THEORIE DES NOMBRES. — *Critères de descente pour le corps de définition des G-revêtements de* $\mathbb{P}^1$. Note de **Pierre Dèbes**.

Résumé. Le résultat principal de cette Note est un critère pour qu'un groupe fini G donné soit le groupe de Galois d'une extension de $\mathbb{Q}(T)$.

NUMBER THEORY. — Descent criteria for the field of definition of G-covers of $\mathbb{P}^1$.

Abstract. The main result of this Note is a criterion for a given finite group G to be the Galois group of an extension of $\mathbb{Q}(T)$.

Abridged english version. Let K be a subfield of $\mathbb{R}$, $\widehat{G}$ be a finite group, $r \geq 2$ be an integer, $\widehat{\mathbf{C}} = (\widehat{C}_1, \ldots, \widehat{C}_r)$ be an r-tuple of conjugacy classes of $\widehat{G}$, $p : \widehat{G} \to G$ be a surjective group homomorphism and $\rho : G_K \to S_r$ be an action of the Galois group $G_K = G(\overline{K}/K)$ on the set $\{1, \ldots, r\}$. Set $C_i = p(\widehat{C}_i), i = 1, \ldots, r$. The main result of this Note is a criterion for the group G to be a Galois group over $K(T)$. More specifically, three hypotheses *(A)*, *(B)*, *(C)* are defined, which guarantee that the group G is the Galois group of a G-cover $\varphi : X \to \mathbb{P}^1$ defined over K, with r branch points $t_1, \ldots, t_r$, with associated inertia canonical classes $C_1, \ldots, C_r$ and with the property that $\rho : G_K \to S_r$ is the action G_K on $t_1, \ldots, t_r$. There are two stages in the descent of the field of definition: first, from $\overline{K}$ to the subfield K^{tr} of all totally real numbers of $\overline{K}$ (i.e., such that all conjugates over K are in $\mathbb{R}$), and then, from the field K^{tr} to the field K. Hypothesis *(A)* is a classical rationality condition on the conjugacy classes $\widehat{C}_1, \ldots, \widehat{C}_r$. Hypothesis *(B)* is a general "real-arithmetico-geometrical" condition on the totally real points of the Hurwitz spaces $\widehat{\mathfrak{H}}$ and $\widehat{\mathfrak{H}}'$ associated with the data $(\widehat{G}, \widehat{\mathbf{C}})$. Under suitable assumptions on $(\widehat{G}, \widehat{\mathbf{C}})$, this condition is a consequence of the following conjecture. Classically attached to the Hurwitz spaces is a commutative diagram

$$\begin{array}{ccc} \widehat{\mathfrak{H}} & \xrightarrow{\pi} & \widehat{\mathfrak{H}}' \\ {\scriptstyle\Psi}\downarrow & & \downarrow{\scriptstyle\Psi'} \\ U_r & \xrightarrow{\nu} & U^r \end{array}$$

of finite morphisms between (not necessarily irreducible) algebraic varieties defined over $\overline{K}$. Under Hypothesis *(A)*, the maps $\Psi : \widehat{\mathfrak{H}} \to U_r$ and $\nu : U^r \to U_r$ are defined over K, and a classical group-theoretical condition, denoted by *(Trans)*, guarantees that $\widehat{\mathfrak{H}}$ is absolutely irreducible. Under these assumptions, can one find points $\mathbf{h}' \in \widehat{\mathfrak{H}}'(\overline{K})$ such that $\pi(\mathbf{h}') \in \widehat{\mathfrak{H}}(K^{tr})$ and $\nu \circ \Psi'(\mathbf{h}') \in U_r(K)$? We conjecture that such points exist on $\widehat{\mathfrak{H}}'$ above each connected component Γ of $\nu^{-1}(U_r(\mathbb{R}))$ satisfying these two conditions:
(i) $\pi(\Psi'^{-1}(\Gamma)) \cap \widehat{\mathfrak{H}}(\mathbb{R}) \neq \emptyset$
(ii) For all $\mathbf{t}$ in a dense subset of $\Gamma \cap U^r(\overline{K})$, the subset $\pi(\Psi'^{-1}(\mathbf{t}))$ of $\widehat{\mathfrak{H}}$ is invariant under the action of G_K.
This conjecture, which can be checked in some special situations, should also be related to Pop's recent result, which asserts that an absolutely irreducible variety defined over $\mathbb{Q}^{tr}$, has totally real points provided it has real points. Hypothesis *(C)* is a pure group-theoretical condition which can be compared to the classical rigidity condition. Both require that the group G act transitively on a certain subset of G^r. The subset of concern in the rigidity context contains the one involved in Hypothesis *(C)*. But in addition, elements of the latter should satisfy a lot of extra conditions given by the action of the complex conjugation on covers of $\mathbb{P}^1$. This makes Hypothesis *(C)* much more likely than the rigidity condition. As a corollary of the main theorem, we obtain a conjectural pure

group-theoretical criterion for a group G to be a Galois group over $K(T)$. The main assumption is the existence of an extension $\widehat{G}$ of G with conjugacy classes $\widehat{C}_1, \ldots, \widehat{C}_r$ such that Hypothesis *(C)* and condition *(Trans)* hold. Using recent results of Conway-Parker and Fried-Völklein, a general procedure, valid for any finite group G, can then be given where the whole problem of realizing G as a Galois group over $\mathbb{Q}(T)$, reduces, under the conjecture above, to checking a single Hypothesis *(C)* type condition.

Soient K un sous-corps de $\mathbb{C}$ et $\varphi : X \to \mathbb{P}^1$ un revêtement galoisien fini de $\mathbb{P}^1$ défini sur $\overline{K}$. Soit G son groupe d'automorphismes. On s'intéresse aux corps de définition du G-revêtement (φ, G), c'est-à-dire du revêtement $\varphi : X \to \mathbb{P}^1$ donné avec ses automorphismes. Cette question a une application fondamentale au Problème Inverse de la Théorie de Galois: par spécialisation, le groupe G peut être réalisé comme groupe de Galois sur tout corps de définition hilbertien du G-revêtement. Le corps des modules du G-revêtement est une autre notion usuelle: contenu dans tout corps de définition, il est défini comme le sous-corps de $\overline{K}$ laissé fixe par le sous-groupe de $G_K = G(\overline{K}/K)$ constitué des éléments $\tau \in G_K$ tels que les G-revêtements φ et φ^τ soient isomorphes. Si G est de centre trivial, le corps des modules est automatiquement un corps de définition. Le revêtement $\varphi : X \to \mathbb{P}^1$ est ramifié au dessus d'un nombre fini de points $t_1, \ldots, t_r$. A chaque point de ramification t_i, correspond une classe de conjugaison C_i de G: la classe des générateurs canoniques des groupes d'inertie au dessus de t_i. Le r-uplet $(C_1, \ldots, C_r)$ est un invariant, appelé i(nvariant) c(anonique) de l'i(nertie) du revêtement.

On se fixe un sous-corps K de $\mathbb{R}$, un groupe fini $\widehat{G}$, un entier $r \geq 2$, un r-uplet $\widehat{\mathbf{C}} = (\widehat{C}_1, \ldots, \widehat{C}_r)$ de classes de conjugaison de $\widehat{G}$, une action $\rho : G_K \to S_r$ du groupe G_K sur l'ensemble $\{1, \ldots, r\}$ et un homomorphisme surjectif de groupes $p : \widehat{G} \to G$. On pose $C_i = p(\widehat{C}_i), i = 1, \ldots, r$. Dans la suite, on va définir trois hypothèses *(A)*, *(B)*, *(C)*. Le résultat central de cette Note est le suivant. Moyennant une conjecture générale sur les "espaces de Hurwitz", on en déduira un corollaire pratique.

THEOREME — *Si les hypothèses (A), (B), (C) sont satisfaites, alors il existe r points distincts $t_1, \ldots, t_r$ dans $\mathbb{P}^1(\overline{K})$ tels que*

$$t_i^\tau = t_{\rho(\tau)(i)}, i = 1, \ldots, r, \text{ pour tout } \tau \in G_K. \tag{1}$$

et un G-revêtement $\varphi : X \to \mathbb{P}^1$ de groupe G, de points de ramification $t_1, \ldots, t_r$, d'i.c.i. le r-uplet $\mathbf{C} = (C_1, \ldots, C_r)$ et de corps des modules égal à K. Si de plus le groupe G est de centre trivial, alors le G-revêtement $\varphi : X \to \mathbb{P}^1$ est défini sur K.

Se donner $\rho : G_K \to S_r$ revient à se fixer a priori l'action de G_K sur les points de ramification $t_1, \ldots, t_r$. On notera U_ρ^r l'ensemble des r-uplets $(t_1, \ldots, t_r)$ pour lesquels la condition (1) est réalisée. Sous la conclusion du Théorème, l'action $\rho : G_K \to S_r$ doit être compatible avec l'"action cyclotomique" de G_K sur les classes $C_1, \ldots, C_r$, i.e.,

$$C_{\rho(\tau)(i)}^{\chi_\tau} = C_i, i = 1 \ldots, r, \text{ pour tout } \tau \in G_K$$

où χ_τ est la valeur en τ du caractère cyclotomique $G_K \to (\mathbb{Z}/N)^\times$ d'ordre $N = |G|$ du corps K (e.g. [De;(iii) p.233]). On fait l'hypothèse un peu plus forte suivante.

Hypothèse *(A). L'action $\rho : G_K \to S_r$ est compatible avec l'action cyclotomique de G_K sur $\widehat{C}_1, \ldots, \widehat{C}_r$.*

Exemples. (a) Le cas particulier $\rho = 1$ correspond à la situation où $t_1, \ldots, t_r$ sont K-rationnels. On a $U_\rho^r = U^r(K)$ où U^r désigne l'ensemble $(\mathbb{P}^1)^r$ privé des points $(t_1, \ldots, t_r)$ dont deux au moins des coordonnées sont égales. L'hypothèse *(A)* est l'hypothèse classique de K-rationalité des classes $\widehat{C}_1, \ldots, \widehat{C}_r$ (e.g. [Se]).

(b) Pour $K = \mathbb{R}$ et r_1 et r_2 deux entiers ≥ 0 tels que $r_1+2r_2 = r$, on note $\rho_{r_1,r_2} : G_{\mathbb{R}} \to S_r$ l'action de $G_{\mathbb{R}} = \{1, c\}$ sur $\{1, \ldots, r\}$ donnée par

$$\rho_{r_1,r_2}(c) = (r_1 + 1\ r)(r_1 + 2\ r - 1)\ldots(r_1 + r_2 + 1\ r_1 + r_2)$$

L'ensemble $U^r_{\rho_{r_1,r_2}}$, noté plus simplement $U^r_{r_1,r_2}$, est alors le sous-ensemble de $U^r(\mathbb{C})$ constitué des r-uplets de la forme $(t_1, \ldots, t_{r_1}, z_1, \ldots, z_{r_2}, \bar{z}_{r_2}, \ldots, \bar{z}_1)$ où $t_i \in \mathbb{P}^1(\mathbb{R}), i = 1, \ldots, r_1$ et $z_i \notin \mathbb{R}, i = 1, \ldots, r_2$. L'hypothèse *(A)* s'écrit: $\widehat{C}_i = (\widehat{C}_i)^{-1}, i = 1, \ldots, r_1$ et $(\widehat{C}_{r_1+i})^{-1} = \widehat{C}_{r+1-i}, i = 1, \ldots, r_2$.

Si $\rho : G_K \to S_r$ est une action de G_K sur $\{1, \ldots, r\}$, alors il existe deux entiers r_1 et r_2 et une indexation de $\{1, \ldots, r\}$ tels que ρ prolonge ρ_{r_1,r_2}. On supposera toujours qu'on a fait le choix préalable d'une telle indexation. On peut montrer alors que:

LEMME — *U^r_ρ est dense dans $U^r_{r_1,r_2}$.*

La descente du corps de définition s'effectue en deux temps: d'abord du corps $\overline{K}$ au sous-corps K^{tr} constitué des éléments totalements réels de $\overline{K}$ (i.e., dont tous les conjugués sur K sont réels), puis du corps K^{tr} au corps K. La première partie de la descente utilise la théorie des espaces de Hurwitz [FrV]. La condition *($\mathfrak{H}$/Ex)* ci-dessous garantit leur existence, pour la donnée $(\widehat{G}, \widehat{\mathbf{C}})$. On note $sni(\widehat{\mathbf{C}})$ l'ensemble

$$sni(\widehat{\mathbf{C}}) = \{\ (g_1, \ldots, g_r) \in \widehat{G}^r |\ g_1 \cdots g_r = 1, < g_1, \ldots, g_r >= \widehat{G}, g_i \in \widehat{C}_i,\ i = 1, \ldots, r\}$$

($\mathfrak{H}$/Ex) Le groupe $\widehat{G}$ est de centre trivial, le "diviseur des classes" $(\widehat{C}_1) + \cdots + (\widehat{C}_r)$ est K-rationnel (i.e., invariant sous l'action de G_K) et l'ensemble $sni(\widehat{\mathbf{C}})$ est non vide.

Plus précisément, sous la condition *($\mathfrak{H}$/Ex)*, il existe une variété algébrique (pas nécessairement irréductible), appelée espace de Hurwitz et notée $\widehat{\mathfrak{H}} = \widehat{\mathfrak{H}}(\widehat{G}, \widehat{\mathbf{C}})$, définie sur K et qui a la propriété suivante: les G-revêtements, ramifiés en r points, de groupe $\widehat{G}$, d'i.c.i. le r-uplet $\widehat{\mathbf{C}}$ (à l'ordre près) et définis sur un corps k contenant K correspondent aux points k-rationnels sur $\widehat{\mathfrak{H}}$. D'autre part, l'application $\Psi : \widehat{\mathfrak{H}} \to Div_r(\mathbb{P}^1)$ qui à un point de $\widehat{\mathfrak{H}}$ associe le diviseur de degré r, $(t_1) + \cdots (t_r)$, des points de ramification du revêtement correspondant, est un morphisme, fini et défini sur K. Son image, notée U_r, est l'image de U^r (qui est défini dans l'exemple (a)) par l'application naturelle $\nu : (\mathbb{P}^1)^r \to Div_r(\mathbb{P}^1)$. On introduit aussi l'espace de Hurwitz "pur" $\widehat{\mathfrak{H}}' = \widehat{\mathfrak{H}}'(G, \mathbf{C})$. Tout point $\mathbf{h}' = (\mathbf{h}, \mathbf{t})$ du produit fibré $\widehat{\mathfrak{H}} \times_\nu U^r$ correspond à un G-revêtement donné avec une indexation $\mathbf{t} = (t_1, \ldots, t_r)$ de ses points de ramification. On peut donc parler de l'i.c.i. du point $\mathbf{h}'$. Cette fonction i.c.i. est constante sur tout sous-ensemble connexe de $\widehat{\mathfrak{H}} \times_\nu U^r$. L'espace $\widehat{\mathfrak{H}}'$ est défini comme la réunion des composantes absolument irréductibles de $\widehat{\mathfrak{H}} \times_\nu U^r$ d'i.c.i. égal au r-uple $\mathbf{C}$. Le diagramme de la première page résume la situation.

La descente sur le corps $\overline{K} \cap \mathbb{R}$ est une première obstruction au problème. Cette question a été traitée dans [DFr]; le paramètre important est l'ensemble

$$sni(\widehat{\mathbf{C}}, r_1, r_2) = \left\{ (g_1, \ldots, g_r) \in sni(\widehat{\mathbf{C}}) \,\middle|\, \exists g_0 \in \widehat{G} \mid \begin{cases} (g_0 \cdots g_i)^2 = 1,\ i = 0, \ldots, r_1 \\ g_{r+1-i} = g_o (g_{r_1+i})^{-1} g_o,\ i = 1, \ldots, r_2 \end{cases} \right\}$$

De façon précise, soit Γ_o la composante connexe de $U^r_{r_1,r_2}$ constituée des r-uplets $(t_1, \ldots, t_r) \in U^r_{r_1,r_2}$ vérifiant la condition

$$t_1 < \cdots < t_{r_1} \quad \text{et} \quad Im(t_i) > 0, i = r_1 + 1, \ldots, r_1 + r_2. \tag{2}$$

On a alors équivalence entre la condition " $\pi(\Psi'^{-1}(\Gamma_o)) \cap \widehat{\mathfrak{H}}(\mathbb{R}) \neq \emptyset$" et la condition "$sni(\widehat{\mathbf{C}}, r_1, r_2) \neq \emptyset$". L'hypothèse *(B)* du Théorème porte sur les points totalement réels des espaces de Hurwitz.

Hypothèse *(B). En plus de l'hypothèse (𝔊/Ex), on suppose qu'il existe* $\mathbf{t} = (t_1, \dots, t_r)$ *dans* $U_\rho^r \cap \Gamma_o$ *tel que* $\pi_($ $\Psi'^{-1}(\mathbf{t})) \cap \widehat{\mathfrak{H}}(K^{tr}) \neq \emptyset$.

L'hypothèse *(B)* est très générale. Nous indiquons ci-dessous un critère pratique garantissant une telle condition (Cf. Remarque (b)). Ce critère est loin d'être optimal. Si, dans le Théorème, on le substitue à l'hypothèse *(B)*, on retrouve le critère classique de rigidité. Les travaux récents de F. Pop notamment (Cf. Remarque (a)) laissent penser qu'il devrait être possible de l'améliorer. Nous faisons la conjecture ci-dessous, qui, sous des hypothèses convenables sur $\widehat{G}$ et $\widehat{\mathbf{C}}$, garantit l'hypothèse *(B)*. Cette conjecture est vraie si $\widehat{\mathfrak{H}}(K)$ est dense dans $\widehat{\mathfrak{H}}(\mathbb{R})$.

DEFINITION — *Une fibre* $\Psi'^{-1}(\mathbf{t})$ *avec* $\mathbf{t} \in U^r(\overline{K})$ *du morphisme* $\Psi' : \widehat{\mathfrak{H}}' \to U^r$ *sera dite* K*-rationnelle sur* $\widehat{\mathfrak{H}}$ *si son image par* $\pi : \widehat{\mathfrak{H}}' \to \widehat{\mathfrak{H}}$ *est invariante sous l'action de* G_K.

Ou, de façon équivalente, si $\nu(\mathbf{t}) = (t_1) + \cdots (t_r)$ est K-rationnel sur U_r et si les actions de G_K sur $\{t_1, \dots, t_r\}$ et sur $\widehat{C}_1, \dots, \widehat{C}_r$ sont compatibles. On introduit aussi les trois conditions suivantes. La dernière garantit l'absolue irréductibilité de l'espace de Hurwitz $\widehat{\mathfrak{H}}(\widehat{G}, \widehat{\mathbf{C}})$ [FrV;§1]; en particulier, *(Trans)*, combiné à *(𝔊/Ex)*, entraine *(𝔊/c.def)*.

(Desc/$\mathbb{R}$*)* *Le groupe* $\widehat{G}$ *est de centre trivial, et, il existe deux entiers* $r_1, r_2 \geq 0$ *tels que* $r_1 + 2r_2 = r$ *et* $sni(\widehat{\mathbf{C}}, r_1, r_2) \neq \emptyset$, *et une action* $G_K \to S_r$ *qui prolonge* ρ_{r_1, r_2} *et qui est compatible avec l'action cyclotomique de* G_K *sur* $\widehat{C}_1, \dots, \widehat{C}_r$.

(𝔊/c.def) *Les composantes irréductibles de* $\widehat{\mathfrak{H}}$ *qui coupent* $\widehat{\mathfrak{H}}(\mathbb{R})$ *sont définies sur* K.

(Trans) *Le groupe des tresses d'Hurwitz* $H(r)$ *opère transitivement sur* $ni(\widehat{\mathbf{C}})^{in}$.

CONJECTURE — *Soient* r, $\widehat{G}$, $\widehat{\mathbf{C}} = (\widehat{C}_1, \dots, \widehat{C}_r)$ *vérifiant les conditions (Desc/*$\mathbb{R}$*) et (𝔊/c.def). Si* Γ *est une composante connexe de* $\nu^{-1}(U_r(\mathbb{R}))$ *vérifiant:*
(i) $\pi(\Psi'^{-1}(\Gamma)) \cap \widehat{\mathfrak{H}}(\mathbb{R}) \neq \emptyset$,
(ii) Pour tout $\mathbf{t}$ *dans une partie dense de* Γ, *la fibre* $\Psi'^{-1}(\mathbf{t})$ *est* K*-rationnelle sur* $\widehat{\mathfrak{H}}$,
alors il existe une fibre $\Psi'^{-1}(\mathbf{t})$ *avec* $\mathbf{t} \in \Gamma \cap U^r(\overline{K})$, K*-rationnelle sur* $\widehat{\mathfrak{H}}$ *et telle que* $\pi(\Psi'^{-1}(\mathbf{t})) \cap \widehat{\mathfrak{H}}(K^{tr}) \neq \emptyset$.

Remarques. (a) F. Pop [Po] a démontré l'implication "$V(\mathbb{R}) \neq \emptyset \Rightarrow V(\mathbb{Q}^{tr}) \neq \emptyset$" pour toute variété absolument irréductible définie sur $\mathbb{Q}^{tr}$. Si l'espace $\widehat{\mathfrak{H}}$ est absolument irréductible, la condition "$sni(\widehat{\mathbf{C}}, r_1, r_2) \neq \emptyset$" entraine donc que "$\widehat{\mathfrak{H}}(\mathbb{Q}^{tr}) \neq \emptyset$". C'est une conclusion plus faible que celle de l'hypothèse *(B)*; elle permet cependant de montrer que tout groupe est groupe de Galois sur $\mathbb{Q}^{tr}(T)$ [DFr].

(b) On peut montrer que, sous l'hypothèse *(A)*, la condition "$sni(\widehat{\mathbf{C}}, r_1, r_2) = sni(\widehat{\mathbf{C}})$" entraine que, pour tout $\mathbf{t} = (t_1, \dots, t_r) \in U_\rho^r \cap \Gamma_o$, on a $\pi_($ $\Psi'^{-1}(\mathbf{t})) \subset \widehat{\mathfrak{H}}(K^{tr})$. En particulier, l'hypothèse *(B)* est satisfaite.

Les notations suivantes apparaissent dans l'énoncé de la dernière hypothèse du Théorème. Pour $\widehat{A} \subset \widehat{G}^r$, $p(\widehat{A})$ désigne l'image de $\widehat{A}$ par l'homomorphisme produit $p \times \cdot \times p$ induit

par p sur $\widehat{G}^r$. Pour $A \subset G^r$, A^{in} désigne l'ensemble A regardé modulo l'action des automorphismes intérieurs de G sur G^r. Par exemple, l'hypothèse classique de rigidité (e.g. [Se]) s'écrit "$\left|sni(\mathbf{C})^{in}\right| = 1$". L'hypothèse *(C)* peut lui être comparée.

Hypothèse *(C).* $\qquad \left|p(sni(\widehat{\mathbf{C}}, r_1, r_2))^{in}\right| = 1$

dém du Théorème. Pour $(t_1, \ldots, t_r)$ un r-uplet dans $U_\rho^r \cap \Gamma_o$, on note $\Pi_{\overline{K}}$ le groupe fondamental géométrique et Π_K le K-groupe fondamental arithmétique de $\mathbb{P}^1 \backslash \{t_1, \ldots, t_r\}$ (e.g. [Se;Ch.7]). On sait que le groupe $\Pi_{\overline{K}}$ est isomorphe au complété profini du groupe libre $F(x_1, \ldots, x_r)/x_1 \cdots x_r$ en r générateurs $x_1, \ldots, x_r$ avec l'unique relation $x_1 \cdots x_r = 1$. Et que, un "point-base" $t_o \in \mathbb{P}^1(K) \backslash \{t_1, \ldots, t_r\}$ étant fixé, il existe une action de G_K sur $\Pi_{\overline{K}}$ pour laquelle on a l'isomorphisme $\Pi_K \simeq \Pi_{\overline{K}} \times^s G_K$. De plus, on peut choisir les générateurs $x_1, \ldots, x_r$ de telle sorte que l'action de la conjugaison complexe c soit donnée par les "formules de Hurwitz" suivantes

$$(3) \qquad \begin{cases} (cx_1 \cdots x_i)^2 = 1, \ i = 1, \ldots, r_1 \\ x_{r+1-i} = c(x_{r_1+i})^{-1} c, \ i = 1, \ldots, r_2 \end{cases}$$

De l'hypothèse *(B)*, on déduit qu'il existe un r-uplet $(t_1, \ldots, t_r) \in U_\rho^r \cap \Gamma_o$ et un homomorphisme surjectif $\widehat{\Phi} : \Pi_{\overline{K}} \to \widehat{G}$ tel que $\widehat{\Phi}(x_i) \in \widehat{C}_i, i = 1, \ldots, r$ et qui se prolonge en un homomorphisme $\widehat{\Phi} : \Pi_{K^{tr}} \to \widehat{G}$. Posons $\Phi = p \circ \widehat{\Phi}$. On déduit de (3) et de l'hypothèse *(A)* que, pour tout $\tau \in G_K$, $(\Phi(x_1^\tau), \ldots, \Phi(x_r^\tau)) \in p(sni(\widehat{\mathbf{C}}, r_1, r_2))$. L'hypothèse *(C)* permet de conclure qu'il existe $\phi_\tau \in G$ tel que $\Phi(x_i^\tau) = \phi_\tau \Phi(x_i)(\phi_\tau)^{-1}, i = 1, \ldots, r$, ce qui signifie exactement que le corps des modules du G-revêtement $\varphi : X \to \mathbb{P}^1$ correspondant à l'homomorphisme $\Phi : \Pi_{\overline{K}} \to G$ est égal à K.

Sous les conditions *(Desc/$\mathbb{R}$)* et *($\mathfrak{H}$/c.def)* qui ne dépendent que de $\widehat{G}$ et $\widehat{\mathbf{C}}$, la Conjecture entraine qu'il existe $\rho : G_K \to S_r$ tel que les hypothèses *(A)* et *(B)* soient vérifiées. D'autre part, la démonstration montre plus précisément que, sous les hypothèses *(A)*, *(B)*, le terme de gauche dans l'hypothèse *(C)* est un majorant du degré sur K du corps des modules du G-revêtement $\varphi : X \to \mathbb{P}^1$. On obtient donc le corollaire suivant.

COROLLAIRE — *Soient $\widehat{G}$ un groupe fini et $(\widehat{C}_1, \ldots, \widehat{C}_r)$ un r-uplet de classes de conjugaison de $\widehat{G}$ satisfaisant les conditions (Trans) (ou plus généralement ($\mathfrak{H}$/c.def)) et (Desc/$\mathbb{R}$). Soit $p : \widehat{G} \to G$ un homomorphisme de groupes surjectif. Alors, sous la Conjecture, il existe un G-revêtement $\varphi : X \to \mathbb{P}^1$ de groupe G, ramifié en r points, d'i.c.i. le r-uplet $\mathbf{C} = (C_1, \ldots, C_r)$ où $C_i = p(\widehat{C}_i)$, $i = 1, \ldots, r$ et dont le corps des modules est une extension de K de degré inférieur ou égal au cardinal de l'ensemble $p(sni(\widehat{\mathbf{C}}, r_1, r_2))^{in}$ (où r_1, r_2 sont donnés par la condition (Desc/$\mathbb{R}$)).*

Exemple. (c) D'après un résultat de Fried et Völklein [FrV;Lemma 2], tout groupe G est quotient d'un groupe $\widehat{G}$ de centre trivial et dont le groupe des multiplicateurs de Schur est "engendré par les commutateurs". Soient $\widehat{B}_1, \ldots, \widehat{B}_s, \widehat{D}_1, \ldots, \widehat{D}_t, (\widehat{D}_1)^{-1}, \ldots, (\widehat{D}_t)^{-1}$ une indexation de toutes les classes de conjugaison non triviales de $\widehat{G}$ telle que les classes $\widehat{B}_i$ soient exactement les classes de $\widehat{G}$ égales à leurs inverses $(\widehat{B}_i)^{-1}, i = 1, \ldots, s$. Pour b entier > 0, on pose $r = b(s + 2t)$, $r_1 = bs$, $r_2 = bt$ et on note $\widehat{\mathbf{C}}$ le r-uplet commençant par le s-uplet $(\widehat{B}_1, \ldots, \widehat{B}_r)$ répété b fois, suivi du t-uplet $(\widehat{D}_1, \ldots, \widehat{D}_t)$ répété b fois et se terminant par le t-uplet $((\widehat{D}_t)^{-1}, \ldots, (\widehat{D}_1)^{-1})$ répété b fois. D'après un résultat de Conway et Parker [FrV;Appendix], la condition *(Trans)* est satisfaite dès que b est suffisamment grand ($b \geq b_o(\widehat{G})$). Sous la Conjecture, on a donc la conclusion suivante:

(4) Pour tout entier $b \geq b_o(\widehat{G})$ tel que $sni(\widehat{\mathbf{C}}, bs, bt) \neq \emptyset$, il existe un G-revêtement $\varphi : X \to \mathbb{P}^1$ ramifié en au plus $r = b(s + 2t)$ points, de groupe G et dont le corps des modules est une extension de K de degré inférieur ou égal au cardinal $|p(sni(\widehat{\mathbf{C}}, bs, bt))^{in}|$.

REFERENCES

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

[DFr] P. Dèbes and M. Fried, Nonrigid situations in constructive Galois theory, submitted to Pacific J. Math.

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

[Po] M. Pop, The totally real numbers are PRC, preprint (1990), 771–800.

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

"Problèmes diophantiens", Univ. P. et M. Curie, Math., UFR 920, Tour 45-46, 5ème étage, BP 172, 4 Place Jussieu,75252 PARIS Cedex 05, E-mail: pde@frunip62.bitnet