

A RELATIVE SHAFAREVICH THEOREM

NIELS BORNE

CONTENTS

1. Introduction	1
1.1. Main statement	1
1.2. Acknowledgements	2
2. Hasse-Witt coefficients	3
2.1. Notations	3
2.2. Definition	4
2.3. Behaviour under quotient : statement	4
2.4. Behaviour under quotient : proof	5
2.5. V -ordinariness	7
3. Extension of covers	7
3.1. Reductions	7
3.2. Fundamental exact sequence	9
3.3. Proof of theorem 1.1	10
4. Profinite proof for the extension of a p' -group by a p -group	12
4.1. Finite quotients of a free pro- p -group with p' -action	12
4.2. Geometric application	13
References	13

ABSTRACT. Suppose given a Galois étale cover $Y \rightarrow X$ of proper non-singular curves over an algebraically closed field k of prime characteristic p . Let H be its Galois group, and G any finite extension of H by a p -group P . We give necessary and sufficient conditions on G to be the Galois group of an étale cover of X dominating $Y \rightarrow X$.

1. INTRODUCTION

1.1. Main statement. Let p be a prime integer, and k an algebraically closed field of characteristic p . In [12], A.Pacheco and K.Stevenson have given necessary and sufficient conditions for an extension G of a p' -group by a p -group to occur as the Galois group of an étale cover of a given proper, non-singular curve X over k . We pursue this work further by solving the case of the extension G of an arbitrary group H (which we suppose of course realized as a Galois group) by a p -group P .

Thanks to the work of S.Nakajima (see [11]), we can define, for any étale H -cover $Y \rightarrow X$, a family of integers $\delta_{Y,V}$ parametrized by the set \mathcal{S}_H of isomorphism classes of simple $k[H]$ -modules. These integers describe the Galois module structure of the space $H^0(Y, \Omega_Y)^s$ of semi-simple differentials on Y in the sense that they are defined by the formula :

$$H^0(Y, \Omega_Y)^s \simeq \Omega^2 k \oplus \bigoplus_{V \in \mathcal{S}_H} P(V)^{\oplus \delta_{Y,V}}$$

(see §2.2 for a precise definition).

These ‘‘Hasse-Witt coefficients’’ seem to be slightly more convenient invariants for our purposes than the previously used generalized Hasse-Witt invariants (see Remark following definition 2.2). Let $Z \rightarrow X$ be an étale G -cover dominating the étale H -cover $Y \rightarrow X$, and $q : G \twoheadrightarrow H$ the corresponding group extension. We show in part 2 the following formula relating the corresponding Hasse-Witt coefficients :

$$\forall V \in \mathcal{S}_H \quad \delta_{Z, q^*V} + \dim_k H^1(G, q^*V) = \delta_{Y, V} + \dim_k H^1(H, V)$$

(see proposition 2.4).

We then use this result in part 3 to prove an extension of the main Theorem of [12] :

Theorem 1.1. *Let k be an algebraically closed field of positive characteristic p . Let also $Y \rightarrow X$ be a Galois étale cover of proper non-singular curves over k , with Galois group H . Suppose*

$$1 \longrightarrow P \longrightarrow G \xrightarrow{q} H \longrightarrow 1$$

is an exact sequence of finite groups, where P is a p -group.

Then the embedding problem

$$\begin{array}{ccccccc} & & & & \pi_1(X) & & \\ & & & & \downarrow & & \\ & & & & \downarrow & & \\ 1 & \longrightarrow & P & \longrightarrow & G & \xrightarrow{q} & H \longrightarrow 1 \\ & & & & \swarrow & & \end{array}$$

has a strong solution if and only if for every simple $k[H]$ -module V the following inequality holds :

$$\dim_k H^1(G, q^*V) - \dim_k H^1(H, V) \leq \delta_{Y, V}$$

Here are some indications about the origins of this theorem.

When $H = 1$, the above result specializes to the classical Theorem of Shafarevich (see for instance [5]) : a given p -group P occurs as the Galois group of an étale cover of Y if and only if the minimal number of generators of P is less than the Hasse-Witt invariant of Y .

The first to consider inequalities as in theorem 1.1 seems to be E.Kani in [8], and for this reason we call them *the Kani inequalities* or *the Kani conditions*. These were given as necessary conditions for the existence of a tame cover, and since Kani considered differentials instead of semi-simple ones, his inequalities coincide with ours only when the curve Y is ordinary.

Our main source of inspiration was [12], which we tried to interpret from the ‘‘Galois module’’ point of view. The original problem and the presentation in terms of an embedding problem is due to the authors of that paper. However, the tools employed here are quite different, in particular since we use some basic results of modular representation theory. Moreover, we make a heavy use of the convenient Proposition 2.4, which seems new, and of independent interest. As an application, we define, in paragraph 2.5, a refinement of the notion of ordinarity of a Galois étale cover, which we call V -ordinarity.

Let us give some details about the organization of the article. We prepare the proof of theorem 1.1 in §2 and §3. The proof is actually given in §3.3. In a last paragraph, we give another proof of theorem 1.1 in the special case solved in [12], namely when H is supposed a p' -group (see Proposition 4.2). This proof is based on the same cohomological argument as the one given in [12], but it uses moreover the existence of an interesting quotient of the fundamental group of X .

1.2. Acknowledgements. I would like to thank both M.Emsalem and B.Erez for their support.

2. HASSE-WITT COEFFICIENTS

2.1. Notations.

2.1.1. *Curves.* In the following we fix an algebraically closed field k of positive characteristic p .

The letters X, Y, \dots will denote connected, complete, non-singular curves over k .

Let S be an effective divisor on a curve X . Then the Cartier operator \mathcal{C} acts on the space $H^0(X, \Omega_X(S))$ (one can define this action directly or as dual of the action of the Frobenius, see [14]). This action is p^{-1} -linear. We will call semi-simple differentials associated to S the subspace

$$H^0(X, \Omega_X(S))^s := k \otimes_{\mathbb{F}_p} H^0(X, \Omega_X(S))^{\mathcal{C}}$$

generated by forms of the whole space $H^0(X, \Omega_X(S))$ which are fixed by \mathcal{C} . When $S = 0$, this subspace has dimension γ_X , the classical Hasse-Witt invariant of the curve X . One defines also a natural supplement of $H^0(X, \Omega_X(S))^s$ in $H^0(X, \Omega_X(S))$, the space $H^0(X, \Omega_X(S))^n$ of nilpotent differentials (see [14]).

We will denote by $\pi_1(X)$ “the” algebraic fundamental group of the curve X , without specifying a base point. When considering morphisms between curves and their fundamental groups, we will always suppose that a coherent choice of base points is made.

2.1.2. *Representation theory.* We also need a few basic notions from module theory over an artinian (not necessarily commutative) ring A . All A -modules will be implicitly supposed of finite type. We will use these notions for the group ring $A = k[H]$ (sometimes $A = \mathbb{F}_p[H]$) where H is a finite group whose order is (possibly) divisible by p . We refer to [2] for more details.

The letter k will always denote the trivial representation.

Every finitely generated A -module M has a well-defined (i.e. unique up to isomorphism) projective cover, which we denote by $P(M) \twoheadrightarrow M$. This allows us to define $\Omega M := \ker(P(M) \twoheadrightarrow M)$ and inductively $\Omega^{i+1}M = \Omega(\Omega^i M)$.

When there are several groups acting, we will also use the notations with indexes $P_H(M)$ and $\Omega_H M$ to stress the fact that H acts.

We will denote by S_A (or S_H when there is no doubt about the field used) a fixed complete set of representatives of the isomorphism classes of simple A -modules.

2.1.3. *Warning.* We make use of the usual notations and vocabulary of both domains, but this is not without certain ambiguities. For an example, the letter Ω is used with two different meanings. Moreover, since we have two different actions (Cartier and Galois) on the differentials, we have also two distinct notions of semi-simplicity.

We hope that this warning and the context will help to give a clear meaning to our assertions.

2.1.4. *Profinite groups.* An embedding problem is a diagram in the category of profinite groups :

$$\begin{array}{ccccccc} & & & & \pi & & \\ & & & & \downarrow \alpha & & \\ & & & & H & & \\ 1 & \longrightarrow & P & \longrightarrow & G & \xrightarrow{q} & H & \longrightarrow & 1 \end{array}$$

where the vertical arrow is an epimorphism and the horizontal sequence is exact. It is said to have a *weak solution* if there exists a continuous homomorphism $\beta : \pi \rightarrow G$ lifting α , i.e. $q \circ \beta = \alpha$. There is a *strong solution* if one can choose moreover β to be an epimorphism. According to [15], Chapitre I, §3.4, Proposition 16, $\text{cd}_p \pi \leq 1$ if and only if every embedding problem with a pro- p -group kernel has a weak solution.

2.2. Definition.

Lemma 2.1. *Let $Y \rightarrow X$ be a Galois étale cover of proper non-singular curves with Galois group H . Then*

(i) *For any reduced non-trivial effective H -invariant divisor S the space $H^0(Y, \Omega_Y(S))^s$ of semi-simple differentials associated to S is projective as a $k[H]$ -module.*

(ii) *There is a projective $k[H]$ -module P , unique up to isomorphism, such that $H^0(Y, \Omega_Y)^s \simeq \Omega^2 k \oplus P$*

Proof. (i) Let P be a p -Sylow of H . According to [11], Theorem 1, applied to the subcover $Y \rightarrow Y/P$, the space $H^0(Y, \Omega_Y(S))^s$ is $k[P]$ -free. But this is equivalent to saying that this space is $k[H]$ -projective (this is easily seen using the fact that any $k[H]$ -module is projective relative to P [see for an example [2], 3.6 for relative projectivity and in particular Corollary 3.6.10]).

(ii) Choose S to be reduced to an orbit under H . Then the short exact sequence of sheaves $0 \rightarrow \Omega_Y \rightarrow \Omega_Y(S) \rightarrow \mathcal{O}_S \rightarrow 0$ gives the long exact sequence

$$0 \rightarrow H^0(Y, \Omega_Y)^s \rightarrow H^0(Y, \Omega_Y(S))^s \rightarrow k[H] \rightarrow k \rightarrow 0$$

(see the proof of [11], Theorem 2 for the fact that nilpotent differentials have trivial residues). In view of (i), it suffices to apply Schanuel's lemma and the Krull-Schmidt theorem to compare this sequence to the beginning of the minimal projective resolution of k . \square

Now, using the Krull-Schmidt theorem again to decompose P , and the fact that the indecomposable projective $k[H]$ -modules are exactly the projective covers of the simple $k[H]$ -modules, we can make the structure of $H^0(Y, \Omega_Y)^s$ more precise :

Definition 2.2. *Let $Y \rightarrow X$ be a Galois étale cover with Galois group H and let S_H be a set of representatives of the isomorphism classes of simple $k[H]$ -modules. We define the Hasse-Witt coefficients of the cover as the only non-negative integers $\delta_{Y,V}$ verifying :*

$$H^0(Y, \Omega_Y)^s \simeq \Omega^2 k \oplus \bigoplus_{V \in S_H} P(V)^{\oplus \delta_{Y,V}}$$

Remark : It would be more coherent with previous work on the subject to consider generalized Hasse-Witt invariants defined by $\gamma_{Y,V} := \delta_{Y,V} \cdot \dim_k P(V)$. However, since $\dim_k P(V)$ is hard to compute in general, and contains no geometric information, we prefer to exclude it from the definition, to concentrate on the computation of $\delta_{Y,V}$'s.

2.3. Behaviour under quotient : statement. First we introduce a useful notation.

Definition 2.3. *If M is any $k[H]$ -module of finite type, we define*

$$h^i(H, M) := \dim_k H^i(H, M)$$

If $q : G \twoheadrightarrow H$ is a group epimorphism and M is a $k[H]$ -module, we denote by q^*M the corresponding inflated $k[G]$ -module. (We will also use $M = q_*N$ for $N = q^*M$).

Proposition 2.4. *Let $Z \rightarrow X$ be a Galois étale cover with Galois group G , and let $Y \rightarrow X$ be any quotient Galois cover, with Galois group H . Denote by q the quotient map $G \twoheadrightarrow H$. Then :*

$$\forall V \in S_H \quad \delta_{Z, q^*V} + h^1(G, q^*V) = \delta_{Y,V} + h^1(H, V)$$

Before giving the proof of Proposition 2.4, we make some remarks, beginning by another useful definition.

Definition 2.5. *Let $Y \rightarrow X$ be a Galois étale H -cover, $\pi_1(X) \twoheadrightarrow H$ the corresponding group epimorphism, and $q : G \twoheadrightarrow H$ an extension of H . We will say that the pair $(\pi_1(X) \twoheadrightarrow H, G \twoheadrightarrow H)$ satisfies the Kani inequalities (or conditions) if and only if :*

$$\forall V \in S_H \quad h^1(G, q^*V) - h^1(H, V) \leq \delta_{Y,V}$$

Remarks :

- (1) In the perspective of the proof of theorem 1.1, it is clear that Proposition 2.4 implies that if the embedding problem of the theorem has a solution, then the Kani inequalities hold for $(\pi_1(X) \twoheadrightarrow H, G \twoheadrightarrow H)$.
- (2) Let us assume that the kernel P of $q : G \twoheadrightarrow H$ is a p -group. Then the inflation map $q^* : \mathcal{S}_H \rightarrow \mathcal{S}_G$ is one to one. Indeed, we have :

Theorem 2.6 (Clifford). *If P is any normal subgroup of G and M is a semi-simple $k[G]$ -module, then $M|_P$ is a semi-simple $k[P]$ -module.*

(see for instance [1], Chapter I.3, Theorem 4). Moreover, it is well known that if P is a p -group, the only simple $k[P]$ -module is the trivial one. Hence, if we suppose that P is a p -group, any simple $k[G]$ -module is trivial when restricted to P .

We can conclude, with this hypothesis on P , that the Hasse-Witt coefficients of the covers $Z \rightarrow X$ and $Y \rightarrow X$ determine each other.

- (3) M.Emsalem suggested to us that one can consider more generally tame covers, and that Proposition 2.4 could also hold in this more general setting. We hope to come back to these questions in a subsequent paper.

2.4. Behaviour under quotient : proof. The idea is quite naturally to take the fixed part under the kernel P of $q : G \twoheadrightarrow H$ of the two members of the isomorphism :

$$H^0(Z, \Omega_Z)^s \simeq \Omega_G^2 k \oplus \bigoplus_{U \in \mathcal{S}_G} P_G(U)^{\oplus \delta_{Z,U}}$$

and then use the three following lemmas.

2.4.1. Algebraic part. In this part we assume only that we have an arbitrary exact sequence of groups :

$$1 \longrightarrow P \xrightarrow{r} G \xrightarrow{q} H \longrightarrow 1$$

Lemma 2.7. *Let $U \in \mathcal{S}_G$.*

$$q_*(P_G(U)^P) \simeq \begin{cases} P_H(V) & \text{if } \exists V \in \mathcal{S}_H \text{ such that } U = q^*V \\ 0 & \text{else} \end{cases}$$

Proof. The proof is a straightforward computation, using the Krull-Schmidt theorem and three facts :

- (1) If $U \in \mathcal{S}_G$, then $\text{soc}(P_G(U)) \simeq U$,
(see [1], Chapter II.6, Theorem 6, or [2], Theorem 1.6.3) ;
- (2) $q_*(k[G]^P) \simeq k[H]$,
so in particular $q_*(\cdot^P)$ sends projectives to projectives ;
- (3) $k[G] \simeq \bigoplus_{U \in \mathcal{S}_G} P_G(U)^{\oplus \dim_k U}$.

□

Lemma 2.8.

$$q_*((\Omega_G^2 k)^P) \simeq \Omega_H^2 k \oplus \bigoplus_{V \in \mathcal{S}_H} P_H(V)^{\oplus h^1(G, q^*V) - h^1(H, V)}$$

Proof. We will suppose that $p \nmid \#P$, the proof in the opposite case being similar, and in fact easier. Then, as Kani notices ([8], §5, Lemma 2), one can easily show inductively that for all i , the module $\Omega_p^i k$ is non-projective, and this implies $H^1(P, \Omega_p^i k) \neq 0$ (see [2], Proposition 3.14.4).

Restricting the exact sequence

$$0 \longrightarrow \Omega_G^i k \longrightarrow P_G(\Omega_G^{i-1} k) \longrightarrow \cdots \longrightarrow P_G(\Omega_G k) \longrightarrow k \longrightarrow 0$$

to P via $r : P \rightarrow G$ (which, in view of $r^*k[G] \simeq k[P]^{\oplus \#H}$, also sends projectives to projectives) and comparing to the minimal $k[P]$ -resolution of the trivial module k , we get an isomorphism $r^*(\Omega_G^i k) \simeq \Omega_p^i k \oplus Q$, where Q is a projective $k[P]$ -module, and this implies

$H^1(P, r^*(\Omega_G^i k)) \simeq H^1(P, \Omega_P^i k)$. So we have shown in particular that for any i , we have $H^1(P, r^*(\Omega_G^i k)) \neq 0$.

Now applying the functor $q_*(\cdot^P)$ to the exact sequence

$$0 \longrightarrow \Omega_G k \longrightarrow P_G k \longrightarrow k \longrightarrow 0$$

we get the exact sequence of $k[H]$ -modules :

$$0 \longrightarrow q_*((\Omega_G k)^P) \longrightarrow q_*((P_G k)^P) \longrightarrow k \longrightarrow H^1(P, \Omega_G k) \longrightarrow 0$$

The k -vector-space underlying $H^1(P, \Omega_G k)$ is $H^1(P, r^*(\Omega_G k)) \neq 0$, hence the middle arrow has to be zero, and thanks to Lemma 2.7 it comes : $q_*((\Omega_G k)^P) \simeq q_*((P_G k)^P) \simeq P_H(k)$.

We proceed similarly, starting with the sequence

$$0 \longrightarrow \Omega_G^2 k \longrightarrow P_G(\Omega_G k) \longrightarrow \Omega_G k \longrightarrow 0$$

we get the exact sequence of $k[H]$ -modules :

$$0 \longrightarrow q_*((\Omega_G^2 k)^P) \longrightarrow q_*((P_G(\Omega_G k))^P) \longrightarrow P_H(k) \longrightarrow H^1(P, \Omega_G^2 k) \longrightarrow 0$$

We claim that $H^1(P, \Omega_G^2 k) \simeq k$. In fact the underlying k -vector-space is $H^1(P, r^*\Omega_G^2 k) \simeq H^1(P, \Omega_P^2 k)$. But the above exact sequence for $G = P$ (hence $H = 1$) shows that $H^1(P, \Omega_P^2 k) \simeq k$. So $H^1(P, \Omega_G^2 k)$ must be simple, and because there is a surjective $k[H]$ -map $P_H(k) \twoheadrightarrow H^1(P, \Omega_G^2 k)$, it can only be the trivial simple module. From this we deduce, comparing the above exact sequence to the minimal $k[H]$ -projective resolution of k , that $q_*((\Omega_G^2 k)^P) \simeq \Omega_H^2 k \oplus R$, where R is a projective $k[H]$ -module. Now, using Lemma 2.7, and the isomorphism

$$P_G(\Omega_G k) \simeq \bigoplus_{U \in \mathcal{S}_G} P_H(U)^{\oplus h^1(G, U)}$$

(see [8], Proposition 5), a direct computation in the Grothendieck ring of the finitely-generated $k[H]$ -modules shows the equality between classes :

$$[R] = \left[\bigoplus_{V \in \mathcal{S}_H} P_H(V)^{\oplus h^1(G, q^*V) - h^1(H, V)} \right]$$

But since both modules involved are $k[H]$ -projective, they have to be isomorphic. \square

2.4.2. *Geometric part.* In this part the hypothesis are those of Proposition 2.4.

Lemma 2.9. *The pullback along $Z \rightarrow Y$ induces isomorphisms*

(i) of $\mathbb{F}_p[H]$ -modules :

$$\text{Pic}_0(Y)[p] \simeq (\text{Pic}_0(Z)[p])^P$$

(ii) of $k[H]$ -modules :

$$H^0(Y, \Omega_Y)^s \simeq (H^0(Z, \Omega_Z)^s)^P$$

Proof. (i) Since the map $Z \rightarrow Y$ commutes with the action of G , it is clear that the pullback is equivariant.

The Hochschild-Serre spectral sequence (see for instance [9], Chapter III, Theorem 2.20) for the P -Galois cover $Z \rightarrow Y$ and the sheaf $\mathbb{G}_{m, Y} = \mathcal{O}_Y^*$ gives the exact sequence of terms of low degree :

$$0 \longrightarrow H^1(P, k^*) \longrightarrow \text{Pic}(Y) \longrightarrow (\text{Pic}(Z))^P \longrightarrow H^2(P, k^*)$$

Now since k is of characteristic p , raising to the power p induces a group isomorphism

$$\begin{aligned} k^* &\longrightarrow k^* \\ x &\longmapsto x^p \end{aligned}$$

In particular, the groups $H^i(P, k^*)$ have no p -torsion and are p -divisible, and an immediate diagram chase allows to conclude the result.

(ii) According to [14], Proposition 10, there is a natural isomorphism

$$\text{Pic}_0(Y)[p] \simeq H^0(Y, \Omega_Y)^C$$

Indeed, if \mathcal{L} is an invertible sheaf on Y such that $\mathcal{L}^{\otimes p} \simeq \mathcal{O}_X$, write $\mathcal{L} \simeq \mathcal{L}_Y(D)$ for a divisor D on Y , and let f be a function on Y such that $pD = (f)$. To \mathcal{L} we can then associate the form $\omega = df/f$, and this gives the map we were looking for. Thanks to this description, one checks immediately that this map is compatible with the action of H , and also with the pull-back along $Z \rightarrow Y$. But then (i) gives

$$H^0(Y, \Omega_Y)^C \simeq (H^0(Z, \Omega_Z)^C)^P$$

and the lemma follows by tensoring both sides by k . □

2.5. V -ordinariness. This section is not necessary for the proof of theorem 1.1 but is just an illustration of the usefulness of Proposition 2.4. Recall that a cover $Y \rightarrow X$ is said ordinary if the curve Y is, that is if $\gamma_Y = g_Y$.

Definition 2.10. Let $Y \rightarrow X$ be an Galois étale cover of group H and $V \in S_H$.

The cover is said V -ordinary if $\delta_{Y,V} = \dim V(g_X - 1) - h^1(H, V) + h^0(H, V)$.

The link with the classical notion is given by the following lemma.

Lemma 2.11. The cover $Y \rightarrow X$ is ordinary if and only if it is V -ordinary for all $V \in S_H$.

Proof. $Y \rightarrow X$ is ordinary if and only if $H^0(Y, \Omega_Y)^s = H^0(Y, \Omega_Y)$. But [8], Theorem 2, gives that

$$H^0(Y, \Omega_Y) \simeq \Omega^2 k \oplus \bigoplus_{V \in S_H} P(V)^{\oplus \dim V(g_X - 1) - h^1(H, V) + h^0(H, V)}$$

and the lemma follows. □

It is well known that a Galois étale p -cover of an ordinary curve is ordinary (this results from the comparison of the Hurwitz and the Shafarevich formulas). Here is a relative version :

Lemma 2.12. Let $Z \rightarrow X$ and $Y \rightarrow X$ be covers as in Proposition 2.4. Then $Z \rightarrow X$ is q^*V -ordinary if and only if $Y \rightarrow X$ is V -ordinary.

Proof. This follows immediately from Proposition 2.4. □

This two lemmas suggest a method to show that a cover is ordinary, by using subcovers.

3. EXTENSION OF COVERS

Let $Y \rightarrow X$ be a Galois étale cover of Galois group H , and $\pi_1(X) \twoheadrightarrow H$ the corresponding group epimorphism. In this section, we show that if the pair $(\pi_1(X) \twoheadrightarrow H, G \twoheadrightarrow H)$ verifies the Kani inequalities, and the kernel P of $G \twoheadrightarrow H$ is a p -group, then the corresponding embedding problem has a solution (see theorem 1.1).

3.1. Reductions. In this section, we give an adaptation of an argument of A.Pacheco and K.Stevenson (see [12]).

$$\begin{array}{ccccccc}
& & & & \pi_1(X) & & \\
& & & & \downarrow & & \\
& & & & \swarrow & & \\
1 & \longrightarrow & \Phi(P) & \longrightarrow & G & \longrightarrow & G/\Phi(P) \longrightarrow 1
\end{array}$$

and this is also a strong solution for the initial embedding problem.

Remark : The fact that we allow some P -part in H enables us to avoid the use of the argument that the p -cohomological dimension of $\pi_1(X)$ is at most 1 (compare with [12]). However, we cannot avoid the use of this argument at a later stage.

3.1.3. *Second reduction.* Suppose next that theorem 1.1 holds with the extra hypothesis that P is abelian p -elementary, and simple as $\mathbb{F}_p[H]$ -module. Then we claim the theorem holds with the restricted extra hypothesis that P is abelian p -elementary. The proof is the same, by induction on $\dim_{\mathbb{F}_p} P$, thanks to Lemma 3.1, applied with O the kernel of $P \rightarrow Q$, where Q is any $\mathbb{F}_p[H]$ -simple quotient of P . As H acts by conjugation on P , the fact that O is H -stable ensures that O is normal in G .

3.2. Fundamental exact sequence.

3.2.1. *Introduction.* In the following, the data will be :

- (1) A Galois étale H -cover $Y \rightarrow X$, or equivalently, a continuous surjective group homomorphism $\pi_1(X) \twoheadrightarrow H$,
- (2) A simple $\mathbb{F}_p[H]$ -module P of finite type, i.e. an irreducible representation of H over \mathbb{F}_p ,
- (3) A group G , extension of H by the $\mathbb{F}_p[H]$ -module P (or equivalently a class $\alpha \in H^2(H, P)$), such that the Kani conditions hold for $(\pi_1(X) \twoheadrightarrow H, G \twoheadrightarrow H)$.

Of course 2 and 3 are equivalent to the previous data of an exact sequence $1 \rightarrow P \rightarrow G \rightarrow H \rightarrow 1$, where P is abelian p -elementary, simple as $\mathbb{F}_p[H]$ -module, such that the Kani conditions hold for $(\pi_1(X) \twoheadrightarrow H, G \twoheadrightarrow H)$.

We split this data in two because 3 appears only at a later stage, and also because we will have to distinguish two cases, depending on whether α is zero or not.

3.2.2. *Inflation-restriction sequence for profinite groups.* In the next general proposition, we use bold letters to distinguish from our previous notations.

Definition 3.2. Let $1 \rightarrow \mathbf{F} \rightarrow \mathbf{G} \rightarrow \mathbf{H} \rightarrow 1$ be an exact sequence of profinite groups, M a discrete abelian group endowed with a continuous action of \mathbf{G} . The transgression morphism is the fourth arrow in the exact sequence of terms of low degree in the Lyndon-Hochschild-Serre spectral sequence :

$$0 \rightarrow H^1(\mathbf{H}, M^{\mathbf{F}}) \rightarrow H^1(\mathbf{G}, M) \rightarrow H^1(\mathbf{F}, M)^{\mathbf{H}} \rightarrow H^2(\mathbf{H}, M^{\mathbf{F}}) \rightarrow H^2(\mathbf{G}, M)$$

Proposition 3.3. Suppose moreover that \mathbf{F} acts trivially on M . Let \mathbf{F}' be the commutator subgroup of \mathbf{F} , and let $\gamma \in H^2(\mathbf{H}, \mathbf{F}/\mathbf{F}')$ be the class of the extension :

$$1 \rightarrow \mathbf{F}/\mathbf{F}' \rightarrow \mathbf{G}/\mathbf{F}' \rightarrow \mathbf{H} \rightarrow 1$$

Then the transgression $\text{trans} : H^1(\mathbf{F}, M)^{\mathbf{H}} \rightarrow H^2(\mathbf{H}, M^{\mathbf{F}})$ is given explicitly by :

$$\forall u \in H^1(\mathbf{F}, M)^{\mathbf{H}} = H^0(\mathbf{H}, \text{Hom}(\mathbf{F}/\mathbf{F}', M)) \quad \text{trans}(u) = -\gamma \cup u$$

Proof. We refer to [6], Theorem 4 for the case of abstract groups. □

Proposition 3.4. *Let $Y \rightarrow X$ be a Galois étale cover with Galois group H , and P a simple $\mathbb{F}_p[H]$ -module.*

(i) *The exact sequence of terms of low degree for the spectral sequence of the extension $1 \rightarrow \pi_1(Y) \rightarrow \pi_1(X) \rightarrow H \rightarrow 1$ is the following exact sequence of finite-dimensional \mathbb{F}_p -vector spaces :*

$$0 \rightarrow H^1(H, P) \rightarrow H^1(\pi_1(X), P) \rightarrow \text{Hom}_H(\pi_1^{ab}(Y), P) \rightarrow H^2(H, P) \rightarrow 0$$

(ii) *The transgression map $\text{trans} : \text{Hom}_H(\pi_1^{ab}(Y), P) \rightarrow H^2(H, P)$ in the sequence above can be described as follows : let $u \in \text{Hom}_H(\pi_1^{ab}(Y), P)$, $u \neq 0$. Then u corresponds canonically to a Galois cover $Z \rightarrow X$ whose Galois group is an extension of H by P , and $\text{trans}(u)$ is precisely the negative of the class of this extension in $H^2(H, P)$.*

Proof. (i) Since P is a trivial $\pi_1(Y)$ -module, we can apply Proposition 3.3. To show the exactness it suffices to show that $H^2(\pi_1(X), P) = 0$. But P is killed by p , so this equality follows directly from $\text{cd}_p(\pi_1(X)) \leq 1$ (for which we refer to [12], Theorem 5.11). Moreover, the largest p -elementary quotient of $\pi_1^{ab}(X)$ is of finite dimension over \mathbb{F}_p (this dimension is nothing else than the Hasse-Witt invariant γ_X), hence so is $\text{Hom}_H(\pi_1^{ab}(Y), P)$ and the $H^i(H, P)$ are also known to be finite-dimensional over \mathbb{F}_p .

(ii) One point here is because u is H -equivariant and not equal 0, and P is a simple $\mathbb{F}_p[H]$ -module, it has to be surjective. Hence u determines a P -Galois cover $Z \rightarrow Y$, and because u is H -invariant, $\pi_1(Z)$ is in fact normal in $\pi_1(X)$, which means that the composite cover $Z \rightarrow X$ is Galois. The last assertion can be deduced from Proposition 3.3 by a direct computation, using the explicit description of cup product of cochains given in [6], Chapter II, §1. \square

3.2.3. *Application to the embedding problem.* We see that Proposition 3.4 implies at once that if the group G is a non-trivial extension of H by P (that is, its class α in $H^2(H, P)$ is non zero), then the corresponding embedding problem has a strong solution (i.e. G is the Galois group of a cover of X dominating the H -cover $Y \rightarrow X$). One can of course also see this quite directly, without using the inflation-restriction sequence, but “only” the inequality $\text{cd}_p(\pi_1(X)) \leq 1$. A rather striking fact is that we do not even use the Kani inequalities here.

So the only thing which remains to be proved to end the proof of theorem 1.1 is that we can also realize the trivial extension. Proposition 3.4 implies that this is equivalent to the following inequality :

$$(1) \quad \dim_{\mathbb{F}_p} \text{Hom}_H(\pi_1^{ab}(Y), P) > \dim_{\mathbb{F}_p} H^2(H, P)$$

because then there exists $u \in \text{Hom}_H(\pi_1^{ab}(Y), P)$, $u \neq 0$, such that $\text{trans}(u) = 0$ which, by proposition 3.4 (ii), gives rise to the desired (split) Galois cover.

3.3. Proof of theorem 1.1.

3.3.1. *Organization of the proof.* The “only if” part of the theorem is a consequence of proposition 2.4.

To show the “if” part, we have to show, using definition 2.5, that if the pair $(\pi_1(X) \rightarrow H, G \rightarrow H)$ satisfies the Kani inequalities, the corresponding embedding problem has a strong solution, i.e., we can extend the cover to G . For this, using §3.1, we reduce to the case where $P = \ker(G \rightarrow H)$ is abelian p -elementary, and simple as $\mathbb{F}_p[H]$ -module. Thanks to §3.2, we then reduce to the case when G is the trivial extension. In this case, the existence of a strong solution has been shown to be equivalent to the inequality 1. Hence the goal of this section is to prove that the Kani inequalities imply the inequality 1. It is reached thanks to lemmas 3.9 and 3.10.

3.3.2. *Rational representations and base extension.*

Lemma 3.5. *Let \mathcal{V} a simple $\mathbb{F}_p[H]$ -module.*

(i) *$k \otimes_{\mathbb{F}_p} \mathcal{V}$ is a semi-simple $k[H]$ -module.*

- (ii) $\dim_{\mathbb{F}_p} H^i(H, \mathcal{V}) = \dim_k H^i(H, k \otimes_{\mathbb{F}_p} \mathcal{V})$
- (iii) The multiplicity of a simple $k[H]$ -module V in $k \otimes_{\mathbb{F}_p} \mathcal{V}$ is at most 1.
- (iv) If moreover V and V' are two simple summands of $k \otimes_{\mathbb{F}_p} \mathcal{V}$ then $h^i(H, V) = h^i(H, V')$.

Proof. (i) See [7], Theorem 1.8.

(ii) This is true without any assumption on \mathcal{V} because

$$H^i(H, k \otimes_{\mathbb{F}_p} \mathcal{V}) \simeq k \otimes_{\mathbb{F}_p} H^i(H, \mathcal{V})$$

(iii) See [7], Lemma 1.15.

(iv) Fix a finite Galois extension F of \mathbb{F}_p such that F is a splitting field for $\mathbb{F}_p[H]$. It is enough to show the corresponding property for F , i.e. if V and V' are two simple summands of $F \otimes_{\mathbb{F}_p} \mathcal{V}$ then $h^i(H, V) = h^i(H, V')$. The group $\text{Gal}(F/\mathbb{F}_p)$ acts on the group ring $F[H]$, hence on $F[H] - \mathbf{Mod}$, and we denote this action by $V \rightarrow V^\sigma$. Because \mathcal{V} is simple, we know by descent theory that $V' \simeq V^\sigma$ for some σ in $\text{Gal}(F/\mathbb{F}_p)$. So it remains to show that $h^i(H, V) = h^i(H, V^\sigma)$. But since the actions of $\text{Gal}(F/\mathbb{F}_p)$ and H commute, we have isomorphisms of F -vector spaces $H^i(H, V^\sigma) \simeq H^i(H, V)^\sigma$ (obtained by deriving the corresponding isomorphism for $i = 0$).

□

Lemma 3.6.

$$H^0(Y, \Omega_Y)^s / \text{rad}(H^0(Y, \Omega_Y)^s) \simeq \bigoplus_{V \in \mathcal{S}_H} V^{\oplus h^2(H, V) + \delta_{Y, V}}$$

Proof. This follows from the definition 2.2 and the isomorphisms $\Omega^2 k / \text{rad} \Omega^2 k \simeq P(\Omega^2 k) / \text{rad} P(\Omega^2 k)$ and $P(\Omega^2 k) \simeq \bigoplus_{V \in \mathcal{S}_H} P(V)^{\oplus h^2(H, V)}$ (see [8], Proposition 5).

□

Proposition 3.7. Let $Y \rightarrow X$ a Galois étale H -cover and \mathcal{V} a simple $\mathbb{F}_p[H]$ -module. If V and V' are two simple summands of $k \otimes_{\mathbb{F}_p} \mathcal{V}$ then $\delta_{Y, V} = \delta_{Y, V'}$.

Proof. According to [7], Theorem 1.5, we have $\text{rad}(k[H]) = k \otimes_{\mathbb{F}_p} \text{rad}(\mathbb{F}_p[H])$. Hence in fact $H^0(Y, \Omega_Y)^s / \text{rad}(H^0(Y, \Omega_Y)^s) \simeq k \otimes_{\mathbb{F}_p} (H^0(Y, \Omega_Y)^C / \text{rad}(H^0(Y, \Omega_Y)^C))$ as semi-simple $k[H]$ -modules. As in the proof of lemma 3.5 (iv), one sees that V and V' are obtained by base change of two conjugate $F[H]$ -modules, where F is a finite Galois splitting field for $\mathbb{F}_p[H]$. So their multiplicities in $k \otimes_{\mathbb{F}_p} (H^0(Y, \Omega_Y)^C / \text{rad}(H^0(Y, \Omega_Y)^C))$ must be the same, hence according to lemma 3.6, $h^2(H, V) + \delta_{Y, V} = h^2(H, V') + \delta_{Y, V'}$, and we conclude thanks to lemma 3.5 (iv).

□

Definition 3.8. Let \mathcal{V} a simple $\mathbb{F}_p[H]$ -module.

(i) Let $V \in \mathcal{S}_H$. We write $V | \mathcal{V}$ to say that V is a summand of $k \otimes_{\mathbb{F}_p} \mathcal{V}$.

(ii) We will denote by $\text{deg } \mathcal{V}$ the number of simple summands of $k \otimes_{\mathbb{F}_p} \mathcal{V}$ in a decomposition into simple $k[H]$ -modules.

3.3.3. *Conclusion.* The two following lemmas end the proof of theorem 1.1.

Lemma 3.9. Let $V \in \mathcal{S}_H$ such that $V | P$. Then :

$$\dim_{\mathbb{F}_p} \text{Hom}_H(\pi_1^{ab}(Y), P) = \text{deg } P \cdot (h^2(H, V) + \delta_{Y, V}) = \dim_{\mathbb{F}_p} H^2(H, P) + \text{deg } P \cdot \delta_{Y, V}$$

Proof. First notice that $\text{Hom}(\pi_1^{ab}(Y), P) \simeq \text{Hom}(\pi_1(Y), \mathbb{F}_p) \otimes_{\mathbb{F}_p} P$. But then using Artin-Schreier theory (see [16] Chapter II Theorem (4.2.1)) we see that :

$$\text{Hom}(\pi_1(Y), \mathbb{F}_p) \simeq H^1(Y, \mathbb{F}_p) \simeq H^1(Y, \mathbb{G}_{a, Y})^F \simeq (H^0(Y, \Omega_Y)^C)^\vee$$

As these isomorphisms commute with the H -action we conclude that :

$$\text{Hom}_H(\pi_1^{ab}(Y), P) \simeq \text{Hom}_H(H^0(Y, \Omega_Y)^C, P)$$

So it suffices to compute :

$$\dim_{\mathbb{F}_p} \text{Hom}_H(H^0(Y, \Omega_Y)^C, P) = \dim_k \text{Hom}_H(H^0(Y, \Omega_Y)^s, k \otimes_{\mathbb{F}_p} P)$$

Because $k \otimes_{\mathbb{F}_p} P$ is semi-simple, we need only to consider the largest semi-simple quotient of $H^0(Y, \Omega_Y)^s$, that is $H^0(Y, \Omega_Y)^s / \text{rad}(H^0(Y, \Omega_Y)^s)$, which has been computed in lemma 3.6. From this decomposition, lemma 3.5, and proposition 3.7 follows :

$$\dim_k \text{Hom}_H(H^0(Y, \Omega_Y)^s, k \otimes_{\mathbb{F}_p} P) = \sum_{V'|P} h^2(H, V') + \delta_{Y, V'} = \text{deg } P(h^2(H, V) + \delta_{Y, V})$$

□

Lemma 3.10. *Let $V \in \mathcal{S}_H$. If the Kani inequalities hold, G is a trivial extension of H by P , and $V|P$, then $\delta_{Y, V} > 0$*

Proof. Because of the Kani inequalities we have $\delta_{Y, V} \geq h^1(G, q^*V) - h^1(H, V)$, where q is the epimorphism $q : G \twoheadrightarrow H$. We will show that $h^1(G, q^*V) - h^1(H, V) = 1$. In fact, using proposition 3.3, and the hypothesis that G is the trivial extension, we get an exact sequence :

$$0 \rightarrow H^1(H, V) \rightarrow H^1(G, q^*V) \rightarrow H^1(P, V)^H \rightarrow 0$$

But now :

$$H^1(P, V)^H \simeq \text{Hom}_{\mathbb{F}_p[H]}(P, V) \simeq \text{Hom}_{k[H]}(k \otimes_{\mathbb{F}_p} P, V) \simeq k$$

□

4. PROFINITE PROOF FOR THE EXTENSION OF A p' -GROUP BY A p -GROUP

In this section, we give another proof, almost purely module-theoretic, of the main Theorem of [12] (i.e. theorem 1.1 in the case of H being a p' -group).

4.1. Finite quotients of a free pro- p -group with p' -action. Let γ be a nonnegative integer and F_γ be a free pro- p -group with γ generators, endowed with a continuous action of a finite p' -group H .

Definition 4.1. *For each $\mathcal{V} \in \mathcal{S}_{\mathbb{F}_p[H]}$ let $\delta_{\mathcal{V}}$ be the integer :*

$$\delta_{\mathcal{V}} := \dim_{\mathbb{F}_p} H^1(F_\gamma \rtimes H, \mathcal{V})$$

Remark :

In this definition, \mathcal{V} is seen as a discrete $F_\gamma \rtimes H$ -module via the canonical map $F_\gamma \rtimes H \twoheadrightarrow H$. Using the exact sequence $0 \rightarrow F_\gamma \rightarrow F_\gamma \rtimes H \rightarrow H \rightarrow 0$ we can also consider \mathcal{V} as a trivial continuous F_γ -module, and the inflation-restriction sequence shows that $\delta_{\mathcal{V}} = \dim_{\mathbb{F}_p} H^1(F_\gamma, \mathcal{V})^H = \dim_{\mathbb{F}_p} \text{Hom}_H(F_\gamma, \mathcal{V})$. But any continuous morphism $F_\gamma \rightarrow \mathcal{V}$ is trivial on the (profinite) Frattini subgroup $\Phi(F_\gamma)$, hence $\delta_{\mathcal{V}} = \dim_{\mathbb{F}_p} \text{Hom}_H(F_\gamma/\Phi(F_\gamma), \mathcal{V})$, which shows that the $\delta_{\mathcal{V}}$'s are actually finite.

Proposition 4.2. *Let P a finite p -group endowed with an action of H .*

The following assertions are equivalent :

- (i) *There exists a continuous H -epimorphism $F_\gamma \twoheadrightarrow P$*
- (ii) $\forall \mathcal{V} \in \mathcal{S}_{\mathbb{F}_p[H]} \quad \dim_{\mathbb{F}_p} H^1(P \rtimes H, \mathcal{V}) \leq \delta_{\mathcal{V}}$.

Proof. It is quite clear that (i) implies (ii) : a H -epimorphism $F_\gamma \twoheadrightarrow P$ provides a continuous group epimorphism $F_\gamma \rtimes H \twoheadrightarrow P \rtimes H$, and the beginning of the corresponding inflation-restriction sequence for \mathcal{V} :

$$0 \rightarrow H^1(P \rtimes H, \mathcal{V}) \rightarrow H^1(F_\gamma \rtimes H, \mathcal{V}) \rightarrow \dots$$

allows to conclude that (ii) holds.

To see that (ii) implies (i) first notice that, as in the remark above, $\dim_{\mathbb{F}_p} H^1(P \rtimes H, \mathcal{V}) = \dim_{\mathbb{F}_p} \text{Hom}_H(P/\Phi(P), \mathcal{V})$. Moreover, since H is a p' -group, the ring $\mathbb{F}_p[H]$ is semi-simple, and for any $\mathbb{F}_p[H]$ -module of finite type, $\dim_{\mathbb{F}_p} \text{Hom}_H(M, \mathcal{V})$ is

exactly $\deg \mathcal{V}$ times the multiplicity of \mathcal{V} in M . From this and (ii) we deduce the existence of a surjective H -map $F_\gamma/\Phi(F_\gamma) \twoheadrightarrow P/\Phi(P)$, and so the existence of a group epimorphism $F_\gamma \rtimes H \twoheadrightarrow P/\Phi(P) \rtimes H$. Consider now the embedding problem :

$$\begin{array}{ccccccc}
 & & & & F_\gamma \rtimes H & & \\
 & & & & \downarrow & & \\
 & & & & \swarrow & & \\
 1 & \longrightarrow & \Phi(P) & \longrightarrow & P \rtimes H & \longrightarrow & P/\Phi(P) \rtimes H \longrightarrow 1
 \end{array}$$

According to [15], Chapitre I, §4.2, Proposition 24, Corollaire 2, et §3.3, Proposition 14, we certainly have $\text{cd}_p(F_\gamma \rtimes H) \leq 1$. Hence (see 2.1.4) this embedding problem has a weak solution $F_\gamma \rtimes H \twoheadrightarrow P \rtimes H$. This arrow commutes with projection on H , so we get a similar diagram without H 's, but for continuous H -morphisms. Now a classical argument (the Frattini subgroup $\Phi(P)$ is precisely the set of non-generators in P) shows that the map $F_\gamma \twoheadrightarrow P$ must be an epimorphism. \square

Remark : One can of course ask if the $\delta_{\mathcal{V}}$'s do characterize the action of H on F_γ . We have no answer.

4.2. Geometric application. Let now $Y \rightarrow X$ be a Galois étale cover of curves with Galois group H , a p' -group. By pushing the exact sequence $0 \rightarrow \pi_1(Y) \rightarrow \pi_1(X) \rightarrow H \rightarrow 0$ via the map $\pi_1(Y) \twoheadrightarrow \pi_1^{(p)}(Y)$ we obtain a split exact sequence (because $\text{cd}_p H = 0$) which shows that H acts naturally on $\pi_1^{(p)}(Y)$. Since this group is known to be pro- p -free of rank γ_Y (the classical Hasse-Witt invariant of Y), we can apply the result of the previous paragraph, with $\gamma = \gamma_Y$.

It is easy to see that Proposition 4.2 is equivalent to theorem 1.1. The main point is that $F_\gamma/\Phi(F_\gamma) \simeq H^0(Y, \Omega_Y)^C$, which allows to see that if $V \in \mathcal{S}_{k[H]}$, $\mathcal{V} \in \mathcal{S}_{\mathbb{F}_p[H]}$ are such that $V|\mathcal{V}$, then the $\delta_{\mathcal{V}}$'s of the previous paragraph coincide with our former $\delta_{Y,V}$'s.

REFERENCES

- [1] Alperin, J. L : Local representation theory. Cambridge Studies in Advanced Mathematics, 11. Cambridge University Press, Cambridge, 1986.
- [2] Benson, D. J. : Representations and cohomology. I. Basic representation theory of finite groups and associative algebras. Cambridge Studies in Advanced Mathematics, 30. Cambridge University Press, Cambridge, 1998.
- [3] Benson, D. J. : Representations and cohomology. II. Cohomology of groups and modules. Cambridge Studies in Advanced Mathematics, 31. Cambridge University Press, Cambridge, 1998.
- [4] Bouw, I. : The p -rank of ramified covers of curves. *Compositio Math.* 126 (2001), no. 3, 295–322.
- [5] Crew, R. : Etale p -covers in characteristic p . *Compositio Math.* 52 (1984), no. 1, 31–45.
- [6] Hochschild, G.; Serre, J.-P : Cohomology of group extensions. *Trans. Amer. Math. Soc.* 74, (1953), 110–134.
- [7] Huppert, B; Blackburn, N : Finite groups. II. *Grundlehren der Mathematischen Wissenschaften*, 242, Springer-Verlag, Berlin-New York, 1982.
- [8] Kani, E. : The Galois-module structure of the space of holomorphic differentials of a curve. *J. reine angew. Math.* 367 (1986), 187-206.
- [9] Milne, J. *Etale cohomology*. Princeton Mathematical Series, 33. Princeton University Press, Princeton, N.J., 1980.
- [10] Nakajima, S : On generalized Hasse-Witt invariants of an algebraic curve. *Galois groups and their representations* (Nagoya, 1981), 69–88, *Adv. Stud. Pure Math.*, 2, North-Holland, Amsterdam, 1983.
- [11] Nakajima, S : Equivariant form of the Deuring-Safarevič formula for Hasse-Witt invariants. *Math. Z.* 190 (1985), no. 4, 559–566.
- [12] Pacheco, A ; Stevenson, K. : Finite quotients of the algebraic fundamental group of projective curves in positive characteristic. *Pacific J. Math.* 192 (2000), no. 1, 143–158.
- [13] Raynaud, M. : Revêtements des courbes en caractéristique $p > 0$ et ordinarité. *Compositio Math.* 123 (2000), no. 1, 73–88.
- [14] Serre, J-P : Sur la topologie des variétés algébriques en caractéristique p . *Œuvres*, Vol. I (1949–1959), 38, 501–530. Springer-Verlag, Berlin, 1986.
- [15] Serre, J-P : *Cohomologie galoisienne*. Fifth edition. *Lecture Notes in Mathematics*, 5. Springer-Verlag, Berlin, 1994.
- [16] Tamme, G : *Introduction to étale cohomology*. Universitext. Springer-Verlag, Berlin, 1994.

- [17] Zhang, Bin : Revêtements étales abéliens de courbes génériques et ordinarité. Ann. Fac. Sci. Toulouse Math. (6) 1 (1992), no. 1, 133–138.

UNIVERSITÀ DI BOLOGNA, DIPARTIMENTO DI MATEMATICA, PIAZZA DI PORTA SAN DONATO, 5, I-40126 BOLOGNA, ITALY

E-mail address: borne@dm.unibo.it