Quelques propriétés des sous-groupes de $\mathrm{Gal}(k((t))/k)$

Bruno DESCHAMPS et Ivan SUAREZ ATIAS

Université du Maine

Résumé.– Dans cet article, nous établissons une série de résultats sur les sous-groupes de $\mathrm{Gal}(k((t))/k)$, le principal d'entre eux étant que, s'ils ne sont pas abéliens alors leurs centres sont toujours des groupes cycliques.

Abstract.– In this article we state some results on subgroups of $\mathrm{Gal}(k((t))/k)$, the main of these being that, if they are not abelian then their centers are always cyclic groups.

1.– Introduction.

Ce texte présente une série de résultats sur les sous-groupes $\mathrm{Gal}(k((t))/k)$. Dans ce qui suit nous adopterons le point de vue artinien de la théorie de Galois : une extension de corps (non nécessairement algébrique) L/k sera dite *galoisienne* si le corps des invariants de L par le groupe $\mathrm{Aut}_k(L)$ est égal au corps k. Dans ce cas, on notera $\mathrm{Gal}(L/k)$ ce groupe qui sera alors appelé *groupe de Galois* de l'extension L/k. On dira qu'une sous-extension M d'une extension galoisienne L/k est fermée si l'extension L/M est galoisienne, le sous-groupe $\mathrm{Gal}(L/M)$ sera alors dit *fermé*.

Un exemple bien connu d'extension transcendante galoisienne est celui de l'extension $k(t)/k$ quand k désigne un corps infini. Le groupe de Galois de cette extension est isomorphe à $\mathrm{PGL}_2(k)$ et les sous-groupes fermés non triviaux de ce groupe sont exactement ses sous-groupes finis. L'extension $k((t))/k$ est elle aussi galoisienne, même si k est fini (corollaire 2). Dans le cas de la caractéristique nulle, nous caractérisons les objets fermés de cette extension dans le §2. : ce sont les sous-groupes finis et ces derniers sont nécessairement cycliques (corollaire 9.a.).

Le §3. de ce texte est consacré à l'étude de la commutation dans $\mathrm{Gal}(k((t))/k)$ quand k est de caractéristique 0. A cet effet, nous décrivons complètement les centralisateurs des éléments qui ne sont pas des éléments de torsion. Nous montrons, en particulier, que ces derniers sont systématiquement abéliens (corollaire 27 et théorèmes 30 et 32). Cette étude montre en particulier que le groupe, $\mathrm{Gal}_{\mathscr{P}}(k((t))/k)$, des automorphismes principaux (i.e. les éléments $\sigma \in \mathrm{Gal}(k((t))/k)$ qui, appliqués à t, vérifient $\sigma(t) = t + \cdots$) est un groupe de type CA (corollaire 29). Rappelons qu'un groupe de type CA est un groupe où le centralisateur de tout élément non trivial est abélien. La classification de ces groupes a joué un rôle important dans le fameux théorème de Feit-Thompson. Cette classification se limite pour le moment au cas des groupes localement finis et le corollaire 29 est intéressant dans la mesure où $\mathrm{Gal}_{\mathscr{P}}(k((t))/k)$ est un groupe « naturel » qui n'est visiblement pas localement fini. L'étude des centralisateurs dans $\mathrm{Gal}(k(((t))/k)$ que nous menons, repose sur celle de la divisibilité (§3.1.) et sur l'introduction d'une composition « continue » (définition 17) dans $\mathrm{Gal}(k((t))/k)$: pour les automorphismes principaux f, nous donnons du sens à f^α, la composée α-ième de f où α désigne un élément quelconque de k. L'application $(\alpha, f) \longmapsto f^\alpha$ jouit alors des propriétés usuelles relatives aux fonctions puissances.

En analogie avec le cas de l'extension $k(t)/k$ et du groupe $\mathrm{PGL}_2(k)$, nous montrons ensuite que le groupe $\mathrm{Gal}(k((t))/k)$ possède la propriété (Z_c) suivante : tout sous-groupe non abélien de $\mathrm{Gal}(k((t))/k)$ possède un centre cyclique (théorème 33). Nous dissertons ensuite un peu sur cette propriété (Z_c) (et d'autres associées) dans un cadre général.

Un résultat montre que la somme amalgamée de deux groupes cycliques possède la propriété (Z_c) (Proposition 35). Ceci nous amène à nous interroger dans le §4. sur la structure des sous-groupes bigènes de $\mathrm{Gal}(k((t))/k)$ quand ces derniers sont engendrés par deux éléments de torsion. Nous donnons une traduction graphique de leur structure qui permet, par la théorie de Serre-Bass, de regarder l'éventualité de l'existence d'amalgamme pour ces sous-groupes. Plus précisément, si l'on considère deux éléments de torsion $\sigma, \rho \in \mathrm{Gal}(k((t))/k)$ d'ordre respectif n et m on se demande si le sous-groupe bigène $< \sigma, \rho >$ est isomorphe ou non à l'amalgamme $\mathbb{Z}/n\mathbb{Z} \underset{\mathbb{Z}/d\mathbb{Z}}{*} \mathbb{Z}/m\mathbb{Z}$ où d désigne l'ordre du sous-groupe $< \sigma > \cap < \rho >$. Sur cette question nous étudions deux situations qui apportent respectivement une réponse positive et négative. Dans le §4.1., nous montrons que, si l'intersection $< \sigma > \cap < \rho >$ est d'indice 2 dans $< \sigma >$ et $< \rho >$, alors il y a bien amalgame (théorème 38). Dans le §4.2., nous montrons que, si σ et ρ sont rationnels (i.e. $\sigma(t), \rho(t) \in k(t)$) alors il n'y a pas amalgame (théorème 41).

2.– Quelques propriétés de l'extension $k((t))/k$.

2.1.– Généralités. On considère un corps k et $k((t))$ le corps des séries de Laurent à coefficients dans k. On note v la valuation usuelle sur $k((t))$, $O_k^\times$ le groupe des unités de $k((t))$, $1 + \mathfrak{M}_k$ le groupe des unités principales et $\mathcal{E}_k = t.O_k^\times$ l'ensemble des séries de valuation 1. Sur $O_k^\times$, on introduit la loi de composition $*$ définie, pour $\alpha(t), \beta(t) \in O^\times$, par

$$(\alpha * \beta)(t) = \alpha(t).\beta(t\alpha(t))$$

Les monoides $(O_k^\times, *)$ et $(\mathcal{E}_k, \circ)^{\mathrm{op}}$ sont isomorphes par $f(t) \longmapsto t.f(t)$. Le point essentiel pour l'étude de $\mathrm{Gal}(k((t))/k)$ repose sur la propriété suivante, dont on pourra trouver une preuve dans [Rib2] et [Des].

Théorème 1.– *a) Pour tout $\sigma \in \mathrm{Gal}(k((t))/k)$, on a $v \circ \sigma = v$. En particulier, pour la topologie induite par v, un k-automorphisme de $k((t))$ est une application continue.*

b) Soient $\sigma \in \mathrm{Gal}(k((t))/k)$ et $S \in k((t))$ une série de valuation > 0. Pour toute suite $(a_n)_{n \geq n_0} \in k^{[[n_0, +\infty[[}$, on a

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

c) Les groupes $\mathrm{Gal}(k((t))/k)$, $(O_k^\times, *)$ et $(\mathcal{E}_k, \circ)^{op}$ sont isomorphes, l'application $\sigma \longmapsto \sigma(t)$ définissant, par exemple, un isomorphisme de $\mathrm{Gal}(k((t))/k)$ sur $\mathcal{E}_k^{op}$.

d) Le groupe $(O_k^\times, *)$ est le produit semi-direct des sous-groupes $(1 + \mathcal{M}_k, *)$ et $(k^*, .)$, l'action par conjugaison de $a \in k^*$ sur un élément $\alpha \in 1 + \mathcal{M}_k$ étant donné par la formule $\alpha^a(t) = (a * \alpha(t) * a^{-1})(t) = \alpha(at)$.

Ainsi les éléments de $\mathrm{Gal}(k((t))/k)$ sont biunivoquement décrit par les séries de valuation 1. Dans la suite de ce texte, on notera $\gamma : \mathrm{Gal}(k((t))/k) \longrightarrow k^*$ le morphisme défini, pour $\sigma \in \mathrm{Gal}(k((t))/k)$, par

$$\gamma(\sigma) = \frac{\sigma(t)}{t}(0)$$

Les éléments $f \in \mathrm{Gal}(k((t))/k)$ vérifiant $\gamma(f) = 1$ forment un sous-groupe que l'on notera $\mathrm{Gal}_{\mathscr{P}}(k((t))/k)$ et que l'on appelera *sous-groupe des automorphismes principaux* (cette terminologie vient du fait que *via* l'isomorphisme avec $(O_k^\times, *)$ il correspond au sous-groupe $1 + \mathcal{M}_k$ des unités principales). La suite exacte

$$1 \longrightarrow \mathrm{Gal}_{\mathscr{P}}(k((t))/k) \longrightarrow \mathrm{Gal}(k((t))/k) \underset{\gamma}{\longrightarrow} k^* \longrightarrow 1$$

est visiblement scindée (à $\alpha \in k^*$ on associe l'automorphisme donné par $t \longmapsto \alpha t$), si bien que $\mathrm{Gal}(k((t))/k)$ s'identifie à un produit semi-direct $\mathrm{Gal}_{\mathscr{P}}(k((t))/k) \rtimes k^*$.

On rappelle que si k est un corps de caractéristique p et que n est un entier non divisble par p, alors une série entière $S(t) \in k[[t]]$ de valuation nulle possède une racine n-ième (pour le produit au sens de Cauchy) dans $k[[t]]$, si et seulement si, l'élément $S(0)$ en possède une dans k. En particulier, si $S(t) \in 1 + \mathcal{M}_k$ alors il existe une (unique) série $s(t) \in 1 + \mathcal{M}_k$ telle que $s(t)^n = S(t)$.

Corollaire 2.– *a) Pour tout sous-groupe infini $G \subset \mathrm{Gal}(k((t))/k)$, on a $k((t))^G = k$. En particulier, l'extension $k((t))/k$ est galoisienne.*

b) Le centre du groupe $\mathrm{Gal}(k((t))/k)$ *est trivial.*

Preuve : a) La preuve repose sur le lemme suivant :

Lemme 3.– *Si $S \in k((t))$ est une série de valuation $v(S) = n \geq 1$ alors on a $[k((t)) : k((S))] = n$.*

Preuve : Quitte à multiplier par une constante, on peut supposer que $S(t) = t^n + \lambda t^{n+1} + \cdots$. Dans $k((t))$ on a alors

$$S(t) - \lambda t S(t) = t^n + \mu t^{n+2} + \cdots$$

pour un certain $\mu \in k$. Par récurrence, on en déduit l'existence d'un polynôme $P_1 \in k[t]$ de degré $\leq n-1$ tel que

$$S(t) - P_1(t)S(t) = t^n + \alpha t^{2n} + \cdots$$

Puisque $S(t)^2 = t^{2n} + \cdots$, le même procédé montre qu'il existe $P_2 \in k[t]$ de degré $\leq n-1$ tel que

$$S(t) - P_1(t)S(t) - P_2(t)S(t)^2 = t^n + \beta t^{3n} + \cdots$$

Par récurrence, on construit ainsi une suite $(P_k)_k$ de polynômes de degrés $\leq n-1$ telle que

$$S(t) - \sum_{k \geq 1} P_k(t) S(t)^k = t^n$$

Si l'on note $P_k(t) = \sum_{i=0}^{n-1} a_{k,i} t^i$, alors puisque $v(S) = n \geq 1$, on voit que la série $\sum_{k \geq 1} a_{k,i} S^k$ converge dans $k((S))$ pour tout $i = 0, \cdots, n-1$. On a alors

$$t^n = S(t) - \sum_{i=0}^{n-1} \left(\sum_{k \geq 1} a_{k,i} S^k \right) t^i$$

et donc l'élément t est algébrique sur $k((S))$, de degré $\leq n$.

Il est clair que la topologie définie sur $k((S))$ par la S-valuation v_S coïncide avec la topologie induite par la valuation usuelle v de $k((t))$, ainsi $k((S))$ est complet pour v. Le corps $k((S))(t)$, en tant qu'extension finie d'un corps complet, est complet pour la valuation v. Il s'ensuit que $k((S))(t) = k((t))$ et que l'extension $k((t))/k((S))$ est de degré $\leq n$. Le groupe de la valuation v sur $k((S))$ est $n\mathbb{Z}$ alors qu'il vaut $\mathbb{Z}$ sur $k((t))$. L'indice de ramification de v dans l'extension vaut donc n, ce qui assure finalement que $[k((t)) : k((S))] = n$.

□

Supposons qu'il existe une série non constante $S \in k((t))$ qui soit invariante sous l'action de G. Quitte éventuellement à considérer $S(t)^{-1}$, $S(t) - S(0)$ et à multiplier par une constante adéquate, on peut supposer que $S(t) = t^n + \lambda t^{n+1} + \cdots$ avec $n \geq 1$. On voit alors, par le théorème 1.b., que le corps $k((S))$ est invariant par G. Le lemme précédent assure que $[k((t)) : k((S))] = n$ et donc le groupe G, en tant que sous-groupe du groupe d'automorphismes d'une extension finie, est fini. Par contraposée, on obtient donc le a).

Remarque : Si n n'est pas divisible par $p = \mathrm{car}(k)$, alors en écrivant $S(t) = t^n S_0(t)$ avec $S_0 \in 1 + \mathfrak{M}$, on voit que, si $s_0(t) \in 1 + \mathfrak{M}$ désigne une racine n-ième de $S_0(t)$, alors l'élément $ts_0(t)$ est primitif de l'extension $k((t))/k((S))$. Dans cette situation, si k possède les racines n-ième de l'unité, l'extension $k((t))/k((S))$ est alors cyclique de degré n.

b) Soit $\alpha \in \mathrm{Gal}(k((t))/k)$ un élément central, $\alpha(t) = \sum_{n\geq 1} a_n t^n$. Pour $\lambda \in k^*$, on considère $\beta \in \mathrm{Gal}(k((t))/k)$ défini par $\beta(t) = \lambda t$. Puisque $\alpha \circ \beta = \beta \circ \alpha$, on voit que, pour tout $n \geq 1$, $a_n = \lambda^{n-1} a_n$.

1) Supposons que k ne soit sous-corps d'aucun $\overline{\mathbb{F}_p}$. Il existe donc un élément $\lambda \in k^*$ qui n'est pas une racine de l'unité. On a donc $a_n = 0$ pour tout $n \geq 2$. Ainsi, $\alpha(t) = a_1 t$ avec $a_1 \neq 0$. En considérant l'élément $\gamma \in \mathrm{Gal}(k((t))/k)$, défini par $\gamma(t) = t + t^2$, on voit que $\gamma \circ \alpha(t) = a_1 t + a_1 t^2 = a_1 t + a_1^2 t^2 = \alpha \circ \gamma(t)$ et, par suite, que $a_1 = 1$.

2) Supposons maintenant que $k \subset \overline{\mathbb{F}_p}$ pour un certain premier p. Si $q = p^k$ est tel que $\mathbb{F}_q \subset k$, alors en prenant pour λ un générateur de $\mathbb{F}_q^*$, on voit que la condition $\alpha \circ \beta = \beta \circ \alpha$ équivaut à $a_n = 0$ pour tout $n \not\equiv 1 \mod (q-1)$.

2.1) Si k est infini, il existe donc une infinité de puissances $q = p^k$ tel que $\mathbb{F}_q \subset k$, et donc $a_n = 0$ pour tout $n \geq 2$. On a donc $\alpha(t) = a_1 t$ et comme précédemment, la condition $\gamma \circ \alpha(t) = \alpha \circ \gamma(t)$, pour $\gamma(t) = t + t^2$, assure que $a_1 = 1$.

2.2) Si $k = \mathbb{F}_q$ pour $q = p^k$, alors

$$\alpha(t) = a_1 t + \sum_{s\geq 1} a_{1+s(q-1)} t^{1+s(q-1)}$$

Pour un entier $m \geq 2$, on considère l'élément $\gamma \in \mathrm{Gal}(k((t))/k)$, défini par $\gamma(t) = t + t^m$. On suppose que $\alpha(t) \neq a_1 t$ et l'on pose

$$\alpha(t) = a_1 t + \sum_{s\geq s_0} a_{1+s(q-1)} t^{1+s(q-1)}$$

avec $a_{1+s_0(q-1)} \neq 0$. Dans la suite, on va choisir des valeurs de m suivant les différents cas, pour que la relation $\alpha \circ \gamma = \gamma \circ \alpha$ conduise à une absurdité.

2.2.1) $q \neq 2$. Le choix $m = 2$ montre que $a_1 = 1$.

2.2.1.1) Si $s_0 \not\equiv 0 \mod p$, choisissons $m = q + 1$, i.e. $\gamma(t) = t + t^{q+1}$. On a alors

$$\alpha \circ \gamma(t) = \begin{cases} t + a_q t^q + t^{q+1} + a_{1+2(q-1)} t^{2q-1} + a_q t^{2q} + \ldots & \text{si } s_0 = 1 \\ t + t^{q+1} \quad + a_{1+s_0(q-1)} t^{1+s_0(q-1)} & \\ \qquad + a_{1+(s_0+1)(q-1)} t^{1+(s_0+1)(q-1)} + a_{1+s_0(q-1)} t^{q+1+s_0(q-1)} + \ldots & \text{si } s_0 > 1 \end{cases}$$

$$\gamma \circ \alpha(t) = \begin{cases} t + a_q t^q + t^{q+1} + a_{1+2(q-1)} t^{2q-1} + 0 \cdot t^{2q} + \ldots & \text{si } s_0 = 1 \\ t + t^{q+1} \quad + a_{1+s_0(q-1)} t^{1+s_0(q-1)} & \\ \qquad + a_{1+(s_0+1)(q-1)} t^{1+(s_0+1)(q-1)} + (1-s_0) a_{1+s_0(q-1)} t^{q+1+s_0(q-1)} + \ldots & \text{si } s_0 > 1 \end{cases}$$

Ce calcul montre bien la non égalité de ces deux expressions lorsque $s_0 \not\equiv 0 \mod p$, d'où la contradiction cherchée.

2.2.1.2) Si $s_0 \equiv 0 \mod p$, choisissons $m = q$, i.e. $\gamma(t) = t + t^q$. Un calcul montre alors que le coefficient du terme de degré $q + s_0(q-1)$ de $\alpha \circ \gamma(t)$ est $a_{1+(s_0+1)(q-1)}$ tandis que celui de $\gamma \circ \alpha(t)$ est $a_{1+(s_0+1)(q-1)} + (1-s_0) a_{1+s_0(q-1)}$. Ceci contredit bien entendu le fait que α et γ commutent lorsque $s_0 \equiv 0 \mod p$.

2.2.2) $q = 2$. On a $\alpha(t) = t + t^{n_0} + \sum_{n>n_0} a_n t^n$. Si $n_0 \geq 4$, alors il existe au moins deux entiers distincts m vérifiant $2 \leq m < n_0$. Pour ces entiers, le coefficient du terme de degré $n_0 + m - 1$

de $\alpha \circ \gamma(t)$ est $a_{n_0+m-1} + m$ tandis que celui de $\gamma \circ \alpha(t)$ est $a_{n_0+m-1} + n_0$. Le choix $m = 2$, suivi du choix $m = 3$, permet d'aboutir à une contradiction.

Finalement, pour $n_0 = 3$, on choisit $m = 2$ et pour $n_0 = 2$, $m = 3$ (la contradiction apparaît pour le terme de degré 4 dans les deux cas).

□

2.2.– Etude de la torsion.

Proposition 4.– *Si α désigne un élément d'ordre n dans* $\mathrm{Gal}(k((t))/k)$*, alors*

$$k((t))^{<\alpha>} = k\left((\mathcal{N}(t))\right)$$

où $\mathcal{N}(t) = t.\alpha(t).\alpha^2(t).\cdots.\alpha^{n-1}(t)$ est la norme de l'élément t dans l'extension $k((t))/k((t))^{<\alpha>}$. En particulier, il existe $A(t) \in 1 + \mathcal{M}_k$ tel que $k((t))^{<\alpha>} = k((t^n A(t)))$.

Si n est premier avec la caractéristique de k et si $a(t)$ désigne l'unique élément de $1 + \mathcal{M}_k$ tel que $a(t)^n = A(t)$, alors $ta(t)$ est un élément primitif de l'extension $k((t))/k((t^n A(t)))$. Dans cette situation, le corps k contient alors toutes les racines n-ième de l'unité et l'extension $k((t))/k((t^n A(t)))$ est donc kummérienne.

Preuve : Puisque α est continu et qu'il laisse invariant $\mathcal{N}(t)$, on en déduit que $k((\mathcal{N}(t))) \subset k((t))^{<\alpha>}$. On peut écrire $\mathcal{N}(t) = \lambda t^n A(t)$ et le lemme 3 montre que $k((t))$ est de degré n sur $k((\mathcal{N}(t))) = k((t^n A(t)))$, ce qui prouve finalement que $k((t))^{<\alpha>} = k((\mathcal{N}(t)))$.

Si n et $\mathrm{car}(k)$ sont premiers entre eux, la remarque de la preuve du corollaire 2.a. montre la fin de la proposition.

□

Théorème 5.– *Soient n un entier et k un corps de caractéristique ne divisant pas n.*

a) Si $\alpha \in \mathrm{Gal}(k((t))/k)$ est un élément d'ordre n alors $\gamma(\alpha)$ est une racine primitive n-ième de l'unité.

b) Si $\alpha, \beta \in \mathrm{Gal}(k((t))/k)$ sont deux éléments d'ordre n, alors α et β sont conjugués si et seulement si $\gamma(\alpha) = \gamma(\beta)$.

Preuve : a) Le fait que $\gamma(\alpha)$ soit une racine n-ième de l'unité, découle du caractère morphique de γ. Pour établir le fait que $\gamma(\alpha)$ est primitive, il faut remarquer la chose suivante : si α est un élément de torsion, alors $\gamma(\alpha) \neq 1$, le caractère primitif de $\gamma(\alpha)$ s'obtient alors par récurence sur la décomposition en nombres premiers de n. Le fait que si $\gamma(\alpha) = 1$ alors α n'est pas de torsion s'obtient, lui, de la manière suivante : soit $\alpha \in \mathrm{Gal}(k((t))/k)$ tel que $\gamma(\alpha) = 1$ et $\alpha^{(n)} = 1$. Posons

$$\alpha(t) = t + a_2 t^2 + \cdots + a_h t^h + \cdots$$

et montrons par récurence sur $h \geq 2$ que $a_h = 0$. Supposons donc que $\alpha(t) = t + a_h t^h + \cdots$. Une récurrence sur i, montre que $\alpha^{(i)}(t) = t + i a_h t^h + \cdots$ ce qui, appliqué au rang $i = n$, nous donne $\alpha^{(n)}(t) = t + n a_h t^h + \cdots = 1$. Ainsi, $n a_h = 0$, mais comme n n'est pas divisible par la caractéristique de k, on trouve bien $a_h = 0$.

b) Supposons qu'il existe $\delta \in \mathrm{Gal}(k((t))/k)$ tel que $\delta \circ \alpha \circ \delta^{-1} = \beta$. On a alors $\gamma(\delta)\gamma(\alpha) = \gamma(\delta \circ \alpha) = \gamma(\beta \circ \delta) = \gamma(\beta)\gamma(\delta)$ et donc $\gamma(\alpha) = \gamma(\beta)$.

Réciproquement, supposons donnés α et β deux éléments de n-torsion tels que $\gamma(\alpha) = \gamma(\beta)$. En utilisant la proposition 4, on peut poser

$$k((t))^{<\alpha>} = k((t^n A(t)))$$
$$k((t))^{<\beta>} = k((t^n B(t)))$$

où $A, B \in 1 + \mathcal{M}_k$. Notons alors $a, b \in 1 + \mathcal{M}_k$ les éléments tels que $a^n = A$ et $b^n = B$. Comme signalé précédement, $ta(t)$ et $tb(t)$ sont respectivement des éléments primitifs des extensions $k((t))/k((t^nA(t)))$et $k((t))/k((t^nB(t)))$. Puisque $k((t^nA(t)))$ et $k((t^nB(t)))$ sont des corps k-isomorphes à $k((t))$, l'application σ satisfaisant

$$\sigma(t^nA(t)) = t^nB(t)$$

définit un unique k-isomorphisme bijectif du corps $k((t^nA(t)))$ sur le corps $k((t^nB(t)))$. Nous allons relever σ en un automorphisme $\widetilde{\sigma}$ de $k((t))$ de la manière suivante : si l'on note $\omega(t) = ta(t)$ et $\omega'(t) = tb(t)$ alors un élément $S \in k((t))$ s'écrit de manière unique sous la forme

$$S = \lambda_0 + \lambda_1\omega + \cdots + \lambda_{n-1}\omega^{n-1}$$

avec $\lambda_0, \cdots, \lambda_{n-1} \in k((t^nA(t)))$. On pose alors

$$\widetilde{\sigma}(S) = \sigma(\lambda_0) + \sigma(\lambda_1)\omega' + \cdots + \sigma(\lambda^{n-1})\omega'^{n-1}$$

L'application $\widetilde{\sigma}$ est déjà un k-automorphisme d'espace vectoriel, le fait que ce soit un automorphisme de corps vient du fait que $\widetilde{\sigma}(\omega^n) = \widetilde{\sigma}(t^nA(t)) = \sigma(t^nA(t)) = t^nB(t) = \omega'^n$ et que l'image par σ du polynôme minimal de ω sur $k((t^nA(t)))$ (à savoir $X^n - t^nA(t)$) est égal au polynôme minimal de ω' sur $k((t^nB(t)))$ (à savoir $X^n - t^nB(t)$).

L'image de ω par $\widetilde{\sigma}$ est ω'. Comme $\beta(\omega')$ est un conjugué de ω' sur $k((t^nB(t)))$, il existe une racine de l'unité ξ_n telle que $\beta(\omega') = \xi_n\omega'$. Comme $\omega' = tb(t)$, on a $\xi_n tb(t) = \beta(\omega') = \beta(t)b(t\beta(t))$ et donc $\xi_n b(0) = \gamma(\beta)b(0)$, c'est-à-dire $\xi_n = \gamma(\beta)$. On en déduit que $\widetilde{\sigma}^{-1} \circ \beta \circ \widetilde{\sigma}(\omega) = \gamma(\beta)\omega$. Puisque $\gamma(\alpha) = \gamma(\beta)$ et que, pour les mêmes raisons que précédement, $\alpha(\omega) = \gamma(\alpha)\omega$, on en déduit $\widetilde{\sigma}^{-1} \circ \beta \circ \widetilde{\sigma}(\omega) = \alpha(\omega)$. Ainsi, $\widetilde{\sigma}^{-1} \circ \beta \circ \widetilde{\sigma} = \alpha$ dans $\mathrm{Gal}(k((t))/k)$.

□

Si le groupe $\mathrm{Gal}(k((t))/k)$ contient des éléments d'ordre n, alors le corps k contient toutes les racines n-ième de l'unité. Par ailleurs, si ξ_n désigne une racine primitive n-ième de l'unité, alors $t \longmapsto \xi_n t$ définit un élément d'ordre n dans $\mathrm{Gal}(k((t))/k)$. On en déduit le théorème suivant :

Théorème 6.– *Soit n un entier non nul et k est un corps de caractéristique ne divisant pas n. Le nombre de classe de conjugaison des éléments d'ordre n dans le groupe* $\mathrm{Gal}(k((t))/k)$ *vaut :*

- 0 *si k ne contient pas de racine primitive n-ième de l'unité,*
- $\varphi(n)$ *(indicateur d'Euler) sinon.*

En particulier, si k est un corps de caractéristique $\neq 2$, alors les involutions de $\mathrm{Gal}(k((t))/k)$ *forment une unique classe de conjugaison.*

Ainsi, si k est un corps réel clos, alors $\mathrm{Gal}(k((t))/k)$ ne contient, comme élément de torsion, que des involutions et c'est dernières forment une unique classe de conjugaison. Notons que, si l'involution de « référence » reste $t \mapsto -t$, il y a bien d'autres involutions. Par exemple, l'élément $t \longmapsto \dfrac{t}{t-1}$ est une involution (y compris dans le cas de la caractéristique 2).

Nous terminons ce paragraphe par une propriété qui sera bien utile pour la suite :

Corollaire 7.– *Si Γ_0 désigne un sous-groupe de torsion de* $\mathrm{Gal}(k((t))/k)$ *dont les ordres des éléments ne sont pas divisibles par la caractéristique de k, alors Γ_0 est isomorphe à un sous-groupe de $\mathbb{Q}/\mathbb{Z}$. C'est, en particulier, un groupe abélien.*

Preuve : La restriction du morphisme γ à Γ_0 est injective (d'après le théorème 5.a.) et à valeurs dans $\mu_\infty(k)$ qui est un groupe isomorphe à un sous-groupe de $\mathbb{Q}/\mathbb{Z}$.

2.3.– Les objets fermés de l'extension $k((t))/k$ en caractéristique nulle.

On supposera dans ce paragraphe que le corps k est de caractéristique nulle. On étudie ici, les sous-extensions fermées de $k((t))/k$ et les sous-groupes fermés de $\mathrm{Gal}(k((t))/k)$.

Théorème 8.– (caractérisation des sous-extensions fermées) *Soit L une sous-extension fermée de $k((t))/k$, non égale à k. L'extension $k((t))/L$ est finie et, plus précisément, si $n = [k((t)) : L]$ alors $\mu_n \subset k$ et il existe $\omega_0 \in 1 + \mathfrak{M}$ tel que*

$$L = k((t^n\omega_0(t)))$$

Réciproquement, si $k((t))/L$ est finie (avec $k \subset L$) de degré n alors il existe $\omega_0 \in 1 + \mathfrak{M}$ tel que $L = k((t^n\omega_0(t)))$ et, dans ces conditions, L est fermée si et seulement si $\mu_n \subset k$.

Preuve : On choisit une série $\omega \in L - k$ de valuation $n = v(\omega) \geq 1$ minimale.

Puisque L est fermée, en utilisant le théorème 1.b., on voit que $k((\omega)) \subset L$. Si l'on pose $\omega = t^n\omega_0$ avec $\omega_0 \in 1 + \mathfrak{M}$ (ce qui peut être fait quitte à multiplier ω par un élément adéquat de k), on a vu que $\left\{1, t{\omega_0}^{1/n}, \cdots, t^{n-1}{\omega_0}^{(n-1)/n}\right\}$ (où ${\omega_0}^{1/n}$ désigne l'unique racine n-ième de ω_0 dans $1 + \mathfrak{M}$) forme une $k((\omega))$-base du $k((\omega))$-espace vectoriel $k((t))$.

Supposons que $L \neq k((\omega))$ et prenons une série $U \in L - k((\omega))$. On écrit

$$U(t) = S_0(\omega(t)) + S_1(\omega(t))t{\omega_0}^{1/n}(t) + \cdots + S_{n-1}(\omega(t))t^{n-1}{\omega_0}^{(n-1)/n}(t)$$

où $S_0, \cdots, S_{n-1} \in k((t))$. Quitte à multiplier U par une bonne puissance de ω, on peut supposer que les S_i sont de valuations positives et qu'au moins une d'entre elles est de valuation nulle. Notons i_0 le plus petit indice tel que $v(S_{i_0}) = 0$. Pour tout $i = 0, \cdots, n-1$, on a

$$v\left(S_i(\omega(t))t^i{\omega_0}^{i/n}(t)\right) = i + nv(S_i) \equiv i \bmod(n)$$

Il s'ensuit que $v(U) = i_0 < n$, ce qui contredit la minimalité de n. Ainsi, on a bien l'égalité $L = k((\omega)) = k((t^n\omega_0(t)))$ avec $\omega_0 \in 1 + \mathfrak{M}$.

Réciproquement, si $k((t))/L$ est finie alors L est un corps complet pour la valuation v (voir [Rib2]). Si S est une uniformisante alors $L = k((S))$, et le lemme 3 assure que $n = v(S)$. Ainsi, quitte à multiplier S par une constante non nulle on en déduit l'existence de $\omega_0 \in 1 + \mathfrak{M}$ telle que $L = k((\omega)) = k((t^n\omega_0(t)))$. Les conjugués de $t{\omega_0}^{1/n}$ sur $k((\omega))$ sont les $\xi_n t{\omega_0}^{1/n}$ avec $\xi_n \in \mu_n$ et donc, $k((t))/k((\omega))$ est fermé (i.e. galoisienne au sens classique puisque l'extension est finie) si et seulement si $\mu_n \subset k$.

□

Remarque : Dans la preuve de la réciproque du théorème précédent, on utilise le fait qu'un sous-corps d'indice fini d'un corps discrêtement valué et complet est complet. Cette propriété est vraie en caractéristique 0, mais pas de manière générale en caractéristique p. Cette pathologie est à relier à une question d'inséparabilité : dans [Rib 2] il est démontré que si K est un corps discrêtement valué d'indice fini sous sa complétion $\widehat{K}$, alors l'extension $\widehat{K}/K$ est purement inséparable. Dans le cas des corps de séries, on obtient alors que si k est un corps de caractéristique p tel que pour tout entier $n \geq 1$, $[k : k^{p^n}]$ est fini (e.g. k parfait), alors tout sous-corps d'indice fini de $k((t))$ contenant k est complet. En effet, si L est d'indice fini dans $k((t))$ et contient k alors sa complétion $\widehat{L}$ contient k et est incluse dans $k((t))$. Ainsi, il existe une série S de valuation minimale telle que $\widehat{L} = k((S))$. L'extension $k((S))/L$ étant radicielle, disons de degré p^n, on a alors $k^{p^n}((S^{p^n})) \subset L$. Comme $[k : k^{p^n}]$ est finie, on a $k((S^{p^n})) = k.k^{p^n}((S^{p^n})) \subset L$ et comme $[k((S)) : k((S^{p^n}))] \leq p^n$, L est complet en tant qu'extension finie d'un corps complet.

Dans le cas général, il existe des exemples de sous-corps d'indice fini de $k((t))$ contenant k et qui ne sont pas complets. Nous allons en donner un.

On considère le corps de fractions $k = \mathbb{F}_p(x_0, x_1, \cdots)$ en une infinité dénombrable de variables et à coefficients dans $\mathbb{F}_p$. On a $k^p = \mathbb{F}_p(x_0^p, x_1^p, \cdots)$ et donc $[k : k^p] = +\infty$. Il convient tout de même de constater que l'extension $k((t))/k^p((t))$ est algébrique, tout élément de $k((t))$ étant d'ordre 1 ou p sur $k^p((t))$. On considère alors le corps

$$L = k^p((t))(x_0, x_1, \cdots) = \bigcup_{n\geq 0} k^p(x_0, \cdots, x_n)((t)) = \bigcup_{n\geq 0} \mathbb{F}_p(x_0, \cdots, x_n, x_{n+1}^p, x_{n+2}^p, \cdots)((t))$$

On a visiblement $k \subset L$ et, par ailleurs, il est clair que la série $S_0(t) = x_0 + x_1 t + x_2 t^2 + \cdots$ n'est pas un élément de L.

Soit maintenant $\mathscr{E}$ l'ensemble des sous-corps M, $L \subset M \subset k((t))$, tels que $S_0 \notin M$. L'ensemble $\mathscr{E}$ est certainement inductif pour l'inclusion et, d'après Zorn, il existe donc un élément maximal $M_0 \in \mathscr{E}$. Puisque $S_0 \notin M_0$ et que S_0 est radiciel d'ordre p sur L, on en déduit que $[M_0(S_0) : M_0] = p$.

Soit maintenant $S \in k((t)) - M_0$ une série quelconque. L'élément S étant radiciel de degré p sur L, on a $[M_0(S) : M_0] = p$. Par maximalité de M_0, on a $S_0 \in M_0(S)$ et donc, à cause des degrés, on a $M_0(S) = M_0(S_0)$. Puisque S est quelconque, on en déduit finalement que $M_0(S_0) = k((t))$.

Ainsi, $[k((t)) : M_0] = p$ et le corps M_0 n'est pas complet. En effet, la suite $(u_n)_n$ définie pour $n \geq 0$ par $u_n = x_0 + x_1 t + \cdots + x_n t^n$, est une suite d'éléments de $L \subset M_0$, qui est visiblement de Cauchy, mais qui ne peut converger dans M_0 car sa limite dans $k((t))$ est justement S_0.

En combinant le résultat du théorème 8 avec ceux de la partie précédente, on obtient alors le

Corollaire 9.– *a) Les sous-groupes fermés non-triviaux de* $\mathrm{Gal}(k((t))/k)$ *sont exactement ses sous-groupes finis et ces derniers sont cycliques.*

b) Il y a des sous-groupes cycliques d'ordre n dans $\mathrm{Gal}(k((t))/k)$ *si et seulement si k contient les racines primitives n-ièmes de l'unité et, dans ces conditions, il y a* $\varphi(n)$ *classes de conjugaisons de tels sous-groupes. En particulier, les seuls sous-groupes fermés distingués sont d'ordre* 2.

On retiendra en particulier de cette étude le résultat fondamental suivant :

Théorème 10.– *Un sous-groupe fini de* $\mathrm{Gal}(k((t))/k)$ *est nécessairement cyclique.*

Remarques : a) Le fait que les sous-groupes fermés de $\mathrm{Gal}(k((t))/k)$ soient finis est à rapprocher du cas de l'extension $k(t)/k$. Pour cette extension, le théorème de Luroth donne la même propriété.

b) La terminologie d'objets « fermés » provient bien sûr du cas des extensions galoisiennes algébriques, pour lesquelles les sous-groupes fermés du groupe de Galois correspondent au sous-groupes fermés pour la topologie de Krull. Il est intéressant de remarquer que dans le cas de l'extension $k((t))/k$ (comme pour celui de $k(t)/k$), il n'existe pas de topologie sur $\mathrm{Gal}(k((t))/k)$ qui lui confère une structure de groupe topologique pour laquelle les sous-groupes fermés (au sens galoisien) correspondent aux sous-groupes fermés pour cette topologie.

En effet, si Γ désigne un groupe topologique dans lequel les sous-groupes fermés non triviaux sont exactement les sous-groupes finis, alors soit Γ est de torsion, soit il est abélien (ce qui n'est pas le cas de $\mathrm{Gal}(k((t))/k)$ ni de $\mathrm{Gal}(k(t)/k)$). Pour voir ceci, il convient d'abord de remarquer que pour un tel groupe Γ donné, les points de Γ sont tous fermés (car translatés de l'élément neutre e). Cette propriété équivaut à dire que, pour tout $x \in \Gamma$, l'intersection de tous les voisinages de x est réduite à $\{x\}$. Considèrons un sous-groupe abélien Γ_0 de Γ alors son adhérence $\overline{\Gamma_0}$ est aussi un sous-groupe abélien. En effet, si $x, y \in \overline{\Gamma_0}$, alors pour tout voisinage U du commutateur $[x, y] = xyx^{-1}y^{-1}$ il existe un voisinage $U_x \times U_y$ du couple (x, y)

tel que $[U_x, U_y] \subset U$ (il s'agit ici de la traduction du fait que l'application $(x,y) \mapsto xyx^{-1}y^{-1}$ est continue). Puisque $U_x \cap \Gamma_0$ et $U_y \cap \Gamma_0$ sont non vides et que Γ_0 est abélien, on en déduit que $e \in U$ pour tout U. Ainsi, $[x,y] = e$ et donc $\overline{\Gamma_0}$ est abélien. Si Γ n'est pas de torsion alors il existe un élément $f \in \Gamma$ d'ordre infini et $\Gamma_0 =< f >$ est donc un sous-groupe abélien infini. D'après ce qui précède, $\Gamma = \overline{\Gamma_0}$ est abélien.

3.– Étude des centralisateurs.

On suppose dans ce paragraphe que k est un corps de caractéristique nulle. Pour un entier $n \geq 1$, on notera $\mu_n(k)$ l'ensemble des racines n-ième de l'unité dans k et $\mu_n = \mu_n(\overline{k})$. On pose $\mu_\infty = \bigcup_{n\geq 0} \mu_n$ et, pour tout nombre premier p, $\mu_{p^\infty} = \bigcup_{n\geq 0} \mu_{p^n}$.

3.1.– Divisibilité.

Nous étudions ici la divisibilité dans $\mathrm{Gal}(k((t))/k)$. Nous attirons l'attention du lecteur sur le fait que les puissances des éléments de $\mathrm{Gal}(k((t))/k)$ s'entendent pour la composition et qu'ainsi, si $f \in \mathrm{Gal}(k((t))/k)$ et $n \in \mathbb{Z}$, la notation $f^n(t)$ ne désigne pas le produit au sens de Cauchy n fois de la série $f(t)$, mais bien l'image de l'élément $t \in k((t))$ par l'automorphisme $f^n \in \mathrm{Gal}(k((t))/k)$.

Pour commencer, il faut remarquer que l'existence de racines dans $\mathrm{Gal}(k((t))/k)$ n'est pas assurée en toutes généralité. Par exemple, les éléments $f \in \mathrm{Gal}(k((t))/k)$ vérifiant $f(t) = -t + \lambda t^3 + \cdots$ avec $\lambda \neq 0$, ne possèdent aucune racine n-ième pour aucun entier n pair. En effet, un petit calcul montre qui si $u(t) = a_1 t + a_2 t^2 + \cdots$ avec $a_1 \neq 0, \pm 1$ alors pour tout $n \geq 2$, on a

$$u^n(t) = a_1^n t + a_2 a_1^{n-1}\left(\frac{a_1^n - 1}{a_1 - 1}\right)t^2 + \frac{a_1^{n-1}}{a_1 - 1}\left(2a_2^2(a_1^{2n-3} - 1) + a_3\left(\frac{a_1^{2n} - 1}{a_1 + 1}\right)\right)t^3 + \cdots$$

L'égalité $u^n(t) = f(t)$ mène à $a_1^n = -1$ et $a_2 = 0$ et donc le coefficient de degré 3 de $u^n(t)$ est nul ce qui est absurde.

Ensuite, il convient de constater que si $f \in \mathrm{Gal}(k((t))/k)$ est un élément de torsion, alors, sous réserve de l'existence de certaines racines de l'unité dans k, f possède pour tout entier $n \geq 2$ une infinité de racines n-ième dans $\mathrm{Gal}(k((t))/k)$:

Théorème 11.– *Si $f \in \mathrm{Gal}(k((t))/k)$ désigne un élément d'ordre d et $n \geq 2$ un entier, alors les propositions suivantes*

i) f possède une racine primitive n-ième (i.e. un élément u tel que $u^n = f$ et $u^a \neq f$ pour $1 \leq a \leq n-1$),

ii) f possède une infinité de racines primitives n-ième,

iii) $\mu_{dn} \subset k$,

sont équivalentes.

Preuve : *i)* $\Longrightarrow$ *iii)* Si u est une racine primitive n-ième de f alors u est d'ordre dn et, en appliquant le théorème 5.a., on voit que $\gamma(u)$ est une racine primitive dn-ième de l'unité.

iii) $\Longrightarrow$ *ii)* Considérons $k((\omega))$ le corps des invariants de $k((t))$ par f. Pour tout $\sigma \in \mathrm{Gal}(k((\omega))/k)$, le corps $\sigma(k((\omega^n))) = k((\sigma(\omega)^n))$ vérifie que $k((\omega))/k((\sigma(\omega)^n))$ est galoisienne de groupe $\mathbb{Z}/n\mathbb{Z}$ (d'après le théorème 8). Notons u_σ un générateur de ce groupe de Galois, c'est aussi une racine primitive n-ième de l'identité dans $\mathrm{Gal}(k((\omega))/k)$. Pour $\sigma, \sigma' \in \mathrm{Gal}(k((\omega))/k)$, l'égalité $k((\sigma(\omega)^n)) = k((\sigma'(\omega)^n))$ équivaut à $\sigma'\sigma^{-1} \in \mathrm{Gal}(k((\omega))/k((\omega^n)))$. En utilisant la proposition 4 on voit alors que l'ensemble des racines primitives n-ième de l'identité dans $\mathrm{Gal}(k((\omega))/k)$ est biunivoquement décrit par l'ensemble

$$\left\{u_\sigma^h /\ (h,n) = 1,\ \sigma \in \mathrm{Gal}(k((\omega))/k((\omega^n)))\backslash\mathrm{Gal}(k((\omega))/k)\right\}$$

Ce dernier ensemble quotient est visiblement infini puisque $\mathrm{Gal}(k((t))/k((t^n)))$ est fini.

Si $\sigma \in \mathrm{Gal}(k((\omega))/k)$, alors l'extension $k((t))/k((\sigma(\omega)^n))$ est de degré dn et, comme $\mu_{dn} \subset k$, les théorèmes 8 et 10 assurent que cette extension est cyclique. Puisque f est un élément de $\mathrm{Gal}(k((t))/k((\sigma(\omega)^n)))$ d'ordre d, il existe donc une racine primitive n-ième de f dans ce groupe de Galois. Ceci étant valable pour tout σ, la remarque précédente sur l'infinitude des racines primitive n-ième de l'identité dans $\mathrm{Gal}(k((\omega))/k)$ prouve alors le ii).

□

Les éléments de torsion sont en fait les seuls éléments à possèder (potentiellement) une infinité de racines n-ième. Plus précisément, on a :

Théorème 12.– *Soit $f \in \mathrm{Gal}(k((t))/k)$ un élément d'ordre infini et $n \geq 1$ un entier. Si α désigne une racine n-ième de $\gamma(f)$ dans k, alors il existe au plus un élément $u \in \mathrm{Gal}(k((t))/k)$ tel que $u^n = f$ et $\gamma(u) = \alpha$. En conséquence de quoi, si f possède une racine n-ième, $u \in \mathrm{Gal}(k((t))/k)$, alors*

a) f possède un nombre fini $1 \leq d \leq n$ de racines n-ième $u_1, \cdots, u_d$.

b) Les éléments $u_1, \cdots, u_d$ commutent deux à deux.

c) Il existe un élément $\theta \in \mathrm{Gal}(k((t))/k)$ d'ordre d qui commute avec u et tel que $u_i = u \circ \theta^i$ pour tout $i = 0, \cdots, d-1$.

d) $d|n$.

Par ailleurs, si $\gamma(f) = 1$ alors f possède toujours une racine n-ième $u \in \mathrm{Gal}_{\mathscr{D}}(k((t))/k)$. Si $\gamma(f) \notin \mu_\infty(k)$, alors f possède une racine n-ième dans $\mathrm{Gal}(k((t))/k)$ si et seulement si $\gamma(f) \in k^n$ et dans ces conditions $d = \sharp\mu_n(k)$.

Preuve : Supposons établie la première partie du théorème. Comme $\gamma(f)$ possède au plus n racines n-ième dans k, il y a au plus n racines de f dans $\mathrm{Gal}(k((t))/k)$, d'où le a).

Soient $v, w \in \mathrm{Gal}(k((t))/k)$ tels que $v^n = w^n = f$. Puisque $(vwv^{-1})^n = vw^nv^{-1} = w^n$, les éléments vwv^{-1} et w sont donc deux racines n-ième de f. Maintenant, on a $\gamma(w) = \gamma(vwv^{-1})$ et donc $vwv^{-1} = w$. Ainsi, v et w commutent, d'où le b).

Pour $i = 1, \cdots, d$ posons $\theta_i = u^{-1}u_i$. Puisque u et u_i commutent, on en déduit que $\theta_i^n = \mathrm{Id}$ et que les θ_i commutent entre eux (ainsi qu'avec tous les u_i). On a donc pour tout i, j, $(u\theta_i\theta_j^{-1})^n = f$ et donc l'ensemble $\{\theta_1, \cdots, \theta_d\}$ est un groupe. Le théorème 8 assure que ce groupe est cyclique, d'où l'existence de θ et le c). La relation $d|n$ du d) vient finalement du fait que $\theta^n = \mathrm{Id}$.

Il reste donc à prouver l'unicité de la racine u à $\gamma(u)$ fixé. Etant donné un élément $u \in \mathrm{Gal}(k((t))/k)$, si l'on pose $u(t) = \alpha t + \cdots + a_h t^h + \cdots$ alors une simple récurrence sur l'entier n montre que, pour tout $h \geq 2$, il existe $R_{n,h} \in k(x_1, \cdots x_{h-1})$ tel que

$$u^n(t) = \alpha^n t + \cdots + \left(a_h c_{n,h} + R_{n,h}(a_1, \cdots, a_{h-1})\right) t^h + \cdots$$

où $c_{n,h} = \frac{\alpha^{nh} - \alpha^n}{\alpha^h - \alpha}$ si $\alpha \notin \mu_{h-1}$ et $c_{n,h} = n\alpha^{n-1}$ si $\alpha \in \mu_{h-1}$.

Posons $f(t) = \lambda t + m_2 t^2 + \cdots$. Les solutions de l'équation $f = u^n$ sont donc les u tels que $\alpha^n = \lambda$ et, pour tout $h \geq 2$, $m_h = a_h c_{n,h} + R_h(a_1, \cdots, a_{h-1})$. Ainsi, si pour tout h le coefficient $c_{n,h}$ est non nul, on voit qu'il existe une unique solution à l'équation à α fixé.

• Si $\gamma(f) \notin \mu_\infty$, alors comme $\alpha^n = \lambda$, on a $\alpha \notin \mu_\infty$. Ainsi, pour tout n et tout h le coefficient $c_{n,h}$ est non nul et l'équation $f = u^n$ possède donc une unique solution. Ceci étant valable pour tout α vérifiant $\alpha^n = \lambda$, on en déduit bien que $d = \sharp\mu_n(k)$ dans ce cas.

• Si $\gamma(f) = 1$. Pour le choix $\alpha = 1$, les $c_{n,h}$ sont alors tous non nuls et l'équation $f = u^n$ possède donc une unique solution de la forme $u(t) = t + \cdots$. Soit maintenant $v(t) = \xi_n t + \cdots$ une autre racine. L'élément ξ_n désigne alors une racine n-ième de l'unité différente de 1 et, toujours à cause de l'unicité de u, le même argument qu'au début de la preuve montre que u et v commutent et donc que $\sigma = uv^{-1}$ est une racine n-ième de l'identité. Quitte à conjuguer le problème par un automorphisme de $k((t))$ (théorème 5), on peut supposer que $\sigma(t) = \xi_n t$. Puisque f commute à u et v, f commute à σ et donc $f(t)$ s'écrit en fait

$$f(t) = t + b_r t^{rn+1} + b_{r+1} t^{(r+1)n+1} + \cdots$$

avec $b_r \neq 0$ ($f(t) \neq t$ car f est d'ordre infini). Supposons donnée w une autre racine n-ième de f, telle que $w(t) = \xi_n t + \cdots$. L'élément $g = uw^{-1}$ est aussi une racine n-ième de l'identité. Posons

$$g(t) = \xi_n t + a_q t^q + a_{q+1} t^{q+1} + \cdots$$

avec $a_q \neq 0$ (puisque $g \neq \sigma$). On remarque que g commute avec f et l'on établit le lemme suivant :

Lemme 13.– *Soient $n \geq 1$ un entier, ξ_n une racine n-ième de l'unité et $f, g \in \mathrm{Gal}(k((t))/k)$ tels que $f(t) = t + b_r t^{rn+1} + b_{r+1} t^{(r+1)n+1} + \cdots$ avec $b_r \neq 0$ et $g(t) = \xi_n t + a_q t^q + a_{q+1} t^{q+1} + \cdots$ avec $a_q \neq 0$. Si $f \circ g = g \circ f$ alors $g^n \neq \mathrm{Id}$.*

Preuve : Si l'on suppose que $q \not\equiv 1 \bmod(n)$ alors le coefficient de degré $nr + q$ de $g \circ f(t)$ vaut $qa_q b_r + a_{nr+q}$ alors que celui de $f \circ g(t)$ vaut $(nr + 1)a_q b_r + a_{nr+q}$ et donc $f \circ g \neq g \circ f$. Ainsi, $q \equiv 1 \bmod(n)$ et une récurrence immédiate montre que $g^h(t) = \xi_n^h t + h\xi_n^{h-1} a_q t^q + \cdots$. On en déduit que $g^n(t) \neq t$.

□

Ainsi, g ne peut pas être d'ordre n et donc v est l'unique racine n-ième de f vérifiant $\gamma(v) = \xi_n$.

• Si $\gamma(f) \in \mu_\infty(k)$, on a $\gamma(f)^h = 1$ pour un certain entier $h \geq 1$ et donc $f^h(t) = t + \cdots$ ($\neq t$, car f est d'ordre infini). Si $u, v \in \mathrm{Gal}(k((t))/k)$ sont deux racines n-ième de f telles que $\gamma(u) = \gamma(v)$ alors u et v sont deux racines nh-ièmes de f^h et donc, en vertu du cas précédent, on a $u = v$.

Ceci achève la preuve du théoreme 12.

□

Considérons un élément $f \in \mathrm{Gal}(k((t))/k)$ d'ordre infini, un entier $n \geq 1$ et $f^{1/n}$, une racine n-ième de f. Si g commute avec f, alors $(gf^{1/n}g^{-1})^n = g(f^{1/n})^n g^{-1} = gfg^{-1} = f = (f^{1/n})^n$ et, puisque $\gamma(f^{1/n}) = \gamma(gf^{1/n}g^{-1})$, on en déduit que $gf^{1/n} = f^{1/n}g$. On peut donc appliquer cette propriété au cas où $g = f^{1/m}$ est une racine m-ième de f pour un autre entier m. Dans cette situation l'élément $(f^{1/n})^a (f^{1/m})^b$ où $am + bn = \mathrm{pgcd}(n, m)$ est alors une racine l-ième de f avec $l = \mathrm{ppcm}(n, m)$.

On considère alors l'ensemble A composé des entiers n tels que f possède une racine n-ième. D'après ce qui précède, l'ensemble A est stable par ppcm et vérifie que si $n \in A$ alors tous les diviseurs de n sont dans A. Pour un élément $n \in A$ donné, on note d_n le nombre de racines n-ième de f. Si $f^{1/n}$ désigne une racine n-ième fixée alors le théorème 12.c,d. assure que l'ensemble

$$C_n = \{(f^{1/n})^{-1} g / \ g^n = f\}$$

est un groupe cyclique d'ordre $d_n | n$. Le théorème 12 assure que si $n | m$ alors $C_n \subset C_m$. Ainsi, puisque A est stable par ppcm, on voit que la réunion des C_n pour $n \in A$ forme un sous-groupe abélien de $\mathrm{Gal}(k((t))/k)$. C'est donc un sous-groupe de $\mathbb{Q}/\mathbb{Z}$ puisqu'il est visiblement de torsion (corollaire 7).

Définition 14.– *On appelle* « traîne » *de l'automorphisme f, le sous-groupe de $\mathbb{Q}/\mathbb{Z}$ introduit ci-dessus. On le note $\mathscr{T}_f$.*

Notons que les sous-groupes de $\mathbb{Q}/\mathbb{Z} \simeq \oplus_p \mu_{p^\infty}$ sont assez facile à décrire, ce sont les sous-groupes de la forme

$$\bigoplus_{p\in\mathscr{P}_0} \mu_{p^{n_p}} \oplus \bigoplus_{p\notin\mathscr{P}_0} \mu_{p^\infty}$$

où $\mathscr{P}_0$ désigne un certain sous-ensemble de nombres premiers.

Dans le cas où $k = \overline{k}$ et $\gamma(f) \notin \mu_\infty(k)$, le théorème 12 assure que l'on a toujours $\mathscr{T}_f \simeq \mathbb{Q}/\mathbb{Z}$. Dans le cas extrême inverse, on peut signaler les éléments $f \in \mathrm{Gal}(k((t))/k)$ de la forme $f(t) = t + \alpha t^2 + \cdots$ où $\alpha \neq 0$. Si $u(t) = a_1 t + a_2 t^2 + \cdots$ avec $a_1 \neq 1$, alors comme nous l'avons vu au début de ce paragraphe, pour tout $n \geq 1$, on a $u^n(t) = a_1^n t + a_2 a_1^{n-1}\left(\frac{a_1^n-1}{a_1-1}\right) t^2 + \cdots$. Ainsi, f possède au maximum une racine n-ième. Dans cette situation, on a donc toujours $\mathscr{T}_f = 1$.

Cet exemple est un cas particulier du corollaire 23 à venir.

3.2.– Centralisateurs.

Pour soulager les notations, nous noterons $\Gamma = \mathrm{Gal}(k((t))/k)$ et $\Gamma_{\mathscr{P}} = \mathrm{Gal}_{\mathscr{P}}(k((t))/k)$. Pour un élément x d'un groupe G, on notera $\mathscr{C}_G(x)$ le centralisateur de x dans G.

Pour commencer, on considère un élément $u \in \Gamma$ d'ordre n. Quitte à conjuguer u, on peut supposer que u est donné par $u(t) = \xi_n t$ où ξ_n désègne une racine primitive n-ième de l'unité (théorème 5). Un élément $f \in \Gamma$ commute alors avec u si et seulement si on a

$$g(t) = \sum_{r\geq 0} a_r t^{rn+1}$$

On constate que $\mathscr{C}_\Gamma(u)$ est un groupe non abélien que l'on pourrait qualifier de « dimension infinie » , puisqu'il est biunivoquement décrit par les suites $(a_r)_r \in k^{\mathbb{N}}$ vérifiant $a_0 \neq 0$. Nous allons voir dans ce qui suit, qu'en dehors du cas des éléments de torsion, les centralisateurs des éléments de Γ sont abéliens et de « petite taille » .

3.2.1.– Centralisateurs des éléments de $\mathrm{Gal}_{\mathscr{P}}(k((t))/k)$.

Proposition 15.– *On considère un élément $f \in \Gamma_{\mathscr{P}}$ qui n'est pas égal à l'identité et l'on pose $f(t) = t + a_l t^l + \cdots$ avec $a_l \neq 0$. Si $g \in \Gamma_{\mathscr{P}}$ commute avec f alors $g(t) = t + \alpha t^l + \cdots$ pour un certain $\alpha \in k$. Réciproquement, si $\alpha \in k$ alors il existe un unique $g \in \Gamma_{\mathscr{P}}$ qui commute avec f et qui vérifie $g(t) = t + \alpha t^l + \cdots$.*

Preuve : Si $f, g \in \Gamma$, en écrivant $f(t) = a_1 t + a_2 t^2 + \cdots$ et $g(t) = b_1 t + b_2 t^2 + \cdots$, le coefficient de degré k de $g \circ f(t)$ vaut formellement

$$c_k = \sum_{h=1}^{k} a_h \sum_{i_1+\cdots+i_h=k} b_{i_1} \cdots b_{i_h}$$

et celui de $f \circ g(t)$ vaut

$$d_k = \sum_{h=1}^{k} b_h \sum_{i_1+\cdots+i_h=k} a_{i_1} \cdots a_{i_h}$$

On se place dans les hypothèses de la proposition et l'on pose $a_1 = b_1 = 1$, $a_2 = \cdots = a_{l-1} = 0$ et $a_l \neq 0$. On cherche dans un premier temps à exprimer la valeur de $c_k - d_k$ pour $k \geq 1$.

- Pour $1 \leq k \leq l-1$, on a $c_k = b_k = d_k$ et donc $c_k - d_k = 0$.
- Pour $k = l$, on a $c_l = a_l + b_l = d_l$ et donc $c_k - d_k = 0$.
- Pour $k = l+1$, on a $c_{l+1} = a_{l+1} + b_{l+1} + l a_l b_2$ et $d_{l+1} = a_{l+1} + b_{l+1} + 2a_l b_2$ et donc $c_k - d_k = (l-2)a_l b_2$.

• Pour $k \geq l+2$, on a

$$c_k = b_k + \left(\sum_{h=l}^{k-1} a_h \sum_{i_1+\cdots+i_h=k} b_{i_1} \cdots b_{i_h} \right) + a_k$$

Dans la double somme entre parenthèse, le plus grand indice i pour lequel b_i apparaisse est $i = k-l+1$ et le coefficient b_{k-l+1} apparaît dans cette somme seulement pour l'indice $h = l$. Ainsi,

$$c_k = la_l b_{k-l+1} + a_k + b_k + R_{1,k}(a_l, \cdots, a_{k-1}, b_2, \cdots, b_{k-l})$$

où $R_{1,k} \in \mathbb{Z}[x_l, \cdots, x_{k-1}, y_2, \cdots, y_{k-l}]$ est un polynôme pour lequel chaque monôme contient au moins un x_i ($i \geq l$) et un y_j ($j \geq 2$). De la même manière, dans

$$d_k = \sum_{h=1}^{k} b_h \sum_{i_1+\cdots+i_h=k} a_{i_1} \cdots a_{i_h}$$

le coefficient qui multiplie b_{k-l+1} est la somme pour les $(k-l+1)$-uplets qui sont une permutation de $(1, \cdots, 1, l)$. Ainsi,

$$d_k = (k-l+1)a_l b_{k-l+1} + a_k + b_k + R_{2,k}(a_l, \cdots, a_{k-1}, b_2, \cdots, b_{k-l})$$

où $R_{2,k} \in \mathbb{Z}[x_l, \cdots, x_{k-1}, y_2, \cdots, y_{k-l}]$ est un polynôme pour lequel chaque monôme contient au moins un x_i ($i \geq l$) et un y_j ($j \geq 2$).

Pour $k \geq l+2$, on a donc

$$c_k - d_k = (k-2l+1)a_l b_{k-l+1} + R_k^2(a_l, \cdots, a_{k-1}, b_2, \cdots, b_{k-l}) - R_k^1(a_l, \cdots, a_{k-1}, b_2, \cdots, b_{k-l})$$

On cherche maintenant une condition nécessaire et suffisante pour que $c_k - d_k = 0$ pour tout $k \geq 1$.

• Si $l = 2$, aucune contrainte n'existe pour b_2, mais la relation $c_k - d_k = 0$ pour $k \geq 4$ définit par récurrence d'uniques valeurs pour les coefficients b_i pour $i \geq 3$.

• Si $l \neq 2$, alors la relation $c_{l+1} - d_{l+1} = 0$ assure que $b_2 = 0$. En utilisant la relation $c_k - d_k = 0$ pour $k \geq l+2$, un raisonnement par récurrence mené pour les indices $l+1 \leq k \leq 2l-2$ montre que $b_2 = \cdots = b_{l-1} = 0$.

Une fois cette nullité obtenue, la relation $c_k - d_k = 0$ pour $k \geq 2l$ définit, par récurrence le coefficient b_{k-l+1} en fonction des coefficients b_i pour $i \leq k-l$. En particulier, il y a existence et unicité de ces coefficients une fois le coefficient b_l choisi, coefficient pour lequel il n'y a aucune contrainte.

□

Ainsi, le centralisateur, $\mathscr{C}_{\Gamma_{\mathscr{P}}}(f)$, de f dans $\Gamma_{\mathscr{P}}$ est un objet que l'on pourrait qualifier de dimension 1. Nous allons essayer de formaliser cette idée de manière rigoureuse et montrer que ce centralisateur a naturellement une structure de k-espace vectoriel de dimension 1. Pour cela, nous allons introduire une fonction puissance dans le groupe $\Gamma_{\mathscr{P}}$.

Lemme 16.– *Il existe une famille (unique) de polynômes $(P_h)_{h\geq 2}$ telle que $P_h \in k[t_2, \cdots, t_h, x]$ pour tout h et telle que pour tout entier $n \geq 0$ et tout $f(t) = t + \alpha_2 t^2 + \alpha_3 t^3 + \cdots$ on ait*

$$f^n(t) = t + P_2(\alpha_2, n)t^2 + P_3(\alpha_2, \alpha_3, n)t^3 + \cdots$$

Par ailleurs, on a $P_h(0) = 0$ et $d^\circ P_h \leq h-1$ pour tout $h \geq 2$.

Preuve : On construit par récurrence la suite $(P_h)_{h\geq 2}$ en question. Une récurrence élémentaire montre que $P_2(x) = \alpha_2 x$. Pour n fixé, notons $f^n(t) = t + \sum_{h\geq 2} \lambda_h^{(n)} t^h$ (évaluation en t de l'itérée

n-ième de f) et pour h, notons $f(t)^h = \sum_{i\geq h} \alpha_i^{(h)} t^i$ (produit au sens de Cauchy de $f(t)$ par elle-même h fois). On a

$$\begin{aligned} f^{n+1}(t) &= f(t) + \sum_{h\geq 2} \lambda_h^{(n)} f(t)^h = t + \sum_{i\geq 2} \alpha_i^{(1)} t^i + \sum_{h\geq 2} \sum_{i\geq h} \lambda_h^{(n)} \alpha_i^{(h)} t^i \\ &= t + \sum_{i\geq 2} \alpha_i^{(1)} t^i + \sum_{i\geq 2} \left(\sum_{h=2}^{i} \lambda_h^{(n)} \alpha_i^{(h)} \right) t^i \end{aligned}$$

On en déduit donc que, pour tout $h \geq 3$ et tout n, on a :

$$\lambda_h^{n+1} = \alpha_h^{(1)} + \sum_{i=2}^{h} \alpha_h^{(i)} \lambda_i^{(n)}$$

et, puisque $\alpha_h^{(h)} = 1$, on trouve finalement

$$\lambda_h^{(n+1)} - \lambda_h^n = \alpha_h^{(1)} + \sum_{i=2}^{h-1} \alpha_h^{(i)} \lambda_i^{(n)}$$

Supposons la propriété que l'on veut démontrer vraie jusqu'au rang $h-1 \geq 2$. On écrit donc $\lambda_i^{(n)} = P_i(n)$ pour tout $i = 2, \cdots, h-1$. On considère la k-base de $k[x]$ constituée des polynôme $Q_0(x) = 1$, et pour tout $j \geq 1$, $Q_i(x) = \frac{x(x-1)\cdots(x-i+1)}{i!}$. Considèrons aussi l'endomorphisme Δ de $k[x]$ défini par $\Delta(P)(x) = P(x+1) - P(x)$. On a $\Delta(Q_{i+1}) = Q_i$ pour tout $i \geq 0$ et le noyau de Δ est égal au polynômes constants. Pour $i \leq h-1$ fixé, on a $P_i(0) = 0$ et $d^\circ P_i \leq i$, on peut donc écrire

$$P_i(x) = \sum_{j=1}^{i-1} \omega_{i,j} Q_j(x)$$

Posons alors

$$\begin{aligned} P_h(x) &= \alpha_h^{(1)} Q_1(x) + \sum_{i=2}^{h-1} \sum_{j=1}^{i-1} \alpha_h^{(i)} \omega_{i,j} Q_{j+1}(x) \\ &= \alpha_h^{(1)} Q_1(x) + \sum_{j=2}^{h-1} \sum_{i=j}^{h-1} \alpha_h^{(i)} \omega_{i,j-1} Q_j(x) \end{aligned}$$

Puisque $\Delta(P_h)(n) = \lambda_h^{(n+1)} - \lambda_h^{(n)}$ et que $P_h(0) = 0 = \lambda_h^{(0)}$, on en déduit bien que $\lambda_h^{(n)} = P_h(n)$. Il est clair qu'on a alors $d^\circ P_h \leq h-1$.

□

La preuve que nous venons de donner permet de calculer simplement et explicitement les polynômes P_h. Pour $h = 2, 3, 4$ on trouve :

$$\begin{cases} P_2(\alpha_2, x) &= \alpha_2 x \\ P_3(\alpha_2, \alpha_3, x) &= \alpha_2^2 x^2 + (\alpha_3 - \alpha_2^2) x \\ P_4(\alpha_2, \alpha_3, \alpha_4, x) &= \alpha_2^3 x^3 + (\frac{5}{2}\alpha_2\alpha_3 - \frac{5}{2}\alpha_2^3) x^2 + (\alpha_4 - \frac{5}{2}\alpha_2\alpha_3 + \frac{3}{2}\alpha_2^3) x \end{cases}$$

Définition 17.– *On garde les notations du lemme précédent. Si $\alpha \in k$, on appelle puissance α de f (pour la composition), l'élément noté f^α et défini par*

$$f^\alpha(t) = t + P_2(\alpha_2, \alpha) t^2 + P_3(\alpha_2, \alpha_3, \alpha) t^3 + \cdots$$

Exemple : Si l'on pose $f(t) = \dfrac{t}{1-t} = \sum_{h\geq 1} t^h$, une petite récurrence montre que pour tout $n \geq 1$, on a $f^n(t) = \dfrac{t}{1-nt} = \sum_{h\geq 1} n^{h-1}t^k$. Pour $h \geq 2$ fixé, on a donc $P_h(n) = n^{h-1}$ pour tout $n \geq 1$, ce qui assure que $P_h(x) = x^{h-1}$, puisque nous sommes en caractéristique 0 et que $\mathbb{N}$ est un ensemble infini. Ainsi, pour tout $\alpha \in k$, on a

$$f^\alpha(t) = \frac{t}{1-\alpha t}$$

Proposition 18.– *Pour tous $\alpha, \beta \in k$ et tout $f \in \Gamma_{\mathscr{P}}$, on a $(f^\alpha)^\beta = f^{\alpha\beta}$ et $f^\alpha f^\beta = f^{\alpha+\beta}$. Si $g \in \Gamma_{\mathscr{P}}$ commute avec f alors $(fg)^\alpha = f^\alpha g^\alpha$. En particulier, pour tout $n \geq 1$, l'élément $f^{1/n}$ est égal à l'unique racine n-ième de f dans $\Gamma_{\mathscr{P}}$.*

Preuve : En appliquant la définition, on a que

$$(f^\alpha)^\beta = t + P_2(P_2(\alpha_2, \alpha), \beta)t^2 + P_3(P_2(\alpha_2, \alpha), P_3(\alpha_2, \alpha_3, \alpha), \beta)t^3 + \cdots$$

et

$$f^{\alpha\beta}(t) = t + P_2(\alpha_2, \alpha\beta)t^2 + P_3(\alpha_2, \alpha_3, \alpha\beta)t^3 + \cdots$$

Puisque pour tous entiers n, m on a $(f^n)^m = f^{nm}$, pour un indice $h \geq 2$ fixé, le polynôme

$$P_h(P_2(\alpha_2, x), \cdots, P_h(\alpha_2, \cdots, \alpha_h, x), y) - P_h(\alpha_2, \cdots, \alpha_h, xy) \in k[x, y]$$

s'annule sur $\mathbb{N} \times \mathbb{N}$. Cette partie est Zariski-dense dans $k \times k$ et donc ce polynôme est nul. Ceci prouve que $(f^\alpha)^\beta = f^{\alpha\beta}$. Les deux autres propriétés s'établissent par la même méthode en explicitant les coefficients des séries $f^\alpha f^\beta(t)$ et $f^{\alpha+\beta}(t)$ (resp. $(f \circ g)^\alpha(t)$ et $f^\alpha g^\alpha(t)$) polynomialement en α et β (resp. en α).

□

Remarque 19.– Les valuations x-adiques des polynômes $P_n(x)$ sont toutes ≥ 1, de sorte que, pour toute série $s(t) \in k[[t]]$, la valuation de $P_n(s(t))$ est positive. Ainsi, la série $t + P_2(\alpha_2, s(t))t^2 + P_3(\alpha_2, \alpha_3, s(t))t^3 + \cdots$ est convergente, ce qui permet d'étendre la définition de la fonction puissance à l'anneau $k[[t]]$ tout entier.

L'application $s(t) \longmapsto f^{s(t)}$ jouit, hélas, de moins de propriétés que sa restriction à k. En effet, les relations établies dans la proposition 18 ne sont plus valables en toute généralité. Par exemple, si l'on considère $f(t) = t + t^2$ et $s(t) = t$, alors on a $f^s(t) = t + t^3 - t^4 + \cdots$ et $ff^s(t) - f^s f(t) = -t^4 + \cdots \neq 0$, ainsi f^s ne commute pas avec f. Le théorème 21 à venir montre en fait que, pour $s \in k[[t]]$, f^s commute avec f si et seulement s'il existe $\alpha \in k$ tel que $f^s = f^\alpha$.

□

Si l'on note $f^{<k>} = \{f^\alpha / \ \alpha \in k\}$, alors l'application $\alpha \longmapsto f^\alpha$ définit un isomorphisme entre $(k, +)$ et $(f^{<k>}, \circ)$ et les propriétés de la proposition précédente, montrent que cet isomorphisme confère aussi à $f^{<k>}$ une structure de k-espace vectoriel de dimension 1. Pour voir que l'isomorphisme en question est bien injectif, il convient d'abord de constater que α_h n'apparait dans P_h que de manière linéaire dans le coefficient de degré 1 en x (ce résultat s'obtient élémentairement par récurrence sur h). Ainsi donc, la nullité simultanée de tous les P_h équivaut à la nullité de tous les α_h ce qui n'a lieu que si $f = \mathrm{Id}$, ce qui est exclu. Il existe donc un indice h_0 tel que $P_{h_0}(x)$ ne soit pas nul. Si $\alpha \neq 0$ était tel que $f^\alpha = \mathrm{Id}$ alors on aurait $f^{n\alpha} = \mathrm{Id}$ pour tout entier n et donc le polynôme $P_{h_0}(x)$ posséderait une infinité de racines, ce qui est bien sûr absurde.

Lemme 20.– *Si $f(t) = t + \alpha_h t^h + \cdots$ avec $\alpha_h \neq 0$, alors pour tout $\alpha \in k$, on a $f^\alpha(t) = t + \alpha\alpha_h t^h + \cdots$.*

Preuve : Il est facile de voir par récurrence sur l'entier n que $f^n(t) = t + n\alpha_h t^h + \cdots$. Le même argument de Zariski-densité que celui utilisé dans la preuve de la proposition 18 montre alors le lemme.

□

Théorème 21.– *Si $f \neq \mathrm{Id}$ est élément de $\Gamma_{\mathscr{P}}$, alors $\mathscr{C}_{\Gamma_{\mathscr{P}}}(f) = f^{<k>}$.*

En particulier, ce centralisateur a une structure de k-espace vectoriel de dimension 1 *et c'est donc un groupe abélien.*

Preuve : Il est clair que $f^{<k>}$ est inclus dans $\mathscr{C}_{\Gamma_{\mathscr{P}}}(f)$. Réciproquement si $f(t) = t + \alpha_h t^h + \cdots$ avec $\alpha_h \neq 0$ et si $g \neq \mathrm{Id}$ commute avec f, alors d'après la proposition 15, il existe $\alpha \in k$ tel que $g(t) = t + \alpha t^h + \cdots$. Puisque $f^{\alpha/\alpha_h}(t) = t + \alpha t^h + \cdots$, la propriété d'unicité de la proposition 15 montre que $g = f^{\alpha/\alpha_h}$.

□

On s'intéresse maintenant aux centralisateurs des éléments de $\Gamma_{\mathscr{P}}$ dans le groupe Γ tout entier.

Lemme 22.– *Soient $f \in \Gamma_{\mathscr{P}}$ tel que $f(t) = t + \lambda t^{n+1} + \cdots$ avec $\lambda \neq 0$ et $g \in \Gamma$. Si $fg = gf$ alors $\gamma(g) \in \mu_n$.*

Preuve : Posons $g(t) = \gamma(g)t + b_2t^2 + b_3t^3 + \cdots$. Le terme de degré $n+1$ de $f \circ g(t)$ est égal à $b_{n+1} + \lambda\gamma(g)^{n+1}$ et celui de $g \circ f(t)$ vaut $b_{n+1} + \lambda\gamma(g)$. On en déduit que $\gamma(g) \in \mu_n$.

□

Corollaire 23.– *Si $f \neq \mathrm{Id}$ est un élément de $\Gamma_{\mathscr{P}}$ alors $\mathscr{T}_f$ est un groupe cyclique.*

Preuve : On pose $f(t) = t + \lambda t^{n+1} + \cdots$ avec $\lambda \neq 0$ et l'on considère un élément $u \in \mathscr{T}_f$. Comme u commute avec f, le lemme 22 assure que $\gamma(u) \in \mu_n$ et donc l'ordre de u divise l'entier n (conséquence du théorème 5.a.). Dans $\mathbb{Q}/\mathbb{Z}$, il n'y a qu'un nombre fini d'éléments d'ordre $\leq n$ et donc, $\mathscr{T}_f$ est fini et finalement cyclique, d'après le théorème 10.

□

Dans la suite de ce texte on appelera *longueur* de la traîne de l'automorphisme principal f (ou plus simplement *longueur* de f) l'entier $\ell(f) \geq 1$ tel que $\mathscr{T}_f \simeq \mathbb{Z}/\ell(f)$. Le lemme 22 assure que si $f(t) = t + \lambda t^{n+1} + \cdots$ alors $\ell(f)|n$. Le lien qui lie n et $\ell(f)$ peut être très précisément déterminé :

Proposition 24.– *Si $f \in \Gamma_{\mathscr{P}}$ désigne un automorphisme principal tel que $f(t) = t + \alpha t^{n+1} + \cdots$ avec $\alpha \neq 0$, alors $\ell(f) = \sharp\mu_n(k)$.*

Preuve : Pour établir cette proposition, commençons par établir un lemme sur la classe de conjugaison de f :

Lemme 25.– *Soient $f \in \Gamma_{\mathscr{P}}$ tel que $f(t) = t + \alpha t^{n+1} + \cdots$ avec $\alpha \neq 0$. Si $g \in \Gamma_{\mathscr{P}}$ est conjugué dans $\Gamma_{\mathscr{P}}$ à f alors $g(t) = t + \alpha t^{n+1} + \cdots$. Par ailleurs, il existe un unique $\beta \in k$ tel que f soit conjugué dans $\Gamma_{\mathscr{P}}$ à l'automorphisme $g \in \Gamma_{\mathscr{P}}$ vérifiant $g(t) = t + \alpha t^{n+1} + \beta t^{2n+1}$.*

Preuve : On pose $f(t) = t + a_{n+1}t^{n+1} + \cdots$ et l'on considère un élément $\sigma \in \Gamma_{\mathscr{P}}$. On pose $\sigma(t) = t + s_2t^2 + \cdots$ et

$$g(\sigma(t)) - \sigma(f(t)) = \lambda_2 t^2 + \cdots$$

Un petit calcul montre qu'il existe une collection de polynômes $P_{n+4}, P_{n+5}, \cdots$ telle que

- Pour $i = 2, \cdots, n+1$, $\lambda_i = 0$.
- $\lambda_{n+2} = (n-1)a_{n+1}s_2 + a_{n+2}$.

• Pour $i = 3, \cdots, n$, $\lambda_{n+i} = (n-i+1)a_{n+1}s_i + P_{n+i}(a_{n+1}, \cdots, a_{n+i}, s_2, \cdots, s_{i-1})$.

• $\lambda_{2n+1} = \beta - P_{2n+1}(a_{n+1}, \cdots, a_{2n+1}, s_2, \cdots, s_n)$.

• Pour $i \geq 1$, $\lambda_{2n+1+i} = -ia_{n+1}s_{n+1+i} + P_{2n+1+i}(a_{n+1}, \cdots, a_{2n+1+i}, s_2, \cdots, s_{n+i}, \beta)$.

On en déduit que l'équation $g(h(t)) - h(f(t)) = 0$ définit de manière unique les valeurs de $s_2, \cdots, s_n$ ainsi que celle de β et que, une fois choisie librement la valeur de l'élément s_{n+1}, cette équation définit de manière unique les valeurs de s_k pour $k \neq n+2$.

□

Remarques : a) La preuve montre que les éléments σ qui conjuguent f en g sont librement paramétrés par leur terme de degré $n+1$.

b) Le lemme montre que les classes de conjugaisons dans $\Gamma_{\mathscr{P}}$ des automorphismes f vérifiant $v(f(t)-t) = n+1$, sont bi-univoquement paramétrées par $k^* \times k$.

c) Puisque $\Gamma = \Gamma_{\mathscr{P}} \ltimes k^*$, un petit calcul montre que les classes de conjugaisons dans Γ des éléments $f \in \Gamma_{\mathscr{P}}$ vérifiant $v(f(t)-t) = n+1$, sont bi-univoquement paramétrées par $k^*/k^n \times k$.

Revenons à la preuve de la proposition. En conjugant le problème, on peut donc supposer que f vérifie $f(t) = t + \alpha t^{n+1} + \beta t^{2n+1}$. On voit alors que les éléments de la traîne de f sont exactement les automorphismes $t \longmapsto ut$ où $u \in \mu_n(k)$, ce qui achève la preuve.

□

Lemme 26.– *Si $f \neq \mathrm{Id}$ est élément de $\Gamma_{\mathscr{P}}$ alors, pour tout $\alpha \in k^*$, on a $\mathscr{T}_f = \mathscr{T}_{f^\alpha}$.*

Preuve : Si $u \in \mathscr{T}_f$, alors u commute avec toutes les puissances entières f^n. Par le même argument de Zariski-densité que dans la preuve de la proposition 18, on en déduit que u commute, pour tout $\beta \in k$, avec f^β. Si $u^n = \mathrm{Id}$, alors $(uf^{\alpha/n})^n = f^\alpha$ et donc $u \in \mathscr{T}_{f^\alpha}$. L'inclusion réciproque $\mathscr{T}_{f^\alpha} \subset \mathscr{T}_f$ s'obtient en utilisant l'inclusion que l'on vient d'établir pour l'élément f^α et l'exposant $1/\alpha$.

□

Corollaire 27.– *Si $f \neq \mathrm{Id}$ est un élément de $\Gamma_{\mathscr{P}}$ alors $\mathscr{C}_\Gamma(f) = \left\{uf^\alpha / \ \alpha \in k,\ u \in \mathscr{T}_f\right\}$.*

En particulier, ce centralisateur est un groupe abélien isomorphe à $k \times \mathbb{Z}/\ell(f)$ où $\ell(f)$ désigne la longueur de f.

Preuve : D'après ce qui précède, il est clair que l'ensemble $\{uf^\alpha / \ \alpha \in k,\ u \in \mathscr{T}_f\}$ est inclus dans le centralisateur de f. Réciproquement, si $g \neq \mathrm{Id}$ commute avec f, alors $\gamma(g) \in \mu_\infty(k)$ (lemme 22). Il existe donc un entier n tel que $g^n \in \Gamma_{\mathscr{P}}$, mais comme g^n commute avec f, il existe $\alpha \in k$ tel que $g^n = f^\alpha$. Puisque $\mathscr{T}_f = \mathscr{T}_{f^\alpha}$, il existe $u \in \mathscr{T}_f$ tel que $g = uf^{\alpha/n}$, ce qui assure l'inclusion réciproque.

Les deux sous-groupes du centralisateur de f, $f^{<k>}$ et $\mathscr{T}_f$ (isomorphes respectivement à k et $\mathbb{Z}/\ell(f)$), sont d'intersection réduite à {Id}, leurs éléments commutent deux à deux et ils engendrent le centralisateur. L'isomorphisme annoncé en découle.

□

Corollaire 28.– *Si $f \in \Gamma_{\mathscr{P}}$ désigne un élément non égal à l'identité alors*

$$\mathscr{T}_f = \{u \text{ de torsion} / \ uf = fu\}$$

(et il y a donc un nombre fini d'éléments de torsion qui commutent avec f).

Corollaire 29.– *Le groupe $\mathrm{Gal}_{\mathscr{P}}(k((t))/k)$ est un groupe de type CA.*

3.2.2.– Centralisateurs des éléments $f \notin \mathrm{Gal}_{\mathscr{P}}(k((t))/k)$.

Les résultats précédents permettent finalement de décrire $\mathscr{C}_\Gamma(f)$ lorsque f n'est pas une racine de l'identité mais que $\gamma(f) \in \mu_\infty(k)$:

Théorème 30.– *Si $f \in \Gamma$ désigne un élément qui n'est pas une racine n-ième de l'identité et tel que $\gamma(f) \in \mu_n$, alors $\mathscr{C}_\Gamma(f) = \left\{u(f^n)^\alpha / \ \alpha \in k,\ u \in \mathscr{T}_{f^n}\right\}$.*

En particulier, ce centralisateur est un groupe abélien isomorphe à $k \times \mathbb{Z}/\ell(f^n)$ où $\ell(f^n)$ désigne la longueur de f^n.

Preuve : L'hypothèse $\gamma(f) \in \mu_n$ implique que $f^n \in \Gamma_{\mathscr{P}}$ et, comme f est une racine n-ième de f^n, il existe alors une racine n-ième de l'identité v tel que $f = v(f^n)^{1/n}$ (théorème 12). Ceci implique que l'on a l'inclusion $\left\{u(f^n)^\alpha / \ \alpha \in k,\ u \in \mathscr{T}_{f^n}\right\} \subset \mathscr{C}_\Gamma(f)$.

Réciproquement, si $g \in \Gamma$ commute avec f alors g^n commute avec f^n et donc, il existe $\alpha \in k$ et une racine m-ième de l'identité $v \in \mathscr{T}_{f^n}$ tel que $g^n = v(f^n)^\alpha$ (corollaire 27). On a alors $g^{nm} \in \Gamma_{\mathscr{P}}$ et g^{nm} commute avec f^n et donc, il existe $w \in \mathscr{T}_{f^n}$ tel que $g = w(f^n)^{\alpha/n}$. Ceci montre l'inclusion réciproque.

□

Remarque : Dans cette situation, on a l'inclusion $\mathscr{T}_f \subset \mathscr{T}_{f^n}$ mais l'inclusion réciproque n'est pas toujours vraie. Ceci montre en particulier, qu'au contraire du cas des automorphismes principaux, $\mathscr{T}_f$ peut très bien être un sous-ensemble strict de l'ensemble $\{u$ de torsion$/\ uf = fu\}$.

Pour illustrer cette remarque, prenons g tel que $g(t) = t + t^3$. La traîne de g est isomorphe à $\mathbb{Z}/2$ en vertu du lemme 22 et du corollaire 23 et du fait que l'involution $u : t \longmapsto -t$ est visiblement dans cette traîne. Si l'on pose $f = ug^{1/2}$, alors u commute avec f, mais n'est pas dans la traîne de f car sinon f possèderait une racine carrée h qui vérifierait alors $\gamma(h) = \pm i$. Ainsi, l'élément $h^{-1}g^{1/4}$ serait dans la traîne de g et serait d'ordre 4 (puisque $\gamma(h^{-1}g^{1/4}) = i$) ce qui est impossible.

Nous terminons ce paragraphe en étudiant les centralisateurs des éléments $f \in \Gamma$ tels que $\gamma(f) \notin \mu_\infty(k)$. Dans cette situation on utilise le lemme suivant :

Lemme 31.– *Si $f, g \in \mathrm{Gal}(k((t))/k)$ sont deux éléments tels que $\gamma(f), \gamma(g) \notin \mu_\infty(k)$ alors f et g sont conjugués si et seulement si $\gamma(f) = \gamma(g)$. Dans cette situation il existe exactement un élément $u \in \mathrm{Gal}(k((t))/k)_{\mathscr{P}}$ tel que $ufu^{-1} = g$.*

Preuve : La condition $\gamma(f) = \gamma(g)$ est évidemment nécessaire. Posons $f(t) = \alpha t + f_2 t^2 + \cdots$ et $u(t) = t + u_2 t + \cdots$. Une récurrence montre que

$$f(u(t)) - u(\alpha t) = (u_2(\alpha - \alpha^2) + f_2)t^2 + \cdots + (u_n(\alpha - \alpha^n) + R_n(f_1, \cdots, f_n, u_2, \cdots, u_{n-1}))t^n + \cdots$$

où $R_n \in K(X_1, \cdots, X_n, Y_2, \cdots, Y_{n-1})$ pour $n \geq 3$. Puisque $\alpha \notin \mu_\infty(k)$, on en déduit qu'il existe une unique suite $(u_n)_{n\geq 2}$ tel que $f(u(t)) - u(\alpha t) = 0$, c'est-à-dire un unique élément $u \in \mathrm{Gal}(k((t))/k)_{\mathscr{P}}$ tel que f soit conjugué par u avec $t \longmapsto \alpha t$.

En appliquant le même résultat à g on en déduit finalement le lemme.

□

Théorème 32.– *Si $f \in \Gamma$ désigne un élément tel que $\gamma(f) \notin \mu_\infty(k)$ alors, pour tout $\alpha \in k^*$, il existe un et un seul élément $g \in \Gamma$ commutant avec f tel que $g(t) = \alpha t + \cdots$.*

En conséquence de quoi, le centralisateur $\mathscr{C}_\Gamma(f)$ de f dans Γ est un groupe abélien isomorphe au groupe multiplicatif k^*.

Preuve : En conjugant f par un automorphisme on peut, grâce au lemme 31, se ramener au cas où $f(t) = \alpha t$ avec $\alpha \notin \mu_\infty(k)$. On voit alors que $\mathscr{C}_\Gamma(f) = \{g \in \Gamma / \ g(t) = \gamma(g)t\}$ et le théorème découle alors du fait que le morphisme γ reste invariant par l'action de conjugaison dans Γ.

La restriction à $\mathscr{C}_\Gamma(f)$ de l'épimorphisme $g \longmapsto \gamma(g)$ est bijective d'après ce qui précède, l'isomorphisme annoncé en découle.

□

Remarque : L'argument de conjugaison introduit dans cette preuve montre qu'un élément $g(t) = \alpha t + \cdots$ commutant avec f est de torsion si et seulement si α est une racine de l'unité. En utilisant le théorème 12, on en déduit dans cette situation que, le fait que $\mathscr{T}_f$ puisse être un sous-ensemble strict de l'ensemble $\{u \text{ de torsion}/\ uf = fu\}$ est directement relié à l'existence d'entiers n tels que $\gamma(f) \notin k^n$. Ainsi, par exemple quand k est algébriquement clos, on a l'égalité $\mathscr{T}_f = \{u \text{ de torsion}/\ uf = fu\}$, comme dans le cas des automorphismes principaux.

En conclusion de ce §3., nous constatons qu'à l'exception des éléments de torsion, tous les autres éléments de $\mathrm{Gal}(k((t))/k)$ ont des centralisateurs abéliens.

3.3.– Conséquences.

Théorème 33.– *Si Γ_0 désigne un sous-groupe non abélien de $\mathrm{Gal}(k((t))/k)$, alors son centre $Z(\Gamma_0)$ est un groupe cyclique.*

Preuve : En premier lieu, constatons que $Z(\Gamma_0)$ est nécessairement un groupe de torsion. En effet, si ce n'était pas le cas, il existerait $f \in Z(\Gamma_0)$ d'ordre infini, mais comme alors $\Gamma_0 \subset \mathscr{C}_{\mathrm{Gal}(k((t))/k)}(f)$ et que ce dernier groupe est abélien d'après la partie §3.2., on en déduirait que Γ_0 est abélien, ce qui est contraire aux hypothèses.

Maintenant, remarquons que le groupe Γ_0 ne peut pas être de torsion en vertu du corollaire 7 et il existe donc un élément $f \in \Gamma_0$ d'ordre infini.

Supposons pour commencer que $\gamma(f) \in \mu_\infty(k)$. Puisque $Z(\Gamma_0)$ est de torsion, le théorème 30 assure que $Z(\Gamma_0) \subset \mathscr{T}_{f^n}$ où n est tel que $\gamma(f) \in \mu_n$ et le corollaire 23 montre que ce dernier groupe est cyclique.

Supposons maintenant que $\gamma(f) \notin \mu_\infty(k)$ et l'on conjugue Γ_0 de sorte que $f(t) = \alpha t$ (ce qui est possible d'après le lemme 31). Puisque le centralisateur de f dans $\mathrm{Gal}(k((t))/k)$ est constitué des automorphisme z tel que $z(t) = \beta t$ avec $\beta \in k^*$, on en déduit que les éléments de $Z(\Gamma_0)$ sont de la forme $r_n = t \longmapsto \xi_n t$ où n parcourt une certaine partie $A \subset \mathbb{N}^*$ et pour tout $n \in A$, ξ_n est une racine primitive n-ième de l'unité. Si $g \in \Gamma_0$ est tel que $g(t) = a_1 t + a_2 t^2 + \cdots$, alors comme remarqué au début du §3.2., puisque g commute avec r_n on a $a_k = 0$ pour tout indice $k \not\equiv 1 \mod (n)$.

Si $Z(\Gamma_0)$ était infini alors A le serait aussi et donc on aurait $g(t) = a_1 t$. Il s'ensuivrait que g commuterait avec f et donc que Γ_0 serait abélien, ce qui est exclu. Ainsi, $Z(\Gamma_0)$ est fini et donc cyclique d'après le théorème 10.

□

Ce résultat montre, par exemple, que le groupe $\mathbb{Z} \rtimes \mathbb{Z}$ (pour l'action non triviale) n'est isomorphe à aucun sous-groupe de $\mathrm{Gal}(k((t))/k)$. Ce théorème 33 suggère d'étudier un peu plus généralement la propriété qu'il comporte.

Définition 34.– *On dit d'un groupe G qu'il possède la propriété (Z_t) (resp. (Z_c), resp. (Z_f)) si, pour tout sous-groupe $G_0 \leq G$ non abélien de G, le centre $Z(G_0)$ de G_0 est trivial (resp. cyclique, resp. fini).*

Il est clair que si G a une des propriétés (Z) alors tous ses sous-groupes ont la même propriété. C'est la seule opération élémentaire sur les groupes que les propriétés (Z) préservent : les propriétés (Z) ne sont stables

• ni par passage au quotient, car les groupes libres ont la propriété (Z_t),

• ni par extension comme le suggère la suite exacte $1 \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Z} \rtimes \mathbb{Z} \longrightarrow \mathbb{Z} \longrightarrow 1$,

• ni par produit cartésien puisque, si A désigne un groupe non abélien ayant (Z_t) et possédant un sous-groupe abélien infini, alors $A \times A$ n'a aucune propriété (Z).

Exemples : • Les groupes finis ont la propriété (Z_f).

• Les groupes abéliens ont la propriété (Z_t). Plus généralement, les groupes de type CA ont la propriété (Z_t), en particulier le groupe $\mathrm{Gal}_{\mathscr{P}}(k((t))/k)$.

• Les groupes libres ont la propriété (Z_t) (c'est une conséquence du théorème de Nielsen-Schreier).

• Les amalgames ne préservent pas forcément les propriétés (Z). Par exemple, $\mathbb{Z} \underset{2\mathbb{Z}}{*} \mathbb{Z}$ est un groupe non abélien avec un centre infini, alors que chaque facteur de l'amalgame possède la propriété (Z_t).

On a toutefois la situation assez générale suivante :

Proposition 35.– *Soit A et B deux groupes et C un sous-groupe commun tel que $C \subset Z(A)$ et $C \subset Z(B)$ (en particulier C est abélien). Si C est fini (resp. cyclique, resp. trivial) alors les propriétés suivantes*

i) les groupes A et B possèdent tout deux la propriété (Z_f) (resp. (Z_c), resp. (Z_t)),

ii) l'amalgame $A \underset{C}{*} B$ possède la propriété (Z_f) (resp. (Z_c), resp. (Z_t)),

sont équivalentes.

En particulier, si A et B désignent deux groupes alors le produit libre $A * B$ possède la propriété (Z_t) (resp. (Z_c), resp. (Z_f)) si et seulement si les groupes A et B la possèdent.

Preuve : Puisque A et B s'injectent dans $A \underset{C}{*} B$, l'implication $ii) \Longrightarrow i)$ est immédiate.

La preuve de l'implication $i) \Longrightarrow ii)$ repose sur le théorème de commutativité dans les amalgames (voir [MKS]) qui affirme que, si $x, y \in A \underset{C}{*} B$ sont deux éléments non triviaux d'un amalgame tels que $xy = yx$ alors :

1/ Si l'un des deux x ou y est dans un conjugué d'un des facteurs A ou B, alors l'autre est aussi dans ce conjugué.

2/ Si ni x ni y ne sont dans un conjugué d'un des facteurs A ou B, alors il existe $g, w \in A \underset{C}{*} B$, $h, h' \in C$ tel que $x = ghg^{-1}w^i$ et $y = gh'g^{-1}w^j$ pour certains entiers i et j et tels que ghg^{-1}, $gh'g^{-1}$ et w commutent deux à deux.

Une fois rappelée cette propriété, considérons $G_0 \subset A \underset{C}{*} B$ un sous-groupe. Si $Z(G_0) \subset C$, alors la propriété est claire. Supposons maintenant qu'il existe $f \in Z(G_0) - C$ et considérons deux cas :

a) f appartient à un conjugué d'un des facteurs A ou B (disons A). Alors en conjugant on peut donc supposer $f \in A$. D'après le 1/ on a $G_0 \subset A$, ce qui permet de conclure.

b) f n'appartient à aucun conjugué des facteurs A et B. Quitte à conjuguer le problème, on peut supposer que f est cycliquement réduit (voir [Ser]) et que sa longueur est ≥ 2. Quitte à inverser f, on peut donc écrire $f = ha_1b_1 \cdots a_nb_n$ avec $h \in C$, $a_1, \cdots, a_n \in A/C$ et $b_1, \cdots, b_n \in B/C$ (on a identifié ici l'ensemble A/C, resp. B/C, à une classe de représentants donnée dans A, resp. B).

Si $w \in A \underset{C}{*} B$ est tel que $w^i = f$ pour un certain entier $i \geq 1$, alors , comme la première lettre de w est nécessairement dans A/C et que sa dernière est nécessairement dans B/C, on voit que $w = h_w a_1 b_1 \cdots a_k b_k$ avec $n = ki$ et $h_w^i = h$.

Considérons alors $w' = h_{w'} a_1 b_1 \cdots a_{k'} b_{k'}$ un autre élément tel que avec $w'^{i'} = f$ pour un entier $i' \geq 1$ (vérifiant donc $n = k'i'$). On a alors $h_w^i = h_{w'}^{i'} = h$ et $(a_1 b_1 \cdots a_k b_k)^i = (a_1 b_1 \cdots a_{k'} b_{k'})^{i'} = a_1 b_1 \cdots a_n b_n$. Si l'on considère $d = \text{pgcd}(k, k')$, quitte à permuter le rôle de k et k', on peut supposer l'existence de $u, v \geq 1$ tels que $uk - vk' = d$. On a alors $(a_1 b_1 \cdots a_k b_k)^{iuv} = (a_1 b_1 \cdots a_{k'} b_{k'})^{uvi'}$ et, en écrivant

$$\begin{aligned} ((a_1 b_1 \cdots a_k b_k)^u)^{iv} &= (a_1 b_1 \cdots a_k b_k)^{u-1} a_1 b_1 \cdots a_k b_k \cdot \cdots \cdot a_1 b_1 \cdots a_k b_k \\ = ((a_1 b_1 \cdots a_{k'} b_{k'})^v)^{i'u} &= (a_1 b_1 \cdots a_{k'} b_{k'})^v a_1 b_1 \cdots a_d b_d \cdot \cdots \cdot a_1 b_1 \cdots a_{k'} b_{k'} \end{aligned}$$

on voit que $a_k b_k = a_d b_d$, $a_{k-1} b_{k-1} = a_{d-1} b_{d-1}$ etc. puis que $a_{k'} b_{k'} = a_d b_d$, $a_{k'-1} b_{k'-1} = a_{d-1} b_{d-1}$ etc et donc que $a_1 b_1 \cdots a_{k'} b_{k'} = (a_1 b_1 \cdots a_{k'-d} b_{k'-d})(a_1 \cdots a_d)$. En réappliquant l'argument k'/d fois, on voit finalement que $(a_1 b_1 \cdots a_{k'} b_{k'}) = (a_1 \cdots a_d)^{k'/d}$, puis que $(a_1 b_1 \cdots a_k b_{k'}) = (a_1 \cdots a_d)^{k/d}$.

Ainsi, si l'on considère un élément $w_0 = a_1 \cdots a_r$ avec r minimal vérifiant que $w_0^{i_0} = a_1 b_1 \cdots a_k b_k$ pour un certain entier $i_0 \geq 1$, alors pour tous $w \in G$ et $i \geq 1$ tels que $w^i = f$, on a $i | i_0$ et $w = h_w w_0^{i_0/i}$.

En utilisant alors la propriété 2/ rappelée plus haut, on en déduit que $G_0 \subset \{h w_0^n / \ h \in C, \ n \in \mathbb{Z}\} \simeq C \times \mathbb{Z}$ et donc que le groupe G_0 est abélien.

□

En particulier, le groupe diédral infini $D_\infty \simeq \mathbb{Z}/2 * \mathbb{Z}/2$ a la propriété (Z_c). On verra plus loin dans cet article que c'est en fait un sous-groupe de $\text{Gal}(k((t))/k)$.

• Un autre exemple de groupe ayant la propriété (Z_c) est le groupe $\text{PGL}_2(k)$ où k est un corps infini. Ce fait est intéressant dans la mesure où $\text{PGL}_2(k)$ est le groupe de Galois de l'extension $k(t)/k$ et que le parallèle avec l'extension $k((t))/k$ est prégnant.

Pour voir que $\text{PGL}_2(k)$ a la propriété (Z_c), on procède comme suit : on suppose que k est algébriquement clos (ce qui n'est pas restrictif puisque les propriétés (Z) sont stables par sous-groupes) et, pour $M \in \text{GL}_2(k)$, on note $\overline{M}$ la classe de M dans $\text{PGL}_2(k)$. Un petit calcul sans difficulté montre que :

1/ Si M est diagonalisable, alors en conjugant le problème on peut prendre $M = \left(\begin{smallmatrix} 1 & 0 \\ 0 & \lambda \end{smallmatrix}\right)$ et l'on a, si $\lambda \neq -1$,

$$\mathscr{C}_{\text{PGL}_2(k)}(\overline{M}) = \left\{ \overline{\left(\begin{smallmatrix} 1 & 0 \\ 0 & \mu \end{smallmatrix}\right)} / \ \mu \in k^* \right\} \simeq k^*$$

et si, $\lambda = -1$,

$$\mathscr{C}_{\text{PGL}_2(k)}(\overline{M}) = \left\{ \overline{\left(\begin{smallmatrix} 1 & 0 \\ 0 & \mu \end{smallmatrix}\right)} / \ \mu \in k^* \right\} \bigcup \left\{ \overline{\left(\begin{smallmatrix} 0 & \mu \\ 1 & 0 \end{smallmatrix}\right)} / \ \mu \in k^* \right\} = \left\langle \overline{\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)}; \ \overline{\left(\begin{smallmatrix} 1 & 0 \\ 0 & \mu \end{smallmatrix}\right)} / \ \mu \in k^* \right\rangle \simeq k^* \rtimes \mathbb{Z}/2$$

2/ Si M n'est pas diagonalisable, alors en conjugant le problème on peut prendre $M = \left(\begin{smallmatrix} 1 & \lambda \\ 0 & 1 \end{smallmatrix}\right)$ et l'on a

$$\mathscr{C}_{\text{PGL}_2(k)}(\overline{M}) = \left\{ \overline{\left(\begin{smallmatrix} 1 & \mu \\ 0 & 1 \end{smallmatrix}\right)} / \ \mu \in k \right\} \simeq k$$

Si G_0 désigne un sous-groupe de $\text{PGL}_2(k)$ et que $Z(G_0)$ compte au moins trois éléments, alors il existe $\overline{M} \in Z(G_0)$ telle que $\overline{M} \neq \overline{\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)}$ et donc, en vertu de ce qui précède, on a

$$G_0 \subset \mathscr{C}_{\text{PGL}_2(k)}(\overline{M}) \simeq k^* \text{ ou } k$$

et G_0 est alors abélien. Ainsi, si G_0 n'est pas abélien, on a $Z(G_0) \simeq 1$ ou $\mathbb{Z}/2$. Le cas $Z(G_0) \simeq \mathbb{Z}/2$ correspond alors à des conjugués de sous-groupes du groupe

$$\Omega = \left\langle \overline{\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)}; \ \overline{\left(\begin{smallmatrix} 1 & 0 \\ 0 & \mu \end{smallmatrix}\right)} / \ \mu \in k^* \right\rangle$$

le groupe Ω vérifiant lui-même $Z(\Omega) \simeq \mathbb{Z}/2$ (ce qui exclu que $\mathrm{PGL}_2(k)$ ait la propriété (Z_t).)

Remarque : Il est à noté que $\mathrm{PGL}_n(k)$ n'a aucune des propriétés (Z) dès que $n \geq 3$. En effet, si $n \geq 3$, alors le groupe $\mathrm{GL}_2(k)$ s'injecte naturellement dans $\mathrm{PGL}_n(k)$ (par matrices par blocs) et le centre de $\mathrm{GL}_2(k)$ est infini.

De la même manière, $\mathrm{PSL}_n(k)$ n'a aucune des propriétés (Z) pour $n \geq 3$. En effet, $\mathrm{GL}_2(k)$ s'injecte naturellement dans $\mathrm{SL}_n(k)$ et son centre est infini, et comme $\mathrm{PSL}_n(k) \simeq \mathrm{SL}_n(k)/\mu_n(k)$ on en déduit que l'image de $\mathrm{GL}_2(k)$ dans $\mathrm{PSL}_n(k)$ est un groupe non abélien de centre infini (isomorphe à $k^*/\mu_n(k) \simeq k^{*n}$). Le groupe $\mathrm{PSL}_2(k)$, en tant que sous-groupe de $\mathrm{PGL}_2(k)$, a bien sûr la propriété (Z_c).

Finissons ce paragraphe sur une autre propriété. On considère un sous-groupe Γ_0 de $\mathrm{Gal}(k((t))/k)$ possédant un sous-groupe normal monogène $\Delta =< f_0 >$. Pour tout $g \in \Gamma_0$, il existe $n \geq 1$ tel que $gf_0g^{-1} = f_0^n$ et, en intérant la conjugaison, on voit qu'il existe un entier $m \geq 1$ tel que $g^m f_0 g^{-m} = f_0$. Ainsi, on a $f_0, g \in \mathscr{C}_{\mathrm{Gal}(k((t))/k)}(g^m)$, de sorte que, si l'on suppose que g est d'ordre infini, on a $f_0 g = g f_0$ puisque g^m étant lui aussi d'ordre infini, son centralisateur est abélien d'après ce qui précède.

Corollaire 36.– *Soit Γ_0 un sous-groupe de $\mathrm{Gal}(k((t))/k)$ possédant un sous-groupe libre de rang 1 distingué $\Delta =< f_0 >$. Si Γ_0 est engendré par des éléments d'ordre infini, alors Γ_0 est abélien.*

Preuve : Soit $\{g_i\}_i$ une famille génératrice de Γ_0 composée d'éléments d'ordre infini. D'après ce qui précède, f_0 commute avec tous les g_i et donc $\Delta \subset Z(\Gamma_0)$, mais comme Δ est infini, on en déduit bien que Γ_0 est abélien.

□

Il n'est pas possible de retirer les hypothèses génératives dans ce corollaire comme le montre l'exemple du groupe diédral infini $D_\infty \simeq \mathbb{Z} \rtimes \mathbb{Z}/2 \simeq \mathbb{Z}/2 * \mathbb{Z}/2$. Par ailleurs , le fait que D_∞ soit engendré par sa torsion est alors conséquence de cet autre corollaire :

Corollaire 37.– *Soit Γ_0 un sous-groupe de $\mathrm{Gal}(k((t))/k)$ possédant un sous-groupe libre de rang 1 distingué $\Delta =< f_0 >$. Si Γ_0 n'est pas abélien, alors Γ_0 est engendré par sa torsion.*

Preuve : Supposons que Γ_0 ne soit pas engendré par sa torsion. Pour tout élément de torsion $u \in \Gamma_0$, il existe alors un élément d'ordre infini g_u tel que ug_u soit d'ordre infini. On a alors, d'après ce qui précède, $f_0 g_u = g_u f_0$ et $f_0 u g_u = u g_u f_0$ et donc $u f_0 = f_0 u$. Ainsi, Δ est central et donc Γ_0 est abélien.

□

4.– Amalgames de torsion.

Le théorème 33 et la proposition 35 nous amènent à considérer la question suivante : si σ, ρ sont des éléments de $\mathrm{Gal}(k((t))/k)$, le sous-groupe $G =< \sigma, \rho >$ est-il une somme amalgamée ? Remarquons dans un premier temps que, si σ et ρ sont deux éléments distincts d'ordre infini, alors le sous-groupe $< \sigma, \rho >$ ne peut pas être une somme amalgamée au dessus d'un sous-groupe non trivial. En effet, s'il existe $n, m \in \mathbb{Z}^*$ tels que $\sigma^n = \rho^m = \tau$, alors $\sigma, \rho \in \mathscr{C}_{\mathrm{Gal}(k((t))/k)}(\tau)$. Par conséquent, σ et ρ commutent, ce qui montre que $< \sigma, \rho >$ n'est pas un amalgame.

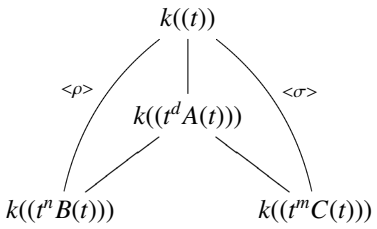
On va s'intéresser dans ce paragraphe au cas où σ et ρ sont des éléments de torsion :

Problème.– *Pour quelles paires $\{\sigma, \rho\} \subset \mathrm{Gal}(k((t))/k)$ d'éléments de torsion a-t-on*

$$< \sigma, \rho > \simeq \mathbb{Z}/n\mathbb{Z} \underset{\mathbb{Z}/d\mathbb{Z}}{*} \mathbb{Z}/m\mathbb{Z}$$

où $n = o(\sigma)$, $m = o(\rho)$ et $d = o(<\sigma> \cap <\rho>)$?

Il existe un moyen assez naturel de faire agir le sous-groupe $G =<\sigma, \rho>$ sur un graphe. En effet, posons $n = o(\sigma)$, $m = o(\rho)$ et $d = o(<\sigma> \cap <\rho>)$ et considérons la tour d'extensions



avec A, B, C des unités principales. Posons $H =<\sigma> \cap <\rho>$, le sous-groupe laissant invariant le corps $k((t^d A(t)))$. Pour $\overline{\omega} \in G/<\rho>$, l'image de $t^n B(t)$ par un relevé de $\overline{\omega}$ dans G/H ne dépend pas du relevé choisi. On pose alors

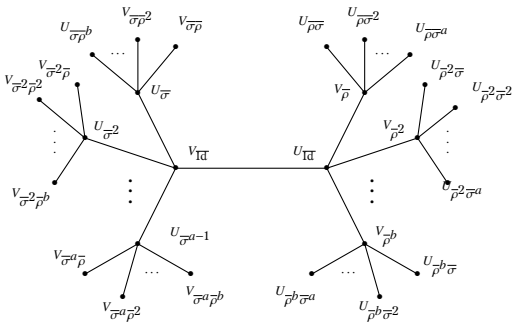
$$U_{\overline{\omega}}(t) = \omega(t^n B(t))$$

où ω est un relevé quelconque de $\overline{\omega}$ dans G/H. De même, pour $\overline{\tau} \in G/<\sigma>$, on pose

$$V_{\overline{\tau}}(t) = \tau(t^m C(t))$$

où τ est un relevé quelconque de $\overline{\tau}$ dans G/H.

On définit alors un graphe Γ dont les sommets sont les $U_{\overline{\omega}}$ et les $V_{\overline{\tau}}$ et les arêtes sont l'arête $[U_{\overline{\mathrm{Id}}}, V_{\overline{\mathrm{Id}}}]$ et les arêtes $[U_{\overline{\omega}}, V_{\overline{\tau}}]$ lorsque $\omega = \tau\sigma^i$ ou $\tau = \omega\rho^i$ pour un certain entier i.

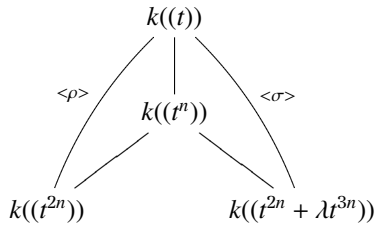


(On a posé $a = n/d - 1$ et $b = m/d - 1$).

Le groupe G agit par multiplication à gauche sur le graphe Γ : $g.U_{\overline{\omega}} = U_{\overline{g\omega}}$ et $g.V_{\overline{\tau}} = V_{\overline{g\tau}}$. Cette action est sans inversion et a pour domaine fondamental le segment $[U_{\overline{\mathrm{Id}}}, V_{\overline{\mathrm{Id}}}]$. La théorie de Serre-Bass montre que si Γ est un arbre, alors comme les stabilisateurs de $U_{\overline{\mathrm{Id}}}, V_{\overline{\mathrm{Id}}}$ et $[U_{\overline{\mathrm{Id}}}, V_{\overline{\mathrm{Id}}}]$ sont respectivement $<\rho> \simeq \mathbb{Z}/m\mathbb{Z}$, $<\sigma> \simeq \mathbb{Z}/n\mathbb{Z}$ et $H \simeq \mathbb{Z}/d\mathbb{Z}$, on a $G \simeq \mathbb{Z}/n\mathbb{Z} \underset{\mathbb{Z}/d\mathbb{Z}}{*} \mathbb{Z}/m\mathbb{Z}$.

La condition combinatoire pour que Γ soit un arbre est que les $U_{\overline{\omega}}$ et $V_{\overline{\tau}}$ soient tous distincts deux à deux, ce qui équivaut encore à dire qu'ils sont tous distincts de $U_{\overline{\mathrm{Id}}}$ et $V_{\overline{\mathrm{Id}}}$. Notons que cette dernière condition équivaut encore à dire qu'il n'y a pas, dans G, de mot formel $\sigma^{j_1}\rho^{i_2}\sigma^{j_2}\cdots\rho^{i_h}\sigma^{j_h}$ ou $\rho^{i_2}\sigma^{j_2}\cdots\rho^{i_h}\sigma^{j_h}$ avec $h \geq 1$, $i_2, \cdots, i_h \in \{1, \cdots, \frac{m}{d} - 1\}$ et $j_1, \cdots, j_h \in \{1, \cdots, \frac{n}{d} - 1\}$ qui vaille l'identité.

Donnons un exemple explicite : on considère $n \geq 1$, $\lambda \in k^*$ et la tour d'extensions



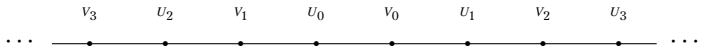
avec $\rho(t) = \xi_{2n}t$ et $\sigma(t) = \sqrt[n]{\dfrac{-(1+\lambda t^n) + \sqrt{1-2\lambda t^n - 3\lambda^2 t^{2n}}}{2\lambda}}$. On considère les suites de séries $(U_n)_n$ et $(V_n)_n$ définies par

$$\begin{array}{ll} U_0(t) = t^{2n} & V_0(t) = t^{2n} + \lambda t^{3n} \\ U_{2h}(t) = (\rho\sigma)^h(U_0(t)) & V_{2h}(t) = (\sigma\rho)^h(V_0(t)) \\ U_{2h+1}(t) = \sigma(U_{2h}(t)) & V_{2h+1}(t) = \rho(V_{2h}(t)) \end{array}$$

Une récurrence montre que, pour tout $h \geq 0$, on a

$$\begin{array}{l} U_{2h}(t) = t^{2n} - 2n\lambda t^{3n} + \cdots \\ U_{2h+1}(t) = t^{2n} - (2n-1)\lambda t^{3n} + \cdots \\ V_{2h}(t) = t^{2n} + (2n+1)\lambda t^{3n} + \cdots \\ V_{2h+1}(t) = t^{2n} - (2n+1)\lambda t^{3n} + \cdots \end{array}$$

En particulier, pour tout entier $n \geq 1$ on a $U_n(t) \neq U_0(t), V_0(t)$ et $V_n(t) \neq U_0(t), V_0(t)$. Ainsi, les U_n et V_n forment une famille de séries distinctes deux à deux. En conséquence de quoi, le groupe $G =< \sigma, \rho >$ agit sans inversion sur l'arbre



avec pour domaine fondamental $[U_0, V_0]$ et donc $G \simeq \mathbb{Z}/2n\mathbb{Z} \underset{\mathbb{Z}/n\mathbb{Z}}{*} \mathbb{Z}/2n\mathbb{Z}$. Cet exemple va être généralisé au paragraphe suivant.

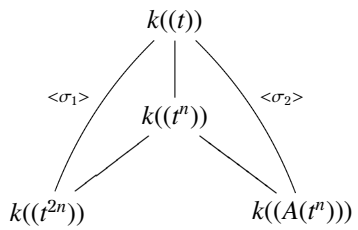
Nous allons maintenant nous intéresser à deux situations pour lesquelles la question de l'amalgamation admet, respectivement, une réponse positive et négative.

4.1.– Cas des sous-groupes communs d'indice 2.

Théorème 38.– *Si $G_1 =< \sigma_1 >$ et $G_2 =< \sigma_2 >$ sont deux sous-groupes finis de* $\mathrm{Gal}(k((t))/k)$ *tels que $G_0 = G_1 \cap G_2$ soit d'indice 2 dans G_1 et G_2, alors*

$$< \sigma_1, \sigma_2 > \simeq G_1 \underset{G_0}{*} G_2$$

Preuve : Soit $n = o(G_0)$, on a donc $o(\sigma_1) = o(\sigma_2) = 2n$. Quitte à conjuguer le problème par un élément de $\mathrm{Gal}(k((t))/k)$, on peut se ramener à la situation suivante



où A est une série de valuation 2 qui n'est pas élément de $k((t^{2n}))$.

Si l'on pose $\sigma_1(t) = \xi_{2n}t$, quitte à considérer une puissance de σ_2, on peut supposer que $\sigma_2(t) = \xi_{2n}^{-1}t + \cdots$.

S'il existait un entier $h \geq 1$ tel que $(\sigma_1\sigma_2)^h = \mathrm{Id}$ (resp. $(\sigma_2\sigma_1)^h = \mathrm{Id}$), alors $\sigma_1\sigma_2$ (resp. $\sigma_2\sigma_1$) serait de torsion, mais comme $\sigma_1\sigma_2(t) = t + \cdots$ (resp. $\sigma_2\sigma_1(t) = t + \cdots$, on déduirait que $o(\sigma_1\sigma_2) = 1$, ce qui impliquerait finalement que $G_1 = G_2$.

Soit $h \geq 1$. On a $\gamma(\sigma_2(\sigma_1\sigma_2)^h = \xi_{2n}^{-1}$ et $\gamma(\sigma_1(\sigma_2\sigma_1)^h) = \xi_{2n}$, égalités qui montrent $\sigma_2(\sigma_1\sigma_2)^h \neq \mathrm{Id}$ et $\sigma_1(\sigma_2\sigma_1)^h \neq \mathrm{Id}$.

□

Remarque : Le théorème ci-dessus décrit en fait exhaustivement la situation où le graphe introduit dans ce paragraphe est un arbre droit infini.

Le théorème 38 s'applique au cas des involutions :

Corollaire 39.– *Si k est de caractéristique 0 et si $\sigma, \tau \in \mathrm{Gal}(k((t))/k)$ désignent deux involutions distinctes alors $< \sigma, \tau > \simeq \mathbb{Z}/2\mathbb{Z} * \mathbb{Z}/2\mathbb{Z}$.*

Remarques : a) Le produit libre $\mathbb{Z}/2\mathbb{Z} * \mathbb{Z}/2\mathbb{Z}$ est en fait isomorphe au groupe diédral infini D_∞. En effet, notons σ et μ des générateurs de chaque facteur $\mathbb{Z}/2\mathbb{Z}$ dans le produit libre $\mathbb{Z}/2\mathbb{Z} * \mathbb{Z}/2\mathbb{Z}$, l'élément $f = \sigma\mu$ est alors d'ordre infini. Mais comme $(\sigma f)^2 = \mu^2 = 1$, on en déduit que $\sigma f \sigma = f^{-1}$ et donc $< \sigma, f > \simeq D_\infty$. Puisque $\mu = \sigma f$, on voit finalement que $< \sigma, \mu > = < \sigma, f >$ et donc que $\mathbb{Z}/2\mathbb{Z} * \mathbb{Z}/2\mathbb{Z} \simeq D_\infty$.

b) On peut déduire de la remarque précédente quelque chose sur la structure de l'amalgame apparaissant dans le théorème 38. En effet, notons σ et μ des représentants du générateur de $\mathbb{Z}/n\mathbb{Z}/\mathbb{Z}/2n\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z}$ dans chacun des facteurs $\mathbb{Z}/2n\mathbb{Z}$. Il existe un épimorphisme tout à fait naturel

$$\mathbb{Z}/2n\mathbb{Z} \underset{\mathbb{Z}/n\mathbb{Z}}{*} \mathbb{Z}/2n\mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z} * \mathbb{Z}/2\mathbb{Z} \longrightarrow 1$$

Ce dernier est donnée par le fait que tout élément de $\mathbb{Z}/2n\mathbb{Z} \underset{\mathbb{Z}/n\mathbb{Z}}{*} \mathbb{Z}/2n\mathbb{Z}$ s'écrit de manière unique sous la forme $a.\sigma^{\lambda_1}.\mu.\sigma.\cdots.\sigma.\mu^{\lambda_2}$ avec $\lambda_1, \lambda_2 = 0, 1$ et $a \in \mathbb{Z}/n\mathbb{Z}$. L'épimorphisme consiste alors en l'application qui au mot réduit $a.\sigma^{\lambda_1}.\mu.\sigma.\cdots.\sigma.\mu^{\lambda_2}$ de $\mathbb{Z}/2n\mathbb{Z} \underset{\mathbb{Z}/n\mathbb{Z}}{*} \mathbb{Z}/2n\mathbb{Z}$ associe le mot $\overline{\sigma}^{\lambda_1}.\overline{\mu}.\overline{\sigma}.\cdots.\overline{\sigma}.\overline{\mu}^{\lambda_2}$ de $\mathbb{Z}/2\mathbb{Z} * \mathbb{Z}/2\mathbb{Z}$. Le noyau de ce morphisme étant visiblement $\mathbb{Z}/n\mathbb{Z}$, on en déduit la suite exacte

$$1 \longrightarrow \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/2n\mathbb{Z} \underset{\mathbb{Z}/n\mathbb{Z}}{*} \mathbb{Z}/2n\mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z} * \mathbb{Z}/2\mathbb{Z} \longrightarrow 1$$

Supposons maintenant que n est un entier impair, il existe alors une section naturelle

$$\mathbb{Z}/2n\mathbb{Z} \underset{\mathbb{Z}/n\mathbb{Z}}{*} \mathbb{Z}/2n\mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z} * \mathbb{Z}/2\mathbb{Z}$$

celle qui est donnée par le choix de $\sigma = \mu = n$. Le groupe $\mathbb{Z}/n\mathbb{Z}$ étant visiblement dans le centre de $\mathbb{Z}/2n\mathbb{Z} \underset{\mathbb{Z}/n\mathbb{Z}}{*} \mathbb{Z}/2n\mathbb{Z}$, on en déduit finalement que

$$\mathbb{Z}/2n\mathbb{Z} \underset{\mathbb{Z}/n\mathbb{Z}}{*} \mathbb{Z}/2n\mathbb{Z} \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} * \mathbb{Z}/2\mathbb{Z} \simeq \mathbb{Z}/n\mathbb{Z} \times D_\infty \simeq (\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}) \times \mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z} \rtimes \mathbb{Z}/2n\mathbb{Z}$$

où le dernier produit semi-direct est celui associé à l'unique action non triviale de $\mathbb{Z}/2n\mathbb{Z}$ sur $\mathbb{Z}$.

c) En caractéristique non nulle, le problème de l'étude des involutions est plus subtile. Par exemple, considérons deux éléments $a \neq b$ d'un corps k de caractéristique $p \neq 0$ et les involutions τ_a et τ_b définies par

$$\tau_a(t) = \frac{-t}{1+at} \text{ et } \tau_b(t) = \frac{-t}{1+bt}$$

Posons $\omega = \tau_a\tau_b : t \longmapsto \dfrac{t}{1+(b-a)t}$. Pour tout entier $n \geq 0$, on a

$$\omega^n : t \longmapsto \frac{t}{1+n(b-a)t}$$

et donc $o(\omega) = p$. Comme $< \tau_a, \tau_b > = < \tau_a, \omega >$ et que $o(\tau_a) = 2$ et $o(\tau_a\omega) = 2$, on en déduit que $< \tau_a, \tau_b >$ est isomorphe au groupe diédral d'ordre $2p$, D_{2p}.

4.2.– Cas de la torsion rationnelle.

On dira d'un élément de torsion $\sigma \in \mathrm{Gal}(k((t))/k)$ qu'il est *rationnel* (resp. *algébrique*, resp. *transcendant*) si $\sigma(t) \in k(t)$ (resp. $\sigma(t) \in \overline{k(t)} - k(t)$, resp. $\sigma(t) \notin \overline{k(t)}$).

Proposition 40.– *On suppose que k est de caractéristique 0. Un élément $\sigma \in \mathrm{Gal}(k((t))/k)$ d'ordre n est rationnel si et seulement si il existe une racine primitive n-ième de l'unité ξ_n et un élément $\lambda \in k$ tels que*

$$\sigma(t) = \frac{\xi_n t}{1+\lambda t}$$

Preuve : Puisque $\sigma(t) \in k(t)$, la restriction de σ à $k(t)$ est un k-monomorphisme de corps. Maintenant, puisque $\sigma^{-1} = \sigma^{n-1}$, on voit que $\sigma^{-1}(t) \in k(t)$ et donc la restriction de σ à $k(t)$ est aussi surjective, c'est-à-dire pour finir que nous sommes en présence d'un k-automorphisme du corps $k(t)$. On peut donc affirmer que $\sigma(t)$ est une homographie. Si l'on pose $\sigma(t) = \frac{a+bt}{c+bt}$, on voit que si $a \neq 0$ alors $v(\sigma(t)) = 0$ ou -1 ce qui est absurde. Ainsi, on a $\sigma(t) = \frac{\omega t}{1+\lambda t} = \omega t + \cdots$. Le fait que σ soit d'ordre n impose alors que ω soit une racine primitive n-ième de l'unité.

Réciproquement, la matrice de $\mathrm{PGL}_2(k)$ associée à $\sigma(t)$ vaut $M = \left(\begin{smallmatrix} \xi_n & 0 \\ \lambda & 1 \end{smallmatrix}\right)$. Pour tout entier h on a $M^h = \left(\begin{smallmatrix} \xi_n^h & 0 \\ \lambda\frac{\xi_n^h - 1}{\xi_n - 1} & 1 \end{smallmatrix}\right)$, ce qui prouve bien que M (et donc σ) est d'ordre n.

□

Le cas général de la structure du sous-groupe engendré par deux éléments de torsion rationnels est très différent du cas des involutions. En effet, on a :

Théorème 41.– *Si k est de caractéristique 0 et si $\sigma, \tau \in \mathrm{Gal}(k((t))/k)$ désignent deux éléments de torsions rationnels qui ne sont pas tous les deux des involutions alors le groupe $< \sigma, \tau >$ n'est pas un amalgame (non trivial) des groupes $< \sigma >$ et $< \tau >$.*

Preuve : Notons $n = o(\sigma)$ et $m = o(\tau)$, d'après la proposition 40 il existe $\lambda, \mu \in k$ tels que

$$\sigma(t) = \frac{\xi_n t}{1+\lambda t} \text{ et } \tau(t) = \frac{\xi_m t}{1+\mu t}$$

Puisque, par hypothèse $(n, m) \neq (2, 2)$, quitte à prendre une puissance première à n (ou m) de σ (ou τ), on peut supposer que $\xi_n\xi_m \neq 1$. Dans ces conditions, on a :

$$\sigma \circ \tau(t) = \frac{\xi_n\xi_m t}{1+(\lambda+\mu\xi_n)t}$$

et il s'ensuit, par application de la proposition 40, que $\sigma \circ \tau$ est de torsion. S'il existe un isomorphisme $< \sigma, \tau > \simeq < \sigma > \underset{G}{*} < \tau >$, alors la description en mots réduits de l'amalgame

montre que l'un des ensembles quotients $< \sigma > /G$ ou $< \tau > /G$ est nécessairement trivial (sinon $\sigma \circ \tau$ serait d'ordre infini). On a donc, par exemple, $G =< \tau >$ et donc $< \tau > \subset < \sigma >$, et l'amalgame est trivial.

□

On peut décrire précisément la structure algébrique du groupe $< \sigma, \tau >$:

Théorème 42.– *Soient k un corps de caractéristique 0 et $\sigma, \tau \in \mathrm{Gal}(k((t))/k)$ deux éléments de torsions rationnels ne commutant pas. Posons et $G =< \sigma, \tau >$, $n = o(< \sigma >)$, $m = o(< \tau >)$ et $q = \mathrm{ppcm(n,m)}$. On a*

$$G \simeq \bigoplus_{h=1}^{\varphi(q)} \mathbb{Z} \rtimes \mathbb{Z}/q\mathbb{Z}$$

Preuve : Le sous-groupe de $\mathrm{Gal}(k((t))/k)$ constitué des automorphismes rationnels est aussi un sous-groupe de $\mathrm{Aut}_k(k(t)) \simeq \mathrm{PGL}_2(k)$. Un automorphisme rationnel est d'ordre k si et seulement si la matrice associée à cet automorphisme est de la forme $\left(\begin{smallmatrix} \xi_h & 0 \\ \lambda & 1 \end{smallmatrix}\right)$ où ξ_h désigne une racine primitive h-ième de l'unité et $\lambda \in k$. Plaçons-nous dans les hypothèses du théorème. Quitte à conjuguer par un automorphisme rationnel et à modifier σ et τ par des puissances adéquates, on peut supposer que σ a pour matrice $\left(\begin{smallmatrix} \xi_{nm}^m & 0 \\ 0 & 1 \end{smallmatrix}\right)$ et que τ a pour matrice $\left(\begin{smallmatrix} \xi_{nm}^n & 0 \\ \lambda & 1 \end{smallmatrix}\right)$. La non comutativité de σ et τ équivaut donc à dire que $\lambda \neq 0$.

On identifie G en un sous-groupe de $\mathrm{PGL}_2(k)$ et on considère le sous-groupe H de G défini par :

$$H = \left\{ M \in G / \ M = \left(\begin{smallmatrix} 1 & 0 \\ \bullet & 1 \end{smallmatrix}\right) \right\}$$

Nous allons montrer que

$$1 \longrightarrow H \longrightarrow G \longrightarrow \mathbb{Z}/q\mathbb{Z} \longrightarrow 1$$

est une suite exacte scindée.

Puisque $\sigma H \sigma^{-1} = H$ et $\tau H \tau^{-1} = H$, on en déduit que H est distingué dans G. Notons $\cdot$ les classes des éléments de G dans G/H. Puisque $\sigma\tau\sigma^{-1}\tau^{-q} \in H$, les éléments $\overline{\sigma}$ et $\overline{\tau}$ commutent et G/H est, par conséquent, abélien. Considérons (α, β) un couple de Bezout de l'équation $\alpha n + \beta m = d = \mathrm{pgcd}(n, m)$. Si l'on pose $g = \sigma^\alpha \tau^\beta$, alors pour $h \geq 0$, on a

$$g^h = \left(\begin{smallmatrix} \xi_{nm}^{hd} & 0 \\ \bullet & 1 \end{smallmatrix}\right)$$

et donc $g^h \in H$ si et seulement si $q | h$. L'élément $\overline{g}$ est donc d'ordre q. Maintenant, comme $\overline{g}^{m/d} = \overline{\sigma}$ et $\overline{g}^{n/d} = \overline{\tau}$, on en déduit que $G/H =< \overline{g} > \simeq \mathbb{Z}/q\mathbb{Z}$.

Maintenant, dans G, si l'on pose $g = \sigma^\alpha \tau^\beta = \left(\begin{smallmatrix} \xi_{nm}^d & 0 \\ \mu & 1 \end{smallmatrix}\right)$, alors

$$g^q = \begin{pmatrix} \xi_{nm}^{qd} & 0 \\ \mu(1 + \xi_{nm}^d + \cdots + \xi_{nm}^{d(q-1)}) & 1 \end{pmatrix} = I$$

et donc g est d'ordre q dans G, ce qui prouve que la suite exacte est scindée.

Le dernier point à vérifier est que H est un $\mathbb{Z}$-module libre de rang $\varphi(q)$. D'abord il faut constater que H ne peut être trivial, car sinon G serait abélien et σ et τ commuteraient, ce qui est exclu par hypothèse. Ensuite, le groupe H est isomorphe au sous-groupe additif H_0 de k formé des $x \in k$ tel que $\left(\begin{smallmatrix} 1 & 0 \\ x & 1 \end{smallmatrix}\right) \in H$. Une récurrence immédiate sur la longueur d'un produit qui définit un élément de G montre que le coefficient de ligne 2 et de colonne 1 des éléments de G sont des éléments de $= \lambda\mathbb{Z}[\xi_q] = \bigoplus_{h < \varphi(q)} \lambda \xi_q^h \mathbb{Z}$. Ainsi, H_0 est un sous-module de $\lambda\mathbb{Z}[\xi_q]$, et donc H est un $\mathbb{Z}$-module libre de rang $\leq \varphi(q)$. Pour tout $h = 0, \cdots, \varphi(q) - 1$, il existe $\alpha_h \neq 0$ tel que $M_h = \left(\begin{smallmatrix} \xi_q^h & 0 \\ \alpha_h & 1 \end{smallmatrix}\right) \in G$. On a alors

$$M_h \left(\begin{smallmatrix} 1 & 0 \\ x & 1 \end{smallmatrix}\right) M_h^{-1} = \left(\begin{smallmatrix} 1 & 0 \\ x\xi_q^{-h} & 1 \end{smallmatrix}\right)$$

et donc $x\xi_q^{-h} \in H_0$. Quand $x \neq 0$ (un tel x existe bien puisque $H_0 \neq \{0\}$), la famille $\{x\xi_q^{-h} / \ h = 0, \cdots, \varphi(q) - 1\}$ est $\mathbb{Z}$-libre et donc $\mathrm{rg}(H_0) = \varphi(q)$.

□

Le groupe H_0 n'a aucune raison d'être égal à $\lambda\mathbb{Z}[\xi_q]$ tout entier. Par exemple, un calcul simple montre que, pour le choix $\sigma = \left(\begin{smallmatrix} j & 0 \\ 1 & 1 \end{smallmatrix}\right)$ et $\tau = \left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ on obtient $H_0 = (1 + j)\mathbb{Z} \oplus (2 - j)\mathbb{Z}$, qui est un sous-groupe strict de $\mathbb{Z}[-j]$.

Bibliographie

[Bou] Nicolas Bourbaki, *Elément de mathématiques, algèbre chapitre VII*, Hermann.

[Des] Bruno Deschamps, *Le corps des séries de Puiseux généréalises*, Acta Arithmetica, XCVI (2001).

[FJ] Mike Fried and Moshe Jarden, *Field arithmetic*, Srpinger-Verlag (1985).

[MKS] W. Magnus, A. Karass, and D. Solitar, *Combinatorial group theory*, J. Wiley & sons (1966).

[Rib1] Paulo Ribenboim, *L'arithmétique des corps*, Hermann (1970).

[Rib2] Paulo Ribenboim, *the theory of classical valuations*, Monographs in Math., Springer-Verlag (1999).

[Ser] Jean-Pierre Serre, *Arbres, amalgames et* SL_2, Astérisque 46, SMF (1977).

Bruno Deschamps, Ivan Suarez Atias
Département de Mathématiques — Université du Maine
Avenue Olivier Messiaen, 72085 Le Mans cedex 9 - France

Laboratoire de Mathématiques Nicolas Oresme
CNRS UMR 6139

E-mail : Bruno.Deschamps@univ-lemans.fr, Ivan.Suarez_Atias@univ-lemans.fr