Contemporary Mathematics
Volume 186, 1995

Existence de points p-adiques pour tout p sur un espace de Hurwitz

BRUNO DESCHAMPS

ABSTRACT. From a result of M.Fried and H.Völklein one can reduce the inverse Galois problem to finding $\mathbb{Q}$-rational points on Hurwitz spaces. Our aim, here, is to construct, for every finite group G, a Hurwitz space $\mathfrak{H}$ such that $\mathbb{Q}$-rational points on $\mathfrak{H}$ yield a Galois regular extension of $\mathbb{Q}(T)$ of Galois group G and which has $\mathbb{Q}_p$-rational points for all primes p (including $p = \infty$).

1. Introduction

1.1. Enoncé du résultat. D'après un résultat fondamental de M.Fried et H.Völklein [**FrV**] on sait que pour tout groupe fini G donné, il existe une variété algébrique irréductible, définie sur $\mathbb{Q}$ vérifiant:

(A) *Pour tout corps commutatif K contenant $\mathbb{Q}$, à tout point K-rationnel de cette variété on peut associer une extension galoisienne régulière de $K(T)$ de groupe de Galois G.*

En fait à un point K-rationnel on associe un G-revêtement défini sur K et de groupe de Galois G.

P.Dèbes [**Deb1**] en reprenant ce résultat et en le combinant avec ceux de D.Harbater et Q.Liu ([**Har**], [**Liu**]) prouve que pour tout p premier (y compris $p = \infty$) il existe une variété, $\mathfrak{H}_p$, irréductible, définie sur $\mathbb{Q}$, vérifiant la propriété (A) et possédant un point $\mathbb{Q}_p$-rationnel (resp. $\mathbb{R}$-rationnel pour $p = \infty$). Grâce à un résultat de F.Pop, il en déduit l'existence d'un point $\mathbb{Q}^{tp}$-rationnel (on rappelle que $\mathbb{Q}^{tp}$ est le corps des nombres totalement p-adiques, i.e., l'ensemble des nombres algébriques p-adiques qui n'ont que des conjugués p-adiques par l'action de $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$) et donc que tout groupe fini est groupe de Galois d'une

1991 *Mathematics Subject Classification.* Primary 12F12, 14H30; Secondary 14G20, 11Gxx.
This paper is in final form and no version of it will be submitted for publication elsewhere.

extension de $\mathbb{Q}^{tp}(T)$. Il pose ensuite la question de savoir si l'on peut choisir $\mathfrak{H}_p$ indépendamment de p.

L'objet de cet article est d'apporter une réponse positive à cette question, plus précisément:

THÉORÈME 1. *Pour tout groupe fini G, il existe une variété algébrique, irréductible et définie sur $\mathbb{Q}$ (vérifiant la propriété (A)) et vérifiant en outre:*

1. Pour réaliser G comme groupe de Galois sur $\mathbb{Q}(T)$ il suffit de trouver un point $\mathbb{Q}$-rationnel sur cette variété.

2. Pour tout p premier (y compris $p = \infty$), il existe un point $\mathbb{Q}_p$-rationnel x_p sur cette variété (il existe même des points $\mathbb{Q}^{tp}$-rationnels).

3. Le G-revêtement défini sur $\mathbb{Q}_p$ associé au point x_p, a des points de ramification dans $\mathbb{P}^1(\mathbb{Q}^{ab})$ qui sont globalement invariants par l'action de $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$.

Il est naturel de se demander si on peut déduire de l'existence de points $\mathbb{Q}_p$-rationnels pour tout p l'existence d'un point $\mathbb{Q}$-rationnel sur les espaces de Hurwitz? Il s'agit d'un problème "local-global", type principe de Hasse, qui est aussi évoqué dans [**Deb1**]: un exemple tiré de [**DFr**] montre que ce n'est pas toujours possible.

1.2. Rappels préliminaires.

1.2.1 Espaces de Hurwitz. On rappelle ici brièvement les propriétés des espaces de Hurwitz, on trouvera tous les détails dans [**FrV**].

Soit G un groupe fini de centre $Z(G)$ trivial, $r > 2$ un entier. Prenons un r-uplet $\mathbf{C} = (C_1, \cdots, C_r)$ de classes de conjugaison d'éléments de G, on suppose que $\mathbf{C}$ est rationnel (i.e., invariant à l'ordre près par élévation à toute puissance première à $card(G)$).

PROPOSITION 1.2.1. *Sous les conditions précédentes, il existe une variété $\mathfrak{H}(\mathbf{C}, G)$ définie sur $\mathbb{Q}$ telle que pour tout corps commutatif K contenant $\mathbb{Q}$, les propriétés suivantes soient équivalentes:*

i) $\mathfrak{H}(K) \neq \emptyset$

ii) Il existe un G-revêtement (i.e., un revêtement galoisien de $\mathbb{P}^1$ de groupe de Galois G donné avec l'action de G) défini sur K, non ramifié en dehors de r points distincts de $\mathbb{P}_1$ et tel que l'invariant canonique de l'inertie (Cf. [**Deb1**] *(§2.2 page 3)) de ce G-revêtement est égal, à l'ordre près, à $\mathbf{C} = (C_1, \cdots, C_r)$.*

On appelle cette variété l'espace de Hurwitz associé à G et à $\mathbf{C}$, on le note parfois simplement $\mathfrak{H}(\mathbf{C})$.

Rappellons aussi, le résultat concernant l'irréductibilité de $\mathfrak{H}(\mathbf{C})$, dû a J.H. Conway et R.A. Parker (Cf. [**CP**] et [**FrV**] (appendix)):

PROPOSITION 1.2.2. *Sous les conditions de la proposition précédente et en supposant de plus que le groupe des multiplicateurs de Schur est engendré par les commutateurs (Cf.* [**FrV**]*), il existe un entier b_0 dépendant de G tel que si chaque classe de conjugaison de G apparaît au moins b_0 fois dans $\mathbf{C}$, alors $\mathfrak{H}(\mathbf{C})$ est irréductible.*

On se placera désormais dans le cas où G vérifie les conditions ci-dessus et on démontrera le théorème suivant:

THÉORÈME 2. *Soit G un groupe fini de centre trivial, tel que le groupe des multiplicateurs de Schur soit engendré par les commutateurs. Il existe un entier r et un r-uplet de classes de conjugaison $\mathbf{C}$ de G tels que l'espace de Hurwitz $\mathfrak{H}(\mathbf{C})$ soit une variété irréductible, définie sur $\mathbb{Q}$ et vérifiant (outre l'équivalence $i) \Leftrightarrow ii)$ de la Prop.1.2.1) les propriétés suivantes:*

1. Pour tout p premier (y compris $p = \infty$), $\mathfrak{H}(\mathbf{C})$ possède un point x_p $\mathbb{Q}_p$-rationnel. Il existe même des points $\mathbb{Q}^{tp}$-rationnels.

2. Le G-revêtement associé à x_p a des points de ramification dans $\mathbb{P}^1(\mathbb{Q}^{ab})$ qui sont globalement invariants par l'action de $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$.

Ce théorème implique le Th.1. En effet grâce au Lemme 2 de [**FrV**], on sait que tout groupe fini est quotient d'un groupe vérifiant les hypothèses du Th.2. La théorie de Galois permet alors de passer du Th.2 au Th.1.

1.2.2 Théorème d'Harbater. Le théorème d'Harbater peut se résumer par l'affirmation suivante:

Tout groupe fini est groupe de Galois d'une extension régulière de $\mathbb{Q}_p(T)$.

Liu dans [**Liu**] démontre ce résultat en reprenant les travaux d'Harbater, mais en utilisant la théorie des espaces analytiques rigides. Voilà le théorème qui lui permet d'arriver à ses fins.

On dit que la fibre au dessus d'un point t_0 d'un revêtement $\phi : X \to \mathbb{P}^1$ définie sur K, est totalement K-rationnelle, si $\phi^{-1}(t_0)$ est composée uniquement de points K-rationnels.

PROPOSITION 1.2.3. *Soit p un nombre premier, G un groupe fini engendré par deux de ses sous-groupes H_1, H_2. On suppose donnés deux G-revêtements $\pi_i : X_i \to \mathbb{P}^1$, $i = 1, 2$ définis sur $\mathbb{Q}_p$ de groupe de Galois respectifs H_1, H_2, ayant respectivement r_1 et r_2 points de ramification et $\mathbf{C_1} = (C_{11}, \cdots, C_{1r_1})$, $\mathbf{C_2} = (C_{21}, \cdots, C_{2r_2})$ pour invariant canonique de l'inertie. On suppose que chacun des deux revêtements possède un point $\mathbb{Q}_p$-rationnel non ramifié t_i, $i = 1, 2$, au dessus duquel la fibre est totalement $\mathbb{Q}_p$-rationnelle.*

Alors il existe un G-revêtement: $\pi : X \to \mathbb{P}^1$ sur $\mathbb{Q}_p$ de groupe de Galois G, avec $r = r_1 + r_2$ points de ramification, ayant $\mathbf{C} = (C_{11}^G, \cdots, C_{1r_1}^G, C_{21}^G, \cdots, C_{2r_2}^G)$ (où C_{ij}^G représente la classe de conjugaison dans G de C_{ij}) pour invariant canonique de l'inertie et possédant un point $\mathbb{Q}_p$-rationnel non ramifié au dessus duquel la fibre est totalement $\mathbb{Q}_p$-rationnelle.

Cette proposition permet de construire "à la main" des G-revêtements de $\mathbb{P}^1$ de groupe de Galois donné (Cf. [**Har**], [**Liu**], [**Des**]).

2. Démonstration du Théorème 2.

Soit G un groupe fini vérifiant les hypothèses du Th.2. Prenons pour chaque $x \in G\backslash\{1\}$ le sous-groupe $H_x =< x >$ engendré par x. On a $H_x \simeq \mathbb{Z}/\sharp x\mathbb{Z}$, où $\sharp x$ est l'ordre de x dans G. Notons $g_{x_1}, \cdots, g_{x_{\varphi(\sharp x)}} \in (\mathbb{Z}/\sharp x\mathbb{Z})^*$ (φ étant l'indicateur d'Euler) les générateurs de H_x et $C_{g_{x_1}}, \cdots, C_{g_{x_{\varphi(\sharp x)}}}$ leurs classes de conjugaison respectives dans G. Notons $C_x = (C_{g_{x_1}}, \cdots, C_{g_{x_{\varphi(\sharp x)}}})$ le r-uplet de ces classes de conjugaison. Notons $y_1, \ldots, y_{\sharp G}$ les éléments de G avec $y_1 = 1$. Considérons l'uplet $\mathbf{C} = (C_{y_2}, \ldots, C_{y_{\sharp G}})$ obtenu en mettant bout à bout les uplets C_{y_i}, $i = 2, \ldots, \sharp G$ (on élimine la classe de conjugaison triviale C_{y_1}). Pour $b \geq 1$ entier notons à présent $\mathbf{C}_b = (C, \cdots, C)$ le uplet obtenu en répétant b fois le uplet C. On a la proposition suivante:

PROPOSITION 2.0.4. *Pour b assez grand (par exemple supérieur à l'entier b_0 de la Prop.1.2.2), l'espace de Hurwitz $\mathfrak{H}(\mathbf{C}_b)$ associé à $\mathbf{C}_b$ est une variété qui vérifie les propriétés du Th.2.*

Les parties suivantes ont pour but de démontrer cette proposition.

2.1. Construction de G-revêtements de $\mathbb{P}^1$ définis sur $\mathbb{Q}_p$. Pour tout groupe fini G fixé, nous allons montrer qu'il est toujours possible de construire un G-revêtement de $\mathbb{P}^1$ défini sur $\mathbb{Q}_p$ de groupe de Galois G tel que le nombre de points de ramification et l'invariant canonique de l'inertie de ces revêtements soient des données indépendantes de p.

2.1.1. Réalisation pour $G = \mathbb{Z}/n\mathbb{Z}$. Soit K un corps commutatif de caractéristique nulle. Il est classique qu'on peut réaliser tout groupe fini sur $\overline{K}(T)$. Le véritable problème est celui de la descente de $\overline{K}$ à K. La théorie du groupe fondamental algébrique permet de poser le problème de la façon suivante. On pourra consulter [**Deb2**] pour plus de détails.

Etant donnés r points distincts $\{t_1, \cdots, t_r\}$ dans $\mathbb{P}^1(\overline{K})$ globalement invariants par $Gal(\overline{K}/K)$, on note Ω l'extension algébrique maximale de $\overline{K}(T)$ non ramifiée en dehors de $t_1, \cdots, t_r$. On note Π^{alg} le groupe de Galois $Gal(\Omega/\overline{K}(T))$, et x_i le générateur canonique des groupe d'inertie au dessus de t_i, $i = 1, \ldots, r$ (Cf. [**Deb2**] page 231 "Structure des groupes d'inertie".). Le groupe Π^{alg} est le groupe profini libre engendré par $x_1, \ldots, x_r$ modulo l'unique relation $x_1 \cdots x_r = 1$.

PROPOSITION 2.1.1. *Un groupe fini G est groupe de Galois d'une extension régulière de $K(T)$ si et seulement si, il existe:*

1. un entier $r > 0$, r points distincts $t_1, \cdots, t_r$ dans $\mathbb{P}^1(\overline{K})$ globalement invariants par $Gal(\overline{K}/K)$ et $t_0 \in \mathbb{P}^1(K)\backslash\{t_1, \cdots, t_r\}$,

2. des éléments $g_1, \cdots, g_r$ de G engendrant G et de produit $g_1 \cdots g_r = 1$,

3. un morphisme de groupes $\tau \to f_\tau$ de $Gal(\overline{K}/K)$ dans G,

tels que le morphisme de groupe $f : \Pi^{alg} \to G$ défini par $f(x_i) = g_i$ vérifie:

$$(1) \qquad f(x_i^\tau) = f_\tau g_i f_\tau^{-1} \text{ pour tout } i = 1, \cdots, r \text{ et tout } \tau \in Gal(\overline{K}/K)$$

Le G-revêtement de $\mathbb{P}^1$ défini sur K associé à cette extension de $K(T)$ est alors de groupe de Galois G, non ramifié en dehors de $t_1, \cdots, t_r$ et a pour invariant canonique de l'inertie le r-uplet $\mathbf{C} = (C_1, \cdots, C_r)$ où C_i est la classe de conjugaison de g_i dans G, $i = 1, \ldots, r$.

Rappellons un lemme dont la démonstration pourra être trouvée dans [**Deb2**].

LEMME 2.1.2. *Avec les notations précédentes on a:*
Pour tout $i = 1, \cdots, r$, x_i^τ est conjugué dans Π^{alg} à $(x_j)^{\chi_K(\tau)}$, où $t_j = t_i^\tau$ et $\chi_K : Gal(\overline{K}/K) \to \prod_{n>0} Gal(K(\xi_n)/K)$ (ξ_n racine primitive n-ième de l'unité), désigne le caractère cyclotomique du corps K.

D'après ce qui précède, pour réaliser $\mathbb{Z}/n\mathbb{Z}$ comme groupe de Galois sur $\mathbb{Q}(T)$ il faut et il suffit de trouver $r \in \mathbb{N}$, $\{t_1, \cdots, t_r\} \in \mathbb{P}^1(\overline{\mathbb{Q}})$ et des générateurs $(g_1, \cdots, g_r) \in (\mathbb{Z}/n\mathbb{Z})^r$ vérifiants $g_1 + \cdots + g_r = 0$ tel que:

$$(2) \qquad \text{Pour tout } \tau \in Gal(\overline{\mathbb{Q}}/\mathbb{Q}) : \ \chi_{\mathbb{Q}}(\tau) g_j = g_i \text{ avec } t_j = t_i^\tau$$

En effet, Lemme 2.1.2 donne que $f(x_i^\tau)$ est conjugué dans G à $f(x_j)^{\chi_{\mathbb{Q}}(\tau)}$. Mais le groupe G étant commutatif. On a $f(x_i^\tau) = f((x_j)^{\chi_{\mathbb{Q}}(\tau)}) = g_j^{\chi_{\mathbb{Q}}(\tau)}$. La formule (1) à réaliser se réduit donc à

$$(3) \qquad g_j^{\chi_{\mathbb{Q}}(\tau)} = f_\tau g_i f_\tau^{-1} = g_i \text{ pour tout } i = 1, \cdots, r \text{ et tout } \tau \in Gal(\overline{K}/K)$$

ce qui correspond bien à la condition (2) (additive notation). De plus tout morphisme $\tau \to f_\tau$ convient. Nous prendrons le morphisme trivial, i.e., $f_\tau = 1$ pour tout $\tau \in Gal(\overline{\mathbb{Q}}/\mathbb{Q})$. Pour ce choix, le G-revêtement associé possède un point $\mathbb{Q}$-rationnel non ramifié au dessus duquel la fibre est totalement $\mathbb{Q}$-rationnelle. Cela résulte du fait général suivant (Prop.2.1 de [**Deb1**]): pour tout $\tau \in Gal(\overline{\mathbb{Q}}/\mathbb{Q})$, l'élément f_τ, vu dans S_d par la représentation régulière $G \hookrightarrow S_d$ de G, correspond à l'action de τ sur la fibre au dessus de t_0.

LEMME 2.1.3. *On peut réaliser $\mathbb{Z}/n\mathbb{Z}$ sur $\mathbb{Q}(T)$ en prenant $r = \varphi(n)$ (φ étant l'indicateur d'Euler), $t_i = \xi_i$ où ξ_i est la i-ième racine n-ième primitive de l'unité $i = 1, \cdots, r$ si $n \neq 2$. Si $n = 2$ il suffit de prendre t_1, t_2 deux points rationnels distincts quelconques pour réaliser $\mathbb{Z}/2\mathbb{Z}$.*

PREUVE.

1) $n \neq 2$: On va réaliser la condition (2) en prenant pour g_i les éléments de $(\mathbb{Z}/n\mathbb{Z})^*$ indicés correctement. Plus précisément, notons $g_1, \cdots, g_r$ les éléments

de $(\mathbb{Z}/n\mathbb{Z})^*$ avec $g_1 = 1$. Soit ξ une racine primitive n-ième de l'unité. On pose $t_i = \xi^{g_i}$. Alors on a:

$$\textit{Pour tout } \tau \in Gal(\overline{\mathbb{Q}}/\mathbb{Q}),\ (\xi)^\tau = \xi^{\chi_{\mathbb{Q}}(\tau)}$$

et ainsi si $(t_i)^\tau = t_j$, c'est à dire si $((\xi)^{g_i})^\tau = \xi^{g_j}$, alors, comme $(\xi^{g_i})^\tau = (\xi^\tau)^{g_i}$, on a nécessairement $\chi_{\mathbb{Q}}(\tau)g_i = g_j$, ce qui est bien ce que l'on demande.

De plus les g_i engendrent $\mathbb{Z}/n\mathbb{Z}$ (chacun d'eux le faisant). Il reste juste à vérifier que $\sum_{1\leq i\leq r} g_i = 0$.

Prenons un élément $x \in (\mathbb{Z}/n\mathbb{Z})^*$. Alors comme $n \neq 2$, on a $-x \neq x$ et $-x \in (\mathbb{Z}/n\mathbb{Z})^*$, ce qui assure bien que:

$$\sum_{x\in(\mathbb{Z}/n\mathbb{Z})^*} x = 0$$

2) $n = 2$: Réaliser $\mathbb{Z}/2\mathbb{Z}$ ne pose pas vraiment de problème. On prend ξ_1, ξ_2 deux points rationnels. Pour tout $\tau \in Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ on a ${\xi_i}^\tau = \xi_i$ $i = 1, 2$. On prend alors

$g_1 = g_2 = 1$ dans $(\mathbb{Z}/2\mathbb{Z})^* = 1$. □

On vient de réaliser les $\mathbb{Z}/n\mathbb{Z}$ comme groupes de Galois de G-revêtements de $\mathbb{P}^1$ définis sur $\mathbb{Q}$ possédant un point rationnel au dessus duquel la fibre est totalement $\mathbb{Q}$-rationnelle.

Par extension des scalaires, on obtient, pour tout p premier, un G-revêtement de $\mathbb{P}^1$, défini sur $\mathbb{Q}_p$, de groupe de Galois $\mathbb{Z}/n\mathbb{Z}$ et possédant un point $\mathbb{Q}_p$-rationnel au dessus duquel sa fibre est totalement $\mathbb{Q}_p$-rationnelle. Le nombre de ses points de ramification vaut $r = \varphi(n)$ (indépendant de p) et son invariant canonique de l'inertie vaut $\mathbf{C} = (C_1, \cdots, C_{\varphi(n)})$ (indépendant de p) où $C_i = \{g_i\}$ et $g_i \in (\mathbb{Z}/n\mathbb{Z})^*$. On appelle ce revêtement le $\mathbb{Z}/n\mathbb{Z}$-revêtement élémentaire de $\mathbb{P}^1$.

Note: Ce n'est pas un résultat nouveau, on sait déjà depuis longtemps réaliser les groupes abéliens sur $\mathbb{Q}(T)$ (e.g. [**Ser**]), mais ici on a un contrôle explicite sur la ramification.

2.1.2 Réalisation pour un groupe fini quelconque. Prenons un nombre premier p quelconque et un groupe fini G. Dans la suite, pour tout élément x dans un groupe G donné, on note n_x l'ordre de x et $H_x \simeq \mathbb{Z}/n_x\mathbb{Z}$ le groupe engendré par x dans G .

Pour tout $x \in G$ on prend le H_x-revêtement élémentaire de $\mathbb{P}^1$, $\phi_x^{elem} : X_x \to \mathbb{P}^1$. On "recolle" ces revêtements grâce à la Prop.1.2.3 et on obtient un G-revêtement $\phi^{HL} : X \to \mathbb{P}^1$ de groupe de Galois G. Le nombre de points de ramification et l'invariant canonique de l'inertie de ce revêtement sont indépendants de p. voir que cet invariant canonique de l'inertie est le uplet $\mathbf{C}$ du préambule de la Partie 2. On note à présent ce revêtement le revêtement HL de $\mathbb{P}^1$ associé à G.

LEMME 2.1.3. *L'invariant canonique de l'inertie du revêtement HL associé à G est un uplet rationnel.*

PREUVE. On pose $r = \sharp G$ (ordre de G) et $G = \{y_1, \cdots, y_r\}$ avec $y_1 = 1$ et on écrit l'invariant canonique de l'inertie $\mathbf{C}$ ainsi:

$$\mathbf{C} = (C_{y_2,1}, \cdots, C_{y_2,\varphi(n_{y_2})}, \cdots\cdots, C_{y_r,1}, \cdots, C_{y_r,\varphi(n_{y_r})})$$

où les $C_{y_i,j}$ sont les classes de conjugaison (notées $C_{g_{(y_i)_j}}$ en §2.0) des générateurs du groupe $< y_i >$. En fait, si on pose $C_i = (C_{y_i,1}, \cdots, C_{y_i,\varphi(n_{y_i})})$, on a alors:

$$\mathbf{C} = (C_2, \cdots, C_r)$$

Montrons que pour tout $a \in \mathbb{N}$ premier avec $\sharp G$ et tout indice $i = 2, \ldots, r$, C_i^a reste globalement invariant. L'application $\psi_a : (\mathbb{Z}/n_{y_i}Z)^* \to (\mathbb{Z}/n_{y_i}Z)^*$ qui à t associe t^a est une bijection. Toute classe $C_{y_i,j}$, $j = 1, \ldots, \varphi(n_{y_i})$, est la classe de conjugaison d'un générateur $t \in < y_i >$. La classe $(C_{y_i,j})^a$ est la classe de conjugaison dans G de t^a qui est aussi un générateur de $< y_i >$. Donc il existe k tel que $(C_{y_i,j})^a = C_{y_i,k}$. Cette correspondance se fait de façon biunivoque du fait de la bijectivité de ψ_a. Ceci achève la preuve.

De façon plus précise on vient de montrer que pour tout entier a premier avec $\sharp G$, il existe $(\sigma_2, \cdots, \sigma_r) \in S_{\varphi(n_{y_2})} \times \cdots \times S_{\varphi(n_{y_r})}$ tel que:

$$\begin{aligned}\mathbf{C}^a &= (C_{y_2,1}, \cdots, C_{y_2,\varphi(n_{y_2})}, \cdots\cdots, C_{y_r,1}, \cdots, C_{y_r,\varphi(n_{y_r})})^a \\ &= (C_{y_2,\sigma_2(1)}, \cdots, C_{y_2,\sigma_2(\varphi(n_{y_2}))}, \cdots\cdots, C_{y_r,\sigma_r(1)}, \cdots, C_{y_r,\sigma_r(\varphi(n_{y_r}))})\end{aligned}$$

Pour tout entier b, on "recolle" (par la Prop.1.2.3) b fois le revêtement HL associé à G, en regardant b fois G comme un de ses sous-groupes. On obtient alors un G-revêtement de $\mathbb{P}^1$ de groupe de Galois G avec un nombre de points de ramification indépendant de p et un invariant canonique de l'inertie égale au $\mathbf{C}_b$ du préambule de la partie 2. Cet uplet reste évidemment rationnel.

2.2. Fin de la preuve. Grâce à la Prop.1.2.2, pour b assez grand (par exemple $b \geq b_0$), l'espace de Hurwitz $\mathfrak{H}(\mathbf{C}_b)$ défini sur $\mathbb{Q}$ est irréductible. On vient de montrer que pour tout nombre premier p, il existe un G-revêtement de $\mathbb{P}^1$ défini sur $\mathbb{Q}_p$, de groupe de Galois G, ayant autant de points de ramification qu'il y a de classes dans $\mathbf{C}_b$ et $\mathbf{C}_b$ pour invariant canonique de l'inertie. Ceci prouve donc qu'il existe un point $\mathbb{Q}_p$-rationnel sur $\mathfrak{H}(\mathbf{C}_b)$.

Il nous reste à traiter le cas où $p = \infty$. C'est à dire qu'il nous faut prouver l'existence d'un G-revêtement $\beta : X \to \mathbb{P}^1$ défini sur $\mathbb{R}$ ayant autant de points de ramification qu'il y a de classes dans $\mathbf{C}_b$, G comme groupe de Galois et $\mathbf{C}_b$ pour invariant canonique de l'inertie.

Pour ce, nous rappellons ce résultat (e.g. [**DFr**;Th.3.1]):

LEMME 2.2.1. *Soit* $\mathbf{C} = (C_1, C_1^{-1} \cdots, C_r, C_r^{-1})$ *un* r*-uplet de couples inverses deux à deux de classes de conjugaison d'éléments de* G*. Supposons qu'il existe* $(g_1, \cdots, g_r) \in C_1 \times \cdots \times C_r$ *tel que* $< g_1, \cdots, g_r >= G$*. Alors il existe un* G*-revêtement de* $\mathbb{P}^1$ *défini sur* $\mathbb{R}$ *de groupe de Galois* G*, ayant* $2r$ *points de ramification et* $\mathbf{C}$ *pour invariant canonique de l'inertie.*

Ce lemme nous permet de conclure. En effet reprenons le uplet $\mathbf{C}_b$ précédent. On rappelle que si $G = \{1 = y_1, y_2, \cdots, y_{\sharp G}\}$ alors $\mathbf{C}_b = (C, \cdots, C)$ (b_0 fois C) avec $C = (C_{y_2}, \cdots, C_{y_{\sharp G}})$ où:

$C_{y_i} = (\{g_{1,y_i}\}^G, \cdots, \{g_{n_{y_i},y_i}\}^G)$ où les g_{j,y_i} sont les générateurs du sous-groupe $< y_i >$, si $n_{y_i} \neq 2$, et

$C_{y_i} = (\{y_i\}^G, \{y_i\}^G)$, si $n_{y_i} = 2$.

Dans les deux cas il est clair que l'on peut grouper par paires

(C_{ij}, C_{ij}^{-1}) les composantes du uplet C_{y_i}, $i = 2, \ldots, \sharp G$. Ceci assure donc que $\mathbf{C}_b$ vérifie les conditions du Lemme 2.2.1. Par conséquent il existe un G-revêtement de $\mathbb{P}^1$ défini sur $\mathbb{R}$, de groupe de Galois G ayant $\mathbf{C}_b$ pour invariant canonique de l'inertie. En conclusion il existe un point $\mathbb{R}$-rationnel sur l'espace de Hurwitz $\mathfrak{H}(\mathbf{C}_b)$.

Rappellons le résultat de Pop ([**PoRoGr**]) qui achèvera la preuve de la première assertion du Th.2:

PROPOSITION 2.2.1. *Dans toute variété lisse, irréductible, définie sur* $\mathbb{Q}$*, l'ensemble des points* $\mathbb{Q}^{tp}$*-rationnels est dense dans l'ensemble des points* $\mathbb{Q}_p$*-rationnels.*

Ainsi, pour tout premier p (y compris $p = \infty$), il existe au moins un point $\mathbb{Q}^{tp}$-rationnel sur $\mathfrak{H}(\mathbf{C}_b)$.

2.3 Des points de ramification sous l'action de $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$.

Cette partie, qui a pour but de prouver la deuxième assertion du Th.2, regarde plus précisément comment sont modifiés les points de ramification quand on "recolle" par le Th.1.2.3 les $\mathbb{Z}/n\mathbb{Z}$-revêtements élémentaires. Il faut rappeler (Cf. [**Liu**], [**Des**]) que la première étape de ce théorème de recollement consiste à mettre les points de ramification des deux revêtements que l'on souhaite recoller "en bonne position". On utilise pour cela des automorphismes de $\mathbb{P}^1$, i.e., des homographies $(az+b)/(cz+d)$ avec $a, b, c, d \in \mathbb{Q}_p$. Le corps $\mathbb{Q}$ étant dense dans le corps $\mathbb{Q}_p$, on peut en fait choisir a, b, c, d dans $\mathbb{Q}$. On obtient donc la conclusion suivante.

LEMME 2.3.1. *Soient* $\pi_i : X_i \to \mathbb{P}^1$, $i = 1, 2$ *deux* G*-revêtements définis sur* $\mathbb{Q}_p$ *vérifiant les hypothèses de la Prop.1.2.3. Supposons que* $t_1^i, t_2^i, \cdots, t_{n_i}^i$, $i = 1, 2$ *soient leurs points de ramification respectifs. Alors il existe* a_1, b_1, c_1, d_1 *et* a_2, b_2, c_2, d_2 *dans* $\mathbb{Q}$ *(dépendant des données précédentes et notamment de* p*) tel que l'ensemble des points* $v_{i,j} = \dfrac{a_i t_j^i + b_i}{c_i t_j^i + d_i}$ *soit l'ensemble des points de ramifications du revêtement* $\pi : X \to \mathbb{P}^1$ *obtenu en recollant* π_1 *et* π_2*.*

Il est clair que les $\mathbb{Z}/n\mathbb{Z}$-revêtements élémentaires ont des points de ramification définis sur $\mathbb{Q}^{ab}$ et globalement invariants par l'action de $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$: c'est toujours l'ensemble des racines primitives n-ièmes de l'unité pour un certain n. Grâce au Lemme précédent, il est alors clair que le revêtement obtenu en §2.2 a des points de ramification définis sur $\mathbb{Q}^{ab}$ et globalement invariants par $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$. Ceci achève la preuve du Th.2.

REFERENCES

[CP] J.H Conway and R.A Parker, *On the Hurwitz number of arrays of group elements*, preprint.

[Deb1] P.Dèbes, *Covers of $\mathbb{P}^1$ over the p-adics*, Proc. AMS.conf in Seattle, Contemporary Mathematics (1993).

[Deb2] P.Dèbes, *Groupes de Galois sur $K(T)$*, Séminaire de théorie des nombres de Bordeaux 2 (1990), 229–243.

[DFr] M.D Fried and P.Dèbes, *Nonrigid constructions in Galois theory*, Pacific J.Math.

[Des] B.Deschamps, *Autour d'un théorème d'Harbater*, Mémoire de DEA, Univ. Paris VI (1993).

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

[Har] D.Harbater, *Galois covering of the arithmetic line*, Lecture note in math. **1240** (1987).

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

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

[Ser] J.P Serre, *Topics in Galois theory*, Course at Harvard University, Jones and Bartlett Publishers, 1988.

"PROBLÈMES DIOPHANTIENS", UNIV. PARIS VI, MATH., UFR 920, TOUR 45-46, 5ÈME ÉTAGE, BP 172, 4 PLACE JUSSIEU, 75252 PARIS CEDEX 05, FRANCE.

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