Corps ψ-libres et théorie inverse de Galois infinie

Pierre Dèbes et Bruno Deschamps

Abstract.— We provide some tools to investigate the Inverse Galois Problem for profinite groups : the notions of ψ-freeness and regular ψ-freeness of a field, a general construction of infinite Galois extensions of $k(T)$ over a complete valued field k. An application is that if k is an henselian field of residue characteristic $p=0$ (*e.g.* $k=\mathbb{Q}((x))$), the free profinite group $\widehat{F}_\omega$ with countably many generators is the Galois group of a regular extension of $k^{\mathrm{cycl}}(T)$. This result extends to the case $p>0$ provided that $\widehat{F}_\omega$ is replaced by its maximal prime-to-p quotient $\widehat{F}_\omega^{(p')}$. We also show that, given a finite group G, if $\mathrm{char}(k)=0$ (or if G is p-perfect), for almost all primes ℓ, the universal ℓ-Frattini cover of G is the Galois group of a regular extension of $k(T)$ (no adjunction of roots of 1 is necessary here). In a parallel way our methods give rise to existence results of projective systems of rational points (over various valued fields) on certain infinite towers of moduli spaces of G-covers, like the modular towers of M. Fried.

Introduction.

Dans [Se2] exercise 1 p.36, J-P. Serre indique que $\mathbb{Z}_p$ n'est groupe de Galois d'aucune extension régulière de $\mathbb{Q}(T)$, ce qui montre que la forme régulière du problème inverse de Galois sur $\mathbb{Q}(T)$ n'est pas vraie pour les groupes profinis. L'énoncé reste vrai avec $\mathbb{Q}$ remplacé par tout corps k tel que $[k(\zeta_{p^n}):k]$ tend vers ∞ quand $n\rightarrow\infty$, où ζ_d désigne une racine primitive d-ième de l'unité dans $\overline{k}$ ($d\geq 1$) ; voir [Fr1] §7 qui montre bien, *via* le "branch cycle argument", que c'est le manque de racines de l'unité qui cause l'impossibilité. Mais si on adjoint à k le sous-groupe $\mu_\infty\subset\overline{k}^\times$ des racines de l'unité, le problème inverse de Galois pour les groupes profinis reste entier. Cet article contient le résultat suivant (§2 et §3.2).

Théorème — *Soit k un corps d'un des deux types suivants :*
(a) *corps valué hensélien de caractéristique résiduelle nulle et contenant μ_∞,*
(b) *corps réel clos.*
Alors le groupe prolibre $\widehat{F}_\omega$ à une infinité dénombrable de générateurs est groupe de Galois d'une extension régulière de $k(T)$ [1]*.*

Ce résultat s'applique par exemple pour le corps $k=\mathbb{Q}^{\mathrm{ab}}((x))$ des séries de Laurent formelles à coefficients dans $\mathbb{Q}^{\mathrm{ab}}$ (type (a)) et pour $k=\mathbb{R}$ (type (b)). Dans la situation (a) mais avec caractéristique résiduelle $p>0$ (*e.g.* $k=\mathbb{Q}_p\mathbb{Q}^{\mathrm{ab}}$), notre méthode fournit une conclusion plus faible où $\widehat{F}_\omega$ doit être remplacé par $\widehat{F}_\omega^{(p')}$ son quotient maximal premier à p. L'énoncé avec $k=\mathbb{Q}_p\mathbb{Q}^{\mathrm{ab}}$ et $\widehat{F}_\omega$ est plausible mais reste ouvert ; la difficulté inhérente à la caractéristique mixte est expliquée dans la remarque 3.3. Le passage à $k=\mathbb{Q}^{\mathrm{ab}}$ paraît même possible mais semble plus difficile ; ce serait une avancée certaine vers la conjecture de Shafarevich (remarque 3.6).

Notre résultat se place dans le prolongement des travaux de M. Fried, D. Harbater, Q. Liu, F. Pop et des deux auteurs sur la réalisation des groupes *finis* comme groupes de Galois sur $\mathbb{Q}_p(T)$. Les résultats connus, notamment le théorème principal de [Des1] sont retrouvés ici, comme cas particulier de notre méthode (§4.3 (d)).

Pour situer nos résultats dans un cadre plus général, nous commençons par introduire une nouvelle notion arithmétique : la ψ-liberté (§1). Un corps K est ψ-libre si et seulement si $\widehat{F}_\omega$ est groupe de Galois d'une extension de K. La ψ-liberté est une propriété strictement intermédiaire entre la propriété (Gal/Inv)(tout groupe fini est groupe de Galois sur K), et celle d'ω-liberté (tout problème de plongement sur K a une solution forte), qui, d'après Iwasawa, entraîne pour K dénombrable que

[0] MSC (2000) : Primary 12F12, 20E18 ; Secondary 14H30 12F10, 12E30

[1] Suivant l'usage nous dirons cela plutôt que "extension de $k(T)$ régulière sur k".

$\mathbf{G}_K \simeq \widehat{F}_\omega$. La ψ-liberté "passe" aux extensions de type fini (proposition 1.7) et une réciproque partielle due à A. Tamagawa (proposition 1.10) est vraie. On en déduit que le groupe de Galois absolu d'un corps ψ-libre dénombrable est quotient de tous ses sous-groupes ouverts (corollaire 1.8). Dans cette perspective, nous montrons qu'aucun corps de nombres n'est ψ-libre, ce qui va dans le sens d'une conjecture d'Uchida (remarque 1.9 (b)).

Nous passons ensuite à la ψ-liberté des corps de fonctions $k(T)$. Le cas où k est un corps réel clos est traité au §2 par des méthodes topologiques comme dans [DeFr] et [KrNe]. Pour les corps valués complets non archimédiens, ces méthodes sont remplacées par des techniques de recollement d'espaces analytiques (géométrie rigide ou formelle), qui sont, depuis les travaux d'Harbater, un outil classique du domaine. Dans cet article, nous adaptons ces techniques à des constructions de "tours infinies" d'extensions. Nous donnons au §3.1 une méthode générale pour la construction d'une tour $(K_n)_{n\geq 0}$ d'extensions galoisiennes de $k(T)$ réalisant (au sens de la théorie inverse de Galois) un système projectif donné $(G_n)_{n\geq 0}$ de groupes finis, de façon compatible. Pour la construction de chaque étage, nous suivons la méthode de Pop dans son travail sur le *demi-théorème d'existence de Riemann* [Po1]. Nous devons veiller en plus à la compatibilité des invariants des étages de la tour, ce qui impose notamment des restrictions sur le choix des points de branchement ; cela constitue l'obstacle technique majeur. Notre stratégie est d'ajouter encore d'autres contraintes pour ne laisser à chaque étage qu'un nombre fini (non nul) de possibilités ; c'est ce qui rend possible le "passage à l'infini" *via* un argument type Tychonoff. Pour cette construction, nous nous plaçons sous des hypothèses aussi générales que possible, notamment en ce qui concerne la caractéristique de k et sa caractéristique résiduelle, et la présence de racines de l'unité dans k.

Dans la dernière section, nous adoptons un point de vue modulaire. Combinée à des résultats de Fried [Fr2], la contruction générale du §3 permet, étant donné un système projectif $(G_n)_{n\geq 0}$ de groupes finis, de construire une tour $(\mathcal{H}_{G_n,r_n}(\mathbf{C}_n))_{n\geq 0}$ d'espaces de modules de G-revêtements possédant des systèmes projectifs de points rationnels sur divers corps k (de type (a) ou (b) comme ci-dessus). Par rapport aux résultats des sections 2 et 3, le théorème 4.1 ajoute ceci : d'une part, la tour $(\mathcal{H}_{G_n,r_n}(\mathbf{C}_n))_{n\geq 0}$ construite est indépendante du corps valué k, d'autre part, sous l'hypothèse supplémentaire $Z(G_n) = \{1\}$ $(n \geq 0)$, il est mis en évidence un système projectif de composantes irréductibles $\mathcal{H}_n^\infty \subset \mathcal{H}_{G_n,r_n}$ $(n \geq 0)$ définies sur $\mathbb{Q}$. On obtient également en §4.2 l'existence de systèmes projectifs de points p-adiques sur les *tours modulaires* de Fried. La construction fournit le résultat suivant (valable ici sans qu'il soit besoin d'adjoindre de racines de l'unité).

Théorème — *Soit (k, v) un corps valué hensélien. Soient G un groupe fini et ℓ un nombre premier tel qu'il existe un système de générateurs de G d'ordre premier à ℓ et à la caractéristique de k. Alors le ℓ-revêtement universel de Frattini ${}_\ell\tilde{G}$ de G est groupe de Galois d'une extension galoisienne régulière de $k(T)$.*

La considération de tours infinies d'extensions de $k(T)$ pose de nouvelles questions. Par exemple dans quelle mesure l'argument de descente sur les corps amples, classique pour des extensions finies, peut être adapté aux tours infinies (*cf.* §4.3 (b)) ? Pour un corps k hilbertien, on peut aussi s'intéresser à l'effet sur une tour de la spécialisation dans k de l'indéterminée T.

Remerciements. L'exemple 1.3 est dû à D. Haran, la proposition 1.10 à A. Tamagawa. Nous leur en sommes reconnaissants. Nous remercions aussi F. Pop pour ses indications très utiles sur la situation d'inégale caractéristique, ainsi que M. Jarden, M. Fried, M. Perret de leur intérêt pour notre travail et de leurs commentaires.

1.— ψ-liberté.

Nous appelons *système complet de groupes finis*, tout système projectif $(G_n, s_n)_{n\in\mathbb{N}}$ de groupes finis G_n $(n \geq 0)$ et d'épimorphismes $s_n : G_n \twoheadrightarrow G_{n-1}$ $(n > 0)$.

Définition 1.1.— *Un corps (commutatif) K est dit ψ-libre si pour tout système complet de groupes finis $(G_n, s_n)_n$, il existe une tour d'extensions galoisiennes finies $(K_n)_n$ de K telle que pour tout $n \in \mathbb{N}$ il existe un isomorphisme $\varepsilon_n : \mathrm{Gal}(K_n/K) \to G_n$ qui rende commutatif le diagramme suivant :*

$$\begin{tikzcd} \mathrm{Gal}(K_{n+1}/K) \arrow[r] \arrow[d, "\varepsilon_{n+1}"] & \mathrm{Gal}(K_n/K) \arrow[d, "\varepsilon_n"] \\ G_{n+1} \arrow[r, "s_{n+1}"] & G_n \end{tikzcd}$$

Si k est un corps, le corps $K = k(T)$ sera dit régulièrement ψ-libre si la condition précédente est satisfaite pour une tour $(K_n)_n$ d'extensions régulières de K.

Rappelons qu'un corps K est dit ω-libre si tout problème de plongement fini pour son groupe de Galois absolu $\mathbf{G}_K = \mathrm{Gal}(K^s/K)$ admet une solution (forte) [FrJa] §20.3. Un corps ω-libre est clairement ψ-libre.

La proposition suivante indique que la ψ-liberté d'un corps K peut-être caractérisée par l'ensemble des quotients de $\mathbf{G}_K$ par des sous-groupes fermés, c'est-à-dire, par l'ensemble des groupes de Galois sur K.

Proposition 1.2.— *Soient k et K deux corps. Les assertions suivantes se valent :*
(i) *K est ψ-libre (resp. $k(T)$ est régulièrement ψ-libre),*
(ii) *tout groupe profini métrisable est groupe de Galois sur K (resp. est le groupe de Galois d'une extension régulière de $k(T)$),*
(iii) *il existe une extension galoisienne de K (resp. une extension galoisienne régulière de $k(T)$) de groupe de Galois $\widehat{F}_\omega$,*
(iv) *tout groupe profini de rang topologique $\leq \aleph_0$ est groupe de Galois sur K (resp. d'une extension régulière de $k(T)$).*
De plus, si K est un corps ψ-libre de groupe de Galois absolu $\mathbf{G}_K$ de rang dénombrable (e.g. K dénombrable), alors les groupes profinis qui sont groupes de Galois sur K sont exactement les groupes profinis métrisables.

Preuve. Cela découle immédiatement de l'équivalence des assertions suivantes, pour tout groupe profini G (voir par exemple [RibZa], [Se1], [Wi]) :
(i) G est métrisable,
(ii) il existe un système complet de groupes finis $(G_n, s_n)_n$ tel que $G \simeq \varprojlim G_n$,
(iii) G a un rang (topologique) $\leq \aleph_0$,
(iv) G est l'image par un morphisme continu de $\widehat{F}_\omega$. $\square$

Un corps ψ-libre vérifie clairement la propriété (Gal/Inv). Réciproquement, supposons que K vérifie (Gal/Inv). Etant donné un système complet $(G_n, s_n)_{n\geq 0}$ de groupes finis, pour tout $n \geq 0$, toute extension galoisienne K_n/K de groupe G_n fournit une tour d'extensions galoisiennes $(K_i/K)_{1\leq i\leq n}$ telle que, pour tout $1 \leq i \leq n$, il existe un isomorphisme $\varepsilon_i : \mathrm{Gal}(K_i/K) \to G_i$ faisant commuter le diagramme

$$\begin{tikzcd} \mathrm{Gal}(K_{i+1}/K) \arrow[r] \arrow[d, "\varepsilon_{i+1}"] & \mathrm{Gal}(K_i/K) \arrow[d, "\varepsilon_i"] \\ G_{i+1} \arrow[r, "s_{i+1}"] & G_i \end{tikzcd}$$

Notons $\mathcal{E}_n$ l'ensemble des réalisations $(K_l)_{1\leq l\leq n}$ du système projectif *fini* $(G_l)_{0\leq l\leq n}$; par hypothèse, $\mathcal{E}_n$ est non vide (et en fait infini). La ψ-liberté de K équivaut à $\varprojlim \mathcal{E}_n \neq \emptyset$. L'exemple suivant montre que cette limite projective peut être vide.

Exemple 1.3. (D. Haran) *Corps non ψ-libre et vérifiant* (Gal/Inv). Considérons le groupe profini $G = \prod_n G_n$ où G_n parcourt l'ensemble des groupes finis et soit $\pi : \overline{G} \to G$ son revêtement de Frattini universel (voir [FrJa] §20.7). Le groupe $\overline{G}$ est projectif, donc il existe un corps K pseudo algébriquement clos de groupe de Galois absolu $\overline{G}$ [FrJa] corollary 20.16. Notons $\Phi(\overline{G})$ le sous-groupe de Frattini de $\overline{G}$; on a $\ker(\pi) \subset \Phi(\overline{G})$. Supposons qu'il existe une extension galoisienne de K de groupe $\widehat{F}_\omega$, c'est-à-dire un morphisme surjectif continu $\rho : \overline{G} \to \widehat{F}_\omega$. On a alors $\rho(\Phi(\overline{G})) \subset \Phi(\widehat{F}_\omega) = \{1\}$, donc $\ker(\pi) \subset \Phi(\overline{G}) \subset \ker(\rho)$. Il existe donc un morphisme surjectif continu $\varphi : G \to \widehat{F}_\omega$ ce qui est impossible puisque $\widehat{F}_\omega$ est sans torsion et que G est topologiquement engendré par des éléments de torsion.

Dans cette même perspective, on a le résultat suivant sur les corps de nombres, qui, conjecturalement, vérifient la propriété (Gal/Inv).

Proposition 1.4 — *Aucun corps de nombres n'est ψ-libre.*

Preuve. Une conséquence classique de la théorie du corps de classes est que si K est un corps de nombres, alors le nombre d de $\mathbb{Z}_p$-extensions de K linéairement disjointes deux à deux est fini et majoré par $[K : \mathbb{Q}]$. Si K était ψ-libre, alors le groupe $\mathbb{Z}_p^{d+1}$ (qui est métrisable) serait groupe de Galois sur K, ce qui impliquerait l'existence de $d+1$ $\mathbb{Z}_p$-extensions de K linéairement disjointes deux à deux (celles correspondant aux sous-groupes $\mathbb{Z}_p \times \cdots \times 0 \times \cdots \times \mathbb{Z}_p$). □

Exemple 1.5. *Corps ψ-libre et non ω-libre.* Considérons un corps k, de caractéristique 0, contenant les racines de l'unité et de groupe de Galois absolu isomorphe à $\widehat{F}_\omega$ (par exemple $k = \overline{\mathbb{Q}}(T)$). Comme $\mathbb{Q}^{\mathrm{ab}} \subset k$, le groupe de Galois absolu de $k((x))$ est isomorphe à $\mathrm{Gal}(\overline{k}/k) \times \widehat{\mathbb{Z}}$ (voir [Des2]), c'est-à-dire ici à $\widehat{F}_\omega \times \widehat{\mathbb{Z}}$. Il existe donc une extension galoisienne de $k((x))$ de groupe $\widehat{F}_\omega$: le corps $k((x))$ est ψ-libre. En revanche, $k((x))$ n'est pas ω-libre puisque son groupe de Galois absolu $\widehat{F}_\omega \times \widehat{\mathbb{Z}}$ est de dimension cohomologique ≥ 2 et donc n'est pas projectif.

Le §2 fournira d'autres exemples : ainsi le corps $\mathbb{R}(T)$ est ψ-libre (théorème 2.1) et il n'est pas ω-libre (puisque $\mathbf{G}_{\mathbb{R}(T)}$ a des éléments de torsion).

En résumé, on a :

$$\begin{array}{l} \omega\text{-liberté} \Longrightarrow \psi\text{-liberté} \Longrightarrow (\mathrm{Gal/Inv}) \\ \omega\text{-liberté} \not\Longleftarrow \psi\text{-liberté} \not\Longleftarrow (\mathrm{Gal/Inv}) \end{array}$$

Remarque 1.6. Définissons le *degré de liberté* $\mathrm{dl}(K)$ d'un corps K par

$$\mathrm{dl}(K) = \sup\{n \in \mathbb{N} / \ \widehat{F}_n \text{ est groupe de Galois sur } K\}$$

Par exemple si K est un corps de nombres alors $\mathrm{dl}(K) \leq [K : \mathbb{Q}]$ (proposition 1.4). Notons aussi que pour tout entier $n \geq 0$, il existe un corps K_n tel que $\mathrm{dl}(K_n) = n$: si $\mathbf{G}_K \simeq \widehat{F}_\omega$ (*e.g.* $K = \overline{\mathbb{Q}}(T)$), le corps $K_n = \overline{K}^{\widehat{F}_n}$ convient.

Les corps ψ-libres sont de degré de liberté $+\infty$. Mais $\mathrm{dl}(K) = +\infty$ ne caractérise pas la ψ-liberté. En effet, si $G = \prod_{n \geq 0} \widehat{F}_n$ et $\pi : \overline{G} \to G$ désigne son revêtement de Frattini universel, alors il existe un corps K PAC de groupe de Galois absolu $\overline{G}$. Comme dans l'exemple 1.3, on a que si K était ψ-libre il existerait un morphisme surjectif continu $\varphi : G \to \widehat{F}_\omega$. L'énoncé suivant va nous permettre de conclure.

(*) *Soient A et B deux groupes profinis et $\varphi : A \times B \to \widehat{F}_\omega$ un morphisme continu. Si φ est surjectif, alors soit $\varphi(A) = 1$ soit $\varphi(B) = 1$.*

En effet, pour $A = \widehat{F}_n$ ($n \geq 0$) et $B = \prod_{m \neq n} \widehat{F}_m$, on obtient $\varphi(\widehat{F}_n) = 1$ (car si $\varphi(B) = 1$, alors $\varphi : \widehat{F}_n \to \widehat{F}_\omega$ devrait être surjective). Comme les groupes $\widehat{F}_n$ ($n \geq 0$) engendrent topologiquement le groupe G et que φ est continu, on a $\varphi = 1$.

Preuve de (*). Posons $A_0 = \varphi(A)$ et $B_0 = \varphi(B)$. On a $\widehat{F}_\omega = A_0 \times B_0$: en effet, les éléments de A_0 et B_0 commutent, $\widehat{F}_\omega = < A_0, B_0 >$ et $A_0 \cap B_0 = \{1\}$ (car $A_0 \cap B_0 \subset Z(< A_0, B_0 >) = Z(\widehat{F}_\omega) = \{1\}$). Supposons A_0 et B_0 tous deux non réduits à 1. Alors tout sous-groupe ouvert strict de A_0 et B_0 est pro-libre ([FrJa] propositions 24.7 et 15.27). Par suite A_0 et B_0 sont d'ordre surnaturel $\prod_p p^\infty$. Il s'ensuit, puisque les deux groupes ont des p-parties non triviales pour au moins un p (en fait pour tous), que $\mathrm{cd}(A_0 \times B_0) \geq 2$. Ce qui contredit $\mathrm{cd}(\widehat{F}_\omega) = 1$. $\square$

Proposition 1.7.— *Toute extension L de type fini et séparable d'un corps ψ-libre K est un corps ψ-libre.*

Preuve. D'après la proposition 1.2, il s'agit de montrer que, si K est ψ-libre, il existe une extension galoisienne de L de groupe $\widehat{F}_\omega$. Il suffit de le prouver dans les deux cas suivants : L/K transcendante pure et L/K finie séparable.

Dans le premier cas, toute extension galoisienne M/K de groupe $\widehat{F}_\omega$ induit une extension galoisienne de L de groupe $\widehat{F}_\omega$ par extension des scalaires.

Supposons L/K finie séparable. Pour tout $n > 0$, le groupe $\widehat{F}_\omega^n$, qui est métrisable, est groupe de Galois d'une extension K_n/K. Les n sous-extensions fixées par les noyaux des projections $\widehat{F}_\omega^n \to \widehat{F}_\omega$ sont linéairement disjointes sur K. Si n est assez grand, il en existe au moins une linéairement disjointe de L/K, qui fournit par extension des scalaires une extension galoisienne de L de groupe $\widehat{F}_\omega$. $\square$

Corollaire 1.8.— *Soit K un corps ψ-libre de groupe de Galois absolu $\mathbf{G}_K$ de rang dénombrable (e.g. K dénombrable). Alors pour toute extension finie séparable L/K, $\mathbf{G}_K$ est un quotient de $\mathbf{G}_L$, ou, de façon équivalente, pour tout sous-groupe ouvert U de $\mathbf{G}_K$, il existe un sous-groupe fermé et distingué N de U tel que $U/N \simeq \mathbf{G}_K$.*

Remarques 1.9. (a) La conclusion du corollaire 1.8 ne caractérise pas la ψ-liberté. Par exemple, le corps $\mathbb{C}((X))$, qui n'est pas ψ-libre, la vérifie.

(b) Dans son article [Uc], Uchida fait une conjecture sur les morphismes de groupes profinis associés aux corps de nombres. Cette conjecture implique que $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ n'est pas quotient de $\mathrm{Gal}(\overline{F}/F)$ quand F est un corps de nombres différent de $\mathbb{Q}$ (comparer avec le corollaire 1.8). Pour $K = \mathbb{Q}$, on a cependant le résultat moins fort suivant : il existe un sous-groupe U fermé de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ et un sous-groupe N fermé distingué dans U tels que $U/N \simeq \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. En effet, d'après Fried-Völklein [FrVo], le corps $\mathbb{Q}^{\mathrm{tr}}(\sqrt{-1})$ est ω-libre, donc ψ-libre (ici, $\mathbb{Q}^{\mathrm{tr}}$ désigne le corps des nombres algébriques totalement réels). Il existe donc une extension galoisienne $L/\mathbb{Q}^{\mathrm{tr}}(\sqrt{-1})$ de groupe $\mathbf{G}_\mathbb{Q}$; on prend alors $U = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}^{\mathrm{tr}}(\sqrt{-1}))$ et $N = \mathrm{Gal}(\overline{\mathbb{Q}}/L)$.

L'énoncé dual de la proposition 1.7 "L/K de type fini et L ψ-libre $\Rightarrow$ K ψ-libre" est faux en général ; prendre par exemple $L = \mathbb{Q}^{\mathrm{tr}}(\sqrt{-1})$ qui est ψ-libre alors que $K = \mathbb{Q}^{\mathrm{tr}}$ ne satisfait même pas (Gal/Inv) (puisque $\mathbf{G}_K$ est engendré par des involutions). Cependant, A. Tamagawa nous a communiqué le résultat suivant.

Proposition 1.10 (A. Tamagawa) — *Soit k un corps de caractéristique* 0 *tel que pour tout nombre premier ℓ, le corps $k(\mu_{\ell^\infty})$ obtenu en adjoignant les racines de l'unité d'ordre une puissance de ℓ est de degré infini sur k. Soit K/k une extension de type fini et régulière. Si K est ψ-libre alors k est ψ-libre. En particulier, $\mathbb{Q}(T)$ et $\mathbb{Q}_p(T)$ ne sont pas ψ-libres.*

Preuve. Par un argument classique (*e.g.* [FrJa] proposition 9.31), on se ramène, par récurrence, au cas où K est de degré de transcendance 1 sur k, c'est-à-dire, est le corps des fonctions $k(C)$ d'une courbe projective lisse géométriquement irréductible et définie sur k.

Dans cette situation, l'argument de Tamagawa consiste à montrer que

(*) un épimorphisme continu $\varphi : \mathbf{G}_{k(C)} \to \widehat{F}_\omega$ n'est ramifié en aucun point fermé de C.

Ceci implique que la restriction de φ à $\mathbf{G}_{\overline{k}(C)}$ se factorise par le groupe fondamental géométrique de C, lequel est un groupe profini de type fini. Or le groupe $\widehat{F}_\omega$ n'admet aucun sous-groupe fermé distingué de type fini non trivial [FrJa] corollary 24.8. On a donc l'inclusion $\mathbf{G}_{\overline{k}(C)} \subset \ker(\varphi)$ ce qui entraîne que φ se factorise par $\mathbf{G}_k$.

Pour démontrer (*), fixons un point fermé $t \in C$ et un nombre premier ℓ. Il suffit de montrer que φ est trivial sur la ℓ-partie, identifiée à $\mathbb{Z}_\ell(1)$, du groupe d'inertie $I_t \simeq \widehat{\mathbb{Z}}(1)$ en t (où le suffixe "(1)" indique, comme il est usuel, que le groupe résiduel $\mathbf{G}_{k(t)}$ agit par le caractère cyclotomique). Par hypothèse sur k, l'extension $k(t)(\mu_{\ell^\infty})/k(t)$ est infinie et donc $\mathrm{Gal}(k(t)(\mu_{\ell^\infty})/k(t))$ est isomorphe à un produit $\mathbb{Z}_\ell \times C$ où C est un groupe cyclique. Choisissons un élément σ_0 dans ce groupe qui engendre $\mathbb{Z}_\ell$ et notons $\sigma \in \mathbf{G}_{k(t)}$ un relevé de σ_0 ; en particulier, l'action de σ sur μ_{ℓ^∞} est non-triviale. Considérons la restriction $\tilde{\varphi}$ du morphisme φ au sous-groupe $\mathbb{Z}_\ell(1) \rtimes < \sigma >$ du groupe de décomposition $D_t \simeq I_t \rtimes \mathbf{G}_{k(t)}$ de t (où $< \sigma >$ est le sous-groupe fermé de $\mathbf{G}_{k(t)}$ engendré par σ). Pour des raisons cohomologiques (présence d'un facteur direct $\mathbb{Z}_\ell$ dans $< \sigma >$), le morphisme $\tilde{\varphi} : \mathbb{Z}_\ell(1) \rtimes < \sigma > \rightarrow \widehat{F}_\omega$ n'est pas injectif. Soient $\gamma \in \ker(\tilde{\varphi}) \setminus \{1\}$ et γ_σ sa projection sur le sous-groupe $< \sigma >$. Si $\gamma_\sigma \neq 1$, alors, par choix de σ_0, il existe $\zeta \in \mathbb{Z}_\ell(1)$ tel que $\gamma_\sigma \zeta \gamma_\sigma^{-1} \neq \zeta$; l'élément $\gamma_\sigma \zeta \gamma_\sigma^{-1} \zeta^{-1}$ est alors non trivial, et appartient à $\mathbb{Z}_\ell(1) \cap \ker(\tilde{\varphi})$. Si $\gamma_\sigma = 1$, alors $\gamma \in \mathbb{Z}_\ell(1) \cap \ker(\tilde{\varphi})$. Dans tous les cas, $\mathbb{Z}_\ell(1) \cap \ker(\tilde{\varphi})$ est un sous-groupe non trivial de $\mathbb{Z}_\ell(1)$. Le quotient correspondant $\mathbb{Z}_\ell(1)/(\mathbb{Z}_\ell(1) \cap \ker(\tilde{\varphi}))$ est alors fini, mais comme il s'injecte dans $\widehat{F}_\omega$, il est trivial, soit $\mathbb{Z}_\ell(1) \subset \ker(\varphi)$. □

2.— ψ-liberté de $\mathbb{R}(T)$.

Si $\overline{k}$ est un corps algébriquement clos, le corps $\overline{k}(T)$ est ω-libre ([Do], [Po2], [Har2]) donc est régulièrement ψ-libre. L'objet de cette partie et de la suivante est l'étude de la régulière ψ-liberté du corps $k(T)$ quand k est réel clos (*i.e.*, k est un corps ordonné maximal) et quand k est un corps valué complet. Nous commençons par le cas réel, qui est plus facile car on connait explicitement (depuis Hurwitz [Hu]) l'action de la conjugaison complexe sur les revêtements de $\mathbb{P}^1$.

Nous utilisons librement le vocabulaire usuel de la théorie des revêtements (voir [De1] §2 ou [Vo]).

Théorème 2.1.— *Le corps $\mathbb{R}(T)$ est régulièrement ψ-libre, i.e. le groupe $\widehat{F}_\omega$ est groupe de Galois d'une extension galoisienne régulière de $\mathbb{R}(T)$.*

La démonstration que nous proposons peut être vue comme une version profinie d'une construction de Krull et Neukirch [KrNe] (voir aussi [MaMat] Ch.I §1). On peut aussi déduire le theórème 2.1 de la description de $\mathbf{G}_{\mathbb{R}(T)}$ que donnent D. Haran et M. Jarden dans [HaJa]. Notre construction nous permettra à la section 4 d'étendre le résultat en un énoncé sur les espaces modulaires de Hurwitz. Cette construction peut aussi servir de préparation à celle de la section 3, qui est du même esprit.

Preuve. Supposons donné un système complet $(G_n, s_n)_{n\geq 0}$ de groupes finis. On fixe des générateurs $h_{o1}, \ldots, h_{o\alpha_o}$ de G_o, et, pour tout $n > 0$, des générateurs, $h_{n1}, \ldots, h_{n\alpha_n}$, du noyau $\ker(s_n)$. On pose $\beta_n = \sum_{0 \leq l \leq n} \alpha_l$ $(n \geq 0)$.

On fixe un ensemble $\{\sigma_{nj} \mid n \in \mathbb{N},\ j = 1, \ldots, \alpha_n\}$ de nombres réels tels que

$$\cdots < \sigma_{n\alpha_n} < \cdots < \sigma_{n1} < \sigma_{n-1\alpha_{n-1}} < \cdots < \sigma_{n-11} < \cdots < \sigma_{o\alpha_o} < \cdots < \sigma_{o1}$$

et un nombre réel $\tau > 0$. On pose alors, en notant $z \rightarrow z^c$ la conjugaison complexe,

$$\begin{cases} x_{nj} = \sigma_{nj} + i\tau,\ n \geq 0,\ j = 1, \ldots, \alpha_n \\ S_n = \{x_{ni}, x_{ni}^c \mid i = 1, \ldots \alpha_n\} \\ U_N = \bigcup_{n=0}^N S_n,\ N \in \mathbb{N} \end{cases}$$

Pour tout $n \geq 0$, on note π_n [resp. $\overline{\pi}_n$] le $\mathbb{R}$-groupe fondamental de $\mathbb{P}^1_{\mathbb{R}} - U_n$ [resp. le $\mathbb{C}$-groupe fondamental de $\mathbb{P}^1_{\mathbb{C}} - U_n$]. Le groupe $\overline{\pi}_n$ est le complété profini du groupe fondamental topologique $\pi_1(\mathbb{P}^1(\mathbb{C}) - U_n, \infty)$ basé au point $\infty \in \mathbb{P}^1(\mathbb{C})$ (par exemple). La structure de $\pi_1(\mathbb{P}^1(\mathbb{C}) - U_n, \infty)$ est bien connue. Pour tout $x = x_{ni}$, notons Γ_x

(la classe d'homotopie d')un lacet basé en ∞, inclus dans le demi-plan supérieur et tournant une fois autour de x dans le sens positif ; notons alors, pour $y = x^c$, Δ_y le lacet $(\Gamma_x^c)^{-1}$, qui tourne une fois autour de y dans le sens positif. Sous quelques conditions techniques facilement réalisables (les lacets ne se croisent qu'au point ∞ (à homotopie près), etc.), le groupe $\pi_1(\mathbb{P}^1(\mathbb{C}){-}U_n, \infty)$ [resp. $\overline{\pi}_n$] est le groupe libre [resp. profini libre] engendré par $\{\Gamma_x, \Delta_y \mid x, y \in U_n\}$ modulo la relation

$$\Gamma_{x_{o1}} \cdots \Gamma_{x_{o\alpha_o}} \cdots \Gamma_{x_{n1}} \cdots \Gamma_{x_{n\alpha_n}} \Delta_{x^c_{n\alpha_n}} \cdots \Delta_{x^c_{n1}} \cdots \Delta_{x^c_{o\alpha_o}} \cdots \Delta_{x^c_{o1}} = 1$$

Le $\mathbb{R}$-groupe fondamental π_n (avec action de c) est également bien connu ([KrNe], [DeFr], [MaMat], [Se2]) : il est isomorphe à $\overline{\pi}_n \rtimes \mathbf{G}_{\mathbb{R}}$ où l'action de c est donnée par

$$\Gamma_x^c = \Delta_y^{-1}, \text{ pour } \; x \in U_n \text{ et } y = x^c$$

Pour tout $n > 0$, on note $\rho_n : \pi_n \to \pi_{n-1}$ l'épimorphisme évident qui envoie Γ_x et Δ_y sur eux-mêmes si $(x, y) \in U_{n-1}$ et qui les envoie sur 1 si $(x, y) \in S_n$.

On construit ensuite une suite d'homomorphismes $\varphi_n : \pi_n \to G_n$ $(n \in \mathbb{N})$ compatibles avec les morphismes $s_n : G_n \to G_{n-1}$. On prend $f_n(c) = 1$ $(n \geq 0)$. La construction de f_n sur $\overline{\pi}_n$ se fait par récurrence. Pour f_o, on pose :

$$\begin{cases} \text{pour } x = x_{oi} \ (i = 1, \ldots, \alpha_o) & \varphi_o(\Gamma_x) = h_{oi} \\ \text{pour } y = x^c & \varphi_o(\Delta_y) = (\varphi_o(\Gamma_x))^{-1} \end{cases}$$

Supposons ensuite φ_{n-1} défini $(n > 0)$. On choisit alors $\widetilde{h}_{li} \in G_n$ tel que $s_n(\widetilde{h}_{li}) = \varphi_{n-1}(\Gamma_{x_{li}})$ $(l = 0, \ldots, n-1,\ i = 1, \ldots, \alpha_l)$ et on pose

$$\begin{cases} \text{pour } x = x_{li} \ (l = 0, \ldots, n-1,\ i = 1, \ldots, \alpha_l) & \varphi_n(\Gamma_x) = \widetilde{h}_{li} \\ \text{pour } x = x_{ni} \ (i = 1, \ldots, \alpha_n) & \varphi_n(\Gamma_x) = h_{ni} \\ \text{pour } y = x^c & \varphi_n(\Delta_y) = (\varphi_n(\Gamma_x))^{-1} \end{cases}$$

On vérifie sans peine qu'on définit ainsi un morphisme $\varphi_n : \pi_n \to G_n$ tel que $\varphi_n(\overline{\pi}_n) = G_n$ et vérifiant $s_n \circ \varphi_n = \varphi_{n-1} \circ \rho_n$:

$$\begin{array}{ccc} \pi_n & \xrightarrow{\varphi_n} & G_n \\ {\scriptstyle \rho_n}\big\downarrow & & \big\downarrow{\scriptstyle s_n} \\ \pi_{n-1} & \xrightarrow[\varphi_{n-1}]{} & G_{n-1} \end{array}$$

Pour tout $n \geq 0$, φ_n correspond à un revêtement galoisien (sur $\mathbb{R}$) $f_n : X_n \to \mathbb{P}^1_{\mathbb{R}}$ de groupe G_n, non ramifié au-dessus de $\mathbb{P}^1_{\mathbb{R}}{-}U_n$ et géométriquement irréductible (à cause de $\varphi_n(\pi_n) = \varphi_n(\overline{\pi}_n) = G_n$). On obtient ainsi une "tour" de revêtements. La tour correspondante des extensions de corps de fonctions réalise le système projectif $(G_n)_{n \geq 0}$ et chacune des extensions est régulière sur $\mathbb{R}$. $\square$

Remarque 2.2. De la condition $\varphi_n(c) = 1$ $(n \geq 0)$ résulte que la tour d'extensions construite peut être plongée dans $\mathbb{R}((1/T))$: l'action de la conjugaison complexe c est triviale sur la fibre au-dessus du point-base ∞ à chaque niveau de la tour.

Le théorème 2.1 se généralise :

Théorème 2.3.— *Soit k un corps réel clos (e.g. $k = \mathbb{R}$, $k = \overline{\mathbb{Q}} \cap \mathbb{R}$, k le corps des séries de Puiseux à coefficients réels). Le corps $k(T)$ est régulièrement ψ-libre.*

Preuve. La preuve du théorème 2.1 est valable avec $\overline{\mathbb{Q}} \cap \mathbb{R}$ à la place de $\mathbb{R}$. Il suffit d'y remplacer $\mathbb{C}$ et $\mathbb{R}$ par $\overline{\mathbb{Q}}$ et $\overline{\mathbb{Q}} \cap \mathbb{R}$ respectivement et de choisir les nombres réels σ_{nj} $(n \in \mathbb{N},\ j = 1, \ldots, \beta_n)$ et τ dans $\overline{\mathbb{Q}} \cap \mathbb{R}$. Pour la descente de $\mathbb{R}$ à $\mathbb{R} \cap \overline{\mathbb{Q}}$, voir ensuite l'argument donné dans le théorème 3.4.

Soit maintenant k_o un sous-corps réel clos quelconque de $\overline{\mathbb{Q}}$. Comme le corps k_o est une extension ordonnée maximale de $\mathbb{Q}$ et que $\mathbb{Q}$ possède un unique ordre compatible, il en résulte que k_o et $\overline{\mathbb{Q}} \cap \mathbb{R}$ sont isomorphes (*e.g.* [Ri]). Il existe donc une extension galoisienne $E_o/k_o(T)$ de groupe $\widehat{F}_\omega$ et régulière sur k_o.

Soit enfin k un corps réel clos quelconque; k est de caractéristique 0 (car ordonnable). De plus, $\overline{k} = k(\sqrt{-1})$ et le corps $k_o = k \cap \overline{\mathbb{Q}}$ vérifie $k_o(\sqrt{-1}) = \overline{\mathbb{Q}}$ et donc est réel clos. Le corps $E = E_o \otimes_{k_o(T)} k(T)$ fournit alors une extension galoisienne régulière de $k(T)$ de groupe $\widehat{F}_\omega$. $\square$

Corollaire 2.4.— *Les groupes profinis qui sont groupes de Galois sur* $(\mathbb{R} \cap \overline{\mathbb{Q}})(T)$ *sont exactement les groupes profinis métrisables.*

3.— Corps de fonctions sur des corps valués non archimédiens.

3.1. Une construction générale.

Le but est de construire une tour $(K_n)_{n \geq 0}$ d'extensions galoisiennes régulières de $k(T)$ réalisant (au sens de la définition 1.1) un système complet donné $(G_n, s_n)_{n \geq 0}$. Nous nous plaçons sous des hypothèses aussi générales que possible. On reconnaîtra dans la première phase de la construction la méthode utilisée dans [Po1].

Le plan de la construction est le suivant. Dans les étapes (1), (2) et (3), nous en fixons le cadre : nous indiquons comment doivent être choisis les points de branchement et l'inertie des revêtements pour que la méthode de Pop puisse s'appliquer, à chacun des groupes G_n, de façon compatible. L'étape (4) consiste en la construction de chaque étage de la tour. Le passage à l'infini est effectué dans l'étape (5).

(1) *Données et notations* :

• on fixe un corps valué complet (k, v) avec v valuation de rang 1 et on note
- $\mathrm{car}(k)$ la caractéristique de k et p la caractéristique résiduelle,
- $\overline{k}$ une clôture algébrique fixée et k^s la sous-extension séparable maximale,
- $\mathbf{G}_k = \mathrm{Gal}(k^s/k)$ le groupe de Galois absolu de k,
- pour $d \geq 1$, ζ_d une racine primitive d-ième de l'unité dans $\overline{k}$, *i.e.*, un générateur du groupe $\mu_d(\overline{k}) \subset \overline{k}$ des racines d-ièmes de l'unité (noter que si $p > 0$, $\mu_d(\overline{k}) = \mu_{dp}(\overline{k})$).
- pour $d \geq 1$, $\chi = \chi_{k,d}$ le caractère cyclotomique $\mathbf{G}_k \to \mathrm{Gal}(k(\zeta_d)/k)$ de degré d, où on identifiera fréquemment $\mathrm{Gal}(k(\zeta_d)/k)$ à un sous-groupe de $(\mathbb{Z}/d\mathbb{Z})^\times$; on note $\chi_\infty = \chi_{k,\infty}$ le caractère cyclotomique $\mathbf{G}_k \to \varprojlim \mathrm{Gal}(k(\zeta_d)/k)$.

• pour tout élément g d'ordre n dans un groupe fini G, l'*ordre cyclotomique* (sur k) de g est défini comme le plus petit entier $d \geq 1$ tel que $k(\zeta_n) \subset k(\zeta_d)$.

• on fixe un système complet de groupes finis $(G_n, s_n)_{n \geq 0}$.

• on fixe un *pro-système générateur* de $(G_n, s_n)_{n \in \mathbb{N}}$, c'est-à-dire, la donnée de :
- *pour tout* $n \geq 0$, *une famille* $(g_{ni})_{i \geq 1}$ *d'éléments de* G_n, *et*
- *une suite* $(\beta_n)_{n \geq 0}$ *croissante d'entiers positifs, tels que* :

(Hyp.) (i) - $s_n(g_{ni}) = g_{n-1i}$ *(*$i, n \geq 1$*).*
- $g_{ni} = 1$ *pour tout* $i > \beta_n$ *(*$n > 0$*).*

(ii) *Les éléments* g_{ni}, $i = 1, \ldots, \beta_n$, *engendrent* G_n *(*$n \geq 0$*).*

Pour obtenir un pro-système générateur, on peut partir de générateurs $g_{o1}, \ldots, g_{o\beta_o}$ de G_o, les relever dans G_1 *via* s_1, puis compléter la liste de relevés $g_{11}, \ldots, g_{1\beta_o}$ par des éléments $g_{1(\beta_0+1)}, \ldots, g_{1\beta_1}$ de $\ker(s_1)$ de telle façon à obtenir un ensemble de générateurs $g_{11}, \ldots, g_{1\beta_1}$ de G_1. On pose évidemment $g_{oi} = 1$ pour $i > \beta_o$ et $g_{1i} = 1$ pour $i > \beta_1$. On répète ensuite ce procédé de façon inductive pour définir les g_{ni} $(i > 0)$ pour les niveaux suivants $n \geq 2$.

On fait l'hypothèse supplémentaire suivante :

(Hyp.) (iii) *Pour tout* $i > 0$, *il existe un entier* δ_i *multiple commun des ordres cyclotomiques sur* k *des éléments* g_{ni} *où* $n \geq 0$.

(iv) *Si* $p > 0$, *il existe un entier* ν *tel que pour tout* $i > 0$ *et tout* $n \geq 0$, *la* p*-partie* *de l'ordre de g_{ni} est $\leq p^\nu$. Si de plus* $\mathrm{car}(k) = p > 0$*, la propriété précédente est satisfaite avec $\nu = 0$ (i.e., chaque g_{ni} est d'ordre premier à p).*

(2) *Points de branchement.* On suppose donnée une suite $(S_i)_{i>0}$ d'ensembles $S_i = \{x_i^\tau, y_i^\tau \mid \tau \in \mathbf{G}_k\}$ constitués d'une paire (x_i, y_i) d'éléments de $\mathbb{P}^1(\overline{k})$ et de leurs conjuguées (x_i^τ, y_i^τ), et tels que, pour tout $i > 0$:

- S_{i+1} est disjoint de $\bigcup_{j=1}^{i} S_j$,
- $k(x_i) = k(y_i) \supset k(\zeta_{\delta_i})$, et
- les conditions suivantes de proximité sont satisfaites

$$\begin{array}{l} |x_i^\sigma - y_i^\sigma| < |x_i^\sigma - x_j^\tau|\,|p|^{\frac{\nu+1}{p-1}} \\ \quad \text{pour } j \leq i,\ \sigma,\tau \in \mathbf{G}_k \\ \quad \text{sauf si } j = i \text{ et } x_i^\sigma = x_i^\tau \end{array}$$

avec la convention que $|p|^{\frac{\nu+1}{p-1}} = 1$ dans le cas d'égale caractéristique $p = \mathrm{car}(k)$.

Pour tout $i > 0$, S_i et $U_i = \bigcup_{j=1}^{i} S_i$ constituent des ensembles *ajustés en paires* au sens de Pop [Po1] et stables sous $\mathbf{G}_k$. Nous noterons "$(x, y) \in U_i$" pour dire que les éléments x et y d'une paire (x, y) sont dans U_i. On fixe aussi un point-base $x^\infty \in \mathbb{P}^1(k) - \bigcup_{i>0} S_i$.

Remarque 3.1. Il est facile de construire une suite $(S_i)_{i>0}$ comme ci-dessus. Par exemple, on fixe un élément $\xi \neq 0$ de l'idéal de valuation de k et on prend :

$$\begin{cases} x_i = \zeta_{\delta_i}\xi^{\epsilon_i} \\ y_i = x_i + \xi^{\lambda_i} \end{cases}$$

où $(\epsilon_i)_{i>0}$ et $(\lambda_i)_{i>0}$ sont deux suites d'entiers > 0 vérifiant, pour tout $i > 0$,

$$\epsilon_i > \max(\epsilon_1, \epsilon_2, \ldots, \epsilon_{i-1}) \qquad \text{et} \qquad \lambda_i > \epsilon_i + \frac{\nu+1}{p-1}v(p)$$

(3) *Constructions d'épimorphismes f_n ($n > 0$).* Pour tout $n \geq 0$, notons $\overline{\Pi}_n$ le groupe profini défini par générateurs et relations :

$$\overline{\Pi}_n = \langle \Gamma_x, \Delta_y \text{ avec } \Gamma_x\Delta_y = 1 \mid (x, y) \in U_{\beta_n} \rangle$$

qu'on munit de l'action à droite de $\mathbf{G}_k$ définie par $(\Gamma_{x^\tau})\tau = (\Gamma_{\underline{x}})^{\chi_\infty(\tau^{-1})}$ et de façon correspondante pour les Δ_y. Pour $n > 0$, on note $r_n : \overline{\Pi}_n \to \overline{\Pi}_{n-1}$ l'épimorphisme évident qui envoie les éléments Γ_x et Δ_y sur eux-mêmes si $(x, y) \in U_{\beta_{n-1}}$ et qui les envoie sur 1 si $(x, y) \in \bigcup_{\beta_{n-1} < i \leq \beta_n} S_i$.

On définit ensuite des homomorphismes $f_n : \overline{\Pi}_n \rtimes \mathbf{G}_k \to G_n$ ($n \in \mathbb{N}$), en posant

$$\begin{cases} \text{pour } x = x_i^\tau \ (i = 1, \ldots, \beta_n) & f_n(\Gamma_x) = g_{ni}^{1/\chi(\tau)} \\ \text{pour } y \text{ associé à } x & f_n(\Delta_y) = (f_n(\Gamma_x))^{-1} \\ \text{pour } \tau \in \mathbf{G}_k & f_n(\tau) = 1 \end{cases}$$

où par $1/\chi(\tau)$ nous entendons un entier m_τ tel que $\chi(\tau)m_\tau = 1$ modulo l'ordre, disons $\nu(g_{ni})$, de g_{ni}. Noter que si, ci-dessus, $x_i^\tau = x_i^\sigma$ pour $\tau, \sigma \in \mathbf{G}_k$, alors $\tau^{-1}\sigma$ fixe le corps $k(x_i)$ et donc aussi le corps $k(\zeta_{\delta_i})$ (par (2)), lequel contient $k(\zeta_{\nu(g_{ni})})$ (par (Hyp.) (iii)), ce qui donne $\chi(\tau) = \chi(\sigma)$ dans $\mathbb{Z}/\nu(g_{ni})\mathbb{Z}$; l'élément $f_n(\Gamma_x) = g_{ni}^{1/\chi(\tau)}$ ne dépend pas du choix de $\tau \in \mathbf{G}_k$ tel que $x = x_i^\tau$.

Le morphisme f_n est surjectif (par (Hyp.)(ii)) et vérifie $s_n \circ f_n = f_{n-1} \circ r_n$

$$\begin{tikzcd} \overline{\Pi}_n \rtimes \mathbf{G}_k \arrow[r, "f_n"] \arrow[d, "r_n"'] & G_n \arrow[d, "s_n"] \\ \overline{\Pi}_{n-1} \rtimes \mathbf{G}_k \arrow[r, "f_{n-1}"'] & G_{n-1} \end{tikzcd}$$

(4) *Construction de G-revêtements F_n $(n \geq 0)$.* Pour tout $n \geq 0$ et toute paire $(x, y) \in U_{\beta_n}$, on note $C_{n,x}$ la classe de conjugaison dans G_n de $f_n(\Gamma_x)$; $C_{n,x}^{-1}$ est alors la classe de $f_n(\Delta_y)$. On note ensuite $\mathbf{C}_n$ l'uplet (non ordonné) dont les composantes sont toutes les classes $C_{n,x}$ ainsi que leurs inverses $C_{n,x}^{-1}$ quand $(x, y) \in U_{\beta_n}$.

Pour tout $n \geq 0$, on note π_n [resp. $\overline{\pi}_n$] le k-groupe fondamental de $\mathbb{P}^1_k - U_{\beta_n}$ [resp. le $\overline{k}$-groupe fondamental de $\mathbb{P}^1_{\overline{k}} - U_{\beta_n}$]. Pour tout $n \geq 0$, on a la suite exacte

$$(*) \qquad 1 \to \overline{\pi}_n \to \pi_n \to \mathbf{G}_k \to 1$$

Pour tout $n \geq 0$, on note $x_n^\infty : \mathbf{G}_k \to \pi_n$ la section associée au point-base x^∞.

Lemme 3.2.— *Pour tout $n \geq 0$, il existe*

- un k-G-revêtement galoisien $F_n : X_n \to \mathbb{P}^1_k$ de groupe G_n, non ramifié au-dessus de $\mathbb{P}^1_k - U_{\beta_n}$, dont l'invariant canonique de l'inertie ([De2] §2.2) *est l'uplet $\mathbf{C}_n$ et dont la fibre $F_n^{-1}(x^\infty)$ est formée de points k-rationnels (i.e., est totalement k-rationnelle), ou, de façon équivalente,*

- un épimorphisme $\varphi_n : \pi_n \to G_n$, dont l'invariant canonique de l'inertie est l'uplet $\mathbf{C}_n$ et tel que $\varphi_n \circ x_n^\infty = 1$.

Preuve. Ce résultat de réalisation du groupe G_n (pour $n \geq 0$ arbitraire) se démontre en employant les techniques de recollement de G-revêtements sur des corps valués complets, dues initialement à D. Harbater [Har1]. Plus précisément, le lemme 3.2 se déduit du 1/2-*théorème d'existence de Riemann* de Pop ([Po1], et aussi [MaMat] Ch.V §3). D'après ce résultat, pour tout $n \geq 0$, la suite exacte (*) ci-dessus a pour quotient la suite exacte

$$1 \to \overline{\Pi}_n \to \overline{\Pi}_n \rtimes \mathbf{G}_k \to \mathbf{G}_k \to 1$$

Pour tout $n \geq 0$, l'épimorphisme $\varphi_n : \pi_n \to G_n$ composé de f_n avec la surjection $p_n : \pi_n \to \overline{\Pi}_n \rtimes \mathbf{G}_k$ vérifie les propriétés demandées. $\square$

Remarque 3.3. On peut aussi déduire directement le lemme 3.2 de l'article de Liu [Li] (voir aussi [MaMat] Ch.V §1,§2 et [De1] theorem 3.4), qui est à l'origine de [Po1]. Cet article explique comment construire un k-G-revêtement $F : X \to \mathbb{P}^1$ de groupe G à partir de deux k-G-revêtements $F_i : X_i \to \mathbb{P}^1$ $(i = 1, 2)$ de groupes respectifs deux sous-groupes G_1, G_2 engendrant G.

La construction, qui s'effectue par recollement analytique rigide, comporte une réduction préalable à une situation où les ensembles des points de branchement de f_1 et f_2 sont respectivement inclus dans des disques D_1 et D_2 disjoints et suffisamment petits. Dans la perspective de la construction d'une *tour infinie* de revêtements, la condition "D_1 et D_2 suffisamment petits" doit être précisée. Cette condition est explicitée dans [Po1] ; elle conduit à la condition d'*ajustement en paires* des points de branchement. En caractéristique mixte, la borne sur les rayons de D_1 et D_2 comporte un terme qui dépend de G_1 et G_2. C'est ici l'hypothèse (Hyp) (iv) qui permet de majorer uniformément en n cette borne, laquelle apparaît, dans la condition de proximité de notre point (2), à travers le terme en puissance de $|p|$.

Il reste à dire quels revêtements élémentaires on recolle. Fixons un entier $n \geq 0$. Pour tout $i = 1, \ldots, \beta_n$, il existe un k-G-revêtement F_{ni} de groupe le sous-groupe cyclique de G engendré par g_{ni}, de points de branchement les points de l'ensemble $S_i = \{x_i^\tau, y_i^\tau \mid \tau \in \mathbf{G}_k\}$, d'invariant canonique de l'inertie l'uplet constitué des classes (réduites ici à un élément) de $f_n(\Gamma_x)$ et $f_n(\Delta_y)$ quand (x, y) décrit S_i, et tel que la fibre $F_{ni}^{-1}(x^\infty)$ soit totalement k-rationnelle. Il s'agit ici seulement de construire un k-G-revêtement cyclique (voir par exemple [Des1] §2.1.1) : il faut et il suffit d'assurer que les points de branchements sont permutés par $\mathbf{G}_k$ de telle façon que pour tout $\tau \in \mathbf{G}_k$, l'inertie dans le revêtement F_{ni}^τ coincide avec celle du revêtement F_{ni} ; cela se traduit ici par la condition

$$\left\{\begin{array}{l} f_n(\Gamma_{x^\tau})^{\chi(\tau)} = f_n(\Gamma_x) \\ f_n(\Delta_{y^\tau})^{\chi(\tau)} = f_n(\Delta_y) \end{array}\right. \qquad \text{pour tout} \quad (x,y) \in S_i$$

qui est satisfaite par construction. Pour tout $n \geq 0$, le k-G-revêtement F_n s'obtient en recollant les G-revêtements F_{ni}, $i = 1, \ldots, \beta_n$.

(5) *Construction d'une tour infinie de k-G-revêtements.* En général les morphismes $\varphi_n : \pi_n \to G_n$ construits dans le lemme 3.2 ne satisfont pas comme dans le théorème 2.1 la condition $s_n \circ \varphi_n = \varphi_{n-1} \circ r_n$ $(n > 0)$: le diagramme

$$\begin{array}{ccc} \pi_n & \xrightarrow{p_n} & \overline{\Pi}_n \rtimes \mathbf{G}_k \\ {\scriptstyle \rho_n}\downarrow & & \downarrow{\scriptstyle r_n} \\ \pi_{n-1} & \xrightarrow[p_{n-1}]{} & \overline{\Pi}_{n-1} \rtimes \mathbf{G}_k \end{array}$$

n'est pas commutatif. La démonstration requiert un argument supplémentaire.

Pour tout $n \geq 0$, notons $\mathcal{F}_n$ l'ensemble des $n+1$-uplets $(\phi_l)_{0 \leq l \leq n}$ d'épimorphismes $\phi_l : \pi_l \to G_l$ vérifiant

- $\phi_l(\overline{\pi}_l) = G_l$ et $\phi_l \circ x_l^\infty = 1$, $l = 0, \ldots, n$,
- $s_l \circ \phi_l = \phi_{l-1} \circ \rho_l$, $l = 1, \ldots, n$, et
- l'invariant canonique de l'inertie de ϕ_l est l'uplet $\mathbf{C}_l$, $l = 0, \ldots, n$.

Pour tout $n > 0$ et tout élément $(\phi_l)_{0 \leq l \leq n} \in \mathcal{F}_n$, le n-uplet $(\phi_l)_{0 \leq l \leq n-1}$ est dans $\mathcal{F}_{n-1}$. Cela fournit une application $\Theta_n : \mathcal{F}_n \to \mathcal{F}_{n-1}$ $(n > 0)$.

Montrons maintenant que $\mathcal{F}_n \neq \emptyset$ pour tout $n \geq 0$. Fixons un entier $n \geq 0$ et considérons l'épimorphisme $\varphi_n : \pi_n \to G_n$ contruit dans le lemme 3.2. L'inertie des points de branchement dans $\bigcup_{\beta_{n-1} < i \leq \beta_n} S_n$ étant par construction dans $\ker(s_n)$, ces points ne sont pas ramifiés dans le revêtement associé à l'épimorphisme $s_n \circ \varphi_n$; ce morphisme se factorise *via* ρ_n en un morphisme $\varphi_{n,n-1} : \pi_{n-1} \to G_{n-1}$. De plus, l'inertie de $\varphi_{n,n-1}$ s'obtient à partir de celle de φ_n en composant avec s_n. La construction permet de répéter l'argument. On construit de cette manière $n+1$ épimorphismes $\varphi_{n,n-l} : \pi_{n-l} \to G_{n-l}$ $(l = 0, \ldots, n)$ vérifiant $s_{n-l} \circ \varphi_{n,n-l} = \varphi_{n,n-l-1} \circ \rho_{n-l}$, $(l = 0, \ldots, n)$. Le $n+1$-uplet $(\varphi_{n,l})_{0 \leq l \leq n}$ est un élément de $\mathcal{F}_n$.

Enfin $\mathcal{F}_n$ est fini pour tout $n \geq 0$. En effet, tout élément $(\phi_l)_{0 \leq l \leq n} \in \mathcal{F}_n$ est déterminé par son n-ième facteur ϕ_n, lequel, à cause de la condition $\phi_n \circ x_n^\infty = 1$, est déterminé par sa restriction $\overline{\phi}_n$ au $\overline{k}$-groupe fondamental $\overline{\pi}_n$. Si $\mathrm{car}(k) = 0$, ce dernier groupe fondamental est de type fini. Si $\mathrm{car}(k) > 0$, en raison de (Hyp.) (iv), le revêtement associé au morphisme $\overline{\phi}_n : \overline{\pi}_n \to G_n$ est modérément ramifié ; $\overline{\phi}_n$ se factorise donc par le quotient $\overline{\pi}_n^{\mathrm{tame}}$ (groupe fondamental modéré), lequel, d'après le théorème de spécialisation de Grothendieck, est de type fini $(n \geq 0)$. Dans les deux cas, on peut conclure qu'il n'y a qu'un nombre fini de possibilités pour $\overline{\phi}_n$, ce qui conclut la preuve de la finitude de $\mathcal{F}_n$ $(n \geq 0)$. Une limite projective d'ensembles finis non vides est non vide. On obtient la conclusion suivante.

Résultat de la construction. *Tout élément de la limite projective du système $(\mathcal{F}_n, \Theta_n)_{n \geq 0}$ fournit une tour régulièrement réalisante du système complet $(G_n)_{n \geq 0}$. Pour tout $n \geq 0$, le n-ième niveau de la tour est un k-G-revêtement de groupe G_n, de points de branchement les éléments de U_n, d'invariant canonique de l'inertie l'uplet $\mathbf{C}_n$ et qui possède une fibre totalement k-rationnelle au-dessus du point $x^\infty \in \mathbb{P}^1(k)$. Cette conclusion est valable sous les hypothèses faites en* (1) *et* (2).

3.2 Applications à la ψ-liberté. Pour tout premier p, nous notons $\widehat{F}_\omega^{(p')}$ le plus grand quotient de $\widehat{F}_\omega$ premier à p. Nous convenons que pour $p = 0$, $\widehat{F}_\omega^{(p')} = \widehat{F}_\omega$. Nous notons aussi $\mu_\infty^{(p')}$ le sous-groupe de μ_∞ des racines de l'unité (dans $\overline{k}$) d'ordre premier à p, avec la convention que $\mu_\infty^{(p')} = \mu_\infty$ si $p = 0$.

Théorème 3.4.— *Soient* (k, v) *un corps valué hensélien de caractéristique résiduelle* p *et tel que* $[k(\mu_\infty^{(p')}) : k] < \infty$. *Le groupe* $\widehat{F}_\omega^{(p')}$ *est groupe de Galois d'une extension galoisienne régulière de* $k(T)$. *En particulier si* $p = 0$ *alors le corps* $k(T)$ *est régulièrement* ψ*-libre.*

Preuve. Soit $(G_n)_{n\geq 0}$ un système complet de groupes finis qu'on suppose d'ordre premier à la caractéristique résiduelle p si $p > 0$. Choisissons ensuite un pro-système générateur $(g_{ni})_{i>0,n\geq 0}$ de $(G_n)_{n\geq 0}$ (*cf.* (Hyp.) (i) et (ii)). Les conditions (iii) et (iv) de (Hyp.) sont alors également satisfaites : pour (iii), noter que l'hypothèse $[k(\mu_\infty^{(p')}) : k] < \infty$ entraîne que tout élément d'ordre fini premier à p est d'ordre cyclotomique majoré par un entier ne dépendant que de k ; en raison de l'hypothèse sur les ordres des groupes G_n $(n \geq 0)$, la condition (iv) est satisfaite avec $\nu = 0$.

Plongeons k dans son complété k_v, fixons une clôture algébrique $\overline{k_v}$ de k_v et identifions $\overline{k}$ à la clôture algébrique de k dans $\overline{k_v}$. On choisit des points x_i et y_i et on construit les ensembles S_i et U_i comme indiqué dans §3.1 (2), mais avec la condition supplémentaire que $x_i, y_i \in \mathbb{P}^1(k^{\mathrm{s}})$ $(i > 0)$; si k contient μ_∞, on peut même choisir les points x_i, y_i dans $\mathbb{P}^1(k)$. On fixe un point-base x^∞ dans $\mathbb{P}^1(k)$.

Sur le corps complet k_v, on dispose de données comme en §3.1. La construction générale aboutit à l'existence d'une tour régulièrement réalisante du système complet $(G_n)_{n\geq 0}$ sur k_v. Les G-revêtements F_n de la tour construite sont *a priori* définis sur k_v $(n \geq 0)$. Fixons l'entier $n \geq 0$ pour expliquer la descente à k. L'argument que nous allons donner est également valable pour $k_v = \mathbb{R}$ et $k = \mathbb{R} \cap \overline{\mathbb{Q}}$.

L'ensemble U_n des points de branchement de F_n étant contenu dans $\mathbb{P}^1(k^{\mathrm{s}})$, il y a un homomorphisme de restriction $\pi_{n,\overline{k_v}}^{(p')} \to \pi_{n,k^{\mathrm{s}}}^{(p')}$ entre les p'-parties des groupes fondamentaux de $(\mathbb{P}^1 - U_n)_{\overline{k_v}}$ et de $(\mathbb{P}^1 - U_n)_{k^{\mathrm{s}}}$. Il est bien connu que cet homomorphisme est un isomorphisme : cela résulte, en caractéristique 0, du théorème d'existence de Riemann (voir aussi [Se2] theorem 6.3.3) et plus généralement du théorème de spécialisation de Grothendieck [SGA1]. La restriction $\mathbf{G}_{k_v} \to \mathbf{G}_k$ est un isomorphisme ; l'injectivité provient du lemme de Krasner et la surjectivité de l'égalité $k = k_v \cap k^{\mathrm{s}}$ (qui est classique pour un corps hensélien pour une valuation de rang 1). Cela, ajouté à la condition $x^\infty \in \mathbb{P}^1(k)$, conduit à la conclusion que la restriction naturelle entre les p'-parties $\pi_{n,k_v}^{(p')}$ et $\pi_{n,k}^{(p')}$ des groupes fondamentaux de $(\mathbb{P}^1 - U_n)_{k_v}$ et de $(\mathbb{P}^1 - U_n)_k$ respectivement est un isomorphisme (la condition $x^\infty \in \mathbb{P}^1(k)$ fournit une section $\mathbf{G}_k \to \pi_{n,k}$, induite par une section $\mathbf{G}_{k_v} \to \pi_{n,k_v}$). Le k_v-G-revêtement F_n possède donc un et un seul k-modèle $\widetilde{F}_n$. Du fait de l'unicité, la descente à k est fonctorielle : on obtient une *tour* régulièrement réalisante du système complet $(G_n)_{n\geq 0}$ où les G-revêtements F_n de la tour sont définis sur k $(n \geq 0)$.

Comme $\widehat{F}_\omega^{(p')}$ peut être écrit comme limite projective d'un système complet de groupe finis, d'ordre premier à p si $p > 0$, on obtient l'énoncé désiré. □

Le théorème 3.4 s'applique par exemple au corps $k = \mathbb{Q}_p(\mu_\infty^{(p')}) = \mathbb{Q}_p^{\mathrm{nr}}$, au corps $k = \mathbb{Q}^{\mathrm{ab}}((x))$, ou même au sous-corps $k = \mathbb{Q}^{\mathrm{ab}}((x))^{\mathrm{alg}}$ des séries de Laurent algébriques sur $\mathbb{Q}^{\mathrm{ab}}(x)$. L'énoncé suivant résulte de la proposition 1.2.

Corollaire 3.5.— *Les groupes profinis qui sont groupes de Galois sur* $\mathbb{Q}^{ab}((x))^{alg}(T)$ *sont exactement les groupes profinis métrisables.*

Remarque 3.6. Pour $k = \mathbb{Q}_p^{\mathrm{nr}}$ ou $k = \mathbb{Q}_p\mathbb{Q}^{\mathrm{ab}}$, le théorème 3.4 ne permet de réaliser que le groupe $\widehat{F}_\omega^{(p')}$. La difficulté pour traiter le groupe $\widehat{F}_\omega$ vient de la méthode. On peut penser que $\mathbb{Q}^{\mathrm{ab}}(T)$ lui-même est régulièrement ψ-libre. Le corps $\mathbb{Q}^{\mathrm{ab}}$ étant hilbertien, une conséquence serait que tout groupe fini est groupe de Galois sur $\mathbb{Q}^{\mathrm{ab}}$. Ce dernier résultat découlerait également de la ψ-liberté de $\mathbb{Q}^{\mathrm{ab}}$, qu'on peut voir comme une forme faible de la conjecture de Shafarevich, selon laquelle $\mathbf{G}_{\mathbb{Q}^{\mathrm{ab}}} \simeq \widehat{F}_\omega$.

4.— Perspectives modulaires.

Nous utilisons librement la théorie des espaces de modules de revêtements de $\mathbb{P}^1$ — les espaces de Hurwitz —. Nous renvoyons au livre de H. Völklein [Vo] (ou à [De2] pour une présentation). Etant donné un groupe fini G, un entier $r \geq 3$, nous notons $\mathcal{H}_{r,G}$ l'espace de Hurwitz des G-revêtements de $\mathbb{P}^1$ sur un corps algébriquement clos de caractéristique 0, de groupe G et ayant r points de branchement. Etant donné un r-uplet $\mathbf{C}$ de classes de conjugaison de G, nous notons $\mathcal{H}_{r,G}(\mathbf{C})$ la réunion des composantes de $\mathcal{H}_{r,G}$ dont les points correspondent à des G-revêtements d'invariant canonique de l'inertie égal à $\mathbf{C}$. Les espaces $\mathcal{H}_{r,G}$ et $\mathcal{H}_{r,G}(\mathbf{C})$ sont des variétés quasi-projectives ; elles peuvent être définies sur $\mathbb{Q}$ et $\mathbb{Q}^{\mathrm{ab}}$ respectivement (comme schémas intègres (non nécessairement géométriquement intègres)).

4.1. Retour sur les théorèmes 2.3 et 3.4

Théorème 4.1.— *Soit $(G_n, s_n)_n$ un système complet de groupes finis. Il existe une suite $(r_n)_{n\geq 0}$ d'entiers $r_n \geq 3$ et une suite $(\mathbf{C}_n)_{n\geq 0}$ de r_n-uplets de classes de conjugaison de G_n et une tour $(\mathcal{H}_{G_n,r_n}(\mathbf{C}_n))_{n\geq 0}$ d'espaces de Hurwitz, où les applications $\mathcal{H}_{G_n,r_n}(\mathbf{C}_n) \to \mathcal{H}_{G_{n-1},r_{n-1}}(\mathbf{C}_{n-1})$ sont des morphismes algébriques, qui possède les propriétés suivantes :*

(a) *il existe un système projectif $(\theta_n^\infty)_{n\geq 0}$ de points $(\mathbb{R}\cap\overline{\mathbb{Q}})$-rationnels θ_n^∞ sur l'espace $\mathcal{H}_{G_n,r_n}(\mathbf{C}_n)$. De plus, si $Z(G_n) = \{1\}$, la composante $\mathcal{H}_n^\infty$ de $\mathcal{H}_{G_n,r_n}(\mathbf{C}_n)$ à laquelle appartient chaque point θ_n^∞ est définie sur $\mathbb{Q}$ ($n \geq 0$).*

(b) *il existe un système projectif $(\theta_n^x)_{n\geq 0}$ de points $\theta_n^x \in \mathcal{H}_{G_n,r_n}(\mathbf{C}_n)$ rationnels sur le corps $\mathbb{Q}^{ab}((x))$. De plus, la composante $\mathcal{H}_n^x$ de $\mathcal{H}_{G_n,r_n}(\mathbf{C}_n)$ à laquelle appartient chaque point θ_n^x est définie sur $\mathbb{Q}^{ab}$ ($n \geq 0$).*

(c) *Si p est un nombre premier ne divisant aucun des ordres des groupes G_n ($n \geq 0$), il existe un système projectif $(\theta_n^p)_{n\geq 0}$ de points $\mathbb{Q}_p^{nr}$-rationnels $\theta_n^p \in \mathcal{H}_{G_n,r_n}(\mathbf{C}_n)$.*

Preuve. Notons $\mathbf{C}_o$ l'uplet constitué de toutes les classes de conjugaison non triviales de G_o répétées chacune 4 fois, et, pour tout entier $n > 0$, $\mathbf{C}'_n$ l'uplet constitué de toutes les classes de conjugaison non triviales de $\ker(s_n)$ répétées chacune 4 fois ; on pose aussi $\mathbf{C}'_o = \mathbf{C}_o$ et $\ker(s_o) = G_o$. Les classes dans les uplets $\mathbf{C}'_n$ peuvent être regroupées en couples (C, C^{-1}) qui apparaissent 4 fois si la classe C vérifie $C \neq C^{-1}$ et 2 fois si $C = C^{-1}$ ($n \geq 0$). Désignons par $2q_n$ le nombre de composantes de $\mathbf{C}'_n$ ($n \geq 0$). Considérons ensuite l'uplet $\mathbf{C}_n$ défini par récurrence à partir de $\mathbf{C}_o$ de la façon suivante. Pour $n > 0$ et chaque paire (C, C^{-1}) avec C classe de conjugaison non-triviale de G_{n-1}, on choisit une classe $\widetilde{C}$ de G_n dans $s_n^{-1}(C)$; l'uplet $\mathbf{C}_n$ est alors la réunion du uplet $\mathbf{C}'_n$ et de tous les couples $(\widetilde{C}, \widetilde{C}^{-1})$ associés aux couples (C, C^{-1}) apparaissant dans $\mathbf{C}_{n-1}$. Le nombre $r_n = 2t_n$ de composantes du uplet $\mathbf{C}_n$ est défini par $r_n = r_{n-1} + 2q_n$ ($n > 0$) et $r_o = 2q_o$.

Pour chaque $n \geq 0$, les uplets $\mathbf{C}_n$ et $\mathbf{C}'_n$ ont les deux propriétés suivantes :

• $\mathbf{C}_n$ et $\mathbf{C}'_n$ consistent en une réunion de couples (C, C^{-1}). Pour la suite, on note $\mathbf{C}_n = (C_{n1}, C_{n1}^{-1}, \ldots, C_{nt_n}, C_{nt_n}^{-1})$ et $\mathbf{C}'_n = (C'_{n1}, (C'_{n1})^{-1}, \ldots, C'_{nq_n}, (C'_{nq_n})^{-1})$.

• si on retire un couple (C, C^{-1}) de $\mathbf{C}'_n$ [resp. de $\mathbf{C}_n$] et qu'on choisit un élément dans chacune des classes restantes, l'ensemble obtenu engendre le groupe $\ker(s_n)$ [resp. G_n]. On utilise pour cela le résultat classique suivant : si un sous-ensemble d'un groupe fini G coupe chaque classe de conjugaison de G, alors il engendre G.

Ces deux propriétés sont introduites dans [Fr2] où les uplets les satisfaisant sont dits "H(arbater)M(umford)-gcomplets".

Considérons l'espace de Hurwitz $\mathcal{H}_{r_n,G_n}(\mathbf{C}_n)$ ($n > 0$). Si $\theta \in \mathcal{H}_{r_n,G_n}(\mathbf{C}_n)(\mathbb{C})$ et F_n est le $\mathbb{C}$-G-revêtement associé, le revêtement quotient par le noyau de s_n est un G-revêtement de groupe G_{n-1} et d'invariant canonique $\mathbf{C}_{n-1}$. Pour ce second point, il faut voir que l'inertie du revêtement quotient est l'image de $\mathbf{C}_n$ par s_n ; en particulier, si une classe C apparaît dans $\mathbf{C}'_n$, alors $C \subset \ker(s_n)$, d'où il découle que le point de branchement de F_n associé à C n'est pas un point de branchement du revêtement quotient. Cette observation fournit un morphisme, pour tout $n > 0$:

$$\psi_n : \mathcal{H}_{r_n,G_n}(\mathbf{C}_n) \to \mathcal{H}_{r_{n-1},G_{n-1}}(\mathbf{C}_{n-1})$$

L'assertion (b) équivaut à l'existence d'un système projectif $(F_n)_n$ de $\mathbb{Q}^{\mathrm{ab}}((x))$-G-revêtements $F_n : X_n \to \mathbb{P}^1$ qui réalise le système complet $(G_n)_{n\geq 0}$, avec la contrainte supplémentaire suivante : pour tout $n \geq 0$, le $\mathbb{Q}^{\mathrm{ab}}((x))$-G-revêtement F_n doit avoir r_n-points de branchement et être d'invariant canonique de l'inertie égal à $\mathbf{C}_n$. La preuve est très similaire à celle du théorème 3.4 (dans le cas $k = \mathbb{Q}^{\mathrm{ab}}((x))$) ; il suffit d'adapter cette dernière aux conditions plus spécifiques demandées ici. Comme $\mu_\infty \subset k$, on peut choisir les points de branchement satisfaisant les conditions du §3.1 (2) dans $\mathbb{P}^1(k)$. On voit facilement qu'on peut garantir la condition (Hyp.) (i) en choisissant en outre les éléments g_{ni} $(i = 1, \ldots, r_n)$ dans les classes constituant $\mathbf{C}_n$ (à l'ordre près). La condition (Hyp.) (ii) est assurée par la HM-gcomplétude des $\mathbf{C}_n$ $(n \geq 0)$. Les conditions (iii) et (iv) de (Hyp.) sont vérifiées de façon évidente.

Pour (c), on fait de même mais en se plaçant sur $k = \mathbb{Q}_p^{\mathrm{nr}}$; l'hypothèse sur p garantit la condition supplémentaire dans (Hyp.) (iv) en inégale caractéristique.

Pour l'existence d'un système projectif $(\theta_n^\infty)_{n>0}$ de points $(\mathbb{R} \cap \overline{\mathbb{Q}})$-rationnels $\theta_n^\infty \in \mathcal{H}_{G_n,r_n}(\mathbf{C}_n)$, on procède comme précédemment mais en remplaçant le théorème 3.4 par le théorème 2.3, et en choisissant les points de branchement comme indiqué dans la preuve des théorèmes 2.1 et 2.3.

Pour tout $n \geq 0$, considérons la composante $\mathcal{H}_n^x$ de $\mathcal{H}_{G_n,r_n}(\mathbf{C}_n)$ à laquelle appartient la n-ième composante θ_n^x du système projectif $(\theta_n^x)_{n\geq 0}$ construit ci-dessus. Cette composante est *a priori* définie sur $\overline{\mathbb{Q}}$. Comme elle possède des points $\mathbb{Q}^{\mathrm{ab}}((x))$-rationnels, elle est définie sur $\mathbb{Q}^{\mathrm{ab}}((x)) \cap \overline{\mathbb{Q}} = \mathbb{Q}^{\mathrm{ab}}$.

Le reste de la preuve concerne la seconde partie de l'assertion (a). Pour cela, nous allons identifier la composante $\mathcal{H}_n^\infty$ de $\mathcal{H}_{G_n,r_n}(\mathbf{C}_n)$ à laquelle appartient chaque point θ_n^∞ $(n \geq 0)$. Nous nous appuyons sur des résultats de M. Fried [Fr2].

Fixons un entier $n \geq 0$. Notons HM_n l'ensemble des r_n-uplets d'éléments de G_n du type $(g_1, g_1^{-1}, \ldots, g_{t_n}, g_{t_n}^{-1})$ où $g_i \in C_{ni}$, $i = 1, \ldots, t_n$ et tels que $g_1, \ldots, g_{t_n}$ engendrent G_n. Par construction, les revêtements de la preuve du théorème 2.3 ont la propriété suivante : il existe un choix de lacets tournant une fois autour des points de branchement, de produit homotopiquement trivial et engendrant $\pi_1(\mathbb{P}^1(\mathbb{C}) - U_n)$, pour lequel le r_n-uplet des cycles de ramification du revêtement donnés par la monodromie le long de ces lacets est un élément de HM_n. Selon la terminologie de Fried, ils sont de type H(arbater)-(M)umford. D'après le théorème 3.21 de [Fr2], la condition "$\mathbf{C}_n$ HM-gcomplet" entraîne que les points de $\mathcal{H}_{G_n,r_n}(\mathbf{C}_n)$ correspondant aux revêtements de type Harbater-Mumford sont dans une même composante connexe, disons $\mathcal{H}_n^\infty$. En particulier $\mathcal{H}_n^\infty$ contient le point θ_n^∞. De plus, d'après le même résultat de Fried, si $Z(G_n) = \{1\}$, la composante $\mathcal{H}_n^\infty$ est définie sur $\mathbb{Q}$. □

4.2. Application aux tours modulaires.

On se donne un groupe fini G et un nombre premier ℓ divisant $|G|$. On note ${}_\ell\tilde{G}$ le ℓ-revêtement universel de Frattini de G. Rappelons (voir [FrJa]) qu'un épimorphisme de groupes $\psi : H \to G$ (un revêtement) est dit *de Frattini* si, pour tout sous-groupe H' de H, $\psi(H') = G \Rightarrow H' = H$. Le produit fibré de deux revêtements de Frattini a la propriété de Frattini. Il y a un objet universel $\tilde{G}$ pour les revêtements de Frattini d'un groupe G donné. Il existe aussi un objet universel pour les revêtements de Frattini $\psi : H \to G$ de G de noyau $\ker(\psi)$ un ℓ-groupe : c'est le groupe profini ${}_\ell\tilde{G}$.

Le but de ce paragraphe est le résultat suivant (cité dans l'introduction).

Théorème 4.2.— *Soit (k, v) un corps valué hensélien. Soient G un groupe fini et ℓ un nombre premier tel qu'il existe un système de générateurs de G d'ordre premier à ℓ, et à* $\mathrm{car}(k)$ *si* $\mathrm{car}(k) > 0$. *Alors le ℓ-revêtement universel de Frattini ${}_\ell\tilde{G}$ de G est groupe de Galois d'une extension galoisienne régulière de $k(T)$.*

Si $\mathrm{car}(k) = p > 0$, on suppose en particulier que G est *p-parfait*, au sens de [BaFr] : G est engendré par ses éléments d'ordre premier à p. Dans ce cas ou bien si $\mathrm{car}(k) = 0$, le théorème 4.2 s'applique pour tout premier ℓ sauf un nombre fini.

En caractéristique 0, la preuve va correspondre à la construction d'un système projectif de points rationnels sur une *tour modulaire* construite à partir de G et ℓ. Nous rappelons succintement la définition des tours modulaires, due à Fried [Fr2].

On définit, à partir du noyau ker de l'homomorphisme ${}_\ell\tilde{G} \to G$, une suite de quotients caractéristiques de ${}_\ell\tilde{G}$:

$$\ker_0 = \ker,\ \ker_1 = \ker_0^\ell[\ker_0, \ker_0], \ldots,\ \ker_n = \ker_{n-1}^\ell[\ker_{n-1}, \ker_{n-1}], \ldots$$

et on note ${}^n_\ell\tilde{G}$ le quotient ${}_\ell\tilde{G}/\ker_n$ $(n \geq 0)$. Le lemme suivant est une des observations de départ de la construction des tours modulaires ([Fr2] lemma 3.7).

Lemme 4.3.— *Si C est une classe de conjugaison d'éléments de ${}^n_\ell\tilde{G}$ d'ordre ρ premier à ℓ, alors il existe une unique classe de conjugaison de ${}^{n+1}_\ell\tilde{G}$ relevant C et dont les éléments sont d'ordre ρ.*

Supposons donné un ensemble $\mathbf{C} = (C_1, \ldots, C_r)$ de classes de conjugaison de G dont les éléments ont un ordre premier à ℓ. Grâce au lemme 4.3, on peut définir, pour tout $n \geq 0$, un r-uplet, noté $\mathbf{C}_n = (C_{n1}, \ldots, C_{nr})$ de classes de conjugaison de ${}^n_\ell\tilde{G}$, de telle façon que $C_{n+1\,i}$ relève C_{ni} et soit de même ordre, $i = 1, \ldots, r$ (par ordre, on entend ici l'ordre des éléments dans la classe). Notons ${}_\ell\mathcal{H}_n^{\mathrm{mod}} = {}_\ell\mathcal{H}_n^{\mathrm{mod}}(r, G, \mathbf{C})$ l'espace de Hurwitz $\mathcal{H}_{r,{}^n_\ell\tilde{G}}(\mathbf{C}_n)$ $(n \geq 0)$. Pour tout $n > 0$, on a un morphisme

$${}_\ell\mathcal{H}_n^{\mathrm{mod}} \to {}_\ell\mathcal{H}_{n-1}^{\mathrm{mod}}$$

La tours des espaces ${}_\ell\mathcal{H}_n^{\mathrm{mod}}$ $(n \geq 0)$ est appelée *tour modulaire* associée au quadruplet $(r, G, \mathbf{C}, \ell)$. Indiquons que l'hypothèse "G ℓ-parfait" entraîne que si $Z(G) = \{1\}$ alors $Z({}^n_\ell\tilde{G}) = \{1\}$ pour tout $n \geq 0$: les espaces ${}_\ell\mathcal{H}_n^{\mathrm{mod}}$ $(n \geq 0)$ sont alors tous des espaces de modules fins [BaFr] Proposition 3.21.

Preuve du théorème 4.2. Fixons un corps complet (k, v). On pose $G_o = G$ et $G_n = {}^n_\ell\tilde{G}$ et on note s_n le morphisme naturel $G_n \to G_{n-1}$ $(n > 0)$; on dispose ainsi d'un système complet $(G_n)_{n\geq 0}$ de groupes finis. Nous allons utiliser une nouvelle fois la construction générale du §3.1. On fixe $g_{o1}, \ldots, g_{o\beta_o}$ des générateurs de G d'ordre premier à ℓ et à $\mathrm{car}(k)$ si $\mathrm{car}(k) > 0$. On définit ensuite la suite $(g_{ni})_{n\geq 0}$ par récurrence en prenant $g_{(n+1)i}$ égal à un élément (quelconque) de *la* classe de conjugaison de G_{n+1} qui relève celle de g_{ni} dans G_n et qui est de même ordre (voir lemme 4.3), $i = 1, \ldots, \beta_o$. Pour $i > \beta_o$ et $n \geq 0$, on prend $g_{ni} = 1$. Les conditions (i), (iii) et (iv) de l'hypothèse (Hyp.) de §3.1 sont alors satisfaites. Quant à la condition (ii), elle résulte de la propriété de Frattini des morphismes $s_n : G_n \to G_{n-1}$ $(n > 0)$.

On choisit ensuite x_i, y_i $(i = 1, \ldots, \beta_o)$ comme indiqué dans la partie (2) de la construction générale; il n'est pas nécessaire de construire x_i, y_i pour $i > \beta_o$, puisque l'inertie associée à ces points a été choisie triviale. Pour tout $n \geq 0$, les points de branchement du G-revêtement F_n construit en §3.1, sont les points de l'ensemble $U_{\beta_o} = \{x_i^\tau, y_i^\tau \mid i = 1, \ldots, \beta_o,\ \tau \in \mathbf{G}_k\}$.

On applique ensuite la partie (3) de la construction générale, qui permet de construire des épimorphismes f_n $(n \geq 0)$. Notons $\mathbf{C} = (C_1, \ldots, C_r)$ le r-uplet (où $r = \mathrm{card}(U_{\beta_o})$) constitué des classes de conjugaison dans G des éléments $f_o(\Gamma_x)$ et $f_o(\Delta_y)$ quand (x, y) décrit U_{β_o}. Par construction, pour tout $n \geq 0$, le r-uplet $\mathbf{C}_n$ défini plus haut à partir de $\mathbf{C}$ par relèvement est alors le r-uplet des classes de conjugaison dans G_n des éléments $f_n(\Gamma_x)$ et $f_n(\Delta_y)$ quand (x, y) décrit U_{β_o}.

La construction fournit finalement un système projectif $(F_n)_{n\geq 0}$ de k-G-revêtements $F_n : X_n \to \mathbb{P}^1$, ou, de façon équivalente, une tour d'extensions galoisiennes régulières $K_n/k(T)$ régulières sur k, qui réalise le système complet $(G_n)_{n\geq 0}$, ou, de façon encore équivalente en caractéristique 0, un système projectif $(\theta_n)_{n\geq 0}$ de points k-rationnels sur la tour modulaire $({}_\ell\mathcal{H}_n^{\rm mod})_{n\geq 0}$ $(n \geq 0)$.

On déduit le résultat dans le cas où k est hensélien de la même façon qu'on a montré le théorème 3.4 à partir du cas complet. $\square$

4.3. Commentaires.

(a) Si on choisit pour $g_{o1}, \ldots, g_{o\beta_o}$ *tous* les éléments de G d'ordre premier à ℓ, l'espace ${}_\ell\mathcal{H}_n^{\rm mod}$ est défini sur $\mathbb{Q}$ (comme schéma intègre) pour tout $n \geq 0$. En effet, il s'agit de vérifier que chaque r-uplet $\mathbf{C}_n$ est (globalement) $\mathbb{Q}$-rationnel, c'est-à-dire, satisfait $\{C_{n1}^{\chi(\tau)}, \ldots, C_{nr}^{\chi(\tau)}\} = \{C_{n1}, \ldots, C_{nr}\}$, pour tout $\tau \in \mathbf{G}_\mathbb{Q}$. Pour $n = 0$, cela résulte de la construction de f_o : pour $i = 1, \ldots, \beta_o$, toutes les puissances de g_{oi} d'ordre premier à l'ordre de g_{oi} figurent (un même nombre de fois) parmi les éléments $f_o(\Gamma_x)$ et $f_o(\Delta_y)$ $((x, y \in U_o)$, lesquels définissent les classes $C_1, \ldots, C_r$. La $\mathbb{Q}$-rationalité de $\mathbf{C}_n$ pour $n > 0$ s'en déduit aisément par récurrence, grâce à l'unicité du relèvement dans le lemme 4.3.

(b) On peut se demander si l'énoncé du théorème 4.2 (ou similairement celui du théorème 3.4) où k est plus généralement un corps *ample* est vrai. Rappelons qu'un corps k est dit ample (ou large) si toute k-courbe lisse géométriquement irréductible a une infinité de k-points si elle en a au moins un, ou, de façon équivalente si k est existentiellement fermé dans $k((x))$ [Po3]. Par un argument classique de spécialisation (*e.g.* [DeDes]), si k est ample, on peut à partir d'une tour réalisant régulièrement ${}_\ell\tilde{G}$ sur $k((x))(T)$, déduire pour tout $n \geq 0$ une extension régulière galoisienne de $k(T)$ de groupe G_n. Il n'est pas clair qu'on puisse spécialiser l'ensemble de la tour. Autrement dit, on peut trouver des points k-rationnels sur tout espace ${}_\ell\mathcal{H}_n^{\rm mod}$ (car ${}_\ell\mathcal{H}_n^{\rm mod}(k((x))) \neq \emptyset$) mais il n'est pas clair que la propriété “existentiellement fermé” s'étende aux systèmes projectifs de points rationnels sur des tours.

(c) Dans le cas particulier où G est le groupe diédral D_ℓ d'ordre 2ℓ avec ℓ premier $\neq 2$, où $r = 4$ et les 4 classes $C_1, \ldots, C_4$ sont toutes égales à la classe des involutions de G, alors, pour tout $n \geq 0$, le groupe G_n est le groupe $D_{\ell^{n+1}}$ et l'espace ${}_\ell\mathcal{H}_n^{\rm mod}$ est une $\mathbb{Q}$-variété géométriquement irréductible qui revêt la courbe modulaire $X_1(\ell^{n+1})$ (privée des pointes) ; le groupe profini ${}_\ell\tilde{G}$ est la limite projective D_{ℓ^∞} des groupes D_{ℓ^n} [Fr2]. Le théorème 4.2 s'applique dans ce contexte. On sait par ailleurs qu'il n'existe pas de réalisation régulière sur $\mathbb{Q}(T)$ du groupe profini D_{ℓ^∞} [Fr1] §7.

(d) Notre construction générale peut être utilisée pour la réalisation des groupes *finis* : à tout groupe fini G, on associe le système projectif complet $(G, s_n)_n$ où $s_n = \mathrm{Id}_G$ $(n > 0)$. Il s'agit d'un cas très particulier de notre construction. Les contraintes (i), (iii) et (iv) de l'hypothèse (Hyp.) de §3.1 disparaissent. En conséquence, il est possible d'effectuer la construction sans adjoindre de racines de l'unité au corps complet k considéré. On obtient l'énoncé suivant, qui redonne le résultat principal de [Des1]. Nous laissons les détails au lecteur.

Théorème 4.4.— *Pour tout groupe fini G, il existe un entier $r \geq 3$ et un r-uplet de classes de conjugaison de G tels que l'espace de Hurwitz $\mathcal{H}_{r,G}(\mathbf{C})$ possède une composante irréductible $\mathcal{H}$ définie sur $\mathbb{Q}$ qui ait des points rationnels sur $\mathbb{Q}((x))$, et donc aussi des points p-adiques pour tout nombre premier p.*

Références

[BaFr] P. Bailey and M. Fried, *Hurwitz monodromy, spin separation and higher levels of Modular Towers*, in *Proceedings of the Von Neumann Symposium on Arithmetic Fundamental Groups and Noncommutative Algebra (MSRI 1999)*, Proceedings of Symposia in Pure Mathematics, AMS, ed. by M. Fried and Y. Ihara, (2002), 79–220

[De1] P. Dèbes, *Covers of $\mathbb{P}^1$ over the p-adics*, in *Recent Developments in the Inverse Galois Problem*, Contemp. Math., **186**, (1995), 217–238.

[De2] P. Dèbes, *Arithmétique et espaces de modules de revêtements*, *Proceedings of the Number Theory conference in Zakopane*, (K. Gyory, H. Iwaniec and J. Urbanowicz ed.), Walter de Gruyter, (1999), 75–102.

[**DeDes**] P. Dèbes and B. Deschamps, *The regular inverse Galois problem over large fields*, in *Geometric Galois actions, 2*, Cambridge University Press. Lond. Math. Soc. Lect. Note Ser. **243**, Schneps, Leila (ed.) et al., (1997), 119–138.
[**DeFr**] P. Dèbes and M. Fried, *Nonrigid constructions in Galois theory*, Pacific J. Math. **163**, No.1, (1994), 81–122.
[**Des1**] B. Deschamps, *Existence de points p-adiques pour tout p sur un espace de Hurwitz*, in *Recent Developments in the Inverse Galois Problem*, Contemp. Math., **186**, (1995), 239–247.
[**Des2**] B. Deschamps, *Clôtures totalement réelles des corps de nombres ordonnables*, Manuscripta Mathematica, **100**, (1999), 291–304.
[**Do**] A. Douady, *Détermination d'un groupe de Galois*, C.R.A.S. Paris, **258**, (1964), 5305–5308.
[**Fr1**] M. Fried, *Topics in Galois Theory*, review of Serre's book [Se2], in *Recent Developments in the Inverse Galois Problem*, Contemp. Math., **186**, (1995), 15–32.
[**Fr2**] M. Fried, *Introduction to modular towers*, in *Recent Developments in the Inverse Galois Problem*, Contemp. Math., **186**, (1995), 111–171.
[**FrJa**] M. Fried and M. Jarden, *Field arithmetic*, Ergeb. der Math., 3. Folge, Band 11, Springer-Verlag, (1986).
[**FrVo**] M. Fried and H. Völklein, *The embedding problem over a Hilbertian PAC-field*, Ann. Math., II. **135**, No.3, (1992), 469–481.
[**HaJa**] D. Haran and M. Jarden, *Real free groups and the absolute Galois group of* $\mathbb{R}(t)$, Journal of Pure and Applied Algebra **37**, (1985), 155–165.
[**Har1**] D. Harbater, *Galois coverings of the arithmetic line*, LNM **1240**, (1987), 165–195.
[**Har2**] D. Harbater, *Fundamental groups and embedding problems in characteristic* p, Contemp. Math., **186**, (1995), 353–369
[**Hu**] A. Hurwitz, *Riemann'sche Flächen mit gegebenen Verzweigungspunkten*, *Mathematische Werke* **I**, 321–383.
[**KrNe**] A. Krull and J. Neukirch, *Die Struktur der absoluten Galoisgruppe über dem Körper* $\mathbb{R}(T)$, Math. Ann. **193**, (1971), 197–209.
[**Li**] Q. Liu, *Tout groupe fini est groupe de Galois sur* $\mathbb{Q}_p(T)$, Contemp. Math., **186**, (1995), 261–265.
[**MaMat**] G. Malle and B.H. Matzat, *Inverse Galois theory*, Springer-Verlag, (1999).
[**Po1**] F. Pop, *Half Riemann's existence theorem*, Algebra and Number Theory (G. Frey and J. Ritter, eds), de Gruyter Proceedings in Mathematics, (1994), 1–26
[**Po2**] F. Pop, *Étale covers of affine smooth curves*, Inv. Math., **120**, (1995), 555–578
[**Po3**] F. Pop, *Embedding problems over large fields*, Ann. Math., **144**, 1–35, (1996).
[**Ri**] P. Ribenboim, *L'arithmétique des corps*, Hermann, (1970).
[**RibZa**] L. Ribes and P. Zalesskii, *Profinite Groups*, Ergeb. der Math. **40**, Springer, (2000).
[**Se1**] J.-P. Serre, *Cohomologie Galoisienne*, LNM **5**, 5ème édition, Springer-Verlag (1994).
[**Se2**] J.-P. Serre, *Topics in Galois theory*, Jones and Bartlett Publ., Boston, (1992).
[**SGA 1**] A. Grothendieck, *Revêtements étales et groupe fondamental*, LNM, **224**, Springer (1971).
[**Uc**] K. Uchida, *Homomorphisms of Galois groups of solvably closed Galois extensions*, Journal of the Mathematics Society of Japan, **33**, (1981), 595–604.
[**Vo**] H. Völklein, *Groups as Galois groups - an introduction*, Cambridge Studies in Advanced Mathematics, **53**, Cambridge Univ. Press, (1996).
[**Wi**] J. Wilson, *Profinite Groups*, London Math. Soc. Monographs new series **19**, Oxford Science Publications, (1998)

Pierre Dèbes, Mathématiques, Université Lille 1 (USTL), 59655 Villeneuve d'Ascq, France
E-mail : Pierre.Debes@univ-lille1.fr
Bruno Deschamps, L.Ar.Al, Faculté des sciences et techniques, Université Jean Monnet, 23 rue du docteur Paul Michelon, 42023 Saint-Etienne, Cedex 2, France.
E-mail : Bruno.Deschamps@univ-st-etienne.fr