_2, x_3, x_4) \mapsto (x_2) + (x_1) + (x_3) + (x_4) \\
w_{(34)}.a_{0,1} :& (x_1, x_2, x_3, x_4) \mapsto (x_1) + (x_2) + (x_4) + (x_3) \\
w_{(12)(34)}.a_{0,1} :& (x_1, x_2, x_3, x_4) \mapsto (x_2) + (x_1) + (x_4) + (x_3) \\
w^{\leftrightarrow}.a_{0,1} :& (x_1, x_2, x_3, x_4) \mapsto (x_3) + (x_4) + (x_1) + (x_2) \\
w_{(12)}^{\leftrightarrow}.a_{0,1} :& (x_1, x_2, x_3, x_4) \mapsto (x_4) + (x_3) + (x_1) + (x_2) \\
w_{(34)}^{\leftrightarrow}.a_{0,1} :& (x_1, x_2, x_3, x_4) \mapsto (x_3) + (x_4) + (x_2) + (x_1) \\
w_{(12)(34)}^{\leftrightarrow}.a_{0,1} :& (x_1, x_2, x_3, x_4) \mapsto (x_4) + (x_3) + (x_2) + (x_1)
\end{aligned}
$$

or

$$
\begin{aligned}
a_{1,1} : (x_1, x_2, x_3, x_4) \mapsto & (x_1) \cdot (x_2) \cdot (x_3) + (x_1) \cdot (x_2) \cdot (x_4) \\
& + (x_3) \cdot (x_4) \cdot (x_1) + (x_3) \cdot (x_4) \cdot (x_2) \\
w_{(12)}.a_{1,1} : (x_1, x_2, x_3, x_4) \mapsto & (x_2) \cdot (x_1) \cdot (x_3) + (x_2) \cdot (x_1) \cdot (x_4) \\
& + (x_3) \cdot (x_4) \cdot (x_2) + (x_3) \cdot (x_4) \cdot (x_1) \\
w_{(34)}.a_{1,1} : (x_1, x_2, x_3, x_4) \mapsto & (x_1) \cdot (x_2) \cdot (x_4) + (x_1) \cdot (x_2) \cdot (x_3) \\
& + (x_4) \cdot (x_3) \cdot (x_1) + (x_4) \cdot (x_3) \cdot (x_2) \\
w_{(12)(34)}.a_{1,1} : (x_1, x_2, x_3, x_4) \mapsto & (x_2) \cdot (x_1) \cdot (x_4) + (x_2) \cdot (x_1) \cdot (x_3) \\
& + (x_4) \cdot (x_3) \cdot (x_2) + (x_4) \cdot (x_3) \cdot (x_1) \\
w^{\leftrightarrow}.a_{1,1} : (x_1, x_2, x_3, x_4) \mapsto & (x_3) \cdot (x_4) \cdot (x_1) + (x_3) \cdot (x_4) \cdot (x_2) \\
& + (x_1) \cdot (x_2) \cdot (x_3) + (x_1) \cdot (x_2) \cdot (x_4) \\
w_{(12)}^{\leftrightarrow}.a_{1,1} : (x_1, x_2, x_3, x_4) \mapsto & (x_4) \cdot (x_3) \cdot (x_1) + (x_4) \cdot (x_3) \cdot (x_2) \\
& + (x_1) \cdot (x_2) \cdot (x_4) + (x_1) \cdot (x_2) \cdot (x_4) \\
w_{(34)}^{\leftrightarrow}.a_{1,1} : (x_1, x_2, x_3, x_4) \mapsto & (x_3) \cdot (x_4) \cdot (x_2) + (x_3) \cdot (x_4) \cdot (x_1) \\
& + (x_2) \cdot (x_1) \cdot (x_3) + (x_2) \cdot (x_1) \cdot (x_3) \\
w_{(12)(34)}^{\leftrightarrow}.a_{1,1} : (x_1, x_2, x_3, x_4) \mapsto & (x_4) \cdot (x_3) \cdot (x_2) + (x_4) \cdot (x_3) \cdot (x_1) \\
& + (x_2) \cdot (x_1) \cdot (x_4) + (x_2) \cdot (x_1) \cdot (x_3).
\end{aligned}
$$

Let us now prove that $\{a_{r,s}\}_{0\leq r,s;r+s\leq 2}$ generates M. Let $a \in M$. There exist some coefficients $c_I \in H^*(k_0, \mathbb{Z}/2\mathbb{Z})$ for any $I \subset \{1,2,3,4\}$ such that

$$\begin{aligned}
a =& \sum_{I\subset\{1,2,3,4\}} c_I \cdot a_I \\
=& c_\emptyset + \sum_{i=0}^{4} c_{\{i\}} \cdot a_{\{i\}} + \big(c_{\{1,2\}} \cdot a_{\{1,2\}} + c_{\{3,4\}} \cdot a_{\{3,4\}}\big) \\
&+ \big(c_{\{1,3\}} \cdot a_{\{1,3\}} + c_{\{1,4\}} \cdot a_{\{1,4\}} + c_{\{2,3\}} \cdot a_{\{2,3\}} + c_{\{2,4\}} \cdot a_{\{2,4\}}\big) \\
&+ \big(c_{\{1,2,3\}} \cdot a_{\{1,2,3\}} + c_{\{1,2,4\}} \cdot a_{\{1,2,4\}} + c_{\{1,3,4\}} \cdot a_{\{1,3,4\}} + c_{\{2,3,4\}} \cdot a_{\{2,3,4\}}\big) \\
&+ c_{\{1,2,3,4\}} \cdot a_{\{1,2,3,4\}}.
\end{aligned}$$

Recall that the family $\{a_I\}_{I\subset\{1,2,3,4\}}$ is free over $H^*(k_0, \mathbb{Z}/2\mathbb{Z})$. Note that

$$\begin{aligned}
w_{(12)(34)}.a_{\{1\}} &= a_{\{2\}}, \\
w_{(12)(34)}.a_{\{3\}} &= a_{\{4\}}, \\
w_{(12)(34)}.a_{\{1,2,3\}} &= a_{\{1,2,4\}} \text{ and} \\
w_{(12)(34)}.a_{\{1,3,4\}} &= a_{\{2,3,4\}}.
\end{aligned}$$

Since $w_{(12)(34)}.a = a$,

$$\begin{aligned}
c_{\{1\}} &= c_{\{2\}}, \\
c_{\{3\}} &= c_{\{4\}}, \\
c_{\{1,2,3\}} &= c_{\{1,2,4\}} \text{ and} \\
c_{\{1,3,4\}} &= c_{\{2,3,4\}}.
\end{aligned}$$

Likewise, note that

$$\begin{aligned}
w^{\leftrightarrow}.a_{\{1\}} &= a_{\{3\}}, \\
w^{\leftrightarrow}.a_{\{1,2\}} &= a_{\{3,4\}}, \\
w^{\leftrightarrow}.a_{\{1,4\}} &= a_{\{2,3\}} \text{ and} \\
w^{\leftrightarrow}.a_{\{1,2,3\}} &= a_{\{1,3,4\}}.
\end{aligned}$$

Since $w^{\leftrightarrow}.a = a$,

$$\begin{aligned}
c_{\{1\}} &= c_{\{3\}}, \\
c_{\{1,2\}} &= c_{\{3,4\}}, \\
c_{\{1,4\}} &= c_{\{2,3\}} \text{ and} \\
c_{\{1,2,3\}} &= c_{\{1,2,4\}}.
\end{aligned}$$

We also have $w^{\leftrightarrow}_{(12)}a_{\{1,3\}} = a_{\{1,4\}}$. Since $w^{\leftrightarrow}.a = a$,

$$c_{\{1,3\}} = c_{\{1,4\}}.$$

Eventually, $w^{\leftrightarrow}_{(34)}a_{\{2,3\}} = a_{\{2,4\}}$. Since $w^{\leftrightarrow}.a = a$,

$$c_{\{2,3\}} = c_{\{2,4\}}.$$

Combining all these equalities, we get

$a = c_{\emptyset} \cdot a_{0,0} + c_{\{1\}} \cdot a_{0,1} + c_{\{1,2\}} \cdot a_{1,0} + c_{\{1,3\}} \cdot a_{0,2} + c_{\{1,2,3\}} \cdot a_{1,1} + c_{\{1,2,3,4\}} \cdot a_{2,0}.$

Therefore, $\{a_{r,s}\}_{0 \leq r,s; r+s \leq 2}$ generates M. ■

5.2 Cohomological invariants of $W(D_n)$: the case n even

Let us first deal with the case n even.

5.2.1 Restriction of Stiefel-Whitney invariants

Let us start with computing the restrictions of the Siefel-Whitney invariants to the subgroup H.

Lemma 5.2. *(i) For any $0 \leq i \leq \frac{n}{2}$,*

$$Res_W^H(w_i) = \begin{cases} a_{0,i} + (2) \cdot a_{0,i-1} & \text{if } i \text{ is even} \\ a_{0,i} & \text{if } i \text{ is odd} \end{cases}$$

(ii) For any $0 \leq i \leq n$ even,

$$Res_W^H(\widetilde{w}_j) = \sum_{r=0}^{\frac{j}{2}} a_{r,j-2r} + (2) \cdot \big(\sum_{r=0}^{\frac{j}{2}-1} a_{r,j-1-2r} \big)$$

Proof. Let k/k_0 be a field extension and let $(L, \alpha) \in H^1(k, W')$ lying in the image of the map $H^1(k, H) \to H^1(k, W')$. Then, by Proposition 4.1, there exist some $x_1, ..., x_n \in k^*$ such that

$$L = k(\sqrt{x_1 x_2}) \times k(\sqrt{x_3 x_4}) \times ... \times k(\sqrt{x_{n-1} x_n}) \text{ and } \alpha = (x_1, x_3, ..., x_{n-1}).$$

(i) Let $0 \leq i \leq \frac{n}{2}$. Then

$$\begin{aligned} w_i(L, \alpha) &= w_i(\langle 2 \rangle . \langle 1, x_1 x_2, 1, x_3 x_4, ..., 1, x_{n-1} x_n \rangle) \\ &= \begin{cases} w_i(\langle x_1 x_2, ..., x_{n-1} x_n \rangle) + (2) \cdot w_{i-1}(\langle x_1 x_2, ..., x_{n-1} x_n \rangle) & \\ \qquad \text{if } i \text{ is even} & \\ w_i(\langle x_1 x_2, ..., x_{n-1} x_n \rangle) \quad \text{if } i \text{ is odd} & \end{cases} \end{aligned}$$

Noting that $w_i(\langle x_1 x_2, ..., x_{n-1} x_n \rangle) = \sum_{\mathbf{1} \in I_i} (x)_{\mathbf{1}} = a_{0,i}(x_1, ..., x_n)$, we get

$$w_i(L, \alpha) = \begin{cases} a_{0,i}(x_1, ..., x_n) + (2) \cdot a_{0,i-1}(x_1, ..., x_n) & \text{if } i \text{ is even} \\ a_{0,i}(x_1, ..., x_n) & \text{if } i \text{ is odd} \end{cases}$$

(ii) Let $0 \leq i \leq n$ and assume that i is even. Hence,

$$\begin{aligned}\widetilde{w}_i(L,\alpha) &= w_i(\langle 2\rangle.\langle x_1,...,x_n\rangle) \\ &= w_i(\langle x_1,...,x_n\rangle) + (2)\cdot w_{i-1}(\langle x_1,...,x_n\rangle)\end{aligned}$$

An easy computation yields

$$w_i(\langle x_1,...,x_n\rangle) = \sum_{r=max(0,i-\frac{n}{2})}^{\frac{i}{2}} a_{r,i-2r}(x_1,...,x_n) = \sum_{r=0}^{\frac{i}{2}} a_{r,i-2r}(x_1,...,x_n),$$

with the convention $a_{r,s}=0$ if $r+s>\frac{n}{2}$. Therefore,

$$\widetilde{w}_i(L,\alpha) = \sum_{r=0}^{\frac{i}{2}} a_{r,i-2r}(x_1,...,x_n) + (2)\cdot\big(\sum_{r=0}^{\frac{i}{2}-1} a_{r,i-1-2r}(x_1,...,x_n)\big). \quad \blacksquare$$

Let $0 \leq i \leq \frac{n}{2}$ and let $0 \leq j \leq n-2i$ with j even. We now write the restrictions $\mathsf{Res}^H_W(w_i \cdot \widetilde{w}_j)$ in the basis $\{a_{r,s}\}$ of $\mathsf{Inv}_{k_0}(H,\mathbb{Z}/2\mathbb{Z})^{N_H/H}$.

Proposition 5.1. *Let $0 \leq i \leq \frac{n}{2}$ and let $0 \leq j \leq n-2i$ with j even. If i is even,*

$$\begin{aligned}Res^H_W(w_i\cdot\widetilde{w}_j) = &\sum_{r=max(0,j-\frac{n}{2})}^{\frac{j}{2}} \sum_{t=0}^{min(i,j-2r)} \binom{j-2r}{t}\binom{i+j-2r-t}{j-2r}(-1)^{\cdot t}\cdot a_{r,i+j-2r-t} \\ &+ (2)\cdot\Big(\sum_{r=max(0,j-1-\frac{n}{2})}^{\frac{j}{2}-1}\binom{i+j-1-2r}{j-1-2r}a_{r,i+j-1-2r}\Big) \\ &+ (2)\cdot\Big(\sum_{r=max(0,j-\frac{n}{2})}^{\frac{j}{2}}\binom{i-1+j-2r}{j-2r}a_{r,i-1+j-2r}\Big)\end{aligned}$$

If i is odd,

$$\begin{aligned}Res^H_W(w_i\cdot\widetilde{w}_j) = &\sum_{r=max(0,j-\frac{n}{2})}^{\frac{j}{2}} \sum_{t=0}^{min(i,j-2r)} \binom{j-2r}{t}\binom{i+j-2r-t}{j-2r}(-1)^{\cdot t}\cdot a_{r,i+j-2r-t} \\ &+ (2)\cdot\Big(\sum_{r=max(0,j-1-\frac{n}{2})}^{\frac{j}{2}-1}\binom{i+j-1-2r}{j-1-2r}a_{r,i+j-1-2r}\Big)\end{aligned}$$

Proof. From Lemma 5.2, we get the following formulae. For any $0 \leq i \leq \frac{n}{2}$ and any $0 \leq j \leq n-2i$ with j even,
if i is even,

$$\mathsf{Res}_W^H(w_i \cdot \widetilde{w}_j) = \sum_{r=0}^{\frac{j}{2}} a_{0,i} \cdot a_{r,j-2r} + (2) \cdot \big(\sum_{r=0}^{\frac{j}{2}-1} a_{0,i} \cdot a_{r,j-1-2r} \big)$$
$$+ (2) \cdot \big(\sum_{r=0}^{\frac{j}{2}} a_{0,i-1} \cdot a_{r,j-2r} \big)$$

if i is odd,

$$\mathsf{Res}_W^H(w_i \cdot \widetilde{w}_j) = \sum_{r=0}^{\frac{j}{2}} a_{0,i} \cdot a_{r,j-2r} + (2) \cdot \big(\sum_{r=0}^{\frac{j}{2}-1} a_{0,i} \cdot a_{r,j-1-2r} \big)$$

In both cases, for $0 \leq i \leq \frac{n}{2}$ and $0 \leq r, s$ such that $r+s \leq \frac{n}{2}$, we have to write the invariant $a_{0,i} \cdot a_{r,s}$ in the basis $\{a_{m,l}\}_{0 \leq m,l | m+l \leq \frac{n}{2}}$. The following lemma gives the answer and allows us to end the proof of Proposition 5.1. ■

Lemma 5.3. *Let $0 \leq i \leq \frac{n}{2}$, $0 \leq r, s$ such that $r+s \leq \frac{n}{2}$. Then*

$$a_{0,i} \cdot a_{r,s} = \sum_{t=0}^{min(i,s)} \binom{s}{t} \binom{i+s-t}{s} (-1)^{\cdot t} \cdot a_{r,i+s-t}$$

Proof. Let us first prove that $a_{0,i} \cdot a_{r,0} = a_{r,i}$. Let k/k_0 be a field extension and let $x_1, ..., x_n \in k^\times / k^{\times 2}$. Then

$$\begin{aligned}
&a_{0,i}(x_1, ..., x_n) \cdot a_{r,0}(x_1, ..., x_n) \\
&\quad = \sum_{\mathbf{l} \in I_i; 1 \leq m_1 < ... < m_r \leq n-1 \text{ odd numbers}} (x)_{\mathbf{l}} \cdot (x_{m_1}) \cdot (x_{m_1+1}) \cdot \cdots \cdot (x_{m_r}) \cdot (x_{m_r+1}) \\
&\quad = \sum_{u=0}^{\mathsf{min}(r,i)} \sum_{\substack{\mathbf{l} \in I_{i-u} \\ 1 \leq m_1 < ... < m_r \leq n-1 \text{ odd numbers} \\ \mathbf{l} \cap \{m_1, m_1+1, ..., m_r, m_r+1\} = \emptyset}} 2^u \binom{r}{u} (-1)^{\cdot (u)} \cdot (x)_{\mathbf{l}} \cdot (x_{m_1}) \cdot (x_{m_1+1}) \cdot \cdots \\
&\qquad\qquad \cdot (x_{m_r}) \cdot (x_{m_r+1}) \\
&\quad = \sum_{\substack{\mathbf{l} \in I_i; 1 \leq m_1 < ... < m_r \leq n-1 \text{ odd numbers} \\ \mathbf{l} \cap \{m_1, m_1+1, m_2, m_2+1, ..., m_r, m_r+1\} = \emptyset}} (x)_{\mathbf{l}} \cdot (x_{m_1}) \cdot (x_{m_1+1}) \cdot \cdots \cdot (x_{m_r}) \cdot (x_{m_r+1}) \\
&\quad = a_{r,i}.
\end{aligned}$$

Likewise, we prove that

$$a_{0,i}(x_1,...,x_n)\cdot a_{r,s}(x_1,...,x_n)$$
$$= \sum_{\substack{\mathbf{l}\in I_i;\mathbf{l}'\in I_s\\ 1\leq m_1<...<m_r\leq n-1 \text{ odd numbers}\\ \mathbf{l}\cap\{m_1,m_1+1,m_2,m_2+1,...,m_r,m_r+1\}=\emptyset\\ \mathbf{l}'\cap\{m_1,m_1+1,m_2,m_2+1,...,m_r,m_r+1\}=\emptyset}} (x)_{\mathbf{l}}\cdot(x_{m_1})\cdot(x_{m_1+1})\cdot\cdot\cdot\cdot\cdot(x_{m_r})\cdot(x_{m_r+1})\cdot(x)_{\mathbf{l}'}.$$

Hence,

$$\begin{aligned}
&a_{0,i}(x_1,...,x_n)\cdot a_{r,s}(x_1,...,x_n)\\
&\quad=\sum_{t=0}^{\min(i,s)}\sum_{\substack{\mathbf{l}\in I_{i-t};\mathbf{l}'\in I_s\\ 1\leq m_1<...<m_r\leq n-1 \text{ odd numbers}\\ \mathbf{l}\cap\{m_1,m_1+1,m_2,m_2+1,...,m_r,m_r+1\}=\emptyset\\ \mathbf{l}'\cap\{m_1,m_1+1,m_2,m_2+1,...,m_r,m_r+1\}=\emptyset\\ \mathbf{l}\cap\mathbf{l}'=\emptyset}} \binom{s}{t}(-1)^{\cdot t}\cdot(x_{m_1})\cdot(x_{m_1+1})\cdot\cdot\cdot\cdot\\
&\qquad\qquad\cdot(x_{m_r})\cdot(x_{m_r+1})\cdot(x)_{\mathbf{l}}\cdot(x)_{\mathbf{l}'}\\
&\quad=\sum_{t=0}^{\min(i,s)}\sum_{u=0}^{\min(i-t,s)}\sum_{\substack{\mathbf{l}\in I_{i-t-u};\mathbf{l}'\in I_{s-u}\\ 1\leq m_1<...<m_r\leq n-1 \text{ odd numbers}\\ 1\leq m'_1<...<m'_u\leq n-1 \text{ odd numbers}\\ \mathbf{l}\cap\{m_1,m_1+1,m_2,m_2+1,...,m_r,m_r+1,m'_1+1,...,m'_u,m'_u+1\}=\emptyset\\ \mathbf{l}'\cap\{m_1,m_1+1,m_2,m_2+1,...,m_r,m_r+1,m'_1,m'_1+1,...,m'_u,m'_u+1\}=\emptyset\\ \mathbf{l}\cap\mathbf{l}'=\emptyset\\ \{m_1,...,m_r\}\cap\{m'_1,...,m'_u\}=\emptyset\\ \mathbf{l}\cup\mathbf{l}'\in I_{s+i-t-2u}}}\\
&\qquad 2^u\binom{s}{t}(-1)^{\cdot t}\cdot(x_{m_1})\cdot(x_{m_1+1})\cdot\cdot\cdot\cdot\cdot(x_{m_r})\cdot(x_{m_r+1})\cdot(x_{m'_1})\\
&\qquad\cdot(x_{m'_1+1})\cdot\cdot\cdot\cdot\cdot(x_{m'_u})\cdot(x_{m'_u+1})\cdot(x)_{\mathbf{l}}\cdot(x)_{\mathbf{l}'}\\
&\quad=\sum_{t=0}^{\min(i,s)}\sum_{\substack{\mathbf{l}\in I_{i+s-t}\\ 1\leq m_1<...<m_r\leq n-1 \text{ odd numbers}\\ \mathbf{l}\cap\{m_1,m_1+1,m_2,m_2+1,...,m_r,m_r+1\}=\emptyset}} \binom{s}{t}\binom{i+s-t}{s}(-1)^{\cdot t}\\
&\qquad\qquad\cdot(x_{m_1})\cdot(x_{m_1+1})\cdot\cdot\cdot\cdot\cdot(x_{m_r})\cdot(x_{m_r+1})\cdot(x)_{\mathbf{l}}
\end{aligned}$$

This allows us to conclude the proof of Lemma 5.3. ■

5.2.2 Proof of Theorem 5.1

Let us now prove Theorem 5.1. Note that the (cohomological) degree of $a_{r,s}$ is $2r+s$. By Proposition 5.1, every element $a_{r,s}$ appearing in the decomposition of

$\mathsf{Res}^H_W(w_i \cdot \widetilde{w}_j)$ has degree $\leq i+j$. Indeed,

$$\begin{aligned}\mathsf{deg}(a_{r,i+j-2r-t}) &= i+j-t,\\ \mathsf{deg}(a_{r,i+j-1-2r}) &= i+j-1,\\ \mathsf{deg}(a_{r,i-1+j-2r}) &= i+j-1.\end{aligned}$$

Moreover, if $\mathsf{deg}(a_{r,i+j-2r-t}) = i+j$, then $t=0$. We then may write

$$\mathsf{Res}^H_W(w_i \cdot \widetilde{w}_j) = \sum_{r=\mathsf{max}(0,j-\frac{n}{2})}^{\frac{j}{2}} \binom{i+j-2r}{j-2r} a_{r,i+j-2r} + A$$

where A is a linear combination of cohomological invariants with degree $< i+j$.

Let us write this restriction as follows

$$\mathsf{Res}^H_W(w_i \cdot \widetilde{w}_j) = a_{\frac{j}{2},i} + \sum_{r=\mathsf{max}(0,j-\frac{n}{2})}^{\frac{j}{2}-1} \binom{i+j-2r}{j-2r} a_{r,i+j-2r} + A. \tag{5.1}$$

We now prove by induction on the cohomological degree $d \geq 0$, that for any couple (r,s) of non negative integers, such that $r+s \leq \frac{n}{2}$ and $2r+s=d$, $a_{r,s}$ may be written as a linear combination of invariants of the family

$$\{\mathsf{Res}^H_W(w_i \cdot \widetilde{w}_j)\}_{0\leq i\leq \frac{n}{2}, 0\leq j\leq n-2i \text{ and } j \text{ even}}.$$

Obviously, $a_{0,0} = \mathsf{Res}^H_W(w_0 \cdot \widetilde{w}_0)$.

Let $0 < d \leq \frac{n}{2}$. Assume that for any $0 \leq d' < d$, the induction hypothesis is true. Let us now make a second induction. We prove by induction on r that, for any $0 \leq r \leq [\frac{d}{2}]$, $a_{r,d-2r}$ may be written as a linear combination of restrictions of invariants of the family

$$\{\mathsf{Res}^H_W(w_i \cdot \widetilde{w}_j)\}_{0\leq i\leq \frac{n}{2}, 0\leq j\leq n-2i \text{ and } j \text{ even}}.$$

Let us first note that

$$a_{0,d} = \begin{cases} \mathsf{Res}^H_W(w_d \cdot \widetilde{w}_0) + (2) \cdot \mathsf{Res}^H_W(w_{d-1} \cdot \widetilde{w}_0) & \text{if } d \text{ is even} \\ \mathsf{Res}^H_W(w_d \cdot \widetilde{w}_0) & \text{if } d \text{ is odd} \end{cases}$$

which allows us to conclude the case $r=0$.

Let now $0 < r \leq [\frac{d}{2}]$. Let us assume that, for any $0 \leq r' < r$, $a_{r',d-2r'}$ can be written as a linear combination of restrictions of invariants $\mathsf{Res}^H_W(w_i \cdot \widetilde{w}_j)$ with

$0 \leq i \leq \frac{n}{2}$, $0 \leq j \leq n-2i$ and j even.

By Equation (5.1),

$$\mathsf{Res}^H_W(w_s \cdot \widetilde{w}_{2r}) = a_{r,s} + \sum_{m=max(0,2r-\frac{n}{2})}^{r-1} \binom{s+2(r-m)}{2(r-m)} a_{m,s+2(r-m)} + A$$

where A is a linear combination of $a_{r',s'}$ with $2r'+s' < 2r+s$.
By the first induction hypothesis on A and the second induction hypothesis on $a_{m,s+2(r-m)}$ for $\mathsf{max}(0, j-\frac{n}{2}) \leq m \leq r-1$, we have

$$a_{r,s} = \mathsf{Res}^H_W(w_s \cdot \widetilde{w}_{2r}) + B$$

where B is a linear combination of invariants $\mathsf{Res}^H_W(w_i \cdot \widetilde{w}_j)$ with $0 \leq i \leq \frac{n}{2}$, $0 \leq j \leq n-2i$ and j even.

This concludes both inductions and ends the proof of Theorem 5.1 in the case where n is even. ■

5.3 Cohomological invariants of $W(D_n)$: the case n odd

Let us now consider the case n odd and let prove Theorem 5.1. Let W'' be the Weyl group of type D_{n-1} associated with the root subsystem

$$\{\pm e_i \pm e_j \mid 1 \leq i \neq j \leq n-1\}.$$

Then H is a subgroup of W''. Therefore, by the vanishing principle (Theorem 5.2), the restriction map $\mathsf{Res}^{W''}_W$ is injective.

For $0 \leq i \leq n-1$, let us denote by $w_i^{W''}$ and $\widetilde{w}_i^{W''}$ the Stiefel-Whitney invariants of the Weyl group W''.

By the vanishing principle (Theorem 5.2), the map $\mathsf{Res}^H_{W''}$ is injective. Yet, for any $0 \leq i \leq \frac{n-1}{2}$ and any $0 \leq j \leq n-1-2i$ with j even, the cohomological invariants $\mathsf{Res}^{W''}_W(w_i \cdot \widetilde{w}_j)$ and $w_i^{W''} \cdot \widetilde{w}_j^{W''}$ of W'' have same restriction to H, then they are equal :

$$\mathsf{Res}^{W''}_W(w_i \cdot \widetilde{w}_j) = w_i^{W''} \cdot \widetilde{w}_j^{W''}$$

By Theorem 5.1 applied to W'' (proved at the previous section in the case even), the family $\{w_i^{W''} \cdot \widetilde{w}_j^{W''}\}_{0 \leq i \leq \frac{n-1}{2}, 0 \leq j \leq n-1-2i, j \text{ even}}$ is a basis of $\mathsf{Inv}_{k_0}(W'', \mathbb{Z}/2\mathbb{Z})$.

Therefore, the restriction map $\mathsf{Res}_W^{W''} : \mathsf{Inv}_{k_0}(W, \mathbb{Z}/2\mathbb{Z}) \to \mathsf{Inv}_{k_0}(W'', \mathbb{Z}/2\mathbb{Z})$ is an isomorphism and the family $\{w_i \cdot \widetilde{w}_j\}_{0 \leq i \leq \frac{n}{2}, 0 \leq j \leq n-2i, \text{ with } j \text{ even}}$ is sent to a basis of $\mathsf{Inv}_{k_0}(W'', \mathbb{Z}/2\mathbb{Z})$. This allows us to conclude. ■

Appendix A

Reflection groups and finite Coxeter groups

This appendix is based on the well-known references [3] and [11].

Let k be a field, let V be a vector space over k.

Definition A.1. *A pseudo-reflection in V is an endomorphism r of V such that $r - \mathsf{id}_V$ has rank 1. A reflection in V is a pseudo-reflection of V such that $r^2 = \mathsf{id}_V$.*

Note that the only pseudo-reflections in a real vector space are reflections.

Definition A.2. *A pseudo-reflection group (resp. a reflection group) over k is a group of linear automorphisms of a k-vector space V which is generated by pseudo-reflections (resp. reflections) in V.*

Let us state Chevalley's theorem (see [3], 5.5, Theorem 4).

Theorem A.1. *Let k be a field, let V be a finite dimensional k-vector space, let S be the symmetric algebra of V, let W be finite group of linear automorphisms of V and let R be the subalgebra of S of the invariant elements under W. Let us assume that the order of W is prime to the characteristic of k. Then the following conditions are equivalent :*

(i) W is generated by pseudo-reflections in V;

(ii) S is a free graded R-module;

(iii) R is a polynomial graded k-algebra.

Let us state some useful properties on reflections. Let us now assume that k has characteristic different from 2. For any reflection r in V, we set $V_r^+ = \mathsf{Ker}(r - \mathsf{id}_V)$ and $V_r^- = \mathsf{Im}(r - \mathsf{id}_V)$. Proofs of the following proposition and its corollary can be found in [3], V.2, Prop.3.

Proposition A.1. *Let r be a reflection in V.*

1. *A subspace V' of V is stable by r if and only if $V_r^- \subset V'$ or $V' \subset V_r^+$.*
2. *An endomorphism u of V commutes with r if and only if V_r^+ and V_r^- are stable by u.*

Corollary A.1. *Two distinct reflections r and r' in in V commute if and only if $V_{r'}^- \subset V_r^+$ and $V_r^- \subset V_{r'}^+$.*

Definition A.3. *Let W be a reflection group over k. A subgroup $H \subset W$ is called an isotropy subgroup if $H = \{w \in W \mid w(v) = v\}$ for some $v \in V$.*

Then an isotropy subgroup is a reflection group (see [11], 1.12).

Proposition A.2. *Let W be a reflection group over $\mathbb{R}$. Any isotropy subgroup of W is generated by the reflections it contains. In particular, an isotropy subgroup is a reflection group over $\mathbb{R}$.*

Note that this is not the case anymore for pseudo-reflection groups and even for reflection groups over $\mathbb{C}$ (see for instance [4]).

Let us now give the classification of finite reflection groups over $\mathbb{R}$.

Definition A.4. *A Coxeter group W is a group with a given presentation of type*

$$\langle r_1, .., r_s \mid \forall i, j \in \{1, .., s\}, (r_i r_j)^{m_{i,j}} = 1 \rangle,$$

where $\forall i, j \in \{1, ..., s\}$, $m_{i,j} \in \mathbb{N} \cup \{+\infty\}$ and $m_{i,i} = 1$ for every $i \in \{1, ..., s\}$.

It is well-known that a finite group G is a Coxeter group if and only if it is a reflection group over $\mathbb{R}$ (see [11]). Note that there are some reflection groups over $\mathbb{C}$ which are not Coxeter groups (see for instance [3],V.5, exercise 4 or [5]).

Definition A.5. *Let V be a finite dimensional $\mathbb{R}$-vector space. A root system S is a finite set of non-zero vectors in V satisfying the conditions :*

1. *for any $\alpha \in S$, $S \cap \mathbb{R}\alpha = \{\pm\alpha\}$*

2. *for any $\alpha \in S$, $r_\alpha(S) = S$, where r_α denotes the orthogonal reflection on V such that $\mathsf{Im}(r_\alpha - \mathsf{id}_V) = \mathbb{R}\alpha$.*

Note that a root system S yields a finite Coxeter group (the group generated by the reflections r_α, for any $\alpha \in S$). Conversely, any finite Coxeter group can be realized in this way, possibly for many different choices for S.

If a root system S cannot be written $S_1 \sqcup S_2$, with S_1 and S_2 two root systems, we say that S is irreducible. Irreducible root systems are completely classified (and so are finite Coxeter groups) (see [11] or [3] for details).

Let $(e_1, ..., e_n)$ be a canonical basis of $\mathbb{R}^n$. Up to linear automorphism, irreducible root systems are classified in several types :

A_n $(n \geq 1)$: let V be the hyperplane of $\mathbb{R}^{n+1}$ such that the sum of coordinates equal to zero. Then $S = \{e_i - e_j \mid 1 \leq i, j \leq n+1, i \neq j\}$. The Coxeter group is isomorphic to $\mathfrak{S}_{n+1}$.

B_n (for $n \geq 2$) : $V = \mathbb{R}^n$, $S = \{\pm e_i, \pm e_j \pm e_l \mid 1 \leq i \leq n, 1 \leq j < l \leq n\}$. The Coxeter group is isomorphic to the semi-direct product $\left(\mathbb{Z}/2\mathbb{Z}\right)^n \rtimes \mathfrak{S}_n$, where $\mathfrak{S}_n$ acts on $(\mathbb{Z}/2\mathbb{Z})^n$ by permuting coordinates.

C_n (for $n \geq 2$) : $V = \mathbb{R}^n$, $S = \{\pm 2e_i, \pm e_j \pm e_l \mid 1 \leq i \leq n, 1 \leq j < l \leq n\}$. The Coxeter group is the same than in the type B_n.

D_n $(n \geq 4)$: $V = \mathbb{R}^n$, $S = \{\pm e_i \pm e_j) \mid 1 \leq i < j \leq n\}$. The Coxeter group W is defined by the exact sequence

$$1 \longrightarrow W \longrightarrow W' \xrightarrow{p} \mathbb{Z}/2\mathbb{Z} \longrightarrow 1 \ ,$$

where W' is the reflection group of type B_n and $p : (\epsilon_1, ..., \epsilon_n, \sigma) \mapsto \prod_{i=1}^{n} \epsilon_i$. Moreover, W is isomorphic to the semi-direct product $\left(\mathbb{Z}/2\mathbb{Z}\right)^{n-1} \rtimes \mathfrak{S}_n$.

E_6 : $V = \{(x_i)_{1 \leq i \leq 8} \in \mathbb{R}^8 \mid x_6 = x_7 = -x_8\}$,

$$S = \{\pm e_i \pm e_j, \pm \frac{1}{2}(e_8 - e_7 - e_6 + \sum_{l=1}^{5} (-1)^{\nu(l)} e_l) \mid 1 \leq i < j \leq 5 \text{ and } \sum_{l=1}^{5} \nu(l) \text{ even}\} \ .$$

E_7 : let V be the hyperplane of $\mathbb{R}^8$ orthogonal to $e_7 + e_8$. Then

$$S = \{\pm e_i \pm e_j, \pm(e_7 - e_8), \pm\frac{1}{2}(e_7 - e_8 + \sum_{l=1}^{6}(-1)^{\nu(l)}e_l) \\ | \ 1 \leq i < j \leq 6 \text{ and } \sum_{l=1}^{6}\nu(l) \text{ odd}\}.$$

E_8 : $V = \mathbb{R}^8$,

$$S = \{\pm e_i \pm e_j, \frac{1}{2}\sum_{l=1}^{8}(-1)^{\nu(l)}e_l \mid 1 \leq i < j \leq 8 \text{ and } \sum_{l=1}^{8}\nu(l) \text{ even}\}.$$

F_4 : $V = \mathbb{R}^4$,

$$S = \{\pm e_i, \pm e_j \pm e_l, \frac{1}{2}(\pm e_1 \pm e_2 \pm e_3 \pm e_4) \mid 1 \leq i \leq 4, 1 \leq j < l \leq 4\}.$$

The Coxeter group is isomorphic to the semi-direct product

$$\left(\left(\mathbb{Z}/2\mathbb{Z}\right)^3 \rtimes \mathfrak{S}_4\right) \rtimes \mathfrak{S}_3,$$

where $\left(\mathbb{Z}/2\mathbb{Z}\right)^3 \rtimes \mathfrak{S}_4$ is the Coxeter group of type D_4 and $\mathfrak{S}_3$ acts on it by permuting vertices of the Dynkin diagram of D_4.

G_2 : let V be the hyperplane of $\mathbb{R}^3$ with the sum of the coordinates equal to zero. Then

$$S = \{\pm(e_1 - e_2), \pm(e_1 - e_3), \pm(e_2 - e_3), \pm(2e_1 - e_2 - e_3), \pm(2e_2 - e_1 - e_3), \\ \pm(2e_3 - e_1 - e_2)\}.$$

The Coxeter group is isomorphic to the dihedral group $\mathbb{D}_6$ of order 12.

H_3 : the Coxeter group is isomorphic to $\mathfrak{A}_5 \times \mathbb{Z}/2\mathbb{Z}$, where $\mathfrak{A}_5$ denotes the alternating subgroup of $\mathfrak{S}_5$.

H_4 : the Coxeter group is the group of isometries of the hecatonicosahedroid.

$I_2(m)$, $m \geq 3$: the Coxeter group is isomorphic to the dihedral group $\mathbb{D}_m$ of order $2m$.

With this classification, we get that every finite Coxeter group is isomorphic to a direct product of Coxeter groups of type A to I.

Definition A.6. *A Weyl group W is a finite Coxeter group with a root system S satisfying the additional integrality condition : for any $\alpha, \beta \in S$, $2\frac{(\alpha,\beta)}{(\alpha,\alpha)} \in \mathbb{Z}$, where $(.,.)$ denotes the usual scalar product.*

Any Weyl group is isomorphic to a direct product of groups of type A to G. For these groups, we have the important following result (see [25], Corollary 1.15).

Theorem A.2. *Let W be a Weyl group. Every irreducible representation of W is realizable over $\mathbb{Q}$. In particular, Weyl groups are reflection groups over $\mathbb{Q}$.*

Therefore, the real representation of a Weyl group as a real reflection group is realizable over $\mathbb{Q}$. By extension of scalars, Weyl groups are reflection groups over any field of characteristic zero. In particular, Theorem 3.1 is true for any Weyl group and any field of characteristic zero.

Theorem A.2 is not true for a Coxeter group which is not a Weyl group. However,

Proposition A.3. *Let W be a finite Coxeter group. There is a finite real extension L of $\mathbb{Q}$ such that W is a reflection group over L.*

Note that $L = \mathbb{Q}(\sqrt{5})$ for the Coxeter groups of type H and $L = \mathbb{Q}(\cos(\frac{2\pi}{m}))$ for the Coxeter groups of type $I_2(m)$, for any $m \geq 3$ are the minimal fields such that Proposition A.3 is satisfied.

More generally, let us state when a finite Coxeter group is a reflection over a fixed field of characteristic zero. Let k_0 be a field of characteristic zero. Thanks to the previous classification, W is isomorphic to a direct product of groups of type A to I. Then if k_0 contains the minimal field extensions over $\mathbb{Q}$ corresponding to the types in the decomposition of W, the representation of W as a finite reflection group extends to k_0 (and the assumption of Theorem 3.1 is satisfied).

Bibliography

[1] G. Berhuy. *An introduction to Galois cohomology and its applications*, volume 377 of *Lecture Notes Series*. London Mathematical Society, Cambridge, 2010.

[2] N. Bourbaki. *Eléments de mathématique : Algèbre: chapitres 4 à 7*, volume 2. Springer, 2006.

[3] N. Bourbaki. *Éléments de mathématique: Groupes et algèbres de Lie*. Eléments de mathématique. Springer, 2007.

[4] M. Broué. *Introduction to complex reflection groups and their braid groups*. Number vol. 1988 in Lecture notes in mathematics. Springer, 2010.

[5] M. Broué, G. Malle, and R. Rouquier. Complex reflection groups, braid groups, Hecke algebras. *J. Reine Angew. Math.*, 500:127–190, 1998.

[6] A. Delzant. Définition des classes de Stiefel-Whitney d'un module quadratique sur un corps de caractéristique différente de 2. *C.R. Acad. Sci. Paris*, 255:1366–1368, 1962.

[7] M. Demazure and A. Grothendieck. *Schémas en groupes. III : Structure des schémas en groupes réductifs*, volume 153. Springer-Verlag, 1970.

[8] B. Eckmann. Cohomology of groups and transfers. *Annals of Mathematics*, 58(3).

[9] R. Elman and T.Y. Lam. Classification theorems for quadratic forms over fields. *Commentarii Mathematici Helvetici*, 49(1):373–381, 1974.

[10] P. Gille and T. Szamuely. *Central Simple Algebras And Galois Cohomology*. Number vol. 13 in Cambridge Studies in Advanced Mathematics. Cambridge University Press, 2006.

[11] J.E. Humphreys. *Reflection groups and Coxeter groups*. Cambridge Studies in Advanced Mathematics. Cambridge University Press, 1992.

[12] M.-A. Knus, A. S. Merkurjev, M. Rost, and J.-P. Tignol. *The Book of Involutions*, volume 44. American Society, Providence, RI, 1998.

[13] M.-A. Knus and J.-P. Tignol. Triality and étale algebras. (arXiv:0912.3405), 2009.

[14] M. L. MacDonald. Cohomological invariants of odd degree Jordan algebras. *Mathematical Proceedings of the Cambridge Philosophical Society*, 145:295–303, 2008.

[15] M. L. MacDonald. Cohomological invariants of Jordan algebras with frames. *Journal of Algebra*, 323:1665–1677, 2010.

[16] J. Milnor. Algebraic K-theory and quadratic forms. *Inventiones Mathematicae*, 9(4):318–344, 1970.

[17] J. Neukirch. *Algebraic number theory.* Grundlehren der mathematischen Wissenschaften. Springer, 1999.

[18] D. Orlov, A. Vishik, and V. Voevodsky. An exact sequence for $k_\star^M/2$ with applications to quadratic forms. *Annals of Mathematics*, 165:1–13, 2007.

[19] W. Scharlau. Quadratischen Formen und Galois cohomologie. *Inventiones Mathematicae*, 4:238–264, 1967.

[20] J-P. Serre. Cohomologie Galoisienne. *Lecture Notes in Mathematics*, 5, 1965.

[21] J-P. Serre. *Cours d'arithmétique.* SUP.: Le Mathématicien. Presses universitaires de France, 1977.

[22] J-P. Serre. L'invariant de Witt de la forme $\mathrm{Tr}(x^2)$. *Comment. Math. Helv.*, 59:651–676, 1984.

[23] J-P. Serre. *Local fields.* Graduate texts in mathematics. Springer-Verlag, 1995.

[24] J-P. Serre. *Cohomological invariants, Witt invariants and trace forms.* In University Lecture Series, 28. Amer. Math. Soc., Providence, RI, 2003.

[25] T. A. Springer. A construction of representations of Weyl groups. *Inventiones Mathematicae*, 44:279–293, 1978.

[26] V. Voevodsky. Motivic cohomology with Z/2-coefficients. *Publ. Math. Inst. Hautes Etudes Sci*, 98:59–104, 2003.

[27] A.R. Wadsworth. Merkurjev's elementary proof of Merkurjev's theorem, Applications of algebraic K-theory to algebraic geometry and number theory, Part I, II (Boulder, Colo., 1983). *Contemporary Mathematics*, 55.

RÉSUMÉ

Cette thèse traite des invariants cohomologiques en cohomologie galoisienne des groupes de Coxeter finis en caractéristique nulle. On établit d'abord un principe général d'annulation vérifié par tout invariant cohomologique d'un groupe de Coxeter fini sur un corps de caractéristique nulle suffisamment grand. On utilise ensuite ce principe pour déterminer tous les invariants cohomologiques des groupes de Weyl de type classique à coefficients dans $\mathbb{Z}/2\mathbb{Z}$ sur un corps de caractéristique nulle.

ABSTRACT

This PhD thesis deals with cohomological invariants in Galois cohomology of finite Coxeter groups in characteristic zero. We first state a general vanishing principle for the cohomological invariants of a finite Coxeter group over a sufficiently large field of characteristic zero. We then use this principle to determine all the cohomological invariants of the Weyl groups of classical type with coefficients in $\mathbb{Z}/2\mathbb{Z}$ over a field of characteristic zero.

KEYWORDS

Galois cohomology, torsors, ramification, residue maps, reflection groups.

MATHEMATICAL CLASSIFICATION

11E04, 11E72, 12G05, 14L15, 20G10, 20G15.