Covers of $\mathbb{P}^1$ over the p-adics

Abstract. Given a field K, the regular inverse Galois problem over K consists in showing that each finite group G is the Galois group of a regular extension of $K(T)$, or equivalently, to finding a G-cover of $\mathbb{P}^1$ of group G defined over K. Generalizing [DeFr], we solve the regular inverse Galois problem over the field of totally p-adic numbers for each prime p and give a criterion for the descent from the totally real number field to $\mathbb{Q}$. The second half of the paper is concerned with "local-to-global" questions. We show that a G-cover defined over $\mathbb{Q}_p$ for all primes p is necessarily defined over $\mathbb{Q}$ (Dew's conjecture). Also related to a question of Dew, our last result asserts that if K is a number field and is the field of moduli of a (G-)cover, then only for finitely many primes $\mathfrak{p}$ may the completion $K_\mathfrak{p}$ of K not be a field of definition.

1. Introduction

This paper is concerned with the regular form of the inverse Galois problem : does each finite group G occur as the Galois group of a regular extension $E/\mathbb{Q}(T)$? Recall that the word "regular" means that the field $\mathbb{Q}$ should be algebraically closed in E, *i.e.*, $E \cap \overline{\mathbb{Q}} = \mathbb{Q}$. The problem has a geometric formulation. Classically a G-cover is a Galois cover $f : X \to \mathbb{P}^1$ given together with its automorphisms (Cf. §2.1). Then the problem amounts to finding a G-cover defined over $\mathbb{Q}$ as a G-cover and with G as automorphism group.

More generally, the regular inverse Galois problem can be considered over an arbitrary field K : does each finite group occur as the automorphism group of a G-cover defined over K ? Throughout this paper we assume that K is of characteristic 0. We will only consider covers defined *a priori* over $\overline{K}$, which is equivalent to requiring that the branch points be in $\overline{K}$. Thus, the problem is a descent problem, namely the descent of the field of definition of G-covers from $\overline{K}$ to K. A second question then immediately arises, in fact the second stage of the original problem, which is concerned with the descent from K to $\mathbb{Q}$: find criteria for descending the field of definition of a G-cover *a priori* defined over K.

We will discuss these questions when $K = \mathbb{Q}_p$ is the field of p-adic numbers and $K = \mathbb{Q}^{tp}$ is the field of totally p-adic numbers, that is, the subfield of $\overline{\mathbb{Q}}$ (viewed as

1991 *Mathematics Subject Classification.* Primary 12F12, 14H30 ; Secondary 14G20, 11Gxx.

This paper is in final form and no version of it will be submitted elsewhere.

a subfield of $\overline{\mathbb{Q}_p}$) consisting of all algebraic numbers such that all conjugates over $\mathbb{Q}$ are p-adic. This includes the prime p at infinity; in that case, "p-adic" should be understood as "real" and $\mathbb{Q}^{tp}$ is denoted by $\mathbb{Q}^{tr}$. The definition of $\mathbb{Q}^{tp}$ does not depend on the choice of an embedding $\mathbb{Q}_p \hookrightarrow \overline{\mathbb{Q}_p}$. This makes the field $\mathbb{Q}^{tp}$ a more intrinsic subfield of $\overline{\mathbb{Q}}$ than $\mathbb{Q}_p \cap \overline{\mathbb{Q}}$.

After some preliminaries in §2 (notation, etc.), we show in §3 that given any prime p, each group is a Galois group over $\mathbb{Q}^{tp}(T)$ (Th.3.1). The proof generalizes the one given in [DeFr] for the special case $p = \infty$. Recently F. Pop has obtained new results which contain Th.3.1 [Po3] : $\mathbb{Q}^{tp}$ can even be replaced by any finite intersection of $\mathbb{Q}^{tp}$s. Both our approach and his rely on patching and glueing techniques introduced by D. Harbater [Har] for formal analytic covers and revisited by Q. Liu [Li] from the rigid point of view. The Hurwitz space theory is the other important tool of our proof.

The following §4 is concerned with the second stage of the descent. Th.4.1, a special case of [De2], is a criterion for a G-cover *a priori* defined over $\mathbb{Q}^{tr}$ and with $\mathbb{Q}$-rational branch points to be defined over $\mathbb{Q}$. We note that the extra condition "with $\mathbb{Q}$-rational branch points" forbids at the moment to combine Th.3.1 and Th.4.1.

The rest of the paper is devoted to "local-to-global" questions. In his thesis, E. Dew conjectures that a G-cover defined over all the completions of a number field K is necessarily defined over K. In §7 we prove that Dew's conjecture holds except possibly in a very special case coming from Grunwald's theorem (Th.7.1). This special case cannot occur if $K = \mathbb{Q}$. I am very much indebted to J-C. Douai for a decisive contribution to the proof.

If a (G-)cover is only defined over all but finitely many completions of K, then only the field of moduli has to be equal to K. In §8 we show that the converse holds as well : only for finitely many primes $\mathfrak{p}$ may the completion $K_\mathfrak{p}$ of the field of moduli K not be a field of definition (Th.8.1). This result also originated in a question of E. Dew. Th.7.1 and Th.8.1 are related to the classical problem of studying the obstruction for the field of moduli to be a field of definition. The appropriate definitions and the necessary tools to prove these results are presented in §5 and §6.

2. Preliminaries

2.1. Covers and G-covers over a field K. Given a field K, by "cover over K" we mean a flat and finite morphism $f : X \to \mathbb{P}^1_K$ with X a smooth projective curve over K. By "G-cover of group G over K" we mean a Galois cover $f : X \to \mathbb{P}^1_K$ over K given together with an isomorphism $h : G \to G(K(X)/K(T))$ (where T is the generic point of $\mathbb{P}^1$). Note that the "G" of "G-cover" is the capital letter G which indicates that the Galois action is part of the data. This "G" is not the name of the group; in the phrase "G-cover of group G", the name of the group is G (italicized). We use the words "cover" and "G-cover" alone (without specifying the base field K) only when the base field is algebraically closed. We use the word "(G-)cover" in statements holding for both covers and G-covers. Isomorphisms of covers are defined in the classical way. Isomorphisms of G-covers are defined as follows. An isomorphism χ between two G-covers of group G is an isomorphism of covers that commutes with the given actions of G (*i.e.*, with notation as above, such that $h'(g)(x') \circ \chi = h(g)(x' \circ \chi)$ for all $g \in G$ and all $x' \in K(X')$). If L/K is a field

extension and f is a (G-)cover over K, the (G-)cover over L obtained from f by extension of scalars is denoted by $f \otimes_K L$. Two (G-)covers $f_i : X_i \to \mathbb{P}_{K_i}$ over K_i, $i = 1, 2$, are said to be isomorphic if both covers $f_1 \otimes_{K_1} \overline{K_1K_2}$ and $f_2 \otimes_{K_2} \overline{K_1K_2}$ are isomorphic.

2.2. Invariants of a cover. A cover $f : X \to \mathbb{P}^1$ (over an algebraically closed field $k \subset \mathbb{C}$) has three basic invariants, which only depend on the isomorphism class of the cover. First the *group* G of the cover, *i.e.*, the monodromy group of the cover $f \otimes_k \mathbb{C}$, or, equivalently, the automorphism group of the Galois closure $\hat{f} : \widehat{X} \to \mathbb{P}^1$ of f, or, also, the Galois group $G(k(\widehat{X})/k(T))$. Second, the *branch point set* $\{t_1, \dots, t_r\}$ of the cover, which will be denoted by $\{\mathbf{t}(f)\}$. Third, the *inertia canonical invariant* of the cover. Recall the definition of the latter. To each branch point t_i, $i = 1, \dots, r$, can be associated a conjugacy class C_i of the group G in the following way. The inertia groups of $\hat{f}$ above t_i are cyclic congugate groups of order equal to the ramification index e_i. Furthermore each of them has a distinguished generator corresponding to the automorphism $(T - t_i)^{1/e_i} \to e^{2i\pi/e_i}(T - t_i)^{1/e_i}$ of $\mathbb{C}(((T - t_i)^{1/e_i}))$. Then C_i is the conjugacy class of all the distinguished generators of the inertia groups above t_i. The inertia canonical invariant of $f : X \to \mathbb{P}^1$ is defined to be the unordered r-tuple $\mathbf{C} = (C_1, \dots, C_r)$. By invariants of a (G-)cover f over a non algebraically closed field k, we always mean the invariants of the cover $f \otimes_k \overline{k}$.

2.3. K-arithmetic fundamental group [Se2 ;Ch.6]**.** The open subset of $(\mathbb{P}^1)^r$ (resp. of $\mathbb{P}^r$) consisting of ordered r-tuples (resp. unordered r-tuples) $(t_1, \dots, t_r)$ with no two equal coordinates is denoted by U^r (resp. by U_r). Given a r-tuple $\mathbf{t} = (t_1, \dots, t_r) \in U_r(K)$, the *$K$-arithmetic fundamendal group* of $\mathbb{P}^1 \backslash \{\mathbf{t}\}$ is denoted by $\Pi_{K,\mathbf{t}}$. It can be defined in the following way. Fix an algebraic closure $\overline{K(T)}$ of $K(T)$. If $\Omega_{\mathbf{t}} \subset \overline{K(T)}$ is the maximal algebraic extension of $\overline{K}(T)$ unramified above $\mathbb{P}^1 \backslash \{t_1, \dots, t_r\}$, then $\Pi_{K,\mathbf{t}}$ is the Galois group of the extension $\Omega_{\mathbf{t}}/K(T)$. The $\overline{K}$-arithmetic fundamental group $\Pi_{\overline{K},\mathbf{t}}$ is also called the *geometrical fundamental group*. From Riemann's existence theorem, the group $\Pi_{\overline{K},\mathbf{t}}$ is the profinite completion of the topological fundamental group of $\mathbb{P}^1 \setminus \{\mathbf{t}\}$. The latter has a classical presentation given by r generators $x_1, \dots, x_r$ and the one relation $x_1 \cdots x_r = 1$. Furthermore the exact sequence

$$1 \to \Pi_{\overline{K},\mathbf{t}} \to \Pi_{K,\mathbf{t}} \to G_K \to 1 \tag{1}$$

splits. More precisely, to each rational base point $t_o \in \mathbb{P}^1(K) \setminus \{\mathbf{t}\}$ corresponds a section $s_{t_o} : G_K \to \Pi_{K,\mathbf{t}}$ obtained by embedding function fields of covers in $\overline{K}((T - t_o))$. The section s_{t_o} is well-defined up to conjugation by an element of $\Pi_{\overline{K},\mathbf{t}}$ (which corresponds to the choice of an embedding in $\overline{K}((T - t_o))$).

2.4. Dictionary "covers/homomorphisms". (G-)covers over K essentially correspond to representations of K-arithmetic fundamental groups. We review this dictionary which transforms the question of descending the field of definition into the question of extending group homomorphisms. Let $\mathbf{t} = (t_1, \dots, t_r) \in U_r(K)$.

2.4.1. Covers. To a degree d cover $f : X \to \mathbb{P}^1$ over K with branch points in $\{\mathbf{t}\}$ can be associated a transitive representation

$$\phi : \Pi_{K,\mathbf{t}} \to S_d$$

such that the restriction to $\Pi_{\overline{K},\mathbf{t}}$ is transitive. Conversely to such a representation can be associated a cover as above. These correspondences, which we briefly recall below, are non-canonical. But they induce canonical one-one correspondences, inverse the one to another, between isomorphism classes, when K is algebraically closed. More specifically, two covers f and f' are isomorphic if and only if the corresponding representations ϕ and ϕ' are conjugate by an element $\varphi \in S_d$, *i.e.*,

$$\phi'(x) = \varphi\phi(x)\varphi^{-1} \text{ for all } x \in \Pi_{\overline{K},\mathbf{t}} \tag{2}$$

Via this dictionary, the group of the cover is $G = \phi(\Pi_{\overline{K},\mathbf{t}})$. The inertia canonical invariant of the cover is the r-tuple of conjugacy classes in the group G of the r elements $\phi(x_1), \dots, \phi(x_r)$.

[**Correspondences.** Let $t_o \in \mathbb{P}^1(K) \setminus \{\mathbf{t}\}$. Fix an embedding $\Omega_{\mathbf{t}} \hookrightarrow \overline{K}((T - t_o))$. A degree d cover $f : X \to \mathbb{P}^1$ over K with branch points in $\{\mathbf{t}\}$ given with a point on X above t_o corresponds, via the functor "function fields" to a specific finite subextension of $\Omega_{\mathbf{t}}/K(T)$, *i.e.*, via Galois theory, to a specific subgroup H of $\Pi_{K,\mathbf{t}}$. Label the left cosets of $\Pi_{K,\mathbf{t}}$ modulo H by the integers $1, \dots, d$ in such a way that H corresponds to 1. The action of $\Pi_{K,\mathbf{t}}$ by left multiplication on the left cosets of $\Pi_{K,\mathbf{t}}$ modulo H provides a representation $\phi : \Pi_{K,\mathbf{t}} \to S_d$ as above.

Conversely, given such a representation, denote the stabilizer of 1 in the representation $\phi : \Pi_{K,\mathbf{t}} \to S_d$ by $\Pi_{K,\mathbf{t}}(1)$. Consider the fixed field $E = \Omega_{\mathbf{t}}^{\Pi_{K,\mathbf{t}}(1)}$ of $\Pi_{K,\mathbf{t}}(1)$ in $\Omega_{\mathbf{t}}$. Then the extension $E\overline{K}/\overline{K}(T)$ is the function field extension associated to a degree d cover $\bar{f} : \bar{X} \to \mathbb{P}^1$. Furthermore this cover is defined over K, *i.e.*, is isomorphic to a cover $f : X_K \to \mathbb{P}^1_K$ over K.]

2.4.2. G-covers. To a G-cover f over K of group G and with branch points in $\{\mathbf{t}\}$ can be associated a surjective homomorphism

$$\phi : \Pi_{K,\mathbf{t}} \to G$$

such that $\phi(\Pi_{\overline{K},\mathbf{t}}) = G$. Conversely to such an homomorphism can be associated a G-cover as above. These (non-canonical) correspondences induce canonical one-one correspondences, inverse the one to another, between isomorphism classes, when K is algebraically closed. More specifically, two G-covers f and f' are isomorphic if and only if the corresponding representations ϕ and ϕ' are conjugate by an element $\varphi \in G$, *i.e.*,

$$\phi'(x) = \varphi\phi(x)\varphi^{-1} \text{ for all } x \in \Pi_{\overline{K},\mathbf{t}} \tag{3}$$

[**Correspondences.** A G-cover $f : X \to \mathbb{P}^1$ over K of group G and with branch points in $\{\mathbf{t}\}$ corresponds, via the functor "function fields" to a specific finite Galois subextension of $\Omega_{\mathbf{t}}/K(T)$, *i.e.*, via Galois theory, to a specific normal subgroup H of $\Pi_{K,\mathbf{t}}$. The group $\Pi_{K,\mathbf{t}}/H$ is canonically identified with the Galois group $G(K(X)/K(T))$. Composing the natural surjection $\Pi_{K,\mathbf{t}} \to \Pi_{K,\mathbf{t}}/H$ with the given isomorphism $G(K(X)/K(T) \to G$ provides a surjective homomorphism $\phi : \Pi_{K,\mathbf{t}} \to G$ as above.

Conversely, given such an homomorphism, consider the fixed field $E = \Omega_{\mathbf{t}}^{Ker(\phi)}$ of $Ker(\phi)$ in $\Omega_{\mathbf{t}}$. Then the extension $E\overline{K}/\overline{K}(T)$ is the function field extension associated to a Galois cover $f : X \to \mathbb{P}^1$ of group $\Pi_{K,\mathbf{t}}/Ker(\phi)$. Furthermore this cover is defined and Galois over K, *i.e.*, is isomorphic to a Galois cover $f_K : X_K \to \mathbb{P}^1_K$ over K. The isomorphism $\Pi_{K,\mathbf{t}}/Ker(\phi) \to G$ endows f_K with a structure of G-cover over K.]

2.5. Galois action. Given a field K, the absolute Galois group $G(\overline{K}/K)$ of K is denoted by G_K.

2.5.1. Galois action on (G-)covers. The Galois group G_K has a natural action on varieties over $\overline{K}$; in particular, G_K acts on (G-)covers of $\mathbb{P}^1$ over $\overline{K}$. Let $f : X \to \mathbb{P}^1$ be a (G-)cover and $\tau \in G_K$. The corresponding conjugate cover will be denoted by $f^\tau : X^\tau \to \mathbb{P}^1$. If the three invariants of the cover f are G, $\{\mathbf{t}\} = \{t_1, \ldots, t_r\}$ and $\mathbf{C} = (C_1, \ldots, C_r)$, then the three invariants of the cover f^τ are respectively G, $\{\mathbf{t}^\tau\} = \{t_1^\tau, \ldots, t_r^\tau\}$ and $\mathbf{C}^{\chi(\tau)} = (C_1^{\chi(\tau)}, \ldots, C_r^{\chi(\tau)})$ where $\chi : G_K \to \mathbb{Z}/|G|\mathbb{Z}$ is the cyclotomic character of K modulo the order of the group G. Assume now that the cover f (resp. G-cover f) corresponds to the homomorphism $\phi : \Pi_{\overline{K},\mathbf{t}} \to S_d$ (resp. $\phi : \Pi_{\overline{K},\mathbf{t}} \to G$). Fix a rational base point $t_o \in \mathbb{P}^1(K) \setminus \{\mathbf{t}\}$ and consider the homomorphism $\phi^\tau : \Pi_{\overline{K},\mathbf{t}} \to S_d$ (resp. $\phi^\tau : \Pi_{\overline{K},\mathbf{t}} \to G$) defined by

$$\phi^\tau(x) = \phi(x^{s_{t_o}(\tau)}) \text{ for all } x \in \Pi_{\overline{K},\mathbf{t}} \tag{4}$$

where $x^{s_{t_o}(\tau)} = s_{t_o}(\tau)x(s_{t_o}(\tau))^{-1}$. Then the homomorphism ϕ^τ corresponds to a cover (resp. a G-cover) that is isomorphic (over $\overline{K}$) to the cover f^τ (resp. to the G-cover f^τ).

2.5.2. Galois action on unramified fibers. If $f : X \to \mathbb{P}^1$ is a cover over K, by "fiber" of the cover f we always mean geometric fiber, *i.e.*, the corresponding fiber of the cover $f \otimes_K \overline{K}$. The following result will be used several times.

Proposition 2.1 — *Let $f : X \to \mathbb{P}^1_K$ be a cover over K and $\phi : \Pi_{K,\mathbf{t}} \to S_d$ be the associated homomorphism. Let $t_o \in \mathbb{P}^1(K) \setminus \{\mathbf{t}\}$. Then for each $\tau \in G_K$, the permutation $\phi(s_{t_o}(\tau))$ is conjugate in S_d to the permutation ω_τ induced by the action of τ on the fiber $f^{-1}(t_o)$.*

Proof. Denote the stabilizer of 1 in the representation $\phi : \Pi_{K,\mathbf{t}} \to S_d$ by $\Pi_{K,\mathbf{t}}(1)$. Then the extension of function fields (over K) associated to the cover $f : X \to \mathbb{P}^1$ is the extension $E/K(T)$ where $E = \Omega_{\mathbf{t}}^{\Pi_{K,\mathbf{t}}(1)}$ is the fixed field of $\Pi_{K,\mathbf{t}}(1)$ in $\Omega_{\mathbf{t}}$. Select d representatives $\xi_1, \ldots, \xi_d$ of the left cosets of $\Pi_{K,\mathbf{t}}$ modulo $\Pi_{K,\mathbf{t}}(1)$ in such a way that $\phi(\xi_i)(1) = i$, $i = 1, \ldots, d$. Then for all $x \in \Pi_K$ and for any two indices $i, j \in \{1, \ldots, d\}$, we have

$$\phi(x)(i) = j \Longleftrightarrow \xi_j^{-1}(x\xi_i) \in \Pi_{K,\mathbf{t}}(1) \tag{5}$$

Let $\tau \in G_K$. In order to compute the permutation ω_τ, we pick a primitive element y_1 of the extension $E/K(T)$. Set $y_i = y_1^{\xi_i}$, $i = 1, \ldots, d$. By definition of E, the conjugates of y_1 over $K(T)$ are the d distinct elements $y_1, \ldots, y_d$, $i = 1, \ldots, d$.

Since t_o is not a branch point of f, the field $K(T, y_1, \dots, y_d)$ can be embedded in $\overline{K}((T - t_o))$. The permutation ω_τ is then equal, up to conjugation in S_d, to the permutation induced by τ on the formal power series $y_1, \dots, y_d$. But this action of τ on coefficients of power series corresponds precisely to the element $s_{t_o}(\tau) \in \Pi_{K,\mathbf{t}}$. Consequently we obtain :

$$\omega_\tau(i) = j \Leftrightarrow y_i^{s_{t_o}(\tau)} = y_j \Leftrightarrow (y_1^{\xi_i})^{s_{t_o}(\tau)} = y_1^{\xi_j} \Leftrightarrow \xi_j^{-1}(s_{t_o}(\tau)\xi_i) \in \Pi_{K,\mathbf{t}}(1)$$

which, in view of (5), completes the proof. □

3. Descent from $\overline{\mathbb{Q}}$ to $\mathbb{Q}^{tp}$

3.1. Statement of the results. This section is aimed at proving this result.

THEOREM 3.1 — *Let p be a prime (possibly $p = \infty$). Then each finite group is the automorphism group of a G-cover defined over $\mathbb{Q}^{tp}$, or, equivalently, the Galois group of a regular extension of $\mathbb{Q}^{tp}(T)$.*

When p is the prime at infinity, this result is due to M. Fried and myself [DeFr]. Galois properties of the field $\mathbb{Q}^{tr}$ were also investigated by M. Fried, D. Haran and H. Völklein who gave a precise description of the absolute Galois group $G(\overline{\mathbb{Q}^{tr}}/\mathbb{Q}^{tr})$ [FrHaVö]. A more general result on $G(\overline{\mathbb{Q}^{tp}}/\mathbb{Q}^{tp})$ with p an arbitrary prime was more recently obtained by F. Pop [Po3]. Here we explain how the proof of [DeFr] extends to finite primes. Like in [DeFr] the proof has two stages : from $\overline{\mathbb{Q}}$ to $\overline{\mathbb{Q}} \cap \mathbb{Q}_p$ first, then from $\overline{\mathbb{Q}} \cap \mathbb{Q}_p$ to $\mathbb{Q}^{tp}$. The second stage can be worked out similarly for finite primes and for $p = \infty$. Only the first stage is specific to each case : for finite primes, it relies on Harbater's techniques which replace Debes-Fried's result on the complex conjugation used in [DeFr].

The following definition plays an important role in the proof of Th.3.1 and in many other places of this paper.

DEFINITION 3.2 — *Let $f_K : X_K \to \mathbb{P}^1_K$ be a cover over K. A fiber $f_K^{-1}(t_o)$ with $t_o \in \mathbb{P}^1(K)$ is said to be totally rational if it consists only of K-rational points on X_K. A (G)-cover $f : X \to \mathbb{P}^1$ is said to be definable over K with a totally rational fiber above t_o if there exists a $(G$-$)$cover $f_K : X_K \to \mathbb{P}^1_K$ over K with a totally rational fiber above t_o and such that the $(G$-$)$covers f_K and f are isomorphic.*

The first stage consists in proving the following result. Recall that an unordered r-tuple $(C_1, \dots, C_r)$ of conjugacy classes of a group G is said to be *rational* if, for all integers m relatively prime to the order of G, we have $(C_1, \dots, C_r) = (C_1^m, \dots, C_r^m)$ as unordered r-tuples(*).

(*) The special case r=1 corresponds to the more classical notion of rational conjugacy class.

LEMMA 3.3 — *Let p be a prime, G be a finite group and $b > 0$ be an integer. Then there exists a G-cover $f : X \to \mathbb{P}^1$ with the following properties.*
(1) The G-cover f is definable over $\mathbb{Q}_p$ with a totally rational fiber above a point $t_o \in \mathbb{P}^1(K) \setminus \{\mathbf{t}(f)\}$.
(2) The automorphism group $Aut(f)$ of the cover f is G.
(3) The inertia canonical invariant of f is a rational tuple $\mathbf{C}$ of conjugacy classes of G.
(4) Each conjugacy class of G appears at least b times in the inertia canonical invariant $\mathbf{C}$ of f.

3.2. Harbater's "patching and glueing" result [Har]**.** The proof of Lemma 3.3 divides into two cases, depending on whether $p = \infty$ or p is finite. We refer to [DeFr ;§5.3] for the first case. The finite case rests on the following Harbater's result.

THEOREM 3.4 (Harbater) — *Let G be a finite group and H_1 and H_2 be two subgroups of G generating G (i.e., $G =< H_1, H_2 >$). For $j = 1, 2$, let $f_j : X_j \to \mathbb{P}^1$ be a G-cover defined over $\mathbb{Q}_p$, of group H_j, with r_j branch points and with inertia canonical invariant the r_j-tuple $\mathbf{C}_j = (C_{j1}, \ldots, C_{jr_j})$. Assume in addition that*

(5) For $j = 1, 2$, f_j has a totally rational fiber above a point $t_{oj} \in \mathbb{P}^1(\mathbb{Q}_p) \setminus \{\mathbf{t}(f_j)\}$.

Then there exists a G-cover $f : X \to \mathbb{P}^1$ defined over $\mathbb{Q}_p$ with a totally rational fiber above a point $t_o \in \mathbb{P}^1(\mathbb{Q}_p) \setminus \{\mathbf{t}(f)\}$, of group G, with $r = r_1 + r_2$ branch points and inertia canonical invariant the r-tuple $\mathbf{C} = (C^G_{11}, \ldots, C^G_{1r_1}, C^G_{21}, \ldots, C^G_{2r_2})$ where C^G_{ji} is the conjugacy class in the group G of elements of C_{ji}, $j = 1, 2$, $i = 1, \ldots, r_j$.

Th.3.4 is slightly more precise than Harbater's statement but can be easily deduced from his construction. Harbater's original proof uses formal analytic geometry. In a short note [Li], Liu gave another proof of Th.3.4 using rigid analytic geometry instead. We briefly sketch Liu's method and explain how to obtain the extra conclusions, in particular, the one relative to the inertia canonical invariant of the cover f.

Sketch of proof. Assumption (5) insures that, for $j = 1, 2$, one can find a small disk O_j about t_{oj} with the following properties :
(i) $f_j^{-1}(\overline{O_j})$ is isomorphic as rigid analytic space over $\mathbb{Q}_p$ to the disjoint union of $d_j = |H_j|$ copies of $\overline{O_j}$(**).
(ii) $f_j^{-1}(\mathbb{P}^1 \setminus O_j)$ is connected.

Set $D_j = \mathbb{P}^1 \setminus \overline{O_j}$ and $\partial D_j = \overline{D_j} \setminus D_j$, $j = 1, 2$. It follows from (i) that the branch points of f_j are in D_j and that $f_j^{-1}(\partial D_j)$ is isomorphic over $\mathbb{Q}_p$ to the disjoint union of $d_j = |H_j|$ copies of ∂D_j, $j = 1, 2$.

One may assume that $\overline{D_1} \cap \overline{D_2} = \emptyset$: otherwise replace f_j by $\chi_j \circ f_j$ with χ_j a suitable automorphism of $\mathbb{P}^1$, $j = 1, 2$. Then consider the three following analytic spaces U_o, U_1 and U_2, which are formed from local pieces of X_1 and X_2 :

- U_o consists of $d = |G|$ disjoint copies of $\mathbb{P}^1 \setminus D_1 \cup D_2$. Note that each of these copies contains one copy of ∂D_1 and one copy of ∂D_2.

(**) As usual, if O is a disk, $\overline{O}$ is the associated closed disk

- U_1 consists of d/d_1 copies of $f_1^{-1}(\overline{D_1})$. Note that each of these copies contains d_1 copies of ∂D_1.

- U_2 consists of d/d_2 copies of $f_2^{-1}(\overline{D_2})$. Note that each of these copies contains d_2 copies of ∂D_2.

Thanks to a general result on analytic spaces, U_o, U_1 and U_2 can be patched and glued to provide a new analytic space X over $\mathbb{Q}_p$. A cover $f : X \to \mathbb{P}^1$ is then easily defined by $f = Id$ on U_o and $f = f_i$ on U_i, $i = 1, 2$. More specifically, U_o is glued, on one hand, to U_1 along the d common copies of ∂D_1 and, on the other hand, to U_2 along the d common copies of ∂D_2. Furthermore, by using a clever labeling of the different copies of ∂D_1 and ∂D_2, Harbater shows that this can be done in such a way that

(a) the resulting space X is connected.

(b) there exists a natural action of G on X which yields an identification $Aut(f) \simeq G$ for which the subgroup H_i of G corresponds to the automorphism group of each of the covers $f_j^{-1}(D_j) \to D_j$, $j = 1, 2$.

From an analog of the GAGA theorem, the resulting analytic cover is still an algebraic cover over $\mathbb{Q}_p$. Clearly this cover has totally rational fibers above any point $\mathbb{Q}_p$-rational point t_o of $\mathbb{P}^1 \setminus D_1 \cup D_2$.

Finally we have

$$\{\mathbf{t}(f)\} = \chi_1(\{\mathbf{t}(f_1)\} \cup \chi_2(\{\mathbf{t}(f_2)\})$$

Let P be a point on X above a branch point of f. The local ring at P is the local ring at some point on $f_j^{-1}(D_j) \subset X_j$, for $j = 1$ or $j = 2$. Therefore, the inertia groups of both these points are the same. In view of the definition of the inertia canonical invariant (§2.2), this completes the proof. □

3.3. Proof of Lemma 3.3. For each element $g \in G$, $g \neq 1$, use Lemma 2.1 of [Har] (or Lemme 1 of [Li]) to construct a G-cover $f_g : X_g \to \mathbb{P}^1$ over $\mathbb{Q}_p$, of group $< g >$ and with a totally rational fiber above a point $t_{g,o} \in \mathbb{P}^1(\mathbb{Q}_p) \setminus \{\mathbf{t}_g\}$ (where $\{\mathbf{t}_g\} = \{\mathbf{t}(f_g)\}$). Consider the associated homomorphism $\phi_g : \Pi_{\mathbb{Q}_p, \mathbf{t}_g} \to < g >$. Set $s_g = s_{t_{g,o}}$. It follows from Prop.2.1 that

$$s_g(G_{\mathbb{Q}_p}) \subset Ker(\phi_g)$$

Now if n_g is the order of g and $k \in (\mathbb{Z}/n_g\mathbb{Z})^\times$ is any unit of $\mathbb{Z}/n_g\mathbb{Z}$, the kth power ϕ_g^k of ϕ_g is still a homomorphism because its image lies in $< g >$, which is abelian. Furthermore $\phi_g^k : \Pi_{\mathbb{Q}_p, \mathbf{t}_g} \to < g >$ is still surjective and satisfies

$$s_g(G_{\mathbb{Q}_p}) \subset Ker(\phi_g^k)$$

Denote the associated G-cover by $f_g^{(k)}$.

Next, for each $g \in G \setminus \{1\}$ and each $k \in (\mathbb{Z}/n_g\mathbb{Z})^\times$, take b copies of the cover $f_g^{(k)}$. Finally use Th.3.4 to patch and glue all these covers together. It is readily checked that the resulting G-cover $f : X \to \mathbb{P}^1$ has the properties (1) and (2).

For each $g \in G \setminus \{1\}$ and each $k \in (\mathbb{Z}/n_g\mathbb{Z})^\times$, let $\mathbf{C}_g^{(k)}$ denote the inertia canonical invariant of $f_g^{(k)}$: $\mathbf{C}_g^{(k)}$ is a tuple with entries in $< g >$ (conjugacy classes of the cyclic group $< g >$ are trivial). Furthermore it has to contain at least one generator

of the cyclic group $< g >$. But then the element g itself necessarily appears in $\mathbf{C}_g^{(k')}$ for some $k' \in (\mathbb{Z}/n_g\mathbb{Z})^\times$. This proves condition (4). As for condition (3), *i.e.*, the rationality of the inertia canonical invariant of f, it is an immediate consequence of the following formula : for each $g \in G \setminus \{1\}$ and all $k, k' \in (\mathbb{Z}/n_g\mathbb{Z})^\times$, we have

$$\left(\mathbf{C}_g^{(k)}\right)^{k'} = \left(\mathbf{C}_g^{(kk')}\right) \qquad \square \tag{6}$$

3.4. Second stage of Th.3.1. The second stage of the proof of Th.3.1 is the same for finite primes and for the prime at ∞. It makes use of the Hurwitz space theory for G-covers.

3.4.1. Hurwitz spaces for G-covers [FrVö]. Under the conditions "$Z(G) = \{1\}$" (*i.e.*, "G has trivial center") and "$\mathbf{C}$ is rational", Fried and Völklein showed the existence of a moduli space $\mathfrak{H}_G^{in}(\mathbf{C})$ for G-covers of group G and inertia canonical invariant equal to $\mathbf{C}$. More precisely, $\mathfrak{H}_G^{in}(\mathbf{C})$ is a smooth algebraic variety defined over $\mathbb{Q}$ with this property : G-covers of group G, with r branch points, with inertia canonical invariant equal to $\mathbf{C}$ and defined over a field k correspond to k-rational points on $\mathfrak{H}_G^{in}(\mathbf{C})$.

3.4.2. End of proof of Th.3.1. With no loss, we may assume that

(7) The group G has trivial center and commutators generate the Schur multiplier of G.

Indeed, from Lemma 2 of [FrVö], each finite group is the quotient of a group with this property. The next ingredient of the proof is Conway-Parker theorem [FrVö ;appendix]. Under condition (7), there exists an integer $b_o(G)$ with this property : if $\mathbf{C}$ is an r-tuple of conjugacy classes such that each conjugacy class of G appears at least $b_o(G)$ times in $\mathbf{C}$, then the Hurwitz space $\mathfrak{H}_G^{in}(\mathbf{C})$ is irreducible.

Applying Lemma 3.3 with $b = b_o(G)$ yields a G-cover $f : X \to \mathbb{P}^1$ with an inertia canonical invariant $\mathbf{C}$ satisfying the preceding property. So the associated Hurwitz space $\mathfrak{H} = \mathfrak{H}_G^{in}(\mathbf{C})$ is irreducible. Furthermore, from properties (1) and (3), $\mathfrak{H}$ is defined over $\mathbb{Q}$ and $\mathfrak{H}(\mathbb{Q}_p) \neq \emptyset$. Conclusion follows from this result of Pop ([PoRoGr] and [Po1]) : if X is a smooth variety defined over $\mathbb{Q}$, then $X(\mathbb{Q}^{tp}) \neq \emptyset$ provided that $X(\mathbb{Q}_p) \neq \emptyset$. (In fact, $X(\mathbb{Q}^{tp})$ is dense in $X(\mathbb{Q}_p)$). $\square$

4. Descent from K to $\mathbb{Q}$

4.1. From $\mathbb{Q}^{tr}$ to $\mathbb{Q}$. Th.4.1 is concerned with the descent from $\mathbb{Q}^{tr}$ to $\mathbb{Q}$. The basic idea is this. The action of complex conjugation c on covers of $\mathbb{P}^1$ can be explicitly described by some formulas due to Hurwitz that give the action of c on suitable generators of the topological fundamental group $\pi_1(\mathbb{P}^1 \setminus \{\mathbf{t}\}, t_o)$ ([Hur],[FrDe],[De2 ;display (3) p.867]). Being defined over $\mathbb{R}$ imposes to a G-cover certain group-theoretic constraints coming from these formulas. If a G-cover f is defined over $\mathbb{Q}^{tr}$, these Hurwitz constraints should be satisfied by all the conjugates of f. Under suitable conditions, these constraints are sufficiently sharp to imply that these conjugate covers are the same cover. More precisely, we proved the following result in [De2]. For simplicity, we restrict to the case where all the branch points are real.

THEOREM 4.1 — *Let $f : X \to \mathbb{P}^1$ be a G-cover of group G and with branch points r points $t_1, \dots, t_r \in \mathbb{P}^1(\mathbb{R})$ such that $t_1 < \dots < t_r$. Let C_i be the inertia cananical class associated to t_i, $i = 1, \dots, r$. Assume that the following holds.*

(1) The center of the group G is trivial.

(2) Each of the conjugacy class C_i is rational, $i = 1, \dots, r$.

(3) The G-cover f is defined over $\mathbb{Q}^{tr}$.

(4) The branch points $t_1, \dots, t_r$ of the cover are in $\mathbb{P}^1(\mathbb{Q})$.

(5) The action of G (by componentwise conjugation) on the set

$$sni(\mathbf{C}, r) = \left\{ (g_1, \dots, g_r) \in G^r \;\middle|\; \begin{array}{l} (i)\ g_1 \cdots g_r = 1 \\ (ii)\ < g_1, \dots, g_r >= G \\ (iii)\ g_i \in C_i, i = 1, \dots, r \\ (iv)\ \exists g_o \in G \text{such that} \left\{ \begin{array}{l} g_o^2 = 1 \\ (g_o g_1)^2 = 1 \\ \vdots \\ (g_o g_1 \cdots g_{r-1})^2 = 1 \end{array} \right. \end{array} \right\}$$

is transitive (*).

Then the G-cover f can be defined over $\mathbb{Q}$.

Condition (5) should be compared to the classical "rigidity assumption". The latter requires that the action of G be transitive on a much bigger subset of G^r, namely the subset denoted by $sni(\mathbf{C})$ consisting of all r-tuples $(g_1, \dots, g_r)$ of G^r satisfying only the first three conditions (i), (ii) and (iii) of the definition of $sni(\mathbf{C}, r)$. The extra set of conditions (iv) makes assumption (5) more likely than the rigidity assumption.

Th.4.1 can be stated more generally. Without assumption (5), it still can be concluded that the G-cover f can be defined over a number field L of degree $[L : \mathbb{Q}]$ less than the number of orbits of the action of G on the set $sni(\mathbf{C}, r)$.

Th.4.1 is a descent criterion over $\mathbb{Q}$ for G-covers *a priori* defined over $\mathbb{Q}^{tr}$ and with branch points in $\mathbb{P}^1(\mathbb{Q})$. One may wish to combine Th.4.1 and Th.3.1. Unfortunately, Th.3.1 is not precise enough yet : assumption (4), that is, that the branch points be in $\mathbb{P}^1(\mathbb{Q})$, is not guaranteed by the conclusion of Th.3.1. Such a version of Th.3.1 with some extra rationality conditions over $\mathbb{Q}$ on the branch points would be a great improvement.

4.2. From $\mathbb{Q}^{tp}$ to $\mathbb{Q}$. In a general way, the knowledge of the action of $G_{\mathbb{Q}_p}$ on fundamental groups $\Pi_{\overline{\mathbb{Q}_p}, \mathbf{t}}$ yields necessary conditions for a cover to be defined over $\mathbb{Q}_p$, so in particular, over $\mathbb{Q}^{tp}$. But in the finite case, the action of $G_{\mathbb{Q}_p}$ on covers of $\mathbb{P}^1$ is not as easy to describe as in the case $p = \infty$. M. Fried and I proved that there is no exact analog of Hurwitz formulas for the p-adics (see [DeFr ;§3.7] for a precise

(*) Nonemptyness of $sni(\mathbf{C},r)$ follows from Hurwitz formulas.

formulation). Now subtler analogs might exist. As recent results of Pop show [Po3], investigating further the action of $G_{\mathbb{Q}_p}$ on covers of $\mathbb{P}^1$ is certainly an interesting direction of work.

Considering covers over the different completions of $\mathbb{Q}$ raises other interesting questions, in particular, various forms of "local-to-global" questions. The rest of this paper will be devoted to these questions.

4.3. Hurwitz spaces and Hasse principle. Let G be a finite group. From Th.3.1, for each prime p, G is the automorphism group of a G-cover $f_p : X_p \to \mathbb{P}^1$ defined over $\mathbb{Q}^{tp}$. We mention in §4.1 a possible improvement of Th.3.1. Another one would consist in showing that one can arrange for the inertia canonical invariant $\mathbf{C}_p$ of f_p not to depend on p. Assume further that the center $Z(G)$ of G is trivial. Then the question can be rephrased as follows : show that there exists an integer r and an r-tuple $\mathbf{C}$ such that the associated Hurwitz space $\mathfrak{H} = \mathfrak{H}_G(\mathbf{C})$ has $\mathbb{Q}^{tp}$-rational points for each prime p (*). When this is achieved, an interesting kind of Hasse problem arises : can one conclude that $\mathfrak{H}(\mathbb{Q}) \neq \emptyset$? The following example shows the answer to be "No" in general.

Example 4.2. Let ℓ be a prime > 7 and G be the dihedral group $G = D_{2\ell}$ of order 2ℓ. Take $r = 4$ and each of the conjugacy classes $C_1, \ldots, C_4$ equal to the set of involutions of $D_{2\ell}$. Then [DeFr] shows that the associated Hurwitz space $\mathfrak{H} = \mathfrak{H}_G(\mathbf{C})$ is irreducible and defined over $\mathbb{Q}$. Furthermore, if k is field, k-rational points on $\mathfrak{H}$ can be interpreted as k-rational points on the modular curve $X_1(\ell)$. Consequently, $\mathfrak{H}(\mathbb{Q}_p) \neq \emptyset$ for each prime p : $\mathbb{Q}_p$-rational points can be found near the cusps which are $\mathbb{Q}$-rational. And $\mathfrak{H}(\mathbb{Q}) = \emptyset$: this is Mazur's theorem [MaSe].

Remark 4.3. In [DeFr], the same example shows that at least six branch points are necessary to realize the dihedral group $D_{2\ell}$ over $\mathbb{Q}(T)$, which is a little striking when one knows only three are sufficient for the Monster. Recent results of Mazur and Kamieny [MaKa] suggest that the following might even be true : there is no integer r_o such that each dihedral group is realized over $\mathbb{Q}(T)$ with at most r_o branch points (see [DeFr] for more details).

5. First variants of Dew's conjecture

In his thesis [Dew], E. Dew makes this conjecture.

Conjecture (Dew) — *Let K be a number field and $f : X \to \mathbb{P}^1$ be a G-cover defined over $\overline{K}$. Then the following conditions are equivalent :*
(i) The G-cover f can be defined over $K_\mathfrak{p}$ for all primes $\mathfrak{p}$ of K (including the primes at infinity).
(ii) The G-cover f can be defined over K.

We will prove in §7 that this conjecture holds except possibly in a very special case coming from Grunwald's theorem [ArTa]. This special case cannot occur if $K = \mathbb{Q}$. It is unknown whether Dew's conjecture holds in the special case ; no

(*) Using [De1 ; 5 p.240], this can be shown for each group G generated by involutions and satisfying condition (7) of §3.

counter-example has yet been found. Dew's conjecture is concerned with G-covers. The same conjecture with covers instead of G-covers is an open question ; it might not hold even over $\mathbb{Q}$ (Cf. Remark 5.4).

The following result consists of three easier variants of Dew's conjecture.

PROPOSITION 5.1 — *Let K be a number field and $f : X \to \mathbb{P}^1$ be a G-cover defined over $\overline{K}$.*

(A) Assume that the G-cover f has a smallest field of definition, that is, there exists a field contained in each field of definition of the G-cover f. Then the conclusion of Dew's conjecture holds true.

(B) Assume that f can be defined over K as a cover, i.e., there exists a cover $f_K : X_K \to \mathbb{P}^1_K$ over K such that f_K and f are isomorphic as covers over $\overline{K}$. Then the following conditions are equivalent :
(i) The cover $f_K \otimes_K K_\mathfrak{p}$ is a Galois cover for all but finitely many primes $\mathfrak{p}$.
(ii) The cover f_K is a Galois cover over K (in particular, the G-cover f can be defined over K).

(C) Let $t_o \in \mathbb{P}^1(K) \setminus \{\mathbf{t}(f)\}$. Then the following conditions are equivalent :
(i) The G-cover f can be defined over $K_\mathfrak{p}$ with a totally rational fiber above t_o for all but finitely many primes $\mathfrak{p}$.
(ii) The G-cover f can be defined over K with a totally rational fiber above t_o.

These three results are consequence of this well-known corollary of the Cebotarev density theorem (e.g. [Sc]) :

LEMMA 5.2 (Frobenius-Hasse) — *Let L/K be a number field extension. If L can be embedded in $K_\mathfrak{p}$ for all but finitely many primes $\mathfrak{p}$ of K, then $L = K$.*

(A) is an immediate consequence of Lemma 5.2. (B) is proved below. The proof of (C) is postponed to §6.2.3.

Proof of (B). Let $E/K(T)$ be the function field extension corresponding to the cover $f_K : X_K \to \mathbb{P}^1_K$. The field extension $E\overline{K}/\overline{K}(T)$ is Galois. There is a smallest subfield $\widehat{K}$ of $\overline{K}$ such that the field extension $E\widehat{K}/\widehat{K}(T)$ is Galois : it is the constant field of the Galois closure $\widehat{E}/K(T)$ of $E/K(T)$, *i.e.*, $\widehat{K} = \widehat{E} \cap \overline{K}$. If $\mathfrak{p}$ is a prime, the cover $f_K \otimes_K K_\mathfrak{p}$ is a Galois cover if and only if the field $\widehat{K}$ can be embedded in $K_\mathfrak{p}$. Conclusion follows from Lemma 5.2. □

REMARK 5.3. A G-cover $f : X \to \mathbb{P}^1$ satisfying condition (i) of Dew's conjecture has necessarily K as field of moduli (see §6). From Coombes-Harbater's theorem (see Th.6.1), $f : X \to \mathbb{P}^1$ can then be defined over K as a cover, that is, f has a model $f_K : X_K \to \mathbb{P}^1_K$ over K as in Prop.5.1 (B). But condition (i) of Prop.5.1 (B) and condition (i) of Dew's conjecture are different. Indeed, that a G-cover $f : X \to \mathbb{P}^1$ can be defined over $K_\mathfrak{p}$ means that there exists a Galois cover $f_\mathfrak{p} : X_\mathfrak{p} \to \mathbb{P}^1_{K_\mathfrak{p}}$ over $K_\mathfrak{p}$ such that $f_\mathfrak{p}$ and f are isomorphic as G-covers over $\overline{K_\mathfrak{p}}$. But in general $f_\mathfrak{p}$ need not be isomorphic to the cover $f_K \otimes_K K_\mathfrak{p}$.

Prop.5.1 shows that the difficulty in Dew's conjecture is that the cover $f : X \to \mathbb{P}^1$ is *a priori* defined over $\overline{K}$ and that there may be several different ways of descending the field of definition.

REMARK 5.4. *Towards a possible counter-example to Dew's conjecture for covers.* Assume that a cover $f : X \to \mathbb{P}^1$ can be defined in three different ways over three real quadratic fields $\mathbb{Q}(\sqrt{a_1})$, $\mathbb{Q}(\sqrt{a_2})$, $\mathbb{Q}(\sqrt{a_3})$ with a_1, a_2, a_3 positive, odd, square-free integers and such that $gcd(a_1, a_2, a_3) = 1$. Assume in addition that the three positive integers a_1, a_2, a_3 can be selected in such a way that the following conditions hold :

(i) $a_1a_2a_3$ is a perfect square.

(ii) Each of the three integers is a square modulo each prime divisor of the product of the two other ones.

(iii) At least one out of the three integers a_1, a_2, a_3 is congruent to 1 mod 8.

(For example, take $a_1 = 13$, $a_2 = 17$, $a_3 = 13.17$). Then it is easily checked that for each finite prime p, at least one out of the fields $\mathbb{Q}(\sqrt{a_i})$, $i = 1, 2, 3$ can be embedded in $\mathbb{Q}_p$. Therefore, the cover can be defined over $\mathbb{Q}_p$ for each prime p. Assume that such a cover can be found that cannot be defined over $\mathbb{Q}$. Then this cover would be a counter-example to the analogue of Dew's conjecture for covers (without the automorphisms). However covers with real quadratic fields as minimal fields of definition do not seem very easy to construct.

This first approach of Dew's conjecture was intended to suggest that it has a lot to do with the existence of a single or several minimal fields of definition for a given G-cover. This is very much related to the classical question of the obstruction for the field of moduli to be a field of definition.

6. Field of moduli versus field of definition

6.1. Definitions. Fix a base field K and its algebraic closure $\overline{K}$. Let $f : X \to \mathbb{P}^1$ be a cover (resp., G-cover) *a priori* defined over $\overline{K}$. Consider the subgroup $M(f)$ (resp. $M_G(f)$) of G_K consisting of all the elements $\tau \in G_K$ such that the covers (resp., the G-covers) f and f^τ are isomorphic. Then the *field of moduli* of the cover f (resp., the G-cover f) is defined to be the fixed field

$$\overline{K}^{M(f)} \text{ (resp. } \overline{K}^{M_G(f)})$$

of $M(f)$ (resp. $M_G(f)$) in $\overline{K}$. The field of moduli of a cover (resp., G-cover) is a finite extension of K contained in each field of definition containing K. So it is the smallest field of definition containing K if it is a field of definition. In particular, from Prop.5.1 (A), Dew's conjecture is true for G-covers defined over their field of moduli. In fact, from Prop. 2.7 of [CoHar], that condition is equivalent to the assumption of Prop.5.1 (A) : if a G-cover has a smallest field of definition, it has to be the field of moduli.

In general the field of moduli need not be a field of definition [CoHar ;Example 2.6]. However, Coombes and Harbater proved this result [CoHar ;Prop.2.5].

THEOREM 6.1 (Coombes-Harbater) — *The field of moduli of a Galois cover f is a field of definition of the cover f (without the automorphisms).*

The dictionary §2.4 provides the following algebraic characterization of field of moduli and field of definition. Let $\phi : \Pi_{\overline{K},\mathbf{t}} \to S_d$ (resp. $\phi : \Pi_{\overline{K},\mathbf{t}} \to G$) be the homomorphism associated to a cover f (resp. a G-cover f). Let $t_o \in \mathbb{P}^1(K) \setminus \{\mathbf{t}\}$ be a rational base point and $s = s_{t_o}$ be the associated section $s_{t_o} : G_K \to \Pi_{K,\mathbf{t}}$.

PROPOSITION 6.2 — *(a) An element $\tau \in G_K$ is in the subgroup $M(f)$ (resp. $M_G(f)$) if and only if there exists $\varphi_\tau \in S_d$ (resp. $\varphi_\tau \in G$) such that*

$$\phi(x^{s(\tau)}) = \varphi_\tau \phi(x) \varphi_\tau^{-1} \text{ for all } x \in \Pi_{\overline{K},\mathbf{t}} \tag{1}$$

In particular, the field of moduli of the cover f (resp. the G-cover f) is the subfield of $\overline{K}$ fixed by all the elements $\tau \in G_K$ such that (1) holds.

(b) An algebraic extension k of K is a field of definition of the cover f (resp. the G-cover f) if and only if $G_k \subset M(f)$ (resp. $G_k \subset M_G(f)$) and if the collection $(\varphi_\tau)_{\tau \in G_k}$ of elements $\varphi_\tau \in S_d$ (resp. $\varphi_\tau \in G$) satisfying (1) can be selected in such a way that the correspondence $\tau \to \varphi_\tau$ is an homomorphism of groups.

The condition

$$(\varphi_{\tau_1 \tau_2})^{-1} \varphi_{\tau_1} \varphi_{\tau_2} = 1 \text{ for all } \tau_1, \tau_2 \in G_K \tag{2}$$

that appears in (b) is the exact algebraic counterpart of the classical Weil's cocycle condition [We]. In general, the left-hand term of (2) lies in the centralizer $Cen_{S_d} G$ of G in S_d for a cover (resp. in the center $Z(G)$ of G for a G-cover). Therefore if $Cen_{S_d} G = \{1\}$ (resp. $Z(G) = \{1\}$), the field of moduli of the cover (resp. G-cover f) is also a field of definition.

6.2. Applications of Prop.6.2.

6.2.1. Algebraic proof of Coombes-Harbater's theorem (Th.6.1). Coombes-Harbater's argument can be rephrased algebraically as follows. If the cover $f : X \to \mathbb{P}^1$ is Galois, then the group $G = \phi(\Pi_{\overline{K},\mathbf{t}}) \subset S_d$ acts freely and transitively on $\{1, \dots, d\}$ and the same is true for the group $Cen_{S_d} G$. By multiplying each φ_τ on the right by an element of $Cen_{S_d} G$, one may assume that

$$\varphi_\tau \text{ fixes 1 for all } \tau \in M(f) \tag{3}$$

Together with (1) this extra condition completely determines each φ_τ, $\tau \in M(f)$. Condition (2) follows then immediately. Hence the field of moduli is a field of definition. In fact it follows from Prop.2.1 and (3) that we have this stronger conclusion : the cover $f : X \to \mathbb{P}^1$ can be defined over its field of moduli in such a way that the fiber above t_o contains at least one rational point. □

6.2.2. Practical criteria. Results of this paragraph are due to J-R. Pycke. Let $f : X \to \mathbb{P}^1$ be a cover defined over $\overline{K}$ and with K as field of moduli. Let $\phi : \Pi_{\overline{K},\mathbf{t}} \to S_d$ be the homomorphism associated to f. Denote the Galois closure over $\overline{K}$ of $f : X \to \mathbb{P}^1$ by $\widehat{f} : \widehat{X} \to \mathbb{P}^1$ and the field of moduli of the G-cover $\widehat{f}$ by K_G. Let $t_o \in \mathbb{P}^1(K) \setminus \{\mathbf{t}\}$. Denote the normalizer of $G = \phi(\Pi_{\overline{K},\mathbf{t}})$ in S_d by $N_{S_d} G$. Consider the map

$$\overline{\varphi}: \begin{cases} G_K = M(f) & \to & N_{S_d}G/Cen_{S_d}G \\ \tau & \to & \overline{\varphi}_\tau \end{cases}$$

(4)

$$\left(\text{resp.} \quad \overline{\varphi}_G: \begin{cases} G_{K_G} = M_G(\widehat{f}) & \to & G/Z(G) \\ \tau & \to & \overline{\varphi}_\tau \end{cases}\right)$$

that assigns to each element $\tau \in M(f)$ (resp. $\tau \in M_G(\widehat{f})$) the left coset modulo $Cen_{S_d}G$ (resp. modulo $Z(G)$) of an element $\varphi_\tau \in N_{S_d}(G)$ (resp. $\varphi_\tau \in G$) satisfying (1). This map is a group homomorphism. Then Prop.6.2 (b) can be reformulated as follows :

Proposition 6.3 (Pycke) — *(a) The field of moduli K is a field of definition of the cover f if and only if the homomorphism $\overline{\varphi}: G_K \to N_{S_d}G/Cen_{S_d}G$ can be lifted up to an homomorphism $\varphi: G_K \to N_{S_d}G$.*

(b) The field of moduli K_G of the G-cover f is a field of definition of the G-cover f if and only if the homomorphism $\overline{\varphi}_G: G_{K_G} \to G/Z(G)$ can be lifted up to an homomorphism $\varphi_G: G_{K_G} \to G$.

The following classical cases where the field of moduli is a field of definition are all trivially covered by Prop.6.3. :

(for the cover f) :
- $Cen_{S_d}G = \{1\}$ *i.e.*, the cover f has no automorphims.
- $Cen_{S_d}G$ is a direct summand of $N_{S_d}G$, *e.g.* the cover f is Galois (Th.6.1).
- The Galois group G_K is a projective profinite group.

(for the G-cover $\widehat{f}$) :
- $Z(G) = \{1\}$ *i.e.* G has a trivial center.
- $Z(G) = G$ (*i.e.* G is abelian).
- The Galois group G_K is a projective profinite group.
- The cover $\widehat{f}$ can be defined over K with a totally rational fiber above a point $t_o \in \mathbb{P}^1(K) \setminus \{\mathbf{t}\}$ (use Prop.2.1).

Remark 6.4. The condition "G_K is projective" holds if K is of cohomological dimension ≤ 1. The fields $\overline{k}((T))$ with $\text{char}(k) = 0$, $\mathbb{Q}_p^{ur}$ (maximal unramified algebraic extension of $\mathbb{Q}_p$), $\overline{k}(T)$, $\mathbb{Q}^{ab}$ are some classical examples of field of cohomological dimension ≤ 1. Over these fields, the field of moduli of a (G-)cover is a field of definition. E. Dew showed that the result also holds over finite fields [Dew]. Finite fields are of cohomological dimension ≤ 1 but there is an extra difficulty : there does not necessarily exist a K-rational base point $t_o \in \mathbb{P}^1(K) \setminus \{\mathbf{t}\}$. However the case of finite fields can still be viewed as a corollary of this paragraph. But rather than using a section s_{t_o}, one should use an arbitrary section of the map $\Pi_{K,\mathbf{t}} \to G_K$. Existence of such a section is guaranteed by the projectivity of G_K.

The following result is also a consequence of Prop.6.3. Both maps $\overline{\varphi}$ and $\overline{\varphi}_G$ have the same kernel, namely the subgroup of G_K, denoted by $M_{t_o}(f)$, consisting of all the elements $\tau \in G_K$ such that

$$\phi(x^{s_{t_o}(\tau)}) = \phi(x) \text{ for each } x \in \Pi_{\overline{K},\mathbf{t}} \tag{5}$$

Denote the fixed field $\overline{K}^{M_{t_o}(f)}$ of $M_{t_o}(f)$ in $\overline{K}$ by $R_{t_o}(f)$.

COROLLARY 6.5 (Pycke) — *The field $R_{t_o}(f)$ is both a field of definition of the cover f and of the G-cover $\widehat{f}$. Furthermore we have*

$$\begin{cases} [R_{t_o}(f) : K] \leq \frac{|N_{S_d}G|}{|Cen_{S_d}G|} \\ [R_{t_o}(f) : K_G] \leq \frac{|G|}{|Z(G)|} \end{cases} \tag{6}$$

6.2.3. Proof of Prop.5.1 (C). From Prop.6.2 and Prop.2.1, the field $R_{t_o}(f)$ is the smallest subfield k of $\overline{K}$ over which the following equivalent conditions hold.

(i) The cover $f : X \to \mathbb{P}^1$ can be defined over k with a totally rational fiber above t_o.
(ii) The function field extension $\overline{K}(X)/\overline{K}(T)$ can be obtained by extension of scalars from a Galois regular extension $E_k/k(T)$ with E_k a subfield of $k((T-t_o))$.

Condition (i) of Prop. 5.1 (C) amounts to saying that the field $R_{t_o}(f)$ can be embedded in $K_{\mathfrak{p}}$ for all but finitely many primes $\mathfrak{p}$. Lemma 5.2 completes the proof. □

REMARK 6.6. The field $R_{t_o}(f)$ can also be described in the following way. The field of moduli K of the cover f clearly contains the field of moduli of the cover $\widehat{f}$. From Th.6.1, $\widehat{f}$ can be defined over K as a cover. That is, there exists a cover $\widehat{f}_K : X_K \to \mathbb{P}^1_K$ such that both covers $\widehat{f}_K$ and $\widehat{f}$ are isomorphic over $\overline{K}$. The function field $K(X_K)$ can be embedded in $\overline{K}((T-t_o))$. Then the field $R_{t_o}(f)$ corresponds to the field generated over K by the coefficients of all the formal power series in $K(X_K)$. Geometrically, this amounts to saying that $R_{t_o}(f)$ is the smallest field of rationality for all the points in the fiber $f_K^{-1}(t_o)$.

6.3. Cohomological approach. In the case of G-covers, the obstruction for the field of moduli to be a field of definition can be characterized in a cohomological way. Namely, the following is easily checked.

PROPOSITION 6.7 — *Let $f : X \to \mathbb{P}^1$ be a G-cover with field of moduli contained in K. With notation of Prop.6.2, we have :*
(a) The collection $((\varphi_{\tau_1\tau_2})^{-1}\varphi_{\tau_1}\varphi_{\tau_2})_{\tau_1,\tau_2\in G_K}$ induces a 2-cocycle $\gamma \in H^2(K, Z(G))$ in the second Galois cohomology group of K with values in the center $Z(G)$ of the group G and where the action of G_K on $Z(G)$ is the trivial one.
(b) The 2-cocycle γ is trivial in $H^2(K, Z(G))$ if and only if the field K is a field of definition of the G-cover f.
(c) The element $\gamma \in H^2(K, Z(G))$ does not depend on the choice of the base point t_o and on the section $s = s_{t_o}$.

REMARK 6.8. For a cover (without the automorphisms) with K as field of moduli, the collection $((\varphi_{\tau_1\tau_2})^{-1}\varphi_{\tau_1}\varphi_{\tau_2})_{\tau_1,\tau_2\in G_K}$ is a collection of elements of

$Cen_{S_d}G$. If $Cen_{S_d}G$ is not an abelian group, this collection does not necessarily satisfy the cocycle condition. Thus there is no such practical cohomological approach for covers as there is for G-covers.

7. Dew's conjecture

A statement of Dew's conjecture was given in §5 together with some comments. This section is devoted to the proof of the following result.

THEOREM 7.1 — *Dew's conjecture is true except possibly if conditions 1., 2., 3. below (which will be referred to as the special case) hold.*

Some extra notation is needed to describe the special case. For each integer $r > 0$, ζ_r is a primitive 2^rth root of 1 and $\eta_r = \zeta_r + \zeta_r^{-1}$. Then denote by s the smallest integer such that $\eta_s \in K$ and $\eta_{s+1} \notin K$. The special case is defined by these three simultaneous conditions :

1. -1, $2+\eta_s$, $-(2+\eta_s)$ are non-squares in K.
2. For each prime $\mathfrak{p}$ of K dividing 2, at least one out of the elements -1, $2+\eta_s$, $-(2+\eta_s)$ is a square in $K_\mathfrak{p}$.
3. The abelian group $Z(G)$ contains an element of order a multiple of 2^t with $t > s$.

If $K = \mathbb{Q}$, then $s = 2$ and $\eta_s = 0$. Since -1, 2 and -2 are non-squares in $\mathbb{Q}_2$, condition 2. cannot be satisfied. Therefore the special case cannot occur if $K = \mathbb{Q}$.

Proof. Let $f : X \to \mathbb{P}^1$ be a G-cover defined over $\overline{K}$ and definable over $K_\mathfrak{p}$ for all primes $\mathfrak{p}$. It follows from Lemma 5.2 that the field of moduli of f is K. Consider the element $\gamma \in H^2(K, Z(G))$ of Prop.6.7. For each prime $\mathfrak{p}$, $K_\mathfrak{p}$ is the field of moduli and a field of definition of the cover $f \otimes_{\overline{K}} \overline{K_\mathfrak{p}}$. Therefore the element γ lies in the kernel of the natural map

$$H^2(K, Z(G)) \to \prod_\mathfrak{p} H^2(K_\mathfrak{p}, Z(G)) \tag{1}$$

The rest of the proof, which consists in showing that this map is injective except possibly in the special case, was explained to me by J-C. Douai. By writing $Z(G)$ as a product of cyclic groups, one may reduce to the case $Z(G) = \mathbb{Z}/n\mathbb{Z}$. Then from the Tate-Poitou theorem [Se1 ;II-§6.3], the kernel of the map (1) is in duality with the kernel of the map

$$H^1(K, \mu_n) \to \prod_\mathfrak{p} H^1(K_\mathfrak{p}, \mu_n) \tag{2}$$

where $\mu_n = Hom(\mathbb{Z}/n\mathbb{Z}, \mathbb{G}_m)$ is the group of nth roots of 1 in $\overline{K}$. Classically we have $H^1(K, \mu_n) \simeq K^\times/(K^\times)^n$. The result then follows from Grunwald's theorem [ArTa ;Ch.10] : for a global field, the natural map

$$K^\times/(K^\times)^n \to \prod_\mathfrak{p} K_\mathfrak{p}^\times/(K_\mathfrak{p}^\times)^n \tag{3}$$

is injective except possibly in the special case described above (which corresponds to the special case of Grunwald's theorem in [ArTa] p. 96 with the extra condition $S = \emptyset$). □

8. Field of moduli versus field of definition over the p-adics

8.1. Statement of the main results. The goal of this section is to prove the following result.

THEOREM 8.1 — *Let K be a number field and $f : X \to \mathbb{P}^1$ be a (G-)cover defined over $\overline{K}$. The following conditions are equivalent.*
(i) The field of moduli of f is K.
(ii) The (G-)cover f can be defined over $K_{\mathfrak{p}}$ for all but finitely many primes $\mathfrak{p}$.

In the case of G-covers, Th.8.1 follows from the fact that the map (1) of §7 has values in the direct sum $\coprod_{\mathfrak{p}} H^2(K_{\mathfrak{p}}, Z(G))$ ([Se1 ;Prop.21 p.131]). The same argument does not apply to covers. Furthermore our proof will be "effective" in the following sense. Prop.21 p.131 of [Se1] uses the ineffective following fact : any element $\gamma \in H^2(K, Z(G))$ comes from some element in $H^2(G(L/K), Z(G))$ for some suitable finite Galois extension L/K. In our proof, such a field L will be described explicitly. This is of importance if one wishes to bound the exceptional primes in Th.8.1 (Cf. Remark 8.3).

Implication $(ii) \Rightarrow (i)$ follows immediately from Lemma 5.2. The converse uses an idea of E. Dew, which consists, for finite primes $\mathfrak{p}$, in trying to descend the field of definition from $\overline{K_{\mathfrak{p}}}$ to $K_{\mathfrak{p}}$ via the intermediate subfield $K_{\mathfrak{p}}^{ur}$, *i.e.*, the maximal algebraic unramified closure of $K_{\mathfrak{p}}$. Both Galois groups $G(\overline{K_{\mathfrak{p}}}/K_{\mathfrak{p}}^{ur})$ and $G(K_{\mathfrak{p}}^{ur}/K_{\mathfrak{p}})$ are of cohomological dimension ≤ 1. It is quite tempting to use twice in a row that under projectivity assumptions, the field of moduli is a field of definition (Cf. §6.2.2). But there is a difficulty. Using the projectivity of $G(\overline{K_{\mathfrak{p}}}/K_{\mathfrak{p}}^{ur})$, one can obtain a (G-)cover $f_{\mathfrak{p}} : X_{\mathfrak{p}} \to \mathbb{P}^1_{K_{\mathfrak{p}}^{ur}}$ over $K_{\mathfrak{p}}^{ur}$ such that $f_{\mathfrak{p}}$ is isomorphic to f as (G-)covers over $\overline{K_{\mathfrak{p}}}$. For (G-)covers over a nonalgebraically closed field L, a more general notion of *field of moduli relative to an extension L/K* can be defined. The difficulty is that the field of moduli of $f_{\mathfrak{p}}$ relative to the extension $K_{\mathfrak{p}}^{ur}/K$ need not be equal to K. The key lemma is the following result.

LEMMA 8.2 — *Let $f : X \to \mathbb{P}^1$ be a (G-)cover defined over $\overline{K}$ and with K as field of moduli. Let L be a Galois extension of K such that*

(1) the Galois group $G(L/K)$ is a profinite projective group.

In addition, assume that

(2) the cover f (without the automorphisms) can be defined over L with a totally rational fiber above a point $t_o \in \mathbb{P}^1(K) \setminus \{\mathbf{t}(f)\}$.

Then K is a field of definition of the (G-)cover f.

8.2. Proof of Lemma 8.2. For simplicity, we only consider the case of G-covers. Only slight changes are necessary for the case of covers. The proof divides into three steps.

8.2.1. 1st step : Descent from $\overline{K}$ to L. Let $\phi : \Pi_{\overline{K},\mathbf{t}} \to G$ be the homomorphism corresponding to the G-cover f. By hypothesis, the cover f is isomorphic over $\overline{K}$ to a cover $f_L : X_L \to \mathbb{P}^1_L$ over L with a totally rational fiber above t_o. Because of this extra condition, f_L also has a structure of G-cover over L of group G (see the

comments after Prop.6.3). Let $\phi_L : \Pi_{L,\mathbf{t}} \to G$ be the homomorphism associated to the G-cover f_L. The homomorphism ϕ_L can be described in the following way.

Consider the splitting of the exact sequence

$$1 \to \Pi_{\overline{K},\mathbf{t}} \to \Pi_{L,\mathbf{t}} \to G_L \to 1 \tag{3}$$

given by the section s_{t_o} (or, more precisely, the restriction to G_L of the section $s_{t_o} : G_K \to \Pi_{K,\mathbf{t}}$). Each element $\mathrm{x} \in \Pi_{L,\mathbf{t}}$ can be written in a unique way :

$$\mathrm{x} = x.s_{t_o}(\tau) \text{ with } x \in \Pi_{\overline{K},\mathbf{t}} \text{ and } \tau \in G_L$$

It follows from (2) and Prop.2.1 that $\phi_L(s_{t_o}(\tau)) = 1$. Whence

$$\phi_L(\mathrm{x}) = \phi(x)$$

8.2.2. 2nd step : K is the field of moduli of the homomorphism ϕ_L relative to the extension L/K. What we exactly mean by this phrase is that for each $\Delta \in \Pi_{K,\mathbf{t}}$, there exists $\varphi_{L,\Delta} \in G$ such that

$$\phi_L(\mathrm{x}^{\Delta}) = \varphi_{L,\Delta}\phi_L(\mathrm{x})\varphi_{L,\Delta}^{-1} \text{ for all } \mathrm{x} \in \Pi_{L,\mathbf{t}} \tag{4}$$

It is sufficient to establish (4) for each element $\Delta = s_{t_o}(\delta) \in s_{t_o}(G_K) \subset \Pi_{K,\mathbf{t}}$. Let $\mathrm{x} = x.s_{t_o}(\tau)$ $(x \in \Pi_{\overline{K},\mathbf{t}}, \tau \in G_L)$ be an arbitrary element of $\Pi_{L,\mathbf{t}}$. For each $\delta \in G_K$, we have $\mathrm{x}^{s_{t_o}(\delta)} = x^{s_{t_o}(\delta)}s_{t_o}(\tau)^{s_{t_o}(\delta)}$. Since $\Pi_{\overline{K},\mathbf{t}}$ is a normal subgroup of $\Pi_{K,\mathbf{t}}$, $x^{s_{t_o}(\delta)}$ still lies in $\Pi_{\overline{K},\mathbf{t}}$. Next we write

$$s_{t_o}(\tau)^{s_{t_o}(\delta)} = s_{t_o}(\tau^{\delta})$$

Since the extension L/K is Galois, then $\tau^{\delta} \in G_L$. Conclude that

$$\mathrm{x}^{s_{t_o}(\delta)} = x^{s_{t_o}(\delta)}s_{t_o}(\tau)^{s_{t_o}(\delta)}$$

is the unique way of writing $\mathrm{x}^{s_{t_o}(\delta)}$ as the product of an element of $\Pi_{\overline{K},\mathbf{t}}$ and an element of $s_{t_o}(G_L)$. Therefore we obtain

$$\phi_L(\mathrm{x}^{s_{t_o}(\delta)}) = \phi(x^{s_{t_o}(\delta)})$$

Since K is the field of moduli of the G-cover f, there exists $\varphi_{L,\delta} \in G$ such that $\phi(x^{s_{t_o}(\delta)}) = \varphi_{L,\delta}\phi(x)\varphi_{L,\delta}^{-1}$ for all $x \in \Pi_{\overline{K},\mathbf{t}}$. Conclusion follows from $\phi(x) = \phi_L(\mathrm{x})$.

8.2.3. 3rd step : K is a field of definition of f. Since $G(L/K)$ is projective the exact sequence

$$1 \to \Pi_{L,\mathbf{t}} \to \Pi_{K,\mathbf{t}} \to G(L/K) \to 1 \tag{5}$$

splits. Let $S : G(L/K) \to \Pi_{K,\mathbf{t}}$ be a section to the map $\Pi_{K,\mathbf{t}} \to G(L/K)$. For each $\delta \in G(L/K)$, the elements $\varphi_{L,S(\delta)} \in G$ satisfying (4) all agree modulo $Z(G)$ and so determine a well-defined element $\overline{\varphi}_{L,S(\delta)} \in G/Z(G)$. The correspondence $\delta \to \overline{\varphi}_{L,S(\delta)}$ yields a group homomorphism $\overline{\varphi}_{L/K} : G(L/K) \to G/Z(G)$. Since $G(L/K)$ is a projective profinite group, $\overline{\varphi}_{L/K}$ can be lifted up to an homomorphism

$\varphi_{L/K} : G(L/K) \to G$. This implies that the homomorphism ϕ_L can be extended to an homomorphism $\Pi_{K,\mathbf{t}} \to G$: namely the extended homomorphism takes $xS(\delta)$ to $\phi_L(x)\varphi_{L/K}(\delta)$. This completes the proof. □

8.3. Proof of $(i) \Rightarrow (ii)$ **in Th.8.1.** The cover f can be defined over some finite extension F of K (from Th.6.1, in the case of Galois covers, one can take $F = K$). Thus there exists a cover $f_F : X_F \to \mathbb{P}^1_F$ such that both covers f_F and f are isomorphic over $\overline{K}$. Let $t_o \in \mathbb{P}^1(K) \setminus \{\mathbf{t}(f)\}$. It follows from Hensel's lemma that for all but finitely many primes $\mathfrak{p}$, we have

$$f_F^{-1}(t_o) \subset X_F(K_{\mathfrak{p}}^{ur}) \tag{6}$$

[Namely let E be a number field such that $f_F^{-1}(t_o) \subset X_F(E)$ and α be a primitive element of the extension E/K that is integral over the ring O_K of integers of K. Then the irreducible polynomial of α is a monic poynomial in $O_K[Y]$. Let $\Delta \in O_K$ be the discriminant of P and $\mathfrak{p}$ be a finite prime such that $|\Delta|_{\mathfrak{p}} = 1$. Denote the local ring and the residue field associated with the prime $\mathfrak{p}$ respectively by $O_{\mathfrak{p}}$ and $k_{\mathfrak{p}}$. The factorization of the polynomial P modulo $\mathfrak{p}$ is of the form

$$\overline{P} = \overline{Q_1} \cdots \overline{Q_r}$$

where $\overline{Q_1}, \ldots, \overline{Q_r} \in k_{\mathfrak{p}}(Y)$ are irreducible distinct monic polynomials with coefficients in the residue field $k_{\mathfrak{p}}$. From Hensel's lemma (e.g. [Am ;p.58]), there exist polynomials $Q_1, \ldots, Q_r \in O_{\mathfrak{p}}(Y)$ such that $Q_i \equiv \overline{Q_i}$ $[mod\ \mathfrak{p}]$, $\deg(Q_i) = \deg(\overline{Q_i})$, $i = 1, \ldots, r$ and $P = Q_1 \cdots Q_r$. By construction, each of the roots of the polynomials $Q_1, \ldots, Q_r$ generates an unramified extension of $K_{\mathfrak{p}}$.]

Let $\mathfrak{p}$ be a prime such that (6) holds. Set $L = K_{\mathfrak{p}}^{ur}$ and consider the (G-)cover $f_{\mathfrak{p}} = f \otimes_{\overline{K}} \overline{K_{\mathfrak{p}}}$. The field of moduli of the (G-)cover $f_{\mathfrak{p}}$ is clearly $K_{\mathfrak{p}}$. The Galois group $G(K_{\mathfrak{p}}^{ur}/K_{\mathfrak{p}})$ is the free profinite group $\widehat{\mathbb{Z}}$, hence is projective. By construction, the cover $f_{\mathfrak{p}}$ satisfies condition (2). From Lemma 8.2, the field $K_{\mathfrak{p}}$ is a field of definition of the (G-)cover $f_{\mathfrak{p}}$. □

Remark 8.3. Trying to bound the exceptional primes $\mathfrak{p}$ in Th.8.1 is a natural question. One should be able to prove that there exists a function $C(|G|, r)$ depending only on the order $|G|$ of the group G and the number r of geometric branch points with the following property :

"Let $f : X \to \mathbb{P}^1$ be a G-cover defined over $\overline{K_{\mathfrak{p}}}$ with $K_{\mathfrak{p}}$ as field of moduli. If $\mathfrak{p}$ does not divide $|G|$ and if $N_{K/\mathbb{Q}}(\mathfrak{p})$ is larger than $C(|G|, r)$, then the G-cover f can be defined over $K_{\mathfrak{p}}$."

References

[Am] Y. Amice, *Les nombres p-adiques*, Presses universitaires de France, (1975).

[ArTa] E. Artin and J. Tate, *Class field theory*, W. A. Benjamin, (1967).

[CoHar] K. Coombes and D. Harbater, *Hurwitz families and arithmetic Galois groups*, Duke Math. J. **52** (1985), 821–839.

[De1] P. Dèbes, *Groupes de Galois sur K(T)* , Séminaire de Théorie des Nombres, Bordeaux **2** (1990), 229–243.

[De2] P. Dèbes, *Critères de descente pour le corps de définition des G-revêtements de* $\mathbb{P}^1$, C.R. Acad. Sc. Paris, Série I, **315**, (1992), 863-868.

[DeFr] P. Dèbes and M. Fried, *Nonrigid situations in constructive Galois theory*, Pacific J. Math. **163**, n$^\bullet$ 1, (1994), 81–122.

[Dew] E. Dew, *Fields of moduli of arithmetic covers*, Thesis, (1991).

[FrDe] M. Fried and P. Dèbes, *Rigidity and real residue class fields*, Acta Arith. **56**, n$^\bullet$ 4, (1990), 13–45.

[FrHaVö] M. Fried, D. Haran and H. Völklein, *Absolute Galois group of the totally real numbers*, C.R. Acad. Sc. Paris, Série I, **317**, (1993), 1-5.

[FrVö] M. Fried and H. Völklein, *The inverse Galois problem and rational points on moduli spaces*, Math. Annalen, **290** (1991), 771–800.

[Har] D. Harbater, *Galois covering of the arithmetic line*, Proc. of the NY Number Thy. Conf., LNM, **1240**, Springer (1985).

[Hur] A. Hurwitz, *Riemann'sche Flächen mit gegebenen Veizweigungspunkten*, Mathematische Werke, **I**, 321–383.

[Li] Q. Liu, *Tout groupe est groupe de Galois sur* $\mathbb{Q}_p(T)$, Univ. Bordeaux I, (1991).

[MaKa] B. Mazur and S. Kamienny, *Rational torsion of prime order in elliptic curves over number fields*, preprint 6/92.

[MaSe] B. Mazur and J.-P. Serre, *Points rationnels des courbes modulaires* $X_o(N)$, Séminaire Bourbaki, 27e année (1974/75), Exposé **469**, Lecture Notes in Math., Springer-Verlag **514** (1976), 238–255.

[Po1] F. Pop, *Classically projective groups and pseudo classically projective groups*, preprint, Heidelberg, (1990).

[Po2] F. Pop, $\frac{1}{2}$ *Riemann Existence Theorem with Galois action*, to appear in Birkhäuser Congress Series, (1993).

[Po3] F. Pop, *Hilbertian fields with a universal local-global principle*, preprint, Heidelberg, (1993).

[PoRoGr] F. Pop, P. Roquette, B.W. Green, *On Rumely's Local-Global principle*, to appear in DMV series, (1993).

[Sc] A. Schinzel, *Selected topics in polynomials*, The Univ. of Michigan press, Ann Arbor, (1982).

[Se1] J.-P. Serre, *Cohomologie galoisienne*, LNM 5, Springer-Verlag, 4ème Edition (1973).

[Se2] J.-P. Serre, *Topics in Galois theory*, Notes written by Henri Darmon, Jones and Bartlett Publ., Boston, (1992).

[We] A. Weil, *The field of definition of a variety, Oeuvres complètes (Collected papers)* **II** , Springer-Verlag, 291–306.

Univ. Lille 1, U.F.R. Math., 59655 Villeneuve d'Ascq Cedex, France.
E-mail address : pde@gat.univ-lille1.fr

or

"Problèmes diophantiens", Univ. P. et M. Curie, Math., UFR 920, Tour 45-46, 5ème étage, BP 172, 4 Place Jussieu,75252 Paris Cedex 05, France.

E-mail address : pde@ccr.jussieu.fr