

Des automorphismes continus d'un corps de séries de Puiseux

par

BRUNO DESCHAMPS (Le Mans)

1. Introduction. Si K désigne un corps, le corps $K((T))$ des séries de Laurent à coefficients dans K est un corps complet pour la valuation usuelle. Plusieurs travaux ont abordé l'étude du groupe des K -automorphismes du corps $K((T))$. Nous nous intéressons dans cet article, pour un corps K de caractéristique 0, à l'étude du groupe des K -automorphismes continus du corps, $\mathbf{Puis}(\overline{K})$, des séries de Puiseux à coefficients dans la clôture algébrique, \overline{K} , de K (la continuité étant ici considérée pour la topologie induite par l'unique extension de la valuation de $\overline{K}((T))$ au corps des séries de Puiseux).

Dans un premier paragraphe, nous nous intéressons aux automorphismes d'un corps discrètement valué de caractéristique et de caractéristique résiduelle égales (appelé ici corps sérié) hensélien. En particulier, nous décrivons une loi de groupe $*$ sur l'ensemble \mathcal{O}_K^\times des unités de $K((T))$ qui fait du groupe $(\mathcal{O}_K^\times, *)$ un groupe isomorphe au groupe, $(\mathbf{Aut}_K(K((T))), \circ)$, des K -automorphismes de $K((T))$ (application de la proposition 1).

Dans un deuxième paragraphe, nous appliquons ces résultats à l'étude du groupe $\mathbf{Aut}_K(\mathbf{Puis}(\overline{K}))$ des K -automorphismes continus du corps $\mathbf{Puis}(\overline{K})$. Nous montrons que ce groupe est isomorphe à un produit semi-direct à quatre facteurs d'objets arithmétiques liés à K (théorème 10).

Un troisième paragraphe est consacré à deux applications que nous faisons de ce résultat de structure. La première application concerne l'étude de sous-groupes du groupe des automorphismes, $\mathbf{Aut}(\mathbb{C})$, du corps des complexes. Nous montrons (théorème 12) que pour tout corps K de caractéristique 0 et de cardinal $\leq 2^{\aleph_0}$, le groupe de Galois absolu, $\mathbf{G}_K = \mathbf{Gal}(\overline{K}/K)$, de K est un sous-groupe de $\mathbf{Aut}(\mathbb{C})$.

La deuxième application concerne l'étude des involutions continues de $\mathbf{Puis}(\overline{K})$. Nous montrons (théorème 14) qu'en caractéristique 0, il existe

2000 *Mathematics Subject Classification*: Primary 12E30, 20E34, 20E45; Secondary 12J10, 12J15, 20E18.

une correspondance bi-univoque entre l'ensemble des classes de conjugaison d'involutions continues du groupe, $\mathbf{Aut}_K(\mathbf{Puis}(\overline{K}))$, des K -automorphismes (non nécessairement continus) du corps $\mathbf{Puis}(\overline{K})$, et l'ensemble des classes de conjugaison d'involutions du groupe $\mathbf{Aut}_K(\overline{K}) = \mathbf{Gal}(\overline{K}/K)$ (qui est lui-même en correspondance bi-univoque avec l'ensemble des ordres compatibles sur le corps K (corollaire 16)). En fin de texte, une série de remarques sur l'existence d'involutions non continues dans et hors de ces classes de conjugaison vient clore cet article.

2. Les automorphismes d'un corps sérié composable hensélien.

Dans cet article, on dira d'un corps Ω qu'il est *sérié* s'il est isomorphe à une extension intermédiaire d'une extension $K((T))/K(T)$. De manière équivalente, un corps Ω est sérié si et seulement s'il existe sur Ω une valuation discrète v telle que le corps résiduel $K = \Omega/v$ soit de même caractéristique que celle de Ω et telle que K se relève en un sous-corps de Ω (cette dernière propriété est automatiquement vérifiée si Ω est hensélien pour v). En effet, si l'on note $(\widehat{\Omega}, \widehat{v})$ le complété de (Ω, v) , alors \widehat{v} est discrète et $\widehat{\Omega}/\widehat{v} = K$. Il s'ensuit (cf. [Ser]) que $\widehat{\Omega}$ est K -isomorphe au corps $K((T))$ des séries de Laurent à coefficients dans K . Si π désigne une uniformisante de Ω , comme K se relève dans Ω , il existe un K -plongement de Ω dans $K((T))$ qui envoie π sur T et donc Ω est bien sérié. On s'intéresse ici à l'étude des K -automorphismes d'un corps sérié, on peut donc, dans cette perspective, regarder un tel corps directement comme un sous-corps de $K((T))$ qui contient $K(T)$.

Un corps sérié Ω sera dit *composable* si la composition laisse stable Ω , c'est-à-dire si

$$\forall S(T), R(T) \in \Omega, \quad v(R(T)) > 0 \Rightarrow S(R(T)) \in \Omega.$$

Par exemple, les corps $\Omega = K(T), K((T))$ sont des corps sériés composables. Tous les corps sériés ne sont pas forcément composables (voir plus loin).

Nous allons nous intéresser ici au groupe des K -automorphismes de Ω lorsque Ω est sérié, composable et hensélien pour v . Un exemple de tel corps est naturellement le corps $K((T))$, car il est complet. Un exemple de corps sérié composable hensélien non complet est le corps $\mathbb{C}\{\{T\}\}$ des séries de Laurent de rayon de convergence > 0 (i.e. le corps des germes de fonctions complexes méromorphes en 0). Il est visiblement composable et non complet et on pourra trouver dans [Art] une preuve du fait qu'il est hensélien.

Un exemple de corps sérié hensélien non composable. Dans le corps $\mathbb{R}\{\{T\}\}$ des séries de Laurent réelles à rayon de convergence non nul, on considère la série

$$e^T = \sum_{n \geq 0} \frac{T^n}{n!}$$

et le corps $L_0 = \mathbb{R}(T)(e^T) \subset \mathbb{R}\{\{T\}\}$. On considère aussi dans $\mathbb{R}\{\{T\}\}$ la série $f(T) = e^{Te^T}$. La série f est transcendante sur L_0 . En effet, supposons au contraire qu'il existe un polynôme irréductible

$$P(X) = X^n + a_{n-1}(T)X^{n-1} + \dots + a_0(T) \in L_0[X]$$

tel que $P(f(T)) = 0$. En considérant la dérivation usuelle sur les séries de Laurent (qui, sur L_0 , correspond à la dérivation analytique) on a alors

$$\begin{aligned} 0 &= (P(f(T)))' \\ &= a'_0(T) + (a'_1(T) + a_1(T)(1+T)e^T)f(T) + \dots \\ &\quad + (a'_{n-1}(T) + (n-1)a_{n-1}(T)(1+T)e^T)f^{n-1}(T) + n(1+T)e^T f^n(T) \\ &= Q(f(T)) \end{aligned}$$

avec

$$Q(X) = n(1+T)e^T X^n + \sum_{k=0}^{n-1} (a'_k(T) + ka_k(T)(1+T)e^T)X^k.$$

On en déduit donc, par minimalité de P , que Q est proportionnel à P et donc que pour tout $k = 0, \dots, n-1$, on a

$$(E_k) \quad a'_k(T) = (n-k)(1+T)e^T a_k(T).$$

La résolution des équations différentielles (E_k) montre que, pour tout $k = 0, \dots, n-1$, il existe une constante $C_k \in \mathbb{R}$ telle que

$$a_k(T) = C_k e^{(n-k)Te^T}.$$

On a alors obligatoirement $C_k = 0$, car si l'on regarde maintenant les séries comme des fonctions de la variable réelle, un simple argument analytique de passage à la limite montre que l'on ne peut pas écrire

$$e^{(n-k)xe^x} = \frac{\sum_{p=0}^{p_0} R_p(x)e^{px}}{\sum_{q=0}^{q_0} S_q(x)e^{qx}}$$

avec $p_0, q_0 \in \mathbb{N}$ et $R_0, \dots, R_{p_0}, S_0, \dots, S_{q_0} \in \mathbb{R}(T)$.

Ainsi, $f(T)$ est bien transcendante sur L_0 et donc n'est pas élément de la clôture algébrique \tilde{L}_0 de L_0 dans $\mathbb{R}\{\{T\}\}$. Le corps \tilde{L}_0 est visiblement sérié et comme il est algébriquement clos dans $\mathbb{R}\{\{T\}\}$ qui est hensélien, il est lui-même hensélien. Par ailleurs, la série composée e^{Te^T} n'est pas dans \tilde{L}_0 comme on vient de le voir, ce qui justifie que \tilde{L}_0 ne soit pas un corps composable.

Étant donné un corps K , on considère \mathcal{O}_K^\times l'ensemble des unités de $K((T))$ (i.e. l'ensemble des séries de valuation nulle). Sur \mathcal{O}_K^\times , on introduit

la loi de composition $*$ définie, pour $\alpha(T), \beta(T) \in \mathcal{O}_K^\times$, par

$$(\alpha * \beta)(T) = \alpha(T) \cdot \beta(T\alpha(T)).$$

Nous allons voir, dans la preuve de la proposition suivante, que $*$ confère à \mathcal{O}_K^\times une structure de groupe. Si Ω désigne un corps sérié de corps résiduel K , alors il est clair que le groupe des unités de Ω vaut $\mathcal{O}_K^\times \cap \Omega$.

PROPOSITION 1. *Soit Ω un corps sérié hensélien de corps résiduel K . Il existe une application injective $\Theta : \mathbf{Aut}_K(\Omega) \rightarrow \mathcal{O}_K^\times \cap \Omega$ morphique pour \circ et $*$ (i.e. $\Theta(\mu \circ \sigma) = \Theta(\mu) * \Theta(\sigma)$). Si, de plus, Ω est composable, alors Θ est un isomorphisme (en particulier, $(\mathcal{O}_K^\times \cap \Omega, *)$ est alors un groupe).*

Etablissons, préalablement, deux lemmes :

LEMME 2. *Soit (Ω, v) un corps discrètement valué hensélien. Si σ est un automorphisme de Ω , alors σ est continu et de plus, si π désigne une uniformisante de Ω , alors $\sigma(\pi)$ est aussi une uniformisante.*

Preuve. De manière générale, si v_0 est une valuation non triviale sur Ω et non équivalente à v , alors (Ω, v_0) n'est pas un corps hensélien (cf. [Rib1, 3.2.W(β)]). Considérons alors, sur Ω , la valuation $v_0 = v \circ \sigma^{-1}$. Puisque σ est un automorphisme de corps, il est clair que la propriété d'Hensel est respectée pour v_0 . On en déduit donc que v et v_0 sont équivalentes et par suite que les anneaux A_v et A_{v_0} des valuations v et v_0 sont égaux. Comme $A_{v_0} = \sigma(A_v)$ on en déduit bien que $\sigma(\pi)$ est une uniformisante.

Par ailleurs, pour les mêmes raisons que précédemment, les valuations v et $v \circ \sigma$ sont équivalentes. Donc, si $(x_n)_n$ désigne une suite convergente vers 0 (i.e. $\lim_n v(x_n) = +\infty$) alors $\lim_n v(\sigma(x_n)) = +\infty$ et donc $(\sigma(x_n))_n$ converge aussi vers 0. On en déduit que σ est continu en 0 et, par suite, partout. ■

LEMME 3. *Soit Ω un corps sérié hensélien de corps résiduel K ($\Omega \subset K((T))$ et $T \in \Omega$) et σ un K -automorphisme de Ω . Pour tout*

$$S(T) = \sum_{n \geq n_0} a_n T^n \in \Omega$$

on a

$$\sigma(S)(T) = \sum_{n \geq n_0} a_n \sigma(T)^n$$

(i.e. $\sigma(S)(T) = S(\sigma(T))$).

Preuve. Dans la preuve du lemme 2, on montre que si σ est un K -automorphisme de Ω , alors $\sigma(A_v) = A_v$ (A_v étant l'anneau de la valuation), c'est-à-dire que la restriction de σ à A_v est un K -automorphisme d'anneau. Il s'ensuit que, puisque les éléments inversibles de A_v sont exactement les

séries de Ω de valuation 0, l'image d'une série de valuation 0, par σ , est de valuation 0.

Toujours d'après le lemme 2, on sait que $\sigma(T)$ est une uniformisante, donc la valuation de $\omega = \sigma(T)$ est 1 et, par suite, la série composée $S(\omega)$ a bien un sens dans $K((T))$. Pour tout $m \geq n_0$, on a alors

$$\sigma(S)(T) - S(\omega) = \sigma\left(\sum_{n>m} a_n T^n\right) - \sum_{n>m} a_n \omega^n.$$

Comme σ est continu et que $v(\omega^n) = n$, on en déduit que le terme de droite de cette équation tend vers 0 quand m tend vers $+\infty$ et, par suite, que $\sigma(S)(T) = S(\sigma(T))$. ■

Preuve de la proposition 1. Soit $\sigma \in \mathbf{Aut}_K(\Omega)$. D'après le lemme 2, il existe un élément $\alpha \in \mathcal{O}_K^\times \cap \Omega$ tel que $\sigma(T) = T\alpha(T)$. Considérons alors l'application

$$\Theta : \mathbf{Aut}_K(\Omega) \rightarrow \mathcal{O}_K^\times \cap \Omega, \quad \sigma \mapsto \alpha(T) = \sigma(T)/T.$$

Le lemme 3 assure que σ est entièrement déterminé par son image en T . On en déduit que Θ est injective. Par ailleurs, un rapide calcul montre que $\Theta(\sigma \circ \mu) = \Theta(\sigma) * \Theta(\mu)$.

Si, maintenant, Ω est supposé composable, alors si $\alpha(T) \in \mathcal{O}_K^\times \cap \Omega$, pour tout $S \in \Omega$, on a $S(T\alpha(T)) \in \Omega$ et l'application $\sigma_\alpha : S(T) \rightarrow S(T\alpha(T))$ définit, dans $\mathbf{Aut}_K(\Omega)$, un antécédent, par Θ , de α . Ceci justifie que, dans ce cas, Θ est bien un isomorphisme. ■

REMARQUES. • La loi $*$ peut paraître un peu compliquée, elle est pourtant équivalente à une composition. En effet, si on considère l'ensemble

$$\mathcal{E} = \{S \in K((T)) \mid v(S) = 1\}$$

alors l'application

$$f : (\mathcal{O}_K^\times, *) \rightarrow (\mathcal{E}, \circ), \quad \alpha(T) \mapsto T\alpha(T)$$

est un isomorphisme de groupe.

• Dans le cas de $\Omega = K((T))$, on trouve donc que $(\mathbf{Aut}_K(K((T))), \circ)$ est isomorphe à $(\mathcal{O}_K^\times, *)$. Considérons, dans \mathcal{O}_K^\times , l'ensemble des unités principales $1 + \mathfrak{M}$:

$$1 + \mathfrak{M} = \{\alpha \in \mathcal{O}_K^\times \mid \alpha(0) = 1\}.$$

On remarque que, muni de la loi $*$, cet ensemble devient un sous-groupe de \mathcal{O}_K^\times . Par ailleurs, on remarque en plus que $K^* \subset \mathcal{O}_K^\times$ est aussi, pour la loi $*$, un sous-groupe de \mathcal{O}_K^\times et qu'en fait, sur ce sous-groupe, la loi $*$ n'est rien d'autre que la multiplication dans K^* . Le sous-groupe (K^*, \cdot) agit alors sur un élément $\alpha \in \mathcal{O}_K^\times$ par conjugaison : si $a \in K$, on a

$$\alpha^a(T) = (a * \alpha(T) * a^{-1})(T) = \alpha(aT).$$

Il est alors à noter que le groupe $(\mathcal{O}_K^\times, *)$ est le produit semi-direct des sous-groupes $(1+\mathfrak{M}, *)$ et (K^*, \cdot) . En effet, il est clair que $(1+\mathfrak{M}) \cap K^* = \{1\}$ et que $1+\mathfrak{M}$ et K^* engendrent $(\mathcal{O}_K^\times, *)$ puisque pour tout $\alpha \in (\mathcal{O}_K^\times, *)$, on a

$$\alpha = \left(\frac{\alpha}{\alpha(0)} \right) * \alpha(0).$$

Par ailleurs, $1 + \mathfrak{M}$ est bien distingué dans \mathcal{O}_K^\times .

3. Les K -automorphismes continus de $\mathbf{Puis}(\overline{K})$. Rappelons que, si K désigne un corps, le corps des séries de Puiseux à coefficients dans K est le corps $\varinjlim K((T^{1/n}))$, où $K((T^{1/n}))$ désigne le corps de rupture sur $K((T))$ du polynôme $X^n - T$ (les flèches du système inductif s'entendant d'elles-mêmes).

On notera, dans la suite de ce texte, $\mathbf{Puis}(K)$ ce corps. Il est célèbre que si K est un corps algébriquement clos de caractéristique 0, alors $\mathbf{Puis}(K)$ est un corps algébriquement clos (c'est une clôture algébrique du corps $K((T))$). Par ailleurs, il existe sur $\mathbf{Puis}(K)$ une valuation ν naturelle (celle qui étend la valuation v de $K((T))$), définie pour $S(T) = \sum_{k \geq k_0} a_k T^{k/n} \in \mathbf{Puis}(K)$ ($a_{k_0} \neq 0$) par

$$\nu(S) = \frac{k_0}{n}.$$

C'est muni de cette valuation que l'on considérera le corps $\mathbf{Puis}(K)$ dans ce paragraphe, qui définit alors une topologie sur $\mathbf{Puis}(K)$. On s'intéresse aux automorphismes continus, plus précisément, pour un corps K de caractéristique 0, on étudie dans ce paragraphe le groupe

$$\Pi = \text{Aut}_K(\mathbf{Puis}(\overline{K}))$$

des K -automorphismes continus de $\mathbf{Puis}(\overline{K})$.

Remarquons, pour commencer, qu'au contraire du cas du corps des séries de Laurent, il existe des K -automorphismes non continus. En effet, la variable T est transcendante sur K . Si l'on considère une extension transcendante pure maximale de K dans $\mathbf{Puis}(\overline{K})$, $L = K(X_i)_{i \in I}$, telle que $X_{i_0} = T$ pour un certain indice $i_0 \in I$, alors l'application

$$X_i \mapsto X_i \quad \text{pour } i \neq i_0, \quad T \mapsto 1/T,$$

définit un K -automorphisme σ de L . Par hypothèse de maximalité, l'extension $\mathbf{Puis}(\overline{K})/L$ est algébrique et comme $\mathbf{Puis}(\overline{K})$ est algébriquement clos, d'après le théorème de Steinitz, σ se relève en un K -automorphisme de $\mathbf{Puis}(\overline{K})$. Ce dernier ne peut être continu (comme le montrera le lemme suivant) puisque $\sigma(T) = T^{-1}$.

Dans la suite, on notera $\mathbf{Puis}[\overline{K}]$ l'anneau des séries entières de Puiseux, c'est-à-dire le sous-anneau de $\mathbf{Puis}(\overline{K})$ composé des séries de valuation ≥ 0 (i.e. l'anneau de la valuation ν). Caractérisons les éléments de Π :

LEMME 4. Soit σ un K -automorphisme de $\mathbf{Puis}(\overline{K})$. Les propositions suivantes sont équivalentes :

- (i) σ est continu,
- (ii) la restriction de σ à $\mathbf{Puis}[\overline{K}]$ est un automorphisme de $\mathbf{Puis}[\overline{K}]$,
- (iii) $\nu(\sigma(T)) > 0$ et $\nu(\sigma(S)) = 0$ pour toutes séries S de valuation 0.

En conséquence, si $\sigma \in \Pi$ alors pour tout $\sum_{k \geq k_0} a_k T^{k/n} \in \mathbf{Puis}(\overline{K})$ on a

$$\sigma\left(\sum_{k \geq k_0} a_k T^{k/n}\right) = \sum_{k \geq k_0} \sigma(a_k) \sigma(T^{1/n})^k.$$

Preuve. (i) \Rightarrow (ii). Prenons un S dans $\mathbf{Puis}[\overline{K}]$, posons $r = \nu(S)$ et considérons deux cas :

- $r > 0$. Comme σ est continu et que $(S^n)_n$ converge vers 0, on a

$$\lim_{n \rightarrow +\infty} \nu(\sigma(S^n)) = \lim_{n \rightarrow +\infty} n\nu(\sigma(S)) = +\infty$$

et ainsi $\nu(\sigma(S)) > 0$.

- $\nu(S) = 0$. Posons alors $S' = S - S(0)$. Alors $\nu(S') > 0$ et, d'après ce qui précède, on a $\nu(\sigma(S')) = \nu(\sigma(S) - \sigma(S(0))) > 0$. Mais comme $S(0) \in \overline{K}$ et que σ est un K -automorphisme, on a alors $\sigma(S(0)) \in \overline{K}$ et donc $\nu(\sigma(S)) \geq 0$.

Ainsi σ envoie injectivement $\mathbf{Puis}[\overline{K}]$ sur lui-même. En appliquant ce résultat à σ^{-1} , on voit aussi que cette application est surjective.

(ii) \Rightarrow (iii). Comme σ est un morphisme d'anneau, il envoie le groupe des inversibles de $\mathbf{Puis}[\overline{K}]$ sur lui-même, de même pour son complémentaire. On a donc $\nu(\sigma(T)) > 0$ et $\nu(\sigma(S)) = 0$ pour toutes séries S de valuation nulle.

(iii) \Rightarrow (i). Par hypothèse, il existe un rationnel $r_0 > 0$ tel que $\sigma(T) = T^{r_0} \alpha_1$ où α_1 est une série de valuation nulle. On en déduit que pour tout entier $n \geq 1$, il existe une série $\alpha_{1/n}$ de valuation nulle telle que

$$\sigma(T^{1/n}) = T^{r_0/n} \alpha_{1/n},$$

la série $\alpha_{1/n}$ étant une des racines n -ièmes de la série α_1 , ces racines existant bien puisque \overline{K} est un corps algébriquement clos de caractéristique 0 (une série $S \in L((T))$ de valuation nulle possède une racine n -ième dans $L((T))$, avec L de caractéristique 0, si et seulement si $S(0)$ en possède une dans L). Ainsi, si $r > 0$ désigne un rationnel, alors il existe une série α_r de valuation nulle telle que

$$\sigma(T^r) = T^{rr_0} \alpha_r.$$

Considérons maintenant une suite $(S_k)_{k \geq 1}$ de séries convergeant vers 0 (i.e. $\lim_{k \rightarrow +\infty} \nu(S_k) = +\infty$). Pour tout $k \geq 1$, posons $r_k = \nu(S_k)$. On a donc

$$S_k = T^{r_k} \omega_k$$

où ω_k est une série de valuation nulle. On en déduit que

$$\sigma(S_k) = T^{r_k r_0} \alpha_{r_k} \sigma(\omega_k);$$

mais comme $\sigma(\omega_k)$ est de valuation nulle, on a $\nu(\sigma(S_k)) = r_k r_0$, et comme $\lim_{k \rightarrow +\infty} r_k = +\infty$, on a bien

$$\lim_{k \rightarrow +\infty} \nu(\sigma(S_k)) = +\infty,$$

c'est-à-dire que la suite $(\sigma(S_k))_k$ converge vers 0. Ainsi σ est continu en 0 et, par suite, continu partout.

Considérons $\sum_{k \geq k_0} a_k T^{k/n} \in \mathbf{Puis}(\bar{K})$ et $\sigma \in \Pi$. D'après ce qui précède, $\omega = \sigma(T^{1/n})$ est de valuation $r > 0$. Pour tout entier $l \geq k_0$, on a donc

$$\begin{aligned} \sigma\left(\sum_{k \geq k_0} a_k T^{k/n}\right) &= \sum_{k \geq k_0} \sigma(a_k) \sigma(T^{1/n})^k \\ &= \sigma\left(\sum_{k \geq l} a_k T^{k/n}\right) - \sum_{k \geq l} \sigma(a_k) \omega^{k/n} \\ &= \omega^{l/n} \left(\sigma\left(\sum_{k \geq l} a_k T^{(k-l)/n}\right) - \sum_{k \geq l} \sigma(a_k) \omega^{(k-l)/n} \right), \end{aligned}$$

ce qui montre que cette série est de valuation $\geq lr/n$ pour tout l , donc de valuation infinie, d'où l'égalité. ■

3.1. Une décomposition du groupe Π . Notons $G_K = \mathbf{Gal}(\bar{K}/K)$ le groupe de Galois absolu du corps K . Remarquons que G_K peut être vu comme sous-groupe de Π . En effet, si $\sigma \in G_K$, alors l'élément $\tilde{\sigma}$ défini par

$$\tilde{\sigma}\left(\sum_{k \geq k_0} a_k T^{k/n}\right) = \sum_{k \geq k_0} \sigma(a_k) T^{k/n}$$

est clairement un élément de Π et la correspondance $\sigma \mapsto \tilde{\sigma}$ est visiblement un morphisme injectif de groupe. C'est *via* ce morphisme que l'on considère maintenant G_K comme sous-groupe de Π . Considérons aussi le sous-groupe de Π suivant :

$$\Delta = \mathbf{Aut}_{\bar{K}}(\mathbf{Puis}(\bar{K}))$$

composé des \bar{K} -automorphismes de $\mathbf{Puis}(\bar{K})$ continus. On a alors

PROPOSITION 5. *Le sous-groupe Δ est distingué dans Π et l'on a*

$$\Pi = G_K \rtimes \Delta.$$

Preuve. Un calcul rapide assure que Δ est bien distingué dans Π . Il est clair que $\Delta \cap G_K = \{\text{Id}\}$. Considérons $\sigma \in \Pi$ et définissons $\tilde{\sigma}$ par

$$\tilde{\sigma}\left(\sum_{k \geq k_0} a_k T^{k/n}\right) = \sum_{k \geq k_0} \sigma(a_k) T^{k/n}.$$

C'est un élément de G_K et l'on a $\tilde{\sigma}^{-1} \circ \sigma \in \Delta$. Ainsi, $\sigma \in G_K \cdot \Delta$. ■

3.2. Une décomposition du groupe Δ . Pour tout rationnel $r > 0$, on définit σ_r par

$$\sigma_r \left(\sum_{k \geq k_0} a_k T^{k/n} \right) = \sum_{k \geq k_0} a_k T^{r(k/n)}.$$

Par le lemme 4, σ_r est bien un élément de Π . Il est aussi clairement dans Δ . Considérons les deux sous-groupes de Δ suivants :

$$\Gamma = \{ \sigma \in \Delta \mid \nu \circ \sigma = \nu \}, \quad \Lambda = \{ \sigma_r \mid r \in \mathbb{Q}^{+*} \}.$$

PROPOSITION 6. *Le sous-groupe Γ est distingué dans Π (donc dans Δ) et l'on a*

$$\Delta = \Lambda \rtimes \Gamma.$$

Preuve. Soit $\sigma \in \Pi$, $\mu \in \Gamma$ et $S \in \mathbf{Puis}(\bar{K})$ non nulle. On écrit

$$S = T^r \alpha$$

avec α une série de valuation 0 et $r \in \mathbb{Q}$. On pose $\sigma(T^r) = T^{r'} \alpha'$ où α' est de valuation nulle. On a alors

$$\sigma(S) = T^{r'} \alpha' \sigma(\alpha)$$

et donc

$$(\mu \circ \sigma)(S) = T^{r'} \alpha' \sigma(\alpha) \gamma$$

où

$$\gamma = \frac{\mu(T^{r'})}{T^{r'}} \cdot \frac{\mu(\alpha')(\mu \circ \sigma)(\alpha)}{\alpha' \sigma(\alpha)}$$

est une série de valuation nulle. On en déduit donc que

$$(\sigma^{-1} \circ \mu \circ \sigma)(S) = T^r \delta$$

avec $\delta = \sigma^{-1}(\gamma)$ de valuation nulle. Ainsi $\nu((\sigma^{-1} \circ \mu \circ \sigma)(S)) = \nu(S)$ et donc Γ est distingué dans Π .

Il est clair que $\Gamma \cap \Lambda = \{\text{Id}\}$. Considérons maintenant un élément $\sigma \in \Delta$. Il existe un rationnel $r_0 > 0$ tel que

$$\sigma(T) = T^{r_0} \alpha(T^{1/n})$$

où α est une série de valuation nulle et $n \geq 1$ un entier. On a donc

$$(\sigma_{r_0^{-1}} \circ \sigma)(T) = T \alpha(T^{r_0^{-1}/n}),$$

ce qui implique que pour tout entier $h \geq 1$, on a

$$(\sigma_{r_0^{-1}} \circ \sigma)(T^{1/h}) = T^{1/h} \alpha^{1/h}(T^{r_0^{-1}/n})$$

où $\alpha^{1/h}$ désigne une des racines h -ièmes (qui existent bien) de α . On en déduit donc que pour tout rationnel $r \geq 0$, on a

$$(\sigma_{r_0^{-1}} \circ \sigma)(T^r) = T^r \beta_r$$

où β_r désigne une série de valuation nulle. Ceci montre que $\sigma_{r_0^{-1}} \circ \sigma \in \Gamma$ et par suite que $\sigma \in \Lambda \cdot \Gamma$. ■

REMARQUE. Il est clair que le groupe Λ est isomorphe au groupe (\mathbb{Q}^{+*}, \cdot) . On trouve donc pour Π une décomposition de la forme

$$\Pi \simeq G_K \rtimes (\mathbb{Q}^{+*} \rtimes \Gamma);$$

mais l'action de G_K sur \mathbb{Q}^{+*} est triviale et comme Γ est distingué dans tout Π on en déduit qu'en fait

$$\Pi \simeq (G_K \times \mathbb{Q}^{+*}) \rtimes \Gamma.$$

3.3. Une décomposition du groupe Γ . Les éléments σ de Γ sont caractérisés (en utilisant le lemme 4) par le fait que pour tout entier $n \geq 1$, la série $\sigma(T^{1/n})/T^{1/n}$ est de valuation 0. On considère alors les sous-groupes

$$H = \left\{ \sigma \in \Gamma \mid \frac{\sigma(T^{1/n})}{T^{1/n}}(0) = 1 \text{ pour tout } n \geq 1 \right\},$$

$$M = \left\{ \sigma \in \Gamma \mid \frac{\sigma(T^{1/n})}{T^{1/n}} \in \overline{K}^* \text{ pour tout } n \geq 1 \right\}.$$

On a alors

PROPOSITION 7. *Le sous-groupe H est distingué dans Γ et l'on a*

$$\Gamma = M \rtimes H.$$

Preuve. Considérons $\sigma \in \Gamma$ et $\mu \in H$. Fixons un entier $n \geq 1$. Il existe une série $\alpha \in \overline{K}((T))$ de valuation nulle telle que

$$\sigma(T^{1/n}) = T^{1/n} \alpha(T^{1/k})$$

pour un certain entier $k \geq 1$. Par hypothèse, il existe deux séries $\beta, \gamma \in \overline{K}((T))$ telles que $\beta(0) = \gamma(0) = 1$ et deux entiers $k', k'' \geq 1$ tels que

$$\mu(T^{1/n}) = T^{1/n} \beta(T^{1/k'}), \quad \mu(T^{1/k}) = T^{1/k} \gamma(T^{1/k''}).$$

On a donc, par application du lemme 4,

$$\begin{aligned} (\mu \circ \sigma)(T^{1/n}) &= T^{1/n} \beta(T^{1/k'}) \alpha(T^{1/k} \gamma(T^{1/k''})) \\ &= T^{1/n} \alpha(T^{1/k}) \frac{\beta(T^{1/k'}) \alpha(T^{1/k} \gamma(T^{1/k''}))}{\alpha(T^{1/k})} \end{aligned}$$

et ainsi

$$(\sigma^{-1} \circ \mu \circ \sigma)(T^{1/n}) = T^{1/n} \sigma^{-1} \left(\frac{\beta(T^{1/k'}) \alpha(T^{1/k} \gamma(T^{1/k''}))}{\alpha(T^{1/k})} \right).$$

Par continuité de σ , on a donc

$$\frac{(\sigma^{-1} \circ \mu \circ \sigma)(T^{1/n})}{T^{1/n}}(0) = \sigma^{-1} \left(\frac{\beta(0) \cdot \alpha(0)}{\alpha(0)} \right) = \sigma^{-1}(1) = 1$$

et par suite H est bien distingué dans Γ .

Il est clair que $M \cap H = \{\text{Id}\}$. Considérons $\sigma \in \Gamma$ et pour tout $n \geq 1$, posons

$$\alpha_n = \frac{\sigma(T^{1/n})}{T^{1/n}}(0)$$

et définissons une application μ de la manière suivante :

$$\mu\left(\sum_{k \geq k_0} a_k T^{k/n}\right) = \sum_{k \geq k_0} a_k \alpha_n^{-k} T^{k/n}.$$

Montrons que la définition de μ ne dépend pas du choix de n . Si $n \mid m$, disons $m = ln$, on a $T^{1/n} = T^{l/m}$ et par suite

$$\alpha_n = \frac{\sigma(T^{1/n})}{T^{1/n}}(0) = \frac{\sigma(T^{l/m})}{T^{l/m}}(0) = \left(\frac{\sigma(T^{1/n})}{T^{1/n}}\right)^l(0) = \alpha_m^l,$$

ce qui justifie bien que la définition de μ en un élément $S \in \mathbf{Puis}(\overline{K})$ ne dépend pas du choix du représentant de S . Il est clair que μ est un élément de M et que pour tout entier $n \geq 1$ on a

$$\frac{(\sigma \circ \mu)(T^{1/n})}{T^{1/n}}(0) = 1.$$

Ainsi $\sigma \in H \cdot M$. ■

3.4. Étude des groupes H et M . Le groupe

$$M = \left\{ \sigma \in \Pi \mid \forall n \in \mathbb{N}^*, \frac{\sigma(T^{1/n})}{T^{1/n}} \in \overline{K}^* \right\}$$

est visiblement abélien. Pour tout couple d'entiers (n, m) non nuls tel que $n \mid m$ (disons $m = kn$), considérons le morphisme

$$\varphi_{m,n} : \overline{K}^* \rightarrow \overline{K}^*, \quad x \mapsto x^k.$$

Il est clair que le système $(\varphi_{m,n}, \overline{K}^*)_n$ est projectif, la limite projective $\varprojlim \overline{K}^*$ a donc une structure de groupe.

PROPOSITION 8. On a

$$M \simeq \varprojlim \overline{K}^*.$$

Preuve. On regarde $\varprojlim \overline{K}^*$ comme sous-groupe du groupe produit $\prod_{\mathbb{N}^*} \overline{K}^*$ et on considère l'application $\Psi : M \rightarrow \prod_{\mathbb{N}^*} \overline{K}^*$ définie par

$$\Psi(\sigma) = \left(\frac{\sigma(T^{1/n})}{T^{1/n}} \right)_n.$$

Cette application est visiblement un morphisme et, en application du lemme 4, comme σ est entièrement déterminé par ses valeurs en les $T^{1/n}$, on en déduit que Ψ est injective. Considérons $(a_n)_n = \Psi(\sigma)$. Pour tout $m = kn$

on a

$$a_n = \frac{\sigma(T^{1/n})}{T^{1/n}} = \frac{\sigma(T^{k/m})}{T^{k/m}} = \left(\frac{\sigma(T^{1/m})}{T^{1/m}} \right)^k = a_m^k ;$$

il s'ensuit que $\Psi(\sigma) \in \varprojlim \overline{K}^*$.

Reste à montrer la surjectivité de Ψ . Considérons $(a_n)_n \in \varprojlim \overline{K}^*$. Alors si $S = \sum_{k \geq k_0} \lambda_k T^{k/n}$, l'application σ définie par

$$\sigma(S) = \sum_{k \geq k_0} \lambda_k a_n^k T^{k/n}$$

(cette définition ne dépend pas du choix de n , à cause de la compatibilité des a_n) est visiblement un élément de M qui vérifie $\Psi(\sigma) = (a_n)_n$, d'où la surjectivité. ■

REMARQUE. Pour tout $n \geq 1$, on considère le sous-groupe U_n des racines n -ièmes de l'unité dans \overline{K}^* . Le groupe $\varprojlim U_n$ est donc un sous-groupe de $\varprojlim \overline{K}^*$. Il est classique qu'il est isomorphe au groupe profini $\widehat{\mathbb{Z}}$. En effet, la donnée d'un système cohérent de racines primitives n -ièmes de l'unité $(\xi_n)_n$ permet de définir, pour tout $n \in \mathbb{N}^*$, des isomorphismes $f_n : U_n \rightarrow \mathbb{Z}/n\mathbb{Z}$ (en posant $f_n(\xi_n) = 1$) tels que, pour tout $n | m$, le diagramme

$$\begin{array}{ccc} U_m & \xrightarrow{f_m} & \mathbb{Z}/m\mathbb{Z} \\ \downarrow \varphi_{m,n} & & \downarrow \\ U_n & \xrightarrow{f_n} & \mathbb{Z}/n\mathbb{Z} \end{array}$$

soit commutatif, d'où l'isomorphisme.

Maintenant, si l'on considère la première projection $M \rightarrow \overline{K}^*$, celle qui à $(a_n)_n$ associe a_1 , on voit que ce morphisme est surjectif. En effet, étant donné $a \in \overline{K}^*$, si pour un entier $n \geq 1$, on note $R_n(a)$ l'ensemble des racines n -ièmes de a dans \overline{K}^* , alors on voit que l'ensemble $\varprojlim R_n(a) \subset \varprojlim \overline{K}^*$ constitue l'ensemble des antécédents de a par la première projection. Or les ensembles $R_n(a)$ étant finis et non vides, l'ordre $n | m$ sur \mathbb{N} étant filtrant à droite, on en déduit que $\varprojlim R_n(a)$ est non vide, d'où la surjectivité.

Le noyau du morphisme $M \rightarrow \overline{K}^*$ est précisément $\varprojlim U_n$, c'est-à-dire que l'on a la suite exacte

$$1 \rightarrow \widehat{\mathbb{Z}} \rightarrow M \rightarrow \overline{K}^* \rightarrow 1.$$

Cette suite n'est pas scindée. En effet, si elle l'était on aurait $M \simeq \widehat{\mathbb{Z}} \times \overline{K}^*$ et par suite il y aurait de la torsion dans M , ce qui est impossible, puisqu'alors il existerait des sous-corps stricts d'indice fini de $\mathbf{Puis}(\overline{K})$ contenant \overline{K} (donc $\sqrt{-1}$), ce qui est absurde d'après la théorie d'Artin-Schreier des corps réels clos.

Il n'est pas anodin de trouver ce facteur $\widehat{\mathbb{Z}}$ dans M . Une fois choisi un système cohérent de racines de l'unité $(\xi_n)_n$, un élément $(a_n)_n \in \widehat{\mathbb{Z}}$ correspond dans M à un automorphisme $\sigma \in M$ vérifiant, pour tout $n \in \mathbb{N}^*$,

$$\sigma(T^{1/n}) = \xi_n^{a_n} T^{1/n},$$

c'est-à-dire à un $\overline{K}((T))$ -automorphisme de $\mathbf{Puis}(\overline{K})$. On voit alors que ce facteur $\widehat{\mathbb{Z}}$ correspond précisément à $\mathbf{Gal}(\mathbf{Puis}(\overline{K})/\overline{K}((T)))$.

Intéressons-nous maintenant au groupe

$$H = \left\{ \sigma \in \Gamma \mid \frac{\sigma(T^{1/n})}{T^{1/n}}(0) = 1 \text{ pour tout } n \geq 1 \right\}.$$

Pour étudier H , considérons pour tout entier $n \geq 1$ le groupe

$$\pi_n = \left\{ \sigma \in \mathbf{Aut}_{\overline{K}}(\overline{K}((T^{1/n}))) \mid \frac{\sigma(T^{1/n})}{T^{1/n}}(0) = 1 \right\}.$$

Comme les corps $\overline{K}((T^{1/n}))$ et $\overline{K}((T))$ sont \overline{K} -isomorphes, on en déduit que les groupes $\mathbf{Aut}_{\overline{K}}(\overline{K}((T^{1/n})))$ et $(\mathcal{O}_{\overline{K}}^\times, *)$ sont isomorphes. Le sous-groupe π_n correspond alors dans ce groupe au sous-groupe $(1 + \mathfrak{M}, *)$, un isomorphisme étant

$$f_n : \pi_n \rightarrow 1 + \mathfrak{M}, \quad \sigma \mapsto \frac{\sigma(T^{1/n})}{T^{1/n}}.$$

Pour $m = kn$, définissons le morphisme

$$\varphi_{n,m} : (1 + \mathfrak{M}, *) \rightarrow (1 + \mathfrak{M}, *), \quad \alpha(T) \mapsto \alpha^{1/k}(T^k),$$

où $\alpha^{1/k}$ désigne l'unique racine k -ième de α dans $1 + \mathfrak{M}$. L'application $\varphi_{n,m}$ est bien un morphisme (injectif) puisque

$$\begin{aligned} \varphi_{n,m}(\alpha * \beta)(T) &= (\alpha * \beta)^{1/k}(T^k) = (\alpha(T)\beta(T\alpha(T)))^{1/k}(T^k) \\ &= (\alpha^{1/k}(T) \cdot \beta^{1/k}(T\alpha(T)))(T^k) \\ &\quad (\text{car dans } 1 + \mathfrak{M}, \text{ on a } (\alpha \cdot \beta)^{1/k} = \alpha^{1/k} \cdot \beta^{1/k}) \\ &= \alpha^{1/k}(T^k) \cdot \beta^{1/k}(T^k \alpha(T^k)) \\ &= (\varphi_{n,m}(\alpha) * \varphi_{n,m}(\beta))(T). \end{aligned}$$

Il est alors clair que le système $(1 + \mathfrak{M}, \varphi_{n,m})_n$ est inductif (l'ensemble ordonné $(\mathbb{N}^*, |)$ est filtrant à droite). En posant, pour tout $n | m$,

$$\theta_{n,m} = f_m^{-1} \circ \varphi_{n,m} \circ f_n$$

on obtient alors un diagramme

$$\begin{array}{ccc} \pi_n & \xrightarrow{f_n} & 1 + \mathfrak{M} \\ \downarrow \theta_{n,m} & & \downarrow \varphi_{n,m} \\ \pi_m & \xrightarrow{f_m} & 1 + \mathfrak{M} \end{array}$$

commutatif. Il s'ensuit que le système $(\pi_n, \theta_{n,m})_n$ est inductif et que

$$\varinjlim \pi_n = \varinjlim (1 + \mathfrak{M}).$$

On a alors

PROPOSITION 9. *On a un isomorphisme*

$$H \simeq \varinjlim (1 + \mathfrak{M}).$$

Preuve. On va montrer que H satisfait la propriété universelle qui définit $\varinjlim \pi_n$. Pour cela, on doit commencer par expliciter, pour tous les entiers $n \neq 0$, des morphismes $h_n : \pi_n \rightarrow H$ qui font commuter les diagrammes (i.e. pour tout $n \mid m$, $h_n = h_m \circ \theta_{n,m}$).

Soit $\sigma_n \in \pi_n$. On définit $\sigma (= h_n(\sigma_n))$ pour tout entier $h \in \mathbb{N}^*$ et tout $S = S_h \in \overline{K}((T^{1/h}))$ par

$$\sigma(S) = \theta_{n,nh}(\sigma_n)(S_h),$$

c'est-à-dire que σ est défini sur $\overline{K}((T^{1/h}))$ par

$$\sigma(T^{1/h}) = T^{1/h} \alpha_n^{n/h} (T^{1/n})$$

avec $\alpha_n = f_n(\sigma_n)$ et où $\alpha_n^{1/h}$ désigne l'unique racine h -ième de α_n dans $1 + \mathfrak{M}$.

Cette définition ne dépend pas du choix de l'entier h . En effet, si $h' = sh$, alors

$$\begin{aligned} \theta_{n,nh'}(\sigma_n)(T^{1/h}) &= (\theta_{n,nh'}(\sigma_n)(T^{1/h'}))^s = (T^{1/h'} \alpha_n^{n/h'} (T^{1/n}))^s \\ &= T^{1/h} \alpha_n^{n/h} (T^{1/n}) = \theta_{n,nh}(\sigma_n)(T^{1/h}). \end{aligned}$$

L'application σ est un \overline{K} -automorphisme. En effet, si $S_h, S_{h'}$ sont deux éléments de $\mathbf{Puis}(\overline{K})$, alors $S_h - S_{h'}$ et $S_h \cdot S_{h'}^{-1}$ sont dans $\overline{K}((T^{1/hh'}))$ et donc

$$\begin{aligned} \sigma(S_h - S_{h'}) &= \theta_{n,nhh'}(\sigma_n)(S_h - S_{h'}) = \sigma(S_h) - \sigma(S_{h'}), \\ \sigma(S_h \cdot S_{h'}^{-1}) &= \theta_{n,nhh'}(\sigma_n)(S_h S_{h'}^{-1}) = \sigma(S_h) \cdot \sigma(S_{h'})^{-1}, \end{aligned}$$

c'est-à-dire que σ est un morphisme de corps. Il est visiblement surjectif, car $\sigma|_{\overline{K}((T^{1/m}))} \in \pi_m$ pour tout $n \mid m$, ce qui assure aussi, pour finir, que $\sigma \in H$.

Il est alors clair que l'application h_n ainsi obtenue est un morphisme de groupes qui satisfait, pour tout $n \mid m$,

$$h_n = h_m \circ \theta_{n,m}.$$

Ce morphisme est visiblement injectif, car $h_n(\sigma_n)|_{\overline{K}((T^{1/n}))} = \sigma_n$.

Considérons maintenant un groupe H' et pour tout $n \in \mathbb{N}^*$ des morphismes $h'_n : \pi_n \rightarrow H'$ qui font commuter les diagrammes. Prenons un élément $\sigma \in H$. Il existe un entier $n \neq 0$ tel que

$$\sigma(T) = T \cdot \alpha(T^{1/n})$$

avec $\alpha(0) = 1$. Par suite, on a

$$\sigma(T^{1/n}) = T^{1/n} \cdot \alpha^{1/n}(T^{1/n})$$

où $\alpha^{1/n}$ désigne l'unique racine n -ième de α vérifiant $\alpha^{1/n}(0) = 1$. On en déduit donc que pour cet entier $n \geq 1$, la restriction $\sigma|_{\overline{K}((T^{1/n}))}$ est un élément $\sigma_n \in \pi_n$. On pose alors

$$\Xi(\sigma) = h'_n(\sigma_n).$$

Puisque le système est inductif, on voit bien que la valeur de $h'_n(\sigma_n)$ ne dépend pas du choix de n et donc cela permet de définir une application $\Xi : H \rightarrow H'$ qui fait commuter les diagrammes (i.e. pour tout $n \neq 0$, on a $h'_n = \Xi \circ h_n$). On voit aussi que Ξ est unique pour cette propriété. Il s'ensuit que H satisfait la propriété universelle qui définit $\varinjlim \pi_n$. ■

On déduit donc de ce qui précède le

THÉORÈME 10. *Si K désigne un corps de caractéristique 0, alors le groupe des K -automorphismes continus du corps $\mathbf{Puis}(\overline{K})$ est isomorphe à*

$$\mathbf{Aut}_K(\mathbf{Puis}(\overline{K})) \simeq (\mathbf{G}_K \times \mathbb{Q}^{*+}) \times (\varinjlim \overline{K}^* \times \varinjlim (1 + \mathfrak{M})).$$

De manière pratique on retiendra que, si $\tau \in \mathbf{Aut}_K(\mathbf{Puis}(\overline{K}))$, on a

$$\tau\left(\sum_{k \geq k_0} a_k T^{k/n}\right) = \sum_{k \geq k_0} \tau(a_k) \tau(T^{1/n})^k$$

(τ est entièrement déterminé par son action sur \overline{K} et sur les $T^{1/n}$), et si on écrit $\tau = g r \sigma \mu$ avec $g \in \mathbf{G}_K$, $r = p/q \in \mathbb{Q}^{*+}$, $\sigma \in M$ et $\mu \in H$, il existe une suite $(\xi_n)_{n \geq 1} \in \overline{K}^{*\mathbb{N}^*}$ vérifiant $\xi_{nm}^m = \xi_n$ pour tous $n, m \geq 1$, un élément $\alpha \in 1 + \mathfrak{M}_{\overline{K}}$ et un entier $N \geq 1$ tel que pour tout $a \in \overline{K}$,

$$g(a) = g(a), \quad r(a) = a, \quad \sigma(a) = a, \quad \mu(a) = a,$$

et tout $n \in \mathbb{N}^*$,

$$\begin{aligned} g(T^{1/n}) &= T^{1/n}, & \sigma(T^{1/n}) &= \xi_n T^{1/n}, \\ r(T^{1/n}) &= T^{r/n} = (T^{1/qn})^p, & \mu(T^{1/n}) &= T^{1/n} \alpha^{N/n} (T^{1/N}), \end{aligned}$$

où $\alpha^{1/n}$ désigne l'unique racine n -ième de α dans $1 + \mathfrak{M}_{\overline{K}}$. On notera alors $\mu = (\alpha, N)$ et $\sigma = (\xi_n)_n$.

4. Applications

4.1. Des sous-groupes de $\mathbf{Aut}(\mathbb{C})$. On peut appliquer ce que nous venons de faire à la description de certains sous-groupes de $\mathbf{Aut}(\mathbb{C})$. En effet, on a la proposition suivante :

PROPOSITION 11. *Soient Ω_1 et Ω_2 deux corps algébriquement clos de même caractéristique et de même cardinal indénombrable. Les corps Ω_1 et Ω_2 sont alors isomorphes.*

Preuve. Les corps Ω_1 et Ω_2 étant de même caractéristique ont des sous-corps premiers F_1 et F_2 isomorphes. Considérons des extensions transcendentes pures maximales, $F_1(X_i)_{i \in I}$ et $F_2(Y_j)_{j \in J}$, de F_1 et F_2 dans Ω_1 et Ω_2 . Pour des raisons évidentes de cardinalité, on a

$$\sharp I = \sharp \Omega_1 = \sharp \Omega_2 = \sharp J.$$

Ceci implique que $F_1(X_i)_{i \in I}$ et $F_2(Y_j)_{j \in J}$ sont isomorphes et, par application du théorème de Steinitz, que Ω_1 et Ω_2 le sont aussi. ■

On en déduit donc que, par exemple, les corps $\mathbb{C}, \mathbb{C}_p, \overline{\mathbb{Q}}_p, \mathbf{Puis}(\mathbb{C})$ sont tous isomorphes. On en déduit aussi que si K est un corps de cardinal $\leq 2^{\aleph_0}$ et de caractéristique nulle, alors \mathbb{C} et $\mathbf{Puis}(\overline{K})$ sont isomorphes. Par suite, en appliquant le théorème 10, on trouve que

THÉORÈME 12. *Si K désigne un corps de caractéristique 0 et de cardinal $\leq 2^{\aleph_0}$, alors le groupe de Galois absolu, $G_K = \mathbf{Gal}(\overline{K}/K)$, de K est un sous-groupe de $\mathbf{Aut}(\mathbb{C})$.*

En particulier, $G_{\mathbb{Q}}$ est un sous-groupe. De même, les groupes \widehat{F}_{\aleph_0} et $\widehat{F}_{2^{\aleph_0}}$ (les groupes prolibres à, respectivement, \aleph_0 et 2^{\aleph_0} générateurs) sont des sous-groupes de $\mathbf{Aut}(\mathbb{C})$. En effet, considérons un élément $x \in \mathbb{C}$ transcendant sur \mathbb{Q} (resp. une famille $(x_i)_{i \in 2^{\aleph_0}}$ d'éléments \mathbb{Q} -algébriquement indépendants de \mathbb{C}) et le corps

$$K = \overline{\mathbb{Q}}(x) \quad (\text{resp. } K = \overline{\mathbb{Q}(x_i)_{i \neq i_0}(x_{i_0})});$$

alors, en conséquence du théorème d'Harbater (voir [Har]), on sait que $G_K \simeq \widehat{F}_{\aleph_0}$ (resp. $G_K \simeq \widehat{F}_{2^{\aleph_0}}$).

4.2. Des involutions continues de Puiseux. Le résultat arithmétique fondamental de la théorie d'Artin–Schreier (dont le lecteur pourra trouver un exposé dans [Rib2]) établit la correspondance qui existe entre les éléments de torsion du groupe $\mathbf{Aut}(\mathcal{A})$ des automorphismes du corps algébriquement clos \mathcal{A} et certains sous-corps ordonnables de \mathcal{A} . Plus précisément si \mathcal{A} est de caractéristique non nulle alors $\mathbf{Aut}(\mathcal{A})$ est sans torsion et \mathcal{A} ne contient aucun sous-corps ordonnable. Si maintenant \mathcal{A} est de caractéristique nulle alors $\mathbf{Aut}(\mathcal{A})$ contient de la torsion et tous les éléments de torsion sont des involutions. Si $c \in \mathbf{Aut}(\mathcal{A})$ est une involution, alors le corps $R_c = \mathcal{A}^{(c)}$ des éléments de \mathcal{A} invariants par l'action de c est un corps réel clos (i.e. un corps ordonné qui ne possède aucune extension ordonnée algébrique stricte ; un tel corps possède un unique ordre compatible). Réciproquement, si R désigne

un sous-corps réel clos ⁽¹⁾ de \mathcal{A} , alors $[\mathcal{A} : R] = 2$ et $\mathcal{A} = R(\sqrt{-1})$. En particulier $\mathbf{Gal}(\mathcal{A}/R)$ permet de définir une involution de $\mathbf{Aut}(\mathcal{A})$.

Un calcul assez simple montre alors que si R et R' sont deux sous-corps réels clos de \mathcal{A} et c, c' sont les deux involutions de $\mathbf{Aut}(\mathcal{A})$ associées respectivement à R et R' , alors pour tout corps K contenu dans $R \cap R'$, les corps R et R' sont K -isomorphes si et seulement si c et c' sont K -conjugués (i.e. conjugués dans le groupe $\mathbf{Aut}_K(\mathcal{A})$ des K -automorphismes de \mathcal{A}). Plus exactement, si $\sigma \in \mathbf{Aut}_K(\mathcal{A})$ est tel que $\sigma(R) = R'$ alors $c' = \sigma c \sigma^{-1}$ et réciproquement. Ainsi, il existe une correspondance bi-univoque entre les classes de conjugaison des involutions dans $\mathbf{Aut}_K(\mathcal{A})$ et les classes de K -isomorphisme de sous-corps réels clos de \mathcal{A} .

Une question légitime d'arithmétique des corps consiste alors à s'interroger sur la possibilité d'une éventuelle "description", pour un corps algébriquement clos \mathcal{A} de caractéristique 0 donné et un sous-corps K de \mathcal{A} fixé, de certaines classes de conjugaison des involutions dans $\mathbf{Aut}_K(\mathcal{A})$. Par exemple, dans le cas où $\mathcal{A} = \overline{K}$ est la clôture algébrique du corps K , la théorie des corps ordonnés permet une description en terme d'ordres compatibles de toutes les classes de conjugaison des involutions dans $\mathbf{Aut}_K(\mathcal{A}) = \mathbf{Gal}(\overline{K}/K)$. Plus précisément, il existe une correspondance bi-univoque entre l'ensemble des classes de conjugaison des involutions de $\mathbf{Gal}(\overline{K}/K)$ et l'ensemble des ordres compatibles sur K (i.e. les relations d'ordres qui font de K un corps ordonné).

Cette correspondance est établie de la manière suivante : à un ordre compatible \leq sur K on associe l'ensemble $\mathcal{C}(\leq)$ des involutions $c \in \mathbf{Gal}(\overline{K}/K)$ telles que le corps réel clos $R_c = \overline{K}^{(c)}$ soit une extension ordonnée de (K, \leq) (i.e. une extension dont l'ordre prolonge \leq). L'ensemble $\mathcal{C}(\leq)$ est non vide, car on sait (cf. [Rib2, Ch. IX, 3.h]) qu'il existe toujours un corps ordonné maximal R , extension algébrique ordonnée de (K, \leq) . Si c, c' sont deux éléments de $\mathcal{C}(\leq)$, les corps R_c et $R_{c'}$ sont alors deux extensions ordonnées algébriques de (K, \leq) et un corollaire du théorème de Sturm affirme alors qu'il existe un (unique) K -isomorphisme σ entre R et R' (cf. [Rib2, Ch. IX, 5, Th. 9]). Un relevé de σ dans $\mathbf{Gal}(\overline{K}/K)$ conjugue alors c et c' . Réciproquement, si c est un élément de $\mathcal{C}(\leq)$, $c' \in \mathbf{Gal}(\overline{K}/K)$ est une involution et $\sigma \in \mathbf{Gal}(\overline{K}/K)$ un K -automorphisme tel que $c' = \sigma c \sigma^{-1}$, alors $\sigma(R_c) = R_{c'}$. Comme l'unique ordre existant sur un corps réel clos est défini par ses carrés, l'isomorphisme σ préserve donc l'ordre et, par suite, le corps $R_{c'}$ est lui aussi une extension ordonnée de (K, \leq) . Il s'ensuit que $\mathcal{C}(\leq)$ est, en fait, une classe de conjugaison dans $\mathbf{Gal}(\overline{K}/K)$ d'involutions.

⁽¹⁾ Dans ce texte la terminologie de *sous-corps réel clos d'un corps algébriquement clos* \mathcal{A} désignera un sous-corps R de \mathcal{A} tel que \mathcal{A}/R soit une extension algébrique et tel que R soit un corps réel clos.

La correspondance $\leq \mapsto \mathcal{C}(\leq)$ est bien sur surjective car si c est une involution de $\mathbf{Gal}(\overline{K}/K)$, l'ordre du corps réel clos R_c induit, par restriction, un ordre compatible sur K qui est un antécédent pour notre correspondance de la classe de conjugaison de c . Cette correspondance est, par ailleurs, bien injective puisque deux ordres compatibles sur K qui ont mêmes images par la correspondance sont tous deux restriction à K de l'ordre unique d'un sous-corps réel clos de \overline{K} et sont, par suite, égaux.

On déduit de ce résultat que, par exemple, dans le cas de $K = \mathbb{Q}$, il n'y a qu'une seule classe de conjugaison d'involutions dans $\mathbf{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, dans le cas de $K = \mathbb{Q}(\sqrt{2})$ il y a deux classes dans $\mathbf{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\sqrt{2}))$ et dans le cas $K = \mathbb{Q}(T)$ il y a une infinité de classes dans $\mathbf{Gal}(\overline{\mathbb{Q}(T)}/\mathbb{Q}(T))$.

La question de la description des classes de conjugaison d'involutions se précise par exemple lorsque le corps \mathcal{A} est un corps topologique et que l'on veut regarder les classes de conjugaison des involutions continues. Par exemple si l'on considère $\mathcal{A} = \mathbb{C}$ muni de la topologie usuelle, il n'y a qu'une seule telle classe (celle de la conjugaison complexe, qui constitue le seul automorphisme non trivial de \mathbb{C} continu). On s'intéresse dans cette partie à cette question dans le cas d'un corps de séries de Puiseux muni de sa topologie naturelle.

Considérons une involution $c \in G_K$. S'il n'y a pas d'ambiguïté, pour $a \in \overline{K}$, on notera \bar{a} à la place de $c(a)$. Si $\alpha(T) = 1 + a_1T + a_2T^2 + \dots \in 1 + \mathfrak{M}_{\overline{K}}$, on notera

$$\bar{\alpha}(T) = 1 + \bar{a}_1T + \bar{a}_2T^2 + \dots$$

On remarque que pour tout $\alpha, \beta \in 1 + \mathfrak{M}_{\overline{K}}$ on a $\overline{\alpha * \beta} = \bar{\alpha} * \bar{\beta}$ et donc qu'en particulier $\alpha^{(-1)} = \bar{\alpha}^{(-1)}$ (nous noterons dans ce texte $\alpha^{(-1)}$ l'inverse pour $*$ de α afin de ne pas confondre avec l'inverse pour le produit au sens de Cauchy). On considère l'ensemble

$$\mathbb{U}(c) = \{a \in \overline{K} \mid a \cdot \bar{a} = 1\},$$

qui est visiblement un sous-groupe de \overline{K}^* . Ce groupe a la propriété suivante : si $x \in \mathbb{U}(c)$, $y \in \overline{K}$ et $n \in \mathbb{N}^*$ sont tels que $x = y^n$ alors $y \in \mathbb{U}(c)$. En effet, le corps R_c est corps réel clos et comme, par hypothèses, on a $(y\bar{y})^n = 1$ et $y\bar{y} \in R_c$, on en déduit que l'élément $y\bar{y}$ est une racine de l'unité d'un corps réel clos. On a donc $y\bar{y} = \pm 1$. Par ailleurs, comme $\overline{K} = R_c(\sqrt{-1})$, si $y = y_0 + \sqrt{-1}y_1$ avec $y_0, y_1 \in R_c$, on a $y\bar{y} = y_0^2 + y_1^2 \geq 0$. Ainsi $y\bar{y} = 1$, c'est-à-dire $y \in \mathbb{U}(c)$.

Pour tout $\lambda \in \overline{K}^*$, on note

$$\Omega(c, \lambda) = \{\alpha \in 1 + \mathfrak{M}_{\overline{K}} \mid \alpha(\lambda T) * \bar{\alpha}(T) = 1\}.$$

On a alors :

PROPOSITION 13. *Un élément $\tau \in \text{Aut}_K(\mathbf{Puis}(\overline{K}))$ est une involution si et seulement si $\tau = c\sigma\mu$ où $c \in G_K$, $\sigma = (\xi_n)_n \in M$ et $\mu = (\alpha, N) \in H$ sont des éléments vérifiant :*

- c est une involution de G_K ,
- $\xi_N \in \mathbb{U}(c)$,
- $\alpha \in \Omega(c, \xi_N)$.

Preuve. Supposons que l'élément $\tau = gr\sigma\mu$ soit une involution avec $g \in G_K$, $r = p/q \in \mathbb{Q}^{+*}$, $\sigma = (\xi_n)_n \in M$ et $\mu = (\alpha, N) \in H$. Comme $\text{Aut}_K(\mathbf{Puis}(\overline{K}))$ est un produit semi-direct $(G_K \times \mathbb{Q}^{+*}) \ltimes (M \ltimes H)$, l'élément gr satisfait $(gr)^2 = \text{Id}$ et, par suite, on a $r = 1$ et $g = \text{Id}$ ou g involution. Supposons que $g = \text{Id}$; la restriction de τ à \overline{K} étant g , on en déduit que \overline{K} est contenu dans le sous-corps de $\mathbf{Puis}(\overline{K})$ laissé fixe par τ . Ceci est impossible car ce sous-corps est ordonnable et $\sqrt{-1} \in \overline{K}$. Ainsi $g = c$ est une involution de G_K .

Fixons un entier $n \in \mathbb{N}^*$ et regardons maintenant l'action de $\tau^2 = (c\sigma\mu)^2$ sur l'élément $T^{1/n}$. On a

$$\begin{aligned} \tau^2(T^{1/n}) &= c\sigma\mu c\sigma(T^{1/n}\alpha^{N/n}(T^{1/N})) = c\sigma\mu c(\xi_n T^{1/n}\alpha^{N/n}(\xi_N T^{1/N})) \\ &= c\sigma\mu(\overline{\xi}_n T^{1/n}\overline{\alpha}^{N/n}(\overline{\xi}_N T^{1/N})) \\ &= c\sigma(\overline{\xi}_n T^{1/n}\alpha^{N/n}(T^{1/N})\overline{\alpha}^{N/n}(\overline{\xi}_N T^{1/N}\alpha(T^{1/N}))) \\ &= c(\overline{\xi}_n \xi_n T^{1/n}\alpha^{N/n}(\xi_N T^{1/N})\overline{\alpha}^{N/n}(\overline{\xi}_N \xi_N T^{1/N}\alpha(\xi_N T^{1/N}))) \\ &= \xi_n \overline{\xi}_n T^{1/n}\overline{\alpha}^{N/n}(\overline{\xi}_N T^{1/N})\alpha^{N/n}(\xi_N \overline{\xi}_N T^{1/N}\overline{\alpha}(\overline{\xi}_N T^{1/N})) = T^{1/n}. \end{aligned}$$

Le terme constant de $\overline{\alpha}^{N/n}(\overline{\xi}_N T^{1/N})\alpha^{N/n}(\xi_N \overline{\xi}_N T^{1/N}\overline{\alpha}(\overline{\xi}_N T^{1/N}))$ étant 1, on en déduit que $\xi_n \overline{\xi}_n = 1$ pour tout $n \in \mathbb{N}^*$, donc en particulier $\xi_N \in \mathbb{U}(c)$. Il s'ensuit, en prenant $n = N$ et en appliquant à nouveau c à l'égalité, que

$$\alpha(\xi_N T^{1/N})\overline{\alpha}(T^{1/N}\alpha(\xi_N T^{1/N})) = 1,$$

c'est-à-dire que $\alpha(\xi_N T) * \overline{\alpha}(T) = 1$ (i.e. $\alpha \in \Omega(c, \xi_N)$).

Réciproquement, si $\xi_N \in \mathbb{U}(c)$, la remarque précédant l'énoncé de la proposition 13 assure alors que $\xi_{nN} \in \mathbb{U}(c)$ pour tout $n \geq 1$ et, par suite, que $\xi_n = \xi_{nN}^N \in \mathbb{U}(c)$. Le calcul précédent montre alors que, sous les hypothèses, $\tau = c\sigma\mu$ est bien une involution. ■

On s'intéresse maintenant aux classes de conjugaisons dans le groupe $\mathbf{Aut}_K(\mathbf{Puis}(\overline{K}))$ des involutions continues ainsi qu'aux classes de K -isomorphismes de sous-corps réels clos (contenant K) de $\mathbf{Puis}(\overline{K})$ associées. On dira dans la suite qu'un sous-corps réel clos (contenant K) de $\mathbf{Puis}(\overline{K})$ est continu si l'involution de $\mathbf{Aut}_K(\mathbf{Puis}(\overline{K}))$ qui le définit est elle-même continue.

THÉORÈME 14. *Soient $\tau = c\sigma\mu$ et $\tau' = c'\sigma'\mu'$ deux involutions continues de $\mathbf{Puis}(\overline{K})$. Les propriétés suivantes sont équivalentes :*

- (i) τ et τ' sont continûment conjuguées (c'est-à-dire conjuguées dans $\mathbf{Aut}_K(\mathbf{Puis}(\overline{K}))$),
- (ii) τ et τ' sont conjuguées dans $\mathbf{Aut}_K(\mathbf{Puis}(\overline{K}))$,
- (iii) $\tau|_{\overline{K}} = c$ et $\tau'|_{\overline{K}} = c'$ sont conjuguées dans \mathbf{G}_K .

En particulier, il existe une correspondance bi-univoque entre les classes de K -isomorphisme de sous-corps réels clos continus de $\mathbf{Puis}(\overline{K})$ et les classes de K -isomorphisme de sous-corps réels clos de \overline{K} ; cette correspondance est celle qui à un représentant R d'une classe d'isomorphisme de \overline{K} associe la classe d'isomorphisme de $\mathbf{Puis}(R)$.

Preuve. (ii) \Rightarrow (iii). Si $\pi \in \mathbf{Aut}_K(\mathbf{Puis}(\overline{K}))$ conjugue τ et τ' , alors $\pi|_{\overline{K}}$ conjugue c et c' .

(iii) \Rightarrow (i). Soient $\tau' = c'\sigma'\mu'$ une involution continue de $\mathbf{Puis}(\overline{K})$, $c \in \mathbf{G}_K$ une involution et $g \in \mathbf{G}_K$ telle que $c = g^{-1}c'g$. Nous allons montrer que τ' est continûment conjuguée à c (vue comme élément de $\mathbf{Aut}_K(\mathbf{Puis}(\overline{K}))$), ce qui prouvera le théorème. Posons $\sigma' = (\xi_n)_n$ et $\mu' = (\alpha, N)$ et conjuguons τ' par g :

$$g^{-1}\tau'g = (g^{-1}c'g)(g^{-1}\sigma'g)(g^{-1}\mu'g) = c\sigma''\mu''$$

avec $\sigma'' = (u_n)_n \in M$ où $u_n = g^{-1}(\xi_n)$ pour tout $n \geq 1$ et $\mu'' = (\beta, N) \in H$ où $\beta = \alpha^{g^{-1}}$ désigne l'élément de $1 + \mathfrak{M}_{\overline{K}}$ dont les coefficients sont obtenus à partir de ceux de α par application de g^{-1} . En effet, pour $n \geq 1$ on a

$$g^{-1}\sigma'g(T^{1/n}) = g^{-1}\sigma'(T^{1/n}) = g^{-1}(\xi_n T^{1/n}) = g^{-1}(\xi_n)T^{1/n} = u_n T^{1/n}$$

et

$$g^{-1}\mu'g(T^{1/n}) = g^{-1}(T^{1/n}\alpha^{N/n}(T^{1/N})) = T^{1/n}(\alpha^{g^{-1}})^{N/n}(T^{1/N}).$$

Considérons maintenant l'élément $s = (s_n)_n \in M$ défini par $s_n = u_{2n}^{-1}$ pour tout $n \geq 1$, et conjuguons $c\sigma''\mu''$ par s :

$$s^{-1}(c\sigma''\mu'')s = c\mu'''$$

où $\mu''' = (\beta(s_N^{-1}T), N) = (\gamma, N)$. En effet, pour $n \geq 1$ on a $u_n \in \mathbb{U}(c)$ et, par suite, $s_n \in \mathbb{U}(c)$. On a donc $s_n^{-1}\overline{u_n s_n} = u_{2n}u_n^{-1}u_{2n} = u_{2n}^2u_n^{-1} = u_nu_n^{-1} = 1$ et ainsi

$$s^{-1}\sigma''s(T^{1/n}) = s_n^{-1}\overline{u_n s_n}T^{1/n} = T^{1/n}.$$

Par ailleurs, on a

$$s^{-1}\mu''s(T^{1/n}) = s_n^{-1}s_nT^{1/n}\beta^{N/n}(s_N^{-1}T^{1/N}).$$

Pour finir la preuve du théorème, nous avons besoin du lemme suivant :

LEMME 15. *Soit $c \in \mathbf{G}_K$ une involution et $\alpha \in \Omega(c, 1)$. Il existe $\beta \in 1 + \mathfrak{M}_{\overline{K}}$ tel que $\overline{\beta^{(-1)}} * \alpha * \beta = 1$.*

Preuve. La condition $\alpha \in \Omega(c, 1)$ est équivalente à $\alpha * \bar{\alpha} = 1$. Étant donné $\alpha, \beta \in 1 + \mathfrak{M}_{\bar{K}}$, disons

$$\begin{aligned} \alpha(T) &= a_0 + a_1T + a_2T^2 + \dots \quad (a_0 = 1), \\ \beta(T) &= b_0 + b_1T + b_2T^2 + \dots \quad (b_0 = 1), \end{aligned}$$

on a

$$\begin{aligned} \beta(T\alpha(T)) &= 1 + \sum_{n \geq 1} b_n T^n \left(\sum_{k \geq 0} a_k T^k \right)^n \\ &= 1 + \sum_{n \geq 1} b_n T^n \left(\sum_{k \geq 0} \left(\sum_{i_1 + \dots + i_n = k} a_{i_1} \dots a_{i_n} \right) T^k \right) \\ &= 1 + \sum_{n \geq 1} \sum_{k \geq 0} b_n \left(\sum_{i_1 + \dots + i_n = k} a_{i_1} \dots a_{i_n} \right) T^{n+k} \\ &= 1 + \sum_{m \geq 1} \left(\sum_{k=0}^{m-1} b_{m-k} \sum_{i_1 + \dots + i_{m-k} = k} a_{i_1} \dots a_{i_{m-k}} \right) T^m \\ &= \sum_{m \geq 0} \lambda_m T^m \quad (\lambda_0 = 1) \end{aligned}$$

et, compte tenu du fait que

$$\alpha(T) \cdot \beta(T\alpha(T)) = \sum_{n \geq 0} \left(\sum_{m=0}^n \lambda_m a_{n-m} \right) T^n,$$

on trouve finalement

$$(\alpha * \beta)(T) = 1 + \sum_{n \geq 1} \left(a_n + \sum_{m=1}^n \sum_{k=0}^{m-1} a_{n-m} b_{m-k} \sum_{i_1 + \dots + i_{m-k} = k} a_{i_1} \dots a_{i_{m-k}} \right) T^n.$$

Ainsi, $\alpha \in \Omega(c, 1)$ ssi pour tout $n \geq 1$ on a

$$(E_n) \quad a_n + \sum_{m=1}^n \sum_{k=0}^{m-1} a_{n-m} \bar{a}_{m-k} \sum_{i_1 + \dots + i_{m-k} = k} a_{i_1} \dots a_{i_{m-k}} = 0.$$

L'existence d'un $\beta \in 1 + \mathfrak{M}_{\bar{K}}$ tel que $\overline{\beta^{(-1)}} * \alpha * \beta = 1$ équivaut donc, sous l'hypothèse précédente, à l'existence d'une suite $(b_n)_n$ d'éléments de \bar{K} tels que $b_0 = 1$ et, pour tout $n \geq 1$,

$$(F_n) \quad a_n + \sum_{m=1}^n \sum_{k=0}^{m-1} a_{n-m} b_{m-k} \sum_{i_1 + \dots + i_{m-k} = k} a_{i_1} \dots a_{i_{m-k}} = \bar{b}_n.$$

On voit alors que le choix $b_n = \bar{a}_n/2$ pour tout $n \geq 1$ permet de passer de l'équation (E_n) à l'équation (F_n) . Ainsi, le choix $\beta = (\bar{\alpha} + 1)/2$ fournit l'élément recherché. ■

On a $\gamma \in \Omega(c, 1)$. Considérons un élément $\delta \in 1 + \mathfrak{M}_{\bar{K}}$ tel que $\overline{\delta^{(-1)}} * \gamma * \delta = 1$ et l'élément $\nu = (\delta, N) \in H$. Pour tout $n \geq 1$ on a

$$\begin{aligned} \nu^{-1}c\mu''' \nu(T^{1/n}) &= \nu^{-1}c\mu'''(T^{1/n} \cdot \delta^{N/n}(T^{1/N})) \\ &= \nu^{-1}c(T^{1/n} \cdot \gamma^{N/n}(T^{1/N}) \cdot \delta^{N/n}(T^{1/N} \gamma(T^{1/N}))) \\ &= \nu^{-1}(T^{1/n} \cdot \bar{\gamma}^{N/n}(T^{1/N}) \cdot \bar{\delta}^{N/n}(T^{1/N} \bar{\gamma}(T^{1/N}))) \\ &= T^{1/n} \cdot \delta^{(-1)N/n}(T^{1/N}) \cdot \bar{\gamma}^{N/n}(T^{1/N} \delta^{(-1)}(T^{1/N})) \\ &\quad \cdot \bar{\delta}^{N/n}(T^{1/N} \delta^{(-1)}(T^{1/N}) \bar{\gamma}(T^{1/N} \delta^{(-1)}(T^{1/N}))) \\ &= T^{1/n} \cdot (\delta^{(-1)}(T^{1/N}) \cdot \bar{\gamma}^{N/n}(T^{1/N} \delta^{(-1)}(T^{1/N})) \\ &\quad \cdot \bar{\delta}(T^{1/N} \delta^{(-1)}(T^{1/N}) \bar{\gamma}(T^{1/N} \delta^{(-1)}(T^{1/N}))))^{N/n} \\ &= T^{1/n}(\delta^{(-1)} * \bar{\gamma} * \bar{\delta})^{N/n}(T^{1/N}) = T^{1/n} \end{aligned}$$

et par suite $\nu^{-1}c\mu''' \nu = c$.

En résumé, l'élément $\omega = gs\nu$ conjugue (continûment) l'involution $c'\sigma'\mu'$ en c .

La conclusion du théorème est alors immédiate une fois constaté que si $c \in G_K$ est une involution et que $R = \bar{K}^{(c)}$ désigne le sous-corps réel clos des éléments invariants de \bar{K} par l'action de c , alors le sous-corps réel clos des éléments invariants de $\mathbf{Puis}(\bar{K})$ par l'action de c (vu comme élément de $\mathbf{Aut}_K(\mathbf{Puis}(\bar{K}))$) est $\mathbf{Puis}(R)$. ■

Compte tenu de la correspondance établie dans l'introduction du §4 entre l'ensemble des classes de conjugaison d'involution de $\mathbf{Gal}(\bar{K}/K)$ et l'ensemble des ordres compatibles sur K , on obtient le

COROLLAIRE 16. *Soit K un corps de caractéristique nulle. Il existe une correspondance bi-univoque entre l'ensemble des ordres compatibles sur K et l'ensemble des classes de K -isomorphisme de sous-corps réels clos continus de $\mathbf{Puis}(\bar{K})$. Cette correspondance est celle qui à un ordre compatible \leq de K associe la classe du corps $\mathbf{Puis}(R_{\leq})$ où R_{\leq} désigne une extension ordonnée algébrique maximale du corps ordonné (K, \leq) .*

REMARQUES. (a) Une classe de conjugaison dans $\mathbf{Aut}_K(\mathbf{Puis}(\bar{K}))$ d'une involution continue n'est pas forcément composée d'involution continues. Nous allons, en effet, montrer ci-dessous que pour tout corps K ordonnable, il existe des conjugués d'involution continues qui ne sont pas continus (ceci assurera, en particulier, que le groupe $\mathbf{Aut}_K(\mathbf{Puis}(\bar{K}))$ n'est jamais distingué dans le groupe $\mathbf{Aut}_K(\mathbf{Puis}(\bar{K}))$).

Pour commencer, considérons un élément $\psi \in \mathbf{Aut}_K(\mathbf{Puis}(\bar{K}))$ vérifiant $\psi(T) = T^{-1}$, dont l'existence a été prouvée au §3. Considérons alors l'élément $\varphi = c\sigma\mu$ où $c \in G_K$ désigne une involution quelconque, $\sigma = (\xi_n)_n$ avec $\xi_1 = -1$ (qui existe bien par application standard du lemme de Zorn)

et $\mu = (1/(1 - T), 1) \in H$. La proposition 13 montre que l'élément φ est une involution, puisque si l'on pose $\alpha(T) = 1/(1 - T)$ on a

$$\alpha(-T) * \bar{\alpha}(T) = \frac{1}{1+T} \cdot \frac{1}{1 - \frac{T}{1+T}} = 1.$$

Par ailleurs,

$$\psi^{-1} \circ \varphi \circ \psi(T) = \psi^{-1} \circ \varphi\left(\frac{1}{T}\right) = \psi^{-1}\left(\frac{-1 - T}{T}\right) = \frac{-1 - T^{-1}}{T^{-1}} = -1 - T.$$

L'automorphisme $\psi^{-1} \circ \varphi \circ \psi$ ne peut donc pas être continu puisque sa restriction aux groupes des unités de $\mathbf{Puis}[\bar{K}]$ n'est pas un automorphisme (lemme 4).

(b) Il existe donc des involutions non continues qui vivent dans des classes de conjugaisons d'involutions continues. Il est intéressant de remarquer que, dans certains cas au moins, il existe aussi des involutions non continues qui ne sont pas conjuguées à des involutions continues. Pour établir ce dernier point commençons par remarquer que les sous-corps réels clos continus de $\mathbf{Puis}(\bar{K})$ ne sont jamais des corps archimédiens. En effet, d'après le théorème 14, ils sont (continûment) isomorphes à des corps de séries de puissances $\mathbf{Puis}(R)$ à coefficients dans des sous-corps R réels clos de \bar{K} . Supposons qu'il existe un sous-corps réel clos R de \bar{K} tel que $\mathbf{Puis}(R)$ soit archimédien. Puisque l'ordre sur $\mathbf{Puis}(R)$ est défini par les carrés, on a $T = (\sqrt{T})^2 > 0$ et, par suite, il doit exister un entier $n \geq 1$ tel que $nT > 1$; mais comme

$$\sqrt{1 - nT} = 1 - \frac{n}{2}T - \frac{n^2}{8}T^2 - \dots \in \mathbf{Puis}(R)$$

on voit que $1 - nT > 0$, ce qui est absurde. Ainsi $\mathbf{Puis}(R)$ n'est pas archimédien et, par suite, aucun sous-corps réel clos continu de $\mathbf{Puis}(\bar{K})$.

D'après la proposition 11, les corps \mathbb{C} et $\mathbf{Puis}(\bar{\mathbb{Q}})$ sont isomorphes. Il existe donc dans $\mathbf{Puis}(\bar{\mathbb{Q}})$ une "copie" du corps des réels \mathbb{R} , mais cette copie provenant d'un isomorphisme entre \mathbb{C} et $\mathbf{Puis}(\bar{\mathbb{Q}})$, elle constitue un sous-corps réel clos de $\mathbf{Puis}(\bar{\mathbb{Q}})$ qui est archimédien et donc n'est pas continu et n'est isomorphe à aucun sous-corps réel clos continu de $\mathbf{Puis}(\bar{\mathbb{Q}})$ (puisque un isomorphisme préserve la propriété d'Archimède). L'involution définie par cette copie de \mathbb{R} dans $\mathbf{Puis}(\bar{\mathbb{Q}})$ constitue donc un exemple d'involution de $\mathbf{Aut}(\mathbf{Puis}(\bar{\mathbb{Q}}))$ qui n'est pas continue et qui n'est pas conjuguée à une involution continue.

(c) Les groupes $\mathbf{Aut}(\mathbf{Puis}(\bar{\mathbb{Q}}))$ et $\mathbf{Aut}(\mathbb{C})$ sont isomorphes (puisque $\mathbf{Puis}(\bar{\mathbb{Q}})$ et \mathbb{C} sont des corps isomorphes). Dans l'introduction du §4 on a remarqué que si l'on muni \mathbb{C} de sa topologie usuelle il n'existe qu'une seule classe de conjugaison d'involution continue dans $\mathbf{Aut}(\mathbb{C})$. Notre théorème

principal montre qu'il en est de même pour $\mathbf{Aut}(\mathbf{Puis}(\overline{\mathbb{Q}}))$ si l'on muni $\mathbf{Puis}(\overline{\mathbb{Q}})$ de sa topologie naturelle (puisqu'il n'y a qu'une seule classe de conjugaison d'involutions dans $\mathbf{Aut}(\overline{\mathbb{Q}})$). On remarque toutefois que si $\mathbf{Aut}(\mathbb{C})$ ne contient qu'une seule involution continue, le groupe $\mathbf{Aut}(\mathbf{Puis}(\overline{\mathbb{Q}}))$ en contient lui une infinité (non dénombrable).

(d) En illustration des remarques précédentes on peut, à partir du théorème 10, donner des exemples explicites de sous-corps réels clos de $\mathbf{Puis}(\mathbb{C})$ qui ne sont pas des corps de séries de Puiseux, c'est-à-dire des corps de la forme $\mathbf{Puis}(R)$ avec R sous-corps réels clos de \mathbb{C} (e.g. $R = \mathbb{R}$). Si l'on prend, dans le théorème 10, $K = \mathbb{R}$, alors G_K correspond au groupe $\{\text{Id}, c\}$ où c désigne la conjugaison complexe, et si $u = (u_n)_n \in M$ est tel que $|u_n| = 1$ pour tout n , alors l'élément cu est bien une involution. Une série de Puiseux $\sum_{k \geq k_0} a_n T^{k/n}$ est alors invariante par cu si et seulement si, pour tout $k \geq k_0$, on a

$$a_k = \overline{a}_k u_n^{-k},$$

c'est-à-dire si et seulement s'il existe, pour tout $k \geq k_0$, un réel r_k tel que

$$a_k = r_k u_{2n}^{-k}.$$

Ainsi, si α désigne un réel non nul, alors l'ensemble

$$E = \left\{ \sum_{k \geq k_0} r_k e^{-i\alpha k/2n} T^{k/n} \mid n \in \mathbb{N}^*, k_0 \in \mathbb{Z}, \forall k \geq k_0, r_k \in \mathbb{R} \right\} \subset \mathbf{Puis}(\mathbb{C})$$

est un sous-corps réel clos de $\mathbf{Puis}(\mathbb{C})$ qui n'est pas un corps de séries de Puiseux.

Pour voir ce dernier point, il faut remarquer qu'étant donnés deux corps K et L , on a l'extension $\mathbf{Puis}(\overline{L})/\mathbf{Puis}(\overline{K})$ si et seulement si on a l'extension L/K et que, dans ces conditions, on a l'égalité

$$[\mathbf{Puis}(\overline{L}) : \mathbf{Puis}(\overline{K})] = [L : K].$$

Ainsi, si E était un corps de séries de Puiseux, il serait de la forme $E = \mathbf{Puis}(R)$ avec R un sous-corps réel clos de \mathbb{C} . Mais comme \mathbb{R} est visiblement un sous-corps de E , on devrait alors avoir $R = \mathbb{R}$ (sinon, on aurait $R \cdot \mathbb{R} = \mathbb{C} \subset E$ et donc $\sqrt{-1} \in E$, ce qui serait contraire au fait que E soit un corps ordonnable), et, par suite, on aurait $E = \mathbf{Puis}(\mathbb{R})$, ce qui n'est visiblement pas le cas.

Références

[Art] E. Artin, *Algebraic Numbers and Algebraic Functions*, Gordon and Breach, 1967.
 [Har] D. Harbater, *Fundamental groups and embedding problems in characteristic p* , dans : *Recent Developments in the Inverse Galois Problem*, M. D. Fried *et al.* (eds.), Contemp. Math. 186, Amer. Math. Soc., 1995, 353–369.

- [Rib1] P. Ribenboim, *The Theory of Classical Valuations*, Springer Monogr. Math., Springer, 1999.
- [Rib2] —, *L'arithmétique des corps*, Collection “Méthodes”, Hermann, 1971.
- [Ser] J.-P. Serre, *Corps locaux*, Hermann, 1960.

Département de Mathématiques
Université du Maine
Avenue Olivier Messiaen
72085 Le Mans Cedex 9, France
E-mail: Bruno.Deschamps@univ-lemans.fr

*Reçu le 9.3.2004
et révisé le 27.1.2005*

(4736)