



ELSEVIER

Contents lists available at ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra



A cohomological treatise of HKG-covers with applications to the Nottingham group



Aristides Kontogeorgis^{*}, Ioannis Tsouknidas

Department of Mathematics, National and Kapodistrian University of Athens, Panepistimioupolis, 15784 Athens, Greece

ARTICLE INFO

Article history:

Received 25 January 2020
Available online 1 April 2020
Communicated by V. Srinivas

Keywords:

Automorphisms of curves
Nottingham group
Cohomology of groups
Harbater-Katz-Gabber curves
Algebraic covers

ABSTRACT

We characterize Harbater-Katz-Gabber curves in terms of a family of cohomology classes satisfying a compatibility condition. Our construction is applied to the description of finite subgroups of the Nottingham Group.

© 2020 Elsevier Inc. All rights reserved.

1. Introduction

In this article we use and extend results from previous work of the first author together with S. Karanikolopoulos [12] on HKG-curves. We will work over an algebraically closed field k of characteristic $p \geq 5$.

Definition 1. A Harbater-Katz-Gabber cover (HKG-cover for short) is a Galois cover $X_{\text{HKG}} \rightarrow \mathbb{P}^1$, such that there are at most two branched k -rational points $P_1, P_2 \in \mathbb{P}^1$,

^{*} Corresponding author.

E-mail addresses: kontogar@math.uoa.gr (A. Kontogeorgis), iotsouknidas@math.uoa.gr (I. Tsouknidas).

URL: <http://users.uoa.gr/~kontogar> (A. Kontogeorgis).

where P_1 is tamely ramified and P_2 is totally and wildly ramified. All other geometric points of \mathbb{P}^1 remain unramified. In this article we are mainly interested in p -groups so our HKG-covers have a unique ramified point, which is totally and wildly ramified.

Work of Harbater [9] and of Katz and Gabber [13] showed that any finite subgroup G of $\text{Aut}(k[[t]])$ can be associated with an HKG-curve X . More precisely, G is the semi-direct product of a cyclic group of order prime to p (the maximal tamely ramified quotient) by a normal p -subgroup (the wild inertia group). We are interested in the latter group, so from now on we will replace the initial group G with the latter, finite p -subgroup of $\text{Aut}(k[[t]])$. The HKG-curves play an important role in the deformation theory of curves with automorphisms and to the celebrated proof of Oort conjecture, [18,19,6,4,5,20].

Working with the HKG-curve X allows us to use several global tools like the genus, the p -rank of the Jacobian etc to the study of $k[[t]]$. In this article we will employ the Weierstrass semigroup attached to the unique ramified point P , and we will use the results of [12] on relating the structure of the Weierstrass semigroup to the jumps of the ramification filtration.

More precisely, to the HKG-cover there is a Weierstrass semigroup $H(P)$ attached to the unique wildly ramified point P . An arithmetic semigroup, and in particular the Weierstrass semigroup, is always finitely generated, i.e. there are $\bar{m}_1, \dots, \bar{m}_h \in \mathbb{N}$ such that

$$H(P) = \mathbb{Z}_+ \bar{m}_1 + \dots + \mathbb{Z}_+ \bar{m}_h.$$

We will denote by m_i the i -th element of $H(P)$, while \bar{m}_i will denote the i -th generator of the semigroup. For every element $m_i \in H(P)$ we will select a function f_i with $(f_i)_\infty = m_i P$. Also each element \bar{m}_i corresponds to some function \bar{f}_i in the function field of the curve. This selection is not unique and we will study later what happens by different choices either of f_i or \bar{f}_i . The ramification filtration gives rise to a series of subgroups of the group G , see eq. (3), which correspond to a sequence of subfields $k(X/G) = F_0 \subset \dots \subset F_{s+1} = k(X)$ of the function field $F = k(X)$ of the curve X . By the properties of the ramification filtration, each extension F_{i+1}/F_i , $i = 0, \dots, s$ is abelian. We will see that $F_{i+1} = F_i(\bar{f}_i)$.

One of the main results of this article is the classification and description of the Galois actions in HKG-covers in terms of group cohomology. Assume that $X \rightarrow \mathbb{P}^1$ is an HKG-cover with a unique wildly ramified point $P \in X$. Consider the ring of holomorphic functions outside the point P

$$\mathbf{A} = \bigcup_{\nu=0}^{\infty} L(\nu P).$$

This ring is equipped with a valuation corresponding to P and elements of \mathbf{A} of valuation smaller or equal than ν , i.e. the Riemann-Roch space $L(\nu P)$, give rise to a vector space

of finite dimension. Notice that these kind of rings are essential in the general definition of Drinfeld modules, see [8, chap. 4].

Write s for the index of the biggest \bar{m}_i , such that $\bar{m}_i < m$. Every intermediate extension F_{i+1}/F_i is elementary abelian hence; isomorphic to $(\mathbb{Z}/p\mathbb{Z})^{n_i}$. Set $\mathbf{n} = (n_1, \dots, n_s) \in \mathbb{N}^s$. In eq. (10) we define the vector space $k_{\mathbf{n},m}[\bar{f}_0, \dots, \bar{f}_s]$ which will be considered as a G -module and prove that it is equal to $L((m-1)P)$.

The polynomial ring $k[f_0]$ is the semigroup ring corresponding to the Weierstrass semigroup \mathbb{N} of the projective line, which has bounded part the vector space $k_m[f_0]$ of polynomials of degree $\leq m$. The module $k_{\mathbf{n},m}[\bar{f}_0, \dots, \bar{f}_s]$ plays a similar role for the more general setting of the Weierstrass semigroup of the HKG-cover.

The action of G will be described by the following:

Theorem 2. *The G -module structure of $k_{\mathbf{n},m}[\bar{f}_0, \dots, \bar{f}_s]$ is described by a series of cohomology classes $\bar{C}_i \in H^1(\text{Gal}(F_{i+1}/F_1), k_{\mathbf{n},\bar{m}_i}[\bar{f}_0, \bar{f}_1, \dots, \bar{f}_{i-1}])$. These classes restricted to the elementary abelian group $\text{Gal}(F_{i+1}/F_i)$ define the additive polynomials $P_i(Y)$ which in turn describe the elementary abelian extensions F_{i+1}/F_i . Moreover, the additive polynomials P_i define maps*

$$H^1(G, k_{\mathbf{n},\bar{m}_i}[\bar{f}_0, \bar{f}_1, \dots, \bar{f}_{i-1}]) \longrightarrow H^1(G, k_{\mathbf{n},\bar{m}_i}[\bar{f}_0, \bar{f}_1, \dots, \bar{f}_{i-1}])$$

and the cocycles \bar{C}_i are in the kernel of P_i , that is

$$P_i(\bar{C}_i) = 0 \in H^1(G, k_{\mathbf{n},\bar{m}_i}[\bar{f}_0, \bar{f}_1, \dots, \bar{f}_{i-1}]). \tag{1}$$

Conversely every such series of elements $\bar{C}_i \in H^1(G, k_{\mathbf{n},\bar{m}_i}[\bar{f}_0, \bar{f}_1, \dots, \bar{f}_{i-1}])$, satisfyng eq. (1) defines in a unique way a HKG-cover.

Proof. We now sketch the ingredients of the proof. The precise proof will be given in the next sections of the article. Notice that the element \bar{C}_i is the image of the class $\bar{f}_i \in L(\bar{m}_iP)/L((\bar{m}_i-1)P)$ under the δ map in

$$\dots \rightarrow H^0(G, L(\bar{m}_iP)/L((\bar{m}_i-1)P)) \xrightarrow{\delta} H^1(G, L(\bar{m}_iP)) \rightarrow \dots$$

coming from the group cohomology long exact sequence corresponding to the short exact

$$0 \longrightarrow L(\bar{m}_i-1)P \longrightarrow L(\bar{m}_iP) \longrightarrow L(\bar{m}_iP)/L((\bar{m}_i-1)P) \longrightarrow 0$$

Since the space $L(\bar{m}_iP)/L((\bar{m}_i-1)P)$ is one dimensional the class \bar{f}_i can be replaced by $\lambda\bar{f}_i$ for some $\lambda \in k^*$. In Lemma 12 we will explain further how the change of the semigroup generators gives rise to coboundaries. It turns out that changing \bar{f}_i to $\lambda\bar{f}_i$ for $\lambda \in k^*$ changes the additive polynomial P_i to $\lambda^{p^{n_i}-1}P_i$ and the cocycle \bar{C}_i to $\lambda\bar{C}_i$. This forces us to consider the projective space to the cohomology groups in order to obtain an

independent of the generators description, see Corollary 3. The definition of the additive polynomials P_i and the compatibility condition is given in Theorems 15 and 17.

The statement of the above theorem requires the selection of elements $\bar{f}_0, \dots, \bar{f}_s$ of corresponding pole orders \bar{m}_i generating the Weierstrass semigroup at the unique ramification point P . The following corollary gives a description independent of such a selection.

Corollary 3. *The HKG-cover X can be completely described in terms of classes*

$$[\bar{C}_i] \in \mathbb{P}H^1(\text{Gal}(F_{i+1}/F_1), L(\bar{m}_i P))$$

satisfying the compatibility conditions

$$[P_i]([\bar{C}_i]) = 0 \in \mathbb{P}H^1(\text{Gal}(F_{i+1}/F_1), L(\bar{m}_i P)),$$

where $[P_i]$ is the map on projective spaces induced by the additive polynomials P_i . Once a selection of elements $\bar{f}_0, \dots, \bar{f}_s$ is made all actions can be expressed in terms of this expression.

We will now indicate how we can construct the HKG-cover from the information of the compatible classes $\bar{C}_i \in H^1(G, k_{\mathbf{n}, m_i}[\bar{f}_0, \bar{f}_1, \dots, \bar{f}_{i-1}])$. We argued that the additive polynomials can be constructed from the classes \bar{C}_i . The compatibility equation $P_i(\bar{C}_i) = 0$ gives us that the cocycle representative \bar{C}_i is a coboundary, that is, there is an element $D_i \in k_{\mathbf{n}, m_i}[\bar{f}_0, \bar{f}_1, \dots, \bar{f}_{i-1}]$ such that $P_i(\bar{C}_i(\sigma)) = (\sigma - 1)D_i$ for all $\sigma \in G$. But then the element \bar{f}_i satisfies the generalized Artin-Schreier extension

$$P_i(\bar{f}_i) = D_i, \tag{2}$$

see section 2.6. This essentially means that we can construct the HKG-cover step by step, adding in each step the generator \bar{f}_i satisfying eq. (2). \square

In fact the above theorem states that all the information for the HKG-cover is inside the sequence of compatible cohomology classes. This result is similar to the cohomological interpretation of Kummer and Artin-Schreier-Witt extensions, see [10, 8.9-8.11], [17, chap. VI, sec. 1-2]. Of course Kummer and Artin-Schreier-Witt extensions are abelian, while the HKG-extensions are solvable. This fits well with the Shafarevich philosophy as expressed in [22].

As an application of the above result we give the following description of finite p -subgroups of the Nottingham group:

Theorem 4. *Let G be a finite p -subgroup of the Nottingham group. There are elements $\bar{f}_0, \dots, \bar{f}_s \in k[[t]]$ acted on by G in terms of the cohomology classes \bar{C}_i as described in Theorem 2, and a local uniformizer $t' = (\bar{f}_s)^{1/m}$ so that*

$$\sigma(t') = t'(1 + \bar{C}_s(\sigma)(t')^m)^{-1/m} \in k[[t']] = k[[t]], \text{ for every } \sigma \in G.$$

Proof. See theorem (17) and the subsequent discussion. \square

The above theorem is applied as follows: We start from a local action of a finite p -group G on $k[[t]]$ and we construct an HKG-cover from it. From this HKG-cover we obtain the series of generators $\bar{f}_0, \dots, \bar{f}_s \in k[[t]][t^{-1}]$ and we define the cohomology class \bar{C}_s , which in turn gives an explicit form of the action of G on $k[[t']]$. Essentially we describe the conjugation class of $G \subset \text{Aut}(k[[t]])$, since the group acting on $k[[t]]$ by

$$\sigma(t) = t(1 + \bar{C}_s(\sigma)t^m)^{-1/m},$$

is conjugate to our original action.

We now describe the structure of this article. In section 2 we will introduce the representation and ramification filtration and their relation and we will also give a description of the Riemann–Roch space $L(m_i P)$ as polynomials of bounded degrees. Then we give a cohomological interpretation of the action of the group G and we also see how the polynomials of each successive abelian extension can be recovered from this construction. In section 3 we apply these tools in the problem of determining finite subgroups of the Nottingham group and in particular we give explicit forms of elements of order p^h . In the cyclic group case the cohomology group can be expressed in terms of coinvariants of group action, see Proposition 25. It seems that in recent years interest on this problem has grown, see [14], [1], [16], [24].

Acknowledgment: The authors would like to thank the anonymous referee for her/his comments on the improvement of the article. This research is co-financed by Greece and the European Union (European Social Fund - ESF) through the Operational Programme “Human Resources Development, Education and Lifelong Learning” in the context of the project “Strengthening Human Resources Research Potential via Doctorate Research” (MIS-5000432), implemented by the State Scholarships Foundation (IKY, 12333).

2. Generalities on HKG-covers

2.1. Ramification filtration

Let $X \rightarrow \mathbb{P}^1$ be a HKG-cover, that is Galois cover with Galois group a p -group G fully ramified over one point $P \in \mathbb{P}^1$. In the associated HKG-curve X , the group G will coincide with the inertia group of the curve at the unique ramified point, $G_T(P) = \{\sigma \in G(P) : v_p(\sigma(t) - t) \geq 1\}$, where t is a local uniformizer at P and v_P is the corresponding valuation. For more information on ramification filtration the reader is referred to [21]. We define $G_i(P)$ to be the subgroup of $\sigma \in G(P)$ that acts trivially on \mathcal{O}_P/m_P^{i+1} , obtaining the following filtration;

$$G_T(P) = G_0(P) = G_1(P) \supseteq G_2(P) \supseteq \dots \supseteq \{1\}. \tag{3}$$

Let us call an integer i a *jump of the ramification filtration* if $G_i(P) \not\supseteq G_{i+1}(P)$ and denote by

$$G_0(P) = G_1(P) = \dots = G_{b_1}(P) \not\supseteq G_{b_1+1}(P) = \dots = G_{b_2}(P) \not\supseteq \dots \not\supseteq G_{b_\mu}(P) \not\supseteq \{1\} \tag{4}$$

the filtration of the jumps, assuming that there are exactly μ jumps.

2.2. The Weierstrass semigroup

The Weierstrass semigroup $H(P)$ is the semigroup consisting of all pole numbers, i.e. $m \in \mathbb{N}$, such that there is a function f on X with $(f)_\infty = mP$. For the Weierstrass semigroup $H(P)$ we consider all pole numbers m_i forming an increasing sequence

$$0 = m_0 < \dots < m_{r-1} < m_r,$$

where m_r is the first pole number not divisible by the characteristic. If $g \geq 2$ and $p \geq 5$ we can prove that $m_r \leq 2g - 1$, see [15, lemma 2.1].

Let $F = k(X)$ be the function field of the HKG-curve X . For every m_i , $0 \leq i \leq r$ in the Weierstrass semigroup we denote by $f_i \in F$ an element of F that has a unique pole at P of order m_i , i.e. $(f_i)_\infty = m_iP$. For each $i \in \{0, \dots, r\}$ the set $\{f_0, \dots, f_i\}$ forms a basis for the Riemann-Roch space $L(m_iP)$. The spaces

$$k = L(m_0P) \subsetneq L(m_1P) \subsetneq \dots \subsetneq L(m_rP) \tag{5}$$

give rise to a natural flag of vector spaces corresponding to the Weierstrass semigroup. Notice that if μ is a pole number in $H(P)$ we have $\mu = m_{\dim L(\mu P) - 1}$.

2.3. Representation filtration

For each $0 \leq i \leq r$ we consider the representations

$$\rho_i : G_1(P) \rightarrow \text{GL}(L(m_iP)) \tag{6}$$

which give rise to a decreasing sequence of groups

$$G_1(P) = \ker \rho_0 \supseteq \ker \rho_1 \supseteq \ker \rho_2 \supseteq \dots \supseteq \ker \rho_r = \{1\}. \tag{7}$$

Recall that r is the index of m_r , the first pole number not divisible by p . In [15] the first author proved that ρ_r is faithful hence the last equality $\ker \rho_r = \{1\}$.

We shall call the last filtration the *representation filtration of G* .

Definition 5. An index i is called a jump of the representation filtration if and only if $\ker \rho_i \not\supseteq \ker \rho_{i+1}$.

We will denote the jumps in the representation filtration by

$$c_1 < c_2 < \dots < c_{n-1} < c_n = r - 1,$$

that is

$$\ker \rho_{c_i} > \ker \rho_{c_{i+1}}.$$

The last equality $c_n = r - 1$ is proved in [12, rem. 9]. We have now a sequence of decreasing groups

$$G_1(P) = \ker \rho_0 = \dots = \ker \rho_{c_1} > \dots \ker \rho_{c_{n-1}} > \ker \rho_{c_n} > \{1\} \tag{8}$$

which gives rise to the following sequence of extensions;

$$F^{G_1(P)} = F^{\text{Ker} \rho_{c_1}} \subset F^{\text{Ker} \rho_{c_2}} \subset \dots \subset F^{\text{Ker} \rho_{c_n}} \subset F. \tag{9}$$

2.4. A relation of the two filtrations in the case of HKG-covers

In [12] Karanikolopoulos and the first author related the filtrations defined in eq. (4), (8) and the Weierstrass semigroup in the following way;

Theorem 6. We distinguish the following two cases:

- If $G_1(P) > G_2(P)$ then the Weierstrass semigroup is minimally generated by $m_{c_i+1} = p^{h_i} \lambda_i$, $(\lambda_i, p) = 1$, $1 \leq i \leq n$ and the cover $F/F^{G_2(P)}$ is an HKG-cover as well. In this case $|G_2(P)| = m_1$.
- If $G_1(P) = G_2(P)$ then the Weierstrass semigroup is minimally generated by $m_{c_i+1} = p^{h_i} \lambda_i$, $(\lambda, p) = 1$, $1 \leq i \leq n$ and by an extra generator $p^h = |G_1(P)|$, which is different by all m_{c_i+1} for all $1 \leq i \leq n$.

Epecially when $X \rightarrow \mathbb{P}^1$ is an HKG-cover, the number of ramification jumps μ coincides with the number of representation jumps n , i.e. $n = \mu$. The integers λ_i , which appear as factors of the integers m_{c_i+1} , $1 \leq i \leq n$ are the jumps of the ramification filtration, i.e. $\lambda_i = b_i$ and $G_{b_i} = \text{Ker} \rho_{c_i}$ for $2 \leq i \leq n$. Summing up we have the following options for the ramification filtration

$$G_1(P) = \dots = G_{\lambda_1} \not\supseteq G_{\lambda_1+1} = \dots = G_{\lambda_2} \not\supseteq G_{\lambda_2+1} = \dots = G_{\lambda_n} \not\supseteq \{1\}$$

or

$$G_1(P) > G_2(P) = \dots = G_{\lambda_1} \not\supseteq G_{\lambda_1+1} = \dots = G_{\lambda_2} \not\supseteq G_{\lambda_2+1} = \dots = G_{\lambda_n} \not\supseteq \{1\}$$

Proof. See [12, th. 13,th. 14]. \square

Remark 7. The reader should notice that $\text{Ker}\rho_{c_1} = \text{Ker}\rho_0 = G_1(P) = G_{b_1}(P)$ by definition, hence $G_{b_i} = \text{Ker}\rho_{c_i}$ for every $i \in \{1, \dots, n = \mu\}$.

Theorem 6 allows us to use the well known fact that the quotients $G_{b_i}/G_{b_{i+1}}$ are elementary abelian p -groups, hence the quotients $\text{Ker}\rho_{c_i}/\text{Ker}\rho_{c_{i+1}}$ are elementary abelian too, and the corresponding sequence of fields in (9) is in fact, a sequence of elementary abelian p -group extensions.

In [12, prop. 27] the first author and S. Karanikolopoulos observed that for a $\sigma \in \text{Ker}\rho_{c_i} - \text{Ker}\rho_{c_{i+1}}$ the following hold;

$$\begin{aligned} \sigma(f_\nu) &= f_\nu \text{ for all } \nu \leq c_i \\ \sigma(f_{c_{i+1}}) &= f_{c_{i+1}} + C(\sigma) \text{ for some } C(\sigma) \in k^*. \end{aligned}$$

They also proved (prop. 20 & rem. 21) that for each $i \in \{1, \dots, n\}$ we have $F^{\text{ker } \rho_{c_{i+1}}} = F^{\text{ker } \rho_{c_i}}(f_{c_{i+1}})$.

In order to simplify notation we set $F_i := F^{\text{ker } \rho_{c_i}}$, $\bar{m}_i := m_{c_{i+1}}$ and $\bar{f}_i := f_{c_{i+1}}$, see also eq. (10).

Example 8. In the Artin-Schreier extension $F = k(x)(y)$ where $y^p - y = x^m$ only the place $P = \infty$ is ramified with the following ramification filtration:

$$\mathbb{Z}/p\mathbb{Z} = G_0 = \dots = G_m > \{1\},$$

i.e. the first and unique ramification jump is at m , see [23, prop. 3.7.8]. The representation filtration is given by

$$G_0 = \text{ker}\rho_0 = \dots = \text{ker}\rho_{m-1} > \{1\},$$

that is, the first representation jump is at $c_1 = m - 1$ and $\bar{f}_1 = f_{c_1+1} = y$, where $c_1 = m - 1$ and $c_1 + 1 = m$. Thus $F = F_2 = F_1(\bar{f}_1)$, and \bar{f}_0 is the generator x of the rational function field $k(x)$.

We will prove in section 2.6 the following

Proposition 9. For a given $m \in H(P)$, in the case of HKG-covers we have

$$L((m - 1)P) = k_{\mathbf{n},m}[\bar{f}_0, \bar{f}_1, \dots, \bar{f}_s],$$

where

$$k_{\mathbf{n},m}[\bar{f}_0, \bar{f}_1, \dots, \bar{f}_s] = \left\langle \begin{array}{l} \bar{f}_0^{a_0} \bar{f}_1^{a_1} \dots \bar{f}_s^{a_s} : 0 \leq a_i < p^{n_i} \text{ for all } 1 \leq i \leq s, \\ \text{and } \deg(\bar{f}_0^{a_0} \bar{f}_1^{a_1} \dots \bar{f}_s^{a_s}) = \sum_{\nu=0}^s a_\nu \bar{m}_\nu < m \end{array} \right\rangle_k. \quad (10)$$

In the above equation $\text{deg}(\bar{f}_i)$ is the pole order of \bar{f}_i at P . The integer s is determined uniquely; it is the greatest index of \bar{m}_i such that $\bar{m}_i < m$ holds. The quantity $\mathbf{n} = (n_1, \dots, n_s) \in \mathbb{N}^s$ depends on the ramification filtration, specifically n_i is the number of $\mathbb{Z}/p\mathbb{Z}$ components in each elementary abelian group G_i/G_{i+1} obtained by quotients of the lower ramification filtration.

2.5. Groups acting on flags

An automorphism of a curve act on all “invariants” of the curve including the Weierstrass semigroup of the unique ramified point. Usually this action on invariants provides useful information about the action. Unfortunately the action of the group G on the semigroup $H(P)$ is trivial. This is not the case when we move to the action on appropriate flags of vector spaces. More precisely we will consider flags of k -vector spaces

$$\bar{V} : k = V_0 \subsetneq V_1 \subsetneq \dots \subsetneq V_m \subsetneq \dots$$

where $V_i = L(iP)$. We will say that a group G is acting on a flag \bar{V} , if there is a homomorphism

$$\rho : G \rightarrow \text{Aut}(\bar{V}),$$

i.e. when $\rho(g)$ is an isomorphism such that $\rho(g)(V_i) = V_i$ for all V_i in the flag.

Remark 10. Since the representation ρ_r is faithful it makes sense to consider the representation not on the whole flag but only up to $L(m_rP)$. The natural isomorphisms on this truncated flag are given by invertible upper triangular matrices.

Recall that s is the the greatest index of \bar{m}_i such that $\bar{m}_i < m$. For every $1 \leq i \leq s$ and for every $1 \leq j \leq r$ we have that

$$\begin{aligned} \sigma(f_i) &= f_i + C_i(\sigma), \text{ where } C_i(\sigma) \in L((m_i - 1)P) \\ \sigma(\bar{f}_i) &= \bar{f}_i + \bar{C}_i(\sigma), \text{ where } \bar{C}_i(\sigma) \in L((\bar{m}_i - 1)P). \end{aligned}$$

Proposition 9, which will be proved in the next section, implies that if $\bar{f}_1, \dots, \bar{f}_s$ are fixed, then the values \bar{C}_i for $1 \leq i \leq s$ determine the action completely.

Also notice that for each $i \in \{1, \dots, r\}$, f_i is a polynomial expression of the $\bar{f}_1, \dots, \bar{f}_s$. By Proposition 9 we have $\bar{C}_i \in L((\bar{m}_i - 1)P) = k_{\mathbf{n}, \bar{m}_i}[\bar{f}_0, \dots, \bar{f}_{i-1}]$. The functions $\sigma \mapsto C_i(\sigma)$ and $\sigma \mapsto \bar{C}_i(\sigma)$ are cocycles, i.e.

$$\bar{C}_i(\sigma\tau) = \bar{C}_i(\sigma) + \sigma\bar{C}_i(\tau).$$

We plan to show that these cocycles define the action of G on X , and in particular the finite subgroup of $\text{Aut}(k[[t]])$.

Remark 11. The selection of the generators \bar{f}_i for $0 \leq i \leq s$ is not unique. Every element $a \in k_{\mathbf{n},m_i}[\bar{f}_0, \bar{f}_1, \dots, \bar{f}_{i-1}]$ gives rise to a new generator $\bar{f}_i + a$.

The new cocycle \bar{C}'_i which is defined in terms of the generator $\bar{f}_i + a$ is given by

$$\sigma(\bar{f}_i + a) = \sigma(\bar{f}_i) + \sigma(a) = \bar{f}_i + a + \bar{C}_i(\sigma) + \sigma(a) - a = \bar{f}_i + a + \bar{C}'_i(\sigma).$$

Therefore

$$\bar{C}'_i(\sigma) = \bar{C}_i(\sigma) + (\sigma - 1)a.$$

Also instead of selecting the generator \bar{f}_i , which has pole order \bar{m}_i at P we can select $\lambda\bar{f}_i$ for any $\lambda \in k^*$. This change leads to cocycle $\lambda\bar{C}_i$. Therefore selecting the generator amounts to giving an element in the projective space

$$\mathbb{P}H^1\left(\frac{G}{\ker \rho_{i-1}}, k_{\mathbf{n},m_i}[\bar{f}_0, \bar{f}_1, \dots, \bar{f}_{i-1}]\right)$$

This gives us the following

Lemma 12. *The cocycles \bar{C}_i, \bar{C}'_i corresponding to different generators \bar{f}_i, \bar{f}'_i with the same pole number \bar{m}_i , that is $\bar{f}'_i = \lambda\bar{f}_i + a, a \in k_{\mathbf{n},m_i}[\bar{f}_0, \bar{f}_1, \dots, \bar{f}_{i-1}]$ satisfy the relation*

$$\bar{C}'_i(\sigma) = \lambda\bar{C}_i(\sigma) + (\sigma - 1)\lambda a$$

and a generator free description of the action is determined by a series of classes \tilde{C}_i in

$$\begin{array}{ccc} H^1\left(\frac{G}{\ker \rho_{i-1}}, k_{\mathbf{n},m_i}[\bar{f}_0, \bar{f}_1, \dots, \bar{f}_{i-1}]\right) & \xrightarrow{\text{inf}} & H^1(G, k_{\mathbf{n},m_i}[\bar{f}_0, \bar{f}_1, \dots, \bar{f}_{i-1}]) \quad . \quad (11) \\ \downarrow & & \downarrow \\ \mathbb{P}H^1\left(\frac{G}{\ker \rho_{i-1}}, k_{\mathbf{n},m_i}[\bar{f}_0, \bar{f}_1, \dots, \bar{f}_{i-1}]\right) & \xrightarrow{\overline{\text{inf}}} & \mathbb{P}H^1(G, k_{\mathbf{n},m_i}[\bar{f}_0, \bar{f}_1, \dots, \bar{f}_{i-1}]) \end{array}$$

These cocycles satisfy certain conditions which will be given in eq. (15) and Theorem 17. The monomorphism inf is the inflation map in group cohomology, see [26, II.2-3, p. 64], while $\overline{\text{inf}}[C]$ of the projective class $[C]$ of the cocycle C is given by

$$\overline{\text{inf}}[C] = [\text{inf}(C)].$$

Remark 13. The vector space $k_{\mathbf{n},m_i}[\bar{f}_0, \bar{f}_1, \dots, \bar{f}_{i-1}]$ has as base the space of monomials $\bar{f}_0^{\nu_0} \bar{f}_1^{\nu_1} \dots \bar{f}_{i-1}^{\nu_{i-1}}$, of degree smaller than m , where $\nu_i < p^{n_i}$. The action on them can be described in terms of the binomial theorem, i.e.

$$\bar{f}_0^{\nu_0} \bar{f}_1^{\nu_1} \cdots \bar{f}_{i-1}^{\nu_{i-1}} \xrightarrow{\sigma} \bar{f}_0^{\nu_0} \sum_{\mu_1}^{\nu_1} \cdots \sum_{\mu_{i-1}}^{\nu_{i-1}} \binom{\mu_1}{\nu_1} \cdots \binom{\mu_{i-1}}{\nu_{i-1}} \bar{f}_1^{\mu_1} \cdots \bar{f}_{i-1}^{\mu_{i-1}} \bar{C}_1^{\nu_1 - \mu_1} \cdots \bar{C}_{i-1}^{\nu_{i-1} - \mu_{i-1}}. \tag{12}$$

2.6. Describing an HKG-cover as a sequence of Artin-Schreier extensions

It is known, see [7], that every elementary abelian field extension L/K , with Galois group $(\mathbb{Z}/p\mathbb{Z})^n$, is given as an Artin-Schreier extension of the form

$$L = K(y) : \quad y^{p^n} - y = b, \quad b \in K.$$

In our case, the elementary abelian field extension F_{i+1}/F_i can be generated by an element $y \in F_{i+1}$ but this element might not be the semigroup generator \bar{f}_i . We can give a description of the Artin-Schreier extension F_{i+1}/F_i using a monic polynomial

$$A_i(X) = X^{p^{n_i}} + a_{n_i-1}X^{p^{n_i-1}} + \cdots + a_1X^p + a_0X - D_i,$$

which can be computed in terms of the Moore determinant [8]. Notice that this polynomial is an additive polynomial minus a constant term. Let $\{\sigma_1, \dots, \sigma_{n_i}\}$ be a basis of the Galois group $\text{Gal}(F_{i+1}/F_i) \cong (\mathbb{Z}/p\mathbb{Z})^{n_i}$, seen as an \mathbb{F}_p -vector space, and let w_1, \dots, w_{n_i} be elements of k^* such that $\sigma_j(\bar{f}_i) = \bar{f}_i + w_j$. Let W be the \mathbb{F}_p -subspace of k spanned by the $w_j, j = 1, \dots, n_i$. We have $\dim_{\mathbb{F}_p} W = n_i$.

Let $P_i(X) = \prod_{a \in W} (X - a)$. Since every w_i is an element of k , $\text{Gal}(F_{i+1}/F_i)$ acts trivially on $P_i(X)$ and we consider the polynomial

$$A_i(X) := P_i(X) - P_i(\bar{f}_i).$$

Notice that, for a $\sigma \in \text{Gal}(F_{i+1}/F_i)$, we can write $\sigma = \sigma_1^{\nu_1} \circ \cdots \circ \sigma_{n_i}^{\nu_{n_i}}$ and

$$\sigma(\bar{f}_i + a) = \bar{f}_i + \nu_1 w_1 + \cdots + \nu_{n_i} w_{n_i} + a, \text{ for all } a \in W \subset k.$$

This means that $P_i(\bar{f}_i)$ is $\text{Gal}(F_{i+1}/F_i)$ invariant, i.e. belongs to F_i . Therefore, the polynomial $A_i(X)$ belongs to $F_i[X]$, is monic of degree $p^{n_i} = [F_{i+1} : F_i]$ and vanishes at \bar{f}_i hence it is the irreducible polynomial of \bar{f}_i over F_i . The polynomial $P_i(X)$ is given by

$$P_i(X) = \frac{\Delta(w_1, w_2, \dots, w_{n_i}, X)}{\Delta(w_1, w_2, \dots, w_{n_i})}, \tag{13}$$

where $\Delta(w_1, \dots, w_n)$ is the Moore determinant;

$$\Delta(w_1, \dots, w_n) = \det \begin{bmatrix} w_1 & w_2 & \cdots & w_n \\ w_1^p & w_2^p & \cdots & w_n^p \\ \vdots & \vdots & & \vdots \\ w_1^{p^{n_i-1}} & w_2^{p^{n_i-1}} & \cdots & w_n^{p^{n_i-1}} \end{bmatrix}.$$

It is an additive polynomial of the form

$$P_i(X) = X^{p^{n_i}} + a_{n_i-1}X^{p^{n_i-1}} + \cdots + a_1X^p + a_0X,$$

where $a_i \in k \subset F_i$. We have proved that the generator \bar{f}_i of the extension F_{i+1}/F_i satisfies an equation of the form

$$\bar{f}_i^{p^{n_i}} + a_{n_i-1}\bar{f}_i^{p^{n_i-1}} + \cdots + a_1\bar{f}_i^p + a_0\bar{f}_i = D_i, \tag{14}$$

for some $a_{n_i-1}, \dots, a_0 \in k, D_i = P_i(\bar{f}_i) \in F_i$.

Remark 14. Instead of \bar{f}_i we can use $\lambda\bar{f}_i$. The additive polynomial corresponding to $\lambda\bar{f}_i$ is equal to $\lambda^{p^{n_i-1}}P_i(X)$, where $P_i(X)$ is the additive polynomial corresponding to \bar{f}_i . Indeed, when we change \bar{f}_i to $\lambda\bar{f}_i$ the \mathbb{F}_p -vector space W is changed to $\lambda \cdot W$, that is the basis elements w_i are changed to λw_i . Hence, the Moore determinant in the numerator of eq. (13) defining $P_i(\lambda X)$ is multiplied by $\lambda^{1+p+\cdots+p^{n_i-1}}$ while the denominator is multiplied by $\lambda^{1+p+\cdots+p^{n_i-2}}$. Therefore $P_i(\lambda X) = \lambda^{p^{n_i-1}}P_i(X)$ follows.

We have the following:

Theorem 15. *The cocycles $\bar{C}_i \in H^1(\text{Gal}(F_{i+1}/F_1), k_{\mathbf{n}, \bar{m}_i}[\bar{f}_0, \bar{f}_1, \dots, \bar{f}_{i-1}])$, when restricted to the elementary abelian group $\text{Gal}(F_{i+1}/F_i) < \text{Gal}(F_{i+1}/F_1)$ describe fully the elementary abelian extension F_{i+1}/F_i given by the equation*

$$P_i(Y) = D_i.$$

Moreover the element $D_i = P_i(\bar{f}_i)$ is described by the additive polynomial $P_i(Y)$ and by the selection of \bar{f}_i . A different selection of \bar{f}'_i , i.e. $\bar{f}'_i = \lambda\bar{f}_i + a$, for some $a \in k_{\mathbf{n}, \bar{m}_i}[\bar{f}_0, \bar{f}_1, \dots, \bar{f}_{i-1}]$, $\lambda \in k^*$ gives rise to the same polynomial $\lambda^{p^{n_i-1}}P_i$ and to a different D'_i given by $D'_i = \lambda^{p^{n_i-1}}D_i + \lambda^{p^{n_i-1}}P_i(a)$. The two extensions $F_i(\bar{f}_i)$ and $F_i(\bar{f}'_i)$ are equal.

Proof. The only part we didn't prove is the dependence of the additive polynomial to the selection of the generator \bar{f}_i . We have seen that changing \bar{f}_i adds a coboundary to \bar{C}_i .

But when σ belongs to $\text{Gal}(F_{i+1}/F_i)$, $\bar{C}_i(\sigma)$ belongs to k , and k admits the trivial action. Therefore, all coboundaries are zero and the result follows by Lemma 12. \square

The additive polynomial $P_i(Y)$, which depends on the values of $\bar{C}_i(\sigma)$ with $\sigma \in \text{Gal}(F_{i+1}/F_i)$ gives also compatibility conditions for the cocycle \bar{C}_i on all elements of $\text{Gal}(F_{i+1}/F_1)$. Namely, by application of σ to eq. (14) we obtain the following

$$\boxed{P_i(\bar{C}_i(\sigma)) = (\sigma - 1)D_i \text{ for all } \sigma \in \text{Gal}(F_i/F_1).} \tag{15}$$

So if σ keeps D_i invariant, for instance when $\sigma \in \text{Gal}(F/F_i)$, then $\bar{C}_i(\sigma) \in \mathbb{F}_{p^n} \subset k$.

Equation (15) is essentially a relation among the cocycles $\bar{C}_i(\sigma)$ and $\bar{C}_\nu(\sigma)$ for $\nu < i$. Indeed, the element $D_i \in k_{\mathbf{n},m_i}[\bar{f}_0, \bar{f}_1, \dots, \bar{f}_{i-1}]$ is a polynomial expression on the elements $\bar{f}_0, \dots, \bar{f}_{i-1}$, and the action is given in terms of the elements $\bar{C}_\nu(\sigma)$ for $\nu < i$ and \bar{f}_i as given in eq. (12).

Lemma 16. *An additive polynomial $P \in k[Y]$ defines a map*

$$H^1(G, k_{\mathbf{n},m_i}[\bar{f}_0, \bar{f}_1, \dots, \bar{f}_{i-1}]) \longrightarrow H^1(G, k_{\mathbf{n},m_i}[\bar{f}_0, \bar{f}_1, \dots, \bar{f}_{i-1}]) \tag{16}$$

$$d \longmapsto P(d).$$

Proof. Notice first that elements in the space $L(\nu P)$, for some $\nu \in \mathbb{N}$, can be multiplied as elements of the ring \mathbf{A} , so a polynomial expression $P(d)$ of a cocycle d makes sense. One has to be careful since the multiplication of two elements in $L(\nu P)$, is not in general an element of $L(\nu P)$, since it can have a pole order greater than ν . Therefore the value $P(d)$ is an element in $L(\mu P)$ for some $\mu \in \mathbb{N}$ for big enough μ . However notice that eq. (15) implies that $P(\bar{C}_i(\sigma)) \in k_{\mathbf{n},\bar{m}_i}[\bar{f}_0, \bar{f}_1, \dots, \bar{f}_{i-1}]$ so that $P_i(\bar{C}_i) \in H^1(G, k_{\mathbf{n},\bar{m}_i}[\bar{f}_0, \bar{f}_1, \dots, \bar{f}_{i-1}])$.

Finally observe now that if d is a cocycle, i.e. $d(\sigma\tau) = d(\sigma) + \sigma d(\tau)$, then

$$P(d(\sigma\tau)) = P(d(\sigma) + \sigma d(\tau)) = P(d(\sigma)) + P(\sigma d(\tau)) = P(d(\sigma)) + \sigma P(d(\tau)).$$

On the other hand if $d(\sigma) = (\sigma - 1)b$ is a coboundary, then

$$P(d(\sigma)) = P((\sigma - 1)b) = (\sigma - 1)P(b)$$

is a coboundary as well. \square

This allows us to give a cohomological interpretation of eq. (15):

Theorem 17. *The cocycles \bar{C}_i given in eq. (11) are in the kernel of the map P_i acting on cohomology as defined in Lemma 16. The corresponding element D_i is then the element expressing $P(C_i)$ as a coboundary. The elementary abelian extension is determined by a series of cocycles $\bar{C}_i \in H^1(\text{Gal}(F_{i+1}/F_i), k_{\mathbf{n},\bar{m}_i}[\bar{f}_0, \bar{f}_1, \dots, \bar{f}_{i-1}])$, which define a series of additive polynomials P_i and extend to cocycles in $\bar{C}_i \in H^1(\text{Gal}(F_{i+1}/F_1), k_{\mathbf{n},\bar{m}_i}[\bar{f}_0, \bar{f}_1, \dots, \bar{f}_{i-1}])$ so that each \bar{C}_i is in the kernel of P_i .*

Remark 18. In Remark 14 we have seen that by changing the generator \bar{f}_0 to $\lambda\bar{f}_0$ the additive polynomial is changed from P_i to $\lambda^{p^{n_i}-1} P_i$. The corresponding map

$$\mathbb{P}H^1(G, k_{\mathbf{n},m_i}[\bar{f}_0, \bar{f}_1, \dots, \bar{f}_{i-1}]) \longrightarrow \mathbb{P}H^1(G, k_{\mathbf{n},m_i}[\bar{f}_0, \bar{f}_1, \dots, \bar{f}_{i-1}])$$

is not affected.

3. Nottingham groups

An automorphism σ of the complete local algebra $k[[t]]$ is determined by the image $\sigma(t)$ of t , where $\sigma(t) = \sum_{i=1}^{\infty} a_i t^i \in k[[t]]$. We consider the subgroup of normalised automorphisms that is, automorphisms of the form

$$\sigma : t \mapsto t + \sum_{i=2}^{\infty} a_i t^i.$$

S. Jennings [11] proved that the set of latter automorphisms forms a group under substitution, denoted by $\mathcal{N}(k)$, called the Nottingham group. This group has many interesting properties, for instance R. Camina proved in [2] that every countably based pro- p group can be embedded, as a closed subgroup, in the Nottingham group. We refer the reader to [3] for more information regarding $\mathcal{N}(k)$. We would like to provide an explicit way to describe the elements of $\mathcal{N}(k)$. It is proved in [14, prop. 1.2] and [16, sec. 4, th. 2.2], that each automorphism of order p is conjugate to the automorphism given by

$$t \mapsto t(1 + ct^m)^{-1/m} = t \left(\sum_{\nu=0}^{\infty} \binom{-1/m}{\nu} c^\nu t^{\nu m} \right) \tag{17}$$

for some $c \in k^\times$ and some positive integer m prime to p .

In [1] F. Bleher, T. Chinburg, B. Poonen and P. Symonds, studied the extension $L/k(t)$, where $L := k(\{\sigma(t) : \sigma \in G\})$, where G is a finite subgroup of $\text{Aut}k[[t]]$. Notice here that each automorphism of order p^n is conjugate to $t \mapsto \sigma(t)$, where $\sigma(t) \in k[[t]]$ is algebraic over $k(t)$. Also in [1] the notion of almost rational automorphism is defined: an automorphism $\sigma \in \text{Aut}(k[[t]])$ is called almost rational if the extension $L/k(t)$ is Artin-Schreier.

The rational function field $k(t)$, despite its simple form, is not natural with respect to the group G acting on the HKG-cover. For example the determination of the algebraic extension $L/k(t)$ and the group of the normal closure seems very difficult.

Here we plan to give another generalization, by using the fact that the “natural” rational function field with respect to the Katz-Gabber cover is X^{G_1} and not $k(t)$.

In [15, p. 473] the first author proposed the following explicit form for an automorphism of an HKG-cover of order p^n ;

$$\sigma(t) = t \left(1 + \sum_{i=1}^r c_i(\sigma) u_i t^{m-m_i} \right)^{-1/m},$$

where m is the first pole number which is not divisible by the characteristic p , u_i/t^{m_i} for $1 \leq i \leq r$ are functions in $L(mP)$ (u_i is a unit) and $1/t^m$ is the function corresponding to m (t being the local uniformizer). In the latter function the unit is absorbed by Hensel’s lemma.

3.1. A canonical selection of uniformizer

In an attempt to describe in explicit form automorphisms of $k[[t]]$ let us quote here some results from [15]. We will work with the corresponding HKG-cover $X \xrightarrow{G} \mathbb{P}^1$ corresponding to a finite subgroup $G \subset \text{Aut}(k[[t]])$. Again let m_r denote the first pole number not divisible by the characteristic and $f_i, i = 1, \dots, \dim L(m_r P) = r$ a basis for the space $L(m_r P)$, such that

$$(f_i)_\infty = m_i. \tag{18}$$

As we have seen this basis is not unique but eq. (18) implies that if the element f_i is selected, then $f'_i = \lambda_i f_i + a_i$, where $a_i \in L((m_i - 1)P)$ is also a basis element of valuation m_r .

This means that the base change we will consider, corresponds to invertible upper triangular matrices, i.e. to linear maps which keep the flag of the vector spaces $L(m_i P)$.

Recall that $m = m_r$ is the first pole number not divisible by p . Let us focus on the element f_r . This element is of the form $f_r = u_m/t^m$, where u_m is a unit. Since $(m, p) = 1$ we know by Hensel’s lemma that u_m is an m -th power so by a change of uniformizer we can assume that $f_r = 1/t^m$. When changing from a uniformizer t to a uniformizer $t' = \phi(t) = tu(t)$ ($u(t)$ is a unit in $k[[t]]$), the automorphism $\sigma \in k[[t]]$ expressed as an element in $k[[t']]$ is a conjugate of the initial automorphism, i.e. $\phi\sigma\phi^{-1}$. By selecting the canonical uniformizer with respect to f_r we see that the expression of an arbitrary σ can take a simpler representation after conjugation. Also this result is in accordance with (and can be seen as a generalization of) the result of Klopsch and Lubin, [14], [16]. The selection of uniformizer $t = t_{f_r}$ is unique once f_r is selected.

Definition 19. We will call the uniformizer $t_{f_r} = f_r^{-1/m}$ the *canonical uniformizer* corresponding to f_r .

What happens if we change the function f_r to $f'_r = f_r + a$, where $a \in L((m - 1)P)$? Then $a = u/t^\mu$, with $0 \leq \mu < m$ and in this case the new uniformizer is given by

$$t_{f'_r} = \left(f_r + \frac{u}{t^\mu}\right)^{-1/m} = t(1 + ut^{m-\mu})^{-1/m} = t(1 + at^m)^{-1/m}.$$

Keep in mind that the set of uniformizers for the local ring $k[[t]]$ equals to $tu(t)$, where u is a unit of the ring $k[[t]]$.

Let $\bar{m}_1, \dots, \bar{m}_s$ be the generators of the Weierstrass semigroup $H(P)$. These elements correspond to a successive sequence of function fields $F_i = F_{i-1}(\bar{f}_{i-1})$ so that $v(\bar{f}_{i-1}) = p^{|\text{Gal}(F/F_i)|} \lambda_{h-1} = \bar{m}_i$. It is not clear that $\bar{m}_i \geq \bar{m}_j$ for $j < i$. However if for some j we have $\bar{m}_j < \bar{m}_i$ for some $i < j$ then

$$\sigma(\bar{f}_j) = \sigma(\bar{f}_j) + \bar{C}_j(\sigma), \text{ where } \bar{C}_j \in k[\bar{f}_0, \dots, \widehat{\bar{f}_i}, \dots, \bar{f}_{j-1}],$$

that is, \bar{f}_i does not appear in any term of the polynomial expression of $\bar{C}_j(\sigma)$, for all $\sigma \in G$. This means that we can generate an HKG-cover with corresponding function field generated by fewer elements than the initial one.

If we assume that among all HKG-covers which correspond to a local action of G on $k[[t]]$ we select one whose function field is minimally generated then $\bar{m}_1 < \bar{m}_2 < \dots < \bar{m}_s$.

Lemma 20. *Let $m = m_r$ be the first pole number not divisible by the characteristic p . Then $m = \bar{m}_s$, that is the pole number corresponding to the last generator \bar{f}_s .*

Proof. It is clear that not all pole numbers are divisible by p since $m \in H(P)$, $p \nmid m$. So at least one generator must be prime to p . On the other hand $F_i = F_{i-1}(\bar{f}_{i-1})$, thus the pole numbers \bar{m}_i of elements \bar{f}_i for $i < s$ are divisible by p , see also [12, eq. (6)]. Therefore only the last generator can be not divisible by p . \square

Theorem 21. *Let $\bar{C}_s \in H^1(G, k_{\mathbf{n},m}[\bar{f}_0, \bar{f}_1, \dots, \bar{f}_{s-1}])$ be the cocycle corresponding to $m = m_s$, where m is the first pole number not divisible by p , see Lemma 20. We choose as uniformizer the canonical uniformizer $t = \bar{f}_s^{-1/m}$. We define the representation:*

$$\begin{aligned} \Phi : G &\longrightarrow \text{Aut}(k[[t]]) \\ \sigma &\longmapsto \left(t \mapsto t(1 + \bar{C}_s(\sigma)t^m)^{-1/m} \right). \end{aligned} \tag{19}$$

The expression $1 + \bar{C}_s(\sigma)t^m)^{-1/m}$ can be expanded as a powerseries using the binomial theorem and determines uniquely an automorphisms of $k[[t]]$. We have that for all $\sigma, \tau \in G$

$$\Phi(\tau\sigma) = \Phi(\sigma)\Phi(\tau).$$

Furthermore Φ is a monomorphism.

Proof. We begin by noticing that $\sigma(\bar{f}_s) = \bar{f}_s + \bar{C}_s(\sigma)$ and we can select t so that $t^{-m} = \bar{f}_s$. Using the above expression we can determine the value of $\sigma(t)$ using

$$\frac{1}{\sigma(t)^m} = \frac{1}{t^m} + \bar{C}_s(\sigma),$$

see also [15, eq. 4]. In this way σ coincides with the image of $\Phi(\sigma) \in \text{Aut}(k[[t]])$ in eq. (19).

Recall that $\sigma \in G$ acts on the elements $\bar{f}_0, \dots, \bar{f}_{s-1}$ by definition in terms of the cocycles $\bar{C}_i(\sigma)$. This was defined to be a left action. Also this action is by construction assumed to be compatible with the action of G on $k[[t]]$ in the sense that when we see the elements \bar{f}_i as elements in $k[[t]][t^{-1}]$, then $\sigma(\bar{f}_i) = \Phi(\sigma)(\bar{f}_i)$, that is the action of σ on \bar{f}_i as elements in $k_{\mathbf{n},m_{i+1}}[\bar{f}_0, \bar{f}_1, \dots, \bar{f}_{s-1}]$ coincides with the action of σ on f_i seen as an element in the quotient field of $k[[t]]$. In other words we have

$$\sigma(f_i(t)) = f_i(\sigma(t)) = f_i(t) + C_i(\sigma).$$

We will prove first that this is a homomorphism i.e.

$$t(1 + \bar{C}_s(\tau\sigma)t^m)^{-1/m} = t(1 + \bar{C}_s(\sigma)t^m)^{-1/m} \circ t(1 + \bar{C}_s(\tau)t^m)^{-1/m}, \tag{20}$$

where \circ denotes the composition of two powerseries. The right hand side of the above equation equals

$$t(1 + \bar{C}_s(\tau)t^m)^{\frac{-1}{m}} \left(1 + \frac{\tau(\bar{C}_s(\sigma))t^m}{1 + \bar{C}_s(\tau)t^m} \right)^{\frac{-1}{m}} = t(1 + (\bar{C}_s(\tau) + \tau\bar{C}_s(\sigma))t^m)^{-1/m}$$

so eq. (20) holds by the cocycle condition for \bar{C}_s .

The kernel of the homomorphism Φ , consists of all elements $\sigma \in G$ such that $\bar{C}_s(\sigma) = 0$. But if $\bar{C}_s(\sigma) = 0$ then $\sigma(t) = t$ and σ is the identity. \square

Remark 22. The above construction behaves well when we substitute f_m with $f'_m = f_m + a$. In any case the representation given in eq. (19) is given in terms of the canonical uniformizer t_{f_r} corresponding to the element $\bar{f}_s = f_r$ which gives rise to the cocycle \bar{C}_s .

Remark 23. Equation (19) implies that the knowledge of the cocycle \bar{C}_s implies the knowledge of $\sigma(t)$, which in turn gives us how σ acts on all other elements \bar{f}_i for all $0 \leq i \leq s - 1$. This seems to imply that \bar{C}_s can determine all other cocycles \bar{C}_ν for all $1 \leq \nu \leq s - 1$. This is not entirely correct. Indeed, \bar{C}_s is a cocycle with values on the G -module $k_{\mathbf{n}, \bar{m}_s}[\bar{f}_0, \bar{f}_1, \dots, \bar{f}_{s-1}]$, therefore the action of G on \bar{f}_i for $0 \leq i \leq s - 1$ is assumed to be known and is part of the definition of the cocycle \bar{C}_s . This means that \bar{C}_i are assumed to be known and part of the definition of \bar{C}_s .

Proposition 24. *If $\sigma \in G$, $\sigma \neq 1$, then*

$$v_P(\sigma(t) - t) = m - v_P(\bar{C}_s(\sigma)) + 1 = I(\sigma),$$

where $-I(\sigma)$ is the Artin character since k is algebraically closed, see [21, VI.2]. Therefore $\sigma \in G_{I(\sigma)} - G_{I(\sigma)+1}$.

Proof. The valuation of $\sigma(t) - t$ comes from the binomial expansion of eq. (19). The rest is the definition of the ramification group. \square

3.2. Application: elements of order \mathbf{p}^h in the Nottingham group

3.2.1. On the form of elements of order p

It is known that every element of order p in $\text{Aut}(k[[t]])$ is conjugate to the automorphism

$$t \mapsto t(1 + ct^m)^{-1/m}, \quad \text{where } c \in k,$$

for some m prime to p , see [14, prop. 1.2] and [16, th. 2.2].

We can obtain this result using Theorem 21. Let σ be an automorphism of $k[[t]]$ of order p . Let $X \rightarrow \mathbb{P}^1$ be the corresponding HKG-cover. The sequence of higher ramification groups equals $\langle \sigma \rangle = G_0 = G_1 = \dots = G_m > \{1\}$, i.e. there is only one jump in the ramification filtration. If $m = 1$ then $G_i(P) = \{1\}$ for $i \geq 2$ and in this case the genus $g_X = 0$. This is a trivial case so we can assume that $m > 1$. From Theorem 6 we know that the Weierstrass semigroup is generated by $p = |G_1(P)|$ and m_r . If m_i is a pole number less than m_r then m_i is a multiple of p , hence the corresponding elements f_i with pole order m_i at P will be powers of f_0 where $(f_0)_\infty = pP$.

Since the ramification filtration jumps only once, the same holds for the representation filtration, i.e.

$$G_1(P) = \text{Ker} \rho_{c_1} > \{1\}$$

So if σ is not the identity then by [12, prop.27] we have that

$$\begin{aligned} \sigma(f_0^i) &= f_0^i \text{ for } i = 0, 1, \dots, \lfloor m_r/p \rfloor \text{ and} \\ \sigma(f_{c_1+1}) &= \sigma(f_r) = f_r + C(\sigma) \text{ where } C(\sigma) \in k^\times. \end{aligned}$$

Compare also with the computation of Proposition 24. To obtain the result we notice the following; changing the local uniformizer to a canonical one imposes the substitution of σ by a conjugate which, by Theorem 21, maps t to the desired form.

3.2.2. Application to the case of cyclic groups

Let us now consider an element σ of order p^h . As before the cyclic group

$$G_0(P) = G_1(P) = \dots = G_{b_1}(P) \not\supseteq G_{b_1+1}(P) = \dots = G_{b_2}(P) \not\supseteq \dots \not\supseteq G_{b_\mu}(P) \not\supseteq \{1\}$$

Since a cyclic group has only cyclic subgroups and all quotients of cyclic groups are cyclic, while $G_{b_i}/G_{b_{i+1}}$ is elementary abelian, we see that the number of gaps μ is equal to h and p^{h-i} is the exact power of p dividing each \bar{m}_i .

Observe that all intermediate elementary abelian extensions $F_{i+1}/F_i = F_i(\bar{f}_i)/F_i$ are cyclic. The additive polynomial describing the extension $F_i(\bar{f}_i)/F_i$ is given by

$$Y^p - \bar{C}_i^{p-1}Y = \bar{f}_i^p - \bar{C}_i^{p-1}\bar{f}_i,$$

by computation of the Moore determinant $\det \begin{pmatrix} C_i & Y \\ \bar{C}_i^p & Y^p \end{pmatrix}$, where \bar{C}_i is computed at a generator σ^{p^i} of the cyclic group $\text{Gal}(F_{i+1}/F_i) = G_{b_{i+1}}/G_{b_i}$, (i.e. $\sigma^{p^i}(\bar{f}_i) = \bar{f}_i + \bar{C}_i(\sigma^{p^i})$). Since $\bar{C}_i \in k$, if we rescale \bar{f}_i by \bar{f}_i/C_i , we can assume without loss of generality that the equation is an Artin-Schreier one:

$$Y^p - Y = \bar{f}_i^p - \bar{f}_i = D_i, \text{ where } D_i \in F_i.$$

Let g be an automorphism of the HKG-cover X . Since $g(\bar{f}_\nu) = \bar{f}_\nu + \bar{c}_\nu(g)$ and $\bar{c}_\nu(g) \in F_{\nu-1}$, the automorphism g gives rise to an automorphism $g : F_\nu \rightarrow F_\nu$ for all ν . We have that

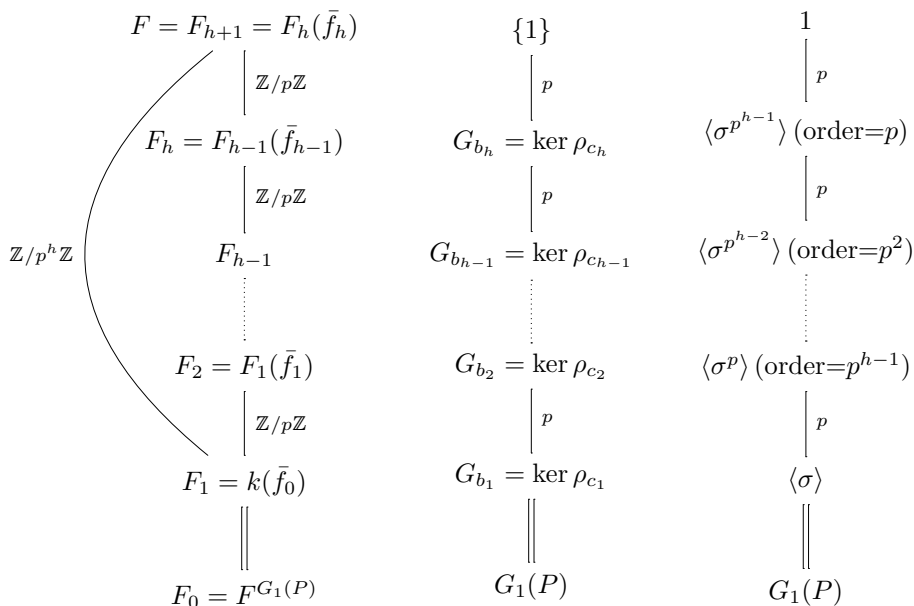
$$\bar{C}_i(g)^p - \bar{C}_i(g) = (g - 1)(\bar{f}_i^p - \bar{f}_i) = (g - 1)D_i. \tag{21}$$

Notice that eq. (21) has many solutions $\bar{C}_i(g)$ for a fixed g , which differ by an element $\bar{c}_i(\sigma)$ for some $\sigma \in \text{Gal}(F_{i+1}/F_i)$, since $(g\sigma - 1)(D_i) = (g - 1)(D_i)$.

The representation filtration has the following form (the filtrations are collectively depicted in the diagrams below)

$$F^{G_1(P)} = F_0 = F^{\ker \rho_0} \subset F_1 = F^{\ker \rho_1} \subset \dots \subset F_r = F^{\ker \rho_r} = F.$$

We have $p^{h-i} = |\ker \rho_{c_{i+1}}|$ for $0 \leq i \leq n - 1$ and $p^h = |G_1(P)|$. The generators of the Weierstrass semigroup are $p^h, p^{h-1}\lambda_1, \dots, p\lambda_{\mu-1}, \lambda_\mu$. We have the following tower of fields:



For every $g \in \text{Gal}(F/F_1)$ we have

$$g(\bar{f}_{r-1}) - \bar{f}_{r-1} = \bar{C}_{r-1}(g).$$

For a cyclic group $\mathbb{Z}/p^i\mathbb{Z}$ the cohomology is given by:

$$H^1(\mathbb{Z}/p^i\mathbb{Z}, A) = \frac{\{a \in A : N(a) = 0\}}{(\sigma_i - 1)A},$$

where σ_i is a generator of the cyclic group $\mathbb{Z}/p^i\mathbb{Z}$ and $N = 1 + \sigma + \dots + \sigma^{p^i-1}$ is the norm, see [25, th. 6.2.2, p. 168]. In view of Theorem 17 we will consider the groups $\text{Gal}(F_{i+1}/F_1)$, which are generated by the generator σ of the cyclic group $\text{Gal}(F_{h+1}/F_1)$ modulo the subgroup $\text{Gal}(F_{h+1}/F_{i+1})$. Thus in the group $\text{Gal}(F_{i+1}/F_1)$ the order of σ equals p^i .

Observe now that $\tau = \sigma^{p^{i-1}}$ acts trivially on $A = k_{\mathbf{n},\bar{m}_i}[\bar{f}_0, \bar{f}_1, \dots, \bar{f}_{i-1}]$. We now compute the norm for $\text{Gal}(F_{i+1}/F_1)$:

$$\begin{aligned} 1 + \sigma + \dots + \sigma^{p^i-1} &= \sum_{\nu=0}^{p^i-1} \sigma^\nu = \sum_{\pi=0}^{p-1} \sum_{v=0}^{p^{i-1}-1} \sigma^{\pi p^{i-1} + v} \\ &= \sum_{\pi=0}^{p-1} \tau^\pi \sum_{v=0}^{p^{i-1}-1} \sigma^v, \end{aligned}$$

where $\tau := \sigma^{p^{i-1}}$, and observe that the above equation restricted on A gives

$$1 + \sigma + \dots + \sigma^{p^i-1} = p \cdot \sum_{v=0}^{p^{i-1}-1} \sigma^v$$

which is zero on A . So we finally arrive at the computation:

$$H^1(\mathbb{Z}/p^i\mathbb{Z}, k_{\mathbf{n},\bar{m}_i}[\bar{f}_0, \bar{f}_1, \dots, \bar{f}_{i-1}]) = k_{\mathbf{n},\bar{m}_i}[\bar{f}_0, \bar{f}_1, \dots, \bar{f}_{i-1}]_{\mathbb{Z}/p^i\mathbb{Z}},$$

where the latter space is the space of $\mathbb{Z}/p^i\mathbb{Z}$ -coinvariants.

Proposition 25. *A cyclic group of the Nottingham group is described by a series of elements $\bar{C}_i \in k_{\mathbf{n},\bar{m}_i}[\bar{f}_0, \dots, \bar{f}_{i-1}]_{\mathbb{Z}/p^i\mathbb{Z}}$ so that $\bar{C}_i^p - \bar{C}_i$ is zero in the space $k_{\mathbf{n},\bar{m}_i}[\bar{f}_0, \dots, \bar{f}_{i-1}]_{\mathbb{Z}/p^i\mathbb{Z}}$.*

In order to ensure that the element σ has order p^h we should have, $\bar{C}_s(\sigma^{p^\nu}) \neq 0$, for all $0 \leq \nu < h$ i.e.

$$(1 + \sigma + \dots + \sigma^{p^\nu-1}) \bar{C}(\sigma) \neq 0.$$

References

[1] Frauke M. Bleher, Ted Chinburg, Bjorn Poonen, Peter Symonds, Automorphisms of Harbater–Katz–Gabber curves, *Math. Ann.* 368 (1) (Jun 2017) 811–836.
 [2] Rachel Camina, Subgroups of the Nottingham group, *J. Algebra* 196 (1) (1997) 101–113.
 [3] Rachel Camina, The Nottingham group, in: *New Horizons in Pro-p Groups*, Springer, 2000, pp. 205–221.
 [4] T. Chinburg, R. Guralnick, D. Harbater, Oort groups and lifting problems, *Compos. Math.* 144 (4) (2008) 849–866.
 [5] Ted Chinburg, Robert Guralnick, David Harbater, The local lifting problem for actions of finite groups on curves, *Ann. Sci. Éc. Norm. Supér. (4)* 44 (4) (2011) 537–605.

- [6] Ted Chinburg, Robert Guralnick, David Harbater, Global Oort groups, *J. Algebra* 473 (2017) 374–396.
- [7] Arnaldo Garcia, Henning Stichtenoth, Elementary abelian p -extensions of algebraic function fields, *Manuscr. Math.* 72 (1) (Dec 1991) 67–79.
- [8] 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.
- [9] David Harbater, Moduli of p -covers of curves, *Commun. Algebra* 8 (12) (1980) 1095–1122.
- [10] Nathan Jacobson, *Basic Algebra. II*, second edition, W. H. Freeman and Company, New York, 1989.
- [11] Stephen Arthur Jennings, Substitution groups of formal power series, *Can. J. Math.* 6 (1954) 325–340.
- [12] Sotiris Karanikolopoulos, Aristides Kontogeorgis, Automorphisms of curves and Weierstrass semi-groups for Harbater-Katz-Gabber covers, *Trans. Am. Math. Soc.* 371 (9) (2019) 6377–6402.
- [13] Nicholas M. Katz, Local-to-global extensions of representations of fundamental groups, *Ann. Inst. Fourier (Grenoble)* 36 (4) (1986) 69–106.
- [14] Benjamin Klopsch, Automorphisms of the Nottingham group, *J. Algebra* 223 (1) (2000) 37–56.
- [15] Aristides Kontogeorgis, The ramification sequence for a fixed point of an automorphism of a curve and the weierstrass gap sequence, *Math. Z.* 259 (3) (2008) 471–479.
- [16] Jonathan Lubin, Torsion in the Nottingham group, *Bull. Lond. Math. Soc.* 43 (3) (2011) 547–560.
- [17] Jürgen Neukirch, Alexander Schmidt, Kay Wingberg, *Cohomology of Number Fields*, second edition, *Grundlehren der Mathematischen Wissenschaften (Fundamental Principles of Mathematical Sciences)*, vol. 323, Springer-Verlag, Berlin, 2008.
- [18] Andrew Obus, The (local) lifting problem for curves, in: *Galois-Teichmüller Theory and Arithmetic Geometry*, in: *Adv. Stud. Pure Math.*, vol. 63, Math. Soc. Japan, Tokyo, 2012, pp. 359–412.
- [19] Andrew Obus, Stefan Wewers, Cyclic extensions and the local lifting problem, *Ann. Math. (2)* 180 (1) (2014) 233–284.
- [20] Florian Pop, The Oort conjecture on lifting covers of curves, *Ann. Math. (2)* 180 (1) (2014) 285–322.
- [21] Jean-Pierre Serre, *Local Fields*, vol. 67, Springer Science & Business Media, 2013.
- [22] I.R. Shafarevich, Abelian and nonabelian mathematics, *Math. Intell.* 13 (1) (1991) 67–75. Translated from the Russian by Smilka Zdravkovska.
- [23] Henning Stichtenoth, *Algebraic Function Fields and Codes*, second edition, *Graduate Texts in Mathematics*, vol. 254, Springer-Verlag, Berlin, 2009.
- [24] Djurre Tijsma, Automata and finite order elements in the Nottingham group, Master’s thesis, Utrecht University, 2018.
- [25] Charles A. Weibel, *An Introduction to Homological Algebra*, Cambridge University Press, Cambridge, 1994.
- [26] Edwin Weiss, *Cohomology of Groups*, Academic Press, New York, 1969.