Big Actions with non abelian derived subgroup.

P. Chrétien and M. Matignon

June 20, 2012

Abstract

For any $p > 2$ we give an example of big action (X, G) with non abelian derived subgroup. It is obtained as a covering of a curve related to the Ree curve.

1 Introduction

Let k be an algebraically closed field of characteristic $p > 0$, a *big action* is a pair (X, G) where X/k is a smooth, projective, integral curve of genus $g(X) \geq 2$ and G is a finite p-group, $G \subseteq \mathrm{Aut}_k(X)$, such that $|G| > \frac{2p}{p-1} g(X)$. Big actions were studied by Lehr and Matignon [LM05] then by Matignon and Rocher [MR08] and Rocher [Roc09]. They study big actions (X, G) with an abelian derived group $\mathrm{D}(G)$. The main goal of this paper is to give the first example, to our knowledge, of big action (X, G) with non abelian $\mathrm{D}(G)$.

The approach in [MR08] to construct big actions (X, G) with an abelian $\mathrm{D}(G)$ is to consider ray class fields of function fields. Let $n \in \mathbb{N} - \{0\}$, $q := p^n$, $m \in \mathbb{N}$, $K := \mathbb{F}_q(x)$ and $S := \{(x - a), a \in \mathbb{F}_q\}$ be the set of finite $\mathbb{F}_q$-rational places of K. One defines the *S-ray class field mod $m\infty$*, denoted by $K_S^{m\infty}$, as the largest abelian extension L/K with conductor $\leq m\infty$ such that every place in S splits completely in L. Denote by $G_S(m) := \mathrm{Gal}(K_S^{m\infty}/K)$ and $C_S(m)/\mathbb{F}_q$ the smooth, projective, integral curve with function field $K_S^{m\infty}/\mathbb{F}_q$. Then, the group of $\mathbb{F}_q$-automorphisms of $\mathbb{P}^1_{\mathbb{F}_q}$ given by $x \mapsto x + a$ with $a \in \mathbb{F}_q$ has a prolongation to a p-group $G(m) \subseteq \mathrm{Aut}_{\mathbb{F}_q}(C_S(m))$ with an exact sequence

$$0 \to G_S(m) \to G(m) \to \mathbb{F}_q \to 0.$$

Moreover, if m is large enough, then $|G(m)| > \frac{q}{-1+m/2} g(C_S(m))$. If moreover $\frac{q}{-1+m/2} \geq \frac{2p}{p-1}$, then the pair $(C_S(m), G(m))$ is a big action and one can show that $\mathrm{D}(G(m)) = G_S(m)$.

The above construction leads to big actions (X, G) with an abelian $\mathrm{D}(G)$. In order to produce big actions with a non abelian derived subgroup, we are going to mimic this construction in a slightly different context. We construct a finite non abelian Galois extension F/K with group $H := \mathrm{Gal}(F/K)$ such that the group of $\mathbb{F}_q$-automorphisms of $\mathbb{P}^1_{\mathbb{F}_q}$ given by $x \mapsto x + a$ with $a \in \mathbb{F}_q$ has a prolongation to a p-group $G \subseteq \mathrm{Aut}_{\mathbb{F}_q}(F)$ with the exact sequence

$$0 \to H \to G \to \mathbb{F}_q \to 0.$$

Let $X/\mathbb{F}_q$ be the smooth, projective, integral curve with function field $F/\mathbb{F}_q$, our construction is such that (X, G) is a big action and, as above, one can show that $\mathrm{D}(G) = H$.

Let $s \in \mathbb{N} - \{0\}$ and $q := 3^{2s+1}$, the *Ree curve* $X_R/\mathbb{F}_q$ has been extensively studied, see for example [Ped92], [HP93] and [Lau99]. It is a Ray class field over $\mathbb{F}_q(x)$ and equations generalizing this situation for $p \geq 3$ are given in [Aue99]. For $p = 3$, the function field $F/\mathbb{F}_q$ is an extension of $F(X_R)/\mathbb{F}_q$.

2 Background

Notations : Let p be a prime number, $q := p^n$ for some $n \in \mathbb{N} - \{0\}$ and et k be an algebraically closed field of characteristic $p > 0$.

1. *Galois Extensions of complete DVRs.* Let (K, v_K) be a local field with uniformizing parameter π_K such that $v_K(\pi_K) = 1$. Let L/K be a finite Galois extension with group G and separable residual extension, denote by v_L the prolongation of v_K to L such that $v_L(\pi_L) = 1$ for some uniformizing parameter π_L of L. Then G is endowed with a *lower ramification filtration* $(G_i)_{i \geq -1}$ where G_i is the *i-th lower ramification group* defined by $G_i := \{\sigma \in G \mid v_L(\sigma(\pi_L) - \pi_L) \geq i + 1\}$. The integers i such that $G_i \neq G_{i+1}$ are called *lower breaks*. The group G is also endowed with a *higher ramification filtration* $(G^i)_{i \geq -1}$ which can be computed from the G_i's by means of the *Herbrand's function* $\varphi_{L/K}$. The real numbers t such that $\forall \epsilon > 0$, $G^{t+\epsilon} \neq G^t$ are called *higher breaks*. The least integer $m \geq 0$ such that $G^m = \{1\}$ is called the *conductor of L/K*. The following theorem is due to Garcia and Stichtenoth, see [GS91].

Theorem 2.1. *Let K be a perfect field of characreristic $p > 0$. Let F/K be an algebraic function field of one variable with full constant field K and genus*

$g(F)$. Consider an elemantary abelian extension E/F of degree p^n such that K is the constant field of E. Denote by $E_1, \dots, E_t$, where $t = (p^n - 1)/(p-1)$, the intermediate fields $F \subseteq E_i \subseteq E$ with $[E_i : F] = p$ and by $g(E)$ (resp. $g(E_i)$), the genus of E/K (resp. E_i/K). Then

$$g(E) = \sum_{i=1}^{t} g(E_i) - \frac{p}{p-1}(p^{n-1} - 1)g(F).$$

2. *Automorphisms in positive characteristic.* See [LM05] for a complete account of big actions. Let G be a group and $\mathrm{D}(G)$ its derived subgroup.

Definition 2.1. *A big action is a pair (X, G) where X/k is a smooth, projective, geometrically connected curve of genus $g(X) \geq 2$ and G is a finite p-group, $G \subseteq \mathrm{Aut}_k(X)$, such that $|G| > \frac{2p}{p-1} g(X)$.*

Proposition 2.1. *Let (X, G) be a big action and $H \subseteq G$ be a subgroup.*

1. *There exists a point of X, say ∞, such that G is the wild inertia group G_1 of G at ∞ and $\mathrm{D}(G)$ is the second ramification subgroup G_2.*
2. *One has $g(X/H) = 0$ if and only if $\mathrm{D}(G) \subseteq H$.*

Definition 2.2. *Let $\pi : X \to \mathbb{P}^1_{\mathbb{F}_q}$ be a smooth, projective, geometrically connected p-cyclic cover . Then, $t_a \in \mathrm{Aut}_{\mathbb{F}_q}(\mathbb{P}^1_{\mathbb{F}_q})$ given by $x \mapsto x + a$ with $a \in \mathbb{F}_q$ has a prolongation $\tilde{t}_a \in \mathrm{Aut}_{\mathbb{F}_q}(X)$ if there is a commutative diagram*

$$\begin{array}{ccc} X & \xrightarrow{\tilde{t}_a} & X \\ {\scriptstyle \pi}\downarrow & & \downarrow{\scriptstyle \pi} \\ \mathbb{P}^1_{\mathbb{F}_q} & \xrightarrow{t_a} & \mathbb{P}^1_{\mathbb{F}_q} \end{array}$$

3. *Ree Curves.* There are three types of irreducible curves arising as the Deligne-Lusztig variety associated to a connected, reductive, algebraic group, these are the Hermitian curves, the Suzuki curves and the Ree curves (see [Lau99]). In this paper we will focus on the Ree curves which have been described in [Ped92] and [HP93]. Let $s \in \mathbb{N} - \{0\}$, $q_0 := 3^s$ and $q := 3q_0^2$.

Definition 2.3. *The Ree curves are the Deligne-Lusztig varieties $X_R/\mathbb{F}_q$ arising from the Ree groups ${}^2G_2(q)$.*

Proposition 2.2. *The Ree curve $X_R/\mathbb{F}_q$ is an irreducible curve of genus $g(X_R) = \frac{3}{2} q_0 (q-1)(q + q_0 + 1)$.*

a) The function field $\mathbb{F}_q(X_R)$ *is* $\mathbb{F}_q$*-isomorphic to* $\mathbb{F}_q(x, y_1, y_2)$ *defined by*

$$\begin{cases} y_1^q - y_1 & = x^{q_0}(x^q - x) \\ y_2^q - y_2 & = x^{2q_0}(x^q - x). \end{cases}$$

b) The curve $X_R/\mathbb{F}_q$ *is optimal. The curve* $X_R/\mathbb{F}_{q^n}$ *is maximal if and only if* $n \equiv 6 \bmod 12$.

c) The ramification filtration of $G := \mathrm{Gal}(\mathbb{F}_q(x, y_1, y_2)/\mathbb{F}_q(x))$ *at* ∞ *is*

$$G = G_0 = \cdots = G_{3q_0+1} \supsetneq G_{3q_0+2} = \cdots = G_{q+3q_0+1} \supsetneq \{1\},$$

and $G_{q+3q_0+1} = \mathrm{Gal}(\mathbb{F}_q(x, y_1, y_2)/\mathbb{F}_q(x, y_1))$.

d) One has $|\operatorname{Aut}_{\mathbb{F}_q^{\mathrm{alg}}}(X_R)| = |\operatorname{Aut}_{\mathbb{F}_q}(X_R)| = q^3(q-1)(q^3+1)$ *and the* 3*-Sylow subgroups* $S_3(X_R)$ *of* $\operatorname{Aut}_{\mathbb{F}_q}(X_R)$ *are such that* $(X_R, S_3(X_R))$ *are big actions.*

The function field $\mathbb{F}_q(X_R)/\mathbb{F}_q$ and its subextension $\mathbb{F}_q(x, y_1)/\mathbb{F}_q$ have a description as Ray class fields, see below.

4. *Ray Class Fields.* See [Aue99] for a detailed account. Let $K := \mathbb{F}_q(x)$ and fix an algebraic closure K^{alg} in which all extensions of K are assumed to lie. In this paper, we consider only Galois extensions of function fields of one variable with full constant field $\mathbb{F}_q$ that are totally ramified over a $\mathbb{F}_q$-rational point, say ∞, and unramified outside ∞. In this setting, the definition of the conductor given above coincide with that given in [Aue99] Part I.3.

Definition 2.4. *Let* $S := \{(x-a), a \in \mathbb{F}_q\}$ *be the set of finite* $\mathbb{F}_q$*-rational places of* K *and* $m \in \mathbb{N}$. *One defines the* S-ray class field mod $m\infty$, *denoted by* $K_S^{m\infty}$, *as the largest abelian extension* L/K *with conductor* $\leq m\infty$ *such that every place in* S *splits completely in* L.

Proposition 2.3 ([Aue99] III. Prop. 8.9 b) and Lemma 8.7 c))**.** *Assume that* $r := \sqrt{pq} \in \mathbb{N}$ *and let* $y_1, \ldots, y_{p-1} \in K^{\mathrm{alg}}$ *satisfy* $y_i^q - y_i = x^{ir/p}(x^q - x)$. *Then* $K_S^{i\infty} = K$ *for* $1 \leq i \leq p$ *and*

$$K_S^{(r+i+1)\infty} = K(y_1, \ldots, y_i) \text{ for } i \in \{1, \ldots, p-1\}.$$

3 Results

Notations : Let $p > 2$ be a prime number, $s \in \mathbb{N} - \{0, 1\}$, $q_0 := p^s$ and $q := pq_0^2$. Let $(\gamma_i)_{i=1}^{2s+1}$ be a $\mathbb{F}_p$-basis of $\mathbb{F}_q$,

$$\begin{aligned} \mathrm{Frob}_p : K^{\mathrm{alg}} &\longrightarrow K^{\mathrm{alg}} \\ x &\longmapsto x^p, \end{aligned}$$

and $\mathrm{Frob}_q = \mathrm{Frob}_p^{2s+1}$. Let $K := \mathbb{F}_q(x)$ and $F/\mathbb{F}_q$ be the function field of one variable with full constant field $\mathbb{F}_q$ defined by

$$\begin{cases} y_1^q - y_1 &= x^{q_0}(x^q - x) =: f_1(x) \\ y_2^q - y_2 &= x^{2q_0}(x^q - x) =: f_2(x) \\ v_1^q - v_1 &= y_1^q x - x^q y_1 \\ v_2^q - v_2 &= y_2^q x - x^q y_2 \\ w^q - w &= f_2(x) y_1 - f_1(x) y_2 = y_2^q y_1 - y_1^q y_2. \end{cases}$$

Remark : The function field $F/\mathbb{F}_q$ is also defined by the equations

$$\begin{cases} y_1^q - y_1 &= x^{q_0}(x^q - x) =: f_1(x) \\ y_2^q - y_2 &= x^{2q_0}(x^q - x) =: f_2(x) \\ v_1'^q - v_1' &= x^{q_0}(x^{2q} - x^2) =: g_1(x) \\ v_2'^q - v_2' &= x^{2q_0}(x^{2q} - x^2) =: g_2(x) \\ w'^q - w' &= 2y_1 f_2(x) + f_1(x) f_2(x), \end{cases}$$

allowing us to view F as the compositum of extensions of $\mathbb{F}_q(x, y_1)$.

Theorem 3.1. *Let $X/\mathbb{F}_q$ be the smooth, projective, integral curve with function field $F/\mathbb{F}_q$. Let $H \subseteq \mathrm{Aut}_{\mathbb{F}_q}(K)$ be the subgroup of translations $x \mapsto x + a$, $a \in \mathbb{F}_q$, then any $h \in H$ has q^5 prolongations to F, the extension F/K^H is Galois, the group $G := \mathrm{Gal}(F/K^H)$ has order q^6, the pair (X, G) is a big action and $\mathrm{D}(G)$ is a non-abelian group.*

Proof. Let $a \in \mathbb{F}_q$ and $t_a \in \mathrm{Aut}_{\mathbb{F}_q}(K)$ given by $x \mapsto x + a$. Let $\sigma : F \hookrightarrow K^{\mathrm{alg}}$ be a morphism such that $\sigma|_K = t_a$, an easy computation shows that

$$\begin{gathered} (\sigma(y_1)^q - \sigma(y_1)) - (y_1^q - y_1),\ (\sigma(y_2)^q - \sigma(y_2)) - (y_2^q - y_2), \\ (\sigma(v_1')^q - \sigma(v_1')) - (v_1'^q - v_1'),\ (\sigma(v_2')^q - \sigma(v_2')) - (v_2'^q - v_2'), \\ (\sigma(w')^q - \sigma(w')) - (w'^q - w'), \end{gathered}$$

are in $\mathrm{Frob}_q(F)$, thus the elements of H have q^5 prolongations to F and F/K^H is a Galois extension of degree q^6.

Using Theorem 2.1, one computes the genus of $K(y_1, y_{2,i})$ defined by the equations

$$\begin{cases} y_1^q - y_1 &= f_1(x) \\ y_{2,i}^p - y_{2,i} &= \gamma_i f_2(x). \end{cases}$$

One obtains

$$g(K(y_1, y_{2,i})) = \frac{q}{2q_0}\big[qp + q_0 p - q_0 - 1\big].$$

Let $K(y_1, v'_{1,i})$ and $K(y_1, v'_{2,i})$ be the function fields defined by the equations

$$\begin{cases} y_1^q - y_1 &= f_1(x) \\ v'^p_{1,i} - v'_{1,i} &= \gamma_i g_1(x), \end{cases} \qquad \begin{cases} y_1^q - y_1 &= f_1(x) \\ v'^p_{2,i} - v'_{2,i} &= \gamma_i g_2(x). \end{cases}$$

One computes their genera as above and one obtains

$$g(K(y_1, v'_{1,i})) = \frac{q}{2q_0}\big[2qp - q - 1\big],$$
$$g(K(y_1, v'_{2,i})) = \frac{q}{2q_0}\big[2qp + q_0 p - q_0 - q - 1\big].$$

Let $K(y_1, w'_i)$ be the function field defined by the equations

$$\begin{cases} y_1^q - y_1 &= f_1(x) \\ w'^p_i - w'_i &= \gamma_i\big[2y_1 f_2(x) + f_1(x) f_2(x)\big] = \gamma_i F(z), \end{cases}$$

in order to compute its genus, one needs an expression of y_1 and x in terms of a uniformizing parameter of $K(y_1)$ at infinity, this is the crucial point of the proof. One defines z by

$$a_1 := \frac{q^2 - qq_0 - q}{q_0}, \; a_2 := \frac{q^2 - q_0 - q}{q_0} \text{ and } x = z^{-q} + z^{a_1} - z^{a_2}.$$

Then, one shows that this change of variable completely splits the place $x = \infty$ in $K(y_1)$. One puts

$$\begin{aligned} b_1 :=& a_1 - qq_0, \quad b_2 := a_2 - qq_0, \\ y_T :=& \frac{1}{z^{q+q_0}} + z^{b_1} - z^{b_2} + z^{a_1 q_0 - q} - z^{a_2 q_0 - q} \\ &+ z^{a_1(1+q_0)} + z^{a_2(1+q_0)} - z^{a_1 + a_2 q_0} - z^{a_1 q_0 + a_2} + T. \end{aligned}$$

By expanding $y_T^q - y_T - f_1(x)$ one gets for some $G(z) \in \mathbb{F}_q[|z|]$

$$y_T^q - y_T - f_1(x) = z^{qb_1}(1 + zG(z)) + T^q - T.$$

According to Hensel's lemma, the equation $T^q - T + z^{qb_1}(1 + zG(z)) = 0$ in $\mathbb{F}_q[|z|][T]$ has a solution $T_0 \in \mathbb{F}_q[|z|]$ such that $v_z(T_0) > 0$, thus $v_z(T_0) = qb_1$. So one has constructed a solution $y_{T_0} \in \mathbb{F}_q[|z|]$ to the equation $Y^q - Y = f_1(x)$. Whence, one has the following diagram

$$\mathbb{F}_q((z)) \supseteq \mathbb{F}_q((\tfrac{1}{x}))[y_{T_0}]$$

$$\mathbb{F}_q((\tfrac{1}{x}))$$

Since $[\mathbb{F}_q((z)) : \mathbb{F}_q((\frac{1}{x}))] = q$ and $[\mathbb{F}_q((\frac{1}{x}))[y_{T_0}] : \mathbb{F}_q((\frac{1}{x}))] = q$, one has $\mathbb{F}_q((\frac{1}{x}))[y_{T_0}] = \mathbb{F}_q((z))$, i.e. z is a uniformizing parameter of $K(y_1)$ at infinity. Note that letting $y_T := \frac{1}{z^{q+q_0}} + z^{b_1} + T$ and using the same process, one still obtains that z is a uniformizing parameter of $K(y_1)$ at infinity, but in this case one has $v(T_0) = b_2$ and one needs a more accurate expansion of y_1 in order to compute the genus of $K(y_1, w'_i)$, see below.

Then, one expands $\gamma_i F(z) \in \mathbb{F}_q((z))$ in terms of z and T_0 and one reads its principal part $P_i(z)$. Note that $v_z(T_0) = qb_1$ implies that the terms in $\gamma_i F(z)$ where T_0 appears do not disturb $P_i(z)$. One has

$$P_i(z) = \gamma_i \Big[\frac{1}{z^{3q_0 q + 2q^2}} + \frac{1}{z^{q^2+q+3q_0 q}} - \frac{1}{z^{q_0+q+qq_0-a_2 q_0+q^2}} - \frac{1}{z^{q_0+q+2qq_0+q^2}} \Big],$$

and mod $(\mathrm{Frob}_p - \mathrm{Id})(\mathbb{F}_q((z)))$

$$P_i(z) \equiv \frac{\gamma_i^{q/q_0}}{z^{3+2pq_0}} + \frac{\gamma_i}{z^{1+3q_0+q}} - \frac{\gamma_i^{q/q_0}}{z^{1+pq_0+q-a_2+pq_0 q}} - \frac{\gamma_i^{q/q_0}}{z^{1+pq_0+2q+pq_0 q}}.$$

Thus, the conductor of the extension $K(y_1, w'_i)/K(y_1)$ is $2 + pq_0 + 2q + pq_0 q$ and applying the Riemann-Hurwitz formula, one obtains

$$g(K(y_1, w'_i)) = \frac{q}{2q_0}\big[2pq + 2pq_0 - q_0 - q - 1\big].$$

Applying [GS91] Theorem 2.1, one obtains that $g(F)$ equals

$$\frac{q-1}{p-1}\big[q^3 g(K(y_1, w'_i)) + q^2 g(K(y_1, v'_{2,i})) + qg(K(y_1, v'_{1,i})) + g(K(y_1, y_{2,i}))\big] - \frac{q-1}{p-1}\frac{q}{2q_0}(q-1). \qquad (1)$$

Then, an easy computation shows that (X, G) is a big action. Actually, the leading term in equation (1) is $\frac{q-1}{p-1} q^3 g(K(y_1, w'_i))$ which, surprisingly, is not too large compared to $|G|$, that is why (X, G) is a big action (note that $\lim_{p\to\infty} \frac{|G|}{g(F)} = q_0$, checking the inequality $|G| > \frac{2p}{p-1} g(F)$ being left to the reader).

One shows that $\mathrm{D}(G) = \mathrm{Gal}(F/K)$. Let $L := F^{\mathrm{D}(G)}$, according to Proposition 2.1 *2*, one has $\mathrm{D}(G) \subseteq \mathrm{Gal}(F/K)$, whence $K \subseteq L$. According to

Proposition 2.1 *2*, the function field L has genus 0, so the Riemann-Hurwitz formula implies that the conductor of L/K is $\leq 2\infty$. Let S be the set of finite $\mathbb{F}_q$-rational places of K, i.e. $S := \{(x-a), a \in \mathbb{F}_q\}$. Then L/K is an abelian extension with conductor $\leq 2\infty$ such that every place in S splits completely in L, then $L \subseteq K_S^{2\infty}$. According to Proposition 2.3, $K_S^{2\infty} = K$, i.e. $L = K$ and $\mathrm{D}(G) = \mathrm{Gal}(F/K)$.

One shows that $\mathrm{D}(G) = \mathrm{Gal}(F/K)$ is non abelian. The K-automorphisms of F/K defined by

$$\begin{cases} \sigma_i(y_1) &= y_1 + \gamma_i \\ \sigma_i(y_2) &= y_2 \\ \sigma_i(v_1') &= v_1' + \gamma_i \\ \sigma_i(v_2') &= v_2' \\ \sigma_i(w) &= w + \gamma_i y_2 \end{cases} \quad \text{and} \quad \begin{cases} \tau_i(y_1) &= y_1 \\ \tau_i(y_2) &= y_2 + \gamma_i \\ \tau_i(v_1') &= v_1' + \gamma_i \\ \tau_i(v_2') &= v_2' \\ \tau_i(w) &= w - \gamma_i y_1 \end{cases}$$

are such that τ_i and σ_j do not commute since $p > 2$. □

References

[Aue99] R. Auer. *Ray Class Fields of Global Function Fields with Many Rational Places.* PhD thesis, Lindau/ Bodensee, 1999.

[GS91] A. Garcia and H. Stichtenoth. *Elementary abelian p-extensions of algebraic function fields.* Manuscripta Mathematica, (**72**), 1991.

[HP93] J.P Hansen and J.P. Pedersen. *Automorphism groups of Ree type, Deligne-Lusztig curves and function fields.* J. reine angew. Math., (**440**), 1993.

[Lau99] K. Lauter. *Deligne-Lusztig curves as ray class fields.* Manuscripta Mathematica, (**98**), 1999.

[LM05] C. Lehr and M. Matignon. *Automorphism groups for p-cyclic covers of the affine line.* Compositio Mathematica, n 5(**141**), 2005.

[MR08] M. Matignon and M. Rocher. *Smooth curves having a large automorphism p-group in characteristic $p > 0$.* Algebra and Number Theory, 2(**8**), 2008.

[Ped92] J. P. Pedersen. *A function field related to the Ree group.* In H. Stichtenothj and M. A. Tsfasman, editors, *Coding Theory and Algebraic Geometry, Proceedings, Luminy 1991.* Springer, Berlin, 1992.

[Roc09] M. Rocher. *Large p-group actions with a p-elementary abelian derived group.* Journal of Algebra, (**321**), 2009.