Journal de Théorie des Nombres de Bordeaux **16** (2004), 429–456

Automorphismes des corps locaux de caractéristique p.

par Jean-Pierre WINTENBERGER

Résumé. Nous donnons une preuve que tout automorphisme sauvagement ramifié d'un corps de séries formelles à une variable et à coefficients dans un corps parfait de caractéristique p provient de la construction du corps des normes d'une $\mathbf{Z}_p$-extension totalement ramifiée d'un corps local de caractéristique 0 ou p.

Abstract. We give a proof of the following theorem : every wildly ramified automorphism of a formal series field of one variable with coefficients in a perfect field of characteristic p is given by field of norms construction from a totally ramified $\mathbf{Z}_p$-extension of a local field of characteristic 0 or p.

0. Introduction

Soit k un corps et $X = k((\pi))$ le corps des séries formelles de Laurent. On note $\mathcal{A}$ le groupe des automorphismes continus et sauvagement ramifiés de X. Un élément σ de $\mathcal{A}$ agit donc trivialement sur k et est déterminé par :

$$\sigma(\pi) = \pi + \alpha_2\pi^2 + \alpha_3\pi^3 + \dots .$$

Si v est la valuation de X définie par $v(\pi) = 1$ et $v(k) = 0$, on pose :

$$i(\sigma) = v(\sigma(\pi) - \pi) - 1,$$

(il est immédiat que cette définition ne dépend pas du choix de l'uniformisante π). On filtre le groupe $\mathcal{A}$ par ses sous-groupes $\mathcal{A}_i = \{\sigma \in \mathcal{A}, i(\sigma) \geq i\}$; le groupe $\mathcal{A}$ est séparé et complet pour la topologie définie par cette filtration. On a, pour $a \in \mathbb{Z}$ et $i = i(\sigma)$:

$$\sigma^a(\pi) = \pi + a\alpha_{i+1}\pi^{i+1} + \dots .$$

On voit que si k est de caractéristique 0, on a $i(\sigma^a) = i(\sigma)$ et le sous-groupe de $\mathcal{A}$ engendré par σ est discret. Si k est de caractéristique $p > 0$, on a $i(\sigma^a) = i(\sigma)$ si a est premier à p, et $i(\sigma^a) > i(\sigma)$ si a est divisible par p. La fermeture du sous-groupe de $\mathcal{A}$ engendré par σ est isomorphe à $\mathbb{Z}_p$ ou à un groupe cyclique d'ordre une puissance de p. Ce dernier cas est donné par les extensions cycliques totalement ramifiés d'ordre une puissance de p d'un corps de séries formelles de Laurent à coefficients dans k.

Si k est de caractéristique 0, σ est conjugué dans $\mathcal{A}$ à un automorphisme défini par :

$$\sigma'(\pi) = \pi + \alpha\pi^{i+1} + \beta\pi^{2i+1},$$

$\alpha \neq 0$ et i entier ≥ 1, et le commutant de σ dans $\mathcal{A}$ est isomorphe au groupe additif de k ([11]).

La situation est plus compliquée si k est de caractéristique p. Supposons k de caractéristique p et de plus parfait. La correspondance entre automorphismes des corps de séries formelles et extensions galoisiennes ne concerne pas que les automorphismes d'ordre fini. Appelons corps local un corps valué complet pour une valuation discrète à corps résiduel parfait de caractéristique p. Si K est un corps local de caractéristique 0 et de corps résiduel k, le corps K est une extension finie du corps des fractions des vecteurs de Witt à coefficients dans k, et si K est un corps local de caractéristique p, K est un corps de séries formelles de Laurent à coefficients dans k ([19] chap. 2). J.-M. Fontaine a donné une construction qui, à un corps local K et à une extension galoisienne L de K, totalement ramifiée et à groupe de Galois Γ isomorphe à $\mathbb{Z}_p$ associe son corps des normes, qui est un corps local $X_K(L)$ de caractéristique p, de même corps résiduel que K et L, avec Γ agissant fidèlement sur $X_K(L)$ par des automorphismes sauvagement ramifiés ([4],[7],[6],[24]).

L'objet de cet article est de donner une démonstration du fait que tous les automorphismes sauvagement ramifiés d'ordre infini des corps locaux de caractéristique p proviennent d'une telle extension de corps locaux ([22],[23]).

Précisons. Soit X un corps local de caractéristique p et de corps résiduel parfait k. Soit σ un automorphisme sauvagement ramifié d'ordre infini de X. Soit $(i_n)_{n\in\mathbb{N}}$ la suite des nombres de ramification (en numérotation inférieure) de σ : $i_n = i(\sigma^{p^n})$. S Sen a prouvé les congruences suivantes : $i_{n+1} \equiv i_n \bmod p^{n+1}$ ([17] ; pour une autre démonstration : [12]). Si σ est d'ordre fini dans $\mathcal{A}$, les congruences démontrées par S. Sen, sont équivalentes au théorème de Hasse-Arf pour l'extension X/X^{σ}. Il n'est pas difficile de prouver que l'on a $i_{n+1} \geq pi_n$ avec égalité si et seulement si i_n est divisible par p ([19] chap.4 exercice 3, [8] lemma 3) (les congruences de S. Sen prouvent que cette dernière condition est équivalente à i_0 divisible par p) . Soit l la limite, éventuellement infinie, de la suite croissante i_n/p^n. La suite des entiers $(i_{n+1} - i_n)/p^{n+1}$ a pour limite $l(p-1)/p$. On en déduit que, soit l est fini et il existe un entier $e(\sigma) \geq 1$ tel que pour, pour n grand, on a : $i_{n+1} - i_n = p^{n+1}e(\sigma)$, soit l est infini, auquel cas on convient que $e(\sigma) = \infty$.

Théorème 1. *Soient X et σ comme ci-dessus. Notons Γ (isomorphe à $\mathbb{Z}_p$) le sous-groupe du groupe $\mathcal{A}$ des automorphismes sauvagement ramifiés de X engendré par σ. Alors, il existe un corps local K de corps résiduel k et* *d'indice de ramification absolu $e(\sigma)$ (de caractéristique p si $e(\sigma) = \infty$) et une extension L de K, totalement ramifiée et à groupe de Galois isomorphe à $\mathbb{Z}_p$, telle que X, muni de son groupe d'automophismes Γ, soit isomorphe à $X_K(L)$, muni de l'image de* $\mathrm{Gal}(L/K)$ *dans le groupe des automorphismes de $X_K(L)$.*

Ce théorème a pour conséquences une généralisation du théorème de Hasse-Arf ([23]), des propriétés de ramification d'éléments de $\mathcal{A}$ commutant ([9], [10]). Il permet de déterminer presque complètement les suites d'entiers qui sont suite des nombres de ramification en numérotation supérieure d'un élément de $\mathcal{A}$ ([9], [10]).

Précisons ce dernier point. Pour e entier ≥ 1 ou $e = \infty$, notons I'_e l'ensemble des entiers qui sont > 0, non divisibles par p, et $\leq pe/(p-1)$. Notons $I_e = I'_e$ si e n'est pas divisible par $p-1$ et $I_e = I'_e \cup \{pe/(p-1)\}$ si $p-1$ divise e. Soit f_e la fonction $n \mapsto \min(pn, n+e)$. Pour une suite d'entiers $0 < b_0 < b_1 < \ldots < b_m$ définissons la propriété (R) (respectivement (R$'$)) par les conditions suivantes, où I est I_e (respectivement I'_e) :

– $b_0 \in I$,

– si $b_n < e/(p-1)$, $\begin{cases} \text{soit } b_{n+1} = f_e(b_n) = pb_n, \\ \text{soit } b_{n+1} > f_e(b_n) \text{ et } b_{n+1} \in I, \end{cases}$

– si $b_n \geq e/(p-1)$, $b_{n+1} = f_e(b_n) = b_n + e$.

Alors ([13]), si (b_n) est la suite des nombres de ramification en numérotation supérieure d'une extension cyclique totalement ramifiée de degré une puissance de p d'un corps local d'indice de ramification absolu e, la suite (b_n) vérifie (R).

Réciproquement, si K est un corps local d'indice de ramification absolu e qui ne contient pas de racine primitive p-ième de l'unité, et si (b_n) est une suite de m entiers vérifiant (R$'$) , il existe une extension cyclique totalement ramifiée de degré p^m de K dont (b_n) est la suite des nombres de ramification en numérotation supérieure ([14],[13],[16]). Il résulte du théorème que si (b_n) est la suite des nombres de ramification en numérotation supérieure d'un automorphisme sauvagement ramifié de X, alors il existe e (entier ou infini) tel que (b_n) satisfasse (R). Si $p \neq 2$, pour tout e il existe un corps local K d'indice de ramification absolu e ne contenant pas de racine primitive p-ième de l'unité et de corps résiduel le corps à p éléments. Pour un tel corps local, toute extension cyclique totalement ramifiée de degré une puissance de p se plonge dans une $\mathbb{Z}_p$-extension totalement ramifiée. Il en résulte facilement que, si $p \neq 2$, si (b_n) est une suite infinie d'entiers > 0 telle qu'il existe $e > 0$ tel que (b_n) vérifie (R$'$), il existe un automorphisme sauvagement ramifié de $\mathbb{F}_p[[\pi]]$ dont la suite des nombres de ramification en numérotation supérieure soit la suite (b_n). Par contre, la suite des entiers > 0 vérifie (R) pour $p = 2$ et $e = 1$ mais n'est pas la suite des nombres de ramification en numérotation supérieure d'un $\sigma \in \mathcal{A}$ si $k = \mathbb{F}_2$. On peut le voir en vérifiant par un calcul simple que si $k = \mathbb{F}_2$, $i_0 = 1$ et $i_1 = 3$ entraîne $i_2 > 7$. Cela résulte aussi du théorème et du fait qu'il n'existe pas de $\mathbb{Z}_2$-extension totalement ramifiée de $\mathbb{Q}_2$, dont les nombres de ramification en numérotation supérieure soit la suite des entiers > 0.

Pour une démonstration n'utilisant pas notre résultat de certaines des propriétés de ramification des automorphismes sauvagement ramifiés des corps locaux de caractéristique p, voir [8]. Comme le groupe des automorphismes sauvagement ramifiés d'un corps local de caractéristique 0 est d'ordre inférieur à son indice de ramification absolu, le théorème entraîne aussi que si $e(\sigma) < \infty$, le sous-groupe de $\mathcal{A}$ engendré par σ est d'indice fini ($\leq e(\sigma)$) dans son normalisateur ; j'ignore si la réciproque est vraie. Pour une étude du groupe $\mathcal{A}$, voir [21] chap. 4 ex. 9 ,[3],[1],[2].

Je remercie F. Laubie dont les remarques m'ont permis de corriger quelques erreurs.

1. Notations.

Si K est un corps local, on note v_K la valuation de K normalisée par $v_K(K^*) = \mathbb{Z}$. Si M est une extension algébrique de K ou le complété d'une telle extension, on note encore v_K l'unique prolongement de v_K à M. On note O_M l'anneau de valuation de M, U_M le groupe des unités de O_M et U_M^+ le sous-groupe de U_M formé des unités qui sont congruentes à 1 modulo l'idéal maximal de O_M. Si σ est un plongement de K dans M qui induit l'inclusion sur les corps résiduels , on pose $i_K(\sigma) = v_K(\sigma(\pi) - \pi) - 1 \in \mathbb{Q} \cup \{\infty\}$, où π est une uniformisante de K (comme, si π' est une autre uniformisante de K, on a : $\pi' = f(\pi)$, avec f série formelle à coefficients des représentants de Teichmuller des éléments de k, on voit que cette définition ne dépend pas du choix de π). Un automorphisme σ de K est dit ramifié s'il agit trivialement sur le corps résiduel et sauvagement ramifié s'il est ramifié et si $i_K(\sigma) > 0$. Si G est un groupe d'automorphismes ramifiés de K et $x \in \mathbb{R}_+$, on note G_x le sous-groupe de ramification de G défini par $G_x = \{\sigma \in G,\ i_K(\sigma) \geq x\}$. Si les G_x sont d'indices finis dans G, on passe à la numérotation supérieure G^x de la manière usuelle ([19] chap. 4) par les fonctions φ_G et ψ_G de Herbrand :

$$\varphi_G(x) = \int_0^x \mathrm{d}t/[G : G_t], \quad G^x = G_{\psi_G(x)},$$

la fonction ψ_G étant la fonction réciproque de φ_G. On note $e_K \in \mathbb{N} \cup \{\infty\}$ l'indice de ramification absolu de K *i.e.* $e_K = v_K(p)$ (e_K est donc infini si et seulement si K est de caractéristique p). Si K' est un corps local contenant K, on note $e_{K'/K}$ l'indice de ramification de K'/K *i.e.* $e_{K'/K} = v_{K'}(\pi)$, pour π uniformisante de K.

Pour G groupe d'automorphismes d'un corps, on fait agir l'algèbre du groupe G sur le groupe multiplicatif, ainsi : $(\sigma - 1)(u) = \sigma(u)/u$.

On note $\widehat{K^*}$ le complété p-adique du groupe multiplicatif de K. La valuation v_K se prolonge en un homomorphisme surjectif de $\widehat{K^*}$ sur $\mathbb{Z}_p$ dont le noyau est le groupe U_K^+ des unités qui sont congruentes à 1 modulo l'idéal maximal : on note encore v_K cet homomorphisme.

2. $\mathbb{Z}_p$-extensions des corps locaux et pleine fidélité du foncteur corps des normes.

2.1. Soit K un corps local et soit L une extension de K totalement ramifiée de groupe de Galois Γ isomorphe à $\mathbb{Z}_p$. Soit b_n la suite des nombres de ramification en numérotation supérieure de l'extension L/K. Le théorème de Hasse-Arf donne que les b_n sont des entiers. On a $\Gamma^{b_n} = p^n\Gamma$, et les nombres de ramification en numérotation inférieure de l'extension de groupe de Galois $\Gamma/p^n\Gamma$ sont les entiers $i_0, i_1, \ldots, i_{n-1}$ avec : $i_0 = b_0$ et $i_m = i_{m-1} + p^m(b_m - b_{m-1})$. Il est bien connu que si K est de caractéristique 0 et si n est suffisamment grand pour que $b_n \geq e/(p-1)$, on a $b_{n+1} = b_n + e_K$; si K est de caractéristique p, on a $b_{n+1} \geq pb_n$ (voir par exemple [13]). On en déduit que la suite croissante i_n/p^n a pour limite $pe_K/(p-1)$. Si σ est un générateur de Γ, la suite des $i_n(\sigma)$ (σ considéré comme un automorphisme du corps des normes $X_K(L)$) coïncide avec la suite des i_n de l'extension L/K ([24]). On voit donc que $e_K = e(\sigma)$, $e(\sigma)$ étant défini comme dans l'introduction, σ agissant sur $X_K(L)$.

2.2. Rappelons brièvement la construction du corps des normes $X_K(L)$ ([24]). Soit, pour n entier ≥ 0, K_n l'extension de K de degré p^n contenue dans L. Notons O_n l'anneau de valuation de K_n et P_n l'idéal maximal de K_n. Notons $N_{n+1,n}$ la norme de K_{n+1}/K_n. Notons r_n le plus petit entier supérieur à $(p-1)i_n/p$. La norme $N_{n+1,n}$ induit un homomorphisme surjectif d'anneaux : $O_{n+1} \to O_n/P_n^{r_n}$ et l'anneau de valuation $O_{X_K(L)}$ de $X_K(L)$ est la limite projective des anneaux $O_n/P_n^{r_n}$, les applications de transition étant induits par la norme. Les éléments de $O_{X_K(L)}$ s'identifient aux suites d'éléments α_n avec $\alpha_n \in K_n$ avec $N_{n+1,n}(\alpha_{n+1}) = \alpha_n$. Soit m un entier et soit $x = (\alpha_n) \in O_{X_K(L)}$. La suite des $(\alpha_n^{p^{n-m}})_{n\geq m}$ converge dans le complété $\hat{L}$ de L vers un élément x_m. La suite des x_m vérifie : $x_{m+1}^p = x_m$. L'ensemble des suites x de $\hat{L}$ vérifiant $x_{m+1}^p = x_m$ forme un corps noté $R(\hat{L})$ qui s'identifie au complété de la clôture radicielle de $X_K(L)$ (la multiplication et l'addition sont données par les formules : $(xx')_m = x_m x'_m$, $(x+x')_m = \lim_{s\to\infty}(x_{m+s} + x'_{m+s})^{p^s}$ ([24]).

2.3. On suppose dans ce numéro que K est de caractéristique p. L'application $x \mapsto x_0$ est un isomorphisme de $R(\hat{L})$ sur $\hat{L}$ ([24]). Le corps $\hat{L}$ est donc parfait, $X_K(L)$ s'identifie à un sous-corps de $\hat{L}$, et $\hat{L}$ s'identifie au complété de la clôture radicielle de $X_K(L)$.

Proposition 1. *Soit $x = x_0 = (\alpha_n) \in X_K(L) \subset \hat{L}$. Soit n un entier ≥ 0. La suite des $(\sum_{i=0}^{p^m-1} \sigma^{p^n i})(x^{\frac{1}{p^{m+n}}})$ (pour la notation, voir 1) converge dans $\hat{L}$ vers α_n lorsque m tend vers l'infini.*

Démonstration. Faisons la pour $n = 0$. Supposons $x \neq 0$. Posons $v = v_K = v_{X_K(L)}$. Posons $z_m = (\sum_{i=0}^{p^m-1} \sigma^i)(x^{\frac{1}{p^m}})$. Il nous faut prouver que z_m tends vers α_0 lorsque m tends vers l'infini. Si $t_m = (\sum_{i=0}^{p-1} \sigma^{ip^m} - p)(x)$, on a :

$$z_{m+1}^{p^{m+1}} / z_m^{p^{m+1}} = (\sum_{i=0}^{p^m-1} \sigma^i)(t_m).$$

Comme $v(t_m - 1) \geq i_m$, on voit que :

$$v(\frac{z_{m+1}}{z_m} - 1) \geq \frac{i_m}{p^{m+1}}.$$

Comme i_m/p^{m+1} tend vers l'infini avec m (*cf* 2.1), la suite des z_m converge dans $\hat{L}$. Notons $N_0(x)$ sa limite et, de même, pour tout entier n, $N_n(x)$ la limite de la suite des $(\sum_{i=0}^{p^m-1} \sigma^{p^n i})(x^{\frac{1}{p^{m+n}}})$. Comme la suite des i_m/p^{m+1} est croissante, on voit que l'on a :

$$v(x - N_0(x)) \geq v(x) + \frac{i_0}{p},$$

et de même :

$$v(x - N_n(x)^{p^n}) \geq v(x) + \frac{i_n}{p}.$$

On a :

$$v(N_{m+1,m}(\alpha_{m+1}) - \alpha_{m+1}^p) \geq pv(\alpha_{m+1}) + \frac{i_m}{p^{m+1}},$$

soit :

$$v(\alpha_m - \alpha_{m+1}^p) \geq v(\alpha_m) + \frac{i_m}{p^{m+1}}.$$

Comme $x = \lim_{m\to\infty} \alpha_m^{p^m}$ et que la suite des i_m/p^{m+1} est croissante, on en déduit que :

$$v(x - \alpha_n^{p^n}) \geq v(x) + \frac{i_n}{p}.$$

Finalement :

$$v(N_n(x) - \alpha_n) \geq p^{-n}v(x) + \frac{i_n}{p^{n+1}}.$$

On a : $N_0(x) = (\sum_{i=0}^{p^n-1} \sigma^i)(N_n(x))$ et $\alpha_0 = (\sum_{i=0}^{p^n-1} \sigma^i)(\alpha_n)$. D'où :

$$v(N_0(x) - \alpha_0) \geq v(x) + i_n/p^{n+1}.$$

Comme i_n/p^{n+1} tend vers l'infini avec n, on en déduit que $N_0(x) = \alpha_0$, et la proposition est prouvée.

Corollaire 1. *Si π est une uniformisante de $X_K(L)$, on a*
$$K_n = k((N_n(\pi))).$$

2.4. Soient $\overline{K}$ une clôture algébrique de K contenant L et K_s la clôture séparable de K dans $\overline{K}$. Notons G et H les groupes de Galois de K_s/K et K_s/L respectivement. Soit, comme dans [24], $X_{L/K}(K_s)$ le corps limite inductive des $X_K(L')$ pour L' extension finie de L contenues dans K_s, de sorte que $X_{L/K}(K_s)$ est une clôture séparable de $X_K(L)$. On la note X_s. Le groupe G s'identifie au groupe des automorphismes de X_s qui laissent stable $X_K(L)$ et induisent sur $X_K(L)$ un automorphisme de Γ et le groupe H s'identifie au groupe de Galois de $X_s/X_K(L)$ ([24]).

2.5. Supposons K de caractéristique 0. Notons C le complété de K_s. Le corps $R(C)$ des suites (x_n) d'éléments de C vérifiant $x_{n+1}^p = x_n$ s'identifie au complété $\hat{X}_s$ de X_s. Soit ϵ un élément de $U^+_{\hat{X}_s}$ tel que ϵ_0 soit une racine primitive p-ième de l'unité. Si χ est le caractère cyclotomique, on a donc $\tau(\epsilon) = \epsilon^{\chi(\tau)}$ pour tout $\tau \in G$.

Proposition 2. *Soient $u \neq 1$ un élément de $U^+_{\hat{X}_s}$ et η un caractère de G à valeurs dans $\mathbb{Z}_p^*$ tels que $\tau(u) = u^{\eta(\tau)}$ pour tout $\tau \in G$. Alors η est le caractère cyclotomique et $u \in \epsilon^{\mathbb{Q}_p}$.*

Démonstration. Soit H' le noyau de η. Le caractère η est ramifié. En effet, sinon posons $K' = C^{H'}$. Le corps K' serait le corps local complété de l'extension non ramifiée $K_s^{H'}$ de K (prop. 10 de [20]). Alors les u_n seraient des éléments de $U^+_{K'}$, vérifiant $u_{n+1}^p = u_n$, on aurait $u_n = 1$ pour tout n contrairement à l'hypothèse $u \neq 1$. Donc η est ramifié et on a $C(\eta)^G = \{0\}$ (th. 2 de [20]). Comme $\tau\log(u_n) = \eta(\tau)\log(u_n)$ pour tout $\tau \in G$, il en résulte que $\log(u_n) = 0$ et les u_n sont bien des racines de l'unité.

2.6. Supposons K de caractéristique 0. Notons $[\epsilon]$ le représentant de Teichmuller dans l'anneau des vecteurs de Witt $W(O_{X_s})$ de ϵ et posons $\xi = \sum_{i=0}^{p-1}[\epsilon]^i$. Le morphisme naturel $W(O_{X_s}) \to O_C$ est surjectif et a pour noyau l'idéal principal de $W(O_{X_s})$ engendré par ξ ([24]). On voit donc qu'on a la proposition :

Proposition 3. *Notons, pour tout entier n, G_n le groupe de Galois de $\overline{K}/K_n$. Alors, pour tout n, l'anneau de valuation O_n de K_n s'identifie à $(W(O_{X_s})/\xi W(O_{X_s}))^{G_n}$.*

2.7. On définit la catégorie ΓEXT : ses objets sont la donnée d'un corps local K et d'une extension L de K totalement ramifiée de groupe de Galois Γ isomorphe à $\mathbb{Z}_p$. Un morphisme $L/K \to L'/K'$ est un plongement continu $i : L \hookrightarrow L'$ tel que $i(K) \subset K'$, $K'/i(K)$ soit séparable, et $i(L)K' = L'$. On définit la catégorie ΓAUT : ses objets sont la donnée d'un corps local X de caractéristique p muni d'un sous-groupe Γ d'automorphismes sauvagement ramifiés de X qui est isomorphe à $\mathbb{Z}_p$. Un morphisme $(X,\Gamma) \to (X',\Gamma')$ est la donnée d'un plongement continu $j : X \hookrightarrow X'$ tels que X' soit une extension séparable de $j(X)$ et que les éléments de Γ' laissent stables $j(X)$ et agissent sur $j(X)$ par des éléments de Γ. On a alors un entier n_0 tel que la restriction à X induise un isomorphisme de Γ' sur le sous-groupe ouvert $p^{n_0}\Gamma$ de Γ. Si on associe à un objet L/K de ΓEXT de groupe de Galois Γ son corps des normes $X_K(L)$ muni de son sous-groupe d'automorphismes défini par l'action de Γ, on définit un foncteur X de ΓEXT vers ΓAUT. Soit i un morphisme dans ΓEXT ; décrivons $X(i)$. A (α_n) de $X_K(L)$, $X(i)$ associe (α'_n) défini par $\alpha'_n = i(\alpha_{n+n_0})$. On vérifie sans peine que l'indice de ramification de $X'/X(i)(X)$ est égal à celui de l'extension K'_n/K_{n+n_0} pour n grand.

Théorème 2. *Le foncteur corps des normes X est pleinement fidèle.*

Démonstration. Soient L/K et L'/K' de ΓEXT et $j : (X_K(L),\Gamma) \to (X_{K'}(L'),\Gamma')$ un morphisme dans ΓEXT. Posons $X = X_K(L)$ et $X' = X_{K'}(L')$. Indiquons comment on construit i tel que $X(i) = j$. Quitte à remplacer K par K_n pour un entier n, on peut supposer que la restriction à $j(X)$ définit un isomorphisme de Γ' sur Γ ($n_0 = 1$). Soit K'_{s} une clôture séparable de K' contenant L' et $X'_{\mathrm{s}} = X_{L'/K'}(K'_{\mathrm{s}})$ (*cf* 2.4). Prolongeons j en un plongement de X_{s} dans X'_{s}. D'après 2.4 , le plongement j induit un homomorphisme du groupe de Galois G' de K'_{s}/K' sur le groupe de Galois G de K_{s}/K.

Notons (i_n) et (i'_n) les suites des nombres de ramification en numérotation inférieure de Γ et Γ' respectivement. Soient $e(\Gamma)$ et $e(\Gamma') \in \mathbb{N} \cup \{\infty\}$ définis par $e(\Gamma) = \lim_{n\to\infty}(i_{n+1} - i_n)/p^{n+1}$ et de même pour $e(\Gamma')$.

Lemme 1. *On a* $e(\Gamma') = e(\Gamma)e_{X'/j(X)}$.

Démonstration. Soit σ' l' élément de Γ' d'image σ dans Γ. Une généralisation immédiate de la proposition 3 du chapitre 4 de [19] donne que, pour tout entier n :

$$i_X(\sigma^{p^n}) = \frac{1}{e_{X'/X}} \sum i_{X'}(\gamma),$$

où γ parcourt l'ensemble des plongements de X' dans X'_{s} qui induisent σ^{p^n} sur $j(X)$. Les γ sont les $\tau\sigma'^{p^n}$, τ décrivant les différents $j(X)$-plongements de X' dans X'_{s}. Pour n grand, on a $i_{X'}(\sigma'^{p^n}) > i_{X'}(\tau)$ pour tout $\tau \neq 1$. L'égalité ci-dessus devient pour n grand :

$$i_X(\sigma^{p^n}) = \frac{i_{X'}(\sigma'^{p^n})}{e_{X'/X}} + \frac{\sum' i_{X'}(\tau)}{e_{X'/X}},$$

la somme portant sur les $j(X)$-plongements de X' dans X'_{s} qui sont différents de l'identité. Le lemme en résulte.

2.8. Il en résulte que $e_{K'} = e_{X'/j(X)} e_K$. On voit donc que K, L, K' et L' sont tous de caractéristique 0 ou tous de caractéristique p.

Supposons tout d'abord que K soit de caractéristique 0. Soit $\epsilon' \in \hat{X}'_{\mathrm{s}}$ défini comme ϵ (*cf* 2.5). Il résulte du 2.4 et de la proposition 2 que l'on a $j(\epsilon) = \epsilon'^{a}$ avec $a \in \mathbb{Q}_p$. Comme $v_X(\epsilon - 1) = e(\Gamma)/(p-1)$ et $v_{X'}(\epsilon' - 1) = e(\Gamma')/(p-1)$, il résulte du lemme ci-dessus que a est une unité de $\mathbb{Z}_p$. Prolongeons j en un plongement de $W(j)$ de $W(O_{X_{\mathrm{s}}})$ dans $W(O_{X'_{\mathrm{s}}})$. Si $\xi' = \sum_{i=0}^{p-1} [\epsilon']^i \in W(O_{X'_{\mathrm{s}}})$, on voit que $W(j)$ envoie l'idéal $\xi W(O_{X_{\mathrm{s}}})$ dans l'idéal $\xi' W(O_{X'_{\mathrm{s}}})$. Comme $W(j)$ est compatible aux actions de G et de G', il résulte de la proposition 3 que $W(j)$ induit un morphisme de O_n dans O'_n pour tout n. Ces morphismes sont nécessairement des plongements et ils induisent un plongement de K_n dans K'_n pour chaque n, ce qui définit i.

Supposons maintenant K de caractéristique p. Soit π une uniformisante de X. On définit les $N'_n : X' \to K'_n$ comme au 2.3. On a : $j(N_n(\pi)) = N'_n(j(\pi))$ et on définit la restriction de i à K_n par cette formule (*cf* cor. 1). Ceci achève la démonstration du théorème.

3. Démonstration du théorème 1 : cas $e(\Gamma) = \infty$.

3.1. Soit (X, Γ) un objet ΓEXT (*cf* 2.7) avec $e(\Gamma) = \infty$, *i.e.* $\lim i_n/p^n = \infty$. Notons σ un générateur de Γ. Avant de prouver le théorème, prouvons la proposition suivante ([5]) :

Proposition 4. *Pour tout n, on a : $b_{n+1} \geq p b_n$. Il existe une suite $(\sigma_n)_{n \in \mathbb{N}}$ d'éléments du groupe $\mathcal{A}$ des automorphismes sauvagement ramifiés de X vérifiant : σ_n est d'ordre p^n dans $\mathcal{A}$ et $i_X(\sigma \circ \sigma_n^{-1}) \geq i_{n-1} + 1$.*

Démonstration. Soit m un entier ≥ 1. Posons : $z_m = (\sum_{i=0}^{p^m - 1} \sigma^i)(\pi)$. Soit Z_m le corps $k((z_m))$; donc X est une extension de degré p^m de Z_m. Soit p^r le degré d'inséparabilité de l'extension X/Z_m. La sous-extension maximale séparable de Z_m contenue dans X est X^{p^r}, donc X est une extension séparable de $Z'_m = Z_m^{p^{-r}}$. Notons X_{s} une clôture séparable de X.

Soit P le polynôme minimal de π sur Z_m. Pour $\gamma \in \Gamma$, on a :

$$v_X(\gamma(z_m) - z_m) \geq v_X(\sigma(z_m) - z_m) = i_m + p^m.$$

Il en résulte que :

$$v_X(P(\gamma(\pi))) = v_X(P(\gamma(\pi)) - \gamma(P)(\gamma(\pi))) \geq i_m + p^m.$$

Soit i un entier ≥ 1. Notons $S(i)$ l'ensemble des $\tau \in \mathrm{Gal}(X_{\mathrm{s}}/Z'_m)$ qui sont tels qu'il existe $\gamma \in \Gamma$ avec $v_X(\tau(\pi) - \gamma(\pi)) \geq i+1$. Notons $S'(i) \subset S(i)$ l'ensemble des $\tau \in \mathrm{Gal}(X_{\mathrm{s}}/Z'_m)$ vérifiant $v_X(\tau(\pi) - \pi) \geq i+1$. Comme $S(i)$ est l'ensemble des τ qui agissent sur $O_X/\pi^{i+1}O_X \subset O_{X_{\mathrm{s}}}/\pi^{i+1}O_{X_{\mathrm{s}}}$ comme un élément de Γ et $S'(i)$ est l'ensemble des τ qui agissent trivialement sur $O_X/\pi^{i+1}O_X \subset O_{X_{\mathrm{s}}}/\pi^{i+1}O_{X_{\mathrm{s}}}$, on voit que $S(i)$ est un sous-groupe de

$\mathrm{Gal}(X_s/Z'_m)$ et $S'(i)$ est un sous-groupe distingué de $S(i)$. Comme Γ/Γ_i agit fidèlement sur $O_X/\pi^{i+1}O_X$, on voit que si à $\tau \in S(i)$ on associe la classe de $\gamma \in \Gamma$ modulo Γ_i telle que $v_X(\tau(\pi) - \gamma(\pi)) \geq i+1$, on définit un homorphisme injectif de $S(i)/S'(i)$ dans Γ/Γ_i. Notons $X_{m,i}$ et $Y_{m,i}$ les extensions de Z'_m qui correspondent à $S'(i)$ et $S(i)$ respectivement. Comme $\mathrm{Gal}(X_s/X) \subset S'(i)$, on a : $Z'_m \subset Y_{m,i} \subset X_{m,i} \subset X$. L'extension $X_{m,i}/Y_{m,i}$ est galoisienne, de groupe de Galois isomorphe à l'image de $S(i)/S'(i)$ dans Γ/Γ_i.

Notons φ la fonction de Herbrand φ_Γ. On a donc : $\varphi(x) = x$ pour $0 \leq x \leq i_0$, $\varphi(x) = b_n + (x - b_n)/p^{n+1}$ pour $b_n \leq x \leq b_{n+1}$.

Lemme 2. *L'homomorphisme $S(i)/S'(i) \to \Gamma/\Gamma_i$ est surjectif pour i tel que $\varphi(i-1) < i_m/p^m$.*

Démonstration. Il n'y a rien à prouver si $i = 1$. Supposons $i \geq 2$ et supposons l'assertion prouvée pour $j \leq i-1$.

Notons $\mathcal{E}$ l'ensemble des Z'_m-plongements ι de X dans X_s. Pour tout entier $j \geq 0$ et tout $\gamma \in \Gamma$, notons $n_{\gamma,j}$ le nombre de $\iota \in \mathcal{E}$ vérifiant $v_X(\iota(\pi) - \gamma(\pi)) \geq j+1$. Soit $\gamma \in \Gamma$. Il s'agit de prouver que $n_{\gamma,i}$ n'est pas nul. Supposons $n_{\gamma,i} = 0$. Comme :

$$P(\gamma(\pi)) = \prod_{\iota \in \mathcal{E}} (\gamma(\pi) - \iota(\pi))^{p^r},$$

on voit que l'on a :

$$v_X(P(\gamma(\pi))) = p^r\Big(\sum_{j=0}^{i-1} (n_{\gamma,j} - n_{\gamma,j+1})(j+1)\Big),$$

soit :

$$v_X(P(\gamma(\pi))) = p^r\Big(\sum_{j=0}^{i-1} n_{\gamma,j}\Big).$$

Il résulte facilement de la définition de $S'(i)$ que l'on a $n_{\gamma,j} = [X : X_{m,j}]$ pour tout $\gamma \in \Gamma$. On a : $p^r[X : X_{m,j}][X_{m,j}, Y_{m,j}] \leq p^m$. D'où, comme d'après l'hypothèse de récurrence, $[X_{m,j}, Y_{m,j}] = [\Gamma : \Gamma_j]$:

$$v_X(P(\gamma(\pi))) \leq p^m\Big(\sum_{j=0}^{i-1} \frac{1}{[\Gamma : \Gamma_j]}\Big),$$

soit :

$$v_X(P(\gamma(\pi))) \leq p^m(1 + \varphi(i-1)).$$

Comme :

$$v_X(P(\gamma(\pi))) \geq i_m + p^m,$$

et que $\varphi(i-1) < i_m/p^m$, c'est que $n_{\gamma,i}$ n'est pas nul, ce qui prouve le lemme.

Lemme 3. *Soit i un entier tel que $\varphi(i-1) < i_m/p^m$. L'isomorphisme entre Γ/Γ_i et $\mathrm{Gal}(X_{m,i}/Y_{m,i})$ est un isomorphisme de groupes filtrés, $\mathrm{Gal}(X_{m,i}/Y_{m,i})$ étant muni de la filtration de ramification, et Γ/Γ_i étant filtré par les sous-groupes Γ_j/Γ_i.*

Démonstration. Soit τ un élément de $S(i)$ n'appartenant pas à $S'(i)$. On a :

$$i_{X_{m,i}}(\tau) = \frac{1}{[X : X_{m,i}]}(\sum_{\iota} i_X(\iota)),$$

la somme portant sur les différents plongements de X dans X_{s} qui agissent comme τ sur $X_{m,i}$. Soit γ un élément de Γ tel que $v_X(\tau(\pi) - \gamma(\pi)) \geq i+1$. Comme $\gamma \notin \Gamma_i$, on a $i_X(\gamma) = i_X(\iota) < i$. Comme tout élément τ' de $S'(i)$ est tel que $i_X(\tau') \geq i$, on voit facilement que tous les termes de la somme ci-dessus sont égaux à $i_X(\gamma)$ ce qui prouve le lemme.

3.2. Soit n un entier ≥ 1. Appliquons le lemme 2 avec $i = i_{n+1} + 1$ et m suffisamment grand ce qui est possible car $\lim_{m\to\infty} i_m/p^m = \infty$. Le lemme 3 dit que les nombres de ramification de l'extension $X_{m,i}/Y_{m,i}$ sont $i_0, i_1, ..., i_{n+1}$. On a donc $b_{n+1} \geq pb_n$ ([13]), ce qui prouve la première partie de la proposition.

On a : $i_n - i_{n-1} = (b_n - b_{n-1})p^n$, donc $i_n/p^n \geq i_{n-1}/p^n + (p-1)b_{n-1} > b_{n-1}$. On peut appliquer le lemme 2 avec $i = i_{n-1}+1$ et $m = n$. On a alors : $X = X_{n,i}$ et $Y_{n,i} = Z'_n = Z_n$, l'extension X/Z_n est cyclique de degré p^n et le générateur de son groupe de Galois σ_n vérifie $i_X(\sigma \circ \sigma_n^{-1}) \geq i_{n-1} + 1$ et donc convient. La proposition est prouvée.

3.3. Prouvons le théorème. Soit $\widehat{X_{\mathrm{r}}}$ le complété de la clôture radicielle X_{r} de X. L'action de Γ sur X se prolonge de manière unique à X_{r} et par continuité à $\widehat{X_{\mathrm{r}}}$. Soit $N_n : X \to \hat{X}_{\mathrm{r}}$ comme dans la proposition 1. Posons $\pi_n = N_n(\pi)$ et $K_n = k((\pi_n))$. Montrons que $K_n \subset K_{n+1}$, que $L = \cup K_n$ est une extension de $K = K_0$ de groupe de Galois $\mathbb{Z}_p$, totalement ramifiée, K_n étant l'unique extension de degré p^n de K contenue dans L, et que $X_K(L)$ muni de l'action de Γ s'identifie à X.

On a $\pi_n = \prod_{i=0}^{p-1} N_{n+1}(\sigma^{ip^n}(\pi))$, et pour prouver que $K_n \subset K_{n+1}$, il suffit de prouver que, pour tout x de X et tout m, $N_m(x) \in K_m$. Faisons le pour $m = 0$. Par un raisonnement par approximations successives immédiat, cela découle du lemme suivant :

Lemme 4. *Soient x_i une famille finie d'éléments de O_X. On a :*

$$v_X(\sum N_0(x_i)) \in \mathbb{N} \cup \infty.$$

Démonstration. Il n'y a rien à prouver si $\sum N_0(x_i) = 0$. Supposons $\sum N_0(x_i) \neq 0$. Soit $v = v_X(\sum N_0(x_i))$. Soit n tel que $(i_{n-1} + 1)/p^n > v$.

Posons $X_n = X^{\sigma_n}$. Pour $x \in X$, il découle de la proposition 4 que l'on a :

$$v_X(N_0(x) - (N_{X/X_n}(x))^{\frac{1}{p^n}}) \geq \frac{i_{n-1}+1}{p^n} > v.$$

Il en résulte que :

$$v_X(\sum N_0(x_i)) = \frac{1}{p^n}\big(v_X(\sum N_{X/X_n}(x_i))\big).$$

Comme $\sum N_{X/X_n}(x_i) \in X_n$, on voit que l'on a bien $v_X(\sum N_0(x_i)) \in \mathbb{N}$, ce qui prouve le lemme.

3.4. On a donc $K_n \subset K_{n+1}$ pour tout n. L'extension K_n/K_0 est totalement ramifiée d'indice de ramification p^n. Elle est donc de degré p^n. L'automorphisme σ laisse stable K_n en laissant fixe les éléments de K_0.

Pour prouver que K_n/K_0 est cyclique de degré p^n de groupe de Galois engendré par la restriction de σ à K_n, il suffit de prouver que $\sigma^{p^{n-1}}$ n'agit pas trivialement sur K_n. Faisons le pour $n = 1$. On a, pour tout $x \in X$: $v_X(N_1(x)-x) \geq v_X(x)+i_1/p$ *cf* 2.3 . Comme $i_1/p > i_0$, on voit que l'on a : $v_X(N_1(\sigma(\pi)) - N_1(\pi)) = i_0 + 1$, ce qui prouve que $N_1(\sigma(\pi)) = \sigma(N_1(\pi)) \neq N_1(\pi)$ et σ n'agit pas trivialement sur K_1.

Pour tout n et tout $x \in X$, on a : $v(x - N_n(x)^{p^n}) \geq v(x) + i_n/p$ *cf* 2.3. Il en résulte que $x = \lim_{n\to\infty} N_n(x)^{p^n}$, ce qui prouve que $X_K(L) = X$ et achève de prouver le théorème dans le cas $e(\Gamma) = \infty$.

4. Démonstration du théorème 1 : cas $e(\Gamma) < \infty$.

Soit (X, Γ) un objet ΓAUT (*cf* 2.7). Notons σ un générateur de Γ. On pose : $e = e(\Gamma)$.

4.1. Le groupe U_Γ^+. Soit $\widehat{X^*}$ le complété p-adique du groupe multiplicatif de X (*cf* 1). On pose :

$$U_\Gamma^+ = U_X^+/(\sigma - 1)(\widehat{X^*}).$$

On munit U_Γ^+ de la topologie quotient pour lequel il est séparé et complet grâce au lemme suivant.

Lemme 5. *On a $X^\sigma = k$ et $(\widehat{X^*})^\sigma = \{1\}$. Le groupe $(\sigma - 1)(\widehat{X^*})$ est fermé dans U_X^+.*

Démonstration. Soit $x \in X$ fixe par σ. On sait que si $v = v_X(x)$, on a : $v_X(\sigma(x) - x) \leq v + i_X(\sigma^v)$ (cor. th. 1 de [17]). Comme σ est d'ordre infini, on a $i_X(\sigma^v) < \infty$ sauf si $v = 0$. Comme $k \subset X^\sigma$, $X^\sigma = k$ en résulte immédiatement.

Soit $x \in \widehat{X^*}$ fixe par σ et montrons que $x = 1$. On se ramène immédiatement au cas où $v_X(x) \in \mathbb{Z}$ auquel cas x est l'image d'un élément $x' \in X$.

On a : $(\sigma - 1)(x') \in k^*$. Comme σ est sauvagement ramifié, cela entraîne $(\sigma - 1)(x') = 1$, donc $x' = 1$ et $x = 1$.

Reste à prouver que $(\sigma - 1)(\widehat{X^*})$ est fermé dans U_X^+. Montrons tout d'abord que $(\sigma - 1)(U_X^+)$ l'est. Pour ceci, il suffit de prouver que si u_n est une suite d'éléments de U_X^+ telle que $(\sigma - 1)(u_n)$ tend vers 1, u_n tend vers 1. Pour une telle suite, posons $x_n = u_n - 1$. Posons $v_n = v_X(x_n)$. On a : $v_X(\sigma(x_n) - x_n) \leq v_n + i_X(\sigma^{v_n})$ ([17] *loc. cit.*).Comme $v_X(\sigma(x_n) - x_n)$ tend vers l'infini, il en résulte que v_n aussi, ce qui prouve que $(\sigma - 1)(U_X^+)$ est fermé. Comme si π est une uniformisante, et si $u = (\sigma - 1)(\pi)$, on a : $(\sigma - 1)(\widehat{X^*}) = u^{\mathbb{Z}_p} \times (\sigma - 1)(U_X^+)$, il en résulte que $(\sigma - 1)(\widehat{X^*})$ est fermé, ce qui achève de prouver le lemme.

4.1.1. La proposition suivante éclaire la démonstration du théorème 1.

Proposition 5. *Soit L/K de* ΓEXT *(cf 2.7). Notons σ un générateur de* Γ, *$X = X_K(L)$ et soit $\widehat{X^*}$ le complété p-adique du groupe multiplicatif de X. Alors, l'homomorphisme $x \mapsto (\sigma - 1)(x)$ induit un isomorphisme de $\widehat{X^*}$ sur le noyau de l'homomorphisme $x = (\alpha_n) \mapsto \alpha_0$ de U_X^+ dans K_0^*.*

Démonstration. L'injectivité résulte du lemme précédent. Avant de prouver la surjectivité, établissons le lemme.

Lemme 6. *Soit Y'/Y une extension finie galoisienne de corps locaux de groupe de Galois G. Alors, on a $(\widehat{Y'^*})^G = \widehat{Y^*}$ et $H^1(G, \widehat{Y'^*}) = \{0\}$.*

Démonstration. On a le diagramme commutatif :

$$\begin{array}{ccccccccc}
U_Y & \longrightarrow & Y^* & \longrightarrow & \mathbb{Z} & \longrightarrow & H^1(G, U_{Y'}) & \longrightarrow & 0 \\
\downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\
U_Y^+ & \longrightarrow & \widehat{Y'^*}^G & \longrightarrow & \mathbb{Z}_p & \longrightarrow & H^1(G, U_{Y'}^+) & \longrightarrow & H^1(G, \widehat{Y'^*})
\end{array}$$

Soit k' le corps résiduel de Y'. Comme $U_{Y'} = k'^* \times U_{Y'}^+$, l'homomorphisme $H^1(G, U_{Y'}) \to H^1(G, U_{Y'}^+)$ est surjectif. Comme $H^1(G, \mathbb{Z}_p) = \{0\}$, l'homomorphisme $H^1(G, U_{Y'}^+) \to H^1(G, \widehat{Y'^*})$ est surjectif. La nullité de $H^1(G, \widehat{Y'^*})$ en découle. Pour prouver que $(\widehat{Y'^*})^G = \widehat{Y^*}$, il suffit de prouver que $v_{Y'}((\widehat{Y'^*})^G) = e_{Y'/Y}\mathbb{Z}_p$, ce que l'on prouve facilement à l'aide du diagramme ci-dessus en remarquant que $H^1(G, k'^*)$ est fini d'ordre premier à p. Ceci achève de prouver le lemme.

4.1.2. Prouvons la surjectivité dans la proposition. Soit donc $x \in U_X^+$, $x = (\alpha_n)$ tel que $\alpha_0 = 1$. Puisque $H^1(K_n/K_0, \widehat{K_n^*}) = \{0\}$, il existe $t_n \in \widehat{K_n^*}$ tel que $\alpha_n = (\sigma - 1)(t_n)$. Pour $m \geq n$, $N_{K_{m+1}/K_m}(t_{m+1})t_m^{-1}$ est une unité fixe par σ, donc est un élément de $U^+_{K_0}$. Par suite, $N_{K_{m+1}/K_n}(t_{m+1}) N_{K_m/K_n}(t_m)^{-1}$ appartient à $(U^+(K_n))^{p^{m-n}}$ et la suite des $N_{K_m/K_n}(t_m)$ converge dans $\widehat{K_n^*}$ vers un élément β_n vérifiant $\alpha_n = (\sigma - 1)(\beta_n)$. On a : $N_{K_{n+1}/K_n}(\beta_{n+1}) = \beta_n$ et la suite des β_n définit un élément de $\widehat{X^*}$. Ceci achève de prouver la proposition.

4.1.3. Puisque pour une extension finie d'un corps local à corps résiduel algébriquement clos la norme est surjective, on a :

Corollaire 2. *Supposons le corps résiduel k algébriquement clos. Alors l'homomorphisme $x = (\alpha_n) \mapsto \alpha_0$ induit un isomorphisme*

$$X^*/(\sigma - 1)(\widehat{X^*}) \simeq K_0^*.$$

4.1.4. Posons $\Gamma_n = p^n\Gamma$. Notons N_n le morphisme naturel $U^+_X \to U^+_{\Gamma_n}$. Soit $n \leq n'$. Soit $v \in U^+_{\Gamma_n}$. Pour $u \in U^+_X$, tel que $N_n(u) = v$, l'image v' de $(\sum_{i=0}^{p^{n'-n}-1} \sigma^{ip^n})(u)$ dans $U^+_{\Gamma_{n'}}$ ne dépend que de v et pas du choix de u. Si à v on associe v', on définit un morphisme $i_{n,n'}$ de $U^+_{\Gamma_n}$ dans $U^+_{\Gamma_{n'}}$.

D'autre part, l'identité de U^+_X définit par passage au quotient un morphisme de $U^+_{\Gamma_{n'}}$ dans $U^+_{\Gamma_n}$; on le note $N_{n',n}$. Le groupe Γ agit de façon naturelle sur les $U^+_{\Gamma_n}$ en commutant aux morphismes $i_{n,n'}$ et $N_{n',n}$.

Lemme 7. *i) Les morphismes $i_{n,n'}$ sont injectifs. On a :*

$$(U^+_{\Gamma_{n'}})^{\Gamma_n} = i_{n,n'}(U^+_{\Gamma_n}).$$

ii) Si à $u \in U^+_X$ on associe la suite des $N_n(u)$, on définit un isomorphisme de U^+_X sur la limite projective des $U^+_{\Gamma_n}$, les morphismes de transition étant les $N_{n',n}$; l'isomorphisme réciproque associe à (v_n) la limite des u_n, si u_n est un élément quelconque de U^+_X tel que $N_n(u_n) = v_n$.

Démonstration. Faisons la démonstration que $i_{0,1}$ est injectif et identifie U^+_Γ avec $(U^+_{\Gamma_1})^\Gamma$. Soit $v \in U^+_\Gamma$ tel que $i_{0,1}(v) = 1$. Soit $u \in U^+_X$ tel que $N_0(u) = v$. Il existe $z \in \widehat{X^*}$ tel que $(\sum_{i=0}^{p-1} \sigma^i)(u) = (\sigma^p - 1)(z)$. On a $(\sigma^p - 1)(u) = (\sigma^p - 1)(\sigma - 1)(z)$. Comme $(\sigma^p - 1)$ est injective, on en déduit que : $u = (\sigma - 1)(z)$ et $v = 1$. Soit $v \in (U^+_{\Gamma_1})^\Gamma$. Soit $u \in U^+_X$ tel que $N_1(u) = v$. Il existe $z \in \widehat{X^*}$ tel que $(\sigma - 1)(u) = (\sigma^p - 1)(z)$, d'où : $u = (\sum_{i=0}^{p-1} \sigma^i)(z)$, si v' est l'image de z dans U^+_Γ, on a bien $i_{0,1}(v') = v$.

Prouvons le ii). Soit u_n et v_n comme dans l'énoncé du lemme. Pour tout n, il existe $z_n \in \widehat{X^*}$ tel que $u_{n+1} = u_n \cdot (\sigma^{p^n} - 1)(z_n)$. Il en résulte que $v_X(u_{n+1} - u_n) \geq i_n$ et la suite des u_n converge vers $u \in U^+_X$. On a :

$$N_n(u) = \lim_{m\to\infty} N_n(u_m) = \lim_{m\to\infty} N_{m,n}(N_m(u_m)) = v_n.$$

Le lemme en résulte immédiatement.

Remarque. Soit L/K de ΓEXT (*cf* 2.7). Posons $X = X_K(L)$. On vérifie sans peine que l'on a : $N_n(U_X^+) = \big(N_{n'}(U_X^+)\big)^{\Gamma_n}$, et les $i_{n,n'}$ correspondent aux inclusions et les $N_{n',n}$ aux normes.

4.1.5. Soient φ et ψ les fonctions de Herbrand de Γ.

Soit π une uniformisante de X. Pour tout entier $i \geq 1$, notons U_X^i le groupe des unités u de X vérifiant $v_X(u-1) \geq i$. Posons $U_{\Gamma,i} = N_0(U_X^i)$. On note $N_{0,i}$ le morphisme surjectif $U_X^i/U_X^{i+1} \to U_{\Gamma,i}/U_{\Gamma,i+1}$ induit par N_0.

Lemme 8. *Soit i un entier ≥ 1. Si $\varphi(i)$ n'est pas entier : $U_{\Gamma,i} = U_{\Gamma,i+1}$. Si $\varphi(i)$ est entier et $i \neq i_n$ pour tout $n \in \mathbb{N}$, $N_{0,i}$ est un isomorphisme. Pour tout entier $n \geq 0$, le noyau de N_{0,i_n} est le groupe cyclique d'ordre p engendré par l'image de $(\sigma^{p^n} - 1)(\pi)$ dans $U_X^{i_n}/U_X^{i_n+1}$.*

Démonstration.

Lemme 9. *(cf lemme 1 de* [15]*). Pour tout entier $v \geq 1$, posons $\Theta(v) = v + i_X(\sigma^v)$. Soit i un entier ≥ 1. Pour que $\varphi(i)$ soit entier, il faut et il suffit que i ne soit pas dans l'image de Θ.*

Démonstration. Soit i un entier ≥ 1.

Supposons que $\varphi(i)$ n'est pas entier. On a $i \geq i_0$ et si $i_n \leq i \leq i_{n+1}$, $i - i_n$ n'est pas divisible par p^{n+1}. Soit p^a, avec $0 \leq a \leq n$, la plus grande puissance de p divisant $i - i_n$. Puisque $i_n \equiv i_a$ mod. p^{a+1} ([17]), la plus grande puissance de p divisant $i - i_a$ est p^a, d'où : $i = \Theta(i - i_a)$ et i est bien dans l'image de Θ.

Supposons $i = \Theta(v)$. Soit a la valuation de v. Comme pour tout $n \in \mathbb{N}$, on a $i_n \equiv i_{n+1}$ mod. p^{n+1} ([17]), on voit facilement que si l est un entier $\geq i_a$ qui est l'image par ψ d'un entier, on a $l - i_a \equiv 0$ mod. p^{a+1}. Ce n'est pas le cas pour i, ce qui achève de prouver le lemme 9.

4.1.6. Prouvons le lemme 8. On a la suite exacte :

$$1 \to (U_X^i \cap (\sigma-1)(\widehat{X^*}))/(U_X^{i+1} \cap (\sigma-1)(\widehat{X^*})) \to U_X^i/U_X^{i+1} \to U_{\Gamma,i}/U_{\Gamma,i+1} \to 1.$$

Supposons $\varphi(i)$ non entier *i.e.* i est dans l'image de Θ. Soit v l'unique entier tel que $i = \Theta(v)$ ([17] lemme 3). Soit x_v un élément de valuation v et spécial au sens de S. Sen ([17]) *i.e.* $v_X(\sigma(x_v) - x_v) = \Theta(v) = i$. Pour tout $\alpha \in k$, posons $u_{v,\alpha} = 1 + \alpha x_v$. On a :

$$(\sigma-1)(u_{v,\alpha}) = 1 + \sum_{l=0}^{\infty} \alpha^{l+1} x_v^l (\sigma(x_v) - x_v),$$

donc :

$$(\sigma-1)(u_{v,\alpha}) \equiv 1 + \alpha(\sigma(x_v) - x_v) \mod. \pi^{i+1}.$$

Il en résulte que $(U_X^i \cap (\sigma-1)(\widehat{X^*}))/(U_X^{i+1} \cap (\sigma-1)(\widehat{X^*})) \simeq U_X^i/U_X^{i+1}$ et $U_{\Gamma,i}/U_{\Gamma,i+1} = \{1\}$, ce qui prouve le lemme si $\varphi(i)$ n'est pas entier.

Pour prouver le lemme lorsque $\varphi(i)$ est entier, il suffit de prouver que pour tout $x \in \widehat{X^*}$, $x \neq 1$, la valuation de $(\sigma-1)(x)-1$ soit appartient à l'image de Θ, soit est un entier i_n et $(\sigma-1)(x) \equiv \left((\sigma^{p^n}-1)(\pi)\right)^a \bmod.\pi^{i_n+1}$ pour un entier a non divisible par p. Soit $x \in \widehat{X^*}$, $x \neq 1$. On a : $v_X(x) = p^n a$ pour un entier $n \geq 0$ et a une unité de $\mathbb{Z}_p$. On peut écrire :

$$x = \Big(\big(\sum_{l=0}^{p^n-1} \sigma^l\big)(\pi)\Big)^a \prod (1+x_v),$$

où, dans le produit, v décrit un ensemble éventuellement infini d'entiers > 0, x_v étant un élément spécial de valuation v. On a :

$$(\sigma-1)(x) = \left((\sigma^{p^n}-1)(\pi)\right)^a \prod (\sigma-1)(1+x_v),$$

avec $v_X((\sigma-1)(1+x_v)-1) = \Theta(v)$. Le lemme résulte de ce que les $\Theta(v)$ sont distincts ([17] lemme 3), et distincts des i_n, puisque les $\Theta(v)$ décrivent les entiers i tels que $\varphi(i)$ ne soit pas entier et que $\varphi(i_n) = b_n$ est entier. Ceci achève de prouver le lemme.

4.1.7. Pour tout entier $j > 0$, on pose : $U_\Gamma^j = U_{\Gamma,\psi(j)}$. Soit n un entier ≥ 0. Notons α_n l'élément de k tel que $(\sigma^{p^n}-1)(\pi) \equiv 1 + \alpha_n \pi^{i_n} mod.\pi^{i_n+1}$ et $Q_n(X)$ le polynôme $X^p - \alpha_n^{p-1}X$. Le lemme précédent montre que l'on a des isomorphismes suivants :

$$U_\Gamma^j/U_\Gamma^{j+1} \simeq k, \text{ si } \forall n,\ j \neq b_n \ ;\ U_\Gamma^j/U_\Gamma^{j+1} \simeq Q_n(k), \text{ si } j = b_n.$$

On les note θ_j (ils dépendent du choix de l'uniformisante π). Si j n'est pas l'un des b_n, $\theta_j(\alpha)$ est l'image par $N_{0,\psi(j)}$ de $1+\alpha\pi^{\psi(j)}$ (pour la définition de $N_{0,j}$ voir le 4.1.5). Si $j = b_n$, et si $\alpha = Q_n(\beta)$, $\theta_j(\alpha)$ est l'image de $1+\beta\pi^{i_n}$ par N_{0,i_n}.

Remarque. Si (X,Γ) provient de L/K, la filtration U_Γ^j sur $U_\Gamma^+ \simeq N_0(U_X^+)$ est la filtration induite par la filtration naturelle de $U_{K_0}^+$ (voir chap. 5 6 de [19]).

Lemme 10. *i) On suppose que $e < \infty$. On suppose de plus que la suite des i_n vérifie les conditions suivantes : p ne divise pas i_0, $i_{n+1} = i_n + p^{n+1}e$, et $e/(p-1) < i_0 < pe/(p-1)$. Notons λ la fonction de $\mathbb{N}$ dans lui-même qui à j associe* $\min(pj, j+e)$. *Alors, pour tout $j > 0$, on a : $(U_\Gamma^j)^p \subset U_\Gamma^{\lambda(j)}$.*

ii) Soit $\bar{u} \to \bar{u}^p$ l'homomorphisme de $U_\Gamma^j/U_\Gamma^{j+1}$ dans $U_\Gamma^{\lambda(j)}/U_\Gamma^{\lambda(j)+1}$ induit par l'élévation à la puissance p. Il existe un polynôme $P_j \in k[X]$, additif et dont le degré séparable (cf. chap. 5 5 de [19]*) est* 1 *si $j \neq e/(p-1)$ et p si $j = e/(p-1)$, qui donne $\bar{u} \to \bar{u}^p$ avec les identifications du numéro précédent, i.e. tel que $P_j(\theta_j(\bar{u})) = \theta_{\lambda(j)}(\bar{u}^p)$.*

4.1.8. *Démonstration.* Montrons le i). Soit j un entier > 0. Posons : $i = \psi(j)$ et $i' = \psi(\lambda(j))$. Soit $u \in U_X^i$.

Si $i < i_0/p$, on a $i' = j' = pi = pj$ et, comme $u^p \in U_X^{pi}$, le i) est clair dans ce cas.

Supposons $i > i_0/p$. Il est facile de voir que, pour l entier > 0 , on a $(\sigma - 1)(U_X^l) \subset U_X^{l+i_0}$. L'homomorphisme : $x \mapsto (\sigma - 1)(x)$ induit donc un homomorphisme de U_X^l/U_X^{l+1} dans $U_X^{l+i_0}/U_X^{l+i_0+1}$. On vérifie aisément que c'est : $\alpha \mapsto l a_0 \alpha$ avec les identifications usuelles $U_X^m/U_X^{m+1} \simeq k$ qui à α associent l'image de $1 + \alpha\pi^m$. Cela entraîne en particulier que, si l est premier à p, on a $U_X^{l+i_0} \subset U_X^{l+i_0+1}\ (\sigma - 1)(U_X^l)$.

Comme p ne divise pas i_0 et que $pi > i_0$, il en résulte qu'il existe v et w avec :

$$(1) : \begin{cases} u^p &= (\sigma - 1)(v) \times w, \\ v &\in U_X^{pi-i_0}, \\ w &\in U_X^{pi+1} \quad \text{et } v_X(w-1) \equiv i_0 \text{ mod. } p \text{ ou } w = 1. \end{cases}$$

Il suffit, pour montrer le i), de prouver que $w \in U_X^{i'}$. Pour cela, posons :

$$S(X) = \frac{(X-1)^p - (X^p - 1)}{p(X-1)}.$$

On a : $S(X) \in \mathbb{Z}[X]$. De (1), on déduit en appliquant $(\sigma - 1)^{p-1}$:

$$(2) : \begin{cases} \big(p(\sigma-1)^{p-1}\big)(u) &= (\sigma^p - 1)(v) \times \big(pS(\sigma)(\sigma - 1)\big)(v) \\ & \quad \times \big((\sigma-1)^{p-1}\big)(w); \\ \big(p(\sigma-1)^{p-1}\big)(u) &\in U_X^{pi+p(p-1)i_0}; \\ (\sigma^p - 1)(v) &\in U_X^{pi-i_0+i_1}; \\ \big(pS(\sigma)(\sigma-1)\big)(v) &\in U_X^{p^2 i}. \end{cases}$$

Des calculs élémentaires montrent que les conditions sur i_n entraînent :

$$(3) : \begin{cases} i' + (p-1)i_0 = p^2 i < pi - i_0 + i_1 < pi + p(p-1)i_0, \\ \text{si} \quad i_0/p < j < e/(p-1); \\ i' + (p-1)i_0 = p^2 i = pi - i_0 + i_1 < pi + p(p-1)i_0, \\ \text{si} \quad j = e/(p-1); \\ i' + (p-1)i_0 = pi - i_0 + i_1 < p^2 i,\ i' + (p-1)i_0 < pi + p(p-1)i_0, \\ \text{si} \quad j > e/(p-1). \end{cases}$$

De (2) et (3), on déduit $((\sigma - 1)^{p-1})(w) \in U_X^{i'+(p-1)i_0}$. Si $w \neq 1$, on a, *cf* (1) : $v_X(w - 1) \equiv i_0$ mod.p. Par suite : $v_X((\sigma - 1)^{p-1})(w) - 1) = v_X(w-1)+(p-1)i_0$. On voit donc que $i \in U_X^{i'}$. Ceci achève la démonstration du i).

4.1.9. Montrons le ii). Soit j un entier ≥ 1.

Si $j < i_0/p$, on voit immédiatement que $P_i(\alpha) = \alpha^p$ pour $\alpha \in k$.

Supposons désormais $j > i_0/p$. Soit u, v et w comme dans le numéro précédent. Notons β l'élément de k tel que $u \equiv 1 + \beta\pi^i \mod. U_X^{i+1}$. Si $\bar{u}$ est l'image de u dans $U_\Gamma^j/U_\Gamma^{j+1}$, on a donc $\theta_j(\bar{u}) = \beta$ si $j \neq b_n$ pour tout n, et $\theta_j(\bar{u}) = Q_n(\beta)$ si $j = b_n$. Comme $u^p \equiv 1 + \beta^p\pi^{pi} \mod. U_X^{pi+1}$, de (1), on déduit $(\sigma - 1)(v) \equiv 1 + \beta^p\pi^{pi} \mod. U_X^{pi+1}$ et donc $v \equiv 1 - (\alpha_0 i_0)^{-1}\beta^p\pi^{pi-i_0} \mod. U_X^{pi-i_0+1}$, d'où :

$$(4) \quad : \quad (\sigma^p - 1)(v) \equiv 1 + \alpha_0^{-1}\alpha_1\beta^p\pi^{pi-i_0+i_1} \mod. U_X^{pi-i_0+i_1+1}.$$

Comme $S(X) \equiv -1 \mod. (X-1)\mathbb{Z}[X]$, on a :

$$(pS(\sigma)(\sigma - 1))(v) \equiv -p(\sigma - 1)(v) \mod. U_X^{p^2 i+1},$$

et donc :

$$(5) \quad : \quad \big(pS(\sigma)(\sigma - 1)\big)(v) \equiv 1 - \beta^{p^2}\pi^{p^2 i} \mod. U_X^{p^2 i+1}.$$

Soit β' l'élément de k tel que $w \equiv 1 + \beta'\pi^{i'} \mod. U_X^{i'+1}$. Un calcul simple montre que : $(\sigma - 1)^{p-1}(w) \equiv 1 - \alpha_0^{p-1}\beta'\pi^{i'+(p-1)i_0} \mod. U_X^{i'+(p-1)i_0+1}$. On voit alors que :

$$\begin{cases} \beta' = -\alpha_0^{1-p}\beta^{p^2}, & \text{si } i_0/p < j < e/(p-1), \\ \beta' = -\alpha_0^{1-p}\beta^{p^2} + \alpha_1\alpha_0^{-p}\beta^p & \text{si } j = e/(p-1), \\ \beta' = \alpha_1\alpha_0^{-p}\beta^p, & \text{si } j > e/(p-1). \end{cases}$$

On en déduit :

$$\begin{cases} P_j(\alpha) = -\alpha_0^{1-p}\alpha^{p^2}, & \text{si } i_0/p < j < e/(p-1), \\ P_j(\alpha) = -\alpha_0^{1-p}\alpha^{p^2} + \alpha_1\alpha_0^{-p}\alpha^p, & \text{si } j = e/(p-1), \\ P_j(\alpha) = \quad \alpha_1\alpha_0^{-p}\alpha^p, & \text{si } j > e/(p-1) \quad \text{et } j \neq b_n \quad \forall n \in \mathbb{N}, \\ P_{b_n}\big(Q_n(\beta)\big) = \quad Q_{n+1}(\alpha_1\alpha_0^{-p}\beta^p), & \text{si } j = b_n. \end{cases}$$

Ceci démontre le ii) si $j \neq b_n$ pour tout $n \in \mathbb{N}$. Si $j = b_n$, on en déduit que si β est un zéro de Q_n alors $\alpha_0^{-p}\alpha_1\beta^p$ est un zéro de Q_{n+1}, d'où $Q_{n+1}(X) = X^p - (\alpha_0^{-p}\alpha_1\alpha_n^p)^{p-1}X$. On voit alors facilement que $P_{b_n}(\alpha) = \alpha_1^p\alpha_0^{-p^2}\alpha^p$. Ceci achève la démonstration du lemme.

Lemme 11. *On se place dans les hypothèses du lemme précédent. On suppose de plus le corps résiduel algébriquement clos. Alors, on a :* $(U_\Gamma^j)^p = U_\Gamma^{j+e}$ *pour tout entier* $j \geq e/(p-1)$ *et pour* $j > e/(p-1)$ *l'élévation à la puissance* p *dans* U_Γ^j *est injective. Le sous-groupe de torsion de* U_Γ^+ *est un groupe fini cyclique d'ordre une puissance de* p. *Il est non trivial si* $p-1$ *divise* e. *Si* $\epsilon \in U_\Gamma^+$ *est une racine primitive* p^n*-ième de* 1, *on a* $\epsilon \in U_\Gamma^{\frac{e}{(p-1)p^n}}$ *et* $\epsilon \notin U_\Gamma^{\frac{e}{(p-1)p^n}+1}$.

Démonstration. On procède comme au 1.7. de [18].

4.2. Le groupe $\mathcal{U}^+$ et sa torsion.

4.2.1. Soit X_{s} une clôture séparable de X. On note G le groupe des automorphismes de X_{s} qui induisent sur X un élément de Γ et on note H le groupe de Galois de X_{s}/X. On note $\eta : G \to \Gamma$ l'homomorphisme induit par la restriction à X. Avec le lemme de Krasner, on voit facilement que X_{s} est la réunion de ses sous-extensions finies galoisiennes X' de X qui sont telles que tout élement de Γ se prolonge à X'. Si, pour une telle extension X', on note $G_{X'}$ le groupe des automorphismes de X' qui induisent sur X un élément de Γ, le groupe G s'identifie à la limite projective des groupes $G_{X'}$. On munit chaque groupe $G_{X'}$ de la topologie définie par sa filtration de ramification et G de la topologie limite projective. On vérifie sans peine que les $G_{X'}$ sont des groupes topologiques profinis, et il en est de même de G. Le groupe G agit de façon continue sur X_{s}.

Soit G' un sous-groupe ouvert de G. On note $H' = H \cap G'$, $X' = (X_{\mathrm{s}})^{H'}$, $\Gamma' = \eta(G')$ qui s'identifie donc à un groupe d'automorphismes de X', et n' l'entier tel que $\Gamma' = p^{n'}\Gamma$. On note σ' l'élément de G' tel que $\eta(\sigma') = \sigma^{p^{n'}}$. Comme Γ' est un pro-p-groupe, on voit facilement que σ' est un automorphisme sauvagement ramifié de X'. On pose :

$$U_{G'}^+ = U_{X'}^+/(\sigma' - 1)(\widehat{X'^*}).$$

On note $N_{G'}$ le morphisme naturel de $U_{X'}^+$ dans $U_{G'}^+$.

Pour $G' \subset G''$, on a : $n' \geq n''$. Soit v'' un élément de $U_{G''}^+$. Pour $u'' \in U_{X''}^+$ avec $v'' = N_{G''}(u'')$, l'image de $(\sum_{i=0}^{p^{n'-n''}-1} \sigma^{ip^{n''}})(u'')$ dans $U_{G'}^+$ ne dépend pas du choix de u''. On définit ainsi un homomorphisme $i_{G'',G'}$ de $U_{G''}^+$ dans $U_{G'}^+$. On voit sans peine que le groupe G agit sur le système inductif des $U_{G'}^+$. De plus, la norme de X' à X'' induit un morphisme de $U_{G'}^+$ dans $U_{G''}^+$; on le note $N_{G',G''}$.

Lemme 12. *Les homomorphismes $i_{G'',G'}$ sont injectifs. Si G' est distingué dans G'', $i_{G'',G'}(U_{G''}^+)$ s'identifie à $(U_{G'}^+)^{G''/G'}$.*

Démonstration. Montrons l'injectivité de $i_{G,G'}$. Soit $v \in U_G^+$, tel que $i_{G,G'}(v) = 1$. Soit $u \in U_X^+$ tel que $N_G(u) = v$; $i_{G,G'}(v) = 1$ se traduit par l'existence de $x' \in \widehat{X'^*}$ tel que :

$$(\sum_{i=0}^{p^{n'}-1} \sigma^i)(u) = (\sigma' - 1)(x').$$

Pour $\tau \in H$, comme $\tau(u) = u$, on voit facilement que $(\sigma'-1)(\tau-1)(x') = 1$. On a donc $(\tau - 1)(x') = 1$ puisque $\sigma' - 1$ est injectif sur $\widehat{X'^*}$ (*cf* lemme 5), d'où : $x' \in \widehat{X^*}$. On a alors : $(\sigma' - 1)(x') = (\sigma^{p^{n'}} - 1)(x')$, d'où :

$$(\sigma^{p^{n'}} - 1)(u) = (\sigma^{p^{n'}} - 1)(\sigma - 1)(x').$$

Il en résulte que $u = (\sigma - 1)(x')$, et on a bien : $v = 1$.

Prouvons que si G' est distingué dans G, on a : $(U^+_{G'})^G = U^+_G$. Soit $v' \in U^+_{G'}$ fixe par G et $u' \in U^+_{X'}$ avec $N_{G'}(u') = v'$. Par dévissage, on se ramène avec le lemme 7 au cas où $n' = 1$. Comme v' est fixe par G, pour tout $\tau \in \mathrm{Gal}(X'/X)$ il existe $x'_\tau \in \widehat{X'^*}$ tel que $(\tau - 1)(u') = (\sigma' - 1)(x'_\tau)$. Les x'_τ définissent un 1-cocycle de $\mathrm{Gal}(X'/X)$ à valeurs dans $\widehat{X'^*}$. Comme $H^1(\mathrm{Gal}(X'/X), \widehat{X'^*}) = \{0\}$ (lemme 6), il existe $x' \in \widehat{X'^*}$ tel que $x_\tau = (\tau - 1)(x')$. On a alors : $(\tau-1)(u') = (\tau-1)(\sigma'-1)(x')$ pour tout $\tau \in \mathrm{Gal}(X'/X)$. On a donc $u' = u \times (\sigma' - 1)(x')$ pour $u \in U^+_X$, ce qui prouve que $v' \in i_{G,G'}(U^+_G)$, et achève de prouver le lemme.

4.2.2. On note $\mathcal{U}^+$ la limite inductive des $U^+_{G'}$, le morphismes de transition étant les $i_{G'',G'}$. La suite du 4.2 est consacrée à prouver le lemme :

Lemme 13. *Le groupe de torsion* $\mathrm{T}(\mathcal{U}^+)$ *de* $\mathcal{U}^+$ *est isomorphe à* $\mathbb{Q}_p/\mathbb{Z}_p$. *Pour tout sous-groupe ouvert* G' *de* G, *le groupe de torsion* $\mathrm{T}(U^+_{G'})$ *est fini et donc le caractère* $\chi : G \to {\mathbb{Z}_p}^*$ *donnant l'action de* G *sur* $\mathrm{T}(\mathcal{U}^+)$ *a une image ouverte.*

Remarque. Si (X, Γ) provient de L/K de ΓAUT, le groupe $\mathcal{U}^+$ est isomorphe au groupe $U^+_{K_s}$.

Démonstration du lemme.

Avec le lemme 11, le fait que les $\mathrm{T}(U^+_{G'})$ soient finis et cycliques résulte du cas $s = 1/p$ du lemme suivant :

Lemme 14. *Soit* s *un réel avec* $1/p \leq s < 1$. *Alors les sous-groupes ouverts* G' *de* G *tels que la suite des* $i'_n = i_{X'}(\sigma'^{p^n})$ *vérifie les conditions du lemme 10 avec de plus* $spe/(p-1) < i_0 < pe/(p-1)$ *forment un système fondamental de voisinage de* 1 *dans* G.

Démonstration. Prouvons que G possède un sous-groupe ouvert G' vérifiant les conditions du lemme. Pour G' sous-groupe ouvert de G, on a, en posant $e' = e(\Gamma')$: $\lim_{n\to\infty} i'_n/p^n = pe'/(p-1)$, et $i'_{n+1} = i'_n + p^{n+1}e'$ pour n grand. Il en résulte que, quitte à remplacer G' par le sous-groupe des automorphismes de X_s qui induisent sur X' un élément de $p^n\Gamma'$ pour n grand, on peut satisfaire aux conditions $i'_{n+1} = i'_n + p^{n+1}e'$ pour tout n et $spe'/(p-1) < i'_0 \leq pe'/(p-1)$. Il reste à voir que l'on peut satisfaire la condition : p ne divise pas i'_0. Si X'/X est une extension cyclique et ramifiée de degré p, son nombre de ramification est premier à p ([19] ex. 3 chap. 4 2). Le lemme suivant prouve que pour n grand, le sous-groupe G' de G formé des automorphismes de X_s qui induisent sur X' un automorphisme de $p^n\Gamma'$ convient.

Lemme 15. *Soit* (X,Γ) *de* ΓAUT. *Soit* X' *une extension ramifiée et cyclique de degré* p *de* X *de nombre de ramification* $b < i_0$. *Alors* σ *se prolonge de manière unique en un automorphisme sauvagement ramifié* σ' *de* X' *dont la suite* i'_n *des nombres de ramification vérifie* $i'_n = pi_n - (p-1)b$. *Le groupe des automorphismes de* X' *qui prolongent les éléments de* Γ *est le produit direct du groupe* Γ' *engendré par* σ' *et du groupe de Galois* $\mathrm{Gal}(X'/X)$.

Démonstration. L'extension X'/X est le corps de décomposition d'un polynôme d'Artin Schreier $X^p - X = t$ avec $v_X(t) = -b$ ([19] ex. 5 chap. 4 2). Comme $b < i_0$, on a $v_X(\sigma(t) - t) > 0$, donc $X^p - X = \sigma(t) - t$ a ses racines dans X. Il en résulte que σ se prolonge à X'. On a $i_X(\sigma) = 1/p(\sum i_{X'}(\tau))$, la somme portant sur les différents prolongements de σ à X'. Il en résulte que σ a un unique prolongement σ' à X' vérifiant $i_{X'}(\sigma') \geq i_X(\sigma)$ et que les autres prolongements τ vérifient $i_{X'}(\tau) = b$. Le lemme en résulte.

4.2.3. Soit (X,Γ) et X' comme au lemme précédent. On note G' le groupe des automorphismes de X_s dont la restriction à X' appartient à Γ' et on note $\underline{i}$ l'injection $i_{G,G'}$ (qui est induite par l'inclusion de X dans X'). Soit π une uniformisante de X et π' une uniformisante de X' vérifiant $v_{X'}(\pi'^p/\pi - 1) > p$. Le choix de ces uniformisantes permet d'identifier les quotients $U^j_\Gamma/U^{j+1}_\Gamma$ et $U^j_{\Gamma'}/U^{j+1}_{\Gamma'}$ avec des sous-groupes du corps résiduel k (*cf* 4.1.7). On note α'_0 l'élément de k tel que $(\sigma' - 1)(\pi') \equiv 1 + \alpha'_0\pi'^{i'_0} \mathrm{mod.}\pi'^{i'_0+1}$.

Lemme 16. *Soient* (X,Γ) *et* X' *comme dans le lemme précédent. On suppose que la suite* i_n *des nombres de ramification de* σ *vérifie la condition du lemme 10 et que* $b < p/(p-1) \times (i_0 - e/(p-1))$. *Alors, pour tout entier* j *vérifiant* $1 \leq j \leq pe/(p-1)$, *on a :* $\underline{i}(U^j_\Gamma) \subset U^{pj}_{\Gamma'}$ *et pour* $j < pe/(p-1)$, $\underline{i}$ *induit une injection* R_j *de* $U^j_\Gamma/U^{j+1}_\Gamma$ *dans* $U^{pj}_{\Gamma'}/U^{pj+1}_{\Gamma'}$. *Avec les identifications du 4.1.7, on a, pour* $\alpha \in k$ *:*

$$\begin{cases} R_j(\alpha) = \alpha, & \text{pour} \quad 1 \leq j < i_0 - (p-1)b/p, \\ R_j(\alpha) = -\alpha'^{1-p}_0\alpha^p & \text{pour} \quad i_0 - (p-1)b/p < j < i_0, \\ R_j(\alpha) = -\alpha'^{1-p}_0\alpha, & \text{pour} \quad j = i_0, \\ R_j(\alpha) = \alpha'^{1-p}_0\alpha_0^{p-1}\alpha & \text{pour} \quad i_0 < j < pe/(p-1). \end{cases}$$

Démonstration. On vérifie avec le lemme 15 que la condition

$$b < p/(p-1) \times (i_0 - e/(p-1))$$

entraîne que la suite i'_n vérifie les conditions du lemme 10 (avec $e' = pe$).

La démonstration est immédiate si $pj < i'_0$, c'est à dire si $j < i_0 - (p-1)b/p$. Supposons désormais $j > i_0 - (p-1)b/p$. Soit $\omega \in U^j_\Gamma$. Si ψ et ψ' sont les fonctions de Herbrand de Γ et Γ' respectivement, posons $i = \psi(j)$

et $i' = \psi(pj)$. Soit $u \in U_X^i$ d'image ω dans U_Γ^+. On voit comme au 4.1.8 qu'il existe $v \in U_{X'}^{pi-i'_0}$ et $w \in U_{X'}^{pi+1}$ avec $v_{X'}(w-1) \equiv i'_0$ mod.p ou $w = 1$ tels que $u = (\sigma' - 1)(v).w$. D'où, en appliquant $(\sigma' - 1)^{p-1}$, et si $S(X) \in \mathbb{Z}$ est comme au 4.1.8 :

$$(1) : \big((\sigma-1)^{p-1}\big)(u) = (\sigma'^p - 1)(v).\big(pS(\sigma')(\sigma'-1)\big)(v).\big((\sigma'-1)^{p-1}\big)(w).$$

On a :

$$(2) : \begin{cases} (\sigma-1)^{p-1}(u) & \in \quad U_{X'}^{pi+p(p-1)i_0}, \\ (\sigma'^p-1)(v) & \in \quad U_{X'}^{pi+p^2e}, \\ \big(pS(\sigma')(\sigma'-1)\big)(v) & \in \quad U_{X'}^{p^2i}. \end{cases}$$

Des calculs élémentaires montrent :

$$(3) : \begin{cases} \text{pour } i_0 - (p-1)b/p < j < i_0 \ : \ i' + (p-1)i'_0 = p^2 i, \\ i' + (p-1)i'_0 < pi + p(p-1)i_0, \ i' + (p-1)i'_0 < \ pi + p^2 e, \\ \text{pour } j = i_0 \ : \ i' + (p-1)i'_0 = pi + p(p-1)i_0 = p^2 i, \\ i' + (p-1)i'_0 < pi + p^2 e, \\ \text{pour } i_0 < j \leq pe/(p-1) \ : \ i' + (p-1)i'_0 = pi + p(p-1)i_0, \\ \ i' + (p-1)i'_0 < p^2 i, \ i' + (p-1)i'_0 < pi + p^2 e. \end{cases}$$

De (1), (2) et (3), on déduit que : $(\sigma' - 1)^{p-1}(w) \in U_{X'}^{i'+(p-1)i'_0}$. Si $w \neq 1$, on a : $v_{X'}(w-1) \equiv i'_0$ mod.p et un raisonnement facile montre alors que :

$$v_{X'}((\sigma-1)^{p-1})(w)) = v_{X'}(w-1) + (p-1)i'_0.$$

On en déduit que $w \in U_{X'}^{j'}$. On a bien : $\underline{i}(\omega) \in U_{\Gamma'}^{pj}$.

Soit $\alpha \in k$. Calculons $R_j(\alpha)$. Pour cela, soient ω, u, v, et w comme ci-dessus, $\bar{\omega}$ l'image de ω dans $U_\Gamma^j/U_\Gamma^{j+1}$ et supposons que $\theta_j(\bar{\omega}) = \alpha$. On a alors : $u \equiv 1 + \beta\pi^i$ mod.U_X^{i+1} avec $\beta = \alpha$ si $j \neq i_0$ et $\beta^p - \alpha_0^{p-1}\beta = \alpha$ si $i = i_0$ (*cf* 4.1.7). Comme $v_{X'}(\pi\pi'^{-p} - 1) > 0$, on en déduit que $u \equiv 1+\beta\pi'^{pi}$ mod.$U_{X'}^{pi+1}$. De (1), on tire alors : $(\sigma'-1)(v) \equiv 1+\beta\pi'^{pi}$ mod.$U_{X'}^{pi+1}$. Par suite, puisque $S(X) + 1 \in (X-1)\mathbb{Z}[X]$:

$$(4) \quad : \quad \big(pS(\sigma')(\sigma'-1)\big)(v) \equiv 1 - \beta^p\pi'^{p^2i} \text{ mod.} U_{X'}^{p^2i+1}.$$

Pour $j \geq i_0$, on a $i \equiv i_0$ mod.p et un calcul simple montre que, comme $u \equiv 1+\beta\pi^j$ mod.U_X^{i+1}, on a $(\sigma-1)^{p-1}(u) \equiv 1-\alpha_0^{p-1}\beta\pi^{i+(p-1)i_0}$ mod.$U_X^{i+(p-1)i_0}$, d'où :

$$(5) \quad : \quad (\sigma-1)^{p-1}(u) \equiv 1 - \alpha_0^{p-1}\beta\pi'^{pi+p(p-1)i_0} \text{ mod.} U_{X'}^{pi+p(p-1)i_0}.$$

L'entier $i' = \psi'(pj)$ n'est pas égal à l'un des i'_n, p ne divisant pas i'_0. On a donc : $w \equiv 1 + R_j(\alpha)\pi'^{i'}$ mod.$U_{X'}^{i'+1}$. Comme $i' \equiv i'_0$ mod.p, on en déduit facilement :

$$(6) \quad : \quad (\sigma-1)^{p-1}(w) \equiv 1 - \alpha_0'^{p-1}R_j(\alpha)\pi'^{i'+(p-1)i'_0} \text{mod.} U_{X'}^{i'+(p-1)i'_0+1}.$$

De (1), (2), (3), (4), (5) et (6), on déduit que :

$$\begin{cases} R_j(\alpha) = -\alpha_0'^{1-p}\alpha^p, & \text{si} \quad i_0 - (p-1)b/p < j < i_0, \\ R_j(\alpha) = -\alpha_0'^{1-p}(\beta^p - \alpha_0^{p-1}\beta) = -\alpha_0'^{1-p}\alpha, & \text{si} \quad j = i_0, \\ R_j(\alpha) = \alpha_0'^{1-p}\alpha_0^{p-1}\alpha, & \text{si} \quad i_0 < j < pe/(p-1). \end{cases}$$

Ceci achève de prouver le lemme.

Lemme 17. *Soient (X,Γ) et b comme au lemme précédent. On suppose de plus le corps résiduel k algébriquement clos et que e est divisible par $p-1$. Soit $t \equiv \alpha\pi^{-b}\mathrm{mod}.\pi^{-b+1} \in X$ et X' l'extension de X engendrée par les racines de l'équation $X^p - X = t$. Soit Γ' comme au lemme 15. Alors $U_{\Gamma'}^+$ contient un élément ω tel que $\omega^p = i_{\Gamma,\Gamma'}(\delta)$ pour $\delta \in U_\Gamma^{\frac{pe}{(p-1)}-b}$ avec $\theta_{pe/(p-1)-b}(\delta)$ polynôme additif bijectif en α qui ne dépend que de X, σ et b.*

Remarque. Ce lemme est inspiré par [25].

Démonstration. Comme k est algébriquement clos et que $p-1$ divise e, U_Γ^+ possède un élément ϵ d'ordre p (*cf* lemme 11). Soit $u \in U_X^+$ tel que $N_\Gamma(u) = \epsilon$. Il existe $z \in U_X^+$ tel que $u^p = (\sigma-1)(z)$. La norme $N_{X'/X}$ est surjective puisque k est algébriquement clos. Soit $z' \in U_{X'}^+$ tel que $N_{X'/X}(z') = z$. On a : $N_{X'/X}(u.(\sigma'-1)(z')) = 1$. Si τ est un générateur de $\mathrm{Gal}(X'/X)$, il existe donc $v \in X'^*$ tel que :

$$(1) \quad u.(\sigma'-1)(z') = (\tau-1)(v).$$

On a $N_{\Gamma'}(u) = i_{\Gamma,\Gamma'}(\epsilon)$, donc, puisque les i'_n vérifient les conditions du lemme 10, $v_{X'}(u.(\sigma'-1)(z')-1) = pe/(p-1) < i'_0$. Comme $b < i_0 < pe/(p-1)$, on voit que l'on peut choisir pour v une unité.

Posons alors : $\omega = N_{\Gamma'}(v)$. On a : $(\tau-1)(\omega) = i_{\Gamma,\Gamma'}(\epsilon)$, donc $\tau(\omega^p) = \omega^p$. Il existe donc $\delta \in U_\Gamma^+$ avec $\omega^p = i_{\Gamma,\Gamma'}(\delta)$. Montrons que l'on peut choisir v tel que δ convienne.

On peut choisir v tel que $v_{X'}(v-1)$ ne soit pas divisible par p. Comme on a vu que $v_{X'}(u.(\sigma'-1)(z')-1) = pe/(p-1)$, on en déduit que $v_{X'}(v-1) = \frac{pe}{(p-1)} - b$. On voit alors que $\omega \in U_{\Gamma'}^{\frac{pe}{(p-1)}-b}$. Cela entraîne grâce au lemme 11 que $\omega^p \in U_{\Gamma'}^{\frac{p^2e}{(p-1)}-pb}$. Comme les R_j, pour $1 \leq j < \frac{pe}{(p-1)} - b$ sont injectifs, on voit que $\delta \in U_\Gamma^{\frac{pe}{(p-1)}-b}$.

Reste à calculer $\theta_{\frac{pe}{(p-1)}-b}(\delta)$. Soit $\gamma_0 = \theta_{e/p-1}(\epsilon)$. Comme $v_{X'}(\frac{\pi'^p}{\pi}-1) > 0$, on a $\gamma_0 = \theta_{pe/p-1}(\underline{i}(\epsilon))$. Comme $N_{\Gamma'}((\tau-1)(\omega)) = \epsilon$, on voit que :

$$(2) \quad : \quad \theta_{pe/(p-1)}((\tau-1)(\omega)) = \gamma_0.$$

Soit x une racine de $X^p - X = t$ dans X'. On a $x^p \equiv \alpha\pi^{-b} \bmod.\pi^{-b+1}$, donc $x \equiv \alpha^{1/p}\pi'^{-b} \bmod.\pi'^{-b+1}$. Prenons comme générateur τ de $\mathrm{Gal}(X'/X)$

l'élément de $\mathrm{Gal}(X'/X)$ tel que : $\tau x = x+1$ On a alors : $\theta_b(N_{\Gamma'}((\tau - 1)(\pi'^{-b})) = \alpha^{-1/p}$, d'où : $\theta_b(N_{\Gamma'}((\tau-1)(\pi'))) = -b^{-1}\alpha^{-1/p}$. On déduit alors de (2) :

$$(3) \quad : \quad \theta_{\frac{pe}{(p-1)}-b}(\omega) = \alpha^{1/p}\gamma_0.$$

Il résulte alors du calcul des P_j au 4.1.9 que :

$$\theta_{\frac{p^2e}{(p-1)}-pb}(\omega^p) = \begin{cases} \gamma_0^p\alpha \text{ si } \frac{pe}{(p-1)} - b < i_0 - \frac{(p-1)b}{p}, \\ \alpha_0'^{\,1-p}\gamma_0^{p^2} \text{si } \frac{pe}{(p-1)} - b > i_0 - \frac{(p-1)b}{p}. \end{cases}$$

Il résulte alors du lemme précédent que :

$$\theta_{\frac{pe}{(p-1)}-b}(\delta) = \begin{cases} \gamma_0^p\alpha, & \text{si} \quad pe/(p-1) - b < i_0 - (p-1)b/p, \\ \gamma_0^p\alpha, & \text{si} \quad i_0 - (p-1)b/p < pe/(p-1) - b < i_0, \\ \gamma_0^{p^2}\alpha^p & \text{si} \quad pe/(p-1) - b = i_0, \\ \alpha_0^{1-p}\gamma_0^{p^2}\alpha^{p^2}, & \text{si} \quad i_0 < pe/(p-1) - b < pe/(p-1). \end{cases}$$

Ceci prouve le lemme.

Lemme 18. *Soit* (X, Γ) *vérifiant les hypothèses du lemme 10 et soit* j *un entier vérifiant* $j > \frac{p}{(p-1)}(\frac{pe}{(p-1)} - i_0)$. *On suppose le corps résiduel* k *algébriquement clos et que* e *est divisible par* $p-1$. *Alors on a :* $U^j_{p\Gamma} \subset (\mathcal{U}^+)^p$.

Démonstration. La condition sur j entraîne : $\frac{p^2e}{(p-1)} - j < \frac{p}{(p-1)}(i_1 - \frac{pe}{(p-1)})$. Le lemme précédent entraîne donc, pour $j \leq j' < p^2e/(p-1)$: $U^{j'}_{p\Gamma} \subset (\mathcal{U}^+)^p\ U^{j'+1}_{p\Gamma}$. Le lemme 10 entraîne que pour j' divisible par p, on a : $U^{j'}_{p\Gamma} \subset (U^+_{p\Gamma})^p\ U^{j'+1}_{p\Gamma}$. Le lemme 11 nous dit que $U^{p^2e/(p-1)}_{p\Gamma} \subset (U^+_{p\Gamma})^p$. Le lemme en résulte.

Lemme 19. *Soit* (X, Γ) *de* ΓAUT. *Alors :*

$$i_{0,1}(U^+_\Gamma) \subset (U^+_{p\Gamma})^p\ U^{i_0}_{p\Gamma}.$$

Démonstration. Soit $\omega \in U^+_\Gamma$. Soit $u \in U^+_X$ tel que $\omega = N_0(u)$. Soit $\omega' = N_1(u)$. On a $i_{0,1}(\omega) = N_1((\sum_{i=0}^{p-1}\sigma^i)(u))$. Comme $v_X((\sum_{i=0}^{p-1}\sigma^i - p)(u) - 1) > i_0$ et que $\psi_{p\Gamma}(i_0) = i_0$, on en déduit que $i_{0,1}(\omega)\omega'^{-p} \in U^{i_0}_{p\Gamma}$. Ceci prouve le lemme.

4.2.4. On suppose le corps résiduel k algébriquemant clos. Montrons que $\mathcal{U}^+$ est p-divisible. Soit s un réel avec $1/p \leq s < 1$. Le lemme 14 nous dit que l'ensemble des sous-groupes ouverts G' de G tels que la suite des i'_n vérifie les conditions du lemme 10 avec de plus $spe'/(p-1) < i'_0 < pe'/(p-1)$ forment un système fondamental de voisinage de 1 dans G. Il en est de même des sous-groupes G' avec de plus e' divisible par $p-1$. Pour $s > \frac{p}{2p-1}$, on a : $i'_0 > \frac{p}{(p-1)}(\frac{pe}{(p-1)} - i'_0)$. Les deux lemmes précédents entraîne alors que $U^+_{\Gamma'} \subset (\mathcal{U}^+)^p$. Il en résulte que $\mathcal{U}^+$ est p-divisible et ceci achève la démonstration du lemme 13.

4.3. Fin de la démonstration du théorème. Soit (X, Γ) un objet de ΓAUT. On suppose $e(\Gamma) < \infty$. Il s'agit de construire L/K de ΓEXT telle que $X(L/K)$ soit isomorphe à (X, Γ). Grâce au théorème de pleine fidélité, on se ramène immédiatement au cas où le corps résiduel k est algébriquement clos, ce que l'on suppose désormais.

Soient $\underline{K}_0$ le corps des fractions de l'anneau des vecteurs de Witt à coefficients dans k, K_{s} une clôture algébrique de $\underline{K}_0$, pour tout entier n, $\underline{K}_n$ l'extension de $\underline{K}_0$ engendrée dans K_{s} par une racine primitive p^n-ième de l'unité, et $\underline{K}_\infty$ la réunion des $\underline{K}_n$. Choisissons une suite $\epsilon' = (\epsilon'_n)$ de racines primitives p^n-ièmes de l'unité telles que $N_{\underline{K}_{n+1}/\underline{K}_n}(\epsilon'_{n+1}) = \epsilon'_n$. La suite (ϵ'_n) définit un élément ϵ' du corps des normes $X_{\underline{K}_0}(\underline{K}_\infty)$ et $X_{\underline{K}_0}(\underline{K}_\infty)$ s'identifie à $k((\epsilon' - 1))$. Le corps $X_{\underline{K}_\infty/\underline{K}_0}(K_{\mathrm{s}})$, réunion des $X_{\underline{K}_0}(M)$, pour M extension finie de $\underline{K}_\infty$ contenue dans K_{s}, s'identifie à une clôture séparable de $X_{\underline{K}_0}(\underline{K}_\infty)$ ([24] 3). Le groupe de Galois $\mathrm{Gal}(K_{\mathrm{s}}/\underline{K}_0)$ s'identifie au groupe des automorphismes τ de $X_{\underline{K}_\infty/\underline{K}_0}(K_{\mathrm{s}})$ qui sont tels que $\tau(\epsilon') = \epsilon'^a$ pour un $a \in (\mathbb{Z}_p)^*$.

On reprend les notations du 4.2. Pour tout entier $n \geq 1$, notons χ_n le composé de $\chi : G \to \mathbb{Z}_p^*$ avec le morphisme : $\mathbb{Z}_p^* \to (\mathbb{Z}/p^n\mathbb{Z})^*$, $G_n = \mathrm{Ker}\ \chi_n$ et $H_n = H \cap G_n$. Soit n_0 un entier ≥ 1 tel que pour $n \geq n_0$, G_{n+1} soit d'indice p dans G_n. Notons $(\epsilon_n)_{n \geq n_0}$ une suite d'éléments de torsion de $\mathcal{U}^+$ telle que ϵ_n soit d'ordre p^n et que : $N_{G_{n+1},G_n}(\epsilon_{n+1}) = \epsilon_n$

Distinguons les deux cas : $\chi(H)$ fini et $\chi(H)$ est un sous-groupe ouvert de $\mathbb{Z}_p^*$.

Si $\chi(H)$ est fini, notons H_{cyc} le noyau de la restriction de χ à H et posons $X' = X_{\mathrm{s}}^{H_{cyc}}$. Il resulte du lemme 7 que la suite (ϵ_n) définit un élément non trivial de $U^+_{X'}$ tel que pour tout $\tau \in G$, on ait $\tau(\epsilon) = \epsilon^{\chi(\tau)}$. Notons $X_{cyc} = k((\epsilon - 1))$, de sorte que X' est une extension finie de X_{cyc}. Cette extension est séparable, car, pour tout $n \geq n_0$, ϵ_n n'est pas une puissance p-ième dans $U^+_{G_n}$. Identifions X_{cyc} et $X_{\underline{K}_0}(\underline{K}_\infty)$ en envoyant ϵ sur ϵ' et prolongeons cet isomorphisme en un isomorphisme de X_{s} sur $X_{\underline{K}_\infty/\underline{K}_0}(K_{\mathrm{s}})$. Le groupe G s'identifie à un sous-groupe ouvert de $\mathrm{Gal}(K_{\mathrm{s}}/\underline{K}_0)$. On pose $K = K_{\mathrm{s}}^G$ et $L = K_{\mathrm{s}}^H$. L'extension L/K convient ([24] 3).

Supposons que $\chi(H)$ soit un sous-groupe ouvert de $\mathbb{Z}_p^*$. Notons $\eta : G \to \Gamma$ le morphisme induit par la restriction à X. Notons $\overline{G}$ l'image de G dans $\mathbb{Z}_p^* \times \Gamma$ et notons encore χ et η les projections sur $\mathbb{Z}_p^*$ et Γ respectivement. Soient $\overline{G_n}$ et $\overline{H_n}$ les images de G_n et de H_n dans $\overline{G}$. Posons $X_n = X_{\mathrm{s}}^{H_n}$, $X_\infty = \cup X_n$. On peut supposer n_0 suffisamment grand pour que $\eta(G_{n_0}) = \eta(\mathrm{Ker}(\chi))$. Notons $\overline{\sigma} \in \overline{G}$ un générateur de $\mathrm{Ker}\chi = \overline{G} \cap \Gamma$. Le groupe $\overline{G}$

agit naturellement sur le corps des normes $X_X(X_\infty)$. Notons i'_n la suite des nombres inférieurs de ramification de $\overline{\sigma}$ agissant sur $X_X(X_\infty)$.

Lemme 20. *On a* $\lim_{n\to\infty} i'_n/p^n = \infty$

Démonstration. Comme le sous-groupe topologique de $\overline{G}$ engendré par $\overline{\sigma}$ est d'indice infini dans $\overline{G}$, il suffit de prouver que $x/[\overline{G} : \overline{G}_x]$ est borné inférieurement par un réel > 0. On a :

$$\frac{x}{[\overline{G} : \overline{G}_x]} = \frac{\varphi_{X_\infty/X}(x)}{[\Gamma : \Gamma_{\varphi_{X_\infty/X}(x)}]} \times \frac{x}{\varphi_{X_\infty/X}(x)\ [\mathrm{Gal}(X_\infty/X) : \mathrm{Gal}(X_\infty/X)_x]}.$$

Comme la suite (i_n/p^n) a une limite finie non nulle, $\varphi_{X_\infty/X}(x)/[\Gamma : \Gamma_{\varphi_{X_\infty}(x)/X}]$ est borné inférieurement par un réel > 0. Si l'on note i''_n et b''_n la suite des nombres de ramification de la Γ-extension X_∞/X_{n_0}, on déduit de l' inégalité $b''_n \geq pb''_{n-1}$ que $i''_n/(p^n b''_n) \geq (p-1)/p$. Il en résulte facilement que

$$x/\varphi_{X_\infty/X}(x)\ [\mathrm{Gal}(X_\infty/X) : \mathrm{Gal}(X_\infty/X)_x]$$

est borné inférieurement par un réel > 0, ce qui achève de prouver le lemme.

4.3.1. Il résulte alors cas $e = \infty$ du théorème 1 qu'il existe X''/X' de ΓEXT, X' et X'' deux sous-corps du complété de la clôture radicielle de $X_X(X_\infty)$, telle que le corps des normes $X_{X'}(X'')$, muni de l'action de $\mathrm{Gal}(X''/X')$, s'identifie à $X_X(X_\infty)$, muni de l'action du sous-groupe d'automorphismes engendré par $\bar{\sigma}$. Le groupe G agit sur X' à travers $\chi(G)$. Notons X'_{s} la clôture séparable de X' dans dans le complété $\widehat{X_{\mathrm{s}}}$ de X_{s}. Comme $\widehat{X_{\mathrm{s}}}$ est algébriquement clos, X'_{s} est une clôture séparable de X'. Il résulte des propriétés fonctorielles du corps des normes ([24], théorème de pleine fidélité démontré au 2) que G s'identifie au groupe des automorphismes de X'_{s} qui induisent sur X' un élément de $\chi(G)$.

On a pour $n \geq n_0$: $U^+_{G_n} = U^+_{X_n}/(\overline{\sigma} - 1)\widehat{X^*_n}$. La suite (ϵ_n) définit un élément de $\varprojlim U^+_{G_n}$, les morphismes de transition étant les N_{G_{n+1},G_n}. Comme $\varprojlim U^+_{X_n} = U^+_{X_X(X_\infty)}$, $\varprojlim \widehat{X^*_n} = \widehat{X_X(X_\infty)}^*$, que la norme N_{X_{n+1}/X_n} induit un morphisme surjectif de $\widehat{X^*_{n+1}}$ sur $\widehat{X^*_n}$, on voit que la limite projective des $U^+_{G_n}$ s'identifie à $U^+_{X_X(X_\infty)}/(\overline{\sigma} - 1)(\widehat{X_X(X_\infty)})^*)$, *i.e.* à $U^+_{X'}$. La suite (ϵ_n) définit donc un élément $\epsilon \neq 1$ de $U^+_{X'}$ tel que, pour tout $\tau \in G$, on ait $\tau(\epsilon) = \epsilon^{\chi(\tau)}$. Identifions $k((\epsilon))$ et $k((\epsilon'))$ en envoyant ϵ sur ϵ'. Comme les ϵ_n ne sont pas des puissances p-ièmes dans les $U^+_{G_n}$, ϵ n'est pas une puissance p-ième dans X'. L'isomorphisme $k((\epsilon)) \simeq k((\epsilon'))$ se prolonge donc en un isomorphisme de X'_{s} sur $X_{\underline{K}_\infty/\underline{K}_0}(K_{\mathrm{s}})$. Comme $\chi(G)$ agit sur ϵ par le caractère χ, on voit que le groupe G s'identifie à un sous-groupe ouvert de $\mathrm{Gal}(K_s/\underline{K}_0)$. L'extension L/K avec $K = K_s^G$ et $L = K_s^H$ convient ([24]).

Ceci achève de prouver le théorème.

Références

[1] RACHEL CAMINA, *The Nottingham group.* In New horizons in pro-p groups, pages 205–221. Birkhäuser Boston, Boston, MA, 2000.

[2] MARCUS DU SAUTOY and IVAN FESENKO, *Where the wild things are : ramification groups and the Nottingham group.* In New horizons in pro-p groups, pages 287–328. Birkhäuser Boston, Boston, MA, 2000.

[3] IVAN FESENKO, *On just infinite pro-p-groups and arithmetically profinite extensions of local fields.* J. Reine Angew. Math. **517** (1999), 61–80.

[4] JEAN-MARC FONTAINE *Corps de séries formelles et extensions galoisiennes des corps locaux.* In Séminaire de Théorie des Nombres de Grenoble, 1971/72, page 10.

[5] JEAN-MARC FONTAINE, *Un résultat de Sen sur les automorphismes dans les corps locaux.* In Séminaire Delange-Pisot-Poitou : 1969/70, Théorie des Nombres, Fasc. 1, Exp. 6, page 13. Secrétariat mathématique, Paris, 1970.

[6] JEAN-MARC FONTAINE and JEAN-PIERRE WINTENBERGER, *Extensions algébrique et corps des normes des extensions APF des corps locaux.* C. R. Acad. Sci. Paris Sér. A-B, **288(8)** (1979), A441–A444.

[7] JEAN-MARC FONTAINE and JEAN-PIERRE WINTENBERGER, *Le "corps des normes" de certaines extensions algébriques de corps locaux.* C. R. Acad. Sci. Paris Sér. A-B, **288(6)** (1979), A367–A370.

[8] KEVIN KEATING, *Automorphisms and extensions of* $k((t))$. J. Number Theory, **41(3)** (1992), 314–321.

[9] F. LAUBIE and M. SAÏNE, *Ramification of automorphisms of* $k((t))$. J. Number Theory, **63(1)** (1997), 143–145.

[10] F. LAUBIE and M. SAÏNE, *Ramification of some automorphisms of local fields.* J. Number Theory, **72(2)** (1997), 174–182.

[11] JONATHAN LUBIN, *Non-Archimedean dynamical systems.* Compositio Math. **94(3)** (1994), 321–346.

[12] JONATHAN LUBIN, *Sen's theorem on iteration of power series.* Proc. Amer. Math. Soc. **123(1)** (1995), 63–66.

[13] MURRAY A. MARSHALL, *Ramification groups of abelian local field extensions.* Canad. J. Math. **23** (1971), 271–281.

[14] ECKART MAUS, *On the jumps in the series of ramifications groups.* In Colloque de Théorie des Nombres (Univ. Bordeaux, Bordeaux, 1969), pages 127–133. Bull. Soc. Math. France, Mém. **25**. Soc. Math. France, Paris, 1971.

[15] HIROO MIKI, *On unramified Abelian extensions of a complete field under a discrete valuation with arbitrary residue field of characteristic* $p \neq 0$ *and its application to wildly ramified* Z_p*-extensions.* J. Math. Soc. Japan, **29(2)** (1977), 363–371.

[16] HIROO MIKI, *On the ramification numbers of cyclic p-extensions over local fields.* J. Reine Angew. Math. **328** (1981), 99–115.

[17] SHANKAR SEN, *On automorphisms of local fields.* Ann. of Math. (2), **90** (1969), 33–46.

[18] JEAN-PIERRE SERRE, *Sur les corps locaux à corps résiduel algébriquement clos.* Bull. Soc. Math. France, **89** (1961), 105–154.

[19] JEAN-PIERRE SERRE, *Corps locaux.* Hermann, Paris, 1968. Deuxième édition, Publications de l'Université de Nancago, No. VIII.

[20] J. T. TATE, *p-divisible groups.* In Proc. Conf. Local Fields (Driebergen, 1966), pages 158–183. Springer, Berlin, 1967.

[21] JOHN S. WILSON, *Profinite groups.* The Clarendon Press Oxford University Press, New York, 1998.

[22] JEAN-PIERRE WINTENBERGER, *Extensions de Lie et groupes d'automorphismes des corps locaux de caractéristique p.* C. R. Acad. Sci. Paris Sér. A-B, **288(9)** (1979), A477–A479.

[23] JEAN-PIERRE WINTENBERGER, *Extensions abéliennes et groupes d'automorphismes de corps locaux.* C. R. Acad. Sci. Paris Sér. A-B, **290(5)** (1980), A201–A203.

[24] JEAN-PIERRE WINTENBERGER, *Le corps des normes de certaines extensions infinies de corps locaux; applications.* Ann. Sci. École Norm. Sup. (4), **16(1)** (1983), 59–89.

[25] BOSTWICK F. WYMAN, *Wildly ramified gamma extensions.* Amer. J. Math. **91** (1969), 135–152.

Jean-Pierre WINTENBERGER
Université Louis Pasteur
Département de Mathématiques, IRMA
7, rue René Descartes
67084 Strasbourg Cedex, France
E-mail : `wintenb@math.u-strasbg.fr`