Quelques considérations galoisiennes relatives à l'extension des constantes d'un corps de fractions tordu

Bruno Deschamps

Résumé.— Dans cet article, nous établissons plusieurs résultats relatifs à l'arithmétique d'une extension des constantes d'un corps de fractions tordu $K[t,\sigma,\delta]$. En guise d'application, nous montrons une version non commutative du théorème de Leptin-Waterhouse : pour tout groupe profini Γ, il existe un corps gauche K et une extension algébrique, extérieure et galoisienne L/K telle que $\mathrm{Gal}(L/K)\simeq\Gamma$.

Abstract.— In this article, we state several results relating to the arithmetic of a constants extension of a skew fractions field $K[t,\sigma,\delta]$. As an application, we show a non-commutative version of the Leptin-Waterhouse theorem : for any profinite group Γ, there exists a skew field K and an algebraic, outer and Galois extension L/K such that $\mathrm{Gal}(L/K)\simeq\Gamma$.

1.— Introduction et notations.

On rappelle qu'étant donné un corps K (non nécessairement commutatif) et un automorphisme σ de K, on appelle σ-dérivation toute application $\delta : K \longrightarrow K$ additive qui vérifie de plus : $\forall x,y\in K$, $\delta(xy)=\delta(x)y+\sigma(x)\delta(y)$. Quand $\sigma=\mathrm{Id}$, on retrouve la définition classique de dérivation. Les travaux de Ore (cf. [Ore]) montrent que le K-espace vectoriel gauche $K[t,\sigma,\delta]=\bigoplus_{n\geq 0}Kt^n$, muni de la loi de composition interne défini par linéarité par les relations $ta=\sigma(a)t+\delta(a)$ et $t^n.t^m=t^{n+m}$ confèrent à $K[t,\sigma,\delta]$ une structure d'anneau de Ore. C'est l'anneau des polynômes tordu par σ et δ et à coefficients dans le corps K. Le corps des fractions $K(t,\sigma,\delta)$ de $K[t,\sigma,\delta]$, constitue ainsi une généralisation du corps des fractions rationnelles $K(t)$ lorsque K est commutatif, $\sigma=\mathrm{Id}$ et $\delta=0$. Pour le lecteur non familiarisé aux fractions tordues ni à la théorie de Galois sur les corps gauches, nous le renvoyons aux livres [Coh], [Jac], [GW].

Lorsque H/K désigne une extension finie (et plus généralement algébrique) de corps commutatifs, l'arithmétique de l'extension $H(t)/K(t)$ est entièrement portée par celle de H/K. Ceci provient du fait que, l'algèbre tensorisée $H\otimes_K K(t)$ est un corps (car H est linéairement disjoint de $K(t)$ et H/K est algébrique) qui se plonge, par propriété universelle, dans le corps $H(t)$. Ce plongement est alors visiblement un $K(t)$-isomorphisme, puisque H et t sont éléments de l'image de $H\otimes_K K(t)$. Lorsque H/K est transcendante l'argument ne fonctionne plus. Par exemple, l'algèbre tensorielle $K(x)\otimes_K K(t)$ est un anneau, certes intègre, mais qui n'est pas un corps (par exemple, $1-xt$ n'est pas inversible). Lorsque H et K ne sont plus et que l'on considère des extensions de corps de fractions tordus $H(t,\sigma,\delta)/K(t,\sigma,\delta)$, on ne peut plus tensoriser et l'argument que l'on vient de donner n'a plus de sens, même lorsque H/K est finie. Pour cette raison, plutôt que de parler *d'extension des scalaires* comme il est d'usage de le faire dans le cas commutatif, on parlera *d'extension des constantes* pour l'étude de l'arithmétique des extensions $H(t,\sigma,\delta)/K(t,\sigma,\delta)$.

0. Classification AMS 2020 : 12E15, 12E30, 16K40, 16K50.

Ces dernières années, plusieurs travaux ont étudié le Problème Inverse de Galois sur ces corps de fractions tordus (voir, par exemple, [Des], [DL], [Beh], [BDL]). Jusqu'à maintenant, l'étude du Problème Inverse de Galois sur un corps de fractions tordus $K(t,\sigma,\delta)$ a surtout consisté à utiliser la méthode « géométrique » de l'extension des scalaire : l'idée consistait à prendre des extensions régulières galoisiennes $E/k(t)$ pour un certain corps commutatif $k \subset K$ qui fournissait, par produit tensoriel, un corps $K(t,\sigma,\delta)\otimes_{k(t)} E$ extension galoisienne à groupe de Galois prescrit. Cette méthode présente certaines limites, par exemple elle ne s'applique que si σ est d'ordre fini et si δ est localement nilpotente. Dans cet article, on s'intéresse à l'étude du Problème Inverse de Galois sur un corps de fractions tordu du point de vue de l'extension des constantes.

2.— Arithmétique d'une extension des constantes de corps de fractions tordu.

Dans tout ce §, l'on fixe une extension de corps H/K, un automorphisme $\sigma \in \mathrm{Aut}(H)$ et une σ-dérivation $\delta \in \sigma\text{-}\mathrm{Der}(H)$ tels que $\sigma_{|K} \in \mathrm{Aut}(K)$ et $\delta_{|K} \in \sigma\text{-}\mathrm{Der}(K)$ et l'on considère l'extension des constantes $H(t,\sigma,\delta)/K(t,\sigma,\delta)$.

2.1.— Permanence du degré.

La première question à se poser est de savoir si, à l'instar du cas commutatif fini, les dimensions des extensions H/K et $H(t,\sigma,\delta)/K(t,\sigma,\delta)$ restent les même. Cette propriété est en fait reliée à une propriété « à la Ore » :

Proposition 1.— *Les propositions suivantes*

i) il existe une K-base à droite de H qui est une $K(t,\sigma,\delta)$-base de $H(t,\sigma,\delta)$,

ii) toute K-base à droite de H est une $K(t,\sigma,\delta)$-base de $H(t,\sigma,\delta)$,

iii) l'anneau $H[t,\sigma,\delta]$ vérifie la propriété $(\Omega_{H/K})$ suivante :

$$(\Omega_{H/K})\ \forall p(t) \in H[t,\sigma,\delta],\ \exists q(t) \in H[t,\sigma,\delta]-\{0\} \text{ tel que } p(t)q(t) \in K[t,\sigma,\delta],$$

iv) l'anneau $R = H[t,\sigma,\delta]$ vérifie la propriété « à la Ore » (relativement à la partie multiplicative $S = K[t,\sigma,\delta]-\{0\}$) suivante : $\forall a,b \in R-\{0\}$, $aR \cap bS \neq \{0\}$ [1],

sont équivalentes.

Preuve : $iv) \Longrightarrow iii)$ On choisit $a = p(t)$ et $b = 1$.

$iii) \Longrightarrow ii)$ Si $(e_i)_{i\in I}$ désigne une K-base à droite de H, il est alors clair qu'elle forme aussi une base à droite du $K[t,\sigma,\delta]$-module à droite $H[t,\sigma,\delta]$:

$$H[t,\sigma,\delta] = \bigoplus_{i\in I} e_i K[t,\sigma,\delta]$$

Considérée dans $H(t,\sigma,\delta)$, la famille $(e_i)_{i\in I}$ reste aussi $K(t,\sigma,\delta)$-libre. En effet, si l'on dispose d'une équation de dépendance linéaire

$$e_{i_1}p_1(t)q_1(t)^{-1} + e_{i_2}p_2(t)q_2(t)^{-1} + \cdots + e_{i_h}p_h(t)q_h(t)^{-1} = 0$$

1. Cette propriété est plus forte que la traditionnelle condition de Ore : $\forall a \in S-\{0\}$, $\forall b \in R-\{0\}$, $aR \cap bS \neq \{0\}$

(avec $p_1(t),\cdots,p_h(t)\neq 0$) alors en multipliant à droite par $q_1(t)$ et en utilisant la propriété de Ore

$$q_2(t)^{-1}q_1(t)=q_{2,1}(t)q_{2,2}(t)^{-1},\cdots,q_h(t)^{-1}q_1(t)=q_{h,1}(t)q_{h,2}(t)^{-1}$$

(où $q_{2,1}(t),q_{2,2}(t),\cdots,q_{h,1}(t),q_{h,2}(t)$ sont des éléments de $K[t,\sigma,\delta]$ tous non nuls), on trouve que

$$e_{i_1}p_1(t)+e_{i_2}p_2(t)q_{2,1}(t)q_{2,2}(t)^{-1}+\cdots+e_{i_h}p_\delta(t)q_{h,1}(t)q_{h,2}(t)^{-1}=0$$

En réitérant le procédé avec $q_{2,2}(t)$, puis avec tous polynômes obtenus en utilisant la propriété de Ore, on finit par obtenir une équation de $K[t,\sigma,\delta]$-dépendance linéaire pour $(e_{i_1},\cdots,e_{i_h})$ qui implique *in fine* que $p_1(t)=\cdots=p_\ell(t)$, car chaque polynôme qui apparait quand on utilise la propriété de Ore est non nul.

Considérons maintenant $p(t),q(t)\in H[t,\sigma,\delta]$, par $(\Omega_{H/K})$, il existe $q_0(t)\in H[t,\sigma,\delta]$ tel que $q(t)q_0(t)=r(t)\in K[t,\sigma,\delta]$ et l'on alors $p(t)q(t)^{-1}=[p(t)q_0(t)]r(t)^{-1}$. Puisque $p(t)q_0(t)\in H[t,\sigma,\delta]=\bigoplus_{i\in I}e_iK[t,\sigma,\delta]$, on voit finalement que $p(t)q(t)^{-1}\in\bigoplus_{i\in I}e_iK(t,\sigma,\delta)$.

$i)\Longrightarrow iv)$ On peut écrire

$$a(t)^{-1}b(t)=e_{i_1}p_1(t)q_1(t)^{-1}+\cdots+e_{i_h}p_{i_h}(t)q_{i_h}(t)^{-1}$$

avec $p_1(t),q_1(t),\cdots,p_h(t),q_h(t)\in K[t,\sigma,\delta]$. Comme dans la preuve précédente, en factorisant successivement les dénominateurs, on peut écrire $a(t)^{-1}b(t)=e_{i_1}p_1^{'}(t)r(t)^{-1}+\cdots+e_{i_h}p_h^{'}(t)r(t)^{-1}$ avec $p_1^{'}(t),\cdots,p_h^{'}(t),r(t)\in K[t,\sigma,\delta]$. On a finalement $a(t)q(t)=b(t)r(t)\neq 0$ avec $q(t)=e_{i_1}p_1^{'}(t)+\cdots+e_{i_h}p_h^{'}(t)\in H[t,\sigma,\delta]$.

□

Remarque : Lorsque H est commutatif, on sait que si H/K est algébrique, alors toute K-base de H est une $K(t)$-base de $H(t)$. Mais lorsque H/K est transcendante ce n'est plus le cas : si $x\in H$ désigne un élément transcendant sur K alors le polynôme $p(t)=1-tx$ ne vérifie pas la condition iii) de la proposition 1.

Théorème 2.— *Si l'extension H/K a une dimension droite $[H:K]_d=\ell$ finie et si δ est une application K-linéaire à droite (i.e. $K\subset H_{\delta\text{-cst}}=\{x\in H,\ \delta(x)=0\}$)* [2]*, alors les propriétés équivalentes de la proposition 1 sont vérifiées. Plus précisément, en ce qui concerne la propriété $(\Omega_{H/K})$, on a que pour tout polynôme $p(t)\in H[t,\sigma,\delta]$ de degré d, il existe un polynôme non nul $q(t)\in H[t,\sigma,\delta]$ de degré $n\le d(\ell-1)$ tel que $p(t)q(t)\in K[t,\sigma]$.*

Ainsi, toute K-base à droite de H est une $K(t,\sigma,\delta)$-base à droite de $H(t,\sigma,\delta)$ et l'on a, en particulier, $[H(t,\sigma,\delta):K(t,\sigma,\delta)]_d=[H:K]_d$.

Preuve : Si $\alpha\in H$, on a

$$\begin{array}{rcl} t^1\alpha &=& \sigma(\alpha)t+\delta(\alpha)\\ t^2\alpha &=& \sigma^2(\alpha)t^2+(\sigma\circ\delta(\alpha)+\delta\circ\sigma(\alpha))t+\delta^2(\alpha)\\ t^3\alpha &=& \sigma^3(\alpha)t^3+(\delta\circ\sigma^2(\alpha)+\sigma\circ\delta\circ\sigma(\alpha)+\sigma^2\circ\delta(\alpha))t^2\\ && +(\delta^2\circ\sigma(\alpha)+\delta\circ\sigma\circ\delta(\alpha)+\sigma\circ\delta^2(\alpha))t+\delta^3(\alpha)\end{array}$$

et, par récurrence pour $n\ge 1$,

$$t^n\alpha=\sum_{k=0}^{n}\Gamma_{k,(n-k)}(\alpha)t^k$$

2. On remarquera que (δ lineaire à droite) $\Longleftrightarrow K\subset H_{\delta\text{-cst}}$ et (δ lineaire à gauche) $\Longleftrightarrow K\subset H_{\delta\text{-cst}}\cap H^\sigma$.

où $\Gamma_{k,(n-k)}(\alpha) = \sum_{\substack{(f_1,\cdots,f_n)\in\{\sigma,\delta\}^n \\ t.q.\ \sharp\{i/f_i=\sigma\}=k}} f_1\circ\cdots\circ f_n(\alpha)$. Puisque σ et δ sont des applications additives, il en est de même de $\Gamma_{k,(n-k)}$:

$$\forall\alpha,\beta\in H,\ \Gamma_{k,(n-k)}(\alpha+\beta) = \Gamma_{k,(n-k)}(\alpha)+\Gamma_{k,(n-k)}(\beta)$$

Par ailleurs, puisque δ est supposée K-linéaire à droite et que σ est un automorphisme de K, on voit que $\Gamma_{k,(n-k)}$ vérifie la relation de pseudo-linéarité suivante :

$$(P)\qquad \forall\alpha\in H\ \forall\lambda\in K,\ \Gamma_{k,(n-k)}(\alpha\lambda) = \Gamma_{k,(n-k)}(\alpha).\sigma^k(\lambda)$$

On pose $p(t) = a_0+a_1t+\cdots+a_dt^d$ avec $a_d\neq 0$ et l'on considére un polynôme $q(t) = \gamma_0+\gamma_1t+\cdots+\gamma_nt^n$ avec $n\geq d$. On exprime formellement le produit $p(t)q(t)$ à l'aide des fonctions $\Gamma_{k,(n-k)}$:

$$\begin{aligned} p(t)q(t) &= \sum_{i=0}^{d}\sum_{j=0}^{n}\sum_{k=0}^{i} a_i\Gamma_{k,(i-k)}(\gamma_j)t^{k+j} = \sum_{j=0}^{n}\sum_{i=0}^{d}\sum_{k=0}^{i} a_i\Gamma_{k,(i-k)}(\gamma_j)t^{k+j} \\ &= \sum_{j=0}^{n}\sum_{k=0}^{d}\left(\sum_{i=k}^{d} a_i\Gamma_{k,(i-k)}(\gamma_j)\right)t^{k+j} \end{aligned}$$

En calculant explicitement le coefficient de degré $h = 0,\cdots,n+d$ du polynôme ainsi obtenu, on voit que $q(t)$ est un polynôme non nul qui vérifie $p(t)q(t)\in K[t,\sigma,\delta]$ si et seulement si, il existe $\lambda_0,\cdots,\lambda_{n+d}\in K$ tels que $(\lambda_0,\cdots,\lambda_{n+d})\neq(0,\cdots 0)$ et tels que

$$\begin{array}{llcl}
(E_0) & \lambda_0 & = & a_d\Gamma_{d,0}(\gamma_n)\ \text{(degré } n+d)\\
(E_1) & \lambda_1 & = & a_d\Gamma_{d,0}(\gamma_{n-1})+a_{d-1}\Gamma_{d-1,0}(\gamma_n)+a_d\Gamma_{d-1,1}(\gamma_n)\ \text{(degré } n+d-1)\\
 & & \vdots & \\
(E_n) & \lambda_n & = & a_d\Gamma_{d,0}(\gamma_0)+(a_{d-1}\Gamma_{d-1,0}(\gamma_1)+a_d\Gamma_{d-1,1}(\gamma_1))+\cdots+\left(\sum_{i=0}^{d} a_i\Gamma_{0,i}(\gamma_d)\right)\ \text{(degré } d)\\
(E_{n+1}) & \lambda_{n+1} & = & \sum_{i=d-1}^{d} a_i\Gamma_{d-1,i}(\gamma_0)+\sum_{i=d-2}^{d} a_i\Gamma_{d-2,i}(\gamma_1)+\cdots+\sum_{i=0}^{d} a_i\Gamma_{0,i}(\gamma_{d-1})\ \text{(degré } d-1)\\
 & & \vdots & \\
(E_{n+d-1}) & \lambda_{n+d-1} & = & \sum_{i=1}^{d} a_i\Gamma_{1,i}(\gamma_0)+\sum_{i=0}^{d} a_i\Gamma_{0,i}(\gamma_1)\ \text{(degré 1)}\\
(E_{n+d}) & \lambda_{n+d} & = & \sum_{i=0}^{d} a_i\Gamma_{0,i}(\gamma_0)\ \text{(degré 0)}
\end{array}$$

(on voit, en effet, que $q(t) = 0 \Longleftrightarrow (\gamma_0,\cdots,\gamma_n) = (0,\cdots 0) \Longleftrightarrow (\lambda_0,\cdots,\lambda_n) = (0,\cdots 0) \Longleftrightarrow (\lambda_0,\cdots,\lambda_{n+d}) = (0,\cdots 0)$).

Examinons, pour commencer, les $n+1$ premières équations :

$$(E_0) \Longleftrightarrow a_d\sigma^d(\gamma_n) = \lambda_0 \Longleftrightarrow \gamma_n = \sigma^{-d}(a_d^{-1}).\sigma^{-d}(\lambda_0)$$

Sous (E_0), on a alors

$$(E_1) \Longleftrightarrow a_d\sigma^d(\gamma_{n-1}) + a_{d-1}\Gamma_{d-1,0}(\sigma^{-d}(a_d^{-1}).\sigma^{-d}(\lambda_0)) + a_d\Gamma_{d-1,1}(\sigma^{-d}(a_d^{-1}).\sigma^{-d}(\lambda_0) = \lambda_1$$

La propriété (P) assure que $\Gamma_{d-1,0}(\sigma^{-d}(a_d^{-1}).\sigma^{-d}(\lambda_n)) = \Gamma_{d-1,0}(\sigma^{-d}(a_d^{-1})).\sigma^{-1}(\lambda_0)$ et $\Gamma_{d-1,1}(\sigma^{-d}(a_d^{-1}).\sigma^{-d}(\lambda_0)) = \Gamma_{d-1,1}(\sigma^{-d}(a_d^{-1})).\sigma^{-1}(\lambda_0)$, de sorte que, il existe $u, v \in H$ tels que

$$(E_1) \Longleftrightarrow \gamma_{n-1} = u\sigma^{-d}(\lambda_1) + v\sigma^{-d-1}(\lambda_0)$$

Par récurrence, on en déduit qu'il existe des constantes $\pi_{i,j}$ dans H, ne dépendant que des constantes $a_0, \cdots, a_d$ et telles que le système $(E_1), \cdots, (E_n)$ équivaut à

$$(S) \quad \left\{ \begin{array}{lcl} \gamma_n & = & \pi_{n,0}.\sigma^{-d}(\lambda_0) \\ \gamma_{n-1} & = & \pi_{n-1,0}.\sigma^{-d}(\lambda_1) + \pi_{n-1,1}.\sigma^{-d-1}(\lambda_0) \\ & \vdots & \\ \gamma_1 & = & \pi_{1,0}.\sigma^{-d}(\lambda_{n-1}) + \pi_{1,1}.\sigma^{-d-1}(\lambda_{n-2}) + \cdots + \pi_{1,n-1}.\sigma^{-d-n+1}(\lambda_0) \\ \gamma_0 & = & \pi_{0,0}.\sigma^{-d}(\lambda_n) + \pi_{0,1}.\sigma^{-d-1}(\lambda_{n-1}) + \cdots + \pi_{0,n-1}.\sigma^{-d-n+1}(\lambda_1) + \pi_{0,n}.\sigma^{-d-n}(\lambda_0) \end{array} \right.$$

A ce stade, la donnée d'un $(n+1)$-uplet $(\lambda_0, \cdots, \lambda_n) \in K^{n+1}$ fixe de manière définitive le polynôme $q(t)$. Le polynôme $q(t)$ ainsi obtenu vérifiera donc $p(t)q(t) \in K[t, \sigma, \delta]$ si, en plus, on peut choisir $(\lambda_{n+1}, \cdots, \lambda_{n+d}) \in K^d$ tels que les équations $(E_{n+1}), \cdots, (E_{n+d})$ soient satisfaites. Puisque σ est bijectif, les équations $(E_{n+1}), \cdots, (E_{n+d})$ équivalent au système

$$\left\{ \begin{array}{llcl} (F_1) & \sigma^{-d+1}(\lambda_{n+1}) & = & \displaystyle\sum_{i=d-1}^{d} \sigma^{-d+1}(a_i)\sigma^{-d+1}(\Gamma_{d-1,i}(\gamma_0)) + \sum_{i=d-2}^{d} \sigma^{-d+1}(a_i)\sigma^{-d+1}(\Gamma_{d-2,i}(\gamma_1)) + \cdots \\ & & & \qquad \cdots + \displaystyle\sum_{i=0}^{d} \sigma^{-d+1}(a_i)\sigma^{-d+1}(\Gamma_{0,i}(\gamma_{d-1})) \\ & & \vdots & \\ (F_h) & \sigma^{-d+h}(\lambda_{n+h}) & = & \displaystyle\sum_{k=0}^{d-h} \sum_{i=d-h-k}^{d} \sigma^{-d+h}(a_i)\sigma^{-d+h}(\Gamma_{d-h-k,i}(\gamma_k)) \\ & & \vdots & \\ (F_{d-1}) & \sigma^{-1}(\lambda_{n+d-1}) & = & \displaystyle\sum_{i=1}^{d} \sigma^{-1}(a_i)\sigma^{-1}(\Gamma_{1,i}(\gamma_0)) + \sum_{i=0}^{d} \sigma^{-1}(a_i)\sigma^{-1}(\Gamma_{0,i}(\gamma_1)) \\ (F_d) & \lambda_{n+d} & = & \displaystyle\sum_{i=0}^{d} a_i\Gamma_{0,i}(\gamma_0) \end{array} \right.$$

En fait, ce système est linéaire relativement aux variables $x_0 = \sigma^{-d-n}(\lambda_0), \cdots, x_n = \sigma^{-d}(\lambda_n)$, $x_{n+1} = \sigma^{-d+1}(\lambda_{n+1}), \cdots, x_{n+d-1} = \sigma^{-1}(\lambda_{n+d-1}), x_{n+d} = \lambda_{n+d}$ $(x_i = \sigma^{-d-n+i}(\lambda_i))$. En effet, pour montrer que l'équation (F_h) est bien linéaire à droite en les variables $x_0, \cdots, x_{n+d}$, il s'agit de remarquer d'une part que $\sigma^{-d+h}(\lambda_{n+h}) = x_{n+h}$ et, d'autre part, que $\sigma^{-d+h}(\Gamma_{d-h-k,i}(\gamma_k))$ est combinaison linéaire à droite des $x_0, \cdots, x_{n+d}$ pour tout k et tout i : puisque

$$\gamma_k = \pi_{k,0}.\sigma^{-d}(\lambda_{n-k}) + \pi_{k,1}.\sigma^{-d-1}(\lambda_{n-k-1}) + \cdots + \pi_{k,n-k}.\sigma^{-d-n+k}(\lambda_0)$$

en utilisant la propriété (P), on trouve que

$$\Gamma_{d-h-k,i}(\gamma_k) = \alpha_0.\sigma^{-h-k}(\lambda_{n-k}) + \alpha_1.\sigma^{-h-k-1}(\lambda_{n-k-1}) + \cdots + \alpha_n.\sigma^{-h-n}(\lambda_0)$$

où $\alpha_h = \Gamma_{d-h-k,i}(\pi_{k,h})$ pour $h = 0, \cdots, n-k$ et, finalement, on a

$$\begin{aligned}\sigma^{-d+h}(\Gamma_{d-h-k,i}(\gamma_k)) &= \sigma^{-d+h}(\alpha_0).\sigma^{-d-k}(\lambda_{n-k}) + \sigma^{-d+h}(\alpha_1)\sigma^{-d-k-1}(\lambda_{n-k-1}) + \cdots + \sigma^{-d+h}(\alpha_n)\sigma^{-d-n}(\lambda_0) \\ &= \sigma^{-d+h}(\alpha_0).x_{n-k} + \sigma^{-d+h}(\alpha_1).x_{n-k-1} + \cdots + \sigma^{-d+h}(\alpha_0).x_0\end{aligned}$$

Les $(n+d+1)$-uplets $(x_0, \cdots, x_{n+d}) \in K^{n+d+1}$ solutions de l'équation (F_h) forment un sous-K-espace vectoriel V_h du K-espace vectoriel à droite K^{n+d+1}. Puisque les coefficients de (F_h) sont des éléments de H et que $[H:K]_d = \ell$, on voit que $\dim(V_h) \geq n+d+1-\ell$. On a alors $\dim(V_1 \cap V_2) = \dim(V_1) + \dim(V_2) - \dim(V_1 + V_2) \geq (n+d+1-\ell) + (n+d+1-\ell) - (n+d+1) = (n+d+1) - 2\ell$, puis, par récurrence, $\dim(V_1 \cap \cdots \cap V_d) \geq (n+d+1) - d\ell$. Si l'on considère un entier $n \geq d(\ell-1)$, on a alors $V_1 \cap \cdots \cap V_d \neq \{0\}$ et il existe donc une solution non nulle $(x_0, \cdots, x_{n+d}) \in K^{n+d+1}$ au système $(E_1), \cdots, (E_n), (F_1), \cdots, (F_d)$.

Tout $(n+d)$-uplet $(x_0, \cdots, x_{n+d})$ solution fournit, par bijectivité de σ, un $(n+1)$-uplet non nul $(\lambda_0, \cdots, \lambda_n)$ qui permet, grâce au système (S), d'expliciter un polynôme $q(t)$ vérifiant $p(t)q(t) \in K[t, \sigma, \delta]$. Ce polynôme est alors de degré $\leq n$ et l'on a vu que l'on pouvait choisir $n = (d-1)\ell$.

La conclusion finale du théorème est alors une conséquence immédiate de la proposition 1.

□

2.2.— Action galoisienne sur les coefficients.

Si, comme dans le cas commutatif, on souhaite fait agir $\mathrm{Aut}(H/K)$ sur l'anneau $H[t, \sigma, \delta]$ par *action sur les coefficients* des polynômes :

$$\begin{array}{rccl}\Theta : & \mathrm{Aut}(H/K) & \longrightarrow & \mathrm{Aut}(H[t,\sigma,\delta]/K[t,\sigma,\delta]) \\ \\ & g & \longmapsto & \Theta(g) : \begin{array}{ccc} H[t,\sigma,\delta] & \longrightarrow & H[t,\sigma,\delta] \\ a_0 + \cdots + a_n t^n & \longmapsto & g(a_0) + \cdots + g(a_n)t^n \end{array}\end{array}$$

on voit qu'une telle chose est possible si et seulement si les éléments de $\mathrm{Aut}(H/K)$ commutent tous avec σ et δ. Sous cette hypothèse, l'action Θ se relève alors à $\mathrm{Aut}(H(t,\sigma,\delta)/K(t,\sigma,\delta))$ de manière unique puisque $H[t,\sigma,\delta]$ est un anneau de Ore et que tout monomorphisme d'un anneau de Ore se relève de manière unique à son corps de fractions (voir [Coh, Corollary 1.3.5.]). Dans la suite de ce §, nous supposerons désormais que les applications σ et δ commutent avec tous les éléments de $\mathrm{Aut}(H/K)$. L'*action sur les coefficients* des éléments de $H(t,\sigma,\delta)$, que nous continuerons à noter Θ, vérifiera donc :

$$\Theta(g)\Big((a_0 + \cdots + a_n t^n)(b_0 + \cdots + b_m t^m)^{-1}\Big) = (g(a_0) + \cdots + g(a_n)t^n)(g(b_0) + \cdots + g(b_m)t^m)^{-1}$$

Cette action est visiblement est clairement fidèle.

Dans cette partie, nous souhaitons étudier l'arithmétique de l'extension $H(t,\sigma,\delta)/K(t,\sigma,\delta)$ lorsque l'extension H/K est supposée algébrique [3], extérieure et galoisienne Ce qui va nous préoccuper dans la suite est le cas où H/K est finie, extérieure et galoisienne. Dans cette situation,

3. On rappelle qu'une extension H/K est dite algébrique (à gauche) si, pour tout $\alpha \in H$, le degré (gauche) $[K(\alpha):K]_g$ est fini.

le groupe $\mathrm{Gal}(H/K)$ s'identifie donc, par Θ, à un sous-groupe de $\mathrm{Aut}(H(t,\sigma,\delta)/K(t,\sigma,\delta))$ et l'on va rechercher des situations pour lesquelles $H(t,\sigma,\delta)/K(t,\sigma,\delta)$ eſt galoisienne de groupe $\Theta(G)$.

Lemme 3.— *Avec les notations précédentes, pour tout $g \in \mathrm{Aut}(H/K)$ on a*

$$\Theta(g) \in \mathrm{Int}(H(t,\sigma,\delta)/K(t,\sigma,\delta)) \Longrightarrow \exists \lambda \in H^\sigma,\ \exists n \in \mathbb{Z},\ g = I_\lambda \circ \sigma^n$$

Par ailleurs, dans les situations particulières suivantes, on a plus précisément :

a) Si $\delta = 0$, alors

$$\Theta(g) \in \mathrm{Int}(H(t,\sigma)/K(t,\sigma)) \Longleftrightarrow \exists \lambda \in H^\sigma,\ \exists n \in \mathbb{Z},\ g = I_\lambda \circ \sigma^n$$

b) Si $\sigma = \mathrm{Id}$, alors

$$\Theta(g) \in \mathrm{Int}(H(t,\mathrm{Id},\delta)/K(t,\mathrm{Id},\delta)) \Longleftrightarrow \exists \lambda \in H_{\delta\text{-cſt}},\ g = I_\lambda$$

Preuve : $\Longleftarrow$: on a $\Theta(g) = I_{\lambda t^n}$ compte-tenu du fait que

$$(\lambda t^n)t(\lambda t^n)^{-1} = \lambda t^n t t^{-n}\lambda^{-1} = \lambda t \lambda^{-1} = \lambda\sigma(\lambda^{-1})t = \lambda\lambda^{-1}t = t = \Theta(g)(t)$$

et du fait que, pour tout $a \in H$,

$$(\lambda t^n)a(\lambda t^n)^{-1} = \lambda t^n a t^{-n}\lambda^{-1} = \lambda\sigma^n(a)t^n t^{-n}\lambda^{-1} = \lambda\sigma^n(a)\lambda^{-1} = I_\lambda \circ \sigma^n(a) = g(a) = \Theta(g)(a)$$

$\Longrightarrow$: si $\Theta(g) = I_{s(t)}$ avec $s(t) \in H(t,\sigma)$, alors en se plaçant dans $H((t,\sigma))$, on peut écrire $s(t) = \lambda_n t^n + \lambda_{n+1}t^{n+1} + \cdots$ avec $\lambda_n \neq 0$. Puisque $\Theta(g)(t) = t$, on a donc $s(t)t = ts(t)$, c'eſt-à-dire

$$\lambda_n t^{n+1} + \lambda_{n+1}t^{n+2} + \cdots = t\lambda_n t^n + t\lambda_{n+1}t^{n+1} + \cdots = \sigma(\lambda_n)t^{n+1} + \sigma(\lambda_{n+1})t^{n+2} + \cdots$$

et, en particulier, $\sigma(\lambda_n) = \lambda_n$. Par ailleurs, pour tout $a \in H$, on a $s(t)a = g(a)s(t)$, c'eſt-à-dire

$$\lambda_n\sigma^n(a)t^n + \lambda_{n+1}\sigma^{n+1}(a)t^{n+1} + \cdots = g(a)\lambda_n t^n + g(a)\lambda_{n+1}t^{n+1} + \cdots$$

et en particulier, $g(a) = I_{\lambda_n} \circ \sigma^n$.

□

Puisque les éléments de $\mathrm{Int}(H^\sigma)$ (vu comme sous-groupe de $\mathrm{Aut}(H)$) commutent avec σ, on voit que le sous groupe $<\sigma, \mathrm{Int}(H^\sigma)>$ s'identifie au produit cartésien $<\sigma> \times \mathrm{Int}(H^\sigma)$. Le lemme 3 se réécrit alors de la manière suivante :

$$\begin{array}{lcll}
\Theta\Big(\mathrm{Aut}(H/K)\Big) \cap \mathrm{Int}(H(t,\mathrm{Id},\delta)/K(t,\mathrm{Id},\delta)) & \subset & \Theta\Big(\mathrm{Aut}(H/K) \cap (<\sigma> \times \mathrm{Int}(H^\sigma))\Big) & \text{en toute généralité} \\
 & = & \Theta\Big(\mathrm{Aut}(H/K) \cap (<\sigma> \times \mathrm{Int}(H^\sigma))\Big) & \text{si } \delta = 0 \\
 & = & \Theta\Big(\mathrm{Int}_{\text{cſt}}(H/K)\Big) & \text{si } \sigma = \mathrm{Id}
\end{array}$$

où $\mathrm{Int}_{\text{cſt}}(H/K) = \{I_a \in \mathrm{Int}(H/K) /\ a \in H_{\text{cſt}}\}$.

Théorème 4.— *Avec les notations et hypothèses précédentes, si H/K eſt galoisienne extérieure de groupe fini G et que $\mathrm{Gal}(H/K) \cap (<\sigma> \times \mathrm{Int}(H^\sigma)) = \{\mathrm{Id}\}$, alors l'extension $H(t,\sigma,\delta)/K(t,\sigma,\delta)$ eſt aussi galoisienne extérieure de groupe $\Theta(G) \simeq G$.*

Preuve : Les hypothèses assurent, par le lemme 3, que le groupe d'automorphismes $\Theta(G)$ du corps $H(t,\sigma,\delta)$ ne contient aucun automorphisme intérieur non trivial. La généralisation du lemme d'Artin pour théorie de Galois assure alors que l'extension $H(t,\sigma,\delta)/H(t,\sigma,\delta)^{\Theta(G)}$ est galoisienne extérieure de groupe $\Theta(G)$. Puisque H/K est aussi galoisienne extérieure, par le théorème 2, on botient la relation sur les degrés

$$[H(t,\sigma,\delta):H(t,\sigma,\delta)^{\Theta(G)}] = |\Theta(G)| = |G| = [H:K] = [H(t,\sigma,\delta):K(t,\sigma,\delta)]$$

et comme $K(t,\sigma,\delta) \subset H(t,\sigma,\delta)^{\Theta(G)}$, on en déduit finalement que $K(t,\sigma,\delta) = H(t,\sigma,\delta)^{\Theta(G)}$.

□

Corollaire 5.— *Soient H/K une extension algébrique extérieure et galoisienne de groupe de Galois (profini) Γ, $\sigma \in \mathrm{Aut}(H)$ et $\delta \in \sigma\text{-}\mathrm{Der}(H)$ tels que σ et δ commute avec tous les éléments de Γ. S'il existe une filtration $\mathscr{F}$ de H/K composée d'extensions intermédiaires $H/L/K$ finies et galoisiennes sur K, telle que, pour tout $L \in \mathscr{F}$, les deux conditions suivantes*

a) $\sigma_{|L}$ et $\delta_{|L}$ sont à valeurs dans L,

b) $\mathrm{Gal}(L/K) \cap (<\sigma> \times \mathrm{Int}(L^{\sigma})) = \{\mathrm{Id}\}$,

sont vérifiées, alors l'extension $H(t,\sigma,\delta)/K(t,\sigma,\delta)$ est aussi algébrique extérieure et galoisienne de groupe de Galois Γ.

Preuve : Si L/K est galoisienne finie, alors elle est extérieure et le corollaire 4 avec les hypothèses a,b) montrent que $L(t,\sigma,\delta)/K(t,\sigma,\delta)$ est aussi extérieure finie et galoisienne. Puisque $H = \bigcup_{L\in\mathscr{L}} L$, on a $H(t,\sigma,\delta) = \bigcup_{L\in\mathscr{L}} L(t,\sigma,\delta)$ et donc $H(t,\sigma,\delta)/K(t,\sigma,\delta)$ est bien une extension algébrique, extérieure et galoisienne, qui est, par ailleurs, filtrée par la famille $\{L(t,\sigma,\delta)\}_{L\in\mathscr{L}}$. Si, maintenant, l'on considère une extension L_2/L_1 avec $L_1, L_2 \in \mathscr{L}$, on voit que le diagramme

$$\begin{tikzcd}
\mathrm{Gal}(L_2/K) \arrow[rr, "g\mapsto\Theta(g)", "\simeq"'] \arrow[d, "g\mapsto g_{|L_1}"'] & & \mathrm{Gal}(L_2(t,\sigma,\delta)/K(t,\sigma,\delta)) \arrow[d, "\Theta(g)\mapsto\Theta(g)_{|L_1(t,\sigma,\delta)}"] \\
\mathrm{Gal}(L_1/K) \arrow[rr, "g\mapsto\Theta(g)", "\simeq"'] & & \mathrm{Gal}(L_1(t,\sigma,\delta)/K(t,\sigma,\delta))
\end{tikzcd}$$

est commutatif. Il s'ensuit que les systèmes projectifs de groupes considérés sont isomorphes et donc que

$$\mathrm{Gal}(H(t,\sigma,\delta)/K(t,\sigma,\delta)) \simeq \varprojlim_{L\in\mathscr{L}} \mathrm{Gal}(L(t,\sigma,\delta)/K(t,\sigma,\delta)) \simeq \varprojlim_{L\in\mathscr{L}} \mathrm{Gal}(L/K) \simeq \mathrm{Gal}(H/K)$$

□

2.3.— Application au problème inverse de Galois

Une conséquence immédiate du corollaire 5 est le

Théorème 6.— *Tout groupe profini réalisable comme groupe de Galois d'une extension galoisienne algébrique et extérieur d'un corps K est aussi réalisable sur le corps $K(x)$* [4]*. En particulier, si K satisfait au problème inverse de Galois alors il en est de même de $K(x)$.*

Le corollaire 5 permet aussi de donner une version du théorème de Leptin-Waterhouse sur les corps gauches (voir [FJ] pour la version commutative) :

Théorème 7.— *Pour tout groupe profini Γ, il existe une extension algébrique extérieure et galoisienne de corps gauches ayant Γ pour groupe de Galois.*

Preuve : Soient Γ un groupe profini de rang topologique α et $\beta = \max(\alpha, \aleph_0)$. On considère Ω un corps algébriquement clos de caractéristique 0 et de cardinal β (par exemple, une clôture algébrique du corps $\mathbb{Q}(y_i)_{i\in\beta}$) et $k = \Omega(u)$ son corps de fractions rationnelles. Le groupe de Galois absolu $G_k = \mathrm{Gal}(\overline{k}/k)$ est alors prolibre de rang β (ce résultat profond est dû à Douady [Dou] en caractéristique nulle et a été généralisé par Harbater et Pop en toute généralité [Pop]). Par proliberté, on dispose d'un épimorphisme $G_k \longrightarrow \Gamma$ et, par suite, d'une extension algébrique galoisienne E/k de groupe de Galois Γ. On considère alors le corps $K = \mathrm{Puis}(k)$ des séries de Puiseux à coefficients dans k, qui est une extension algébrique du corps de séries de Laurent $k((x))$. Le corps $\mathrm{Puis}(\overline{k})$ est algébriquement clos et, dans $\mathrm{Puis}(\overline{k})$, la clôture algébrique $\overline{k((x))} = \overline{K}$ est égale au corps

$$\bigcup_{L/k \text{ finie}} \mathrm{Puis}(L) = \bigcup_{n\geq 1} \bigcup_{L/k \text{ finie}} L((x^{1/n}))$$

Par ailleurs, l'extension $H = \bigcup_{E/L/k \text{ finie}} \mathrm{Puis}(L)$ est galoisienne sur K de groupe Γ. On a alors le diagramme suivant :

$$\begin{tikzcd}
 & & \mathrm{Puis}(\overline{k}) \arrow[d, dash] & & \\
 & & \overline{k((x))} = \overline{K} \arrow[dl, dash] \arrow[ddd, dash, "G_k\times\widehat{\mathbb{Z}}"'] \arrow[ddrr, dash, "\widehat{\mathbb{Z}}"] \arrow[ddll, dash, bend right, "G_k"'] & & \\
 & H \arrow[dl, dash, "\Gamma"] & & & \\
K = \mathrm{Puis}(k) \arrow[drr, dash, "\widehat{\mathbb{Z}}"'] & & & & \bigcup_{L/k \text{ finie}} L((x)) \arrow[dll, dash, "G_k"] \\
 & & k((x)) & &
\end{tikzcd}$$

On considère un élément non trivial $\sigma \in \{\mathrm{Id}\} \times \widehat{\mathbb{Z}} \subset \mathrm{Gal}(\overline{k((x))}/k((x)))$. Il est d'ordre infini et

4. Le corps $K(x)$ des fractions à indéterminée centrale et à coefficients dans le corps K est, par définition, le corps de fractions tordu $K(x) = K(x, \mathrm{Id}, 0)$

induit par restriction un élément de $\mathrm{Aut}(K)$ (resp. de $\mathrm{Aut}(H)$) d'ordre infini. Comme le montre le diagramme, dans $\mathrm{Aut}(H)$, on a $< \sigma > \cap \mathrm{Gal}(H/K) = \{\mathrm{Id}\}$ et comme H est un corps commutatif, on a $\mathrm{Int}(H^\sigma) = \{\mathrm{Id}\}$. On peut donc appliquer le corollaire 5 et en déduire que $H(t,\sigma)/K(t,\sigma)$ est galoisienne extérieure de groupe Γ. Puisque $\sigma \neq \mathrm{Id}$, le corps $K(t,\sigma)$ est bien gauche.

Bibliographie

[Beh] Angelot Behajaina, *Théorie inverse de Galois sur les corps des fractions rationnelles tordus*, J. Pure Appl. Algebra, , no. 4, Paper No. 106549 (2021)

[BDH] Angelot Behajaina, Bruno Deschamps et François Legrand, *Problèmes de plongement finis sur les corps non commutatifs*, 249, no. 2, 617-650 (2022).

[Coh] Paul Moritz Cohn, *Skew fields. Theory of general division rings*, Encyclopedia of Mathematics and its Applications, 57. Cambridge University Press, Cambridge, (1995)

[Des] Bruno Deschamps, *La méthode Behajaina appliquée aux corps de fractions tordus par une dérivation*, Research in Number Theory, no. 2, Paper no. 39 (2021)

[Dou] A Douady, *Détermination d'un groupe de Galois*, C.R. Acad. Sc. Paris, 258 (1964)

[DL] Bruno Deschamps et François Legrand, *Le problème inverse de Galois sur les corps des fractions tordus à indéterminée centrale*, J. Pure Appl. Algebra, 224(5) (2020)

[GW] Kenneth Goodearl and Robert Breckenridge Warfield, *An introduction to noncommutative Noetherian rings. Second edition*, London Mathematical Society Student Texts, 61. Cambridge University Press, Cambridge (2004)

[Jac] Nathan Jacobson, *Structure of rings*, American mathematical society colloquium publications (1956)

[Jar] Moshe Jarden, *Algebraic patching*, Springer Monographs in Mathematics (2011)

[Ore] Oystein Ore, *Theory of non-commutative polynomials*, Ann. of Math.(2), 34(3), 480-508 (1933)

[Pop] Florian Pop, *The geometric case of a conjecture of Shafarevich — $G_{\overline{k}(t)}$ is profinite free —*, Heidelberg Mannheim Preprint Series "Arithmetik", Heft 8 (1993).

Bruno Deschamps
Laboratoire de Mathématiques Nicolas Oresme, CNRS UMR 6139
Université de Caen - Normandie
BP 5186, 14032 Caen Cedex - France

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