Table des matières

Responsabilités administratives

1. Responsabilités au sein de l'UJF

1. Responsable des enseignements /responsable de l'école de Mathématiques (depuis Septembre 2011).

Cette lourde tâche consiste en premier lieu à faire en sorte que tous les enseignements attribués à l'UFR IM2AG soient assurés. La fonction impose également de participer à toute décision relative à la grille des enseignements, au contenu de nos formations, et aux recrutements des ATER. En particulier, cela implique, de façon non exhaustive :

- de trouver de nombreux vacataires pour compléter la grille des enseignements

- s'assurer du bon déroulement des enseignements, et à gérer éventuellement les problèmes entre enseignants et étudiants s'il y a lieu.

- s'assurer que chaque enseignant a assuré un service complet, et à transmettre le nombre d'heures de CM/TD/TP assurés pour chaque UE et chaque enseignant au service compétent.

- d'organiser et/ou participer aux réunions de classements/interclassements pour l'UFR IM2AG concernant les demandes de délégations CNRS et CRCT (en conseil restreint et en commission formation)

- d'établir le classement des candidats ATER à l' institut Fourier et participer à la réunion d'interclassement en commission formation

- de participer à la réunion sur le référentiel des décharges (référentiel I)

- de préparer une liste de propositions de réductions substantielles de nos formations (en termes de volume d'heures enseignées), suite aux restrictions budgétaires

- de superviser une réflexion sur chacune nos formations en vue de la prochaine accréditation.

Ces deux derniers points ont impliqué (et impliquent toujours) l'organisation de nombreuses réunions de l'école de mathématiques, de discussions et de débats entre collègues, etc...

2. Président du comité de sélection MCF (2012).

Le travail consiste à contacter les membres internes et externes du comité de sélection, répartir les dossiers entre les divers rapporteurs, collecter les

rapports, organiser les réunions du comité, conduire les débats de façon à obtenir une liste de candidats à auditionner, puis un classement provisoire, et présenter ce classement au CA.

3. Correspondant Relations Internationales (2009-2010)

Mon rôle a consisté à me renseigner sur la possibilité de monter un projet ERASMUS MUNDUS (type Filière Master International+ Diplôme de Doctorat international). J'ai donc dû assister aux réunions d'information ERASMUS MUNDUS, me renseigner les modalités de candidature, constituer un réseau d'universités voulant devenir partenaires potentiels, assurer la liaison avec la vice-présidence du service Relations Internationales, et négocier le soutien logistique de la vice-présidence Relations Internationales.

2. Expertise (jurys, refeering, reviews)

2.1. Expertise (jurys, refeering, reviews).

1. Rapporteur externe pour la thèse de Ong Soon Sheng "Lattices codes for wiretap fading channels", NTU, Singapore (2014)

2. Rapporteur pour le projet de publication d'un ouvrage dans la collection LMS Lectures Notes, Cambridge University Press (2013).

3. Rapporteur pour le projet de publication d'un ouvrage aux Presses universitaires de Grenoble (2013).

4. Rapporteur pour une demande de bourse postdoctorale (2012).

5. Rapporteur pour la thèse de D. Barry, "Square central elements in algebras of exponent 2", Paris 13/UCL (2012).

6. Rapporteur pour la thèse de K.-T. Ruehl, "Annihilating polynomials for quadratic forms", EPFL (2010).

7. Membre du jury (rôle d'"Opponent") pour la thèse de R. Vehlakhati, "Class field theoretic methods in the design of lattice signal constellations", Turku (2008)

8. Membre du jury de thèse de M. Razcek, "Ternary cubic forms and central simple algebras of degree 3", UCL (2007)

9. Rapporteur pour divers journaux internationaux

10. Reviewer pour Mathscinet (articles et livres). En particulier, j'ai été sollicité pour écrire une review des ouvrages suivants :

• R.S. Garibaldi, A.S. Merkurjev, J.-.P Serre, *Cohomological invariants in Galois cohomology.* University Lecture Notes Series **28**, AMS, Providence, 2003.

• P. Gille, T. Szamuely, *Central simple algebras and Galois cohomology.* Cambride University Press, Cambridge, 2006.

3. Demandes de financement

Financement pour 2 ans, Nuffield foundation. Montant accordé : 4000 GBP (6000 EUR).

4. Organisation de conférences

1. Co-organisateur du Worshop “Arithmétique, algèbre et applications” à l’EPFL, 27-29 Juin 2011.

2. Co-organisateur du Workshop “Galois cohomology and linear algebraic groups” à l’EPFL, 24-29 Juin 2002.

3. Co-organisateur du Workshop “Linear algebraic groups and related topics” à l’EPFL, 29 Avril-3 Mai 2001.

Activités pédagogiques

5. Description succinte de l'enseignement

Depuis mon recrutement, j'ai enseigné à tous les niveaux du L1 au M2, aussi bien des cours magistraux que des séances de travaux dirigés, dans ma spécialité ou non :

• L1 : Langage mathématique, géométrie du plan et de l'espace, systèmes linéaires, espaces vectoriels et calcul matriciel (cours/TD)

• L2 : Suites et séries de fonctions (TD), Algèbre bilinéaire et séries de Fourier (Cours/TD)

• L3 : Théorie des groupes et des aneeaux, compléments d'algèbre linéaire (Cours), théorie de Galois (TD)

• M1 : Anneaux factoriels, théorie des corps, corps finis, théorie des modules (Cours)

• M2 : Introduction à la cohomologie galoisienne (Cours).

6. Minicours (sur invitation)

1. Introduction à la cohomologie galoisienne, Juin 2010, EPFL, Lausanne, Suisse

2. Introduction to Galois cohomology, May 2010, Université de Turku, Finlande

3. Introduction to Galois cohomology, Août 2009, NTU, Singapour

4. Introduction à la dimension essentielle, Juin 2007, Lens

5. Introduction à la dimension canonique, Juin 2005, EPFL, Lausanne, Suisse

6. Introduction to essential dimension , Novembre 2003, University of Western Ontario, London, Canada.

7. Responsabilités en enseignement

1. MAT242 : 60 étudiants/ 5 enseignants (2013-)

2. MAT244 : 170 étudiants/8 enseignants (2008 et 2009).

3. Chercheur intervenant dans le cadre de plusieurs projets de TPE et projets Maths en Jeans (2010-11), de la 3ème à la Terminale.

Le travail a consisté à présenter aux élèves des sujets de recherche, et à les guider si besoin dans leurs recherches et la préparation de leur présentation. Les thèmes proposés étaient la formule de Pick (qui permet de trouver l'aire d'un polygône dont les sommets sont à coordonnées entières à partir du nombre de points intérieurs et du nombre de points sur la frontière), et le problème des ponts de Koenigsberg.

8. Rédaction de livres et de documents pédagogiques, vulgarisation scientifique

1. Je me suis beaucoup attaché à rédiger des polycopiés complets et clairs correspondants à la majorité de mes cours, et à les mettre à la disposition de mes étudiants. Tous ces polycopiés sont disponibles sur ma page web (dans la section Enseignement).

2. Je rédige également régulièrement quelques textes sans rapport direct avec mon enseignement, afin de proposer aux étudiants (quels qu'ils soient) la possibilité d'approfondir ou d'illustrer un sujet abordé dans les diverses UE. Ces documents sont également disponibles en libre accès sur ma page web (dans la section Textes Divers).

Un texte (niveau L1/L2) proposant une application de l'algèbre linéaire élémentaire aux jeux d'ampoules, a été publié dans le journal Quadrature [**25**].

Enfin, un autre texte introductif (niveau L2) expliquant comment la théorie des corps gauches, et en particulier les corps de quaternions, s'appliquent au design de codes wifis performants paraîtra prochainement dans ce même journal [**28**].

3. J'ai fait deux conférences d'une heure chacune pour les étudiants de MP et MP* au lycée Champollion, à Grenoble.

Activités scientifiques

9. Directions de thèses et de mémoires de M2

9.1. Direction de thèses.

1. J. Ducoat. Invariants cohomologiques et invariants de Witt de groupes de Coxeter (Université de Grenoble). Soutenue le 22 Octobre 2012.

Il est maintenant postdoctorant à Nanyang Technological University, Singapour.

2. R. Slessor. Optimality of codes based on crossed product algebras (University of Southampton). Soutenue en Avril 2011.

Il travaille maintenant sur la sécurité du réseau pour une entreprise basée au Maroc.

9.2. Direction de mémoires de M2.

1. E.-M. Talon. Multiples de G-formes (2010).

2. J. Ducoat. Invariants cohomologiques des algèbres étales (2009).

10. Exposés sur invitation

10.1. Conférences sur invitation (2002-).

1. Juin 2009 : Conférence "Quadratic forms and linear algebraic groups", Oberwolfach

2. Avril 2005 : Conference "Applications of torsors to Galois cohomology and Lie theory", Banff

3. Octobre 2003 : Conférence "Quadratic forms, algebraic groups and related topics", Banff (Canada)

4. Juin 2003 : Conférence "Quadratic forms, algebraic groups and related topics", Lens

5. Mai 2002 : Conférence "Quadratic forms and algebraic groups", Oberwolfach

10.2. Exposés de séminaires (2005-).

1. Séminaire de topologie, Université Paris 13, Novembre 2012

2. Séminaire d'algèbre, Université d'Orléans, Février 2012

3. Séminaire de topologie, Université Paris 13, Juin 2009

4. Séminaire de théorie des nombres, University of Turku, Avril 2008

5. Séminaire d'algèbre, UCL, Louvain-La-Neuve, Juin 2007

6. Séminaire d'algèbre et géométrie, Université de Bâle, Mai 2007

7. Séminaire de Géométrie Algébrique, University of Cambridge, Février 2005

8. Séminaire "Variétés rationnelles", E.N.S., Paris, Janvier 2005

11. Séjours de recherche (sur invitation)

1. 3 semaines à Nanyang Technological University, Singapour (2013).

2. 1 mois à l'EPFL, Lausanne, Suisse (2010)

3. 15 jours à l'Université de Turku, Finlande (2010)

4. 2 mois à Nanyang Technological University, Singapour (2009).

12. Publications

Bibliographie

Livres

[1] *An introduction to Galois cohomology and its applications.* LMS Lecture notes **377**, Cambridge University Press (2010)

[2] *Modules : théorie, pratique...et un peu d'arithmétique !* A paraître aux éditions Calvage et Mounet (Avril 2012)

[3] *Introduction to central simple algebras and their applications to wireless communication.* (avec F.Oggier). AMS Mathematical Surveys and Monographs Series **191** (2013)

Publications dans des revues à comité de lecture

[4] *Calcul des classes de Stiefel-Whitney des formes de Pfister*, Pub.Math. Besançon, Théorie des nombres (96/97-97/98)

[5] *Characterization of hermitian trace forms*, J. of Algebra **210**, 690-696 (1998)

[6] *Réalisation de formes $\mathbb{Z}$-bilinéaires symétriques comme formes trace hermitiennes amplifiées* . J. Th. des Nombres de Bordeaux **12**, 25-36 (2000)

[7] *On hermitian trace forms over hilbertian fields.* Math.Z. **237**, 561-570 (2001)

[8] *On the computation of trace forms of algebras with involution.* Comm. in Algebra **29** (1), 457-463 (2001)

[9] *Autour des formes trace des algèbres cycliques.* Pub. Math. Besançon, Théorie des nombres, 1-9 (1998/2001)

[10] *Divisible subgroups of Brauer groups and trace forms of central simple algebras* (avec D.B Leep). Documenta Math. **6**, 486-500 (2001)

[11] *On the second trace form of central simple algebras in characteristic two* (avec C. Frings). Manuscripta. Math. **106**, 1-12 (2001)

[12] *The discriminant of a symplectic involution* (avec M. Monsurrò and J.-P. Tignol). Pacific J. of Math. **209**, 201-218 (2003)

[13] *Essential dimension : a functorial point of view* (avec G. Favi). Documenta Math. **8** , 279–330 (2003)

[14] *CM-fields and skew-symmetric matrices.* (avec E. Bayer and P. Chuard). Manuscripta Math. **114**, No 3, 351–359 (2004)

[15] *Cohomological invariants and R-triviality of adjoint classical groups* (avec M. Monsurrò and J.-P. Tignol). Math. Z. **248**, No 2, 313–323 (2004)

[16] *Essential dimension of cubics* (avec G. Favi). J. of Algebra **278**, No 1, 199–216 (2004)

[17] *On the notion of canonical dimension for algebraic groups* (avec Z. Reichstein). Adv. in Maths **198**, No. 1, 128–171 (2005)

[18] *On the set of discriminants of quadratic pairs.* J. Pure Appl. Algebra **188**/1-3, 33-44 (2004) (Erratum : J. Pure and Appl. Algebra **195**, No 1, 125–126 (2005))

[19] (avec F.Oggier) *On Improving* 4×4 *Space-Time Codes.* Proceedings of the 40*th* ACSSC conference (2006), 1284 – 1286

[20] *Finiteness of R-equivalence groups of some adjoint classical groups of type* ${}^2D_3$. J. of Algebra **309**, No 1, 360–366 (2007)

[21] *Cohomological invariants of quaternionic skew-hermitian forms.* Archiv der Math. **88** (2007), 434–447

[22] *Serre's Conjecture II for classical groups over imperfect fields.* (avec C. Frings and J.-P. Tignol) J. Pure App. Algebra **211** (2007), 307–341.

[23] (avec F.Oggier) *Space-Time Codes from Crossed Product Algebras of degree 4.* Applied Algebra, algebraic algorithms and error-correcting codes, 90–99, Lecture Notes in Comput. Sci. 4851, Springer, Berlin (2007)

[24] *On the existence of perfect space-time codes (avec F. Oggier).* IEEE Trans. Inform. Theory 55, no 5, 2078–2082 (2009)

[25] *Jeux d'ampoules (ou comment éviter la crise de nerfs à un électricien dépressif à coup d'algèbre linéaire sur* $\mathbb{F}_2$. Quadrature 79, Janvier-Février-Mars 2011.

[26] (avec S. Baek) *Cohomological invariants of central simple algebras of degree 4.* Archiv der Math. **98**, 415–425 (2012)

[27] *Sums of values represented by a quadratic form* (avec N. Grenier-Boley et M. Mahmoudi). Manuscripta Math., May 2012, 1–26

[28] *Corps gauches et codes Wifi.* A paraître dans Quadrature (2014) .

[29] *Algebraic space-time codes based on division algebras with a unitary involution.* A paraître dans Advances in Mathematics of Communication (2014).

Prépublications

[30] (avec N. Markyn et B. Sethuraman) *Fast lattice decodability of space-time codes.* 5 p. Soumis pour publication. (2014)

[31] (avec N. Markyn et B. Sethuraman) *Fast lattice decodability and complexity bounds for space-time codes.*20 p. Soumis pour publication. (2014)

[32] (avec R. Slessor) *Optimality of codes based on crossed product algebras* Version révisée. 40 p. Soumis pour publication. (2014)

13. Travaux scientifiques

Mes travaux s'orientent essentiellement autour de 4 axes principaux.

1. L'étude de certaines formes quadratiques, associées à des algèbres, appelées formes trace : calcul, calculs des invariants classiques, caractérisations diverses. Les articles [4]-[9] issus de ma thèse, ainsis que les articles [10], [11] et [14] concernent ce genre de questions.

2. L'étude des invariants cohomologiques de structures algébriques : définition de nouveaux invariants, détermination de tous les invariants cohomologiques d'un foncteur donné (en particulier pour le foncteur des G-torseurs), construction de structures algébriques dont les invariants sont donnés, applications à des calculs d'obstruction, applications au problème de classification. Ces questions sont abordées dans les articles [12],[15],[18],[26],[22], [21],[20], ainsi que dans le livre [1].

3. L'étude des invariants discrets de structures algébriques : définition de nouveaux invariants, construction de structures algébriques dont les invariants sont donnés, applications diverses. Certains exemples de ces invariants sont définis et étudiés dans [13],[16],[17] et [27], ainsi que dans [1].

4. L'application des algèbres centrales simples et de la théorie des nombres, et des techniques d'algèbre non commutative à la communication sans fil. Les articles [19],[23],[24], [32], [29], [30], [31], ainsi que l'ouvrage [3] sont consacrés à ces questions.

Mots-clés : Structures algébriques, formes quadratiques, formes hermitiennes, algèbres centrales simples avec et sans involution, produits croisés, torseurs sous un groupe algébrique, cohomologie galoisienne, dimension essentielle, dimension canonique , invariants cohomologiques, communication sans fil, codes MIMO.

13.1. Motivations.

13.1.1. *Invariants de structures algébriques.* Ces travaux de recherche sont axés principalement autour des invariants de structures algébriques, avec un intéret particulier pour les invariants cohomologiques de groupes algébriques. Etant donné une classe de structures algébriques (formes quadratiques, cubiques en n variables, torseurs sous un groupe algébriques, algèbres centrales simples...), il est naturel de chercher à les classer à isomorphisme près. Ce genre de problème étant extremement difficile à aborder directement, une méthode naturelle pour l'attaquer est de définir des invariants attachés à ces structures, et de prouver que ces invariants sont suffisants pour la classification. Cette approche a été fructueuse au cours des années, de la classification des formes quadratiques sur $\mathbb{Q}$ par Minkowski à la récente preuve de Voevodsky de la conjecture de Milnor, qui peut Ã[a]tre considérée comme résolvant le problème de classification des formes quadratiques sur un corps quelconque de caractéristique différente de 2.

Afin d'étudier une structure algébrique donnée, il est parfois plus aisé d'étudier son groupe d'automorphismes, et d'essayer d'en déduire des résultats sur la structure elle-mÃ[a]me. L'avantage de cette approche est que ce groupe possède (dans la plupart des cas) une structure de groupe algébrique, et que l'on peut utiliser les outils de géométrie algébrique pour attaquer le problème de classification. De plus, cette approche permet de réinterpreter ces questions en des termes cohomologiques. Par exemple, si q est une forme quadratique de dimension n sur F, le groupe d'automorphismes associé est le groupe orthogonal $\mathbf{O}(q)$ et l'ensemble pointé $H^1(F, \mathbf{O}(q))$ est en correspondance bijective avec les classes d'isomorphismes de formes quadratiques de dimension n. Si G est le groupe d'automorphismes d'une F-algèbre centrale simple à involution (A, σ), l'ensemble pointé $H^1(F, G)$ est en correspondance bijective avec les classes d'isomorphismes d'algèbres à involution devenant isomorphes à (A, σ) sur une clôture séparable F_s du corps F. De plus, par les travaux fondamentaux de Weil, tout groupe classique adjoint absolument simple est isomorphe à la composante connexe d'un tel groupe d'automorphismes lorsque F est de caractéristique différente de 2.

De nombreux invariants de structures algébriques peuvent Ãªtre ainsi considérés comme des invariants cohomologiques. Par exemple, le discriminant des formes quadratiques peut Ãªtre considéré comme une transformation naturelle $H^1(\_, \mathbf{O}(q)) \to H^1(\_, \mu_2)$. D'autres types d'invariants peuvent Ãªtre naturellement associés à des structures algébriques, comme par exemple les $GW - invariants$, qui associent à une structure algébrique une forme quadratique (e.g. la forme trace des algèbres étales ou centrales simples) ou les invariants discrets (e.g la dimension essentielle).

Un problème primordial est la construction d'invariants non triviaux pour une classe de structures algébriques. Cela peut se révéler extremement ardu, comme le montre par exemple la construction de l'invariant de Rost d'un groupe algébrique absolument simple simplement connexe. Pour un invariant donné, plusieurs questions naturelles se posent ensuite : description de l'ensemble des valeurs atteintes par cet invariant, calcul de cet invariant pour une structure algébrique donnée, résolution du problème de classification. Certaines de ces questions ne sont pas indépendantes. Par exemple, la construction d'un invariant cohomologique non trivial (au sens fort) permet de borner inférieurement la dimension essentielle d'un groupe algébrique. Un intéret supplémentaire de l'étude de ces invariants est leur éventuelle interaction avec d'autres problèmes, comme nous le verrons plus loin. Par exemple, la théorie des formes trace hermitiennes amplifiées des algèbres étales à involution permet de donner des théorèmes de structures des corps CM, et les invariants cohomologiques de groupes algébriques permettent de donner des obstructions à la stable rationalité de ces groupes. Enfin la dimension canonique d'un groupe algébrique G est reliée étroitement au degré de transcendance de corps de déploiement générique de G-torseurs.

Signalons également que Serre a prouvé que l'invariant de Witt de la forme trace d'une extension galoisienne caractérise l'obstruction à un certain problème de plongement galoisien ; ce résultat a été utilisé par de nombreux mathématiciens pour résoudre le problème de Galois inverse dans de nombreux nouveaux cas. De plus, l'existence d'un invariant non ramifié non nul pour un groupe fini G implique le problème de Noether a une réponse négative pour ce groupe. Ce fait a permis à Serre de construire de nouvelles familles de groupes finis pour lesquels le problème de Noether sur $\mathbb{Q}$ admet une réponse négative. Enfin les propriétés de l'invariant de Rost ont permis à Bayer et Parimala de montrer le principe de Hasse pour les groupes classiques simplement connexes définis sur un corps de dimension cohomologique virtuelle au plus 2.

Pour finir, notons que la notion d'invariant peut Ãªtre naturellement défini plus généralement pour des foncteurs. Le point de vue fonctoriel étant utilisé dans l'étude la dimension essentielle, nous rappelons maintenant pour clôre cette section la définition des diverses sortes d'invariants mentionnées plus haut dans ce cadre plus général.

Soit k un corps, et soit $\mathfrak{C}_k$ la catégorie des extensions de corps de k. Soit $\mathbf{F} : \mathfrak{C}_k \to \mathbf{Ens}$ un foncteur covariant.

Un invariant cohomologique de $\mathbf{F}$ de degré d à valeurs dans un Γ_k-module discret M est une transformation naturelle de foncteurs $\mathbf{F} \to H^d(\_, M)$.

Lorsque $\mathbf{F} = H^1(\_, G)$, on suppose que l'invariant est normalisé, c'est-à-dire qu'il envoie le cocycle trivial sur le cocycle trivial. On note par $\mathrm{Inv}^d(G, M)$ le groupe des invariants normalisés.

Un GW-invariant de $\mathbf{F}$ est une transformation naturelle de foncteurs $\mathbf{F} \to GW(\_)$, où $GW(E)$ est le groupe de Grothendieck-Witt du corps E.

Un invariant discret de $\mathbf{F}$ est une application $\mathbf{F} \to \mathbb{Z} \cup \{\pm\infty\}$.

13.1.2. *Algèbres centrales simples et communication sans fil.* Supposons que l'on veuille transmettres des symboles d'information sans utiliser aucun câble. Typiquement, c'est le cas lorsque l'on utilise un téléphone portable ou une connection Internet sans fil. Durant la transmission, deux phénomènes peuvent se produirent : une atténuation du signal, due par exemple aux obstacles rencontrés comme des arbres ou des batîments (c'est pourquoi la voix peut sembler plus faible lors d'une conversation téléphonique), et une perturbation du signal due à l'addition de bruit (causant de la "friture"). Ainsi l'information récupérée par le récepteur diffère de l'information originale.

Le problème est donc d'encoder l'information et de la transmettre de façon à mininimiser la probabilité d'erreur. Bien sûr, un moyen de procéder est de transmettre la mÃ$^{\text{a}}$me information pplusieurs fois de suite, mais cela un coût au niveau de la mémoire nécessaire, ainsi qu'un coû énergétique, et peu d'information est transmise, et ce procédé de transmission n'est donc pas satisfaisant.

Supposons que l'on a deux antennes émettrices et deux antennes réceptrices. Les symboles d'information qui sont transmis sont des nombres complexes. Chaque antenne émettrice envoie un symbole d'information qui sera envoyé par deux chemins différents reçu par chaque antenne réceptrice. En pratique, on peut supposer que les propriétés du réseau ne changent pas au cours de deux utilisations successives.

Lors de la première utilisation, la première antenne envoie x_0 et la seconde envoie x_2. Chaque de ces symboles sont envoyés à travers les deux chemins possibles et sont reus par les deux antennes réceptrices.

Le symbole x_0 est reçu par la premi‘ère antenne comme étant $h_1 x_0$ et par la seconde comme étant $h_3 x_0$, où h_1, h_3 sont des coefficients représentant l'atténuation du signal. Le symbole x_2 est reçu par la premi‘ère antenne comme étant $h_2 x_0$ et par la seconde comme étant $h_4 x_0$, où h_2, h_4 sont aussi des coefficients représentant l'atténuation du signal.

Ainsi, la première antenne réceptrice reçoit un signal y_0 qui est la somme de 3 différents signaux : $h_1 x_0, h_3 x_1$ et du bruit ν_1, donc

$$y_0 = h_1 x_0 + h_3 x_2 + \nu_1.$$

De mÃ$^{\text{a}}$me, la seconde antenne réceptrice reçit un signal y_2 de la forme

$$y_2 = h_2 x_0 + h_4 x_2 + \nu_2.$$

Lors de la seconde utilisation, la première antenne envoie x_1 et la seconde envoie x_3. Comme le réseau ne change pas entre les deux utilisations, les coefficients d'atténuation sont les mÃ$^{\text{a}}$mes, et les deux antennes recevront

respectivement des signaux y_1 et y_3 de la forme

$$y_1 = h_1 x_1 + h_3 x_3 + \nu_3$$

et

$$y_3 = h_2 x_1 + h_4 x_3 + \nu_4.$$

Ainsi, en posant

$$H = \begin{pmatrix} h_1 & h_3 \\ h_2 & h_4 \end{pmatrix}, N = \begin{pmatrix} \nu_1 & \nu_3 \\ \nu_2 & \nu_4 \end{pmatrix}$$

et

$$X = \begin{pmatrix} x_0 & x_1 \\ x_2 & x_3 \end{pmatrix}, Y = \begin{pmatrix} y_0 & y_1 \\ y_2 & y_3 \end{pmatrix},$$

on obtient l'équation matricielle

$$Y = HX + N.$$

Les matrices H et N sont des matrices aléatoires suivant une loi gaussienne. Nous envoyons ainsi une matrice $X \in M_2(\mathbb{C})$, et nous recevons une matrice $Y \in M_2(\mathbb{C})$. Le récepteur est supposé connaître l'ensemble $\mathcal{C}$ de toutes les matrices X qui sont envoyées, appelé le *code*. Un élement $X \in \mathcal{C}$ est appelé un *mot de code*. Le récepteur connaît aussi le réseau, c'est-à-dire la matrice H. Le problème majeur est que $Y \notin \mathcal{C}$ en général. Comment décoder ? C'est-à-dire, comment trouver un mot de code $\hat{X} \in \mathcal{C}$ à partir de Y, de sorte que la probabilité $\mathbb{P}(X \to \hat{X})$ d'envoyer X et de décoder $\hat{X} \neq X$ est aussi petite que possible ?

Le procédé est le suivant : pour tout $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, on pose

$$||M||_2 = \sqrt{|a|^2 + |b|^2 + |c|^2 + |d|^2}.$$

Le mot de code $\hat{X}$ sera un mot de code tel que $||Y - HX'||_2$ soit minimal parmi touts les mots de code $X' \in \mathcal{C}$ (si on a plusieurs mots de code satisfaisant cette condition, on en choisit un au hasard). Le récepteur peut toujours calculer $\hat{X}$ puisqu'il connaît $\mathcal{C}$ et H.

On a alors

$$\mathbb{P}(X \to \hat{X}) \leq \frac{C}{\min\limits_{X \neq X' \in \mathcal{C}} |\det(X - X')|^4},$$

où C est une constante ne d
'ependant que du réseau et X, X' parcourent $\mathcal{C}$. Ainsi la question suivante est maintenant : comment choisir $\mathcal{C}$? Le critère est : fiabilité ! Pour avoir une borne supériere intéressante, et pour s'assurer que $\mathbb{P}(X \to \hat{X})$ soit petite, nous devons maximiser $\min\limits_{X \neq X' \in \mathcal{C}} |\det(X - X')|^4$, la première étape étant de s'assurer que $\mathcal{C}$ est choisi de façon à ce que $\det(X - X') \neq 0$ pour tout $X \neq X'$.

La difficulté principale est la non-linéarité du déterminant. L'idée est de prendre pour $\mathcal{C}$ un sous-ensemble fini d'un sous-anneau D de $M_2(\mathbb{C})$ qui est aussi un anneau à division. On aura ainsi $X - X' \in D \backslash \{0\}$ puisque D est un anneau, et le fait que D est à division assurera que $X - X'$ est inversible

dans D, donc dans $M_2(\mathbb{C})$, ce qui veut dire que l'on aura $\det(X - X') \neq 0$ pour tout $X \neq X' \in C$.

Tout ce qui précède peut-Ã[a]tre généralisé à un plus grand nombre d'antennes, et la question devient : : comment construire un code sur un sous-anneau à division de $M_n(\mathbb{C})$, tel que $\delta_{min}(\mathcal{C}) \min_{X \neq 0 \in \mathcal{C}} |\det(X)|$ soit aussi grand que possible ?

Un moyen d'y parvenir est d'utiliser des algèbres centrales simples à division sur un corps de nombres K. En effet, si D est une telle algèbre, on sait alorss qu'il existe une extension finie L/K L telle que $D \otimes_K L \simeq M_n(L)$. On obtient alors immédiatement une injection $D \hookrightarrow M_n(L) \subseteq M_n(\mathbb{C})$.

Remarquons néanmoins que ce n'est que le premier pas. Le codage doit tenir compte d'autres difficultés, parmi lesquelles :

(1) *l'encodage*, c'est-à-dire la façon dont les symboles d'informations sont envoyés sous forme matricielle ,

(2) *le taux d'information*, c'est-à-dire le nombre de matrices que nous pouvons construire enfonction du nombre de symboles envoyés et du nombre d'antennes émettrices,

(3) *le décodage*, c'est-à-dire comment récupérer les symboles d'information à partir de la matrice reçue

(4) *les coûts énergétiques.*

La construction de codes efficaces sur des algèbres à division est assez délicate, mais des codes intéressants ont déjà été construits sur des algèbres cycliques.

14. Description des travaux

14.1. ***GW*-invariants.** Soit A une algèbre centrale simple sur un corps F arbitraire. Si $a \in A$, et si $\mathrm{Prd}_A(a) := X^n - s_1 X^{n-1} + s_2 X^{n-2} + \cdots$ est son polynôme caractéristique réduit, on définit la trace réduite de a et la seconde trace réduite de a respectivement par $\mathrm{Trd}_A(a) = s_1$ et $\mathrm{Srd}_A(a) := s_2$. On note alors $\mathcal{T}_A$ la forme quadratique

$$a \in A \mapsto \mathrm{Trd}_A(x^2)$$

et on note $\mathcal{T}_{2,A}$ la forme quadratique

$$a \in A \mapsto \mathrm{Srd}_A(a).$$

Cela fournit des *GW*-invariants des algèbres centrales simples dès que ces formes sont non dégénérées.

• Dans [10], on prouve ses résultats de réalisation de formes trace d'algèbres centrales simples. Dans la suite, F désignera un corps de caractéristique différente de 2, et $K = F(\sqrt{-1})$. Si F est un corps, $I^n(F)$ désignera la nième puissance de l'idéal fondamental de l' anneau de Witt de F, et Ω_F désignera l'espace des ordres de F.

Dans une première partie, nous étudions la structure du sous-groupe de torsion de la partie 2-primaire du groupe de Brauer. Nous obtenons ainsi le

théorème de structure suivant, qui généralise celui bien connu pour les corps de nombres :

THÉORÈME 1. *Soit F un corps satisfaisant la propriété d'approximation forte et tel que $I^3(F)_t = 0$. Soit T (resp. Λ) un ensemble d'indices d'une $\mathbb{Z}/2\mathbb{Z}$-base de $\mathrm{Br}_2(F)_t$ (resp. de $F^\times/\sum F^{\times 2}$). Alors on a un isomorphisme de groupes :*

$$ {}_2\,\mathrm{Br}(F) \simeq \mathbb{Z}(2^\infty)^{(T)} \times (\mathbb{Z}/2\mathbb{Z})^{(\Lambda)}. $$

Rappelons qu'un corps F vérifie la propriété d'approximation forte si pour tout sous-ensemble $X \subset \Omega_F$ ouvert et fermé il existe $a \in F^\times$ tel que a est positif par rapport à tout ordre de X et négatif par rapport à tout ordre de X^c.

Comme application, nous caractérisons complètement les formes quadratiques pouvant se réaliser comme formes trace d'une F-algèbre centrale simple de degré n sur certains corps. Nous obtenons ainsi les résultats suivants :

THÉORÈME 2. *Soit $n = 2m \geq 2$ un entier pair. Supposons que $I^2(K) = 0$. Alors une forme quadratique q sur F est isomorphe à la forme trace d'une algèbre centrale simple de degré n si et seulement si les conditions suivantes sont satisfaites :*

(1) $\dim q = n^2$
(2) $\det q = (-1)^{\frac{n(n-1)}{2}}$
(3) $\mathrm{sign}_v q = \pm n$, *pour tout* $v \in \Omega_F$.

THÉORÈME 3. *Supposons que F vérifie les conditions suivantes :*

(a) *$I^3(F)$ est sans torsion*
(b) *Pour tout $r \geq 0$ and tout $[A] \in \mathrm{Br}(F)$ tels que $2^{r+1}[A] = 0$, il existe A', $\deg A' = 2^{r+1}$ telle que $[A'] = [A]$.*

Alors une forme quadratique q sur F est isomorphe à la forme trace d'une algèbre centrale simple de degré n si et seulement si les conditions suivantes sont satisfaites :

(1) $\dim q = n^2$
(2) $\det q = (-1)^{\frac{n(n-1)}{2}}$
(3) $\mathrm{sign}_v q = \pm n$, *pour tout* $v \in \Omega_F$.

En particulier, ce résultat est valable pour les corps locaux, les corps globaux ou les corps de fractions des anneaux locaux excellents de dimension 2, avec un corps résiduel algébriquement clos de caractéristique nulle (e.g. les extensions finies de $\mathbb{C}((X,Y))$).

Les preuves de ces théorèmes de réalisation sont basés sur les théorèmes de classification des formes quadratiques sur des corps F vérifiant $I^2(F)_t = 0$ ou $I^3(F)_t = 0$, ainsi que sur le théorème de structure précédent.

• Dans [11], nous nous interessons à la forme seconde trace des F-algèbres centrales simples lorsque $\mathrm{car}(F) = 2$, et au calcul de son discriminant et de

son invariant de Clifford. Lorsque $\mathrm{car}(F) \neq 2$, cet invariant ne donne pas plus d'information que la forme trace elle-mÃªme, puisque $\mathcal{T}_A \simeq \mathcal{T}_B \iff \mathcal{T}_{2,A} \simeq \mathcal{T}_{2,B}$. Lorsque $\mathrm{car}(F) = 2$, la forme trace est de rang nul, mais la forme seconde trace est non singulière. Les mÃªmes phénomènes se produisent pour les formes trace et formes seconde trace associées aux algèbres étales. Par ailleurs Bergé et Martinet ont montré que la forme seconde trace d'une algèbre étale sur un corps de caractéristique 2 était entièrement déterminé par son invariant de Arf, montrant ainsi que cette forme est un très mauvais substitut à la forme trace. On peut se demander s'il en est de mÃªme dans le cas des algèbres centrales simples. Lorsque $\mathrm{car}(F) \neq 2$, le discriminant et l'invariant de Clifford de $\mathcal{T}_A$ ont été calculés par de nombreux auteurs. En particulier, le discriminant de la forme trace ne dépend que du degré de A et son invariant de Clifford ne dépend que de $\frac{n}{2}[A]$ (lorsque n est pair).

Nous prouvons dans [11] un résultat analogue pour la seconde trace en caractéristique 2 (montrant ainsi que la forme seconde trace est un bon substitut à la forme trace dans ce cas).

Avant d'énoncer le résultat, introduisons quelques notations.

Soit F un corps de caractéristique 2. On note $\wp(F)$ le groupe $\{x^2 + x, x \in F\}$. Si $\alpha \in F^\times$ et $\beta \in F$, on dénote par $(\alpha, \beta]$ l'algèbre de quaternions correspondante, ainsi que sa classe dans le groupe de Brauer par abus de notation. Cette algèbre a pour F-basis $1, e, f, ef$ où relations $e^2 = \alpha$, $f^2 + f = \beta$ and $ef + fe = e$. Si $a, b \in F$, on note $[a, b]$ la forme quadratique $(x, y) \in K^2 \mapsto ax^2 + xy + by^2$. Une forme quadratique non dégénérée sur F est de dimension paire et est isomorphe à une somme orthogonale de formes $[a, b]$. Si $q \simeq [a_1, b_1] \perp \cdots \perp [a_r, b_r]$, *l'invariant de Arf de* q est l'élément de $F/\wp(F)$ défini par $\mathrm{Arf}(q) := a_1b_1 + \cdots + a_rb_r + \wp(F)$. On définit aussi *l' invariant de Clifford* q, noté $c(q)$, comme étant la classe de l'algèbre de Clifford de q dans le groupe de Brauer.

On a alors :

Théorème 4. *Soit F un corps de caractéristique 2, et soit A une algèbre centrale simple de degré n pair. Alors la forme quadratique $\mathcal{T}_{2,A}$ est non dégénérée, et on a :*

(1) $\mathrm{Arf}(\mathcal{T}_{2,A}) = \mathrm{Arf}(\mathcal{T}_{2,M_n(F)}) = [\frac{n}{4}]$
(2) *L'invariant de Clifford de la seconde trace est donné par* $c(\mathcal{T}_{2,A}) = \frac{n}{2}[A]$

• Dans [14], nous utilisons la théorie des formes trace hermitiennes amplifiées pour montrer qu'un corps CM de degré $2n$ sur $\mathbb{Q}$ est engendré par une valeur propre d'une matrice anti-symétrique à coefficients rationnels de dimension au plus $2n+3$, ce qui améliore un résultat de Cohen et Odoni. Nous utilisons pour cela un résultat prouvé dans [7].

Rappelons qu'un corps de nombres K est appelé *corps CM* s'il est de la forme $K = F(\sqrt{-\theta})$, où $F/\mathbb{Q}$ est totalement réelle et où $\theta \in F^\times$ est totalement positif. Cohen et Odoni ont montré que $\sqrt{-\theta}$ était valeur propre d'une matrice antisymétrique à coefficients rationnels de dimension au plus $4n + 2$, où $[K : \mathbb{Q}] = 2n$.

Dans [14], nous prouvons le résultat suivant :

THÉORÈME 5. (1) *Si $n \equiv 3[4]$, $\sqrt{-\theta}$ est valeur propre d'une matrice antisymétrique M à coefficients rationnels de dimension $2n+1$, et cette borne est optimale.*

(2) *Si $n \equiv 1[4]$, $\sqrt{-\theta}$ est valeur propre d'une matrice antisymétrique M à coefficients rationnels de dimension $2n+3$, et cette borne est optimale si l'on exige de plus que le polynôme caractéristique de M soit séparable.*

(3) *Si n est pair, $\sqrt{-\theta}$ est valeur propre d'une matrice antisymétrique M à coefficients rationnels de dimension $2n+4$.*

La stratégie de la preuve est la suivante : si f désigne le polynôme irréductible de $\sqrt{-\theta}$ sur $\mathbb{Q}$, alors f divise le polynôme caractéristique de M, qui est nécessairement pair ou impair. Le problème revient alors à savoir si on peut trouver un polynôme P divisible par f de degré $2n+1, 2n+3$ ou $2n+4$ qui se réalise comme polynôme caractéristique d'une telle matrice.

On utilise alors le résultat suivant :

PROPOSITION 6. *Soit k un corps de caractéristique différente de 2, et soit $P \in k[X]$ un polynôme séparable de degré m, satisfaisant $P(-X) = \pm P(X)$. Soit $E = k[X]/(P)$ et soit σ l'involution sur E définie par $\sigma(X) = -X$.*

Alors P est le polynôme caractéristique d'une matrice antisymétrique à coefficients dans k de dimension m si et seulement s'il existe un élément σ-symétrique $\lambda \in E^\times$ tel que $\mathrm{Tr}_{E/k}(\lambda x x^\sigma)$ soit isomorphe à la forme unité.

14.2. Invariants cohomologiques. On décrit dans cette partie les résultats obtenus sur les invariants cohomologiques de structures algébriques.

Rappelons tout d'abord quelques définitions. Soit A une algèbre centrale simple de centre K. Une involution σ sur A est un anti-automorphisme de A d'ordre 2.

On note F le sous-corps de K des éléments fixés par σ.

Une involution σ est dite *de première espèce* si $\sigma_{|K} = \mathrm{Id}_K$, et (de type) *unitaire* sinon. Dans le premier cas, $K = F$, et dans le second cas, K/F est une extension quadratique séparable et $\sigma_{|K}$ est l'unique F-automorphisme non trivial de K.

Si $A = \mathrm{End}(V)$, toute involution de première espèce est adjointe à une forme bilinéaire symétrique non alternée ou à une forme bilinéaire alternée. Si A est arbitraire et si σ est une involution de première espèce, on dit que σ est *orthogonale* (ou de type orthogonal), respectivement (de type) *symplectique* si $\sigma \otimes \mathrm{Id}_{F_s}$ est adjointe à une forme bilinéaire symétrique non alternée, respectivement à une forme bilinéaire alternée.

Supposons que $\mathrm{car}(F) \neq 2$. Si σ est orthogonale et A est de degré pair, on pose

$$\mathrm{disc}(\sigma) = \mathrm{Nrd}_A(u) \in F^\times / F^{\times 2},$$

où $u \in A^\times$ satisfait $\sigma(u) = -u$. La classe $\mathrm{disc}(\sigma)$ est appelé *le discriminant de* σ.

Si σ est unitaire, on peut définir une F-algèbre centrale simple $D(A,\sigma)$ d'exposant au plus 2, appelé *l'algèbre discriminante*. L'application $\sigma \mapsto [D(A,\sigma)]$ fournit ainsi un invariant cohomologique de degré 2 à valeurs dans $\mathbb{Z}/2\,\mathbb{Z}$ des involutions unitaires sur A. On peut montrer qu'il n'existe pas d'invariants cohomologiques de degré 1.

Si (A,σ) est une algèbre à involution, on dit que σ est *hyperbolique* s'il existe $e \in A$ tel que $e^2 = e$ et $\sigma(e) = 1 - e$.

Pour toute algèbre à involution, on définit le schéma en groupes des similitudes de (A,σ), noté $\mathbf{Sim}(A,\sigma)$, par

$$\mathbf{Sim}(A,\sigma)(R) = \{u \in A \otimes_F R \mid (\sigma \otimes \mathrm{Id})(u)u \in R^\times\}$$

pour toute F-algèbre commutative R, et on définit le schéma en groupes des similitudes projectives de (A,σ), noté $\mathbf{PSim}(A,\sigma)$ par

$$\mathbf{PSim}(A,\sigma) = \mathbf{Sim}(A,\sigma)/R_{K/F}(\mathbb{G}_{\mathrm{m},K})$$

On désigne par $\mathbf{Sim}^+(A,\sigma)$ et $\mathbf{PSim}^+(A,\sigma)$ la composante connexe du neutre de ces groupes.

Si $g \in \mathbf{Sim}(A,\sigma)(F)$, on pose $\mu(g) = \sigma(g)g \in F^\times$. On dit que g est *propre* si $g \in \mathbf{Sim}^+(A,\sigma)(F)$ et *impropre* sinon. Les similitudes impropres n'existent éventuellement que pour les involutions orthogonales, les groupes de similitudes étant connexes dans les deux autres cas.

Deux involutions σ et σ' sur A sont dite *conjuguées* s'il existe $a \in A^\times$ tel que $\sigma' = \mathrm{Int}(a) \circ \sigma \circ \mathrm{Int}(a)^{-1}$.

L'ensemble de cohomologie $H^1(F, \mathbf{Sim}(A,\sigma))$ est alors en correspondance bijective avec les classes de conjugaison d'involutions sur A de mÃªme type que σ.

• Contrairement au cas des involutions orthogonales, où des analogues du discriminant et de l'algèbre de Clifford des formes quadratiques sont définis, aucun invariant cohomologique associé aux involutions symplectiques n'avait été construit jusqu'à présent.

Dans [12], nous définissons un invariant cohomologique appelé *discriminant*, associé à une involution symplectique σ sur une F-algèbre centrale simple A de degré $2m$, noté $\Delta(\sigma)$, et à valeurs dans $H^3(F,\mu_2)$, de la manière suivante.

Rappelons tout d'abord que, si θ est une involution symplectique sur A, la norme réduite pfaffienne est la fonction polynomiale homogène de degré m

$$\mathrm{Nrp}_\theta \colon \ \mathrm{Sym}(A,\theta) \to F$$

uniquement déterminée par les conditions suivantes :

$$\mathrm{Nrp}_\theta(1) = 1 \qquad \text{and} \qquad \mathrm{Nrp}_\theta(x)^2 = \mathrm{Nrd}_A(x) \qquad \text{for } x \in \mathrm{Sym}(A,\theta).$$

On suppose que $\mathrm{car}(F) \neq 2$, et que A possède une involution hyperbolique symplectique θ, ce qui revient à dire que $A \simeq M_2(A_0)$, où A_0 est une algèbre centrale simple d'exposant au plus 2.

DÉFINITION. Soit A une F-algèbre centrale simple de degré $n = 2m \equiv 0 \bmod 4$ possédant une involution symplectique hyperbolique θ. Soit σ une involution symplectique sur A. Il existe $s \in \mathrm{Sym}(A,\theta)^\times$ tel que

$$\sigma = \mathrm{Int}(s) \circ \theta$$

On définit le *discriminant* de σ, noté $\Delta(\sigma)$, en posant

$$\Delta_\theta(\sigma) := \big(\mathrm{Nrp}_\theta(s)\big)_2 \cup [A] \in H^3(F,\mu_2).$$

On montre que cette quantité ne dépend que de la classe de conjugaison de σ. Cet invariant est le premier invariant non trivial associé aux involutions symplectiques. On montre d'ailleurs qu'il n'existe pas d'autre invariant cohomologique de degré 3 à valeurs dans $\mathbb{Z}/2\,\mathbb{Z}$ associé aux involutions symplectiques. Plus précisement, on a :

PROPOSITION 7. *Soit (A,θ) une algèbre à involution symplectique.*

Si A est déployée, on a $H^1\big(L, \mathbf{Sim}(A,\theta)\big) = 1$ pour tout $L \in \mathfrak{C}_F$, et donc

$$\mathrm{Inv}^d(\mathbf{Sim}(A,\theta), \mathbb{Z}/2\mathbb{Z}) = 0 \qquad \textit{pour tout } d.$$

Si A n'est pas déployée, on a

$$\mathrm{Inv}^d(\mathbf{Sim}(A,\theta), \mathbb{Z}/2\mathbb{Z}) = 0 \qquad \textit{pour } d = 1,\ 2$$

et

$$\mathrm{Inv}^3((\mathbf{Sim}(A,\theta), \mathbb{Z}/2\mathbb{Z}) = \begin{cases} 0 & \textit{si } \deg A \equiv 2 \mod 4, \\ \mathbb{Z}/2\mathbb{Z} & \textit{si } \deg A \equiv 0 \mod 4. \end{cases}$$

Dans le cas des involutions orthogonales et unitaires sur des algèbres de degré 4, la nullité du discriminant et de l'algèbre discriminante est équivalente à la décomposabilité de ces involutions en produit tensoriel de deux algèbres à involution. Dans le cas des involutions symplectiques, une telle décomposition existe toujours en degré 4. On peut alors se demander si la trivialité du discriminant est reliée à la décomposition des involutions symplectiques sur des algèbres de degré 8. La réponse est affirmative, et on montre dans [**12**] le résultat de décomposabilité suivant :

THÉORÈME 8. *Soit A une F-algèbre centrale simple de degré 8 possédant une involution symplectique hyperbolique. Pour toute involution symplectique σ sur A, $\Delta(\sigma) = 0$ si et seulement s'il existe une décomposition*

$$(A,\sigma) = (A_1,\sigma_1) \otimes_F (A_2,\sigma_2) \otimes_F (A_3,\gamma_3)$$

où A_1, A_2, A_3 sont des sous-algèbres de quaternions de A, σ_1, σ_2 sont des involutions orthogonales sur A_1 et A_2 respectivement, γ_3 est l'involution canonique sur A_3, et A_1 est déployée,

$$A_1 \simeq M_2(F).$$

• Si X est une variété irréductible définie sur F, on dit que X est *rationnelle* si X est birationellement équivalente à un espace affine, et *stablement rationnelle* s'il existe $m \geq 0$ tel que $X \times \mathbb{A}^m_F$ soit rationnelle. Un problème naturel est de savoir si une variété X donnée est (stablement) rationnelle ou non.

Lorsque X est un groupe algébrique linéaire, Manin a défini une obstruction à la rationnalité comme suit :

si G est un groupe algébrique linéaire défini sur F, on dit que $g \in G(F)$ est R-trivial s'il existe une application rationnelle $f : \mathbb{A}^1_F \dashrightarrow G(F)$, définie aux points 0 et 1, telle que $f(0) = 1$ et $f(1) = g$. On note $RG(F)$ le sous-groupe normal des éléments R-triviaux de $G(F)$. Le groupe quotient est noté $G(F)/R$, et appelé le groupe de R-équivalence de G.

Le groupe G est alors dit R-trivial si pour toute extension E/F, $G(E)/R = 1$. Un groupe connexe stablement rationnel comme variété est alors R-trivial.

Très peu de résultats sur la rationnalité des groupes adjoints absolument simples étaient connus jusqu'à présent. Les groupes de type ${}^1A_{n-1}$ et B_n sont rationnels, et les groupes de type ${}^2A_{n-1}$ et C_n pour n impair sont stablements rationnels. D'autre part, Merkurjev a donné des exemples de groupes de type ${}^2D_n$ non R-triviaux (donc non stablement rationnels) pour tout $n \geq 3$.

Dans [15], nous donnons les premieres familles de groupes adjoints absolument simples de type C_n, ${}^2A_{n-1}$ et ${}^1D_n$ avec n pair, qui sont non R-triviaux, donc non stablement rationnels.

Rappelons qu'un groupe adjoint absolument simple de type classique est isomorphe à $\mathbf{PSim}^+(A, \sigma)$. Le type ${}^2A_{n-1}$ correspond à $\deg A = n$ et σ unitaire, le type C_n à $\deg A = 2n$ et σ symplectique, et le type ${}^1D_n$ à $\deg A = 2n$ et σ orthogonale de discriminant trivial.

Nous avons alors précisement les résultats suivants :

THÉORÈME 9. *Soient Q, H des F-algèbres de quaternions ($\mathrm{car}(F) \neq 2$) satisfaisant*

$$(-1) \cup [H] = 0 \text{ in } H^3(F, \mu_2) \qquad \text{et} \qquad [H] \cup [Q] \neq 0 \text{ in } H^4(F, \mu_2).$$

Soit $A = M_{2r}(H) \otimes M_s(Q)$, où r est arbitraire et s est impair. Soit ρ une involution orthogonale sur $M_{2r}(H)$ possédant des similitudes impropres, et soit τ une involution de première espèce sur $M_s(Q)$. Alors $\mathbf{PSim}^+(A, \rho \otimes \tau)$ n'est pas R-trivial.

THÉORÈME 10. *Soit r un entier arbitraire. Soit H une F-algèbre de quaternions ($\mathrm{car}(F) \neq 2$), $\alpha \in F^\times$, $K = F[X]/(X^2 - \alpha)$, et soit ι l'automorphisme non trivial de K/F. On suppose que*

$$(-1) \cup [H] = 0 \text{ in } H^3(F, \mu_2) \qquad \text{et} \qquad (\alpha) \cup [H] \neq 0 \text{ in } H^3(F, \mu_2).$$

Soit ρ une involution orthogonale sur $M_{2r}(H)$ possédant des similitudes impropres. Alors $\mathbf{PSim}^+(M_{2r}(H) \otimes_F K, \rho \otimes \iota)$ n'est pas R-trivial.

L'existence d'une involution orthogonale ρ sur $M_{2r}(H)$ possédant une similitude impropre est assurée par la condition $(-1) \cup [H] = 0$. En fait, on peut montrer qu'une algèbre A de degré pair admettant des involutions de première espèce possède une involution orthogonale ρ avec des similitudes impropres si et seulement A est d'indice au plus 2 et si $(-1) \cup [A] = 0$ lorsque $n \equiv 0[4]$.

La stratégie de la construction de ces exemples est la suivante : l'idée est de définir un morphisme non trivial $\theta : \mathbf{PSim}^+(A,\sigma) \to H^*(\_, \mathbb{Z}/2\mathbb{Z})$ qui s'annule sur les éléments R-triviaux.

Ce morphisme induit alors par passage au quotient un morphisme

$$\overline{\theta} : \mathbf{PSim}^+(A,\sigma)(\_)/R \to H^*(\_, \mathbb{Z}/2\mathbb{Z})$$

ayant une image non triviale, ce qui entraîne a fortiori la non R-trivialité du groupe $\mathbf{PSim}^+(A,\sigma)$.

Pour définir ce morphisme θ, on utilise des invariants cohomologiques du groupe $\mathbf{Sim}(A,\sigma)$.

Lorsque σ est unitaire, le morphisme θ est donné par

$$\theta_E : g \in \mathbf{PSim}^+(A,\sigma)(E) \to (\mu(g)) \cup [D(A,\sigma)] \in H^3(E, \mathbb{Z}/2\mathbb{Z}),$$

pour toute extension de corps E/F.

Lorsque σ est de première espèce, on définit un nouvel invariant cohomologique de degré 3.

Soit $\mathcal{T}_\sigma^+$ la restriction de la forme trace à l'espace des éléments σ-symétriques. On a alors le lemme suivant :

LEMME 11. *Soient σ, σ_0 deux involutions de première espèce sur A.*

- *Si σ et σ_0 sont symplectiques, alors $T_\sigma^+ - T_{\sigma_0}^+ \in I^3F$.*
- *Si σ et σ_0 sont orthogonales, et si $\operatorname{disc}\sigma = \operatorname{disc}\sigma_0$, alors $T_\sigma^+ - T_{\sigma_0}^+ \in I^3F$.*

On obtient alors un invariant cohomologique non trivial de degré 3 en prenant l'invariant d'Arason de $T_\sigma^+ - T_{\sigma_0}^+$.

On définit alors θ par

$$\theta_E : g \in \mathbf{PSim}^+(A,\sigma)(E) \to (\mu(g)) \cup e_3(T_\sigma^+ - T_{\sigma_0}^+) \in H^4(E, \mathbb{Z}/2\mathbb{Z}),$$

pour toute extension de corps E/F, où σ_0 est hyperbolique et $d(\sigma) = 1$.

On montre alors que le morphisme θ obtenu est non trivial en prouvant que $\theta(g_0 \otimes 1) \neq 0$ si g_0 est une similitude impropre de ρ, et qu'il se factorise par R-equivalence en utilisant la description explicite du groupe R-equivalence de $\mathbf{PSim}^+(A,\sigma)$ obtenue par Merkurjev.

Une autre question naturelle concernant la R-équivalence est la suivante : soit G un groupe algébrique défini sur k. Si G n'est pas R-trivial, $G(k)/R$ est-il fini ou infini ? Il a été conjecturé par Colliot-Thélène et Sansuc que si k un corps finiment et séparablement engendré sur son sous-corps premier. alors pour tout groupe réductif défini sur k le groupe $G(k)/R$ est fini. A part lorsque k est un corps global (auquel cas, la conjecture est vraie), aucun exemple ou contre-exemple à cette conjecture est connu.

Dans [20], on construit des familles de groupes adjoints G of type ${}^2D_3$ définis sur un corps F tels que $G(F)/R$ est fini, pour des corps F qui sont finiment engendrés sur leur sous-corps premiers. On construit aussi des familles de groupes G pour lesquels $G(F)/R \simeq \mathbb{Z}/2\mathbb{Z}$ lorsque $F = k(t)$, et k est un corps arbitraire. Cela donne les premiers exemples de groupes adjoints G qui ne

sont pas semi-déployés ou définis sur un corps global, tels que $G(F)/R$ soi un groupe fini non trivial.

• Soit F un corps de caractéristique 2, et soit A une F-algèbre centrale simple munie d'une involution de première espèce.

Une paire quadratique sur A est un couple (σ, f), où σ est une involution symplectique sur A et $f : \mathrm{Sym}(A,\sigma) \to F$ est une forme linéaire satisfaisant

$$f(a+\sigma(a)) = \mathrm{Trd}_A(a) \text{ pour tout } a \in A.$$

Par exemple, si σ est une involution symplectique sur A, alors pour tout $\ell \in A$ tel que $\ell+\sigma(\ell) = 1$, le couple (σ, f), où $f : s \in \mathrm{Sym}(A,\sigma) \mapsto \mathrm{Trd}_A(\ell s)$, est une paire quadratique sur A. Inversement, pour toute paire quadratique (σ, f) sur A, il existe un élément $\ell \in A$, unique à l'addition près d'un élément de $\mathrm{Alt}(A,\sigma)$, tel que $f(s) = \mathrm{Trd}_A(\ell s)$ pour tout $s \in \mathrm{Sym}(A,\sigma)$. De plus, cet élément vérifie $\ell + \sigma(\ell) = 1$. Le discriminant de (σ, f), noté $\mathrm{disc}(\sigma, f)$, est l'élément de $F/\wp(F)$ défini par $\mathrm{disc}(\sigma, f) = \mathrm{Srd}_A(\ell) + \frac{m(m-1)}{2} + \wp(F)$.

Les paires quadratiques jouent un rôle analogue aux involutions orthogonales dans la cas de la caractéristique différente de 2, puisque toute paire quadratique est adjointe à une forme quadratique q lorsque A est déployée, et dans ce cas le discriminant de la paire quadratique est l'invariant de Arf de q.

Lorsque F est de caractéristique différente de 2, Knus, Parimala et Sridharan ont montré que l'ensemble des discriminants des involutions orthogonales sur une algèbre à division D de degré au moins 4 est égal à $\mathrm{Nrd}_D(D^\times)$. Les considérations précédentes montrent qu'il est naturel de vouloir un résultat analogue pour les paires quadratiques.

Pour toute involution symplectique σ, on pose $\mathfrak{d}(A,\sigma) := \{\mathrm{Srd}_A(\ell)+\frac{m(m-1)}{2}+\wp(F), \ell+\sigma(\ell) = 1\}$.

Autrement dit, $\mathfrak{d}(A,\sigma)$ est l'ensemble des discriminants de paires quadratiques sur A de la forme (σ, f).

On montre le résultat suivant (cf. [18]) :

Théorème 12. *Soit F un corps de caractéristique 2, et soit A une F-algèbre à involution symplectique, qui n'est pas une algèbre de quaternions à division. Alors il existe une involution symplectique σ sur A telle que $\mathfrak{d}(A,\sigma) = F/\wp(F)$. En particulier, tout élément $\alpha \in F/\wp(F)$ est le discriminant d'une paire quadratique sur A.*

• Dans [21], on s'intéresse à la classification des formes anti-hermitiennes sur des algèbres de quaternions. Contrairement au cas des formes quadratiques, aucun système complet d'invariants pour les formes (anti)-hermitiennes sur une algèbre à division n'est connu. En fait, très peu d'invariants ont été construits. Une avancée majeure dans cette direction est la construction due à Rost d'un invariant cohomologique $H^1(\_, G) \to H^3(\_, \mathbb{Q}/\mathbb{Z}(2))$, o'u G est un groupe algébrique linéaire semi-simple simplement connexe, et qui a été utilisé par Bayer-Fluckiger et Parimala pour construire un invariant de Rost

pour les formes anti-hermitiennes sur une algèbre à division munie d'une involution symplectique.

De cet article, nous définissons des invariants $e_{n,Q}$ pour les formes anti-hermitiennes sur des algèbres de quaternions, qui sont des versions tordues des invariants e_n. Nous prouvons alors que ces invariants $e_{n,Q}$ forment un système complet d'invariants pour ces formes anti-hermitiennes. Comme application, nous montrons que formes anti-hermitiennes sur des algèbres de quaternions définies sur un corps de 2-dimension cohomologique au plus 3 sont classées par le rang, le discriminant, l'invariant de Clifford et l'invariant de Rost définis par Bayer-Fluckiger et Parimala.

Plus précisement, on montre le résultat suivant. Si h est une formes anti-hermitiennes de rang n sur une k-algèbre de quaternions Q ($\mathrm{char}(k) \neq 2$), alors $h_{k(Q)}$ correspond à une forme quadratique $q_{h_{k(Q)}}$ de rang $2n$ sur $k(Q)$ (le corps des fonctions de la conique associée àQ). On a alors la proposition suivante :

PROPOSITION 13. *Soit h une forme anti-hermitienne sur Q, et supposons que $q_{h_{k(Q)}} \in I^n(k(Q)), n \geq 1$. Alors :*

1) *Si $d = 1$, il existe un unique element $e_{n,Q}(h) \in H^1(k, \mathbb{Z}/2\mathbb{Z})$ tel que*

$$\mathrm{Res}_{k(Q)/k}(e_{n,Q}(h)) = e_n(q_{h_{k(Q)}}).$$

2) *Si $d \geq 2$, il existe un unique element $e_{n,Q}(h) \in H^d(k, \mu_4^{\otimes d})/[Q] \cup H^{d-2}(k, \mu_2)$ tel que*

$$\mathrm{Res}_{k(Q)/k}(e_{n,Q}(h)) = e_n(q_{h_{k(Q)}}).$$

Ici $[Q] \cup H^{d-2}(k, \mu_2)$ est identifié à un sous-groupe de $H^d(k, \mu_4^{\otimes d-1})$.

La démonstration repose sur le fait que la cohomologie non ramifiée de $k(Q)$ provient de $H^*(k, \mu_2)$. Cette proposition n'est pas spécifique à e_n et peut Ã[a]tre généralisée à des invariants cohomologiques de foncteurs satisfaisant des propriétés raisonnables. Voir[21] pour plus de détails.

On définit aussi un invariant $e_{0,Q}$ par la formule

$$e_{0,Q}(h) = 2\mathrm{rk}(h) \in \mathbb{Z}/4\mathbb{Z}.$$

On obtient alors un analogue du théorème de classification pour les formes quadratiques :

THÉORÈME 14. *Soit h une forme anti-hermitienne sur Q. Alors h est hyperbolique si et seulement si $e_{n,Q}(h) = 0$ pour tout $n \geq 0$.*

Dans [22], nous prouvons la version forte de la conjecture II de Serre pour les groupes algébriques linéaires absolument simples simplement connexes de type classique sur un corps arbitraire. Plus précisement, on a :

THÉORÈME 15. *Soit G un groupe algébrique linéaire absolument simple simplement connexe de type A, B, C or D (non trialitaire) défini sur un corps F de caractéristique quelconque. Supposons que pour tout premier p de torsion du système de racines de G, et pour toute extension finie séparable E/F,*

la norme réduite de toute algèbre centrale simple p-primaire est surjective. Alors $H^1(F, G) = 1$.

Ce résultat a été démontré par Bayer-Fluckiger et Parimala lorsque car(F) $\neq 2$ ou lorsque F est un corps parfait de caractéristique 2. Ainsi ce résultat est nouveau lorsque F est imparfait de caractéristique 2. Notre démonstration est valable en toute caractéristique ; en particulier, on retrouve le résultat de Bayer-Fluckiger et Parimala.

Enfin, dans [**?**], on démontre un résultat de Rost (non publié) qui décrit tous les invariants cohomologiques des algèbres centrales simples de degré 4 sur un corps de caractéristique différente de 2, contenant $\sqrt{-1}$.

Avant de décrire le résultat principal, introduisons quelques notations. Si A est une F-algÃ¨bre centrale simple de degré 4, alors l'application

$$f_2 : A \in \mathbf{CSA}_4(F) \mapsto 2[A] \in H^2(F, \mu_2)$$

définit un invariant cohomologique de degré 2 à valeurs dans μ_2. D'autre par, Rost, Serre et Tignol ont démontré que l'on a

$$\mathcal{T}_A \sim \pi_{2,A} + \pi_{4,A} \in W(F),$$

où π_j est une j-forme de Pfister. On obtient alors un invariant cohomologique de degré 4

$$e_4 : A \in \mathbf{CSA}_4(F) \mapsto e_4(\pi_{4,A}) \in H^4(F, \mu_2).$$

On note 1 l'invariant constant de degré 0. On montre alors le théorème suivant :

THÉORÈME 16. *Les invariants* $1, f_2$ *et* e_4 *forment une base du* $H^*(\_, \mu_2)$*-module* $Inv(\mathbf{PGL}_4, \mu_2)$.

14.3. Dimension essentielle. La notion de dimension essentielle d'un groupe algébrique G défini sur k a été introduite par Reichstein. Rost a également défini la dimension essentielle d'une certaine classe de sous-foncteurs de la K-théorie de Milnor. Enfin, dans des notes non publiées, Merkurjev a défini plus généralement la dimension essentielle d'un foncteur $\mathbf{F} : \mathfrak{C}_k \to \mathbf{Ens}$, de la manière suivante :

Soit k un corps, et soit $\mathbf{F} : \mathfrak{C}_k \to \mathbf{Ens}$ un foncteur covariant.

Soit K/k une extension, et $a \in \mathbf{F}(K)$. Soit $n \geq 0$ un entier. On dit que la dimension essentielle de a est inférieure ou égale à n, et on note $\mathrm{ed}_k(a) \leq n$, s'il existe un corps E, $k \subseteq E \subseteq K$ tel que :

(1) $\mathrm{trdeg}_k E \leq n$
(2) $a \in \mathrm{Im}(\mathbf{F}(E) \to \mathbf{F}(K))$.

On dit que $\mathrm{ed}_k(a) = n$ si $\mathrm{ed}_k(a) \leq n$ et $\mathrm{ed}_k(a) \not\leq n - 1$.

La dimension essentielle de $\mathbf{F}$, notée $\mathrm{ed}_k(\mathbf{F})$ est le supremum des dimensions essentielles $\mathrm{ed}_k(a)$, pour tout $a \in \mathbf{F}(K)$ et toute extension K/k.

Si G est un groupe algébrique linéaire défini sur k, on note $\mathrm{ed}_k(G)$ la dimension essentielle du foncteur $H^1(\_, G)$.

La notion de dimension essentielle est toute récente. Cet invariant est particulièrement intéressant mais difficile à calculer pour une structure algébrique fixée car il contient beaucoup d'informations arithmétiques et algébriques. Par exemple si G est un groupe fini constant, $\mathrm{ed}(G)$ est le nombre minimal de paramètres nécessaires pour construire une extension galoisienne générique de groupe G. Ceci explique pourquoi il est mÃªme difficile de trouver de bonnes bornes supérieures pour cet entier, car cela impliquerait de connaître de bonnes paramétrisations des extensions galoisiennes sur un corps quelconque. Si $G = S_n$, alors $H^1(\_, G)$ classe les algèbres étales de rang n, et donc $\mathrm{ed}(S_n)$ est le nombre minimal de coefficients algébriquement indépendants d'un polynôme minimal définissant une telle algèbre ; ainsi cette question est reliée au problème de réductions des équations, un problème très ancien et loin d'être résolu.

La dimension essentielle est aussi reliée à un des plus fameux problème d'algèbre non-commutative : une ancienne conjecture d'Albert dit que toute k-algèbre centrale simple de degré premier p contient un sous-corps commutatif cyclique de degré p. Cette conjecture est toujours ouverte pour $p \geq 5$. Par contre, il est facile de voir que si cette conjecture est vraie, alors $\mathrm{ed}_{\mathbb{C}}(\mathbf{PGL}_p) = 2$. Ainsi une preuve de l'inégalité $\mathrm{ed}_{\mathbb{C}}(\mathbf{PGL}_p) \geq 3$ prouverait que cette conjecture est fausse. Finalement, la dimension essentielle des groupes finis est reliée aux propriétés de déploiement des torseurs, ainsi qu'à de très importantes conjectures arithmétiques comme nous l'expliquons maintenant.

Soit k un corps algébriquement clos de caractéristique nulle. Pour toute extension K/k, on note K_{ab} (resp. K_{sol}) l'extension abélienne (resp. résoluble) maximale de K. Supposons que l'on puisse prouver la propriété suivante : pour tout $n \geq 1$, pour toute extension K/k et tout $\alpha \in H^1(K, S_n)$, il existe une extension abélienne (resp. résoluble) L/K telle que $\mathrm{ed}_k(\alpha_L) \leq 1$. Alors cela impliquerait que K_{ab} (resp. K_{sol}) a une dimension cohomologique au plus 1, ce qui est une conjecture très difficile et toujours ouverte. Une conséquence directe de ce résultat serait que pour tout groupe connexe G défini sur k, et pour tout $\alpha \in H^1(K, G)$, la classe α peut être déployé par une extension abélienne (resp. résoluble) de K ; en particulier, cela impliquerait que la conjecture II de Serre est vraie pour les groupes de type E_8, cas encore ouvert et extrêmement ardu.

Dans [**13**], on s'intéresse (en collaboration avec G.Favi) à dégager des propriétés de base de la dimension essentielle et également à réconcilier les trois différentes notions. Cet article est divisé en huit sections.

Dans la section 1, on étudie le comportement de cette notion par produit direct, coproduit et extension des scalaires. Au passage, nous définissons la notion de fibration de foncteurs.

Dans la section 2, nous introduisons la dimension essentielle d'un groupe algébrique G défini sur un corps k arbitraire. Puis nous donnons des exemples de calcul de cette dimension essentielle, y compris dans le cas du cercle.

Dans la section 3, nous nous intéressons aux actions de groupes sur des k-schémas algébriques.

Rappelons qu'un groupe algébrique G agit génériquement librement sur un k-schéma X de type fini si le stabilisateur schématique de tout point de X est trivial.

On prouve alors le résultat suivant :

THÉORÈME 17. *Soit G un groupe algébrique défini sur k, agissant linéairement et génériquement librement sur un espace affine $\mathbb{A}(V)$ (où V est un k-espace vectoriel de dimension finie). Alors on a*

$$\mathrm{ed}_k(G) \leq \dim V - \dim G.$$

En application, nous montrons que la dimension essentielle d'un groupe algébrique est finie. Nous montrons aussi qu'un schéma en groupes fini étale agit linéairement et génériquement librement sur un espace affine $\mathbb{A}(V)$ si et seulement si G agit fidèlement sur $\mathbb{A}(V)$. Nous appliquons ensuite les résultats précédents pour estimer la dimension essentielle des groupes abéliens finis et des groupes diédraux lorsque le corps de base est suffisament gros.

Dans la section 4, nous introduisons la notion (due à Merkurjev) de foncteur n-simple et l'appliquons pour donner des bornes inférieures à la dimension essentielle de certains groupes finis (e.g. les groupes symétriques).

Nous obtenons ainsi le résultat suivant, qui donne un intérÃªt supplémentaire aux invariants cohomologiques :

PROPOSITION 18. *Si $\mathbf{F}$ possède un invariant cohomologique non trivial de degré n, alors* $\mathrm{ed}_k(\mathbf{F}) \geq n$.

Rappelons qu'un invariant cohomologique est dit *non trivial* si pour toute extension K/k il existe $L \supseteq K$ et $a \in \mathbf{F}(L)$ tel que $\varphi_L(a) \neq 0$.

Dans la section 5, inspirés par la définition de dimension essentielle introduite par Rost pour certains sous-foncteurs de la k-théorie de Milnor, nous définissons la notion de paire verselle pour des foncteurs allant de la catégorie des F-algèbres commutatives unitaires vers la catégorie des ensembles. Nous définissons alors une nouvelle sorte de dimension essentielle, que nous appelons dimension essentielle de Rost, et la comparons avec la dimension essentielle de Merkurjev.

Plus précisement, soit k un corps et soit $\mathfrak{A}_k$ la catégorie des k-algèbres commutatives.

Soit K/k une extension de corps. Si $\mathcal{O}$ est une sous k-algèbre locale de K, d'idéal maximal $\mathfrak{m}$, on note $\kappa(\mathcal{O}) = \mathcal{O} \,/\, \mathfrak{m}$ son corps résiduel et $\pi : \mathcal{O} \to \kappa(\mathcal{O})$ la projection canonique.

Soit K et L deux extensions de k. Une *pseudo k-place* $f : K \rightsquigarrow L$ est un couple $(\mathcal{O}_f, \alpha_f)$ où $\mathcal{O}_f$ est est une sous k-algèbre locale de K et $\alpha_f : \kappa(\mathcal{O}_f) \to L$ est un k-morphisme.

Soit $\mathbf{F} : \mathfrak{A}_k \to \mathbf{Ens}$ un foncteur et soit $f : K \rightsquigarrow L$ une pseudo k-place. On dit que $a \in \mathbf{F}(K)$ est *non ramifié* en f si a appartient à l'image de l'application

$\mathbf{F}(\mathcal{O}_f) \to \mathbf{F}(K)$. Dans ce cas, on définit *l'ensemble des spécialisations de a* par

$$f^*(a) = \big\{ \mathbf{F}(\alpha_f \circ \pi)(c) \mid c \in \mathbf{F}(\mathcal{O}_f) \text{ avec } c_K = a \big\}.$$

On dit que (a, K) avec $a \in \mathbf{F}(K)$ est *une paire verselle pour* $\mathbf{F}$ si pour toute extension L/k et tout $b \in \mathbf{F}(L)$ il existe une pseudo k-place $f : K \rightsquigarrow L$ telle que a est non ramifiée en f et telle que $b \in f^*(a)$.

Soit maintenant $\mathbf{F} : \mathfrak{A}_k \to \mathbf{Ens}$ un foncteur possédant une paire verselle. On définit sa *dimension essentielle à la Rost* (notée $\mathrm{ed}'(\mathbf{F})$) par $\mathrm{ed}'(\mathbf{F}) = \min \mathrm{trdeg}(K : k)$ pour tous les K/k tels qu'il existe $a \in \mathbf{F}(K)$ tel que (a, K) est une paire verselle pour $\mathbf{F}$.

On dit qu'une paire verselle (a, K) est *sympathique* si pour tout $L \subset K$ et $a' \in \mathbf{F}(L)$ tels que $a = a'_K$, la paire (a', L) est verselle. On dit que $\mathbf{F}$ est *sympathique* s'il possède une paire verselle sympathique.

On a alors :

Proposition 19. *Soit* $\mathbf{F} : \mathfrak{A}_k \to \mathbf{Ens}$ *un foncteur possédant une paire verselle. On a*

$$\mathrm{ed}_k(\mathbf{F}) \leq \mathrm{ed}'_k(\mathbf{F})$$

Si de plus $\mathbf{F}$ *est sympathique, alors*

$$\mathrm{ed}'_k(\mathbf{F}) = \mathrm{ed}_k(\mathbf{F}) = \mathrm{ed}(a),$$

où (a, K) *est une paire verselle sympathique arbitraire.*

Dans la section 6, on relie la dimension essentielle d'un groupe algébrique G à celle d'un G-torseur générique.

Soit G un groupe algébrique défini sur k, K/k une extension de corps et $P \to \mathrm{Spec}(K)$ un G-torseur. On dit que P est *générique* si

i) il existe un schéma irréductible Y (dont le point générique est noté η) denoted by η) tel que $k(Y) \simeq K$ et un G-torseur $f : X \to Y$ dont la fibre générique $f^{-1}(\eta) \to \mathrm{Spec}(K)$ est isomorphe à $P \to \mathrm{Spec}(K)$. En d'autres termes,

$$\begin{array}{ccc} P & \longrightarrow & X \\ \downarrow & & \downarrow \\ \mathrm{Spec}(K) & \longrightarrow & Y \end{array}$$

est un pull-back.

ii) Pour tout extension k'/k avec k' infini, pour tout ouvert non vide U de Y et pour tout G-torseur $P' \to \mathrm{Spec}(k')$, il existe un point k'-rationnel $x \in U$ tel que $f^{-1}(x) \simeq P'$.

Si G est un groupe algébrique, on note $G - \mathrm{Tors} : \mathfrak{A}_k \to \mathbf{Ens}$ le foncteur des G-torseurs. La restriction de foncteur à $\mathfrak{C}_k$ est isomorphe au foncteur $H^1(\_, G)$. On note $\mathrm{ed}'_k(G)$ la dimension essentielle à la Rost de ce foncteur.

On prouve alors :

THÉORÈME 20. *Soit G un groupe algébrique défini sur k, et soit $T \in H^1(K, G)$ un G-torseur générique. Alors (T, K) est une paire verselle sympathique pour le foncteur des G-torseurs. En particulier, on a*

$$\mathrm{ed}_k(G) = \mathrm{ed}'_k(G) = \mathrm{ed}_k(T).$$

Nous faisons également le lien entre la dimension essentielle au sens de Reichstein avec celle au sens de Merkurjev.

Soient $f : X \to Y$ et $f' : X' \to Y'$ deux G-torseurs.

On dit que f' est une *compression* de f s'il existe un diagramme

$$\begin{array}{ccc} X & \overset{g}{\dashrightarrow} & X' \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle f'} \\ Y & \underset{h}{\dashrightarrow} & Y' \end{array}$$

où g est un morphisme rationnel G-équivariant et dominant, et où h est un morphisme rationnel. La *dimension essentielle* du G-torseur f est la plus petite dimension de Y' possible dans une compression f' de f. On la note $\mathrm{ed}(f)$.

La *dimension essentielle de G* au sens de Reichstein est alors le maximum des $\mathrm{ed}(f)$ lorsque f parcoure l'ensemble des G-torseurs. On a alors :

PROPOSITION 21. *Soit $f : X \to Y$ un G-torseur et soit T sa fibre générique. Alors* $\mathrm{ed}(f) = \mathrm{ed}_k(T)$.

Cette proposition, combinée au théorème précédent montre que les trois notions de dimension essentielle d'un groupe algébrique coïncident.

Dans la section 7, nous nous intéressons particulièrement à la dimension essentielle des groupes finis constants. Tout d'abord, nous montrons que la dimension essentielle d'un tel groupe est le minimum des $\mathrm{trdeg}(E : k)$ lorsque E parcourt l'ensemble des sous-corps de $k(V)$ sur lequel G agit fidèlement, ce qui est la définition originale de Reichstein et Bühler de la dimension essentielle d'un groupe fini. Nous appliquons alors ce résultat pour calculer la dimension essentielle des groupes cycliques et diédraux sur le corps des réels, ainsi que la dimension essentielle des groupes cycliques d'ordre au plus 6 sur n'importe quel corps de base.

Finalement dans la section 8, nous montrons le théorème d'invariance homotopique suivant :

THÉORÈME 22. *Soit k un corps infini, et soit G un groupe algébrique défini sur k. Alors* $\mathrm{ed}_k(G) = \mathrm{ed}_{k(t)}(G_{k(t)})$.

• Dans [16], avec G.Favi, nous calculons la dimension essentielle des cubiques en 2 et 3 variables. Nous utilisons pour cela les techniques développées dans [13].

Soient P, P' deux polynômes homogènes de degré d en n variables à coefficients dans un corps L. On dit que P et P' sont équivalents s'il existe $\lambda \in L^\times$ et $f \in GL_n(L)$ tels que $P' = \lambda P \circ f$. Le foncteur des classes d' équivalence est noté $\mathbf{F}_{d,n}$. Si $d = 3$, il est simplement noté $\mathbf{Cub}_n$.

Problème : Calculer $\mathrm{ed}_k([P])$.

Cette question est motivée par ce qui suit : il est facile de voir que si $\varphi : \mathbf{F} \to \mathbf{G}$ est une application naturelle, alors $\mathrm{ed}_k(a)) \geq \mathrm{ed}_k(\varphi_K(a))$ pour tout $a \in \mathbf{F}(K)$. Puisqu'il arrive fréquemment que l'on puisse associer fonctoriellement une forme homogène à des structures algébriques classiques (la forme trace, la forme norme...), il est fondamental d'en apprendre plus sur la dimension essentielle de telles formes.

Nous avons obtenu le résultat suivant :

THÉORÈME 23. *Soit k un corps.*

1. *Si $car(k) \neq 3$, alors* $\mathrm{ed}_k(\mathbf{Cub}_2) = 1$.
2. *Si $car(k) \neq 2, 3$, alors* $\mathrm{ed}_k(\mathbf{Cub}_3) = 3$.

L'idée sous-jacente de la preuve est la suivante : pour définir une cubique en 3 variables à équivalence projective près, il suffit de choisir 9 points d'inflexion et la valeur du j-invariant, et ces choix peuvent se faire de manière indépendante. On étudie alors le foncteur des cubiques ayant des points d'inflexion fixés, ainsi que celui des cubiques de j-invariant fixé, et on utilise un lemme de descente galoisienne pour les identifier à des foncteurs de cohomologie galoisienne. On utilise alors les techniques développées dans [13] pour calculer la dimension essentielle des groupes algébriques correspondants.

14.4. Dimension canonique. Dans [17], avec Z. Reichstein, nous avons défini la notion de dimension canonique d'une G-variété X définie sur un corps k algébriquement clos de caractéristique nulle (où G est un groupe algébrique défini sur k) comme suit : si G agit sur X, on dit que $F : X \dashrightarrow X$ est *une forme canonique de* X s'il existe $f : X \dashrightarrow G$ telle que $F(x) = f(x) \cdot x$. On pose alors

$$\mathrm{cd}(X, G) = \inf_F \dim F(X) - \dim X/G,$$

où F parcourt toutes les formes canoniques, et où X/G est un quotient rationnel de X par G.

Il se toruve que la notion de dimension essentielle donne un lien géométrique entre le déploiement générique des algèbres centrales simples et la dimension essentielle des formes homogènes génériques ; la dimension essentielle de la forme homogène générique peut Ã[a]tre ainsi calculée lorsque (n, d) est une puissance d'un nombre premier, en utilisant une formule de degré prouvée par Merkurjev et ses conséquences sur l'incompressibilité de variétés.

Nous décrivons maintenant plus précisement les résultats obtenus dans [17] :

Dans [17], nous avons relié cet invariant à la dimension essentielle du foncteur $\mathbf{Orb}_{X,G}$ défini par $\mathbf{Orb}_{X,G}(L) := X(L)/G(L)$. En fait, nous montrons le résultat suivant :

PROPOSITION 24. *Soit $\eta \in X(k(X))$ le point générique de X, et soit $[\eta]$ sa classe dans $\mathbf{Orb}_{X,G}(k(X))$. Alors on a l'égalité :*

$$\mathrm{ed}([\eta]) = \mathrm{cd}(X,G) + \dim X/G.$$

Nous étudions également les propriétés de base de la dimension canonique d'une G-variété X.

Soit S un groupe algébrique et Y une variété. On définit l'entier $e(Y,S)$ comme étant le plus petit entier e satisfaisant la propriété suivante : étant donné un point $y \in Y$ en position générale, il existe une application rationnelle S-équivariante $f : Y \dashrightarrow Y$ telle que $s \in f(Y)$ et $\dim f(Y) \leq e + \dim S$.

On a alors le résultat suivant :

PROPOSITION 25. *Soit X une G-variété possédant un stabilisateur S en position générale, et soit N_S le normalisateur de S dans G. Alors*

$$e(G,S) \leq \mathrm{cd}(X,G) \leq e(G,N_S) - \dim S + \dim N_S.$$

Nous introduisons également la notion de G-variété déployée. Soit X une G-variété possédant un stabilisateur S en position générale. On dit que X est *déployée* si elle est birationnellement isomorphe comme G-variété à $G/S \times X/G$ (où G agit par translations à gauche sur le premier facteur, et trivialement sur le second). Si X est génériquement libre (i.e. G agit génériquement librement sur X), on retrouve la notion de G-torseur déployé.

On a alors le résultat suivant :

PROPOSITION 26. *Soit X une G-variété possédant un stabilisateur S en position générale. Si X est déployée, on a :*

$$\mathrm{cd}(X,G) = e(G,S).$$

Remarquons que l'on a toujours l'inégalité $e(G,S) \geq \mathrm{ed}(S)$, et que l'égalité a lieu si G est spécial.

Lorsque X est génériquement libre, c'est-à-dire un G-torseur défini sur $\mathrm{Spec}(k(X)^G)$, nous relions la dimension canonique de X aux degrés de transcendance des corps de déploiement générique de ce torseur de la façon suivante :

THÉORÈME 27. *Soit G un groupe algébrique connexe, et soit X une G-variété irréductible génériquement libre. Soit $E = k(X/G) = k(X)^G$, soit $\alpha = [X] \in H^1(E,G)$ la classe de cohomologie correspondante et soit $F : X \dashrightarrow X$ une forme canonique de X. Alors :*

1. *L'extension $k(X)/E$ est une extension de déploiement générique de α.*
2. $\mathrm{cd}(X,G) = \min\{\mathrm{trdeg}_E(K) \mid K/E$ *est une extension de déploiement générique pour* $\alpha\}$

Ici, le terme "générique" se rapporte indifféremment à la propriété de spécialisation simple ou à la propriété de spécialisation rationnelle.

Si X est une G-représentation linéaire génériquement libre V, nous montrons que $\mathrm{cd}(V,G)$ est indépendante du choix de V. On l'appelle *la dimension canonique de G*, et on la note $\mathrm{cd}(G)$.

On a alors les propriétés suivantes :

LEMME 28. (1) $\mathrm{cd}(G) = \max \mathrm{cd}(X, G)$, *où* X *décrit l'ensemble des* G*-variétés génériquement libres.*

(2) $\mathrm{cd}(G) = \mathrm{cd}(G^0)$.

(3) *Si* G *est connexe,* $\mathrm{cd}(G) = 0 \iff G$ *est spécial.*

Nous relions alors dimension essentielle des formes homogènes génériques de degré d en n variables à la dimension canonique du groupe algébrique $\mathbf{GL}_n/\mu_d$ comme suit :

PROPOSITION 29. *Soit* k *un corps algébriquement clos de caractéristique* 0. *Soit* $P_0 = \sum_I t_I X^I$ *le polynôme homogène générique de degré* d *en* n *variables, et soit* $[P_0]$ *sa classe d'équivalence. Si* $d \geq 3$, *et si* $(n, d) \neq (2, 3)$, $(2, 4)$ *ou* $(3, 3)$, *alors*

$$\mathrm{ed}([P_0]) = \binom{n+d-1}{d} - n^2 + \mathrm{cd}(\mathbf{GL}_n/\mu_d).$$

Cela conduit en particulier au résultat suivant :

THÉORÈME 30. *Supposons que* $(n, d) = p^m, m \geq 0$, *où* p *est un nombre premier. Alors*

$$\mathrm{ed}([P_0]) = \begin{cases} \binom{n+d-1}{d} - n^2 & \text{si } m = 0 \\ \binom{n+d-1}{d} - n^2 + p^{v_p(n)} - 1 & \text{sinon} \end{cases}$$

Enfin, l'interprétation de la dimension canonique en termes d'extensions génériquement déployantes nous permet de donner des exemples de groupes algébriques de dimension canonique au moins égale à 2 ou 3, et de donner la classification des groupes simples de dimension canonique égale à 1.

On a ainsi le résultat suivant :

THÉORÈME 31. *Soit* k *un corps de caractéristique* 0 *algébriquement clos, et soit* G *un groupe simple défini sur* k. *Alors*

$$\mathrm{cd}(G) = 1 \iff G \simeq \mathbf{SO}_3, \mathbf{SO}_4, \mathbf{SL}_{2m}/\mu_2, \mathbf{PGSp}_{2m}, m \text{ impair}\ .$$

14.5. Algèbres centrales simples et communication sans fil. Comme indiqué plus haut, on peut construire des codes $\mathcal{C}$ performants sur des algèbres cycliques à division.

Le code doit aussi satisfaire des conditions supplémentaires pour Ã[a]tre efficace et utilisable d'un point de vue industriel. Le code $\mathcal{C}$ pouvant en pratique contenir un très grand nombre de matrices, on doit s'assurer que $\delta_{min}(\mathcal{C})$ est minoré par une constante strictement positive (sans quoi il pourrait être très proche de zéro, ce qui nuirait aux performances du code).

Pour ce faire, on modifie un peu la façon de construire les matrices du code. Si $A = (\gamma, L/K, \sigma)$ est une algèbre cyclique de degré n à division sur $K = \mathbb{Q}(i)$ ou $\mathbb{Q}(j)$ (cette condition est imposée par les méthodes de traitement du

signal), on encode les éléments comme suit. On choisit $\lambda \in L \cap \mathbb{R}$ totalement positif, et un idéal I de $\mathcal{O}_L$. Le code sera alors construit ainsi :

$$\mathcal{C} = \{M_a D_\lambda \mid a \in I + eI + \cdots + e^{n-1}I\},$$

où $D_\lambda = diag(\lambda, \sigma^{n-1}(\lambda), \ldots, \sigma(\lambda))$, et M_a est la matrice de multiplication à gauche dans la L-base $(1, e, \ldots, e^{n-1})$.

Il faut aussi s'assurer que l'encodage des symboles d'information dans les matrices servant de mots de code ne requiert pas d'énergie supplémentaire. Cette condition sur l'énergie peut-Ã^atre traduite en termes mathématiques de la façon suivante (sous une condition supplémentaire sur l'extension L/K) : le réseau

$$h_\lambda : I \times I \to \mathcal{O}_K, (x, y) \mapsto Tr_{L/K}(\lambda x \bar{y})$$

soit isomorphe à $\mathcal{O}_K^n$.

Si le code $\mathcal{C}$ satisfait ces conditions, on dit qu'il est *parfait*.

On pose $d_{L/K} = \det(h_1)$. C'est un entier positif. On peut alors montrer que maximiser $\det_{min}(\mathcal{C})$ revient à minimiser $d_{L/K}$.

Dans [24], on montre que les codes parfaits construits sur les algèbres cycliques à division existent seulement pour un nombre d'antennes n égal à $2, 3, 4$ ou 6.

Dans [19], on construit un code pour $n = 4$, qui n'est pas parfait mais qui a de meilleures performances que le meilleur code connu à ce jour.

Dans [23], on construit un code pour $n = 4$ sur un produit croisé biquadratique à division.

Dans [32], on explique comment les considérations précédentes peuvent se généraliser aux produits croisés quelconques. On démontre ensuite que les codes construits sur des algèbres cycliques de degré 4 et 6 par Oggier et al., ainsi que celui construit dans [23] ont des performances optimales.

Dans [29], on développre une méthode systématique pour estimer les performances d'un code algébrique basé sur une algèbre à division, dans le cas où les propriétés du canal ne sont pas connues du récepteur, grâce à la théorie des algèbres centrales simples unitaires.

Enfin, les articles [30] et [31] étudient la complexité de décodage des codes espaces-temps et la possibilité de décodage rapide. En particulier, on montre que la complexité de décodage ne peut pas être meilleure que $M^{\lceil n^2/2 \rceil}$ (où M est la taille de la constellation et n est la taille des matrices envoyées), en utilisant des techniques d'algèbre linéaire et la théorie des algèbres d'Azumaya, lorsque le code est construit sur une algèbre à division.