SORBONNE UNIVERSITÉS

Institut de Mathématiques de Jussieu - Paris Rive Gauche (UMR 7586 CNRS)

Mémoire présenté pour l'obtention du

Diplôme d'habilitation à diriger les recherches de Sorbonne Universités

Spécialité : Mathématiques

par

Mathieu FLORENCE

Soutenu le 13 janvier 2021 devant la commission d'examen :

Michel Brion	Directeur de recherche (Institut Joseph Fourier, Grenoble)
Patrick Brosnan	Professeur (Department of Mathematics, University of Maryland)
Jean-Louis Colliot-Thélène	Directeur de recherche (Département de Mathématiques, Paris-Saclay)
Pierre Colmez	Directeur de recherche (IMJ, Sorbonne Université)
Philippe Gille	Directeur de recherche (ICJ, Université Claude Bernard Lyon I)
Raman Parimala	Professeure (Emory University, Atlanta)
Burt Totaro	Professeur (UCLA, Los Angeles)
Zinovy Reichstein	Professeur (UBC, Vancouver)

au vu des rapports de :

Michel Brion	Directeur de recherche (Institut Joseph Fourier, Grenoble)
Nikita Karpenko	Professeur (University of Alberta, Edmonton)
Burt Totaro	Professeur (UCLA, Los Angeles)

Remerciements

Je remercie chaleureusement les membres de l'équipe de Topologie et Géométrie Algébriques de Jussieu, pour nos interactions quotidiennes. Discussions mathématiques, déjeuners, moments de détente au coin café...
Un merci à Cyril Demarche, Vincent Maillot, Antoine Ducros, Marco Maculan, Gérard Freixas i Montplet et Gregor Masbaum. Merci aussi à l'équipe voisine, Analyse Complexe et Géométrie, pour de sympathiques instants de partage.
Un merci particulier à Émilie Jacquemot et à Ariane Mézard, qui m'ont rappelé que soutenir l'HDR est important, et moins compliqué qu'il n'y paraît!
J'ai beaucoup bénéficié des échanges à plusieurs. Parfois, et dans la même journée, une incompréhension hésitante se transformait en vision mathématique novatrice. Parfois aussi, ce phénomène se produisait dans l'ordre inverse;-)
Dans le désordre, merci donc à Lara Thomas, Philippe Gille, Dave Anderson, Giordano Favi, Giancarlo Lucchini-Arteche, Bart de Smit, Zinovy Reichstein, Charles De Clercq et Michel Van Garrel. Grand merci à Michel Brion, Nikita Karpenko et Burt Totaro, pour leur précieux travail de rapporteurs. Merci à Michel Brion, Patrick Brosnan, Jean-Louis Colliot-Thélène, Pierre Colmez, Philippe Gille, Raman Parimala, Burt Totaro et Zinovy Reichstein, pour m'avoir fait l'honneur d'être présents dans le jury.
Merci à ceux qui y croient, ainsi qu'à ceux qui n'y croient pas- surtout quand ce sont les mêmes personnes:)

Table des matières

1 Combinatoire algébrique **5**

2 Espaces homogènes **7**

3 Dimension essentielle **10**
3.1 Les p-groupes cycliques. 11
3.2 Formes traces. 11

4 Géométrie birationnelle et rationalité **12**
4.1 Autour des conjectures d'Amitsur et de Voskresenskiĭ. 12
4.2 Formes des espaces de modules de courbes marquées. 14
4.3 Action adjointe d'un groupe algébrique sur son algèbre de Lie. . . . 16

5 Un peu de caractéristique positive. **17**
5.1 Critère valuatif pour les générateurs de bases normales. 17
5.2 Algèbres simples centrales et longueur de symboles. 18

6 Caractéristique positive et théories galoisiennes. **19**
6.1 Ind-variétés de déploiement. 19
6.2 Relèvement des fibrés en vecteurs de Witt. 20
6.3 Groupes profinis lisses, relèvements modulo p^2. 21

7 Résidus sur les grassmanniennes affines. **26**

Introduction

Je me propose de faire le récit de mes travaux de recherche, et du paysage où ils s'insèrent. J'ai choisi de mettre en avant lisibilité et concision. Les détails historiques et techniques se trouvent dans les textes auxquels je fais référence.
Et, pour rire: ce pot-pourri, avec un peu de pot, ne sera pas trop pourri!

1

Combinatoire algébrique

Soit G un graphe fini (collection de sommets et d'arêtes les reliant, avec boucles possibles). On autorise à ses sommets de prendre deux états: allumé et éteint. Le jeu σ, sur G, a une seule règle simple: en appuyant sur un sommet, on modifie son état, ainsi que celui de tous les sommets adjacents. On se pose la question suivante. Partant de la configuration "tout éteint", quelles configurations peut-on obtenir en jouant à σ? Un célèbre résultat de Sutner ([37]) affirme que la configuration "tout allumé" peut être obtenue, pourvu que G contienne toutes les boucles. On parle alors d'un jeu σ^+. En introduisant la matrice d'incidence de G sur le corps fini $\mathbb{F}_2$, ceci s'interprète comme un problème d'algèbre linéaire élémentaire.
Soit $I_d = [1, \ldots, d]$ l'intervalle de taille d. On le munit d'une structure de graphe, où un entier est relié à ses voisins. Matrice d'incidence:

$$J_d = \begin{pmatrix} 0 & 1 & 0 & \cdots & \cdots & 0 \\ 1 & \ddots & \ddots & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \ddots & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & \ddots & \ddots & 1 \\ 0 & \cdots & \cdots & 0 & 1 & 0 \end{pmatrix}$$

Soit $G = I_{d_1} \times \ldots \times I_{d_n}$ une grille de dimension n. On met sur G une structure de graphe, dont la matrice d'incidence commute aux matrices

$$\mathrm{Id}_{d_1} \otimes \ldots \otimes \mathrm{Id}_{d_{i-1}} \otimes J_{d_i} \otimes \mathrm{Id}_{d_{i+1}} \otimes \ldots \mathrm{Id}_{d_n},$$

pour $i = 1, \ldots, n$- correspondant aux jeux élémentaires suivant chaque dimension. Supposons $n = 2$. Avec Frédéric Meunier, on donne dans [24] une condition nécessaire et suffisante simple pour que toute configuration doublement symétrique (c'est-à-dire symétrique par rapport aux deux médianes du damier) puisse être atteinte, en jouant à σ sur G. Comme corollaire, on répond favorablement à une conjecture de Nicolas Vaillant: lorsque G est donné par $J_{d_1} \otimes J_{d_2}$ (jeu σ^-), la configuration "tout allumé" peut être atteinte si, et seulement si, d_1 et d_2 sont impairs, et $d_1 + 1$ a même valuation 2-adique que $d_2 + 1$.
En dimension n quelconque, on démontre que toute configuration complètement

symétrique est atteinte, pour les jeux σ^+ donnés par

$$J_{d_1} \otimes \ldots \otimes J_{d_n} + \mathrm{Id}$$

et

$$(J_{d_1} + \mathrm{Id}_{d_1}) \otimes \ldots \otimes (J_{d_n} + \mathrm{Id}_{d_n}).$$

Le cas général (d'un jeu commutant aux jeux élémentaires) est aujourd'hui encore ouvert.

2

Espaces homogènes

Durant ma thèse, et quelque temps ensuite, j'ai étudié les points rationnels sur une "famille-test" célèbre de variétés algébriques: les espaces homogènes. Ceux-ci sont des variétés algébriques sur un corps, munis d'une action transitive d'un groupe algébrique- souvent linéaire. Il surgissent, de manière parfois inattendue, dans de nombreuses questions de géométrie. On peut citer comme exemples élémentaires les espaces affines, les quadriques et les grassmanniennes. Les espaces affines, considérés avec l'action de leur groupe vectoriel sous-jacent, entrent dans la classe des espaces principaux homogènes de groupes algébriques- aussi appelés torseurs. Pour ceux-ci, Serre a formulé la question suivante.

Question 2.0.1. Soit G un groupe algébrique lisse et connexe sur un corps k. Soit X un espace principal homogène de G sur k. Supposons que la variété X possède un zéro-cycle de degré un. Possède-t-elle alors un point k-rationnel?

Remarque 2.0.2. Je rappelle qu'une k-variété X possède un zéro-cycle de degré $d \geq 1$ si, et seulement si, il existe une famille d'extensions finies de corps l_i/k, dont le pgcd des degrés divise d, et telle que $X(l_i) \neq \varnothing$ pour tout i.

Remarque 2.0.3. L'hypothèse de connexité sur G est nécessaire. Pour certains G finis, on montre que la réponse à 2.0.1 est négative, à l'aide d'automorphismes de Coleman.

Notons que, si G est commutatif (par exemple une variété abélienne), la réponse est positive. Pour le voir, l'argument habituellement utilisé est la "restriction-corestriction" en cohomologie galoisienne. Je propose, dans l'exercice suivant (qui se veut léger et récréatif), une approche reposant sur l'arithmétique élémentaire.

Exercice 2.0.4. On s'intéresse à la question 2.0.1, dans le cas où G est commutatif, et k de caractéristique nulle. Soit $\overline{k}$ une clôture algébrique de k.

1) Expliquer pourquoi l'ensemble $X(\overline{k})$ est naturellement muni d'une structure d'espace affine sur $\mathbb{Z}$. On donnera sens au barycentre

$$\lambda_1 x_1 + \ldots + \lambda_r x_r \in X(\overline{k}),$$

où les x_i sont dans $X(\overline{k})$, et les λ_i sont des entiers relatifs, de somme 1.

2) Montrer que la donnée d'un zéro-cycle de degré 1 sur X apporte naturellement les informations suivantes.

i) Une égalité

$$a_1 n_1 + \ldots + a_s n_s = 1,$$

où les a_i et les n_i sont des entiers, avec $n_i \geq 1$ pour tout i.
ii) Pour tout i, un sous-ensemble $P_i \subset X(\overline{k})$, de taille n_i, et globalement invariant par le groupe $\mathrm{Gal}(\overline{k}/k)$.

3) A l'aide d'un barycentre, récupérer un point k-rationnel de X.

4) Adapter cet exercice à un corps k de caractéristique positive.

La question 2.0.1 est, aujourd'hui encore, très largement ouverte.
Veisfeiler, puis Totaro dans [41], l'ont étendue au cadre des espaces homogènes, avec la formulation suivante.

Question 2.0.5. Soit G un groupe algébrique sur un corps k. Soit X un espace homogène de G, sur k. Supposons que la variété X possède un zéro-cycle de degré $d \geq 1$. Possède-t-elle alors un point dans une extension finie de k, de degré divisant d?

Remarque 2.0.6. Les énoncés des questions 2.0.1 et 2.0.5 présents dans la littérature peuvent légèrement varier. Ainsi, on y suppose parfois G semi-simple. On impose aussi souvent aux zéro-cycles et aux extensions finies d'être séparables.

Dans [16], j'ai montré que la question 2.0.5 admet une réponse négative, même pour $d = 1$. Simultanément, Parimala a fourni des contre-exemples d'une toute autre nature, dans [35]. Plus précisément, mes contre-exemples existent sur le corps $\mathbb{C}((x, y))$, sur un un corps p-adique, ou sur un corps de nombres totalement imaginaire k. Ils concernent des espaces homogènes à stabilisateurs finis abéliens de $G = \mathrm{PGL}(Q)$, pour Q une algèbre de quaternions sur k. Ce sont donc des variétés affines. Ceux de Parimala arrivent sur des corps de plus grande dimension cohomologique, et sont des variétés projectives. Dans les deux cas, les variétés considérées sont géométriquement rationnelles.
Très récemment, Gordon-Sarney et Suresh ont donné un contre-exemple remarquable à la question 2.0.5, lorsque X est un G-torseur (voir [32]). Dans leur construction, le degré d vaut 2, et k est un corps local, de corps résiduel un corps global.
Dans mes propres travaux, les contre-exemples, comme suggéré par Gabber, vérifient la propriété suivante. Pour toute k-compactification lisse X_c de X, on a $X_c(k) = \varnothing$. Dans la publication [17], je propose une généralisation de ce phénomène, comme suit.

Théorème 2.0.7. *Soit X un espace homogène d'un groupe algébrique G, sur un corps parfait k. On suppose qu'il existe une k-compactification lisse de X possédant un point rationnel. Alors X lui-même en admet un.*

On pourra noter qu'aucune hypothèse n'est faite, ni sur G, ni sur X. Par contraste, la démonstration utilise une machinerie complexe. Michel Raynaud m'a suggéré que l'hypothèse de perfection sur k est probablement superflue- une piste qui reste à explorer.

Dans ces premiers travaux, j'utilise principalement deux outils techniques. Le premier est la cohomologie non abélienne, telle qu'élaborée par Springer. On peut la voir comme une "version galoisienne" de la cohomologie non abélienne

de Giraud. Elle permet de résoudre certaines questions relatives à l'existence de points rationnels, par des calculs de 2-cocycles. Le second outil, aujourd'hui très classique, est un procédé de dévissage d'un groupe algébrique lisse connexe sur un corps parfait k, à quotients successifs de l'un des types suivants: k-groupe étale, variété abélienne, groupe unipotent connexe déployé, tore, groupe semi-simple. Pour les questions considérées plus haut, ce dernier cas est de loin le plus délicat. Pour l'aborder efficacement, j'ai utilisé la théorie de Bruhat et Tits.

3

Dimension essentielle

Introduite par Buhler et Reichstein dans [5], la dimension essentielle mesure la complexité des structures algébro-géométriques.
On se fixe un corps de base k, et un "type de structure algébrique" $\mathcal{T}$. Par exemple, $\mathcal{T}$ peut être un espace vectoriel, une forme quadratique, une variété algébrique, ou un torseur sous un k-groupe algébrique donné.
Soit F une extension de k, et soit S une structure de type $\mathcal{T}$, sur le corps F. La dimension essentielle de S (sur k) est le nombre minimum de paramètres algébriquement indépendants sur k requis pour la définir. On la note $\mathrm{ed}_k(S)$. La dimension essentielle de $\mathcal{T}$ est le supremum des quantités $\mathrm{ed}_k(S)$, pour S décrivant toutes les structures de type $\mathcal{T}$ (sur toutes les extensions F/k). Ce nombre peut être infini. Il est cependant fini dans le cas particulier important où $\mathcal{T}$ = "G-torseurs", avec G un k-groupe algébrique linéaire.

Voyons quelques exemples, lorsque $k = \mathbb{Q}$.

Exemples 3.0.1. a) Prenons $\mathcal{T}$ = "endomorphisme diagonalisable ϕ d'un espace vectoriel V de dimension finie n". Un tel endomorphisme peut être défini, dans une base convenable de V, par n paramètres (ses valeurs propres, comptées avec multiplicités). La dimension essentielle de ϕ est ainsi au plus n, et il est facile de voir que cette borne est atteinte. On peut même retirer l'hypothèse "ϕ diagonalisable", en utilisant la forme de Frobenius.
b) Ici $\mathcal{T}$= "extension cubique de corps". Si E/F est cubique séparable, il est classique qu'il existe un élément $x \in E$ dont le polynôme minimal sur F s'écrit $x^3 + ax + a$. Si E/F est inséparable (ce qui implique que k est de caractéristique 3), on a un résultat analogue, avec x^3+a. La dimension essentielle d'une extension cubique est donc, en général, égale à 1. Pour une généralisation de ce résultat, due à Hermite, voir l'article récent [3].
c) La dimension essentielle d'une algèbre de quaternions "générique" est égale à 2.

Écartés les exemples simples, les calculs de dimension essentielle sont souvent hors de portée des techniques actuelles. Par exemple, la dimension essentielle des extensions séparables finies de degré n (qui est celle du groupe symétrique S_n) n'est connue que pour $n \leq 7$. Pour le cas $n = 7$, ce nombre est 4. C'est un résultat d'Alexandre Duncan. Pour $n \geq 8$, on a l'encadrement $\frac{n}{2} \leq \mathrm{ed}_{\mathbb{C}}(S_n) \leq n - 3$. Je

soupçonne fortement que la balance penche vers $n-3$.

Voici deux contributions au développement de la dimension essentielle.

3.1 Les p-groupes cycliques.

Dans [18], rédigé durant mon année de postdoctorat à l'École Polytechnique Fédérale de Lausanne, j'ai calculé la dimension essentielle des p-groupes cycliques.

Théorème 3.1.1. *([18], Theorem 4.1) Soit k un corps de caractéristique différente de p, contenant les racines p-ièmes de l'unité. Soit $r \geq 1$ un entier. Le degré de l'extension cyclotomique $k(\mu_{p^r})/k$, obtenue en adjoignant à k les racines p^r-ièmes de l'unité, est alors une puissance de p. Notons-la p^s. La dimension essentielle d'un p-groupe cyclique est alors donnée par*

$$\mathrm{ed}_k(\mathbb{Z}/p^r\mathbb{Z}) = p^s.$$

Par la suite, Karpenko et Merkurjev ont étendu ce résultat au cas d'un p-groupe G, comme suit. Le nombre $\mathrm{ed}_k(G)$ est égal à la plus petite dimension d'une représentation fidèle de G sur k ([34]). Dans la foulée, citons aussi l'article [4], qui avait créé la surprise: la dimension essentielle du groupe Spin_n croît exponentiellement avec n, sur tout corps de caractéristique $\neq 2$.
Il existe une notion "locale en p" de la dimension essentielle, qui se calcule bien mieux. Elle est définie comme la dimension essentielle, en se limitant aux corps F qui sont p-clos, c'est-à-dire qui n'ont pas d'extension finie de degré premier à p.

3.2 Formes traces.

Pour achever ce paragraphe sur la dimension essentielle, je voudrais discuter la publication [20]. Elle se distingue du reste de mes travaux par sa taille remarquable: trois pages seulement;-)
Soit l une k-algèbre séparable (non nécessairement commutative), de dimension finie n. Il est naturel de considérer sa trace réduite, comme forme bilinéaire non-dégénérée

$$\mathrm{Tr} = \mathrm{Tr}_{l/k} : l \times l \longrightarrow k,$$
$$(x, y) \mapsto \mathrm{Tr}(xy).$$

La k-algèbre l ne peut pas, en général, être récupérée à partir de la donnée de Tr. Par exemple, si l est commutatif, et si l/k est galoisienne de degré impair, Tr est isomorphe à la forme déployée $\sum_1^n x_i y_i$. C'est une porte d'entrée vers la théorie des bases normales autoduales de Bayer-Lenstra ([2]).
Dans [20], je démontre que la dimension essentielle de l/k est égale à celle de sa forme trace en trois variables (ou plus)

$$(x, y, z) \mapsto \mathrm{Tr}(xyz).$$

Ceci généralise un résultat de Reichstein.

4

Géométrie birationnelle et rationalité

Dans ce chapitre, j'évoque des résultats que j'ai obtenus concernant la (stable) rationalité de variétés algébriques, dans différents contextes. Ceux-ci sont pour la plupart positifs.

4.1 Autour des conjectures d'Amitsur et de Voskresenskiĭ.

Définition 4.1.1. *Soit F un corps, et soit X, Y deux F-variétés.*
On écrit $X \overset{\sim}{\dashrightarrow} Y$ pour signifier que X et Y sont F-birationnelles.
On dit que X est F-rationnelle si X est F-birationnelle à un espace affine $\mathbb{A}^n_F$ (ou à un espace projectif $\mathbb{P}^n_F$; c'est pareil).
On dit que X et Y sont stablement F-birationnelles, s'il existe $m, n \in \mathbb{N}$, avec $X \times \mathbb{A}^n_F \overset{\sim}{\dashrightarrow} Y \times \mathbb{A}^m_F$.
On dit que X est stablement F-rationnelle, s'il existe $n \in \mathbb{N}$, tel que $X \times \mathbb{A}^n_F$ est F-rationnelle.

Étudiant en thèse, j'ai (trop) longuement réfléchi à ces conjectures, sans les résoudre.

Conjecture 4.1.2. *($\mathcal{CA}$: Conjecture d'Amitsur) Soit F un corps. Soient A et B deux algèbres simples centrales sur F, de même degré, et engendrant le même sous-groupe cyclique du groupe de Brauer de F. Alors les variétés de Severi-Brauer $\mathcal{SB}(A)$ et $\mathcal{SB}(B)$ sont F-birationnelles.*

Conjecture 4.1.3. *($\mathcal{CV}$: Conjecture de Voskresenskiĭ) Soit F un corps. Soit T un tore algébrique sur F. Si T est une variété stablement F-rationnelle, alors T est F-rationnelle.*

Ces conjectures sont très largement ouvertes.
Il n'est pas difficile de démontrer la conjecture d'Amistur lorsque $B = A^{\mathrm{op}}$ est l'algèbre opposée de A, i.e. si $[B] = -[A]$ dans $\mathrm{Br}(F)$. Un résultat significatif, et de démonstration remarquable, est dû à Tregub ([42]). Il affirme que $\mathcal{C}A$ est vraie si $[B] = 2[A]$ dans $\mathrm{Br}(F)$ (ce qui sous-entend que A et B sont de degré impair).

Grâce aux travaux de Kunyavskiĭ et Lemire notamment, il est connu que $\mathcal{CV}$ est vraie pour les tores de dimension ≤ 3, et pour "presque" tous ceux de dimension 4.
Un beau théorème de Klyachko donne une classe intéressante de tores dont il n'est pas bien difficile de montrer la rationalité stable, mais dont la rationalité demande une étude bien plus soigneuse. Un tel tore T apparaît dans la suite exacte naturelle

$$1 \longrightarrow \mathbb{G}_m \overset{x\mapsto(x,x^{-1})}{\longrightarrow} \mathrm{R}_{A/F}(\mathbb{G}_m)\times\mathrm{R}_{B/F}(\mathbb{G}_m) \overset{(x,y)\mapsto xy}{\longrightarrow} \mathrm{R}_{A\otimes_F B/F}(\mathbb{G}_m) \longrightarrow T \longrightarrow 1,$$

où A/F et B/F sont deux algèbres étales, de degrés premiers entre eux, et où $\mathrm{R}_{./.}$ dénote la restriction de Weil. La démonstration de Klyachko, de nature cohomologique, ne fournit pas de paramétrisation explicite de T. Dans l'article [28] (collaboration avec Michel Van Garrel), on donne une démonstration constructive, menant à des isomorphismes birationnels facilement calculables, et donc bien adaptés à la cryptographie torique.

Notons qu'il est possible de formuler une question dont $\mathcal{CA}$ et $\mathcal{CV}$ sont des cas particuliers. Elle est bien connue des spécialistes.

Question 4.1.4. Soit F un corps. Soient T et T' deux tores algébriques sur F, de même dimension. Soit X (resp. X') un torseur sous T (resp. sous T'). On suppose que les variétés X et X' sont stablement F-birationnelles. Sont-elles alors F-birationnelles?

Les conjectures $\mathcal{CA}$ (où $T = T'$ est de la forme $\mathrm{R}_{E/F}(\mathbb{G}_m)/\mathbb{G}_m$, avec F/E une extension finie séparable) et $\mathcal{CV}$ (où T' est déployé, et où les torseurs X et X' sont triviaux) en sont les cas opposés.
J'attends une réponse positive à la conjecture d'Amitsur, mais suis plus réservé concernant celle de Voskresenskiĭ.

Dans [19], je m'intéresse à des questions de géométrie birationnelle équivariante, naturellement soulevées par $\mathcal{CA}$ et $\mathcal{CV}$. Le résultat principal de cet article s'énonce ainsi. Sa démonstration, délicate, peut être vue comme une géométrisation de l'algorithme d'Euclide.

Théorème 4.1.5. *Soit F un corps. Soit A/F une algèbre étale, de degré n. Posons*

$$G := \mathbb{R}_{A/F}(\mathbb{G}_m)/\mathbb{G}_m = \mathrm{PGL}_1(A);$$

c'est un tore algébrique sur F. Soit $1 \leq r \leq n$ un entier, et soit $d := \mathrm{pgcd}(r,n)$. Alors il existe un isomorphisme birationnel G-équivariant

$$\mathrm{Gr}(r,A) \overset{\sim}{\dashrightarrow} \mathrm{Gr}(d,A)\times\mathbb{P}^N,$$

où $\mathrm{Gr}(r,A)$ désigne la Grassmannienne des r-plans de A, munie de l'action multiplicative naturelle de G, et où $\mathbb{P}^N$ est un espace projectif de dimension convenable, sur lequel G agit trivialement.

Remarque 4.1.6. Au niveau des F-points, l'action de G sur $\mathrm{Gr}(r,A)$ est définie comme suit. Si $V \subset A$ est un sous-F-vectoriel, et si $a \in A^\times$, on a

$$a.V := \{a.v, v \in V\}.$$

Par torsion (par des $\mathrm{PGL}_1(A)$-torseurs bien choisis), j'en déduis plusieurs résultats de rationalité, anciens et nouveaux. En particulier, on peut retrouver le théorème de Klyachko mentionné plus haut- ainsi qu'un célèbre théorème d'Enriques, Manin et Swinnerton-Dyer: la rationalité des surfaces de Del Pezzo de degré cinq (voir [39]). Ceci a été le point de départ d'un travail en commun avec Zinovy Reichstein, que je vais maintenant discuter.

4.2 Formes des espaces de modules de courbes marquées.

Soit $g \geq 0$ et $n \geq 1$ deux entiers. Soit F un corps. L'espace de modules des courbes de genre g, marquées par n points distincts ordonnés, est un objet médiatique en géométrie algébrique. Pour simplifier, j'ai choisi d'appeler ici $\mathcal{M}_{g,n}$ l'espace de modules grossier des courbes C/F, lisses, connexes et de genre g, marquées par n points distincts. C'est donc une F-variété. Les problèmes abordés ici étant de nature birationnelle, il n'est en réalité pas si important de savoir si l'on regarde $\mathcal{M}_{g,n}$ ou sa compactification $\overline{\mathcal{M}_{g,n}}$ (donnée par les courbes marquées stables). Je supposerai partout que l'on a $2g+n \geq 5$, ce qui implique que le groupe d'automorphismes d'une courbe marquée 'générique' est trivial.
Par les travaux de Bruno-Mella et Fantechi-Massarenti ([25]), on a le résultat suivant.

Théorème 4.2.1. *(BMFM) Le morphisme*

$$S_n \longrightarrow \mathrm{Aut}_F(\overline{\mathcal{M}_{g,n}}),$$

donné par l'action naturelle du groupe symétrique S_n, est un isomorphisme.

On attend le même résultat pour

$$S_n \longrightarrow \mathrm{Aut}_F(\mathcal{M}_{g,n});$$

cela ne figure pas dans la littérature.

Un question tout à fait naturelle est de considérer les courbes marquées, non pas par n points, mais par un point dans une E-algèbre étale de degré n. Plus précisément, soit E/F une algèbre étale de degré n. On peut alors définir une F-variété $\mathcal{M}^E_{g,n}$ (resp. sa compactification $\overline{\mathcal{M}^E_{g,n}}$) comme l'espace de modules de F-courbes lisses (resp. stables) C, de genre g, équipées d'un F-plongement (=immersion fermée)

$$\mathrm{Spec}(E) \longrightarrow C.$$

Si $E = F^n$, on retrouve les espaces de modules classiques. Si E/F est $\mathbb{C}/\mathbb{R}$, on obtient une variété réelle, dont les points sur $\mathbb{R}$ sont donnés par des courbes sur $\mathbb{R}$, équipées d'un point complexe non réel.

On sait que E/F est donnée par un S_n-torseur P sur F. Explicitement, P est le F-schéma (fini étale) des isomorphismes entre E et l'algèbre étale déployée F^n. Par descente galoisienne, on peut tordre $\mathcal{M}_{g,n}$ (ou $\overline{\mathcal{M}_{g,n}}$) par P; c'est le produit contracté

$${}^P\mathcal{M}_{g,n} := (P \times_F \mathcal{M}_{g,n})/S_n.$$

On a alors des isomorphismes canoniques

$$^P\mathcal{M}_{g,n} \simeq \mathcal{M}^E_{g,n}$$

et

$$^P\overline{\mathcal{M}_{g,n}} \simeq \overline{\mathcal{M}^E_{g,n}}.$$

Par le théorème BMFM cité plus haut, combiné au yoga des formes, on voit ainsi que toute F-forme de la variété $\overline{\mathcal{M}_{g,n}}$ est du type $\overline{\mathcal{M}^E_{g,n}}$, pour une algèbre étale E/F, de degré n.
Nous allons nous intéresser à la rationalité de $\mathcal{M}^E_{g,n}$. Pour une discussion de l'état de la connaissance sur la rationalité (ou non) de la forme déployée $\mathcal{M}_{g,n}$, je renvoie à [27]. Je rappelle simplement que $\mathcal{M}_{0,n}$ est F-rationnelle, puisqu'isomorphe à l'ouvert de $(\mathbb{P}^1)^{n-3}$ formé des $(n-3)$-uplets de points distincts, distincts de $0, 1$ et ∞.
Le théorème principal de [26], en collaboration avec Zinovy Reichstein, est le suivant.

Théorème 4.2.2. *Soit F un corps infini.*
Si $n \geq 5$ est impair, alors toute F-forme de $\overline{\mathcal{M}_{0,n}}$ est une variété F-rationnelle.
Supposons maintenant $n \geq 6$ pair, F de caractéristique $\neq 2$, -1 carré dans F, et la 2-torsion du groupe de Brauer de F non triviale (exemple: $F = \mathbb{C}(x, y)$). Il existe alors une F-forme de $\overline{\mathcal{M}_{0,n}}$ qui n'est pas une variété F- rationnelle.

Remarque 4.2.3. Les F-formes de $\overline{\mathcal{M}_{0,n}}$ sont toujours F-unirationnelles. Pour n pair, sous les hypothèses précédentes, on construit en réalité une forme de $\overline{\mathcal{M}_{0,n}}$ qui n'est pas rétract-rationnelle, au sens de Saltman. Rappelons qu'une variété intègre est dite rétract-rationnelle, si son morphisme "identité" se factorise rationnellement par un espace affine.

Dans l'article [27], en collaboration avec Norbert Hoffmann et Zinovy Reichstein, on étudie les formes de $\overline{\mathcal{M}_{g,n}}$, en genre $g \geq 1$. On s'intéresse cette fois à leur stable F-rationalité. Les principaux résultats obtenus se résument comme suit.

Théorème 4.2.4. *Soit F un corps, de caractéristique $\neq 2$.*
Les F-formes de $\overline{\mathcal{M}_{g,n}}$ sont alors des variétés stablement F-rationnelles, dans tous les cas suivants.

On a $g = 2$ et $2 \leq n \leq 3$;
On a $g = 3$ et $1 \leq n \leq 14$;
On a $g = 4$ et $1 \leq n \leq 9$;
On a $g = 5$ et $1 \leq n \leq 12$.

Remarque 4.2.5. Pour tous les couples (g, n) listés ci-dessus, la F-rationalité des espaces $\overline{\mathcal{M}_{g,n}}$ est bien connue, par les travaux de Logan et de Casnati-Fontanari ([7]). Pour montrer la stable rationalité de leurs formes, on utilise des techniques bien différentes.

Remarque 4.2.6. Dans certains cas, on arrive à montrer la F-rationalité des formes, au prix d'efforts plus coûteux. La stable rationalité s'obtient par une méthode uniforme. La philosophie consiste à traiter les n points marqués de manière symétrique. Dans chaque cas, certaines "coïncidences numériques" jouent un rôle crucial- par exemple le fait que le degré d'un certain fibré en droite, et la dimension de son espace de sections globales, soient premiers entre eux.

Remarque 4.2.7. On ne sait pas s'il existe un corps F, et un couple (g, n), avec $g \geq 1$, tels que $\overline{\mathcal{M}_{g,n}}$ soit F-rationnelle, mais admette une F-forme non rationnelle.

4.3 Action adjointe d'un groupe algébrique sur son algèbre de Lie.

Soit G un groupe algébrique linéaire, connexe, réductif et déployé, sur un corps k. Soit $\mathfrak{G}$ son algèbre de Lie, munie de l'action adjointe de G. Suivant les lignes de [8], il est naturel de se demander si l'extension de corps $k(\mathfrak{G})/k(\mathfrak{G})^G$ est transcendante pure. Dans *loc. cit.*, les auteurs réduisent la question au cas G simple, et démontrent que la réponse est alors affirmative pour les types A_n et C_n, et négative pour les autres types- sauf peut-être pour G_2. Dans la note [1], écrite avec D. Anderson et Z. Reichstein, on traite ce dernier cas: pour $G = G_2$, $k(\mathfrak{G})$ est purement transcendante sur son corps des invariants. Voici les grandes lignes de la démonstration. Passée à la moulinette de la cohomologie galoisienne, la question devient équivalente à la rationalité d'une certaine hypersurface cubique- qui ne peut être tranchée par aucune technique connue. Le point-clé est alors d'effectuer un changement de variables astucieux, permettant de convertir cette cubique en une quadrique. Il est facile de voir que celle-ci possède un zéro-cycle de degré 3, et l'on conclut à l'aide du théorème de Springer.

5

Un peu de caractéristique positive.

5.1 Critère valuatif pour les générateurs de bases normales.

Soit L/K une extension de corps finie et galoisienne, de groupe G. Il est classique que L/K possède un générateur de base normale. Précisément, il existe $x \in L$ tel que l'ensemble $\{g.x, g \in G\}$ forme une base de L sur K. On appelera un tel élément x *normal*.
Lorsque K est un corps local (i.e. complet pour une valuation discrète), on peut se demander s'il existe un critère valuatif assurant qu'un élément donné $x \in L$ est normal. Cette question a été soulevée par Byott et Elder ([6]).

Définition 5.1.1. *Soit $d \in \mathbb{Z}$. On dira que le critère $VC(L/K, d)$ est vérifié si tout élément de L, de valuation d, est normal.*

En collaboration avec Bart de Smit et Lara Thomas, on démontre dans [15] que $VC(L/K, d)$ équivaut à la combinaison des propriétés suivantes.

(1) L'extension L/K est sauvagement ramifiée (i.e totalement ramifiée, de degé e une puissance de la caractéristique résiduelle $p > 0$).
(2) On a $d \equiv -d_{L/K} - 1 \bmod e$, où $d_{L/K}$ est la valuation de la différente de L/K.
(3) Tout sous-$K[G]$-module de L contient un élément de valuation non nulle.

Définition 5.1.2. *Si (1), (2) et (3) sont réalisés, on dira simplement que $VC(L/K)$ est vérifié.*

Dans [40], Lara Thomas donne une condition nécessaire et suffisante pour que $VC(L/K)$ soit vérifié, dans le cas d'égale caractéristique. Avec Bart De Smit et Lara Thomas, nous nous intéressons au cas délicat de l'inégale caractéristique. On obtient le résultat suivant. Avant de l'énoncer, rappelons qu'une extension galoisienne finie L/K est dite de Kummer, lorsque son groupe de Galois est abélien d'exposant $m \geq 1$, les racines m-ièmes de l'unité étant contenues dans K.

Théorème 5.1.3. *[15, Theorem 1.3] Soit L/K une extension de Kummer sauvagement ramifiée. Alors $VC(L/K)$ est vérifié si et seulement si L/K est Kummer-unitaire, i.e. si L s'obtient en extrayant des racines d'unités de $\mathcal{O}_K$.*

On étend ensuite cet énoncé au cas d'une extension sauvagement ramifiée abélienne ([15, Theorem 1.4]).

5.2 Algèbres simples centrales et longueur de symboles.

Soit F un corps, et soit p un nombre premier. Soit A/F une algèbre centrale simple, d'indice p^d et d'exposant p^e.
Supposons, dans un premier temps, que $p \in F^\times$, et que F contient les racines p^e-ièmes de l'unité. Fixons un isomorphisme $\mathbb{Z}/p^e\mathbb{Z} \simeq \mu_{p^e}$. Soit alors $c \in H^2(\mathrm{Gal}(F_s/F), \mu_{p^e}^{\otimes 2})$ la classe de cohomologie de A. Par le théorème de Merkurjev-Suslin (voir [31]), on sait alors que c peut s'écrire comme un cup-produit

$$c = \sum_{i=1}^{N} (a_i) \cup (b_i),$$

avec $a_i, b_i \in F^\times$. En d'autres termes, A est équivalente à un produit tensoriel $\bigotimes_{i=1}^{N} A_i$, où $A_i = (a_i, b_i)$ est l'algèbre cyclique de degré p^e associée à a_i et à b_i. L'algèbre A étant donnée, très peu de choses sont connues sur la valeur minimale possible pour N. Si $d = e = 1$, il n'est pas bien difficile de démontrer qu'elle est $\leq (p-1)!$, en utilisant le lemme de Rosset et Tate en K-théorie de Milnor. À ma connaissance, une borne comparable n'est pas connue si $d \geq 2$. La première difficulté est alors que l'algèbre "générique", d'indice p^d et d'exposant p^e, ne peut être rendue cyclique par une extension de degré premier à p.
Supposons maintenant, et jusqu'à la fin de cette section, que F est de caractéristique p. L'étude de la cohomologie galoisienne modulo p de F est alors bien plus simple, grâce notamment à la théorie d'Artin-Schreier. Un résultat dû à Teichmüller affirme alors que A est équivalente à un produit tensoriel de $p^d!(p^d! - 1)$ algèbres cycliques de degré p^e. Dans l'article [21], j'en donne une nette amélioration, comme suit.

Théorème 5.2.1. *([21, Thm 1.1]) Soit F un corps de caractéristique $p > 0$. Soit A/F une algèbre simple centrale, d'indice p^d et d'exposant p^e. Alors A est Brauer-équivalente à un produit tensoriel de $p^d - 1$ algèbres cycliques de degré p^e.*

Au cours de la preuve, je propose une nouvelle démonstration d'un résultat de Albert (attribué à Hochschild dans [31], Theorem 9.1.1), donnant une description explicite du noyau de la restriction $\mathrm{Br}(F) \longrightarrow \mathrm{Br}(E)$, pour une extension E/F purement inséparable.

6

Caractéristique positive et théories galoisiennes.

6.1 Ind-variétés de déploiement.

Soit k un corps infini, de groupe de Galois absolu $G = \mathrm{Gal}(k_s/k)$. Soit d un entier inversible dans F.
Par la théorie de Kummer, on a un isomorphisme naturel $k^\times/(k^\times)^d \xrightarrow{\sim} H^1(k, \mu_d)$. C'est la composante de degré un de l'anneau gradué $H(k) := \bigoplus_{n=0}^{\infty} H^n(k, \mu_d^{\otimes n})$, qui joue un rôle central en géométrie algébrique. La conjecture de Bloch-Kato, promue en théorème grâce aux travaux de Rost, Suslin, Voevodsky et Weibel, stipule que $H(k)$ est engendré en degré un, avec les relations quadratiques données par Steinberg: $(x) \cup (1-x) = 0$, pour tout $x \in k - \{0, 1\}$. La démonstration proposée utilise la cohomologie motivique de Voevodsky, appliquée aux variétés de normes de Rost. Plus précisément, soit $x_1, \ldots, x_n \in k^\times$. Lorsque $d = p$ est premier, Rost définit une k-variété $X = X(x_1, \ldots, x_n)$, telle que, sur toute extension l de k, la présence d'un zéro-cycle de degré premier à p sur X_l est équivalente à la trivialité du symbole $\mathrm{Res}((x_1) \cup \ldots \cup (x_n)) \in H^n(l, \mu_p^{\otimes n})$ (voir [38]). La variété X, projective et lisse, de dimension $p^{n-1} - 1$, est bien comprise géométriquement. Sa construction est algorithmique. C'est une variété de norme, pour le symbole pur $c = (x_1) \cup \ldots \cup (x_n)$. Pour un élément arbitraire (non pur) $c \in H^n(k, \mu_p^{\otimes n})$, on ne sait pas s'il existe une variété de norme pour c. Dans un travail avec Cyril Demarche ([14]), on démontre le résultat suivant.

Théorème 6.1.1. *Soit A un G-module discret, fini et de d-torsion sur k (en abrégé: un $(\mathbb{Z}/d, G)$-module).*
Soit $n \geq 2$, et soit c un élément du groupe de cohomologie galoisienne $H^n(k, A)$.
Il existe alors une ind-k-variété $X = X(c)$, telle que, pour toute extension l/k, $X(l)$ est non vide si et seulement si $\mathrm{Res}(c) \in H^n(l, A)$ est trivial.

Voici quelques remarques.
1) Une ind-k-variété est une limite $\varinjlim X_i$ de k-variétés, indexée par $i \in \mathbb{N}$, et où les morphismes de transition $X_i \longrightarrow X_{i+1}$ sont des immersions fermées. Dans l'énoncé du théorème, les X_i sont affines, lisses et géométriquement intègres.
2) Comme l'a remarqué Colliot-Thélène, pour toute extension l/k, on a $X(l) \neq \varnothing$

si et seulement si X possède un zéro-cycle de degré 1 sur l.
3) Lorsque $n = 2$, on peut prendre pour $X = X_0$ une k-variété. Ce résultat était déjà connu, par les travaux de Daniel Krashen ([33], Theorem 6.3).
4) On obtient en réalité un résultat un peu plus fort, concernant les éléments c des groupes ${\mathrm{Ext}_{\mathrm{G}}}^n(A, B)$, où A et B sont $(\mathbb{Z}/d, G)$-modules. En tout état de cause, notre point de vue consiste à interpréter c comme la classe (à la Yoneda) d'un complexe de $(\mathbb{Z}/d, G)$-modules. Sa trivialité équivaut à l'existence de certains diagrammes de $(\mathbb{Z}/d, G)$-modules. Un point essentiel dans la démonstration est alors la construction de variétés de relèvements pour les torseurs ([14], Proposition 2.1). Celle-ci étend la construction des torseurs versels, pour les groupes algébriques linéaires, aux morphismes de groupes algébriques linéaires. On l'applique à des surjections bien choisies entre les groupes finis d'automorphismes de diagrammes, construits suivant une étude attentive des complexes de $\mathbb{Z}/d\mathbb{Z}$-modules.
On ne sait pas si l'on peut remplacer "ind-variété" par "variété" dans l'énoncé du théorème. Je soupçonne que c'est possible.

6.2 Relèvement des fibrés en vecteurs de Witt.

Soit p un nombre premier. Pour un entier $r \geq 1$, je désigne par $\mathbf{W}_r$ les vecteurs de Witt p-typiques de longueur r. On peut les voir comme une structure naturelle de schéma en anneaux sur l'espace affine $\mathbb{A}^r$, définie sur $\mathbb{Z}$. On a $\mathbf{W}_r(\mathbb{F}_p) = \mathbb{Z}/p^r\mathbb{Z}$.
Soit S un schéma de caractéristique p. Pour un entier $r \geq 1$, on appelle fibré en vecteurs de Witt sur S, de hauteur r (ou simplement $\mathbf{W}_r$-fibré), un faisceau localement libre de rang fini de $\mathbf{W}_r(\mathcal{O}_S)$-modules sur S, pour la topologie de Zariski. De manière équivalente, un $\mathbf{W}_r$-fibré est un fibré vectoriel sur l'épaississement $\mathbf{W}_r(S)$ de S.
Avec Charles De Clercq et Giancarlo Lucchini-Arteche, nous avons initié dans [12] l'étude systématique des $\mathbf{W}_r$ fibrés en vecteurs de Witt, et de leurs relèvements à des $\mathbf{W}_s$-fibrés, pour $s > r$. À ma connaissance, cette approche n'avait jamais été considérée dans la littérature. Néanmoins, elle est reliée à la question du relèvement des variétés, lisses sur un corps parfait k de caractéristique p, en schémas lisses sur $\mathbf{W}_r(k)$. Celle-ci est le sujet d'une intense activité mathématique, depuis les travaux de Deligne-Illusie ([13]). Le cas $r = 2$ est déjà très riche!

Avant de poursuivre, je souhaite préciser que le relèvement des $\mathbf{W}_r$-fibrés, tel qu'envisagé dans [12], n'est pas une finalité. Ce travail sert de fondation géométrique pour aborder efficacement la délicate question du relèvement des (drapeaux complets) de représentations galoisiennes modulo p. Ce point est évoqué dans la section suivante. Je vais maintenant discuter certains résultats choisis dans [12].

Soit L un fibré en droites sur S, et soit $r \in \mathbb{N} \cup \{\infty\}$ un nombre. En utilisant la section multiplicative de Teichmüller, $\tau_r : \mathbf{W}_1^\times \longrightarrow \mathbf{W}_r^\times$, il n'est pas difficile de montrer que L se relève fonctoriellement en un $\mathbf{W}_r$-fibré en droites sur S, noté $\mathbf{W}_r(L)$ ([12], section 3). Je souhaite promouvoir l'utilisation systématique de ce procédé, qui n'a jamais été exploité dans la littérature- peut-être parce qu'il est trop évident. En voici trois nouvelles applications.
Soit L un fibré en droite sur S. Soit $P = \mathrm{Spec}(\bigoplus_{n\in\mathbb{Z}} L^{\otimes n}) \longrightarrow S$ le $\mathbb{G}_m$-torseur associé à L. Dans [12], section 3.3, on propose une description nouvelle, simple et explicite, du schéma $\mathbf{W}_r(P)$.
Soit V un fibré vectoriel sur S. Dans [12], Proposition 5.29, on donne une descrip-

tion explicite de la catégorie des relèvements de V en un $\mathbf{W}_2$-fibré. Celle-ci utilise, entre autres, le relevé $\mathbf{W}_2(\mathcal{O}(1))$ du fibré en droites $\mathcal{O}(1)$ sur le fibré projectif $\mathbb{P}_S(V)$. Comme corollaire, on obtient une description, concrète et nouvelle, de la classe de 2-cohomologie qui tranche le problème d'existence d'un tel relèvement.

Théorème 6.2.1. *([12], Remark 5.30).*
Soit V un fibré vectoriel sur S. L'obstruction à relever V en un $\mathbf{W}_2$-fibré est la classe, dans $\mathrm{Ext}^2_{\mathcal{O}_S}(\mathrm{Frob}^*(V), \mathrm{Frob}^*(V))$, de la 2-extension naturelle de fibrés vectoriels sur S

$$0 \longrightarrow \mathrm{Frob}^*(V) \overset{\mathrm{Ver_V}}{\longrightarrow} \mathrm{Sym}^p_{\mathcal{O}_S}(V) \longrightarrow \Gamma^p_{\mathcal{O}_S}(V) \overset{\mathrm{Frob_V}}{\longrightarrow} \mathrm{Frob}^*(V) \longrightarrow 0.$$

J'ai noté par

$$\mathrm{Ver_V} : \mathrm{Frob}^*(V) \longrightarrow \mathrm{Sym}^p_{\mathcal{O}_S}(V),$$
$$v \mapsto v^p$$

le Verschiebung de V, et par $\mathrm{Frob_V}$ son Frobenius, dual de $\mathrm{Ver_{V^\vee}}$.

Remarque 6.2.2. Le résultat précédent est présenté géométriquement. Si l'on souhaite le concevoir de manière purement algébrique, on voudra peut-être échanger les appellations "Verschiebung" et "Frobenius".

Grâce à un calcul, court mais délicat, d'extensions de fibrés vectoriels sur une grassmannienne, on démontre le résultat suivant.

Théorème 6.2.3. *([12], Theorem 5.32).*
Soit m et n deux entiers, avec $2 \leq m \leq n-2$. Alors, sur toute base S de caractéristique p, le fibré tautologique sur la grassmannienne $\mathrm{Gr}(m,n)$ (des m-plans d'un vectoriel de dimension n) ne se relève pas en un $\mathbf{W}_2$-fibré.

Remarque 6.2.4. En utilisant la fonctorialité du relèvement multiplicatif des fibrés en droites, ou à l'aide d'un calcul de cohomologie cohérente, on peut montrer que le fibré tautologique se relève lorsque $m = n-1$ ([12], section 4).

Dans l'appendice de [12], on propose une contruction algébrique nouvelle des vecteurs de Witt p-typiques, par générateurs et relations, à l'aide du foncteur $\Gamma^p_{\mathbb{Z}}$-des p-ièmes puissances divisées de $\mathbb{Z}$-modules.

6.3 Groupes profinis lisses, relèvements modulo p^2.

Soit p un nombre premier.
Considérons la tâche suivante.

(T_2): Caractériser les groupes profinis G, tels que toute représentation (continue, de dimension finie)

$$\rho_1 : G \longrightarrow \mathbf{GL}_d(\mathbb{F}_p)$$

se relève modulo p^2, en

$$\rho_2 : G \longrightarrow \mathbf{GL}_d(\mathbb{Z}/p^2).$$

Il est bien sûr naturel de s'intéresser à l'existence de relèvements $\rho_r : G \longrightarrow \mathbf{GL}_d(\mathbb{Z}/p^r)$, pour $r \geq 3$, ainsi qu'à un relèvement p-adique $\rho_\infty : G \longrightarrow \mathbf{GL}_d(\mathbb{Z}_p)$. Dans ce mémoire, j'ai choisi de n'exposer que les résultats relatifs aux relèvements modulo p^2. À bien des égards, c'est une question suffisamment délicate.
La tâche T_2 est un objet d'étude extrêmement médiatique en théorie des nombres,

dans l'univers des représentations galoisiennes des corps locaux et globaux. On y pose l'hypothèse supplémentaire que $G = \mathrm{Gal}(F_s/F)$ est le groupe de Galois absolu d'un corps local ou global F. Des questions de ramification apparaissent alors naturellement, et leur contrôle conduit à des problèmes complexes, que je n'aborderai pas ici. Par ailleurs, les méthodes que je souhaite promouvoir diffèrent largement des techniques habituellement employées dans ce contexte.
La formulation de (T_2) est venue naturellement, lors de la recherche d'une démonstration "élémentaire" de la conjecture de Bloch et Kato- un théorème de Rost, Suslin, Voevodsky et Weibel. Le point de départ de cette recherche est l'intuition suivante.

(I_2): Soit $G = \mathrm{Gal}(F_s/F)$ le groupe de Galois absolu d'un corps F, de caractéristique différente de p. Soit $n \geq 1$ un entier.
La surjectivité de la flèche

$$s_n : H^n(G, \mu_{p^2}^{\otimes n}) \longrightarrow H^n(G, \mu_p^{\otimes n})$$

serait conséquence formelle de la surjectivité de

$$s_1 : H^1(H, \mu_{p^2}) \longrightarrow H^1(H, \mu_p),$$

pour tout sous-groupe ouvert $H \subset G$.

Notons que la surjectivité de s_n entraîne la validité de la conjecture de Bloch et Kato, à un coût raisonnable. Voir, par exemple, [30].
Je souhaite rendre apparent le lien entre (T_2) et (I_2). Il sera clairement établi lorsque j'aurai énoncé, un peu plus bas, le Théorème de Lissité 6.3.5.
Commençons par énoncer une variante "filtrée" de (T_2).
Désignons par $\mathbf{B}_d \subset \mathbf{GL}_d$ le sous-groupe de Borel des matrices triangulaires supérieures.

$(T_{2,fil})$: Caractériser les groupes profinis G, tels que toute représentation munie d'un drapeau complet (continue, de dimension finie)

$$\rho_1 : G \longrightarrow \mathbf{B}_d(\mathbb{F}_p)$$

se relève modulo p^2, en

$$\rho_2 : G \longrightarrow \mathbf{B}_d(\mathbb{Z}/p^2).$$

Par un argument de restriction-corestriction relativement à un pro-p-Sylow de G, on montre que les groupes vérifiant la propriété de $(T_{2,fil})$, vérifient aussi celle de (T_2) ([22], Corollary 12.10).
Supposons momentanément que $G = \mathrm{Gal}(F_s/F)$ est le groupe de Galois absolu d'un corps F, de caractéristique différente de p.
La suite exacte de Kummer

$$1 \longrightarrow \mu_p \longrightarrow \mu_{p^2} \longrightarrow \mu_p \longrightarrow 1$$

donne lieu à une surjection

$$s_1 : H^1(G, \mu_{p^2}) \twoheadrightarrow H^1(G, \mu_p).$$

Ceci découle du théorème 90 de Hilbert.
Pour faire le rapprochement avec les drapeaux de représentations (aussi appelés représentations complètement filtrées), on utilise la description

$$H^1(G, \mu_p) = \mathrm{Ext}^1_{(\mathbb{F}_p, G)}(\mathbb{F}_p, \mu_p),$$

où le membre de droite désigne le groupe (des classes d'isomorphie) d'extensions de représentations de G sur $\mathbb{F}_p$

$$\mathcal{E}_1 : 0 \longrightarrow \mu_p \longrightarrow E_1 \longrightarrow \mathbb{F}_p \longrightarrow 0.$$

La représentation E_1, de dimension 2, est munie d'un drapeau complet évident, dont les termes gradués sont μ_p et $\mathbb{F}_p$. Il lui correspond ainsi un morphisme

$$\rho_1 : G \longrightarrow \mathbf{B}_2(\mathbb{F}_p).$$

On a la description analogue pour les représentations modulo p^2, c'est-à-dire les $\mathbb{Z}/p^2$-modules libres munis d'une action continue de G.
La surjectivité de s_1 montre alors que $\mathcal{E}_1$ se relève en

$$\mathcal{E}_2 : 0 \longrightarrow \mu_{p^2} \longrightarrow E_2 \longrightarrow \mathbb{Z}/p^2 \longrightarrow 0.$$

En particulier, ρ_1 se relève en

$$\rho_2 : G \longrightarrow \mathbf{B}_2(\mathbb{Z}/p^2).$$

En utilisant le relèvement de Teichmüller, on étend le procédé aux drapeaux complets de dimension 2, de gradués quelconques. Ceci montre que $G = \mathrm{Gal}(F_s/F)$ vérifie la conclusion de (T_2), en dimension $d = 2$.
Pour s'attaquer à (T_2) en toute généralité, la stratégie employée dans [11] et [22] consiste tout d'abord à axiomatiser la théorie de Kummer. Ceci conduit à la définition d'une paire cyclotomique.
À partir de maintenant, G désigne un groupe profini quelconque, et $e \in \mathbb{N} \cup \{\infty\}$ est un nombre. Je noterai par $\mathbb{Z}/p^{1+e}(1)$ un $\mathbb{Z}/p^{1+e}$-module libre de rang 1, muni d'une action continue de G (avec la convention $\mathbb{Z}/p^\infty = \mathbb{Z}_p$). Si M est un $\mathbb{Z}_p$-module, je pose $M(1) := M \otimes_{\mathbb{Z}_p} \mathbb{Z}/p^{1+e}(1)$. En première approche, cette notation semble porter à confusion, dans les exemples et applications où G est le groupe fondamental d'un schéma où p est inversible. Pour y remédier, je préciserai alors si $\mathbb{Z}/p^{1+e}(1)$ désigne le module habituel, des racines de l'unité (ou le module de Tate lorsque $e = \infty$).

Définition 6.3.1. *Soit $e \in \mathbb{N} \cup \{\infty\}$. Une paire $(1, e)$-cyclotomique est la donnée d'un couple $(G, \mathbb{Z}/p^{1+e}(1))$, où $\mathbb{Z}/p^{1+e}(1)$ est un $\mathbb{Z}/p^{1+e}$-module libre de rang un, muni d'une action continue d'un groupe profini G, vérifiant la condition suivante. Pour tout sous-groupe ouvert $H \subset G$, la flèche naturelle*

$$H^1(H, \mathbb{Z}/p^{1+e}(1)) \longrightarrow H^1(H, \mathbb{F}_p(1)),$$

fournie par la réduction $\mathbb{Z}/p^{1+e}(1) \longrightarrow \mathbb{F}_p(1)$, est surjective.

Dans [10], écrit en collaboration avec Charles De Clercq, on donne beaucoup d'exemples de paires cyclotomiques. Par exemple, considérons les schémas X de l'un des types suivants.

1) Un schéma semi-local où p est inversible.
2) Une courbe lisse sur un corps algébriquement clos.
3) Un schéma affine de caractéristique p.

Soit $G = \pi_1(X)$ le groupe fondamental de X, et soit $\mathbb{Z}/p^{1+e}(1)$ le caractère p^{1+e}-cyclotomique usuel dans les cas 1) et 2), ou le caractère trivial $\mathbb{Z}/p^{1+e}$ dans le cas

3). Alors, la paire $(G, \mathbb{Z}/p^{1+e}(1))$ est $(1, e)$-cyclotomique.

Dans la suite, je vais me limiter aux paires $(1, 1)$-cyclotomiques. C'est déjà beaucoup.
Le résultat principal de [11], en collaboration avec Charles De Clercq, est le théorème de relèvement faible. C'est une amélioration des coefficients dans la définition 6.3.1, où $\mathbb{F}_p$ est remplacé par une $(\mathbb{F}_p, G)$-algèbre parfaite.

Théorème 6.3.2. *([11], Theorem 9.1)*
Soit $(G, \mathbb{Z}/p^2(1))$ une paire $(1, 1)$-cyclotomique. Soit A une $\mathbb{F}_p$-algèbre parfaite, munie d'une action de G, dont le noyau est ouvert. Soit $H \subset G$ un sous-groupe ouvert. Alors la flèche naturelle

$$H^1(H, \mathbf{W}_2(A)(1)) \longrightarrow H^1(H, A(1))$$

est surjective.

La démonstration de ce théorème met en jeu un résultat algébrique captivant: le théorème intégral de Frobenius (FIT, [11], Theorem 10.3).
Sous l'éclairage du théorème de relèvement faible, on est amené à poser la définition suivante. Elle est intrinsèque au groupe profini G.

Définition 6.3.3. *Un groupe profini est dit $(1, 1)$-lisse, si la propriété suivante vaut.*
Soit A une $\mathbb{F}_p$-algèbre parfaite, munie d'une action de G, dont le noyau est ouvert. Alors la flèche naturelle

$$H^1(G, \mathbf{B}_2(\mathbf{W}_2(A))) \longrightarrow H^1(G, \mathbf{B}_2(A))$$

est surjective.

Le théorème de relèvement faible implique alors que, si $(G, \mathbb{Z}/p^2(1))$ est une paire $(1, 1)$-cyclotomique, le groupe G est $(1, 1)$-lisse. En particulier, les groupes fondamentaux des schémas semi-locaux sont $(1, 1)$-lisses.

Le résultat principal de [22] s'énonce alors simplement. C'est un résultat de relèvement inconditionnelle des drapeaux complets de représentations semi-linéaires des groupes 1-lisses.

Théorème 6.3.4. *([22], Uplifting Theorem, énoncé 11.2)*
Soit G un groupe $(1, 1)$-lisse. Soit $d \geq 2$ un entier. Soit A une $\mathbb{F}_p$-algèbre parfaite, munie d'une action de G, dont le noyau est ouvert. Alors la flèche naturelle

$$H^1(G, \mathbf{B}_d(\mathbf{W}_2(A))) \longrightarrow H^1(G, \mathbf{B}_d(A))$$

est surjective.

La démonstration de ce théorème est, de très loin, la plus délicate que j'ai écrite. Elle nécessite trois ingrédients principaux, en caractéristique p.
1) Les fibrés G-linéarisés en vecteurs de Witt, sur un G-schéma.
2) Des extensions naturelles de fibrés vectoriels sur des schémas de drapeaux, et leurs schémas de déploiement.
3) De bonnes filtrations sur les modules quasi-cohérents, permettant des raisonnements par dévissage.

Ces points sont abordés en détails dans les neuf premières sections de [22].

Ce théorème s'étend formellement à une vaste collection de groupes algébriques lisses résolubles, en remplacement de $\mathbf{B}_d$ (voir [22], section 15).
En exploitant les méthodes de [14], cela produit des relèvements modulo p^2, des suites exactes complètement filtrées de représentations semi-linéaires des groupes $(1,1)$ -lisses- (voir [22], section 16).
Grâce à la description de la cohomologie galoisienne en termes d'extensions "à la Yoneda" de représentations galoisiennes, j'obtiens un résultat optimal de relèvement de la cohomologie modulo p, des pro-p-groupes G qui sont $(1,1)$-lisses.
L'hypothèse "pro-p" est là pour garantir que les suites exactes de représentations $\mathbb{F}_p$-linéaires de G peuvent être complètement filtrées.

Théorème 6.3.5. *([22], Théorème de Lissité 17.1)*
Soit G un pro-p-groupe $(1,1)$-lisse. Soit $n \geq 2$ un entier.
Soit $c_1 \in H^n(G, \mathbb{F}_p)$ une classe de cohomologie.
Alors, il existe un $\mathbb{Z}/p^2$-module libre $\mathbb{Z}/p^2[c_1]$, muni d'une action continue de G, vérifiant les propriétés suivantes.
1) La réduction modulo p de $\mathbb{Z}/p^2[c_1]$ est le G-module trivial $\mathbb{F}_p$.
2) La classe c_1 se relève en $c_2 \in H^n(G, \mathbb{Z}/p^2[c_1])$.

Ce résultat soulève deux questions intéressantes, qui feront l'objet d'études futures.

Question 6.3.6. Soit $(G, \mathbb{Z}/p^2(1))$ une paire $(1,1)$-cyclotomique- par exemple, un groupe de Galois absolu et son caractère cyclotomique modulo p^2.
Par le théorème de relèvement faible, on sait que G est $(1,1)$-lisse.
Dans le Théorème de Lissité, est-il loisible de prendre $\mathbb{Z}/p^2(n)$ pour $\mathbb{Z}/p^2[c_1]$?
Dans l'affirmative, cela validerait l'intuition I_2- le point de départ de ce travail.

Question 6.3.7. (Conjecture des Symboles)
Soit G un pro-p-groupe $(1,1)$-lisse.
L'algèbre graduée de cohomologie $\bigoplus_{n \in \mathbb{N}} H^n(G, \mathbb{F}_p)$ est-elle engendrée en degré 1?
Dans l'affirmative, cela validerait l'intuition I_2- de manière bien plus probante qu'à la question précédente.

7

Résidus sur les grassmanniennes affines.

Soit k un corps, de clôture séparable k_s.

Définition 7.0.1. *Soit G un groupe algébrique linéaire sur k.*
On dit que G est k-ployé, s'il ne contient aucun k-sous-groupe isomorphe au groupe additif $\mathbb{G}_a$, ou au groupe multiplicatif $\mathbb{G}_m$.

Exemple 7.0.2. 1) Si G est un k-tore, G est ployé si, et seulement si

$$H^0(\mathrm{Gal}(k_s/k), \hat{G}) = 0,$$

où $\hat{G} := \mathrm{Hom}_{k_s}(G, \mathbb{G}_m)$ désigne le module galoisien des caractères de G.
2) Supposons k parfait, et G unipotent lisse connexe. Alors G est *déployé*, i.e. possède une suite de composition à quotients successifs des groupes additifs $\mathbb{G}_a$.
3) Supposons k imparfait. Soit l/k une extension finie purement inséparable. Alors le quotient $G := R_{l/k}(\mathbb{G}_m)/\mathbb{G}_m$ est un k-groupe unipotent lisse et k-ployé.

Le résultat suivant découle de l'existence des k-compactifications de Gabber (voir [29]).

Théorème 7.0.3. *Soit G un groupe algébrique linéaire sur k. Alors G est k-ployé, si et seulement si l'inclusion naturelle $G(k[[t]]) \subset G(k((t)))$ est une égalité.*

Remarque 7.0.4. Si G/k est réductif, le théorème précédent porte les noms de Bruhat, Tits et Rousseau. Notez que la théorie de Bruhat et Tits ne permet pas de traiter le cas d'un groupe unipotent ployé sur un corps imparfait- qui est en quelque sorte l'extrême opposé du cas réductif.

Dans un projet en commun avec Philippe Gille, nous avons souhaité proposer une preuve élémentaire du théorème 7.0.3, n'utilisant aucune propriété spécifique de G. Après évolution, cet objectif a donné lieu à la prépublication [23], dont je vais maintenant présenter certains résultats.

Soit A un anneau commutatif, et soit G un schéma en groupes affine et de type fini sur $\mathrm{Spec}(A)$.
Je suppose qu'il existe un entier $N \geq 1$, et un A-plongement $G \hookrightarrow \mathrm{SL}_N$; une hypothèse mise dans [23]. Elle est probablement superflue, de même que le caractère affine de G. Elle permet cependant de démontrer les énoncés qui suivent à l'aide

de calculs explicites.

Définition 7.0.5. *Soit $r = \frac{m}{n} \in \mathbb{Q}$, écrit en fraction irréductible.*
On utilise la notation $\lambda = 1 + u$.
Posons $A_r^\lambda = A[\lambda, \lambda^{-1}][[t^{\frac{1}{n}}]]$ et $\mathcal{A}_r^\lambda = A[\lambda, \lambda^{-1}]((t^{\frac{1}{n}}))$.
Un élément de $\mathcal{A}_r^\lambda$ est donc une série de Laurent en $t^{\frac{1}{n}}$, à coefficient dans les polynômes de Laurent en λ.
Soit

$$j : A_r^\lambda \longrightarrow A[\lambda, \lambda^{-1}]$$
$$t^{\frac{1}{n}} \mapsto 0$$

le morphisme de spécialisation.
Soit

$$\sigma_r : \mathcal{A}_1^\lambda \longrightarrow \mathcal{A}_r^\lambda,$$
$$t \mapsto t(1 + ut^r) = t(1 + (1 - \lambda)t^r);$$

c'est un plongement de $A[\lambda, \lambda^{-1}]$-algèbres.

Soit $g \in G(A((t)))$.
Si $g \in G(A[[t]])$, on définit l'indice de ramification de g comme $r(g) = -1$.
Si $g \in G(A((t))) \setminus G(A[[t]])$, on définit l'indice de ramification $r(g)$, ainsi que le résidu associé, à l'aide de la proposition suivante.

Proposition 7.0.6. *([23], Proposition 2.1 et Theorem 3.4)*
Supposons donné un élément $g \in G(A((t))) \setminus G(A[[t]])$.
Posons

$$\Delta_r(g) := g^{-1}\sigma_r(g) \in G(\mathcal{A}_r^\lambda)$$

L'ensemble

$$\Sigma(g) = \{r \in \mathbb{Q}_{>0},\ \Delta_r(g) \in G(A_r^\lambda)\}$$

est non vide. On dénote par $r(g)$ sa borne inférieure dans $\mathbb{R}$.
C'est un nombre rationnel, appelé indice de ramification de g.
Si $r(g) = 0$ (cas multiplicatif), on note

$$\mathrm{Res}(g) : \mathbb{G}_m = \mathrm{Spec}(A[\lambda, \lambda^{-1}]) \longrightarrow G$$

le morphisme de A-schémas donné par $j(\Delta_r(g)) \in G(A[\lambda, \lambda^{-1}])$.
Si $r(g) > 0$ (cas additif), on note

$$\mathrm{Res}(g) : \mathbb{G}_a = \mathrm{Spec}(A[u]) \longrightarrow G$$

le morphisme de A-schémas donné par $j(\Delta_r(g)) \in G(A[u]) \subset G(A[\lambda, \lambda^{-1}])$.

Alors $\mathrm{Res}(g)$ *est un homomorphisme non trivial de A-schémas en groupes.*

Remarque 7.0.7. Le fait que $r(g) \in \mathbb{Q}$ découle d'un calcul explicite, qui utilise pour l'instant le plongement $G \hookrightarrow \mathrm{SL}_N$.

Remarque 7.0.8. Supposons A intègre. Si $\mathbb{Z} \subset A$ (resp. $\mathbb{F}_p \subset A$), on montre que $r(g) \in \mathbb{Z}$ (resp. $r(g) \in \mathbb{Z}[\frac{1}{p}]$). Voir [23], Corollary 3.5.

L'existence même des résidus fournit une extension du théorème 7.0.3, comme suit.

Proposition 7.0.9. *([23], Corollary 3.8)*
Soit G un schéma en groupes affine et de type fini sur A.
On a l'équivalence des propriétés suivantes.
1) $G(A[[t]]) = G(A((t)))$*;*
2) $G(A) = G(A[\lambda, \lambda^{-1}])$*;*
3) $\mathrm{Hom}_{A-gp}(\mathbb{G}_a, G) = \mathrm{Hom}_{A-gp}(\mathbb{G}_m, G) = 0$.

Si ces conditions équivalentes sont vérifiées, on dit que G est A-ployé.

Comme la lectrice l'aura peut-être remarqué, les notions d'indice de ramification et de résidu s'étendent directement au cas des torseurs. Plus précisément, soit X un G-torseur sur $\mathrm{Spec}(A)$, et soit $x \in X(A((t)))$. On peut alors associer à x un indice de ramification $r(x)$ et un résidu $\mathrm{Res}(x)$, à l'aide de la construction de la Proposition 7.0.6.

En utilisant les résidus, on fournit une preuve courte du résultat suivant.

Théorème 7.0.10. *([23], Theorem 5.5)*
Soit G un groupe algébrique linéaire sur le corps k (= schéma en groupes affine et de type fini sur k).
Alors la flèche naturelle

$$H^1_{fppf}(k, G) \longrightarrow H^1_{fppf}(k((t)), G)$$

a un noyau trivial.
Par torsion (voir [36], chapitre I.5.3), en appliquant ce résultat à toutes les formes internes de G, on en déduit qu'elle est injective.

Dans les deux dernières sections de [23], on expose la construction de l'indice de ramification et du résidu dans un contexte plus général, en utilisant le schéma en groupes des automorphismes des séries de Laurent, et la cohomologie de Hochschild. On montre comment l'indice de ramification permet d'obtenir une nouvelle filtration naturelle sur les grassmanniennes affines. Pour G réductif, on donne une description explicite du cran "multiplicatif" de cette filtration (Proposition 9.10).

Bibliographie

[1] D. Anderson, M. Florence, Z. Reichstein, *The Lie algebra of type G_2 is rational over its quotient by the adjoint action*, Comptes Rendus Acad. Sci. 351, 2013, 871-875.

[2] E. Bayer, H. Lenstra, *Self-dual normal basis*, Indagationes Math. 92, 1989, 379-383.

[3] M. Brassil, Z. Reichstein, *Hermite's theorem via Galois cohomology*, Archiv der Math. 112, 2019, 467-473.

[4] P. Brosnan, Z. Reichstein, A. Vistoli, *Essential dimension, spinor groups, and quadratic forms*, Annals of Math. 171, 2010, 533-544.

[5] J. Buhler, Z. Reichstein, *On the essential dimension of a finite group*, Comp. Math. 106, 1997, 159–179.

[6] N. P. Byott, G.G. Elder, *A valuation criterion for normal bases in elementary abelian extensions*, Bull. London Math. Soc 39, 2007, 705-708.

[7] G. Casnati, C. Fontanari, *On the rationality of moduli spaces of pointed curves*, J. Lond. Math.Soc. 75, 2007, 582–596.

[8] J.-L. Colliot-Thélène, B. Kunyavskiĭ, V. L. Popov, Z. Reichstein, *Is the function field of a reductive Lie algebra purely transcendental over the field of invariants for the adjoint action*, Comp. Math. 147, 2011, 428-466.

[9] C. De Clercq, M. Florence, *Lifting theorems and smooth profinite groups,* preprint, available at https://arxiv.org/abs/1710.10631

[10] C. De Clercq, M. Florence, *Lifting low-dimensional local systems,* preprint, available at https://arxiv.org/abs/1812.08068

[11] C. De Clercq, M. Florence, *Smooth profinite groups I: geometrizing Kummer theory,* preprint, available at https://arxiv.org/abs/2009.11130.

[12] C. De Clercq, M. Florence, G. Lucchini-Arteche, *Lifting vector bundles to Witt vector bundles*, https://arxiv.org/abs/1807.04859.

[13] P. Deligne, L. Illusie, *relèvements modulo p^2 et décomposition du complexe de de Rham*, Inv. Math. 89, 1987, 247–270.

[14] C. Demarche, M. Florence, *Splitting families in Galois cohomology*, accepté pour publication dans Ann. Sci. ENS.

[15] B. De Smit, M. Florence, L.Thomas, *The valuation criterion for normal basis generators*, Bull. London Math. Soc 44, 2012, 729-737.

[16] M. Florence, *Zéro-cycles de degré un sur les espaces homogènes*, IMRN 54, 2004, 2898-2914.

[17] M. Florence, *Points rationnels sur les espaces homogènes et leurs compactifications*, Transformation Groups 11, 2006, 161-176.

[18] M. Florence, *On the essential dimension of cyclic p-groups*, Inv. Math. 171, 2008, 175-189.

[19] M. Florence, *Géométrie birationnelle équivariante des grassmanniennes*, Crelle 674, 2013, 81—98.

[20] M. Florence, *On higher trace forms of separable algebras*, Archiv der Math. 97, 2011, 247-249.

[21] M. Florence, *On the symbol length of p-algebras*, Compositio Math 149 (2013), 1353-1363.

[22] M. Florence, *Smooth Profinite Groups, II: the Uplifting Theorem*, https://arxiv.org/pdf/2009.11140.pdf

[23] M. Florence, P. Gille, *Residues on affine grassmannians*, https://arxiv.org/abs/1910.14509.

[24] M. Florence, F. Meunier, *Completely symmetric configurations for σ-games on grid graphs*, J. of Alg. Combinatorics 31, 2010, 533-545.

[25] B. Fantechi, A. Massarenti, *On the rigidity of moduli of curves in arbitrary characteristic*, Int. Math. Res. Not. 8, 2017,2431–2463.

[26] M. Florence, Z. Reichstein, *The rationality problem for forms of moduli spaces of stable curves of genus zero*, Bulletin of the London Math. Soc. 50, 2018, 148-158.

[27] M. Florence, N. Hoffmann, Z. Reichstein, *On the rationality problem for forms of moduli spaces of stable marked curves of positive genus*, accepté pour publication dans Ann. Sc. Norm. Pisa.

[28] M. Florence, M. Van Garrel, *A constructive approach to a conjecture by Voskresenskiĭ*, Selecta Math. 23, 2017, 2899–2906.

[29] O. Gabber, *On pseudo-reductive groups and compactification theorems*, Oberwolfach Reports(2012), 2371-2374.

[30] P. Gille, *Symbole galoisien l-adique et théorème de Suslin-Voevodsky*, J. Math. Kyoto. Univ. 47 (2007), 665-690.

[31] P. Gille, T. Szamuely, *Central simple algebras and Galois cohomology*, 2nd edition, Cambridge Studies in Advanced Mathematics, 2017.

[32] R. Gordon-Sarney, V. Suresh, *Totaro's question on zero-cycles on torsors*, Duke Math. J. 167 (2), 2018, 385-395.

[33] D. Krashen, *Period and index, symbol lengths, and generic splittings in Galois cohomology*, Bull. London Math. Soc. 48 (6), 2016, 985-1000.

[34] N. Karpenko, A. Merkurjev, *Essential dimension of finite p-groups*, Inv. Math. 172 (2008), 491–508.

[35] R. Parimala, *Homogeneous varieties—zero-cycles of degree one versus rational points*, Asian J. Math. 9 (2005), 251-256.

[36] J.-P. Serre, *Cohomologie galoisienne*, Springer Lecture Notes in Math, 1997.

[37] K. Sutner, *Linear cellular automata and the Garden-of-Eden*, Math. Intelligencer 11, 1989, 49–53.

[38] A. Suslin, S. Joukhovitski, *Norm varieties*, J. of Pure and Applied Algebra 206, 2006, 245-276.

[39] H.P.F. Swinnerton-Dyer, *Rational points on del Pezzo surfaces of degree 5* In: 5th Nordic Summer School in Math, 1970, 287-290.

[40] L.Thomas, *A valuation criterion for normal basis generators in equal positive characteristics*, J. of Algebra 320 (10), 2008, 3811-3820.

[41] B. Totaro, *Splitting fields for E_8-torsors* Duke Math. J. 121, 2004, 425-455.

[42] S.L. Tregub, *Birational equivalence of Brauer–Severi manifolds* Uspekhi Mat. Nauk 46 , 1991, 217-218.