JOURNAL de Théorie des Nombres de BORDEAUX

anciennement Séminaire de Théorie des Nombres de Bordeaux

Aristides KONTOGEORGIS

Field of moduli versus field of definition for cyclic covers of the projective line

Tome 21, n° 3 (2009), p. 679-693.

<http://jtnb.cedram.org/item?id=JTNB_2009__21_3_679_0>

Journal de Théorie des Nombres
de Bordeaux **21** (2009), 679-693

Field of moduli versus field of definition for cyclic covers of the projective line

par Aristides KONTOGEORGIS

Résumé. Nous donnons un critère, dépendant du groupe des automorphismes, pour que certains revêtements cycliques de la droite projective soient définis sur leur corps de modules. Nous donnons aussi un exemple de revêtement cyclique de la droite projective complexe de corps de module $\mathbb{R}$ qui ne peut pas être défini sur $\mathbb{R}$.

Abstract. We give a criterion, based on the automorphism group, for certain cyclic covers of the projective line to be defined over their field of moduli. An example of a cyclic cover of the complex projective line with field of moduli $\mathbb{R}$ that can not be defined over $\mathbb{R}$ is also given.

1. Introduction

Let k be a perfect field of characteristic $p \geq 0$. Fix an algebraic closure $\bar{k}$ of k. A k-curve X is a smooth, geometrically connected proper scheme $X \to \mathrm{Spec}k$ of dimension one. In this paper we will focus on deciding whether the field of moduli is a field of definition. Let g denote the genus of the curve X. It is known that if $g \leq 1$ then the fields of moduli and definition of X coincide. If $g \geq 2$ then a field of moduli for the curve X does not need to be a field of definition. In what follows we will assume that $g \geq 2$.

Hyperelliptic curves, i.e., 2-cyclic covers of the projective line of genus $g \geq 2$, are favoured among other curves since they have a simple form, which allows us to perform explicit computations. B. Huggins in [6] studied hyperelliptic curves, for $p \neq 2$ and using the results of P. Dèbes, M. Emsalem, J.C. Douai [3],[4] she proved that if $X \to \mathrm{Spec}\bar{k}$ is a hyperelliptic curve of genus $g \geq 2$ with hyperelliptic involution i, then $X \to \mathrm{Spec}\bar{k}$ is defined over its field of moduli, provided that $\mathrm{Aut}_{\bar{k}}(X)/\langle i \rangle$ is not a cyclic group of order prime to p.

The aim of this paper is to extend the result of Huggins to the case of q-cyclic covers $X \to \mathbb{P}^1_{\bar{k}}$, where q is a prime number. Let $C_q := \mathrm{Gal}(X/\mathbb{P}^1_{\bar{k}}) \cong$

Manuscrit reçu le 16 mai 2007.

$\mathbb{Z}/q\mathbb{Z}$. It is not true in general that C_q is a normal subgroup of $\mathrm{Aut}_{\bar{k}}(X)$, see [9],[8].

We will treat the following cases of q-cyclic covers X of the projective line:

(1) Kummer covers ($(p,q)=1$) of the form
$$y^q = \prod_{1\le i\le s} (x-\rho_i)^{d_i},$$
where $2q < s$ and $(d_i, q) = 1$,
(2) Artin-Schreier covers ($q = p$) of the form:
   (a) $y^p - y = \frac{a}{x^p - x}$, $a \in \bar{k}$;
   (b) $p = 3, y^3 - y = \frac{i}{x(x-1)}$, $i^2 = 2$;
   (c) $y^p - y = \frac{1}{x^b}$, $b \mid p+1$.
   (d) Artin-Schreier covers that are not birational to one of the cases (2a),(2b),(2c) above.

If the cover $X \to \mathbb{P}^1_{\bar{k}}$ is birational to a cover of type (1) or (2d) then C_q is a normal subgroup of the full automorphism group. In this case we can form the quotient $\mathrm{Aut}_{\bar{k}}(X)/C_q$ which is a finite subgroup of $\mathrm{PGL}(2,\bar{k})$. We show that the analysis carried out in [6] can be used in this more general case and we are able to prove:

Theorem 1.1. (1) *Let X be a q-cyclic cover of $\mathbb{P}^1_{\bar{k}}$ of type (1),(2d). If $\mathrm{Aut}_{\bar{k}}(X)/C_q$ is not a cyclic group of order prime to the characteristic of k, then the curve X can be defined over its field of moduli.*
(2) *If $X \to \mathbb{P}^1_{\bar{k}}$ is of type (2a),(2b),(2c) then X can be defined over its field of moduli.*
(3) *If X is an Artin-Schreier cover of $\mathbb{P}^1_{\bar{k}}$ of type (2d) and $\mathrm{Aut}_{\bar{k}}(X)/C_q$ is a cyclic group of order prime to the characteristic, then the group $\mathrm{Aut}_{\bar{k}}(X)$ is isomorphic to the semidirect product $C_p \rtimes C_\ell$, where C_ℓ acts on C_p in terms of a homomorphism $\alpha : C_\ell \to \mathrm{Aut}(C_p) \cong C_{p-1}$. If $\ker(\alpha) = \{1\}$ and $(|\alpha(C_\ell)|, (p-1)/|\alpha(C_\ell)|) = 1$ then X can be defined over its field of moduli.*

The paper is organised as follows: In section 2 we fix the notation and we state some properties of cyclic covers of the projective line. In section 3 we follow the ideas developed in [6] in the the more general setting of prime degree covers of the projective line. We also consider the three exceptional Artin-Schreier curves (2a), (2b), (2c) and the case of Artin-Schreier curves of the form (3) of theorem 1.1. All technical results needed in section 3 are proved in section 4. We prove there, that under certain assumptions, function fields of cyclic covers of the projective line have a unique rational subfield. This fact allows us to give the characterisation of maps between prime order covers of the projective line, which was essential for the proof

of (1) of theorem 1.1. Finally in section 5 we present an example of a Riemann surface which is a degree-q cyclic cover of the projective line, has field of moduli $\mathbb{R}$, but is not defined over $\mathbb{R}$.

2. Notation

2.1. Field of moduli and field of definition. Let k be a perfect field of characteristic $p \geq 0$. Fix an algebraic closure $\bar{k}$ of k. Set $\Gamma = \mathrm{Gal}(\bar{k}/k)$. Define the group

$$H = \{\sigma \in \Gamma : X \cong X^\sigma \text{ the isomorphism is defined over } \bar{k}\}.$$

The *field of moduli* of X, relative to the extension $\bar{k}/k$ is defined to be the fixed field of H, i.e. $\bar{k}^H$. A *field of definition* for the curve X is a subfield $E \subset \bar{k}$ such that there is a curve X_E defined over E, with the additional property $X_E \times_E \bar{k} \cong X$. If B is a curve defined over the field k, and E is an extension of k we will denote by B_E the curve $B \times_k E$.

Notice that the notions of field of moduli and field of definition can be defined in many categories with a suitable notion of isomorphism between the objects of the categories. Let B be a curve defined over k. The action of Γ on the covers over $\bar{k}$ with k-base B is defined as follows [4, §2]: An element $\sigma \in G$ transforms a cover $\pi : X \to B_{\bar{k}}$ into a cover $\pi^\sigma : X^\sigma \to B^\sigma_{\bar{k}}$. Attached to the k-model B of $B_{\bar{k}}$ there is a canonical isomorphism $\chi_\sigma : B^\sigma_{\bar{k}} \to B_{\bar{k}}$. In the category of covers with fixed k-base B, the conjugate cover of $\pi : X \to B_{\bar{k}}$ is the cover $\chi_\sigma \pi^\sigma : X^\sigma \to B_{\bar{k}}$.

2.2. Prime degree cyclic covers of the projective line. In this paper we will consider a curve X which is a cyclic cover $X \to \mathbb{P}^1_{\bar{k}}$ for some prime q. As it is observed in [3, §.2.1] the function field functor allows us to work with function fields instead. Denote the function field of X by F and the function field of $\mathbb{P}^1_{\bar{k}}$ by F_0. The extension F/F_0 is a cyclic Galois extension which is a Kummer extension if $p \neq q$ and an Artin-Schreier extension if $p = q$. We will recall some basic facts about Kummer and Artin-Schreier extensions. For more details we refer to [12, VI.3,VI.4].

2.2.1. *Kummer covers $p \neq q$.* A Kummer extension of $F_0 = \bar{k}(x)$ is birationaly isomorphic to a function field F of the form:

$$\bar{k}(x, y) : y^q = \prod_{1 \leq i \leq s} (x - \rho_i)^{d_i},$$

where $d_i \in \mathbb{Z}$, $(d_i, q) = 1$. The extension F/F_0 is a Kummer extension and the ramification of places in this type of extensions is known [12, prop. III.7.3]. Namely, the only places of F_0 that are ramified are the places P_i which correspond to the points $x = \rho_i$ and the corresponding ramification

indices are given by

$$e_i = \frac{q}{(q, d_i)}.$$

Moreover if $(q, d_i) = 1$ then the places P_i are ramified completely and the Riemann-Hurwitz formula implies that the function field F has genus

$$g = \frac{(q-1)(s-2)}{2}. \tag{1}$$

Notice that the condition $g \geq 2$ is equivalent to $s \geq 2\frac{q+1}{q-1}$. In particular, $s > 2$. If $\delta := \sum_{i=1}^{s} d_i \equiv 0 \bmod q$ then the place at infinity does not ramify in the extension F/F_0 [8, p.667].

2.2.2. ***Artin-Schreier covers.*** An Artin-Schreier extension F/F_0 is a cyclic extension of $F_0 = \bar{k}(x)$ of order p and such an extension admits the following model:

$$y^p - y = g(x), \text{ where } g(x) \in \bar{k}(x). \tag{2}$$

If we assume that the place at infinity does not ramify in the above extension, then $g(x)$ can be chosen so that

$$g(x) = \frac{f(x)}{\prod_{i=1}^{r}(x - a_i)^{\lambda_i}},$$

where $a_i \in \bar{k}$ are the roots of the denominator, $\lambda_i > 0$, $(\lambda_i, p) = 1$, and $f(x)$ is relatively prime to the polynomials $(x - a_i)$. The only places that are ramified in the extension $F/\bar{k}(x)$ are the poles of $g(x)$. The contribution to the different can be computed [12, prop. III.7.8] or [13, §. 2], and the following formula for the genus holds:

$$g = \frac{p-1}{2}\left(-2 + \sum_{i=1}^{r}(\lambda_i + 1)\right).$$

3. Proof of the main result

Let X be a $\bar{k}$-curve of genus $g \geq 2$, of type (1),(2a),(2b),(2c),(2d) and with field of moduli k. If X is of type (1) or (2d), let $X \to \mathbb{P}^1_{\bar{k}}$ be the degree q-cyclic cover corresponding to the unique rational subfield F_0 of the function field F of X.

As in [6], our main tool is the idea introduced in [3] and which consists in comparing the field of moduli X and of the Galois cover $X \to X/\mathrm{Aut}_{\bar{k}}(X)$. By assumption, for any $\sigma \in \Gamma$ there exists a $\bar{k}$-isomorphism $\phi_\sigma : X \xrightarrow{\sim} {}^{\sigma}X$ inducing a $\bar{k}$-isomorphism $\tilde{\phi}_\sigma : X/\mathrm{Aut}_{\bar{k}}(X) \xrightarrow{\sim} {}^{\sigma}X/\mathrm{Aut}_{\bar{k}}({}^{\sigma}X)$. Composing $\tilde{\phi}_\sigma$ with the canonical $\bar{k}$-isomorphism $i_\sigma : {}^{\sigma}X/\mathrm{Aut}_{\bar{k}}({}^{\sigma}X) \xrightarrow{\sim} {}^{\sigma}(X/\mathrm{Aut}_{\bar{k}}(X))$, one

gets a $\bar{k}$-isomorphism $\bar{\phi}_\sigma : X/\mathrm{Aut}_{\bar{k}}(X) \xrightarrow{\sim} {}^\sigma(X/\mathrm{Aut}_{\bar{k}}(X))$. In [3, thm. 3.1], it is shown that the $\bar{\phi}_\sigma$, $\sigma \in \Gamma$ satisfy Weil's cocycle conditions:

$$\bar{\phi}_{\sigma\tau} = \bar{\phi}_\tau^\sigma \bar{\phi}_\sigma, \ \ \sigma, \tau \in \Gamma,$$

hence there exists a unique k-curve $B \to k$ and a $\bar{k}$-isomorphism $c : B_{\bar{k}} \xrightarrow{\sim} X/\mathrm{Aut}_{\bar{k}}(X)$ such that:

$$\bar{\phi}_\sigma = {}^\sigma c c^{-1}, \ \ \sigma \in \Gamma.$$

We will call this model B *the canonical model* of the cover. Notice, as observed in [6], that assumption $p \nmid |\mathrm{Aut}(X)|$ posed in [4, th. 3.1] is not needed.

In addition, one has [3, Cor. 4.3]:

- $X \to B_{\bar{k}}$ has field of moduli k;
- X is defined over k if and only if $X \to B_{\bar{k}}$ is defined over k as a B-cover;
- $X \to B_{\bar{k}}$ is defined over k in the following cases:
  (1) k is of cohomological dimension ≤ 1
  (2) $G := \mathrm{Aut}_{\bar{k}}(X)$ has trivial center and the short exact sequence
  $$1 \to G \to \mathrm{Aut}(G) \to \mathrm{Out}(G) \to 1$$
  splits.
  (3) $B(k) \neq \emptyset$.

We will use criterion (3) to prove (1) of theorem 1.1 and criterion (2) to prove (3) of theorem 1.1. Part (2) will be proved using directly Weil's cocycle criterion ((2a)) or by showing that we are in situation (1) ((2b),(2c)).

We now complete the techinical details of the proof of theorem 1.1.

3.1. Proof of (1) of theorem 1.1. The possible subgroups $\mathfrak{B}$ of the group $\mathrm{PGL}(2, \bar{k})$ and their normalisers $N(\mathfrak{B})$ are known, see [13],[6]. One exceptional group in the list of those groups is the group which is isomorphic to the semidirect product of a cyclic group C_μ of order μ prime to the characteristic and of an elementary Abelian group of the form C_p^r. We can select the parameter x of the rational function field $\bar{k}(x)$ such that this group is given by $\mathfrak{B}_{\beta,A} := \left\{ \begin{pmatrix} \beta^k & a \\ 0 & 1 \end{pmatrix} \ \ a \in A \right\}$, where A is a finite additive subgroup of $\bar{k}$ containing 1 and β is an μ-th root of unity such that $\beta A = A$.

Let $F = \bar{k}(t)$ be the function field of $B_{\bar{k}}$. For any $\tau \in \Gamma$ suppose that $\bar{\phi}_\tau : B_{\bar{k}} \xrightarrow{\sim} B_{\bar{k}}$ is given by $\bar{\phi}(t) = \frac{a_\tau t + b_\tau}{c_\tau t + d_\tau}$ and define $\tau^* : F \to F$ by

$$\tau^*(t) = \frac{a_\tau t + b_\tau}{c_\tau t + d_\tau}, \ \ \tau^*(\alpha) = \tau(\alpha), \text{ for } \alpha \in \bar{k}.$$

The canonical k-model of B is the quotient corresponding to the fixed field F^{Γ^*} of $\Gamma^* = \{\tau^*\}_{\tau \in \Gamma}$.

For an element $\tau \in \Gamma$ let ϕ_τ be the isomorphism $\phi_\tau : X \to {}^\tau X$. This isomorphism reduces by propositions 4.2, 4.3 to an element $M \in \mathrm{PGL}(2, \bar{k})$. Let $\mathfrak{B}$ be the reduced automorphism group of X. According to [6, lemma 4.2] if $\mathfrak{B} \neq \mathfrak{B}_{\beta,A}$ then M is an element in $N(\mathfrak{B})$.

We distinguish two cases:

Case 1. In this case we assume $N(\mathfrak{B}) = \mathfrak{B}$. By [6, lemma 3.3] we have that $\mathfrak{B}$ is isomorphic to one of the groups $S_4, A_5, \mathrm{PGL}(2, \mathbb{F}_{p^r})$. We consider a generator x for the rational function field corresponding to the curve $\mathbb{P}^1 = X/\mathrm{C_q}$. The group $\mathfrak{B}$ acts on x and there is an invariant element t which is a rational function of x. The field $\bar{k}(t)$ is the function field of the quotient $X/\mathrm{Aut}_{\bar{k}}(X) = B_{\bar{k}}$. Since we have seen that $M \in N(\mathfrak{B}) = \mathfrak{B}$ we have that $M(t) = t$. Therefore, Γ^* acts on $B_{\bar{k}}$ by action of Γ on $\bar{k}$, and B_k corresponds to the function field $k(t)$, that has many rational places.

Case 2. In this case $N(\mathfrak{B}) \neq \mathfrak{B}$. All these cases were studied in [6, proof of th. 5.3]. It turns out that the canonical model B_k has a rational point.

3.2. Proof of (2) of theorem 1.1. According to lemma 3.1 two curves $X_{a_i} : (y^p - y)(x^p - y) = a_i$ with $a_1, a_2 \in \bar{k}$ are isomorphic if an only if $a_1 = a_2\lambda$ for some $\lambda \in \mathbb{F}_p$. Moreover an isomorphism ψ between X_a and $X_{\lambda a}$ is given by $\psi(x) = \lambda x$, $\psi(y) = y$. Every element τ in Γ transfers the curve X_a to X_{a^τ} and these two curves are isomorphic if and only if $a = a^\tau \lambda_\tau$, for some element $\lambda_\tau \in \mathbb{F}_p$.

A curve X is defined over its field of moduli k if and only if for all $\sigma \in \Gamma = \mathrm{Gal}(\bar{k}/k)$ there are $\bar{k}$-isomorphisms $f_\sigma : X \to X^\sigma$, such that

$$f_\tau^\sigma f_\sigma = f_{\sigma\tau} \text{ for all } \sigma, \tau \in \Gamma. \tag{3}$$

This criterion is known in the literature as *the Weil cocycle condition* [14, th. 1].

The function $\Gamma \to \mathbb{F}_p$ sending $\tau \mapsto \lambda_\tau$ is a homomorphism and the cocycle criterion of Weil implies that X can be defined over k.

The curve $y^3 - y = ix^{-1}(x-1)^{-1}$, $i^2 = 2$ appears in Case (4) in the paper of Valentini-Madan [13], is hyperelliptic and has as automorphism group an extension of a cyclic group of order 2 by S_4. By [6, th. 5.3] it can be defined over k.

The curves $y^p - y = 1/x^b$, $b \mid p+1$ are allready defined over the field of moduli k since they are allready defined over $\mathbb{F}_p$. It is nice to point out that if $b < n$ then these curves are birational to the curves $x^n + y^b + 1 = 0$ $b \mid n$, $n = p+1$ [9, p. 125] and the curve defined by $y^p - y = 1/x^{p+1}$ is the Hermitian curve (which is isomorphic to the Fermat curve $x^{p+1} + y^{p+1} + 1$ [10]).

Lemma 3.1. *The two curves* $X_{a_i} : (x^p - x)(y^p - y) = a_i$, $i = 1, 2$ $a_i \in \bar{k}$ *are isomorphic if and only if* $a_1/a_2 \in \mathbb{F}_p$. *Let* $\lambda \in \mathbb{F}_p$. *An isomorphism* ψ *between* X_a *and* $X_{\lambda a}$ *is given by* $\psi(x) = \lambda x$, $\psi(y) = y$.

Proof. The group $\mathrm{Aut}(X_a)$ of the curve $X_a : (x^p - x)(y^p - y) = a$ is generated by the following elements: $\tau_{a,b}(x, y) = (x + a, y + b)$ where $a, b \in \mathbb{F}_p$, $\sigma_1(x, y) = (y, x)$, $\sigma_2(x, y) = (\epsilon x, \epsilon^{-1} y)$, where ϵ is a primitive $(p - 1)$-th root of 1 [13, th.7].

Let F_a be the function field of the curve X_a. All possible rational subfields F_i of F_a such that F_a/F_i is cyclic extension of degree p and $\mathrm{Gal}(F/F_i)$ is a subgroup of $\mathrm{Aut}(X_a)$, correspond to the set Σ of subgroups A of $\langle \tau_{a,b} \rangle_{(a,b) \in \mathbb{F}_p^2} \cong \mathbb{F}_p^2$ which are isomorphic to $\mathbb{F}_p$. We compute that $\sigma_1^{-1} \tau_{a,b} \sigma_1 = \tau_{b,a}$ and $\sigma_2^{-1} \tau_{a,b} \sigma_2 = \tau_{\epsilon a, \epsilon^{-1} b}$.

We distinguish the following two cases:

• If $p \neq 2, 3$ then the only subgroups of order p of $\mathrm{Aut}(X)$, that are invariant under the conjugation action of $\langle \sigma_2 \rangle$ are $\langle \tau_{a,0} \rangle$ and $\langle \tau_{0,b} \rangle$.

• If $p = 2$ then also the subgroup generated by $\tau_{1,1}$ is fixed by conjugation action of $\langle \sigma_2 \rangle$ and by the conjugation action of $\langle \sigma_1 \rangle$. If $p = 3$ then the subgroups generated by $\tau_{1,1}$ and $\tau_{1,2}$ respectivelly, are fixed by the conjugation action of $\langle \sigma_1, \sigma_2 \rangle$. In this case the only subgroups of order p of $\mathrm{Aut}(X)$, that are invariant under the conjugation action of $\langle \sigma_2 \rangle$ and are not invariant by the conjugation action of $\langle \sigma_1 \rangle$ are $\langle \tau_{a,0} \rangle$ and $\langle \tau_{0,b} \rangle$.

In both of the above cases the subgroups $\langle \tau_{a,0} \rangle$ and $\langle \tau_{0,b} \rangle$ are uniquelly determined in group theoretic means as subgroups of $\mathrm{Aut}(X)$. We will call *good subgroups* of $\mathrm{Aut}(X)$, the unique subgroups of order p of $\mathrm{Aut}(X)$ which are fixed by the conjugation action of $\langle \sigma_2 \rangle$ if $p \neq 2, 3$ and the unique subgroups of order p of $\mathrm{Aut}(X)$ which are fixed by the conjugation action of $\langle \sigma_2 \rangle$ and are not fixed by the conjugation action of $\langle \sigma_1 \rangle$. The rational fields that are stabilized by the action of the groups $\langle \tau_{a,0} \rangle, \langle \tau_{0,b} \rangle$ are $k(y), k(x)$, respectivelly.

Consider the two curves $X_{a_i} : (x^p - x)(y^p - y) = a_i$, $i = 1, 2$ $a_i \in \bar{k}$ with corresponding function fields F_{a_i} and let $\psi : F_{a_1} \to F_{a_2}$ be an isomorphism. The map

$$\begin{aligned} \mathrm{Aut}(F_{a_1}) &\to \mathrm{Aut}(F_{a_2}), \\ \sigma &\mapsto \psi \sigma \psi^{-1}, \end{aligned} \tag{4}$$

is an isomorphism of the corresponding automorphism groups. Consider the Galois group $\mathrm{Gal}(F_{a_1}/k(x)) = \langle \tau_{0,b} \rangle$. The element $\psi(x)$ generates a rational function field of the function field F_{a_2} of the curve X_{a_2} and $k(\psi(x)) = F_{a_2}^{\psi \langle \tau_{0,b} \rangle \psi^{-1}}$. The action given in eq. (4) is an isomorphism of groups and transfers good subgroups to good subgroups. Thus, the subfield $k(\psi(x))$ of F_{a_2} is either $k(x)$ of $k(y)$. There is an automorphism $\sigma \in \mathrm{Aut}(F_{a_2})$ such that $\psi' := \psi\sigma$ is an isomorphism $F_{a_1} \to F_{a_2}$ with the additional property

$k(\psi'(x)) = k(x)$, and this implies that $\psi'(x) = \frac{ax+b}{cx+d}$. By taking ψ' in both sides of the defining equation of X_{a_1} we obtain that

$$(\psi'(y)^p - \psi'(y)) \left(\left(\frac{ax+b}{cx+d} \right)^p - \left(\frac{ax+b}{cx+d} \right) \right) = a_1$$

Thus $\psi'(y)$ is a generator of the Artin-Schreier extension $F_{a_2}/k(x)$ and according to Hasse [5, eq. 3'] it is related to the genarator y by a relation of the form

$$\psi'(y) = \lambda y + B_0, \text{where} \frac{a_2}{x^p - x} = \lambda \frac{a_1}{\left(\frac{ax+b}{cx+d} \right)^p - \left(\frac{ax+b}{cx+d} \right)} + B_0^p - B_0. \tag{5}$$

On the other hand $\psi'(y)$ is a generator of a p-degree rational subfield of the function field F_{a_2} of X_{a_2} such that $\mathrm{Gal}(F_{a_2}/k(\psi'(y))$ is the other good subgroup, hence of the form

$$\psi'(y) = (a_1 y + b_1)/(c_1 y + d_1). \tag{6}$$

Comparing equations (5),(6) we obtain that $\psi'(y) = \lambda y + b$, with $\lambda \in \mathbb{F}_p^*$, $b \in \bar{k}$ and putting this into the defining equation of X_{a_2} we obtain that $\psi'(x) = \lambda' x + b'$, $\lambda' \in \mathbb{F}_p^*$ and $b, b' \in \mathbb{F}_p$. Thus $a_1/a_2 \in \mathbb{F}_p^*$.

Conversely, if $a_1/a_2 = \lambda \in \mathbb{F}_p^*$ then the transformation $\psi(x) = \lambda x$, $\psi(y) = y$ makes the function fields F_{a_i}, $i = 1, 2$ isomorphic. □

Remark: This theorem is a special case of a theorem determining isomorphism classes of the curves $(x^{p^n} - x)(y^{p^n} - y) = a$ that can be found in [2].

3.3. Proof of (3) of theorem 1.1. Since $(\ell, p) = 1$ by Zassenhaus theorem we obtain that $\mathrm{Aut}_{\bar{k}}(X)$ is isomorphic to the semidirect product $C_p \rtimes C_\ell$. Since C_p is normal in $\mathrm{Aut}_{\bar{k}}(X)$, we can consider the conjugation action of C_ℓ on C_p given by a map $\alpha : C_\ell \to \mathrm{Aut}(C_p) \cong C_{p-1}$.

Lemma 3.2. *The center $Z(C_p \rtimes C_\ell)$ equals:*

$$Z(C_p \rtimes C_\ell) = \begin{cases} \ker(\alpha) & \text{if } \ker(\alpha) < C_\ell \\ C_p \rtimes C_\ell & \text{if } \ker(\alpha) = C_\ell \end{cases}.$$

In particular if $\alpha : C_\ell \to \mathrm{Aut}(C_p) \cong C_{p-1}$ is a monomorphism then the group $C_p \rtimes C_\ell$ has trivial center.

Proof. If $\ker(\alpha) = C_\ell$ then the group is Abelian and everything is in the center. If $\ker(\alpha) < C_\ell$ then a generator $\sigma \in C_\ell$ is not in $\ker(\alpha)$. Thus $\alpha(\sigma)$ is not a trivial automorphism of C_p. Let τ be a generator of C_p. We have that $\alpha(\sigma)(\tau) = \tau^\ell$ where $\ell \not\equiv 1 \bmod p$ and $\alpha(\sigma)(\tau^k) = \tau^{k\ell}$. Therefore no element in C_p is in the center. The only elements which can be in the center are the elements in the kernel of α. □

Consider the group $G := \mathrm{Aut}_{\bar{k}}(X) = C_p \rtimes C_\ell$. We will assume that α is a monomorphism therefore G has trivial center. According to proposition 3.1 in [3], if the sequence

$$1 \to \mathrm{Inn}(G) \to \mathrm{Aut}(G) \to \mathrm{Out}(G) \to 1$$

splits, then the curve X is defined over its field of moduli. The desired result will follow using the group theoretic lemma 3.3 which characterises the splitting property of the above short exact sequence.

Lemma 3.3. *Consider the group* $G = \langle \tau, \sigma : \tau^p = \sigma^t = 1, \sigma\tau\sigma^{-1} = \tau^\ell \rangle$. *The group* G *is isomorphic to the semidirect product* $C_p \rtimes C_t$. *Assume that the map* $\alpha : C_t \to \mathrm{Aut}(C_p) \cong C_{p-1}$ *sending* τ^x *to* $\alpha(\tau^x) = \ell^x$ *is a monomorphism. Then the group* G *has trivial center and the group* $\mathrm{Aut}(G)$ *of automorphisms of* G *is isomorphic to* $C_p \rtimes C_{p-1}$. *The inner automorphisms* $\mathrm{Inn}(G)$ *is isomorphic to* $C_p \rtimes \alpha(C_t)$. *The short exact sequence*

$$1 \to \mathrm{Inn}(G) \to \mathrm{Aut}(G) \to \mathrm{Out}(G) \to 1 \tag{7}$$

splits if and only if $(t, (p-1)/t) = 1$.

Proof. Since α is a monomorphism, lemma 3.2 implies that G has trivial center. We compute that

$$\sigma^i \tau^j \sigma^{-i} = \tau^{j\ell^i}.$$

The map α is assumed to be a monomorphism, therefore $\ell^i = 1$ if and only if $i = 0$.

Let now ϕ be an arbitrary automorphism of G. We observe first that ϕ should preserve the normal subgroup generated by τ, i.e., $\phi(\tau) = \tau^\mu$ for some $0 < \mu < p-1$. Set $\phi(\sigma) = \tau^{\nu_1}\sigma^{\nu_2}$. We have

$$\phi(\sigma\tau\sigma^{-1}) = \phi(\tau^\ell) \Rightarrow \tau^{\mu\ell^{\nu_2}} = \tau^{\mu\ell}.$$

This implies that $\mu\ell^{\nu_2} \equiv \ell\mu \bmod p$ and since $(\mu, p) = 1$ we have that $\ell^{\nu_2 - 1} \equiv 1 \bmod p$. We have assumed that α is a monomorphism, therefore $\nu_2 = 1$. Thus the automorphism ϕ depends on the two parameters (μ, ν_1). Denote by $\phi(\nu, \mu)$ the automorphism corresponding to (ν, μ). The composition of $\phi(\nu_1, \mu_1)$, $\phi(\nu_2, \mu_2)$ is given by $\phi(\nu_2\mu_1 + \nu_1, \mu_1\mu_2)$, and it is easy to see that $\mathrm{Aut}(G) \cong C_p \rtimes C_{p-1}$, where C_{p-1} acts on C_p by multiplication by μ.

We will compute now the group of inner automorphisms $\mathrm{Inn}(G)$. An arbitrary element in G can be written as $\sigma^i\tau^j$ for some $0 \le i \le t-1$, $0 \le j \le p-1$. The corresponding inner automorphism $\phi_{i,j}$ sends the generators σ, τ of G to

$$\begin{aligned} \phi_{i,j}(\tau) &= \sigma^i\tau^j\tau\left(\sigma^i\tau^j\right)^{-1} = \tau^{\ell^i} \\ \phi_{i,j}(\sigma) &= \sigma^i\tau^j\sigma\left(\sigma^i\tau^j\right)^{-1} = \tau^{-j(\ell-1)\ell^i}\sigma. \end{aligned}$$

We identify $\mathrm{Aut}(C_p)$ with $\mathbb{Z}_p^* \cong C_{p-1}$. If $\mu \in \mathrm{Im}(\alpha)$, then there is an i_0 such that $\ell^{i_0} \equiv \mu \bmod p$. Moreover the equation

$$-j(\ell-1)\ell^{i_0} = \nu \bmod p,$$

has always a unique solution j_0 since $((\ell-1)\ell^{i_0}, p) = 1$. In this case $\phi(\nu,\mu) = \phi_{i_0,j_0}$. The short exact sequence given in eq. (7) can be written as

$$1 \to C_p \rtimes C_t \to C_p \rtimes C_{p-1} \to C_{(p-1)/t} \to 1,$$

and this sequence splits if and only if $(t,(p-1)/t) = 1$. □

4. Properties of q-covers of the projective line

4.1. Rational subfields. It is known that for hyperelliptic curves the hyperelliptic involution is always normal in the whole automorphism group, and that the corresponding hyperelliptic function field F has a unique rational subfield F_0 such that $[F : F_0] = 2$. This result is not true for the general case of q-covers for the projective line [9],[8]. However the following holds:

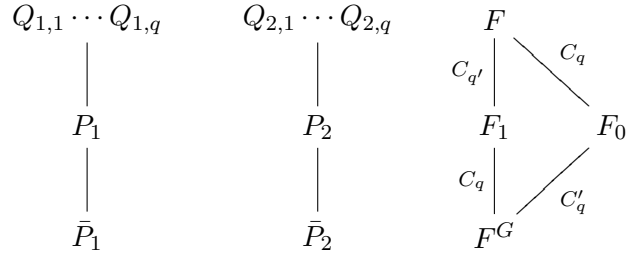
Proposition 4.1. *Consider a q-cyclic extension F/F_0 of the rational function field $F_0 = \bar{k}(x)$, such that the genus g of F is $g \geq 2$. If F is birational to one of the curves given in (1),(2d) then F_0 is the unique rational subfield E of F such that F/E is Galois with cyclic Galois group of order q.*

Proof. For the case $p = q$ the result is proved by Valentini-Madan [13, th. 6].

We will treat now the case $q \neq p$. It is known that the condition $2q < s$ implies that C_q is a normal subgroup of the whole automorphism group [8, prop. 1]. Suppose that there is one more rational subfield F_1 such that the extension F/F_1 is Galois and $C_q' = \mathrm{Gal}(F/F_1)$ is cyclic of order q. Since q is prime we have either $C_q \cap C_q' = \{1\}$ or $C_q = C_q'$. But since $F^{C_q} = F_0 \neq F_1 = F^{C_q'}$ we have $C_q \cap C_q' = \{1\}$.

Let G be the subgroup of $\mathrm{Aut}_{\bar{k}}(F)$ generated by C_q, C_q'. Since C_q is normal in the whole automorphism group it is normal in G as well. The group G is of order q^2 and is Abelian since q is prime. The group G is not cyclic. Indeed, it is known that for a cyclic group G_1 and for every divisor δ of the order of G_1 there is a unique subgroup G_0 of G_1 of order δ. This is not the case for G. Therefore the group G is isomorphic to the product $C_q \times C_q'$.

We have the following picture of subfields of F:



The cyclic group C_q acts on the rational function field F_1 and we can choose a parameter t on F_1 such that the action is given by $t \mapsto \zeta t$, where ζ is a primitive q-th root of unity. There are exactly two places $P_1 = P_{t=0}, P_2 = P_\infty$ of F_1 which are ramified in $F_1/F_1^{C_q}$. Consider a place Q of F above P_i for $i = 1$ or $i = 2$. Either Q/P_i is ramified completely or Q/P_i is decomposed. If Q/P_i is ramified completely then it is ramified completely in the extension F/F^G. In this case the decomposition group $G(Q)$ is the whole group G and this is not possible since decomposition groups of order prime to the characteristic are cyclic [12, III.8.6].

Hence, there are q places $Q_{1,\nu}$, $\nu = 1, \ldots, q$ of F above P_1 and q places $Q_{2,\nu}$, $\nu = 1, \ldots, q$ of F above P_2. Let $\bar{P}_1, \bar{P}_2$ be the restrictions of P_1, P_2 in F^G. We know that $e(Q_{i,\nu}/\bar{P}_i) = q$ and every place $Q_{i,\nu}$ is fixed by C_q. But then at least $2q$ places of F_0 are ramified in F/F_0, a contradiction since $2q < s$. □

4.2. Automorphisms. From now on we will assume that the conditions of proposition 4.1 are fulfilled, in particular $C_q = \mathrm{Gal}(F/F_0)$ is a normal subgroup of the automorphism group $\mathrm{Aut}_{\bar{k}}(X)$. This allows us to consider the reduced automorphism group $\mathfrak{B} = \mathrm{Aut}_{\bar{k}}(X)/C_q$. This is a finite subgroup of $\mathrm{PGL}(2, \bar{k})$ which permutes the ramification points of the extension F/F_0.

Assume first that we are in the $p \neq q$ case. Let $X : y^q = f(x)$ and $X' : w^q = g(z)$ be two isomorphic curves, and let $\phi : F \to F'$ be an isomorphism of the corresponding function fields. Obviously, $\phi(k(x))$ is a Galois subfield of F' with cyclic Galois group of order q. Proposition 4.1 implies that $\bar{k}(\phi(x)) = \bar{k}(z)$, and this gives us that $\phi(x) = \frac{az+b}{cz+d}$, where $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is a representative of an element in $\mathrm{PGL}(2, \bar{k})$.

We apply the automorphism ϕ on the defining equation $y^q = f(x)$ and we obtain:

$$\phi(y)^q = f(\phi(x)) = f\left(\frac{az+b}{cz+d}\right). \tag{8}$$

Let us write

$$f(x) = \prod_{i=1}^{s} (x - \rho_i)^{d_i},$$

and set $\delta = \sum_{i=1}^{s} d_i$. We can choose a parameter x such that the place at infinity is not ramified. The choice of such a parameter implies that $\delta \equiv 0 \bmod q$. The element $\phi(y)$ is a generating radicant of the extension $F'/\bar{k}(z)$, therefore it is of the form $w^i a(z)$ with $1 \leq i < q$, where $a(z) \in \bar{k}(z)$. On the other hand a simple computation shows that:

$$f\left(\frac{az+b}{cz+d}\right) = \left(\frac{c}{cz+d}\right)^{\delta} f(a/c) \prod_{i=1}^{s} \left(z - \frac{\rho_i d - b}{-\rho_i c + a}\right)^{d_i}.$$

Therefore, (8) implies that

$$g(z)^i a(z)^q = \left(\frac{c}{cz+d}\right)^{\delta} f(a/c) \prod_{i=1}^{s} \left(z - \frac{\rho_i d - b}{-\rho_i c + a}\right)^{d_i},$$

and since $g(z), f(z)$ are not q powers we have that $a(z) = \left(\frac{1}{cz+d}\right)^{\delta/q}$ multiplied by a constant. The above ideas allows us to prove:

Proposition 4.2. *Let F' be another function field given by an equation $y^q = f'(x)$, where $f'(x) \in \bar{k}[x]$ is a polynomial which is not a q-power. Every isomorphism $\phi : F \to F'$, is given by an expression of the form:*

$$\phi(x) = \frac{ax+b}{cx+d}, \quad \phi(y) = \frac{ey^i}{(cx+d)^{\delta/q}}, \text{ for some } 1 \leq i < q, e \in \bar{k}^*.$$

The pair $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\bar{k})$ and $e \in \bar{k}^*$ is unique up to replacement by $(\lambda M, e\lambda^{\delta/q})$ If $\phi' : F' \to F''$ is another isomorphism given by (M', e') then the composition $\phi'\phi$ is given by $(M'M, e'e)$.

We will now focus on the case of Artin-Schreier extensions of the projective line. Assume that F, F' are two Artin-Schreier extensions of the fields $F_0 = \bar{k}(x), F_0' = \bar{k}(z)$ which do not fall to one of the excluded cases (2a),(2b),(2c), in particular F_0 (resp. F_0') is the unique rational function field of F (resp. F') of degree p. Assume also that F, F' are given by the equations:

$$F = \bar{k}(y, x) : y^p - y = f(x), \qquad F' : w^p - w = g(z). \tag{9}$$

Since F_0' is the unique rational subfield of F' of degree p we have that $\sigma(F_0) = F_0'$ and in particular $\sigma(x) = \frac{az+b}{cz+d}$ for some invertible matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $a, b, c, d \in \bar{k}$. On the other hand, $\sigma(y)$ is a generating element of the Artin-Schreier extension F'/F_0', therefore it is of the form $\sigma(y) =$

$\lambda_\sigma w + \alpha_\sigma(z)$, for some $\lambda_\sigma \in \mathbb{F}_p^*$ and $\alpha_\sigma(z) \in \bar{k}(z)$. By applying σ to the defining equation (9) we obtain that

$$\lambda_\sigma g(z) - f\left(\frac{az+b}{cz+d}\right) = \alpha_\sigma(z)^p - \alpha_\sigma(z). \tag{10}$$

Thus we have the following:

Proposition 4.3. *Let F, F' be two Artin-Schreier extensions of the fields $F_0 = \bar{k}(x), F_0' = \bar{k}(z)$ which do not fall to one of the excluded cases (2a),(2b),(2c), defined in terms of equation (9). Every isomorphism $F \to F'$ is given by*

$$\sigma(x) = \frac{az+b}{cz+d}, \quad \sigma(y) = \lambda_\sigma w + \alpha_\sigma(z)^p - \alpha_\sigma(z)$$

where $\lambda_\sigma \in \mathbb{F}_p^*$ and $\alpha_\sigma(z) \in \bar{k}(z)$ satisfies equation (10). On the coordinate x of the function field F_0 the isomorphism σ acts as a Möbius transformation.

Remark: The exact value of $\alpha_\sigma(z)$ corresponds to the solution of the first order "Frobenious Differential Equation" (10) in the sense of [7, 1.9].

5. Example of curves not defined over their field of moduli.

In this section, $k = \mathbb{R}$. We provide an example of degree q-cyclic cover of the projective line with field of moduli $\mathbb{R}$ but not defined over $\mathbb{R}$, which generalizes the one of [6, §6].

Consider a cyclic cover X of the projective line of the form $y^q = f(x)$ with function field F such that the cyclic group $C_q = \mathrm{Gal}(F/k(x))$ is a normal subgroup of the whole automorphism group. The reduced group $B = \mathrm{Aut}(X)/C_q$ is determined by the relative position of the roots of the polynomial $f(x)$ [8] [1], and does not depend on the value of q.

Let $n, m \in \mathbb{Z}_{>1}$ with m odd. Let c denote complex conjugation and set

$$f(x) := \prod_{1 \le i \le m} (x^n - a_i)\left(x^n + \frac{1}{a_i^c}\right),$$

where $a_i := (i+1)\zeta_m^i$, $i = 1, \ldots, m$ and ζ_m is a primitive m-th root of unity. Then the maximal subgroup of $\mathrm{PGL}_2(\mathbb{C})$ permuting the roots of f is the order n-cyclic group generated by

$$x \mapsto \zeta_n x.$$

Assume furthermore that $2q < 2mn$ and that $q \mid 2m$ Then the curve X defined by

$$y^q = f(x)$$

has automorphism group $C_q \times C_n$, where C_q is generated by $\gamma(x, y) = (x, \zeta_q y)$ and C_n is generated by $\nu(x, y) = (\zeta_n x, y)$.

Proposition 5.1. *The curve X has field of moduli $\mathbb{R}$, but is not defined over $\mathbb{R}$.*

Proof. Consider the conjugate curve ${}^cX$ given by

$$y^q = \prod_{1 \le i \le m} (x^n - a_i^c)(x^n + 1/a_i).$$

The curves X, X^c are isomorphic by the isomorphism

$$\mu(x, y) = \left(\frac{1}{\omega x}, \frac{\omega' y}{x^{2mn/q}} \right),$$

where $\omega^n = -1$ and $\omega'^q = -1$.

Since the automorphism group of X is $C_q \times C_n$ any isomorphism $u_c : X \to X^c$ is given by $u_c := \mu\gamma^i\nu^j$, where $0 \le i < q$ and $0 \le j < n$. Straightforward computations show that:

$$\begin{aligned} \mu\gamma &= \gamma\mu \\ \mu\nu &= \nu^c\mu \\ \mu^c\mu &= \nu^{l_0}\gamma^{l_1} \text{ for some } l_0, l_1 \text{ with } q \nmid l_1. \end{aligned}$$

Hence,

$$u_c^c u_c = \nu^{2j+l_0}\gamma^{l_1} \neq \mathrm{Id}.$$

Therefore Weil's cocycle condition (3) does not hold and X cannot be defined over $\mathbb{R}$. □

Acknowledgments. The author would like to thank the referee for his corrections and valuable remarks.

References

1. Jannis A. Antoniadis and Aristides Kontogeorgis, *On cyclic covers of the projective line*. Manuscripta Math. **121** (2006), no. 1, 105–130. MR2258533
2. Gunter Cornelissen, Fumiharu Kato and Aristides Kontogeorgis, *Three examples of the relation between rigid-analytic and algebraic deformation parameters*. ArXiv:0809.4579 (to appear in Israel Journal of Mathematics)
3. Pierre Dèbes and Jean-Claude Douai, *Algebraic covers: field of moduli versus field of definition*. Ann. Sci. École Norm. Sup. (4) **30** (1997), no. 3, 303–338. MR1443489 (98k:11081)
4. Pierre Dèbes and Michel Emsalem, *On fields of moduli of curves*. J. Algebra **211** (1999), no. 1, 42–56. MR1656571 (99k:14044)
5. Helmut Hasse, *Theorie der relativ-zyklischen algebraischen Funktionenkörper, insbesondere bei endlichem Konstantenkörper*. J. Reine Angew. Math. **172** (1934), 37–54.
6. Bonnie Huggins, *Fields of moduli of hyperelliptic curves*. Math. Res. Lett. **14** (2007), no. 00, 10001–10014.
7. David Goss, *Basic structures of function field arithmetic*. Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], vol. 35, Springer-Verlag, Berlin, 1996. MR1423131 (97i:11062)
8. Aristides Kontogeorgis, *The group of automorphisms of cyclic extensions of rational function fields*, J. Algebra **216** (1999), no. 2, 665–706. MR1692965 (2000f:12005)
9. Aristides Kontogeorgis, *The group of automorphisms of the function fields of the curve $x^n + y^m + 1 = 0$*. J. Number Theory **72** (1998), no. 1, 110–136.

10. Heinrich-Wolfgang Leopoldt, *Über die Automorphismengruppe des Fermatkörpers*. J. Number Theory **56** (1996), no. 2, 256–282.
11. Henning Stichtenoth, *Über die Automorphismengruppe eines algebraischen Funktionenkörpers von Primzahlcharakteristik. I. Eine Abschätzung der Ordnung der Automorphismengruppe*. Arch. Math. (Basel) **24** (1973), 527–544. 49 #2749
12. Henning Stichtenoth, *Algebraic function fields and codes*. Springer-Verlag, Berlin, 1993. 94k:14016
13. Robert C. Valentini and Manohar L. Madan, *A Hauptsatz of L. E. Dickson and Artin-Schreier extensions*. J. Reine Angew. Math. **318** (1980), 156–177. 82e:12030
14. André Weil, *The field of definition of a variety*. Amer. J. Math. **78** (1956), 509–524. MR 0082726 (18,601a)

Aristides Kontogeorgis
Department of Mathematics,
University of the Ægean, 83200
Karlovassi, Samos, Greece
E-mail: kontogar@aegean.gr
URL: http://myria.math.aegean.gr/~kontogar