Research statement and research plans.

Magali ROCHER.

Main research interest : Arithmetic geometry.

1 Keywords.

Automorphisms, curves, p-groups, ray class fields, Artin-Schreier-Witt theory, additive polynomials, families, moduli of curves.

2 Connected topics.

Moduli of curves endowed with an automorphism group. Construction of universal families.

Automorphism groups of smooth curves in characteristic $p > 0$.

Ray class fields for global functions fields.

Algebraic curves with many rational points over a finite field.

Group theory : p-groups, nilpotent groups, Sylow subgroups, Frattini subgroups.

Semi-stable reduction over a p-adic field and arithmetic monodromy.

3 Setting and motivation.

For more than a century, the study of finite groups G acting faithfully on smooth complete curves defined over an algebraically closed field k of characteristic $p \geq 0$ has produced a vast literature. Already back in the nineteenth century progress was made in the case of characteristic zero, with the works of Schwartz, Klein, Hurwitz, Wiman and others. The full automorphism group of a compact Riemann surface C of genus $g \geq 2$ was proved by Hurwitz to be finite and of order at most $84\,(g-1)$. An open question concerns the classification of full automorphism groups of compact Riemann surfaces of fixed genus $g \geq 2$. This classification has been partially achieved for *large* automorphism groups G, *large* meaning that the order of G is greater than $4\,(g-1)$ (cf. Kulkarni). This lower bound imposes strict restrictions on the genus g_0 of the quotient curve C/G, namely $g_0 = 0$, on the number r of points of C/G ramified in C, namely $r \in \{3, 4\}$, and on the corresponding ramification indices. Following the works of Kulkarni, Kuribayashi and Breuer, Magaard et alii exhibited the list of large groups $\mathrm{Aut}(C)$ of compact Riemann surfaces of genus g up to $g = 10$, determining in each case the dimension and number of components of the corresponding loci in the moduli space of genus g curves.

General results on Hurwitz spaces and other moduli spaces parametrizing deformations have been obtained in the case of characteristic zero and extended to positive characteristic $p > 0$ when p does not divide the order of the automorphism group (see Breuer). For instance, if C is a compact Riemann surface with genus $g \geq 2$ and G an automorphism group of C, the deformations of the cover $\varphi : C \to C/G$ are parametrized by a moduli space of dimension $3g_0 - 3 + |\mathcal{B}| + \dim \mathrm{Aut}\,(C/G - \mathcal{B})$, where g_0 is the genus of C/G and $\mathcal{B}$ the branch locus of φ. By the Hurwitz genus formula, g_0 only depends on $|G|$, g, $|\mathcal{B}|$ and the orders of the inertia groups. All these results are no longer true in positive characteristic $p > 0$ when φ is widly ramified. Likewise, in positive characteristic $p > 0$, the Hurwitz bound is no longer true for automorphism groups G whose order is not prime to p. The finiteness result still holds but the Hurwitz linear bound is replaced with biquadratic bounds (cf. Stichtenoth). These biquadratic bounds are optimal : so, in positive characteristic, the automorphism groups may be very large compared with the case of characteristic zero, as a result of wild ramification.

Wild ramification points also contribute to the dimension of the tangent space to the global infinitesimal deformation functor of a curve C together with an automorphism group G, and it is precisely this that makes computations difficult. Following Bertin and Mézard's work in the case where G is cyclic of order p , Pries and Kontogeorgis have obtained lower and upper bounds for the dimension of the tangent space, with explicit computations when G is an abelian p-group.

To rigidify the situation in characteristic $p > 0$ as has been done in characteristic zero, one idea is to consider large automorphism p-groups. So, following Lehr and Matignon (*Automorphism groups for p-cyclic covers of the affine line*. Compositio Math. **141** , no. 5,(2005)), we define a *big action* as a pair (C, G) where G is a p-subgroup of $\mathrm{Aut}_k(C)$ such that $|G| > \frac{2\,p}{p-1}\, g$.

When this inequality is satisfied, the Hurwitz and the Deuring-Shafarevitch formulas applied to $C \to C/G$ imply that $g_{C/G} = 0$ and that only one point $\infty \in C$ is ramified (and even totally ramified) in C/G. Call G_i the i-th lower ramification group of G at ∞. Then, $G = G_{-1} = G_0 = G_1$ and the quotient curve C/G_2 is isomorphic to the projective line. In particular, G_2 is nontrivial. The choice of the bound $|G| > \frac{2\,p}{p-1}\, g$ is also necessary to get the strict inclusion $G_2 \subsetneq G_1 = G$. It follows that the quotient group G/G_2 acts as a group of translations of the affine line $C/G_2 - \{\infty\} = \mathrm{Spec}\, k[X]$, through $X \to X + y$, where y runs over a subgroup V of k. This gives the exact sequence

$$0 \longrightarrow G_2 \longrightarrow G = G_1 \xrightarrow{\pi} V \simeq (\mathbb{Z}/\,p\,\mathbb{Z})^v \longrightarrow 0.$$

4 Outline of the thesis.

The first chapter of my thesis is devoted to general results on G-actions on smooth complete curves defined over an algebraically closed field k, when k has characteristic zero and then, when k has characteristic $p > 0$. In particular, I mention recent works by Bertin-Mézard, Pries and Kontogeorgis concerning the deformation of such actions in characteristic $p > 0$ in the case of wild ramification. In some special cases, I compare the bound they obtain for the dimension of the deformation space with my own results.

The purpose of the second chapter is twofold : to give necessary conditions on G_2 for (C, G) to be a big action and to display realizations of big actions with G_2 abelian of large exponent. Indeed, in the first sections, I show that G_2 is equal to $D(G)$, the commutator subgroup of G. I also prove that G_2 cannot be cyclic unless G_2 has order p. Then, the second part of this chaper is devoted to examples of big actions with G_2 abelian of arbitrary large exponent, knowing that we do not know yet examples of big actions with a nonabelian G_2. My main source of examples comes from the construction of curves with many rational points using ray class field theory for global function fields, as initiated by J-P. Serre and continued by K. Lauter and by R. Auer.

The aim of the third chapter is to describe big actions (C, G) with a p-elementary abelian G_2. The main result of this chapter is a structure theorem for the functions parametrizing the Artin-Schreier cover $C \to C/G_2$. More precisely, I show this cover is parametrized by n equations $W_i^p - W_i = f_i(X) \in k[X]$ where each function f_i can be written as a linear combination over k of products of at most $i + 1$ additive polynomials.

I also give a group-theoretic characterization of a special case of main interest, namely the case where each $f_i \in \Sigma_{i+1} - \Sigma_i$. Then, I display a universal family parametrizing the big actions (C, G) satisfying this condition, for $p = 5$, a given $n \leq p - 1$ and $\dim_{\mathbb{F}_p} V = 2$. This leads to discuss the deformation space of such a big action.

In the last chapter, I study finiteness results on the values taken by the quotients $\frac{|G|}{g^2}$ and $\frac{|G|}{g^2}$ when (C, G) runs over the big actions satisfying $\frac{|G|}{g^2} \geq M$, for a given positive real $M > 0$. This question leads to a purely group-theoretic discussion around the inclusion $\mathrm{Fratt}(G_2) \subset [G_2, G]$, where $\mathrm{Fratt}(G_2)$ means the Frattini subgroup of G_2 and $[G_2, G]$ denotes the commutator subgroup of G_2 and G. In the last part of this chapter, I finally exhibit a classification and a parametrization of such big actions when $M = \frac{4}{(p^2-1)^2}$.

5 Publications and preprints.

5.1 Publications.

1. Magali Rocher (joint with Michel Matignon) : *Smooth curves having a large automorphism p-group in characteristic* $p > 0$, Algebra Number Theory **2**, n° 8, (2008), 887–926.

2. Magali Rocher : *Large p-group actions with a p-elementary abelian derived group*, Journal of Algebra **321** (2009), 704–740.

5.2 Prepublications.

1. Magali Rocher : *Large p-group actions with $\frac{|G|}{g^2} \geq \frac{4}{(p^2-1)^2}$.* (2008) -(26 pages) - available on arXiv : `http ://arxiv.org/abs/0804.3494`

5.3 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.

6 Research plans.

1. There are still many open questions concerning the so-called *big actions*. For instance, we have seen that for a big action, G_2 equals the derived subgroup $D(G)$ of G. Since G_2 cannot be trivial, it follows that G cannot be abelian. The same question can be raised for G_2, namely can G_2 be non-abelian ?
   On the one hand, we showed a number of restrictions on G_2 : for example, it cannot be cyclic except for $G_2 \simeq \mathbb{Z}/p\mathbb{Z}$. On the other hand, we gave examples of big actions with G_2 abelian of arbitrary large exponent. It now remains to determine whether there can exist big actions with a non-abelian G_2.
   An idea to find some may be to consider towers of extensions as those studied by Auer and Lauter and mentioned in my thesis. Indeed, starting from $K = \mathbb{F}_q(X)$, where $q = p^e$, one first defines K^m as the largest abelian extension of K with conductor at most $m\infty$ and such that every finite rational place of K totally splits in this extension. The group of translations $\{X \to X + y,\ y \in \mathbb{F}_q\}$ extends to a p-group of automorphisms of K^m and, for m and e large enough, this gives a big action with $G_2 = \mathrm{Gal}(K^m/K)$ abelian of arbitrary large exponent.
   One can now reiterate the process and consider L^n the largest abelian extension of K^m with conductor at most $n\infty$ and such that every finite rational place of K^m totally splits in this extension. Once again, due to the maximality and the uniqueness of L^n, the $\mathbb{F}_q$-automorphism group of K^m can be extended to an automorphism p-group of L^n. In this way, for well-chosen parameters, we expect to obtain a big action with a non-abelian G_2.

2. Another idea to enlarge the problem of big actions and connect it with other areas would be to relate it to supersingular curves and maximal curves, both of these curves playing a major role in coding theory and cryptography.
   Indeed, the examples of big actions given in my thesis highlights the well-known link between curves endowed with a large automorphism group and curves defined over a finite field with many rational points. In this spirit, a natural idea would be to make the connection between big actions and $\mathbb{F}_q$-maximal curves, namely curves defined over the finite field $\mathbb{F}_q$ whose number of $\mathbb{F}_q$-rational points attains the Hasse-Weil bound, namely $1 + q + 2g\sqrt{q}$.
   Another kind of curves which are naturally related to maximal curves are the supersingular curves, that is the curves whose Jacobian is isogeneous to a product of supersingular elliptic curves (i.e. elliptic curves defined over a field of characteristic $p > 0$ having no geometric point of order p). These supersingular curves are of main interest in coding theory insofar as, over certain extensions, they have a maximal number of rational points. More precisely, if the curve C is $\mathbb{F}_q$-maximal, then C is supersingular. Conversely, if C is supersingular, C is maximal over some extension of $\mathbb{F}_q$.
   A vast literature has been recently devoted to supersingular curves in relation with Artin-Schreier curves (see e.g. the works of Hui June Zhu and Jasper Scholten : *Supersingular abelian varieties over finite fields* J. Number Theory, 86 (2001) or *Slope estimates on Artin-Schreier curves* Compositio Math. 137 (2003)...)

   We now emphasize the link with *big actions*. It is already known that the curves parametrized by an Artin-Schreier equation of the type $W^p - W = XS(X)$ where S is an additive polynomial of $k[X]$, k being a finite field of characteristic $p > 0$, are supersingular. This is due to G. van der Geer and M. van der Vlugt in a work related to Reed Muller codes (*Reed-Muller codes and supersingular curves. I.* Compositio Math. 84 (1992), no. 3). Using the works of E. Kani and M. Rosen (*Idempotent relations and factors of Jacobians.* Math. Ann. 284 (1989), no. 2, 307–327), one can generalize this result to any algebraically closed field k of characteristic $p > 0$.

As seen in my thesis, this type of curves corresponds to the big actions with a p-cyclic G_2. The same question can now be raised for the big actions with a p-elementary abelian G_2, namely parametrized by n Artin-Schreier equations $W_i^p - W_i = f_i(X) \in k[X]$, each f_i being the linear combination of products of at most $i+1$ additive polynomials. Are these curves supersingular ? Otherwise, can we give a decomposition of their Jacobian ? To answer this question, it may be fruitful to use the results of Kani and Rosen (op. cit.) who exhibit the decomposition of the Jacobian through the Jacobians of some well-chosen quotient curves.

Another approach to this problem may be more computational. Indeed, recall that, in the case $g = 1$, a curve C is supersingular if and only if its p-rank is zero. Note that, in the case of a big action, the Deuring-Shafarevitch formula implies that the the p-rank vanishes. Nevertheless, in the higher dimensional case $g \geq 2$, it is no more true that C is supersingular if its p-rank is zero. To answer this question, one has to consider a finite set of $g \times g$ matrices, called the Cartier-Manin matrices, whose vanishing is equivalent to C being supersingular. Accordingly, to make up one's mind, it may be a good idea to start computing these matrices on some examples (with the possible help of an adapted computing system).

3. What played a major role in the parametrization of the curves that I study is the additive polynomials. So it seems natural to search for the connections with other aeras such that geometry, arithmetic or algebra where these polynomials also appear. Indeed, as noticed by N. Elkies (*Linearized algebra and finite groups of Lie type. I. Linear and symplectic groups. Applications of curves over finite fields* Contemp. Math., 245, Amer. Math. Soc., Providence, RI, 1999.), these polynomials that first arose in Galois' construction and analysis of finite fields, have since figured in the theory of Drinfeld modules, in the construction of supersingular curves (see point above) but also in the Abhyankar's approach to the inverse Galois problem for $k(T)$. Moreover, Elkies explains how the additive polynomials can provide close analogues to linear differential operators. In this spirit, B. H. Matzat use them in his recents works on Frobenius structure in positive characteristic and thus proves their crucial role in differential Galois Theory.
   Off course the purpose is not really the same as mine but the tools and techniques are actually very close. That is why I feel very interested to learn more about these methods to enlarge my own research field.