

Synthèse de mes travaux et projets de recherche.

Magali ROCHER.

1 Travaux de thèse :

Titre : Courbes algébriques lisses en caractéristique $p > 0$ munies d'un gros p -groupe d'automorphismes.

Date de soutenance : 14 novembre 2008.

Rapporteurs : Ted Chinburg (Université de Pennsylvanie) et Aristides Kontogeorgis (Université d'Athènes).

Membres du jury : Pierre Dèbes (Université de Lille 1), Aristides Kontogeorgis (Université d'Athènes), Qing Liu (Université de Bordeaux 1), Michel Matignon (Université de Bordeaux 1), Ariane Mézard (Université de Versailles-Saint-Quentin), Christophe Ritzenthaler (Université de Marseille 2).

Mots clefs : Automorphismes, courbes, p -groupes, corps de classes de rayons, théorie d'Artin-Schreier-Witt, polynômes additifs, points rationnels.

Thèmes de recherche :

Groupes d'automorphismes des courbes algébriques en caractéristique $p > 0$.

Espaces de module des courbes munies d'un groupe d'automorphismes.

Construction de familles universelles. Espace des déformations.

Corps de classes de rayons et comptage de points rationnels sur les courbes sur un corps fini.

Courbes supersingulières, courbes \mathbb{F}_q -maximales.

Théorie des groupes : groupes nilpotents, p -groupes, sous-groupes de Sylow, sous-groupes de Frattini.

Réduction semi-stable sur un corps p -adique et monodromie arithmétique.

Résumé : Soit k un corps algébriquement clos de caractéristique $p > 0$. Soit C/k une courbe algébrique, propre, lisse et de genre $g \geq 2$, munie d'un p -groupe G d'automorphismes tel que $|G| > \frac{2p}{p-1}g$. Un tel couple (C, G) est appelé une *grosse action*. Sous ces hypothèses, les formules de Riemann-Hurwitz et Deuring-Shafarevitch impliquent que $C \rightarrow C/G$ est un revêtement étale de la droite affine $\text{Spec } k[X]$, complètement ramifié à l'infini.

On précise d'abord certaines propriétés du deuxième groupe de ramification G_2 de G à l'infini. On montre en particulier qu'il est égal au groupe dérivé G' de G et qu'il ne peut être cyclique sauf s'il est d'ordre p .

On donne ensuite des exemples de telles actions avec G' abélien d'exposant quelconque. Ces exemples trouvent leur source dans la construction, via les corps de classes de rayons, de courbes algébriques sur un corps fini possédant beaucoup de points rationnels.

On se concentre ensuite sur le cas où G' est un p -groupe abélien élémentaire. En considérant une filtration d'anneau de $k[X]$ liée aux polynômes additifs, on obtient un théorème de structure pour les fonctions paramétrant le revêtement d'Artin-Schreier $C \rightarrow C/G'$. On exhibe alors des familles universelles et on discute de l'espace de déformation correspondant lorsque $p = 5$.

Dans le dernier chapitre de la thèse, on tente d'amorcer une classification des *grosses actions*. On discute tout d'abord de la finitude des valeurs prises par les quotients $\frac{|G|}{g}$ et $\frac{|G|}{g^2}$ lorsque (C, G) parcourt l'ensemble des *grosses actions* telles que $\frac{|G|}{g^2} \geq M > 0$. Pour $M = \frac{4}{(p^2-1)^2}$, on donne une classification et une paramétrisation complète de telles actions.

A noter que le chapitre introductif de la thèse est consacré à des généralités sur les G -actions de courbes en caractéristique nulle et en caractéristique $p > 0$. On y rappelle un certain nombre de résultats connus mais on évoque également des problèmes toujours en discussion, notamment ceux portant sur les déformations de telles actions (travaux de [Bertin-Mezard 2000], [Cornelissen- Kato 2003], [Pries 2005, 2006, 2008], [Kontogeorgis 2006, 2007], [Bertin-Romagny 2008], [Maugeais 2008]...). J'établis finalement le lien avec mes propres travaux en comparant, dans certains cas particuliers, la dimension de l'espace des paramètres de mes courbes avec les bornes données par Pries et Kontogeorgis.

2 Publications et prépublications.

2.1 Articles parus.

1. Magali Rocher (avec Michel Matignon) [MR] : *Smooth curves having a large automorphism p -group in characteristic $p > 0$* , Algebra Number Theory **2**, n° 8, (2008), 887–926.
Cet article correspond essentiellement au deuxième chapitre de ma thèse.
2. Magali Rocher [Ro1] : *Large p -group actions with a p -elementary abelian derived group*, Journal of Algebra **321** (2009), 704–740.
Cet article correspond essentiellement au troisième chapitre de ma thèse.

2.2 Article soumis.

1. Magali Rocher [Ro2] : *Large p -group actions with $\frac{|G|}{g^2} \geq \frac{4}{(p^2-1)^2}$* . (2008) -(26 pages) -
Une première version est disponible sur arXiv : <http://arxiv.org/abs/0804.3494>
Cet article correspond essentiellement au dernier chapitre de ma thèse.

2.3 Oberwolfach reports.

1. Magali Rocher : *On smooth curves endowed with a big automorphism group*. Mathematisches Forschungsinstitut Oberwolfach, Report No 26/2007.
2. Magali Rocher : *Smooth curves endowed with a large automorphism p -group in characteristic $p > 0$* . Mathematisches Forschungsinstitut Oberwolfach, Report No 54/2008.

3 Projets de recherche.

Les notations sont celles définies dans le résumé de ma thèse ci-dessus. Les références bibliographiques sont consignées ci-dessous.

Il reste de nombreuses questions ouvertes autour des *grosses actions*. En particulier, si nous avons pu donner des exemples de telles actions avec un groupe dérivé G' abélien d'exposant quelconque et si nous avons éliminé les cas cycliques autre que $G' \simeq \mathbb{Z}/p\mathbb{Z}$ (cf. [MR]), nous ne savons pas encore s'il est possible de trouver des *grosses actions* avec un G' non abélien. Une piste d'étude serait de poursuivre, comme il a été fait dans le deuxième chapitre de la thèse, la construction de tours d'extensions via la théorie du corps de classe à la manière de K. Lauter ([Lau99]) et R. Auer ([Au99] et [Au00]).

Un autre projet de recherche, ayant davantage pour vocation d'élargir le problème des *grosses actions* et de le relier à d'autres thématiques, serait de faire le lien avec les courbes supersingulières et les courbes maximales, ces deux types de courbes présentant un intérêt majeur en cryptographie.

Nous avons en effet pu remarquer que certaines courbes définies sur un corps fini et possédant beaucoup de points rationnels donnaient naturellement des exemples de courbes avec de gros groupes d'automorphismes, et donc des *grosses actions*. (voir [MR]). Dans cette optique, il semble naturel de chercher à approfondir les liens entre les *grosses actions* et les courbes maximales, i.e. les courbes définies sur \mathbb{F}_q dont le nombre de points \mathbb{F}_q -rationnels atteint la borne de Hasse-Weil, i.e. $1 + q + 2g\sqrt{q}$.

Un autre lien tout aussi naturel serait à chercher avec les courbes supersingulières (i.e. les courbes dont la jacobienne est isogène à un produit de courbes elliptiques supersingulières). Il existe en effet des rapports étroits entre courbes supersingulières et courbes maximales, une courbe supersingulière définie sur \mathbb{F}_q étant maximale sur une certaine extension de \mathbb{F}_q . Une vaste littérature a été consacrée à ces deux types de courbes ces dernières années, parfois en lien avec les extensions d'Artin-Schreier ([SZ], [Bl08]) et les polynômes additifs ([GT08b]).

Ceci annonce déjà en filigrane un lien avec les *grosses actions*. Il est déjà établi que les courbes paramétrées par $W^p - W = XS(X)$, où $S(X)$ est un polynôme additif de $k[X]$, k étant un corps fini de caractéristique $p > 0$, sont supersingulières (cf. [VG92]). En utilisant les travaux de E. Kani et M. Rosen ([KR89]), il est possible de généraliser cet énoncé pour tout corps k algébriquement clos. Or ces courbes correspondent précisément aux *grosses actions* avec un G' d'ordre p . L'étape suivante serait donc d'étudier la jacobienne des courbes correspondant aux grosses actions dont le G' est p -abélien élémentaire. Pour ce faire, on peut songer à utiliser les techniques de Kani et Rosen (op. cit.) permettant de décomposer la jacobienne

d'une courbe via les jacobiniennes de certaines courbes quotients.

NB : Les premiers résultats obtenus quant à la supersingularité des grosses actions ont été exposés lors d'un séminaire à Toulouse le 30 avril 2008. Les notes de cet exposé sont disponibles à l'adresse : <http://www.math.u-bordeaux.fr/~mrocher/recherche.html>

Les polynômes additifs jouant un rôle crucial dans mon travail sur les *grosses actions*, on pourrait enfin penser à faire le lien avec d'autres domaines de la géométrie, de l'arithmétique et de l'algèbre qui les utilisent. Comme l'a déjà remarqué N. Elkies ([El99]), les polynômes additifs sont au coeur de thématiques aussi variées que les modules de Drinfeld, la construction de courbes supersingulières (voir le point précédent) mais encore les problèmes de Galois inverse (notamment dans les travaux d'Abhyankar). De même, les travaux récents du professeur B. Matzat ([Mat04]) autour des structures de Frobenius en caractéristique $p > 0$ leur accordent également une place de choix et établissent des liens avec la théorie de Galois différentiel. Remarquons que N. Elkies (op. cit.) établissait déjà une analogie entre les polynômes additifs et certains opérateurs différentiels linéaires.

Même si l'usage que je fais des polynômes additifs n'est a priori pas le même, bon nombre de techniques sont assez similaires et des analogies peuvent être faites à la manière d'Elkies. Je pense donc que les polynômes additifs pourraient constituer un fil conducteur pour faire le lien avec d'autres travaux.

4 Bibliographie sélective en lien avec mes travaux.

Références

- [Au99] R. Auer, *Ray Class Fields of Global Function Fields with Many Rational Places*. Dissertation at the University of Oldenburg, www.bis.uni-oldenburg.de/dissertation/ediss.html, (1999).
- [Au00] R. Auer, *Ray class fields of global function fields with many rational places*. Acta Arith. **95** (2000), no. 2, 97-122.
- [Bl08] R. Blache *p-Density, exponential sums and Artin-Schreier curves* (2008) arXiv :0812.3382
- [Br00] T. Breuer, *Characters and automorphism groups of compact Riemann surfaces*. London Mathematical Society Lecture Note Series, 280. Cambridge University Press, Cambridge, (2000).
- [Co90] M. Conder, *Hurwitz groups : a brief survey*. Bull. Amer. Math. Soc. (N.S.) **23** (1990), no. 2, 359-370.
- [El99] N. Elkies, *The Klein quartic in number theory. The eightfold way*, 51-101, Math. Sci. Res. Inst. Publ., 35, Cambridge Univ. Press, Cambridge, (1999).
- [GS91] A. Garcia, H. Stichtenoth, *Elementary abelian p -extensions of algebraic function fields*. Manuscripta Mat. **72** (1991), no. 1
- [GT08] A. Garcia, S. Tafazolian, *Certain maximal curves and Cartier operators*. Acta Arith. **135** (2008), no. 3, 199-218.
- [GT08b] A. Garcia, S. Tafazolian, *On additive polynomials and certain maximal curves*. J. Pure Appl. Algebra **212** (2008), no. 11, 2513-2521.
- [Ga01] *Supersingular curves in cryptography*. Advances in cryptology—ASIACRYPT 2001 (Gold Coast), 495-513, Lecture Notes in Comput. Sci., 2248, Springer, Berlin, 2001.
- [GK07] M. Giulietti, G. Korchmáros, *On large automorphism groups of algebraic curves in positive characteristic* arXiv :0706.2320 , 15 Jun 2007
- [KR89] E. Kani, M. Rosen, *Idempotent relations and factors of Jacobians*. Math. Ann. **284** (1989), no. 2, 307-327.
- [Ku91] R. Kulkarni, *Riemann surfaces admitting large automorphism groups*. Extremal Riemann surfaces (San Francisco, CA, 1995), 63-79, Contemp. Math., 201, Amer. Math. Soc., Providence, RI, (1997).
- [Lau99] K. Lauter, *A Formula for Constructing Curves over Finite Fields with Many Rational Points*. Journal of Number Theory **74** (1999), no. 1, 56-72.
- [LM05] C. Lehr, M. Matignon, *Automorphism groups for p -cyclic covers of the affine line*. Compositio Math. **141** (2005).
- [Mat04] B. H. Matzat, *Frobenius modules and Galois groups. Galois theory and modular forms*, 233-267, Dev. Math., 11, Kluwer Acad. Publ., Boston, MA, 2004.

- [Na87] S. Nakajima, *p-ranks and automorphism groups of algebraic curves*. Trans. Amer. Math. Soc. **303** (1987).
- [Ny83] N. Nygaard, *On supersingular abelian varieties*. Algebraic geometry (Ann Arbor, Mich., 1981), 83–101, Lecture Notes in Math., 1008, Springer, Berlin, 1983.
- [St73] H. Stichtenoth, *Über die Automorphismengruppe eines algebraischen Funktionkörpers von Primzahlcharakteristik I, II*, Arch. Math. (Basel) **24** (1973).
- [SZ] J. Scholten, H. Zhu, *Slope estimates of Artin-Schreier curves*. Compositio Math. 137 (2003), no. 3, 275–292.
- [St93] H. Stichtenoth, *Algebraic function fields and codes*. Universitext. Springer-Verlag, Berlin, (1993).
- [VG92] G. van der Geer, M. van der Vlugt, *Reed-Muller codes and supersingular curves. I*. Compositio Math. 84 (1992), no. 3