Le théorème de Lüroth pour les corps de fractions tordus par un automorphisme fini

Bruno DESCHAMPS
(LMNO & Le Mans Université)

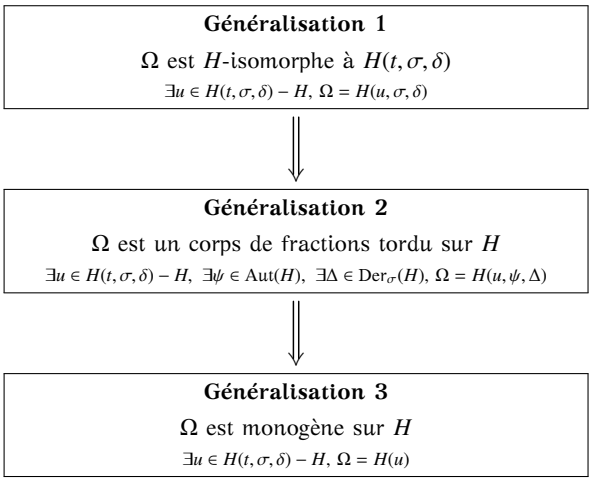
Résumé.– L'objet principal de cet article est de montrer la généralisation du théorème de Lüroth au cas d'un corps de fractions tordu $H(t,\sigma)$, où H désigne une algèbre à division et $\sigma \in \mathrm{Aut}(H)$ un automorphisme d'ordre fini.

Résumé.– The main object of this article is to show the generalization of Lüroth's theorem to the case of a skew fraction field $H(t,\sigma)$, where H denotes a field of finite dimension over its center and $\sigma \in \mathrm{Aut}(H)$ an automorphism of finite order.

0.– Introduction.

Le théorème de Lüroth (voir [Lür] et [Ste]) joue un grand rôle en arithmétique et en géométrie algébrique. Il établit qu'un sous-corps Ω d'un corps de fractions rationnelles $H(t)$ à coefficients dans un corps commutatif H est monogène dés qu'il contient H : $H(t)/\Omega/H \Longrightarrow \exists x \in H(t),\ \Omega = H(x)$. Les travaux de Ore (voir [Ore]) montrent qu'il existe une généralisation pertinente de la notion de polynômes dans le cas des corps non commutatifs : étant donné un corps H, éventuellement gauche, on peut considérer le H-espace vectoriel à gauche $\bigoplus_{n\geq 0} H.t^n$ et tenter de définir une multiplication dessus. Par linéarité cela revient à définir le produit $t.a$ lorsque $a \in H$. On souhaite garder une notion de degré, si bien que l'on impose des relations du type $t.a = \sigma(a).t + \delta(a)$. L'associativité du produit implique alors que σ est un endomorphisme du corps H et que δ est une σ-dérivation (i.e. δ est additif et $\delta(ab) = \delta(a)b + \sigma(a)\delta(b)$). On montre que ces seules conditions font de $\bigoplus_{n\geq 0} H.t^n$ un anneau, l'*anneau des polynômes* (à coefficients dans H) *tordu* (par σ et δ), que l'on note $H[t,\sigma,\delta]$. Lorsque H est commutatif, $\sigma = \mathrm{Id}$ et $\delta = 0$, on retombe bien sur l'anneau des polynômes classique. L'étude de ces anneaux montre que, lorsque σ est un automorphisme, l'anneau $H[t,\sigma,\delta]$ possède un unique corps de fractions, le *corps des fractions rationnelles tordu*, que l'on note $H(t,\sigma,\delta)$ (et $H(t,\sigma)$ lorsque $\delta = 0$). Il s'agit d'un corps bien moins facile à manipuler que dans le cas commutatif mais pour lequel bien des propriétés arithmétiques se généralisent, parfois avec difficulté.

C'est un problème très largement ouvert de savoir si, sur les corps de fractions rationnelles tordus, on dispose d'une généralisation du théorème de Lüroth. Il convient de préciser ce que l'on entend par *généralisation du théorème de Lüroth* : dans le cas commutatif affirmer qu'une extension intermédiaire $H(t)/\Omega/H$, avec $\Omega \neq H$, s'écrit $\Omega = H(u)$ avec $u \in H(t) - H$ est équivalent à dire que, en tant que H-algèbre, les corps Ω et $H(t)$ sont isomorphes. Cet énoncé est lui-même équivalent à dire que le corps Ω est un corps de fractions rationnelles à coefficients dans H. Dans $H(t,\sigma,\delta)$ ces trois propriétés ne sont plus forcément équivalentes et l'on peut ainsi généraliser de plusieurs manières : pour un corps H, un automorphisme $\sigma \in \mathrm{Aut}(H)$, une σ-dérivation $\delta \in \mathrm{Der}_\sigma(H)$ et Ω un sous-corps intermédiaire de $H(t,\sigma,\delta)/H$ non égal à H, on a



La généralisation 1 n'a aucune chance d'être vraie : il suffit de considérer $H(t,\sigma)$ avec H commutatif et σ d'ordre fini $n \geq 2$, le sous-corps $H(t^n)$ est alors commutatif. L'adjonction d'une σ-dérivation δ complique radicalement les choses, aussi ne nous considérerons la question de la généralisation du théorème de Lüroth que dans le cas où δ est nulle. Pour préciser encore les choses notons que, dans l'étude générale de l'extension $H(t)/H$ avec H commutatif, on sait que pour tout $f \notin H$ l'extension $H(t)/H(f)$ est de degré fini. C'est une propriété qui n'est pas claire dans le cas non commutatif. Ainsi, étant donné un corps H et un automorphisme $\sigma \in \mathrm{Aut}(H)$ nous dirons que le corps $H(t,\sigma)$ vérifie la

Généralisation du théorème de Lüroth si, *pour toute extension intermédiaire $H(t,\sigma)/\Omega/H$ différente de H, on a $[H(t,\sigma)/\Omega]_g = [H(t,\sigma)/\Omega]_d < +\infty$ et il existe $u \in H(t,\sigma)$ tel que $\Omega = H(u)$.*

Propriété de Lüroth forte si, *pour toute extension intermédiaire $H(t,\sigma)/\Omega/H$ différente de H, on a $[H(t,\sigma)/\Omega]_g = [H(t,\sigma)/\Omega]_d < +\infty$ et il existe $u \in H(t,\sigma)$ et $\psi \in \mathrm{Aut}(H)$ tel que $\Omega = H(u,\psi)$.*

Dans un récent travail, Legrand et Paran se sont attaqués à la généralisation du théorème de Lüroth dans le cas $\sigma = \mathrm{Id}$ et $\delta = 0$: ils montrent dans [LP] que celle-ci est vraie pour $H(t) = H(t, \mathrm{Id})$ dans le cas particulier où H désigne une k-algèbre à division (i.e. un corps de dimension finie sur son centre). A notre connaissance, c'est pour le moment la seule généralisation du théorème de Lüroth à avoir été établie pour des corps de fractions tordus. Il s'agit d'une généralisation qui porte sur la nature du corps des coefficients mais pas sur une éventuelle déformation du corps par un automorphisme.

Dans cet article, on s'intéresse à la situation générale où H est un corps quelconque et où $\sigma \in \mathrm{Aut}(H)$ est un autormorphisme d'ordre fini.

Dans le §2 on établit un résultat de réduction : on montre au théorème 13 que si H désigne un corps quelconque pour lequel la généralisation du théorème de Lüroth est vraie pour le corps des fractions à indéterminée centrale $H(t)$ alors celle pour $H(t,\sigma)$ est aussi vraie dés lors que σ est un automorphisme *complétement kummérien* (voir définition 8). Il découle de ce résultat que, sous cette hypothèse faite sur σ, la généralisation du théorème de Lüroth est vraie pour $H(t,\sigma)$ lorsque H est un corps commutatif et même, grâce à [LP], quand H est une algèbre à division (corollaire 14).

Le §3 de ce texte est consacré au cas où H est commutatif où l'on souhaite étudier la propriété de Lüroth forte. Une description très précise des corps intermédiaires $H(t,\sigma)/\Omega/H$, donnée au §3.1, permet au §3.2 de caractériser le fait que le corps $H(t,\sigma)$ vérifie la propriété de Lüroth forte par une propriété ne faisant intervenir que l'arithmétique de l'extension de corps commutatifs H/H^σ (théorème 18).

Finalement, une étude sur la hauteur vient compléter ce texte au §4 : dans le cas commutatif, si $x \in H(t) - H$, on sait que l'extension $H(t)/H(x)$ est finie et que son degré est égal à la hauteur de la fraction rationnelle x. Lorsque l'on tord par un automorphisme σ alors l'extension $H(t,\sigma)/H(x)$ est aussi

de degré fini mais, après avoir généralisé au §4.1 la notion de hauteur, nous montrons au §4.2 que ce degré n'est pas toujours égal à la hauteur de x.

Le §1 est consacré à une série de résultats généraux d'arithmétique des corps de fractions tordus, utiles pour les § suivants.

Pour le lecteur non familiarisé aux corps gauches et notamment à la généralisation de la théorie de Galois sur ces corps ainsi qu'aux corps de fractions (resp. de séries) tordus, nous renvoyons à [Coh] et [Jac] pour un exposé des notions de base que nous utilisons dans cet article.

Notations et rappels.

• Pour un corps H donné et un élément $a \in H^*$, on note $I(a) : x \longmapsto axa^{-1}$ l'automorphisme intérieur de H associé à a et pour une partie $A \subset H$, on note $I(A) = \{I(a)/\ a \in A\}$.

• Pour un corps H et une partie $X \subset H$ donnés, on note $\mathscr{C}_H(X) = \{y \in H/\ \forall x \in X,\ xy = yx\}$ le *commutant* (ou *centralisateur*) de X dans H. Lorsqu'il n'y a pas d'ambiguïté sur le corps à l'intérieur duquel on travaille, on note plus volontiers $\widetilde{X}$ à la place de $\mathscr{C}_H(X)$.

• Toute extension de corps H/K possède un degré à gauche et un degré à droite, notés respectivement $[H : K]_g$ et $[H : K]_d$, suivant le coté par lequel on fait agir K sur H en tant qu'espace vectoriel. Lorsque que l'on parle de degré de l'extension sans précision c'est toujours du degré à gauche dont on parle. Lorsque H/K est galoisienne, ces degrés coïncident.

• Une k-algèbre à division est un corps de dimension finie sur son centre k. La collection des algèbres à division est décrite par la théorie du groupe de Brauer. Il s'agit d'une petite mer tranquille, orée de l'immense et tumultueux océan des corps gauches. On rappelle que si $\mathscr{H}$ désigne une k-algèbre à division alors :

a) Toute extension intermédiaire $\mathscr{H}/L/k$ bicommute i.e. $\widetilde{\widetilde{L}} = L$.

b) Si L_1 et L_2 sont deux corps intermédiaires k-isomorphes, alors ils sont conjugués par un certain automorphisme intérieur de $\mathscr{H}$ (théorème de Skolem-Noether).

c) Les corps commutatifs maximaux L, extensions intermédiaires de $\mathscr{H}/k$, sont caractérisés par la relation $\widetilde{L} = L$. Pour un tel corps, on a $[\mathscr{H} : L] = [L : k]$ et cet entier est égal à l'indice de la classe de $\mathscr{H}$ dans le groupe de Brauer $\mathrm{Br}(k)$ de k. Si l'on suppose de plus que L/k soit une extension galoisienne alors toute famille $\{a_1, \cdots, a_n\}$ de $\mathscr{H}$ telle que $\{I(a_1)_{|L}, \cdots, I(a_n)_{|L}\} = \mathrm{Gal}(L/k)$ est une L-base de $\mathscr{H}$. L'application

$$\begin{array}{ccc} \mathrm{Gal}(L/k) \times \mathrm{Gal}(L/k) & \longrightarrow & L^* \\ (I(a_i), I(a_j)) & \longmapsto & a_i a_j a_\ell^{-1} \quad (\text{où } a_\ell \text{ est tel que } I(a_\ell) = I(a_i a_j)) \end{array}$$

est alors un 2-cocyle et $\mathscr{H}$ s'identifie au produit croisé de l'extension L/k par ce 2-cocycle. Lorsque l'extension L/k est cyclique, on dira que $\mathscr{H}$ *est un produit croisé cyclique*.

• Pour un automorphisme σ donné dans corps H nous noterons $H((t, \sigma))$ le corps des séries à coefficients dans H tordu par σ. Le plongement canonique de l'anneau $H[t, \sigma]$ dans $H((t, \sigma))$ induit, par unicité du corps de fractions de cet anneau, un plongement de $H(t, \sigma)$ dans $H((t, \sigma))$. Nous noterons abusivement $H(t, \sigma) \subset H((t, \sigma))$ ce plongement.

• Étant donnée une extension de corps H/K et une partie $A \subset H$, on notera $K(A)$ le sous-corps de H engendré par A sur K, c'est-à-dire le plus petit sous-corps de H qui contienne K et A. Lorsque $H = K(t, \sigma)$ on a donc $H = K(t)$ mais la réciproque n'est visiblement pas vraie. On fera ainsi très attention à la notation $K(t)$ qui peut sous-entendre parfois, comme l'usage le veut, que $K(t) = K(t, \mathrm{Id})$ est un fait un corps de fractions tordu à indéterminée centrale t. Par exemple, si σ désigne un automorphisme d'ordre n du corps K alors le corps $K(t^n)$ est bien un corps de fractions tordu à indéterminée centrale t^n puisque $K(t^n) = K(t^n, \sigma^n) = K(t^n, \mathrm{Id})$, mais nous continuerons à le noter $K(t^n)$ pour plus de commodité.

I.— Résultats préliminaires.

On établit ici des résultats techniques, utiles pour la suite de ce texte.

Lemme 1.— *On se donne une extension de corps H/K et une partie A de H. Le sous-anneau $K[A]$ de H, engendré par K et A, est égal à*

$$K[A] = \left\{ \sum_{i\in I \text{ fini}} m_i /\ m_i = \prod_{j\in J_i \text{ fini}} x_{i,j},\ x_{i,j} \in A \cup K \right\}$$

En conséquence de quoi, si A désigne une partie de H, on a

$$K(A) = \bigcup_n A_n \text{ où la suite } (A_n)_n \text{ est définie par } A_0 = K[A] \text{ et, pour tout } n \geq 0,\ A_{n+1} = K[A_n \cup A_n^{-1}]$$

Preuve : Puisque $K[A]$ contient K et A et est stable par sommes et produits, on voit que

$$\left\{ \sum_{i\in I \text{ fini}} m_i /\ m_i = \prod_{j\in J_i \text{ fini}} x_{i,j},\ x_{i,j} \in A \cup K \right\} \subset K[A]$$

mais comme cet ensemble est visiblement un sous-anneau de H qui contient K et A, on en déduit l'égalité. Il est clair que tous les sous-anneaux A_n sont inclus dans $K(A)$, mais comme tout élément de A_n est inversible dans A_{n+1}, on voit que $\bigcup_n A_n$ est un corps, nécessairement égale à $K(A)$.

□

Corollaire 2.— *On se donne une extension de corps H/K et une partie A de H.*

a) On a $\mathscr{C}_H(K(A)) = \mathscr{C}_H(K) \cap \mathscr{C}_H(A)$.

b) Si $\theta \in \mathrm{End}(H)$ désigne un endomorphisme du corps H tel que $\theta_{|K} \in \mathrm{End}(K)$ alors les propriétés suivantes

i) $\theta(A) \subset K(A)$,

ii) $\theta_{|K(A)} \in \mathrm{End}(K(A))$,

sont équivalentes.

Preuve : On reprend la description de $K(A)$ faite au lemme 1.

a) Si $X \subset H$, comme $X \cup K \subset K[X]$ on a $\mathscr{C}_H(K[X]) \subset \mathscr{C}_H(X \cup K) = \mathscr{C}_H(X) \cap \mathscr{C}_H(K)$. Vue la description de $K[X]$, on voit que, réciproquement $\mathscr{C}_H(X) \cap \mathscr{C}_H(K) \subset \mathscr{C}_H(K[X])$. On en déduit, par récurrence, que

$$\begin{array}{lcll}
\mathscr{C}_H(A_0) & = & \mathscr{C}_H(K[A]) & = \mathscr{C}_H(A) \cap \mathscr{C}_H(K) \\
\mathscr{C}_H(A_1) & = & \mathscr{C}_H(K[A_0 \cup A_0^{-1}]) = \mathscr{C}_H(A_0 \cup A_0^{-1}) \cap \mathscr{C}_H(K) & \\
 & = & \left(\mathscr{C}_H(A_0) \cap \mathscr{C}_H(A_0^{-1})\right) \cap \mathscr{C}_H(K) = \mathscr{C}_H(A_0) \cap \mathscr{C}_H(K) & = \mathscr{C}_H(A) \cap \mathscr{C}_H(K) \\
 & \vdots & & \\
\mathscr{C}_H(A_{n+1}) & = & \mathscr{C}_H(K[A_n \cup A_n^{-1}]) = \mathscr{C}_H(A_n \cup A_n^{-1}) \cap \mathscr{C}_H(K) & \\
 & = & \left(\mathscr{C}_H(A_n) \cap \mathscr{C}_H(A_n^{-1})\right) \cap \mathscr{C}_H(K) = \mathscr{C}_H(A_n) \cap \mathscr{C}_H(K) & = \mathscr{C}_H(A) \cap \mathscr{C}_H(K) \\
 & \vdots & &
\end{array}$$

Finalement, $\mathscr{C}_H(K(A)) = \mathscr{C}_H\left(\bigcup_n A_n\right) = \bigcap_n \mathscr{C}_H(A_n) = \mathscr{C}_H(A) \cap \mathscr{C}_H(K)$.

b) Vue la description de $A_0 = K[A]$ on voit que, sous l'hypothèse i), on a $\theta(A_0) \subset K(A)$. Par suite, $\theta(A_0^{-1}) = (\theta(A_0))^{-1} \subset K(A)$. Il s'ensuit, par récurrence, que $\theta(A_n) \subset K(A)$ pour tout $n \geq 0$, et donc que $\theta(K(A)) \subset K(A)$, c'est-à-dire ii).

□

Lemme 3.– *Soient H un corps et $\sigma \in \mathrm{Aut}(H)$. Si $f \in H(t,\sigma)$ est tel qu'une des dimensions droite ou gauche $[H(f) : H]_{d\,\mathrm{ou}\,g}$ est finie, alors $f \in H$ et donc $H(f) = H$. En conséquence de quoi, si $H(t,\sigma)/\Omega/H$ désigne une extension intermédiaire, alors on a*

$$[\Omega : H]_{d\,\mathrm{ou}\,g} \text{ finie} \Longleftrightarrow \Omega = H$$

Preuve : Soit $f \notin H$. Plongeons $H(t,\sigma)$ dans son corps de séries tordu $H((t,\sigma))$ et écrivons $f = f_0 t^v$ où $f_0 \in H((t,\sigma))$ est de valuation nulle. Si $v \neq 0$, alors la famille $\{f^n\}_n$ est étagée en valuation et forme donc une famille H-libre à droite et à gauche dans $H((t,\sigma))$ et donc *a fortiori* dans $H(t,\sigma)$. On a donc $[H(f) : H]_{d\,\mathrm{et}\,g} = +\infty$.
Si $v = 0$, quitte à multiplier f par l'inverse de son terme constant (ce qui ne change pas le corps $H(f)$), on peut écrire $f = f_0 = 1 + f_1.t^k$ avec $k \geq 1$ et $f_1 \in H((t,\sigma))$ de valuation nulle. On montre, par récurrence, que pour tout $n \geq 1$, on a $f^n = 1 + nf_1.t^k + s_n$ où $s_n \in H((t,\sigma))$ est de valuation $v(s_n) \geq 2k$:

$$f^{n+1} = (1 + f_1.t^k)(1 + nf_1.t^k + s_n) = 1 + (n+1)f_1.t^k + \overbrace{\underbrace{n.(f_1.t^k)^2}_{v=2k \text{ ou } +\infty} + \underbrace{s_n}_{v\geq 2k} + \underbrace{f_1.t^k.s_n}_{v\geq 3k}}^{s_{n+1}}$$

On choisit un entier $n \geq 2$ tel que $(n-1)$ soit premier à la caractéristique de H. On pose alors $g = f^n - f = (n-1)f_1.t^k + s_n \in H(f)$ qui est visiblement non nul et de valuation $v = k \geq 1$. L'étude du cas précédent assure alors que $[H(f) : H]_{d\,\mathrm{et}\,g} \geq [H(g) : H]_{d\,\mathrm{et}\,g} = +\infty$.

Si $[\Omega : H]_{d\,\mathrm{ou}\,g}$ est finie, alors il existe une famille finie $f_1, \cdots, f_n \in \Omega$ tels que $\Omega = H(f_1, \cdots, f_n)$. Comme chaque $H(f_i)$ est de dimension droite ou gauche finie sur H, on a d'après ce qui précède

$$\Omega = H(f_1, f_2, \cdots, f_n) = H(f_1)(f_2)\cdots(f_n) = H(f_2)\cdots(f_n) = \cdots = H(f_n) = H$$

□

Définition 4.– *On dit qu'une extension H/K est* superalgébrique *si pour tout partie finie $A \subset H$, le corps $K(A)$ est de dimension finie sur K.*

Etant donné un automorphisme $\sigma \in \mathrm{Aut}(H)$, on dit que H/K est superalgébrique relativement à σ *si pour tout partie finie $A \subset H$, il existe un corps intermédiaire $H/\Omega/K$ tel que* $\begin{cases} \bullet\ A \subset \Omega \\ \bullet\ [\Omega : K]_d < +\infty \\ \bullet\ \sigma_{|\Omega} \in \mathrm{Aut}(\Omega) \end{cases}$

La situation la plus classique rentrant dans le cadre de cette définition est celle d'une extension H/K qui est, algébrique, galoisienne et extérieure. La généralisation de la théorie de Galois à cette situation (due à Jacobson, voir [Coh] et [Jac]), montre que l'extension H/K est superalgébrique relativement à tout élément $\sigma \in \mathrm{Gal}(H/K)$.

Lemme 5.– *a) Soient H/K une extension de corps, $\sigma \in \mathrm{Aut}(H)$ tel que $\sigma_{|K} \in \mathrm{Aut}(K)$ et $\varphi : H(t,\sigma) \longrightarrow H((t,\sigma))$ le plongement canonique de $H(t,\sigma)$ dans le corps des séries tordu. Si H/K est* superalgébrique relativement à σ *alors, pour tout $R \in H(t,\sigma)$, on a*

$$R \in K(t,\sigma) \Longleftrightarrow \varphi(R) \in K((t,\sigma))$$

b) Soient K un corps, $\sigma \in \mathrm{Aut}(K)$ et $n \geq 1$ un entier. Pour tout $R \in K(t,\sigma)$, on a

$$R \in K(t^n, \sigma^n) \Longleftrightarrow \varphi(R) \in K((t^n, \sigma^n))$$

Preuve : Notons, pour commencer, que les équivalences sont vraies en toute généralité si l'on suppose que R est un polynôme.

a) **Cas** $[H : K]_d < +\infty$: Soit $R = PQ^{-1} \in H(t,\sigma)$ tel que $\varphi(R) \in K((t,\sigma))$. D'après [Des2,Prop.1], il existe $Q_0 \in H(t,\sigma)$ tel que $QQ_0 \in K[t,\sigma]$. On a alors $R = PQ^{-1} = (\underbrace{PQ_0}_{\in H[t,\sigma]}).(\underbrace{QQ_0}_{\in K[t,\sigma]})^{-1}$ et donc

$$\varphi(PQ_0) = \underbrace{\varphi(R)}_{\in K((t,\sigma))}.\underbrace{\varphi(QQ_0)}_{\in K[[t,\sigma]]} \in K((t,\sigma))$$

Puisque PQ_0 est un polynôme, ceci implique que $PQ_0 \in K[t,\sigma]$ et donc que finalement $R \in K(t,\sigma)$.

Cas général : Soit $R = PQ^{-1} \in H(t,\sigma)$ et A l'ensemble (fini) des coefficients des polynômes P et Q. On prend un sous-corps Ω vérifiant les conditions de superalgébricité pour la partie A et l'automorphisme σ, de sorte que $R \in \Omega(t,\sigma)$. En appliquant le premier cas on en déduit alors que $R \in K(t,\sigma)$.

b) On suit la même stratégie que pour le a), en établissant d'abord un analogue de [Des2,Prop.1] :

Lemme 6.– *Soient K un corps, $\sigma \in \mathrm{Aut}(K)$ et $n \geq 1$ un entier. Pour tout $Q \in K[t,\sigma]$ de degré k, il existe un polynôme non nul $Q_0 \in K[t,\sigma]$ de degré $m \leq k(n-1)$ tel que $Q_0Q \in K(t^n,\sigma^n)$.*

Preuve du Lemme 6: Posons $Q(t) = a_0 + \cdots + a_kt^k$ et formellement $Q_0(t) = x_0 + \cdots + x_mt^m$. On a alors

$$Q_0(t)Q(t) = \sum_{\ell=0}^{k+m} \underbrace{\left(\sum_{\substack{i+j=\ell \\ i\leq m, j\leq k}} x_i\sigma^i(a_j) \right)}_{E_\ell} t^\ell$$

L'équation $E_\ell = 0$ est alors une équation K-linéaire à droite, d'indéterminées $x_0, \cdots, x_m$. On voit alors que $Q_0 \neq 0$ vérifie $Q_0(t)Q(t) \in K[t^n,\sigma^n]$ si et seulement si le $(m+1)$-uplet $(x_0, \cdots, x_m) \in K^{m+1}$ est solution non nulle du système linéaire $\{E_\ell = 0\}_{\ell \not\equiv 0 \bmod(n)}$. Ce système contient $k + m - [\frac{k+m}{n}]$ équations et $m+1$ inconnues. Pour le choix $m = k(n-1)$, on a $k + m - [\frac{k+m}{n}] = m < m+1$ et il y a donc strictement plus d'inconnues que d'équations dans le système $\{E_\ell = 0\}_{\ell \not\equiv 0 \bmod(n)}$. Ce dernier possède donc une solution non nulle[1].

□

On considère $R = Q^{-1}P$ tel que $\varphi(R) \in K((t^n,\sigma^n))$, on écrit $R = (Q_0Q)^{-1}(Q_0P)$ où $Q_0 \in K[t,\sigma]$ est tel $Q_0Q \in K[t^n,\sigma^n]$ et l'on a alors $\varphi(Q_0P) = \varphi(Q_0Q)\varphi(R) \in K((t^n,\sigma^n))$. Puisque $Q_0P \in K[t,\sigma]$, on a donc $Q_0P \in K[t^n,\sigma^n]$ et finalement que $R \in K(t^n,\sigma^n)$.

□

Lemme 7.– *a) Soient H/K une extension de corps et $\sigma \in \mathrm{Aut}(H)$ tel que $\sigma_{|K} \in \mathrm{Aut}(K)$. Si $[H : K]_d$ est finie alors $[H(t,\sigma) : K(t,\sigma)]_d = [H : K]_d$.*

b) Pour tout corps K, tout isomorphisme $\sigma \in \mathrm{Aut}(K)$ et tout entier $n \geq 1$, on a $[K(t,\sigma) : K(t^n,\sigma^n]_d = [K(t,\sigma) : K(t^n,\sigma^n)]_g = n$.

Preuve : a) Il s'agit du théorème 2 de [Des2].

b) En plongeant $K(t,\sigma)$ dans $K((t,\sigma))$ et en remarquant que $\{1, t, \cdots, t^{n-1}\}$ est une $K((t^n,\sigma^n))$-base à droite et à gauche de $K((t,\sigma))$, on voit que la famille $\{1, t, \cdots, t^{n-1}\}$ est $K(t^n,\sigma^n)$-libre à droite et à gauche. Dans $K(t,\sigma)$, considérons le $K(t^n,\sigma^n)$-espace vectoriel à gauche (resp. à droite) $\Omega = \bigoplus_{i=0}^{n-1} K(t^n,\sigma^n).t^i$ (resp.

[1]Les théorèmes de dimension, en algèbre linéaire sur un corps gauche, sont les même que dans le cas commutatif. En particulier l'égalité $\dim(F_1 + F_2) = \dim(F_1) + \dim(F_2) - \dim(F_1 \cap F_2)$ est valable pour toute paire F_1, F_2 de sous-espaces d'un K-espace vectoriel (à gauche ou à droite) donné. Ici, les solutions de (E_ℓ) forment un sous-espace de dimension $\geq m$ du K-espace vectoriel à droite K^{m+1} et l'application de la formule précédente prouve finalement, par récurrence, que l'intersection de ces sous-espaces est de dimension au moins 1.

$\Omega = \bigoplus_{i=0}^{n-1} t^i.K(t^n, \sigma^n))$. Puisque $K(t^n, \sigma^n)$ est visiblement invariant par conjugaison par t, on voit que Ω est en fait un sous-anneau de $K(t, \sigma)$. Puisque Ω est inclus dans le corps $K(t, \sigma)$, c'est un anneau sans diviseur de zéro qui est, par ailleurs, de dimension finie n sur le corps $K(t^n, \sigma^n)$, il s'agit donc d'un sous-corps de $K(t, \sigma)$[2] de dimension n sur $K(t^n\sigma^n)$. Puisque $K \subset \Omega$ et $t \in \Omega$, on a finalement $\Omega = K(t, \sigma)$.

□

Lorsque H/K désigne une extension extérieure, les centres sont aussi en extension $Z(H)/Z(K)$. Si l'on suppose en plus que H/K est galoisienne finie alors $Z(H)/Z(K)$ l'est aussi et l'application de restriction à $Z(H)$ induit un épimorphisme de groupes $\mathrm{Gal}(H/K) \longrightarrow \mathrm{Gal}(Z(H)/Z(K))$ (voir [Des1,Prop.6]). Dans le cas cyclique, on introduit la terminologie suivante :

Définition 8.– *a) Une extension H/K sera dite "complétement kummérienne" si*

- *H/K est galoisienne, extérieure et cyclique,*
- *la caractéristique de H est première à $n = [H : K]$ et $\mu_n \subset Z(K)$,*
- $[Z(H) : Z(K)] = [H : K]$.

b) Étant donné un corps H on dira d'un automorphisme $\sigma \in \mathrm{Aut}(H)$ qu'il est "complétement kummérien", si l'extension H/H^σ est complétement kummérienne.

On voit que, si H/K est complétement kummérienne, alors $Z(H)/Z(K)$ est kummérienne au sens classique du terme et que les groupes de Galois $\mathrm{Gal}(H/K)$ et $\mathrm{Gal}(Z(H)/Z(K))$ sont canoniquement isomorphes. Remarquons que la condition $[Z(H) : Z(K)] = [H : K]$ n'est pas induite par les autres conditions : si L/k désigne une $\mathbb{Z}_3$-extension (de corps commutatifs) et si σ désigne un générateur topologique de $\mathrm{Gal}(L/k) \simeq \mathbb{Z}_3$ alors l'extension $L(t, \sigma)/L(t^2, \sigma^2)$ est extérieure cyclique de degré 2, mais comme σ^2 est aussi un générateur topologique de $\mathrm{Gal}(L/k)$ (puisque 2 est premier à 3), on déduit que $Z(L(t, \sigma)) = Z(L(t^2, \sigma^2)) = k$.

Lemme 9.–[3] *Si H/K désigne une extension complétement kummérienne et σ est un générateur de $\mathrm{Gal}(H/K)$ alors il existe alors une K-base à gauche de H, $\{a_0, \cdots, a_{n-1}\} \subset Z(H)^n$ telle que, pour tout $i = 1, \cdots, n$, on ait*

$$\sigma(a_i) = \xi_n^i a_i$$

Preuve : On considère le sous-K-espace vectoriel à gauche H_i de H défini par :

$$H_i = \left\{ x \in H / \ \sigma(x) = \xi_n^i x \right\}$$

Si l'on considère un sous-corps commutatif $k \subset K$, on peut voir σ comme un k-endomorphisme de H. Comme $\sigma^n = \mathrm{Id}$, le polynôme $X^n - 1 \in k[X]$ est annulateur de σ et les hypothèses assurent que ce polynôme est scindé à racines simples. Le lemme des noyaux prouve alors que $H = \bigoplus_{i=0}^{n-1} H_i$. L'extension $Z(H)/Z(K)$ est aussi cyclique (d'ordre n par hypothèse), son groupe de Galois étant engendré par (la restriction à $Z(H)$ de) σ. Les hypothèses assurent que $Z(H)/Z(K)$ est kumérienne et il existe donc $a \in Z(K)$ tel que $Z(H) = Z(K)(\sqrt[n]{a})$. Pour tout $i = 0, \cdots, n-1$, on pose $a_i = \sqrt[n]{a^i}$ et l'on voit alors que $\sigma(a_i) = \xi_n^i.\sqrt[n]{a}$, c'est-à-dire $a_i \in H_i$. On en déduit que les H_i sont tous des K-droites linéaires et la famille $\{\sqrt[n]{a^i}\}_{i=0,\cdots,n-1}$ fournit alors la base recherchée.

□

Proposition 10.– *Soient H un corps, $\sigma \in \mathrm{Aut}(H)$ un automorphisme complétement kummérien d'ordre n et $K = H^\sigma$.*

[2] Tout anneau qui est sans diviseur de zéro et qui est de dimension finie sur un corps est lui-même un corps. En effet, pour $a \neq 0$ fixé, l'endomorphisme $x \longmapsto ax$ est injectif par intégrité de l'anneau et, par suite, surjectif puisque l'anneau est un espace vectoriel de dimension finie. Ainsi, il existe x tel que $ax = 1$.

[3] Ce lemme est un raffinement de [Coh, Prop.3.7.2].

a) En tant que $H(t^n)$-espace vectoriel à gauche, on a $H(t,\sigma) = \bigoplus_{i=0}^{n-1} H(t^n).t^i$.

b) Considérons un élément $f = f_0 + \cdots + f_{n-1} \in H(t,\sigma)$ avec $f_i \in H(t^n).t^i$. Pour tout $i = 0, \cdots, n-1$ on a $f_i \in H(f)$.

Preuve : a) La famille $\{1, t, \cdots, t^{n-1}\}$ est visiblement une $H((t^n))$-base à gauche de $H((t,\sigma))$, on en déduit qu'elle est $H(t^n)$-libre à gauche, vue comme famille d'éléments de $H(t,\sigma)$. Puisque, d'après le lemme 7, on a $[H(t,\sigma) : H(t^n)] = n$, on en déduit finalement que $H(t,\sigma) = \bigoplus_{i=0}^{n-1} H(t^n).t^i$.

b) Puisque l'extension est complétement kummérienne, on peut se doter d'une K-base $\{a_0, \cdots, a_{n-1}\}$ du corps H qui vérifie les propriétés du lemme 9. Comme t^n est central dans $H(t,\sigma)$ et que $a_i \in Z(H)$, l'automorphisme $I(a_i^{-1})$ laisse invariants les éléments de $H(t^n)$. Il s'ensuit que, pour tout $k = 0, \cdots, n-1$, on a $I(a_i^{-1})(f_k) = a_i^{-1}\sigma^k(a_i)f_k = \xi_n^{ik} f_k$. Ainsi, en appliquant $I(a_i^{-1})$ à l'élément f pour $i = 0, \cdots, n-1$, on obtient

$$(S)\ \begin{cases} f_0 + & f_1 + & \cdots + & f_{n-1} = \alpha_0 \\ f_0 + & \xi_n f_1 + & \cdots + & \xi_n^{n-1} f_{n-1} = \alpha_1 \\ & & \vdots & \\ f_0 + & \xi_n^{n-1} f_1 + & \cdots + & \xi_n^{(n-1)^2} f_{n-1} = \alpha_{n-1} \end{cases}$$

où $\alpha_i = I(a_i^{-1})(f)$. Puisque $\mu_n \subset Z(K)$, on peut considérer (S) comme un système $Z(K)$-linéaire dont le n-uplet $(f_0, \cdots, f_{n-1})$ est une solution dans le $Z(K)$-espace vectoriel $K(t,\sigma)$. Le déterminant du système homogène est un déterminant de Vandermonde

$$\begin{vmatrix} 1 & 1 & \cdots & \cdots & 1 \\ 1 & \xi_n & \cdots & \cdots & \xi_n^{n-1} \\ \vdots & \vdots & & & \vdots \\ \vdots & \vdots & & & \vdots \\ 1 & \xi_n^{n-1} & \cdots & \cdots & \xi_n^{(n-1)^2} \end{vmatrix} = \prod_{0 \le i < j \le n-1} (\xi_n^i - \xi_n^j) \neq 0$$

qui est non nul. On en déduit que (S) possède une unique solution dans $K(t,\sigma)$: $(f_0, \cdots, f_{n-1})$. Maintenant, comme $a_i \in H$, on a $\alpha_i \in H(f)$ et l'on peut regarder (S) comme $Z(K)$-système linéaire dans $H(f)$. Ce système admet aussi une unique solution dans $H(f)$ et comme $H(f) \subset H(t,\sigma)$, on a finalement $f_0, \cdots, f_{n-1} \in H(f)$.

□

2.— Réduction au cas d'une indéterminée centrale.

2.1.— Réduction.

Dans ce §2.1. l'on considère un corps H (non nécessairement commutatif), un automorphisme $\sigma \in \mathrm{Aut}(H)$ complétement kummérien d'ordre $n \geq 1$ et l'on pose $K = H^\sigma$.

Proposition 11.— *1) a) L'extension $H(t,\sigma)/K(t^n)$ est une extension galoisienne, intérieure, finie et concentrique, de centre commun $Z(K)(t^n)$.*

b) $H(t,\sigma) = K(t^n) \otimes_{Z(K)(t^n)} Z(H)(t,\sigma)$.

c) L'extension $H(t^n)/K(t^n)$ est galoisienne extérieure cyclique et $H(t,\sigma)$ est un produit croisé (au sens généralisé de [Des1]) cyclique.

d) L'extension $H(t,\sigma)/H(t^n)$ est galoisienne intérieure et l'on a plus précisément $H(t^n) = H(t,\sigma)^{I(A)}$ où $A = \{a_0, \cdots, a_{n-1}\}$ désigne une K-base de H vérifiant les propriétés du lemme 9.

2) On considère $H(t,\sigma)/\Omega/H$ un corps intermédiaire et, pour tout $i = 0, \cdots, n-1$, on pose $D_i = \Omega \cap H(t^n).t^i$, de sorte que $D_0 = \Omega \cap H(t^n)$ est un sous-corps de Ω et que D_i est un sous-D_0-espace vectoriel à gauche de Ω. On a alors :

a) En tant que D_0-espace vectoriel à gauche, $\Omega = \bigoplus_{i=0}^{n-1} D_i$.

b) Pour tout $i = 0, \cdots, n-1$, $\dim_{D_0}(D_i) = 0$ ou 1.

c) On a $D_0 = \Omega^{I(A)}$ et, en particulier, l'extension Ω/D_0 est galoisienne intérieure finie.

3) Si Ω désigne une extension intermédiaire de $H(t,\sigma)/H$ différente de H alors $D_0 = \Omega \cap H(t^n)$ est une extension intermédiaire de $H(t^n)/H$ différente de H.

Preuve : a) Par application de [Coh,Th.2.2.10], on a $Z(K(t^n)) = Z(K)(t^n)$ et $Z(H(t,\sigma)) = Z(H)^\sigma(t^n)$. Comme $Z(H)^\sigma = Z(H) \cap H^\sigma = Z(H) \cap K$ et que, par extériorité, on a $Z(K) \subset Z(H)$, on en déduit que $Z(H(t,\sigma)) = Z(K)(t^n) = Z(K(t^n))$, c'est-à-dire que l'extension $H(t,\sigma)/K(t^n)$ est concentrique. On remarque que cette propriété découle juste du fait que l'extension H/K est extérieure.
Puisque $[Z(H) : Z(K)] = [H : K] = n$, on dispose, par restriction des automorphismes, d'un isomorphisme de groupes $\mathrm{Gal}(H/K) \longrightarrow \mathrm{Gal}(Z(H)/Z(K))$. Étudions le bicommutant $\widetilde{\widetilde{K(t^n)}}$: puisque t^n est central, on a $\widetilde{K(t^n)} = \widetilde{K}$ et l'on voit alors qu'un élément $\sum_i \lambda_i t^i \in H(t,\sigma) \subset H((t,\sigma))$ est élément de $\widetilde{K(t^n)}$, si et seulement si $\lambda_i \in \mathscr{C}_H(K) = Z(H)$ (cette dernière égalité venant de l'hypothèse d'intériorité) pour tout i, c'est-à-dire que $\widetilde{K(t^n)} = H(t,\sigma) \cap Z(H)((t,\sigma))$. On a visiblement $Z(H)(t,\sigma) \subset \widetilde{K(t^n)}$ et donc $\widetilde{\widetilde{K(t^n)}} \subset Z(\widetilde{H)(t,\sigma)}$. Réciproquement, si $f \in Z(\widetilde{H)(t,\sigma)} = \widetilde{Z(H)} \cap \{t\}$ alors l'image de f dans $H((t,\sigma))$ commute visiblement avec tous les éléments de $Z(H)((t,\sigma))$ et donc $f \in \widetilde{\widetilde{K(t^n)}}$. On a donc finalement $\widetilde{\widetilde{K(t^n)}} = \widetilde{Z(H)} \cap \{t\} = Z(\widetilde{H)(t)}$. Ainsi, pour tout élément $f = \sum_i \lambda_i t^i \in H(t,\sigma) \subset H((t,\sigma))$, on a

$$f \in \widetilde{\widetilde{K(t^n)}} \iff \begin{cases} tf = ft \\ \forall x \in Z(H)\ xf = fx \end{cases} \iff \begin{cases} \forall i\ \sigma(\lambda_i) = \lambda_i \\ \forall i\ \forall x \in Z(H)\ x\lambda_i = \sigma^i(x)\lambda_i \end{cases} \iff \begin{cases} \forall i\ \lambda_i \in K \\ \forall i \not\equiv 0(n)\ \lambda_i = 0 \end{cases}$$

$$\iff f \in K((t^n)) \cap H(t,\sigma)$$

Le lemme 5 montre finalement que $\widetilde{\widetilde{K(t^n)}} = K(t^n)$: en plus d'être concentrique, l'extension $H(t,\sigma)/K(t^n)$ est donc galoisienne, intérieure (de groupe $I(\widetilde{K(t^n)})$) et finie (par le lemme 7).

b) On peut appliquer les résultats [Des1] qui montrent que $\widetilde{K(t^n)}$ est une $Z(K(t^n))$-algèbre à division d'indice n et que $H(t,\sigma) = K(t^n) \otimes_{Z(K(t^n))} \widetilde{K(t^n)}$. Comme $Z(Z(H)(t,\sigma)) = Z(H)^\sigma(t^n) = Z(K)(t^n)$, le lemme 5 montre que $[Z(H)(t,\sigma) : Z(K)(t^n)] = n^2$ mais comme $Z(K(t^n)) = Z(K)(t^n)$ et que $Z(H)(t,\sigma) \subset \widetilde{K(t^n)}$ on en déduit que $\widetilde{K(t^n)} = Z(H)(t,\sigma)$. On en déduit finalement, par application de [Des1], que

$$H(t,\sigma) = K(t^n) \otimes_{Z(K)(t^n)} Z(H)(t,\sigma)$$

c) Le fait que $H(t^n)/K(t^n)$ soit galoisienne extérieure cyclique découle immédiatement de [Des2,th.4]. L'algèbre à division associée à l'extension $H(t,\sigma)/K(t^n)$ est $Z(H)(t,\sigma)$ et c'est un produit croisé car l'extension $Z(H)(t^n)/Z(K)(t^n)$ est galoisienne. Ceci assure, d'après [Des1,Coro.30], que $H(t,\sigma)$ est bien le produit croisé de l'extension cyclique $H(t^n)/K(t^n)$ par un certain 2-cocyle à valeurs dans $Z(H(t^n))^*$.

d) On considère le plongement $H(t,\sigma) \subset H((t,\sigma))$. On a

$$y = \sum_k \lambda_k t^k \in H(t,\sigma)^{I(a_1)} \iff a_1\left(\sum_k \lambda_k t^k\right)a_1^{-1} = \sum_k \xi_n^{-k}\lambda_k t^k = \sum_k \lambda_k t^k \iff y \in H((t^n))$$

et, par application du lemme 5, on a $y \in H(t,\sigma)^{I(a_1)} \iff y \in H(t^n)$. On a donc $H(t,\sigma)^{I(A)} \subset H(t,\sigma)^{I(a_1)} = H(t^n) \subset H(t,\sigma)^{I(A)}$.

2) a) Puisque les $H(t^n).t^i$ sont en somme directe en tant que $H(t^n)$-espaces vectoriels à gauche, il en est de même des D_i en tant que D_0-espaces vectoriels à gauche. Si $f = f_0 + \cdots + f_{n-1} \in \Omega$, la proposition 10.b) montre que $f_i \in H(f) \subset \Omega$ et donc que $f_i \in D_i$. Ceci prouve bien que, finalement, $\Omega = \bigoplus_{i=0}^{n-1} D_i$.

b) Si $D_i \neq \{0\}$, on prend un élément $a \in D_i$ non nul et l'on remarque que si $b \in D_i$ alors $ba^{-1} \in H(t^n) \cap \Omega = D_0$. On a donc $D_i = D_0.a$.

c) Puisque chaque a_i est élément de $Z(H)$ et que $H \subset \Omega$, les éléments de l'ensemble $I(A)$ agissent, par restriction, sur Ω. On a alors $\Omega^{I(A)} = \Omega \cap H(t,\sigma)^{I(A)} = \Omega \cap H(t^n) = D_0$. La finitude de Ω/D_0 découle immédiatement de a) et b).

3) Si $f \in \Omega - H$ alors, par la proposition 10.a), on peut écrire $f = f_0 + \cdots + f_{n-1}$ avec $f_i \in H(t^n).t^i$ pour tout $i = 0, \cdots, n-1$ et l'on sait par 10.b) que $f_0, \cdots, f_{n-1} \in H(f) \subset \Omega$. Si $f_0 \notin H$, on pose $y = f_0 \in \Omega \cap H(t^n) = D_0$, sinon il existe un indice $p \geq 1$ tel que $f_p \neq 0$ et l'on pose alors $y = f_p^n$. On écrit $f_p = gt^p$ avec $g \in H(t^n)$ et l'on voit que, une fois $H(t,\sigma)$ plongé dans $H((t,\sigma))$, la valuation de f_p est élément de $n\mathbb{Z} + p$ et ne peut donc être nulle. Puisque $v(y) = nv(f_p)$, l'élément y est aussi de valuation non nulle ce qui assure que $y \notin H$. Par ailleurs, l'action de $I(t^p)$ laisse globalement invariant le corps $H(t^n)$ puisque t^n est central et que $I(t^p)_{|H} = \sigma^p$. On en déduit que

$$y = (gt^p).\cdots.(gt^p) = g.(t^p g t^{-p}).\cdots.(t^{(n-1)p} g t^{-(n-1)p}).t^{(n-1)p}.t^p = g.I(t^p)(g).\cdots.I(t^{(n-1)p})(g).t^{np} \in H(t^n)$$

et ainsi que $y \in \Omega \cap H(t^n) = D_0$. On vient de montrer qu'il existe $y \in D_0$ tel que $y \notin H$ c'est-à-dire que D_0 est une extension intermédiaire de $H(t^n)/H$ non égale à H

□

Comme première application de cette proposition, établissons un résultat de finitudes :

Théorème 12.– *Si Ω désigne une extension intermédiaire de $H(t,\sigma)/H$ différente de H alors :*

a) Les dimensions droite et gauche $[H(t,\sigma) : \Omega]_{d,g}$ sont égales et finies.

b) L'extension Ω/H est de type fini.

Preuve : Cas particulier où $\sigma = \mathrm{Id}$.

a) Puisque Ω n'est pas égal à H, on peut donc considérer un élément $f = p(t)q(t)^{-1} \notin H$ avec $p(t), q(t) \in H[t]$. Le fait que $f \notin H$ assure que l'équation $p(t) - fq(t) = 0$ est une équation de dépendance $H(f)$-linéaire à gauche non triviale d'une certaine famille $\{1, t, \cdots, t^n\}$ de puissances de t avec $n \geq 1$. Parmi toutes les équations de dépendance Ω-linéaire à gauche du type

$$t^n = \lambda_0 + \cdots + \lambda_{n-1} t^{n-1}$$

il en existe une avec $n = n_0 \geq 2$ minimal et celle-ci est visiblement unique pour cette propriété (c'est l'analogue du polynôme minimal dans le cas commutatif). La famille $\{1, t, \cdots, t^{n_0}\}$ est ainsi Ω-libre à gauche et l'on voit, par récurrence immédiate, que $t^n \in \Omega_0 = \bigoplus_{i=0}^{n_0-1} \Omega.t^i$ pour tout $n \geq 0$. Puisque l'élément t est central dans $H(t)$, on voit que Ω_0 est en fait un sous-anneau de $H(t)$ et comme il est de dimension finie sur un corps, c'est lui-même un corps. Puisque $H \cup \{t\} \subset \Omega_0$ on en déduit que $\Omega_0 = H(t)$ et que $\{1, t, \cdots, t^{n_0}\}$ est une Ω-base à gauche de $H(t)$. C'est aussi une Ω-base à droite puisque tous ses éléments sont centraux.

b) Si l'on considère $f \in \Omega - H$, alors d'après a) on a $[H(t) : H(f)] < +\infty$ et donc $[\Omega : H(f)] < +\infty$. L'extension Ω/H est donc bien de type fini.

Cas général.

a) La proposition 11.3) assure que le corps $D_0 = \Omega \cap H(t^n)$ est différent de H et l'on peut donc appliquer le cas particulier afin d'assurer que $[H(t^n) : \Omega]_g = [H(t^n) : \Omega]_d < +\infty$. D'après proposition 11, les extensions

$H(t,\sigma)/H(t^n)$ et Ω/D_0 sont galoisiennes et finies. On a donc $[H(t,\sigma):H(t^n)]_d = [H(t,\sigma):H(t^n)]_g = n$ et $[\Omega:D_0]_d = [\Omega:D_0]_g \leq n$. La transitivité des degrés permet alors de conclure.

b) Puisque $[\Omega:D_0] < +\infty$ et que, d'après le cas particulier, D_0/H est de type fini, on en déduit bien que Ω/H est de type fini.

□

Examinons maintenant la réduction au cas de l'indéterminée centrale pour la généralisation du théorème de Lüroth :

Théorème 13.– *Si le corps des fractions à indéterminée centrale $H(t) = H(t,\mathrm{Id})$ vérifie la généralisation du théorème de Lüroth alors le corps de fractions tordu $H(t,\sigma)$ vérifie aussi la généralisation du théorème de Lüroth pour tout automorphisme complétement kummérien $\sigma \in \mathrm{Aut}(H)$.*

Preuve : D'après la proposition 11.3), le corps $D_0 = \Omega \cap H(t^n)$ est une extension intermédiaire de $H(t^n)/H$ non égale à H et puisque, par hypothèse, le corps $H(t^n)$ vérifie la généralisation du théorème de Lüroth, il existe donc $\gamma_0 \in H(t^n)$ tel que $D_0 = H(\gamma_0)$. En utilisant la proposition 11.2), pour tout $i = 0,\cdots,n-1$, on peut considérer un générateur (éventuellement nul) $x_i \in \Omega$ du sous-espace D_i et l'on a alors, grâce à la proposition 10.b),

$$\Omega = \bigoplus_{i=0}^{n-1} D_0.x_i = \bigoplus_{i=0}^{n-1} H(\gamma_0).x_i \subset H(\gamma_0,x_1,\cdots,x_{n-1}) = H(\gamma_0+x_1+\cdots+x_{n-1}) \subset \Omega$$

L'élément $u = \gamma_0+x_1+\cdots+x_{n-1} \in \Omega$ vérifie donc $\Omega = H(u)$. Le fait que $[H(t,\sigma):\Omega]_g = [H(t,\sigma):\Omega]_d < +\infty$ est assuré par le théorème 12.a).

□

Remarque : La condition $[Z(H):Z(K)] = [H:K]$ incluse dans l'hypothèse *complétement* kummérien caractérise le fait que l'extension est $H(t,\sigma)/K(t^n)$ est une extension galoisienne, intérieure, finie et concentrique. En effet, on sait déjà qu'elle est concentrique en toute généralité et le fait qu'elle soit galoisienne, intérieure, finie équivaut à dire que $\widetilde{\widetilde{K(t^n)}} = K(t^n)$. On note $d = [Z(H):Z(K)]$ et l'on sait alors que $d|n$ et que l'on dispose, par restriction des automorphismes, d'un épimorphisme de groupes $\mathrm{Gal}(H/K) \longrightarrow \mathrm{Gal}(Z(H)/Z(K))$ dont le noyau est visiblement engendré par σ^d. Le même calcul que dans la preuve de la proposition 11.a) montre que $\widetilde{\widetilde{K(t^n)}} = K(t^d)$ et qu'en conclusion

L'extension $H(t,\sigma)/K(t^n)$ est galoisienne, intérieure, finie et concentrique $\Longleftrightarrow [Z(H):Z(K)] = [H:K]$

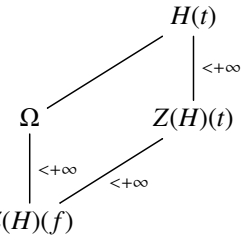
2.2.– Applications.

L'application du théorème 13 la plus immédiate est celle où H est un corps commutatif. Grâce à [LP] on peut généraliser aux cas des algèbres à division :

Corollaire 14.– (Généralisation de Lüroth) *Si H désigne une algèbre à division et si $\sigma \in \mathrm{Aut}(H)$ est un automorphisme complètement kummérien alors le corps $H(t,\sigma)$ vérifie la généralisation du théorème de Lüroth.*

Preuve : Le théorème [LP,Th.1.1] affirme que pour tout corps intermédiaire $H(t)/\Omega/H$ différent de H, il existe $f \in Z(H)(t) - Z(H)$ tel que $\Omega = H(f)$. Puisque $Z(H(t)) = Z(H)(t)$ (conséquence de [Coh,Th.2.2.10]) et que, par hypothèse, $[H:Z(H)] < +\infty$, on a $[H(t):Z(H)(t)]_d < +\infty$ (lemme 7.a)) et donc $H(t)$ est une $Z(H)(t)$-algèbre à division. On en déduit que $[H(t):Z(H)(f)]_g = [H(t):Z(H)(f)]_d < +\infty$. Par ailleurs, comme f est central dans $H(f) = \Omega$ on a $Z(H)(f) \subset Z(\Omega)$ et donc $[\Omega:Z(H)(f)]_g = [\Omega:Z(H)(f)]_d < +\infty$

et le diagramme suivant



prouve finalement que $[H(t) : \Omega]_g = [H(t) : \Omega]_d < +\infty$: le corps $H(t)$ vérifie bien la généralisation du théorème de Lüroth et l'on peut donc appliquer le théorème 13.

□

Remarque : L'étude de l'arithmétique de $H(t)$ menée dans [DL] permet de bien décrire le cadre d'application du corollaire 14 : si H/K désigne une extension galoisienne extérieure finie et que H est une algèbre à division, alors

1/ K est aussi une algèbre à division,

2/ $Z(H)/Z(K)$ est une extension galoisienne de même groupe que celui de H/K,

3/ $H = K \otimes_{Z(K)} Z(H)$,

(le 2/ et le 3/ viennent de [DL,Cor.2] et le 1/ découle immédiatement de 2/) et réciproquement, si K est une algèbre à division et $L/Z(K)$ désigne une extension galoisienne de corps commutatifs qui a un groupe de Galois fini G, alors si $H = K \otimes_Z (K)L$ est un corps, c'est une L-algèbre à division et l'extension H/K est galoisienne extérieure de groupe G. Enfin, la condition "$H = K \otimes_Z (K)L$ est un corps" équivaut à dire que la forme associée à la norme réduite (relativement au choix d'une $Z(K)$-base de K) ne possède que le zéro trivial sur L (proposition 6 et théorème 7 de [DL]). Pour trouver des exemples d'illustration, on a donc tout intérêt à fixer K et trouver des extensions cycliques de $L/Z(K)$ telle que la forme réduite de K reste sans zéro sur L.

3.— Cas où le corps des constantes est commutatif.

Dans tout le §3 on considère un corps commutatif H et un automorphisme $\sigma \in \mathrm{Aut}(H)$ complétement kummérien (ce qui revient ici à supposer que H/K est kummérienne) d'ordre $n \geq 1$ et l'on pose $K = H^\sigma$.

3.1.— Structure des extensions intermédiaires.

Regardons, pour commencer, la structure de $H(t, \sigma)$:

Proposition 15.— *a) Le corps $H(t^n) = H(t^n, \sigma^n)$ est commutatif et c'est le commutant $\widetilde{H}$ du corps H dans $H(t, \sigma)$. Tout sous-corps commutatif Z de $H(t, \sigma)$ qui contient H est un sous-corps de $H(t^n)$ (i.e. le corps $H(t^n)$ est le plus grand élément de l'ensemble des sous-corps commutatifs de $H(t, \sigma)$ qui contiennent H).*

b) Le corps $H(t, \sigma)$ est une $K(t^n)$-algèbre à division d'indice n. Le corps $H(t^n)$ est un sous-corps commutatif maximal de l'extension $H(t, \sigma)/K(t^n)$ et l'extension $H(t^n)/K(t^n)$ est cyclique de groupe de Galois canoniquement isomorphe à $\mathrm{Gal}(H/K)$. Le corps $H(t, \sigma)$ est ainsi un produit croisé cyclique.

c) Si $f \in H(t, \sigma)$ est un élément non nul, alors pour tout $i = 0, \cdots, n-1$,

$$I(f)_{|H} = \sigma^i \Longleftrightarrow f \in H(t^n).t^i$$

Preuve : On regarde les éléments de $H(t, \sigma)$ comme des séries *via* le plongement canonique $H(t, \sigma) \subset H((t, \sigma))$.

a) L'élément t^n est visiblement central dans $K(t,\sigma)$ et comme H est commutatif il s'ensuit que $H(t^n)$ est bien commutatif. Soit $y = \sum_k \lambda_k t^k \in H(t,\sigma)$. On a

$$\begin{aligned} y \in \widetilde{H} &\iff \forall \lambda \in H,\ \lambda\left(\sum_k \lambda_k t^k\right) = \left(\sum_k \lambda_k t^k\right)\lambda \iff \forall \lambda \in H,\ \sum_k \lambda\lambda_k t^k = \sum_k \sigma^k(\lambda)\lambda_k t^k \\ &\iff \forall \lambda \in H, \forall k,\ \lambda\lambda_k = \sigma^k(\lambda)\lambda_k \iff \forall k \not\equiv 0 \bmod(n),\ \lambda_k = 0 \\ &\iff y = \sum_k \lambda_{kn} t^{kn} \in H((t^n)) \end{aligned}$$

Le lemme 5.b) prouve alors que $y \in \widetilde{H} \iff y \in H(t^n)$.

Si $Z \subset H(t,\sigma)$ est commutatif et contient H alors tout élément de Z commute avec tout élément de H et donc $Z \subset \widetilde{H} = H(t^n)$.

b) L'application de [Coh,Th.2.2.10] montre que $Z(H(t,\sigma)) = K(t^n)$. L'application du lemme 7 à la tour $H(t,\sigma)/H(t^n)/K(t^n)$ montre que l'on a

$$\begin{array}{c} H(t,\sigma) \\ \Big| n \\ H(t^n) \\ \Big| n \\ K(t^n) \end{array}$$

et ainsi, $H(t,\sigma)$ est une $K(t^n)$-algèbre à division d'indice n. Puisque d'après a), $H(t^n)$ est commutatif et que $[H(t^n) = Z(H(t,\sigma))] = n$ il s'agit d'un corps commutatif maximal dans $H(t,\sigma)/Z(H(t,\sigma))$. Puisque H/K est une extension galoisienne cyclique, l'extension $H(t^n)/K(t^n)$ est aussi galoisienne cyclique de même groupe de Galois que $\mathrm{Gal}(H/K)$. Tout ceci montre que $H(t,\sigma)$ est bien un produit croisé cyclique.

c) Soit $y = \sum_k \lambda_k t^k \in H(t,\sigma)$ non nul et $i \in \{0, \cdots, n-1\}$. On a

$$\begin{aligned} I(y)_{|H} = \sigma^i &\iff \forall \lambda \in H,\ \sigma^i(\lambda)\left(\sum_k \lambda_k t^k\right) = \left(\sum_k \lambda_k t^k\right)\lambda \iff \forall \lambda \in H,\ \sum_k \sigma^i(\lambda)\lambda_k t^k = \sum_k \sigma^k(\lambda)\lambda_k t^k \\ &\iff \forall \lambda \in H, \forall k,\ \sigma^i(\lambda)\lambda_k = \sigma^k(\lambda)\lambda_k \iff \forall k \not\equiv i \bmod(n),\ \lambda_k = 0 \\ &\iff y = \sum_k \lambda_{kn+i} t^{kn+i} \in H((t^n)).t^i \iff y.t^{-i} \in H((t^n)) \end{aligned}$$

Le lemme 5.b) prouve alors que $I(y)_{|H} = \sigma^i \iff y \in H(t^n).t^i$.

□

On pourra remarquer que la proposition 15 est vraie dans un cadre un peu plus général, puisque sa preuve de n'utilise pas l'hypothèse "H/K kummérienne". Regardons maintenant la structure des extensions intermédiaires :

Théorème 16.– *Soit $H(t,\sigma)/\Omega/H$ une extension intermédiaire différente de H.*

1) a) Le corps Ω est une algèbre à division d'indice $d|n$.

b) Si l'on considère le corps $L = H^{\sigma^{n/d}}$, alors il existe $\gamma_0 \in L(t^n) - L$ tel que $Z(\Omega) = L(\gamma_0)$. En particulier, le degré $m = [L(t^n) : Z(\Omega)]$ est fini.

c) Le corps $D_0 = \Omega \cap H(t^n)$ est égal à $H(\gamma_0)$ et est une extension de corps commutatifs maximale de $Z(\Omega)$ dans Ω. Cette extension est cyclique d'ordre d si bien que, l'algèbre à division Ω est un produit croisé cyclique.

2) Le corps Ω est commutatif si et seulement si $d = 1$, et dans ces conditions, on a $L = H$ et $\Omega = H(\gamma_0)$. Si Ω n'est pas commutatif alors $H(t^n).t^{n/d} \cap \Omega \neq \{0\}$ et quelque soit $x_1 \in H(t^n).t^{n/d} \cap \Omega$ non nul, on a $\Omega = H(\gamma_0 + x_1)$.

Preuve : La proposition 11.2.c) assure que le corps Ω est de dimension finie (droite et gauche) sur le corps commutatif D_0, on en déduit que Ω est aussi de dimension finie sur son centre (voir [Des4.Lem.2.1.]), ce qui assure que c'est bien une algèbre à division.

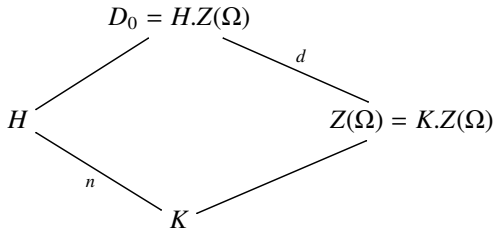
Puisque H est commutatif et inclus dans Ω, le compositum $H.Z(\Omega)$ est un corps commutatif, extension intermédiaire de $\Omega/Z(\Omega)$ contenant H. On en déduit, par la proposition 15.a), que $H.Z(\Omega) \subset H(t^n) \cap \Omega = D_0$. Le corps D_0 est donc une extension de $Z(\Omega)$ mais, toujours à cause de la proposition 15.a), c'est une extension de corps commutatifs de $Z(\Omega)$, maximale dans Ω. On a donc $[\Omega : D_0] = [D_0 : Z(\Omega)] = d$ où d désigne l'indice de Ω.

Montrons que $D_0 = H.Z(\Omega)$: par la proposition 11.2.c), on sait que $\Omega^{I(A)} = D_0$ où $A = \{a_0, \cdots, a_{n-1}\} \subset H$ désigne une K-base de H vérifiant les propriétés du lemme 9. Le corps K est central dans $H(t, \sigma)$ et comme $K \subset \Omega$, on a $K \subset Z(\Omega)$ et, par suite, $Z(\Omega)(A) = H.Z(\Omega)$. Par application du corollaire 2.a), on a alors

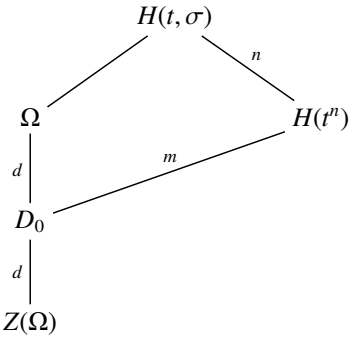
$$\mathscr{C}_\Omega(H.Z(\Omega)) = \mathscr{C}_\Omega(Z(\Omega)(A)) = \mathscr{C}_\Omega(Z(\Omega)) \cap \mathscr{C}_\Omega(A) = \Omega \cap \mathscr{C}_\Omega(A) = \mathscr{C}_\Omega(A) = \Omega^{I(A)} = D_0$$

De l'égalité $\mathscr{C}_\Omega(H.Z(\Omega)) = D_0$ on trouve, par bicommutation, que $H.Z(\Omega) = \mathscr{C}_\Omega(\mathscr{C}_\Omega(H.Z(\Omega))) = \mathscr{C}_\Omega(D_0)$ et, puisque D_0 est commutatif maximal dans Ω, on a finalement $H.Z(\Omega) = \mathscr{C}_\Omega(D_0) = D_0$.

Par extension des scalaires par $Z(\Omega)$, on obtient le diagramme de corps commutatifs suivant :



La théorie de Galois assure alors que $D_0/Z(\Omega)$ est galoisienne et que $\mathrm{Gal}(D_0/Z(\Omega))$ est isomorphe, par restriction des automorphismes à H, à un sous-groupe de $\mathrm{Gal}(H/K)$. Finalement, $D_0/Z(\Omega)$ est cyclique de degré $d|n$, ce qui assure par maximalité de D_0 que Ω est un produit croisé cyclique d'indice d. On a ainsi le diagramme suivant :



(la finitude de $[H(t^n) : D_0]$ étant assurée la proposition 11.3) et le fait que $H(t^n)$ est commutatif). Ainsi, le corps Ω est commutatif si et seulement si $d = 1$ et, dans cette situation, Ω devient un sous-corps de $H(t^n)$ contenant strictement H. Par application du théorème de Lüroth, il existe bien $\gamma_0 \in H(t^n)$ tel que $\Omega = Z(\Omega) = H(\gamma_0)$.

Supposons maintenant que Ω soit gauche, c'est-à-dire que $d \geq 2$. Le morphisme canonique $\mathrm{Gal}(D_0/Z(\Omega)) \longrightarrow \mathrm{Gal}(H/K)$ étant obtenu par restriction des applications au corps H, on peut choisir un générateur θ de

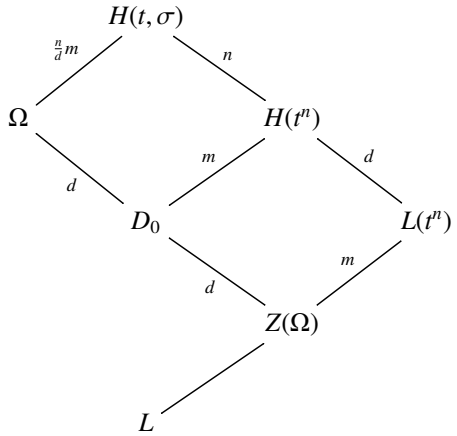
$\mathrm{Gal}(D_0/Z(\Omega))$ tel que $\theta_{|H} = \sigma^{n/d}$. Le théorème de Skolem-Noether assure que θ se relève en un automorphisme intérieur $I(x_1)$ de Ω et la proposition 15.c) assure alors que $x_1 \in H(t^n).t^{n/d} \neq \{0\}$. Pour $i = 1, \cdots, d-1$, on pose $x_i = x_1^i$ et, comme $I(t^{n/d})$ laisse globalement fixe H (et donc $H(t^n)$), on voit que $x_i \in H(t^n).t^{in/d} \cap \Omega$ et que $I(x_i)_{|D_0} = \theta^i$ i.e. $I(x_i)$ relève θ^i à Ω. Par ailleurs, par application du théorème de Lüroth, il existe $x_0 \in H(t^n)$ tel que $D_0 = H(x_0)$ et l'on sait alors que la famille $\{x_0, \cdots, x_{d-1}\}$ est une D_0-base de Ω. On a donc, en posant $x = x_0 + \cdots + x_{d-1}$ et par application de la proposition 10.b),

$$\Omega = \bigoplus_{i=0}^{d-1} D_0.x_i = H(x_0, \cdots, x_{d-1}) = H(x_0 + \cdots + x_{d-1}) = H(x)$$

Par le corollaire 2.a) on a, pour un élément $f \in H(t, \sigma)$,

$$\begin{aligned} f \in \widetilde{\Omega} &\iff \begin{cases} f \in \widetilde{H} = H(t^n) \text{ (proposition 15.a))} \\ fx = xf \end{cases} \\ &\iff \begin{cases} f \in H(t^n) \\ \forall i = 0, \cdots, d-1,\ fx_i = x_i f \text{ (car } x_i \in H(x)) \end{cases} \end{aligned}$$

Chaque élément x_i est non nul et s'écrit $x_i = u_i t^{in/d}$ avec $u_i \in H(t^n)$. Sous la condition $f \in H(t^n)$, on voit que la condition $fx_i = x_i f$ équivaut alors à $ft^{in/d} = t^{in/d} f$ ce qui équivaut encore à $f \in H^{\sigma^{in/d}}(t^n)$ (cela se voit en plongeant $f \in H(t, \sigma)$ dans $H((t, \sigma))$, en faisant agir $I(t^{in/d})$ sur la série f et en utilisant le lemme 5, comme nous l'avons déjà fait précédemment). Finalement, on voit que $\widetilde{\Omega} = L(t^n)$ et donc $Z(\Omega) = \Omega \cap L(t^n)$. On a ainsi,



Par application du théorème de Lüroth, il existe $\gamma_0 \in L(t^n) - L$ tel que $Z(\Omega) = L(\gamma_0)$. Puisque γ_0 est central dans Ω, on voit que $H(\gamma_0)$ est un corps commutatif et comme $[H(\gamma_0) : L(\gamma_0)] = [H : L] = d$, on en déduit que $H(\gamma_0)$ est un sous-corps commutatif maximal intermédiaire de $\Omega/Z(\Omega)$ qui contient H. De la proposition 15.a) on déduit finalement que $D_0 = H(\gamma_0)$.

Considérons maintenant x_1 n'importe quel élément non nul de $\Omega \cap H(t^n).t^{n/d}$ et, pour tout $i = 1, \cdots, d-1$ posons $x_i = x_1^i \in \Omega \cap H(t^n).t^{in/d}$. Puisque $I(x_i)_{|H} = \sigma^{in/d}$ (proposition 15.c)) et que γ_0 est central, on a $I(x_i)_{|D_0} = \theta^i$. Comme précédemment, on obtient que

$$\Omega = H(\gamma_0)(x_1, \cdots, x_{d-1}) = H(\gamma_0)(x_1) = H(\gamma_0 + x_1)$$

et, finalement, on a bien

$$\begin{array}{c} \Omega = H(\gamma_0 + x_1) \\ \Big| \, d \\ M = H(\gamma_0) \\ \Big| \, d \\ Z(\Omega) = L(\gamma_0) \end{array}$$

où x_1 désigne n'importe quel élément non nul de $\Omega \cap H(t^n).t^{n/d}$.

□

Les corps intermédiaires $H(t,\sigma)/\Omega/H$ différents de H sont donc de la forme $\Omega = H(\gamma_0 + x_1)$ avec $\gamma_0 \in L(t^n)$ pour un certain corps intermédiaire $H/L/K$ et $x_1 \in H(t^n).t^{n/d}$. Réciproquement, on a la

Proposition 17.– *On se donne un entier $d|n$, l'automorphisme $\sigma_0 = \sigma^{n/d}$, le corps $L = H^{\sigma_0}$ et deux éléments, $\gamma_0 \in L(t^n) - L$ et $x_1 \in H(t^n).t^{n/d}$, que l'on écrit $x_1 = f_1 t^{n/d}$ avec $f_1 \in H(t^n)$. On note N_L la norme de l'extension $H(t^n)/L(t^n)$ et l'on considère le corps $\Omega = H(\gamma_0 + x_1)$. Les propriétés suivantes*

i) Ω est une $L(\gamma_0)$-algèbre à division ayant $H(\gamma_0)$ comme sous-corps commutatif maximal,

ii) $x_1^d \in H(\gamma_0)$,

ii)' $x_1^d \in L(\gamma_0)$,

iii) $N_L(f_1)t^n \in H(\gamma_0)$,

iii)' $N_L(f_1)t^n \in L(\gamma_0)$,

sont équivalentes. Par ailleurs, si $x_1, x_1' \in H(t^n).t^{n/d}$ sont tels que $x_1^d, x_1'^d \in H(\gamma_0)$ alors les corps $H(\gamma_0 + x_1)$ et $H(\gamma_0 + x_1')$ sont $L(\gamma_0)$-isomorphes si et seulement si $x_1^d(x_1'^d)^{-1} \in N_L(H(\gamma_0)^*)$.

Preuve : Les équivalences *ii)* $\iff$ *iii)* et *ii)'* $\iff$ *iii)'* sont immédiates compte-tenu du fait que la restriction de $I(t^{n/d})$ au corps $H(t^n)$ est un générateur de $\mathrm{Gal}(H(t^n)/L(t^n))$ et donc que

$$x_1^d = f_1.(t^{n/d} f_1 t^{-n/d}).\cdots.(t^{(d-1)n/d} f_1 t^{-(d-1)n/d}).t^n = f_1.I(t^{n/d})(f_1).\cdots.I(t^{(d-1)n/d})(f_1).t^n = N_L(f_1).t^n$$

i) $\Longrightarrow$ *ii)* D'après ce qui précède, on a $x_1^d \in H(t^n) \cap \Omega = H(\gamma_0)$.

ii) $\Longrightarrow$ *ii)'* L'extension de corps commutatifs $H(\gamma_0)/L(\gamma_0)$ est cyclique et son groupe de Galois est engendré par la restriction à $H(\gamma_0)$ de l'automorphisme intérieur $I(x_1)$ (l'action de $I(x_1)$ sur γ_0 est triviale car $\gamma_0 \in L(t^n)$ et, sur le corps H, l'action de $I(x_1)$ est celle de σ_0). Comme $x_1^d \in H(\gamma_0)$ et que $I(x_1)(x_1^d) = x_1^d$, on en déduit que $x_1^d \in L(\gamma_0)$.

ii) $\Longrightarrow$ *i)* La famille $\{1, x_1, \cdots, x_1^{d-1}\}$ est $H(t^n)$-libre, elle est donc $H(\gamma_0)$-libre et l'on peut considérer le $H(\gamma_0)$-espace vectoriel $\Omega_0 = \bigoplus_{i=0}^{d-1} H(\gamma_0).x_1^i \subset \Omega$. Puisque $x_1^d \in H(\gamma_0)$, on voit que, pour tous $\lambda, \mu \in H(\gamma_0)$, $i, j \in \{1, \cdots, d-1\}$, on a

$$(\lambda x_1^i).(\mu x_1^j) = \lambda \mu^{\sigma_0^i} x_1^{i+j} = \left\{ \begin{array}{ll} \lambda\mu^{\sigma_0^i}.x_1^{i+j} \in H(\gamma_0).x_1^{i+j} & \text{si } i+j < d \\ \lambda\mu^{\sigma_0^i} x_1^d.x_1^{i+j-d} \in H(\gamma_0).x_1^{i+j-d} & \text{si } i+j \geq d \end{array} \right. \in \Omega_0$$

de sorte que Ω_0 est un sous-anneau de Ω. Il s'agit donc d'un anneau sans diviseur de zéro et qui est de dimension finie sur un corps, on en déduit que Ω_0 est un corps et, par suite, que $\Omega = \Omega_0$. On a donc $[\Omega : H(\gamma_0)] = d$ et, grâce à la formule ci-dessus, on voit que Ω est le produit croisé de l'extension galoisienne $H(\gamma_0)/L(\gamma_0)$ par le 2-cocycle $f : \mathrm{Gal}(H(\gamma_0)/L(\gamma_0)) =< \sigma_0 > \longrightarrow H(\gamma_0)^*$ suivant

$$f(\sigma_0^i, \sigma_0^j) = \left\{ \begin{array}{ll} 1 & \text{si } i+j < d \\ x_1^d & \text{si } i+j \geq d \end{array} \right.$$

Il découle de cette propriété que $Z(\Omega) = L(\gamma_0)$ et que $H(\gamma_0)$ est un sous-corps commutatif maximal de Ω.

Si l'on note f et f' les 2-cocycles associés respectivement au corps $H(\gamma_0 + x_1)$ et $H(\gamma_0 + x_1')$, dire que ces corps sont $L(\gamma_0)$-isomorphes équivaut à dire que le 2-cocycle

$$f f'^{-1}(\sigma_0^i, \sigma_0^j) = \left\{ \begin{array}{ll} 1 & \text{si } i+j < d \\ x_1^d(x_1'^d)^{-1} & \text{si } i+j \geq d \end{array} \right.$$

est en fait un 2-cobord. On pose $x_1 = r.t^{n/d}$ et $x_1' = r'.t^{n/d}$ avec $r, r' \in H(t^n)$, de sorte que

$$x_1^d = r.t^{n/d}.\cdots.r.t^{n/d} = r.(t^{n/d} r t^{-n/d}).(t^{2n/d} r t^{-2n/d}).\cdots.(t^{(d-1)n/d} r t^{-(d-1)n/d}).t^{dn/d} = r.\sigma_0(r).\cdots.\sigma_0^{d-1}(r).t^n = N_L(r)t^n$$

et, de même, $x_1^{'d} = N_L(r').t^n$. Il s'ensuit que

$$x_1^d(x_1^{'d})^{-1} = (N_L(r)t^n)(N_L(r')t^n)^{-1} = N_L(r)t^n t^{-n}N_L(r')^{-1} = N_L(rr'^{-1}) \in N_L(H(t^n)^*) \cap L(\gamma_0)^*$$

Puisque $\mathrm{Gal}(H(\gamma_0)/L(\gamma_0))$ est isomorphe, par restriction des automorphismes de $H(t^n)$ à $H(\gamma_0)$, à $\mathrm{Gal}(H(t^n)/L(t^n))$, on voit que $N_L(H(\gamma_0)^*) \subset N_L(H(t^n)^*) \cap L(\gamma_0)^*$.

S'il existe un élément $h_1 \in H(\gamma_0)$ tel que $N_L(h_1) = x_1^d(x_1^{'d})^{-1}$ alors on pose $h_0 = 1$ et, pour tout $i = 1, \cdots, d-1$, $h_i = h_1.h_1^{\sigma_0}.\cdots.h_1^{\sigma_0^{i-1}}$. Le 2-cobord associé à la 1-cochaine h, définie par $h(\sigma_0^i) = h_i$, est alors égal au 2-cocycle ff'^{-1}. En effet, pour tout $i, j \in \{1, \cdots, d-1\}$, on a

$$h_j^{\sigma_0^i}h_i = h_1.h_1^{\sigma_0}.\cdots.h_1^{\sigma_0^{i+j-1}}$$

et donc, si $i + j \leq d - 1$, on a

$$h(\sigma_0^j)^{\sigma_0^i}.h(\sigma_0^j\sigma_0^i)^{-1}.h(\sigma_0^i) = h_j^{\sigma_0^i}.h_{i+j}^{-1}.h_i = 1$$

et, si $i + j \geq d - 1$,

$$\begin{aligned} h(\sigma_0^j)^{\sigma_0^i}.h(\sigma_0^j\sigma_0^i)^{-1}.h(\sigma_0^i) &= h_j^{\sigma_0^i}.h_{i+j-d}^{-1}.h_i = h_1^{\sigma_0^{i+j-d}}.\cdots.h_1^{\sigma_0^{i+j-1}} = (h_1.\cdots.h_1^{\sigma_0^{d-1}})^{\sigma_0^{i+j-d}} \\ &= N_L(h_1)^{\sigma_0^{i+j-d}} = N_L(h_1) = x_1^d(x_1^{'d})^{-1} \end{aligned}$$

Réciproquement, si ff'^{-1} est un 2-cobord associé à une 1-cochaine $h : \mathrm{Gal}(H(\gamma_0)/L(\gamma_0)) \longrightarrow H(\gamma_0)^*$, on a

$$ff'^{-1}(\sigma_0^j, \sigma_0^j) = h_j^{\sigma_0^i}.h_{i+j \bmod(d)}^{-1}.h_i = \begin{cases} 1 & \text{si } i + j < d \\ x_1^d(x_1^{'d})^{-1} & \text{si } i + j \geq d \end{cases}$$

avec $h_i = h(\sigma_0^i)$. On en déduit

$$\begin{array}{ll} 1 = f(\sigma_0^0, \sigma_0^0) = h_0h_0^{-1}h_0 & \Longrightarrow h_0 = 1 \\ 1 = f(\sigma_0^1, \sigma_0) = h_1^{\sigma_0}h_2^{-1}h_1 & \Longrightarrow h_2 = h_1h_1^{\sigma_0} \\ 1 = f(\sigma_0^2, \sigma_0) = h_1^{\sigma_0^2}h_3^{-1}h_2 & \Longrightarrow h_3 = h_2h_1^{\sigma_0^2} = h_1h_1^{\sigma_0}h_1^{\sigma_0^2} \\ & \vdots \\ 1 = f(\sigma_0^{d-2}, \sigma_0) = h_1^{\sigma_0^{d-2}}h_{d-1}^{-1}h_{d-2} & \Longrightarrow h_{d-1} = h_{d-2}h_1^{\sigma_0^{d-2}} = h_1h_1^{\sigma_0}\cdots h_1^{\sigma_0^{d-2}} \\ x_1^d(x_1^{'d}))^{-1} = f(\sigma_0^{d-1}, \sigma_0) = h_1^{\sigma_0^{d-1}}h_0^{-1}h_{d-2} & \Longrightarrow x_1^d(x_1^{'d}))^{-1} = h_1h_1^{\sigma_0}\cdots h_1^{\sigma_0^{d-2}}h_1^{\sigma_0^{d-1}} = N_L(h_1) \end{array}$$

et donc $x_1^d(x_1^{'d})^{-1} \in N_L(H(\gamma_0)^*)$.

□

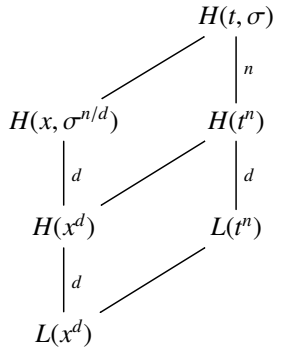
3.2.– Propriété de Lüroth forte.

On garde les même hypothèses et notations qu'au §3.1 et l'on considère un élément $x \in H(t, \sigma) - H$ tel que $H(x)$ soit un corps de fractions rationnelles tordu en la variable x, i.e. $H(x) = H(x, \theta)$ avec $\theta \in \mathrm{Aut}(H)$. Pour tout $\lambda \in H$, on a $x\lambda x^{-1} = \theta(\lambda)$ et donc, si l'on écrit $x = \sum_k \lambda_k t^k \in H((t, \sigma))$, alors

$$\begin{aligned} x\lambda = \theta(\lambda)x \quad &\Longrightarrow \textstyle\sum_k \lambda_k\sigma^k(\lambda)t^k = \sum_k \lambda_k\theta(\lambda)t^k \\ &\Longrightarrow \forall k,\ \left[\lambda_k \neq 0 \Longrightarrow \forall \lambda \in H,\ \theta(\lambda) = \sigma^k(\lambda)\right] \\ &\Longrightarrow \exists d|n,\ \theta = \sigma^{n/d} \end{aligned}$$

La proposition 15.b,c) assure que $Z(H(x)) = L(x^d)$, que $H(x^d)/L(x^d)$ est une extension de corps commutatifs

maximale et que $x \in H(t^n).t^{n/d}$. On a donc la tour



Les théorèmes 16 et 17 assurent que les extensions intermédiaires $H \subsetneq \Omega \subset H(t,\sigma)$ sont entièrement décrites par les entiers $d|n$ et les paires d'éléments $\gamma_0 \in L(t^n) - L$ et $x_1 = f_1.t^{n/d} \in H(t^n).t^{n/d}$ (avec $f_1 \in H(t^n)$) tels que $x_1^d = N_L(f_1).t^n \in L(\gamma_0)$, et la relation $\Omega = H(\gamma_0 + x_1) = H(\gamma_0)(x_1)$. D'après ce qui précède, pour une telle donnée, le corps Ω est un corps de fractions tordu si et seulement si il existe un élément $x \in H(t^n).t^{n/d} \cap \Omega$ tel que $L(x^d) = L(\gamma_0)$. Puisque, d'après la proposition 11.2), on a $H(t^n).t^{n/d} \cap \Omega = x_1.H(\gamma_0)$, on voit que x existe si et seulement si il existe $f \in H(\gamma_0)$ tel que $x = fx_1$ vérifie $L(x^d) = L(\gamma_0)$ c'est-à-dire $L(N_L(ff_1).t^n) = L(\gamma_0)$. En changeant génériquement t^n en t, on en déduit le

Théorème 18.– *Soient H un corps commutatif, $\sigma \in \mathrm{Aut}(H)$ un automorphisme d'ordre fini et $K = H^\sigma$ tels que l'extension cyclique H/K soit kummérienne. Pour que le corps $H(t,\sigma)$ vérifie la propriété de Lüroth forte, il faut et il suffit que*

$$\forall H/L/K,\ \forall \gamma_0 \in L(t) - L,\ \forall f_1 \in H(t)^*,\ N_L(f_1).t \in L(\gamma_0) \Longrightarrow \exists f \in H(\gamma_0) \text{ tel que } L(N_L(ff_1).t) = L(\gamma_0)$$

où N_L désigne la norme de l'extension $H(t)/L(t)$.

Remarques : a) La condition équivalente du théorème 18 ne porte que sur l'extension H/K et l'on a donc ramené le problème est une pure question d'arithmétique des corps commutatifs.

b) La condition $L(N_L(ff_1).t) = L(\gamma_0)$ s'écrit plus simplement $N_L(ff_1).t = \dfrac{a\gamma_0 + b}{c\gamma_0 + d}$ avec $a,b,c,d \in L$.

4.– Question de hauteur.

Dans le cas d'un corps commutatif H et d'un élément $y \in H(t) - H$, le degré de l'extension $H(t)/H(y)$ est égal à la hauteur $h(y)$ de y, qui est, par définition,

$$h(y) = \max\left(d^\circ p(t), d^\circ q(t)\right)$$

où $p(t), q(t) \in H[t]$ sont des polynômes premiers entre eux tels que $y = p(t)/q(t)$. La preuve de cette propriété est élémentaire : l'élément t est racine du polynôme $P(x) = p(x) - yq(x) \in H[y][x]$ et ce dernier est irréductible puisque, vu dans $H[x][y]$, il s'agit d'un polynôme de degré 1 dont le contenu vaut 1. Dans le cas d'un corps de fractions tordu $H(t,\sigma)$, l'argument ne tient plus puisque l'anneau de polynômes $H[t,\sigma]$ a beaucoup moins de propriétés : il est rarement factoriel et donc encore plus rarement principal.

On peut, toutefois, définir une généralisation de la notion de hauteur, comme nous allons le voir dans le §3.1, en remarquant que pour le cas commutatif, $h(y)$ est aussi le minimum des $\max(d^\circ p(t), d^\circ q(t))$ pour $y = p(t)/q(t)$. Pour autant, cette notion généralisée n'est guère utile pour étudier le degré $H(t,\sigma)/H(y)$ en toute généralité : dans le §3.2 nous donnons l'exemple de situations où le degré vaut 1 mais où la hauteur est arbitrairement grande.

4.1.– Mise sous forme irréductible d'une fraction et hauteur.

Le degré d'un élément $f \in H(t,\sigma)$ est, par définition, l'entier $d^\circ f = d^\circ P - d^\circ Q$ où $P, Q \in H[t,\sigma]$ sont tels que $f = PQ^{-1}$. Le degré de f est défini de manière non équivoque : si $f = PQ^{-1} = P'Q'^{-1}$, comme $PQ^{-1} = Q_0^{-1}P_0$ pour certains $P_0, Q_0 \in H[t,\sigma]$, alors on a $Q_0P = P_0Q$ et $Q_0P' = P_0Q'$ et ainsi, en prenant les degrés, on trouve $d^\circ P - d^\circ Q = d^\circ P_0 - d^\circ Q_0 = d^\circ P' - d^\circ Q'$.

Lemme 19.– *Pour tout couple $(P,Q) \in H[t,\sigma]$ de polynômes non nuls, il existe un couple $(P_0,Q_0) \in H[t,\sigma]$ tel que $PQ^{-1} = Q_0^{-1}P_0$ (resp. $Q^{-1}P = P_0Q_0^{-1}$) et tel que $d^\circ P_0 \leq d^\circ P$, $d^\circ Q_0 \leq d^\circ Q$.*

Preuve : Si $P(t) = a_0 + \cdots + a_n t^n$ et $Q(t) = b_0 + \cdots + b_m t^m$, alors on pose formellement $P_0(t) = \alpha_0 + \cdots + \alpha_n t^n$ et $Q_0(t) = \beta_0 + \cdots + \beta_m t^m$ et l'on voit que $Q_0(t)P(t) = P_0(t)Q(t)$ si et seulement si, pour tout $h = 0, \cdots, n+m$, on a

$$(E_h) \qquad \sum_{i+j=h} \beta_i \sigma^i(a_j) - \alpha_i \sigma^i(b_j) = 0$$

Chacune des équations (E_h) est une équation linéaire à droite et l'on voit donc que l'existence du couple (P_0,Q_0) équivaut à l'existence d'une solution $(\alpha_0, \cdots, \alpha_n, \beta_0, \cdots \beta_m)$ non triviale au système $\{(E_h)\}_h$. Ce système compte au plus $n+m+1$ équations et il y a $n+m+2$ inconnues, ce qui assure l'existence d'une solution non triviale[4].

Pour $Q^{-1}P = P_0Q_0^{-1}$, on remarque que $\{t^i\}_{i\geq 0}$ est aussi une H-base à droite du H-espace vectoriel à droite $H[t,\sigma]$. On reprend alors la même stratégie que précédemment, mais en considérant alors un système d'équations linéaires à gauche.

□

Corollaire-Définition 20.– *Pour $f \in H(t,\sigma)$, on définit la hauteur $h(f)$ de f comme étant l'entier*

$$\begin{aligned} h(f) &= \min\left\{\max(d^\circ P, d^\circ Q)/\ P,Q \in H[t,\sigma] \text{ tels que } f(t) = P(t)Q(t)^{-1}\right\} \\ &= \min\left\{\max(d^\circ P, d^\circ Q)/\ P,Q \in H[t,\sigma] \text{ tels que } f(t) = Q(t)^{-1}P(t)\right\} \end{aligned}$$

Preuve : L'égalité des min découle facilement du lemme 19.

□

Théorème 21.– (Forme irréductible d'une fraction rationnelle tordue) *Pour tout $f \in H(t,\sigma)$, il existe un unique couple $(P_f^g, Q_f^g) \in H[t,\sigma]$ et un unique couple $(P_f^d, Q_f^d) \in H[t,\sigma]$ vérifiant*

- *P_f^g et P_f^d unitaires*
- *$h(f) = \max(d^\circ P_f^g, d^\circ Q_f^g) = \max(d^\circ P_f^d, d^\circ Q_f^d)$*
- *$f = P_f^g (Q_f^g)^{-1} = (Q_f^d)^{-1} P_f^d$*

cette dernière écriture $f = P_f^g(Q_f^g)^{-1}$ (resp. $f = (Q_f^d)^{-1}P_f^d$) s'appelle la forme irréductible à gauche *(resp.* à droite*), de la fraction f.*

Preuve : L'existence est immédiate. Soient (P_1,Q_1) et (P_2,Q_2) vérifiant les hypothèses de l'énoncé et $f = B^{-1}A$. On a alors $BP_i = AQ_i$ pour $i = 1,2$. Si $h(f) = d^\circ P_1$, alors $d^\circ f = P_1 - Q_1 = P_2 - Q_2 \geq 0$ et donc $d^\circ P_2 = h(f) = d^\circ P_1$. Ceci implique aussi que $d^\circ Q_1 = d^\circ P_1 - d^\circ f = d^\circ P_2 - d^\circ f = d^\circ Q_2$. Ces résultats sur les degrés sont les mêmes en supposant $h(f) = d^\circ Q_1$. On a, par ailleurs, $B(P_1 - P_2) = A(Q_1 - Q_2)$ si bien que, si $P_1 \neq P_2$ alors $f = (P_1 - P_2)(Q_1 - Q_2)^{-1}$. Comme P_1 et P_2 sont supposés tous les deux unitaires, on a $d^\circ(P_1 - P_2) < d^\circ P_1$ et comme $d^\circ(P_1 - P_2) - d^\circ(Q_1 - Q_2) = d^\circ f = d^\circ P_1 - d^\circ Q_1$, on a aussi $d^\circ(Q_1 - Q_2) < d^\circ Q_1$. Il s'ensuit que $h(f) \leq \max(d^\circ(P_1 - P_2), d^\circ(Q_1 - Q_2) < \max(d^\circ P_1, d^\circ Q_1) = h(f)$, ce qui est absurde. Ainsi, $P_1 = P_2$ et, par suite, $Q_1 = Q_2$.
Le cas où c'est Q_f qui est supposé unitaire se traite de la même manière.

[4] Pour les raisons expliquées dans la note 1.

□

4.2.– Contre-exemples.

On considère, un corps commutatif H, un automorphisme $\sigma \in \mathrm{Aut}(H)$ d'ordre fini $n \geq 2$ et $K = H^{\sigma}$, tels que H/K soit kummérienne. Pour tout entier $h \geq 1$, on considère l'élément $f = t^{hn} + t^{hn}.t + \cdots + t^{hn}.t^{n-1} \in H(t,\sigma)$. La proposition 10.b) montre alors que

$$H(f) = H(t^{hn} + t^{hn}.t + \cdots + t^{hn}.t^{n-1}) = H(t^{hn}, t^{hn}.t, \cdots, t^{hn}.t^{n-1}) = H(t,\sigma)$$

et l'on a donc $[H(t,\sigma) : H(f)] = 1$ alors que, puisque $f \in H[t,\sigma]$, on a visiblement $h(f) = d^{\circ}f = (h+1)n-1$.

Bibliographie

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

[Des1] B. Deschamps, *Arithmétique des extensions intérieures*, J. of Algebra, 620, 50-88 (2023).

[Des2] B. Deschamps, *Quelques considérations galoisiennes relatives à l'extension des constantes d'un corps de fractions tordu*, préprint disponible à https://perso.univ-lemans.fr/~bdesch/27.pdf (2024).

[Des3] B. Deschamps, *Des extensions plus petites que leurs groupes de Galois*, Communications in Algebra, 46-10, 4555-4560 (2018).

[Des4] B. Deschamps, *A propos d'un théorème de Frobenius*, Annales Mathématiques Blaise Pascal 8-2, 61-66 (2001).

[DL] B. Deschamps & F. Legrand, *Le Problème Inverse de Galois sur les corps des fractions tordus à indéterminée centrale*, Journal of Pure and Applied Algebra, 224-5 (2020).

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

[Lür] J. Lüroth, *Beweis eines Satzes über rationale Curven*, Math. Ann., 9(2):163-165 (1875).

[LP] F. Legrand & E. Paran, *Lüroth's and Igusa's theorems over division rings*, Osaka J. Math., 61, no.2, 261-274 (2024).

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

[Ste] E. Steinitz, *Algebraische Theorie der Körper*, J. Reine Angew. Math., 137:167-309 (1910).

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