La structure profinie du groupe des unités d'un anneau de séries entières à coefficients dans un anneau fini.

Bruno DESCHAMPS — Gérard LELOUP

Université du Maine

Abstract.— In this article we show that for a given commutative unitary finite ring A, the units group of the ring $A[[T]]$ of power series over A is isomorphic, as profinite group, to the direct product $A^* \times \Gamma \times \prod_{p|\sharp A} \mathbf{Z}_p^{\aleph_0}$ where Γ is a profinite abelian group of finite exponent. We give a sufficient condition on A (including the case of direct products) to have $\Gamma \simeq N^{\aleph_0}$ where $N = \sqrt{\{0\}}$ is the group of nilpotent elements of A.

Abstract.— Dans cet article nous montrons que, pour un anneau commutatif unitaire fini A donné, le groupe des unités de l'anneau $A[[T]]$ des séries entières à coefficients dans A est isomorphe, en tant que groupe profini, à un produit direct $A^* \times \Gamma \times \prod_{p|\sharp A} \mathbf{Z}_p^{\aleph_0}$ où Γ est un groupe profini abélien d'exposant. Nous donnons une condition suffisante sur A (incluant le cas des produits directs) pour que $\Gamma \simeq N^{\aleph_0}$ où $N = \sqrt{\{0\}}$ désigne le groupe des éléments nilpotents de A.

1.— Introduction, notations et objectifs.

Considérons un anneau commutatif A et l'anneau $A[[T]]$ des séries entières à coefficients dans A. Sur $A[[T]]$ l'application

$$v(a_0 + a_1 T + \cdots) = \inf\{n \in \mathbf{N} / \ a_n \neq 0\}$$

définit une *presque-valuation* (i.e. une application qui vérifie les axiomes d'une valuation sauf l'égalité $v(PQ) = v(P) + v(Q)$ qui est remplacée par l'inégalité $v(PQ) \geq v(P) + v(Q)$). Pour $n \geq 0$, on considère l'idéal

$$I_n = \{f \in A[[T]] / \ v(f) \geq n+1\}$$

(lorsque A est unitaire, I_n est l'idéal $(T^{n+1}) = T^{n+1}A[[T]]$). On voit que l'anneau quotient $A[[T]]/I_n$ s'identifie à l'anneau $A_n[T]$ des polynômes de degré $\leq n$ (le produit considéré sur cet anneau étant le produit des polynômes tronqué au rang n) et, par suite, que l'anneau $A[[T]]$ s'identifie à la limite projective $\varprojlim A[[T]]/I_n$. En particulier, si A est fini alors $A[[T]]$ est un anneau profini.

La presque-valuation v définit sur $A[[T]]$ une topologie. Quand A est fini, on voit que cette topologie correspond à celle de la structure profinie de $A[[T]]$. Cette topologie est alors métrisable (cf [S, p.5 exercice 2]).

Lorsque A est unitaire, l'anneau $A[[T]]$ l'est aussi et l'on sait alors qu'une série $f \in A[[T]]$ est inversible si et seulement si $f(0)$ est inversible dans A. Si A^* désigne le groupe des inversibles de A alors le groupe des inversibles de $A[[T]]$, noté dans ce texte $\mathbf{U}(A)$, s'identifie au produit cartésien $A^* \times \mathbf{P}(A)$ où

$$\mathbf{P}(A) = \{f \in A[[T]] / \ f(0) = 1\}$$

[0]Mathematical Subject classification 2000 : 20E18, 13J05.

désigne le groupe des unités principales. Lorsque A est fini, les groupes $\mathbf{U}(A)$ et $\mathbf{P}(A)$ sont des sous-ensembles fermés de $A[[T]]$ pour la topologie profinie et ce sont des groupes profinis pour cette topologie. En effet, de manière générale si $R = \varprojlim R_i$ est un anneau profini unitaire alors on a $R^* = \varprojlim R_i^*$. Les groupes R_i^* étant finis, on voit que R^* est profini et que sa topologie profinie est bien celle induite par R.

Ainsi, $\mathbf{U}(A)$ s'identifie au groupe profini $\varprojlim (A[[T]]/I_n)^*$. On peut donner explicitement une *bonne filtration* de sous-groupes ouverts de $\mathbf{P}(A)$: ce sont les sous-groupes $U_n = 1+T^{n+1}A[[T]]$. En effet, les U_n sont des ensembles ouverts dans $A[[T]]$ (puisque ce sont les translatés par 1 des ouverts I_n), ce sont donc des sous-groupes ouverts de $\mathbf{P}(A)$ et comme $\bigcap_n U_n = \{1\}$ il s'ensuit que $\mathbf{P}(A) \simeq \varprojlim \mathbf{P}(A)/U_n$. Ce dernier point permet, en particulier, de justifier que $\mathbf{P}(A)$ est un groupe profini de rang $\leq \aleph_0$, puisqu'il est limite projective d'un système projectif indexé par $\mathbf{N}$ (cf [FJ, p.188 example 15.13]).

Par ailleurs, pour tout entier $n \geq 1$, une famille de réprésentants dans $\mathbf{P}(A)$ du groupe quotient $\mathbf{P}(A)/U_n$ est l'ensemble

$$E_n = \{1 + a_1T + \cdots + a_nT^n / \ a_1, \cdots, a_n \in A\}$$

En effet, soit $S(T) = 1+\lambda_1 T+\cdots \in \mathbf{P}(A)$. Considérons $P(T) = 1+\lambda_1 T+\cdots+\lambda_n T^n \in E_n$, alors $S(T) = P(T) + T^{n+1}\Omega(T)$ avec $v(\Omega) \geq 0$ et par suite, puisque $v(P^{-1}) = 0$, on a

$$P^{-1}(T).S(T) = 1 + T^{n+1}\Omega(T)P^{-1}(T) \in U_n$$

et donc P est un représentant de S.

Soit maintenant $G, H \in E_n$ avec $G \neq H$. On a $1 \leq v(G-H) \leq n$, mais par ailleurs on a aussi

$$\begin{array}{rcl} v(G-H) & = & v((G-H)HH^{-1}) \geq v((G-H)H^{-1}) + v(H) \\ & = & v((G-H)H^{-1}) = v(1-GH^{-1}) \\ & \geq & v(G-H) + v(H^{-1}) = v(G-H) \end{array}$$

et donc $v(1-GH^{-1}) = v(G-H) \leq n$. Ceci justifie donc que G et H ne sont pas dans la même classe modulo U_n.

On déduit en particulier de cette remarque que si A est un p-anneau (i.e. un anneau qui est un p-groupe) alors $\mathbf{P}(A)/U_n$ est un p-groupe pour tout $n \geq 0$ et donc que $\mathbf{P}(A)$ est un pro-p-groupe (ce qui n'est pas le cas de $\mathbf{U}(A)$).

Le but de cet article est de donner une description de la structure profinie du groupe $\mathbf{U}(A)$ lorsque A est un anneau commutatif unitaire fini. Pour ce faire, remarquons préliminairement que, étant donné un anneau fini A (*a priori* non nécessairement commutatif ni unitaire), le groupe $(A,+)$ étant abélien, on sait qu'il est isomorphe au produit de ses p-sous-groupes de Sylow (qui sont uniques pour p donné)

$$(A,+) = S_{p_1} \oplus \cdots \oplus S_{p_n} \simeq S_{p_1} \times \cdots \times S_{p_n}$$

Maintenant, du fait des théorèmes de Sylow, on voit facilement que

$$S_{p_i} = \{a \in (A,+) / \ \exists \alpha \geq 0, \ o(a) = p_i^\alpha\}$$

On en déduit donc que S_{p_i} est un idéal bilatère de A et que l'on a $S_{p_i} \cap S_{p_j} = \{0\}$ pour tout $i \neq j$. Considérons maintenant l'isomorphisme de groupe

$$\begin{array}{rccc} \theta : & S_{p_1} \times \cdots \times S_{p_n} & \longrightarrow & A \\ & (a_1, \cdots, a_n) & \longmapsto & a_1 + \cdots + a_n \end{array}$$

Si $i \neq j$ et $a_i \in S_{p_i}$ et $a_j \in S_{p_j}$, comme S_{p_i} et S_{p_j} sont deux idéaux bilatères, on a

$$a_i a_j \in S_{p_i} \cap S_{p_j} = \{0\}$$

et donc $a_i a_j = 0$. Cette relation implique en particulier que θ est un isomorphisme d'anneau et donc que l'anneau A est isomorphe au produit direct des idéaux S_{p_i}. Par suite on a l'isomorphisme d'anneau

$$A[[T]] \simeq S_{p_1}[[T]] \times \cdots \times S_{p_n}[[T]]$$

qui, lorsque A est commutatif et unitaire, induit les isomorphismes de groupes

$$\mathbf{U}(A) \simeq \mathbf{U}(S_{p_1}) \times \cdots \times \mathbf{U}(S_{p_n}) \text{ et } \mathbf{P}(A) \simeq \mathbf{P}(S_{p_1}) \times \cdots \times \mathbf{P}(S_{p_n})$$

Ainsi, pour déterminer la structure du groupe $\mathbf{U}(A)$ en toute généralité, il suffit de savoir le faire lorsque A est un p-anneau.

Dans ce texte, nous montrons que, lorsque A est un p-anneau commutatif fini unitaire, $\mathbf{P}(A)$ est isomorphe (en tant que groupe profini) au produit direct $\mathbf{Tors}(\mathbf{P}(A)) \times \widehat{F}_\omega(\mathcal{C}_p^{ab})$ où $\widehat{F}_\omega(\mathcal{C}_p^{ab}) = (\mathbf{Z}_p)^{\aleph_0}$ désigne le pro-p-groupe abélien libre de rang $\aleph_0$ (dans ce texte $\mathcal{C}_p^{ab}$ désigne la classe des p-groupes abéliens finis) et $\mathbf{Tors}(\mathbf{P}(A))$ désigne le sous-groupe de torsion de $\mathbf{P}(A)$ (théorème 7).

Ensuite nous étudions le groupe $\mathbf{Tors}(\mathbf{P}(A))$. Nous montrons qu'il est égal à $1 + T.N[[T]]$ où $N = \sqrt{\{0\}}$ désigne le nilradical de A (proposition 5) et que, sous une certaine condition sur A, il est isomorphe au groupe produit $N^{\aleph_0}$ (proposition 9).

2.— A propos de la structure des groupes profinis abéliens.

On pourra trouver dans [RZ, p.133 Theorem 4.3.3] une preuve du fait qu'un groupe profini abélien sans torsion est isomorphe à un produit cartésien de groupes $\mathbf{Z}_p$ (p pouvant varier) (voir aussi [S, p.2 exercice 1]). En particulier, on en déduit ce résultat fondamental : un pro-p-groupe abélien est libre si et seulement si il est sans torsion. Ce résultat permet alors de décrire les groupes profinis abéliens à torsion fermée :

Proposition 1.— *Soit G un pro-p-groupe abélien et $\mathbf{Tors}(G)$ son sous-groupe de torsion. Les propriétés suivantes sont équivalentes :*

i) $\mathbf{Tors}(G)$ est fermé dans G,

ii) G est isomorphe (en tant que groupe profini) au produit cartésien $\widehat{F}_\alpha(\mathcal{C}_p^{ab}) \times \mathbf{Tors}(G)$ pour un certain cardinal α où $\widehat{F}_\alpha(\mathcal{C}_p^{ab}) = (\mathbf{Z}_p)^\alpha$ désigne le pro-p-groupe abélien libre de rang α.

Preuve : *ii)* $\Rightarrow$ *i)* est évident.

i) $\Rightarrow$ *ii)* La suite exacte

$$1 \longrightarrow \mathbf{Tors}(G) \longrightarrow G \longrightarrow \frac{G}{\mathbf{Tors}(G)} \longrightarrow 1$$

a des applications continues. Si $\mathbf{Tors}(G)$ est fermé dans G alors le groupe $G/\mathbf{Tors}(G)$ est un groupe profini et sa topologie profinie correspond à la topologie quotient.

En vertu du rappel précédent, le groupe $G/\mathbf{Tors}(G)$ (étant sans torsion) est pro-$\mathcal{C}_p^{ab}$-libre. Maintenant, si $\mathcal{C}$ désigne une classe presque pleine (au sens de [FJ,

p.189]) de groupes finis alors le théorème de Gruenberg (cf [G], [FJ, p.290 lemma 20.8]) implique qu'un pro-$\mathcal{C}$-groupe libre est $\mathcal{C}$-projectif. En appliquant ce résultat au $\mathcal{C}_p^{ab}$-problème de plongement suivant :

$$\begin{array}{ccccccccc} & & & & & & & & \dfrac{G}{\mathbf{Tors}(G)} \\ & & & & & & & & \Big\downarrow \\ 1 & \longrightarrow & \mathbf{Tors}(G) & \longrightarrow & G & \longrightarrow & \dfrac{G}{\mathbf{Tors}(G)} & \longrightarrow & 1 \end{array}$$

on déduit que la suite exacte $1 \longrightarrow \mathbf{Tors}(G) \longrightarrow G \longrightarrow G/\mathbf{Tors}(G) \longrightarrow 1$ est une suite exacte scindée de groupes profinis abéliens ce qui permet d'affirmer que

$$G \simeq \mathbf{Tors}(G) \times \frac{G}{\mathbf{Tors}(G)} \simeq \mathbf{Tors}(G) \times \widehat{F}_\alpha(\mathcal{C}_p^{ab})$$

où $\alpha = \mathrm{rg}\left(\dfrac{G}{\mathbf{Tors}(G)}\right)$.

La fermeture de $\mathbf{Tors}(G)$ dans G a donc une conséquence importante sur la structure du pro-p-groupe abélien G. On peut, par ailleurs, caractériser cette propriété topologique de manière purement algébrique :

Proposition 2.— *Soit G un pro-p-groupe abélien et $\mathbf{Tors}(G)$ son sous-groupe de torsion. Les propriétés suivantes sont équivalentes :*

i) $\mathbf{Tors}(G)$ *est fermé dans G,*

ii) $\mathbf{Tors}(G)$ *est d'exposant.*

Preuve : *i)* $\Rightarrow$ *ii)* Le groupe $\mathbf{Tors}(G)$ (étant fermé dans G) est compact et un groupe compact abélien de torsion est d'exposant (cf [RZ]). Rappelons une courte et élégante preuve de ce dernier résultat : soit Γ un groupe compact abélien de torsion et pour tout $n \geq 1$, H_n le noyau de l'application $x \mapsto x^n$. Les sous-groupes H_n sont fermés et de réunion égale à Γ. Comme Γ est compact, c'est un espace de Baire et, par suite, il existe un entier n_0 tel que H_{n_0} soit d'intérieur non vide. Le sous-groupe H_{n_0} est donc ouvert et, par suite, d'indice fini. Si l'on note $x_1, \cdots, x_k \in \Gamma$ une classe de représentant dans Γ du groupe quotient G/H_{n_0} on voit alors que $\mathrm{p.p.c.m}(n_0, o(x_1), \cdots, o(x_n))$ est un exposant pour le groupe Γ.

ii) $\Rightarrow$ *i)* Si $n \geq 1$ est un exposant du groupe $\mathbf{Tors}(G)$ alors $\mathbf{Tors}(G)$ est le noyau du morphisme continu $x \mapsto x^n$ et donc, par suite, est fermé dans G.

3.— Une décomposition de $\mathbf{P}(A)$.

3.1.— Le cas des corps. On considère un nombre entier $q = p^r$ puissance non nulle d'un nombre premier p et $K = \mathbf{F}_q$ le corps fini à q éléments. Comme K est intègre (ce qui est équivalent dans le cas fini à être un corps), il est clair que $\mathbf{P}(K)$

est sans torsion. En vertu de ce qui a été rappelé dans le paragraphe précédent, puisque $\mathbf{P}(K)$ est un pro-p-groupe sans torsion il est libre. Reste à déterminer son rang pour le décrire complètement. On a vu que $\mathrm{rg}(\mathbf{P}(K)) \leq \aleph_0$.

On reprend les notations de l'introduction : pour tout entier $n \geq 0$, on note

$$U_n = 1 + T^{n+1}K[[T]] = \{S \in K[[T]] / \ v(S-1) \geq n+1\}$$
$$E_n = \{1 + a_1T + \cdots + a_nT^n / \ a_1, \cdots, a_n \in K\}$$

La suite $(U_n)_n$ forme alors une bonne filtration de $\mathbf{P}(K)$. La sous-suite $(U_{p^k-1})_k$ constitue également une bonne filtration de $\mathbf{P}(K)$ ce qui assure aussi que

$$\mathbf{P}(K) \simeq \varprojlim \frac{\mathbf{P}(K)}{U_{p^k-1}}$$

Lemme 3.— *Pour tout entier $k \geq 1$, on a*

$$\Gamma_k = \frac{\mathbf{P}(K)}{U_{p^k-1}} \simeq (\mathbf{Z}/p)^{\alpha_1} \times \left(\mathbf{Z}/p^2\right)^{\alpha_2} \times \cdots \times \left(\mathbf{Z}/p^k\right)^{\alpha_k}$$

avec

$$\alpha_i = rp^{k-i-1}(p-1)^2, \ \textit{pour } i = 1, \cdots, k-1 \ \textit{et } \alpha_k = r(p-1)$$

Preuve : Si h est un entier tel que $n < p^h$, alors pour tout $1+\lambda_1T+\cdots+\lambda_nT^n \in E_n$, on a

$$(1 + \lambda_1T + \cdots + \lambda_nT^n)^{p^h} = 1 + \lambda_1^{p^h}T^{p^h} + \cdots + \lambda_n^{p^h}T^{np^h} \in U_n$$

ce qui justifie que l'ordre d'un élément de $\frac{\mathbf{P}(K)}{U_n}$ est toujours inférieur à p^h.

• Prenons maintenant $n = p^k - 1$, la remarque précédente justifie qu'il existe des entiers $\alpha_1, \cdots, \alpha_k$ tels que $\Gamma_k \simeq (\mathbf{Z}/p)^{\alpha_1} \times \left(\mathbf{Z}/p^2\right)^{\alpha_2} \times \cdots \times \left(\mathbf{Z}/p^k\right)^{\alpha_k}$

Fixons-nous un entier $i \in \{1, \cdots, k\}$ et dénombrons les éléments de Γ_k d'ordre $\leq p^i$. Dans $\mathbf{Z}/p^j$, il y a p^j tels éléments si $j \leq i$ et p^i sinon. Ainsi, dans $(\mathbf{Z}/p)^{\alpha_1} \times \left(\mathbf{Z}/p^2\right)^{\alpha_2} \times \cdots \times \left(\mathbf{Z}/p^k\right)^{\alpha_k}$ il y a $p^{\alpha_1+2\alpha_2+\cdots+i\alpha_i+i\alpha_{i+1}+\cdots+i\alpha_k}$ éléments d'ordre $\leq p^i$.

Maintenant, un élément $S \in E_n$ est d'ordre $\leq p^i$ si et seulement si on peut écrire

$$S = 1 + \lambda_hT^h + \cdots + \lambda_nT^n$$

avec $h = p^{k-i}$. Il y a donc $q^{p^k-p^{k-i}}$ éléments d'ordre $\leq p^i$ dans Γ_k.

On en déduit donc que les entiers $\alpha_1, \cdots, \alpha_k$ sont solutions du système linéaire suivant

$$\left\{\begin{array}{ccccccccccc}
\alpha_1 & + & 2\alpha_2 & + & \cdots & + & (k-1)\alpha_{k-1} & + & k\alpha_k & = & r(p^k-1) \\
\alpha_1 & + & 2\alpha_2 & + & \cdots & + & (k-1)\alpha_{k-1} & + & (k-1)\alpha_k & = & r(p^k-p) \\
 & & & & & & & & \vdots & & \\
\alpha_1 & + & 2\alpha_2 & + & \cdots & + & 2\alpha_{k-1} & + & 2\alpha_k & = & r(p^k-p^{k-2}) \\
\alpha_1 & + & \alpha_2 & + & \cdots & + & \alpha_{k-1} & + & \alpha_k & = & r(p^k-p^{k-1})
\end{array}\right.$$

La résolution du système conduit alors au résultat annoncé.

Corollaire 4.— *On a $\mathrm{rg}(\Gamma_k) = r(p-1)p^{k-1}$ et, par conséquent, $\mathrm{rg}(\mathbf{P}(K)) = \aleph_0$.*

Preuve : L'égalité $\mathrm{rg}(\Gamma_k) = r(p-1)p^{k-1}$ est immédiate. On en déduit que $\lim_k \mathrm{rg}(\Gamma_k) = +\infty$, ce qui justifie que $\mathrm{rg}(\mathbf{P}(K)) = +\infty$ puisque chaque Γ_k est un quotient continu de $\mathbf{P}(K)$. Par ailleurs, on a vu que $\mathrm{rg}(\mathbf{P}(K)) \leq \aleph_0$, d'où le résultat.

La conclusion de cette étude est donc que $\mathbf{P}(\mathbf{F}_q) \simeq \widehat{F}_\omega(\mathcal{C}_p^{ab}) = (\mathbf{Z}_p)^{\aleph_0}$.

3.2.— Le cas général. Soit A un p-anneau commutatif unitaire fini (disons $\sharp A = p^g$). Notons

$$N = \sqrt{\{0\}} = \sqrt{pA} \text{ (car } \{0\} \subset pA \subset N)$$

l'idéal constitué des éléments nilpotents de A. On a

Proposition 5.— *Soit $f(T) = 1 + a_1T + a_2T^2 + \cdots \in \mathbf{P}(A)$. Les propositions suivantes sont équivalentes :*

i) $f \in \mathbf{Tors}(\mathbf{P}(A))$,

ii) pour tout $n \geq 1$, $a_n \in N$ (i.e. $f \in 1 + T.N[[T]]$).

Preuve : *i)* $\Rightarrow$ *ii)* Considérons l'anneau quotient A/pA et l'épimorphisme naturel $s : A \longrightarrow A/pA$ que l'on étend à $A[[T]] \longrightarrow (A/pA)[[T]]$. Comme $\mathbf{P}(A)$ est un pro-p-groupe, si $f \in \mathbf{Tors}(\mathbf{P}(A))$ alors il existe $\alpha \geq 1$ tel que $f^{p^\alpha} = 1$. On a donc

$$1 = s(f^{p^\alpha}) = s(f)^{p^\alpha} = \left(1 + s(a_1)T + s(a_2)T^2 + \cdots\right)^{p^\alpha}$$

mais comme A/pA est de caractéristique p on en déduit que

$$1 + s(a_1)^{p^\alpha}T^{p^\alpha} + s(a_2)^{p^\alpha}T^{2p^\alpha} + \cdots = 1$$

et donc que pour tout $n \geq 1$, $s(a_n)^{p^\alpha} = 0$ c'est-à-dire $a_n^{p^\alpha} \in pA$ et, par suite, $a_n \in \sqrt{pA} = N$.

ii) $\Rightarrow$ *i)* Supposons que $\mathrm{car}(A) = p^\alpha$. Comme A est fini, l'entier

$$\beta = \inf\{h \geq 1/\ \forall x \in N,\ x^{p^h} \in pA\}$$

existe. On a donc, puisque A/pA est de caractéristique p,

$$s(f^{p^\beta}) = s(f)^{p^\beta} = 1 + s(a_1)^{p^\beta}T^{p^\beta} + \cdots = 1 + s(a_1^{p^\beta})T^{p^\beta} + \cdots = 1$$

et, par suite, $f^{p^\beta} - 1$ est à coefficients dans pA et donc pour montrer que f est de torsion, on peut supposer que $f \in 1 + T.pA[[T]]$. Pour la suite de la preuve nous allons avoir besoin du lemme suivant :

Lemme 6.— *Notons v_p la valuation p-adique. Pour tout $r = 1, \cdots, p^k$ on a*

$$v_p(C_{p^k}^r) = k - v_p(r)$$

Preuve du lemme : On a

$$C_{p^k}^r = \frac{p^k(p^k-1)\cdots(p^k-r+1)}{1.2.\cdots.r} = \frac{p^k}{r}.\frac{p^k-1}{1}.\cdots.\frac{p^k-(r-1)}{r-1}$$

Si $r < p^k$, alors pour tout $i = 1, \cdots, r$ on a $v_p(p^k - i) = v_p(i)$ et donc

$$v_p\left(\frac{p^k-i}{i}\right) = 0$$

Ainsi on a

$$v_p(C_{p^k}^r) = v_p\left(\frac{p^k}{r}\right) = k - v_p(r)$$

La proposition est clairement vraie pour $r = p^k$.

Supposons donc que $a_1, a_2, \cdots \in pA$, disons pour $n \geq 1$, $a_n = pb_n$. On a

$$f^{p^{\alpha-1}} = 1 + \sum_{n\geq 1} \left(\sum_{i_1+\cdots+i_{p^{\alpha-1}}=n} a_{i_1} \cdots a_{i_{p^{\alpha-1}}} \right) T^n$$

en posant $a_0 = 1$. Pour tout $n \geq 1$ on a

$$\begin{aligned} \sum_{i_1+\cdots+i_{p^{\alpha-1}}=n} a_{i_1} \cdots a_{i_{p^{\alpha-1}}} &= \sum_{k=1}^{p^{\alpha-1}} C^k_{p^{\alpha-1}} \sum_{\substack{j_1+\cdots+j_k=n \\ j_1,\cdots,j_k\geq 1}} a_{j_1} \cdots a_{j_k} \\ &= \sum_{k=1}^{p^{\alpha-1}} p^k C^k_{p^{\alpha-1}} \sum_{\substack{j_1+\cdots+j_k=n \\ j_1,\cdots,j_k\geq 1}} b_{j_1} \cdots b_{j_k} \end{aligned}$$

or pour tout $k = 1, \cdots, p^{\alpha-1}$ on a

$$v_p(p^k C^k_{p^{\alpha-1}}) = (\alpha - 1) + k - v_p(k) \geq \alpha$$

et donc

$$\sum_{i_1+\cdots+i_{p^{\alpha-1}}=n} a_{i_1} \cdots a_{i_{p^{\alpha-1}}} = 0$$

c'est-à-dire $f^{p^{\alpha-1}} = 1$.

Remarque : Dans la preuve de la proposition précédente on a, en particulier, démontré que le groupe $\mathbf{Tors}(\mathbf{P}(A))$ est d'exposant $\leq p^{\alpha-1+\beta}$ avec

$$p^\alpha = \mathrm{car}(A) \text{ et } \beta = \inf\{h \geq 1 / \ \forall x \in N,\ x^{p^h} \in pA\}$$

(Un majorant possible de β est alors g ($p^g = \sharp A$), compte tenu du fait que pour tout $a \in N$ on a $a^{p^g} = 0$.)

On peut donc, par la proposition 2, en déduire que $\mathbf{Tors}(\mathbf{P}(A))$ est un sous-groupe fermé de $\mathbf{P}(A)$ (fait que l'on aurait pu aussi remarquer à partir de la relation $\mathbf{Tors}(\mathbf{P}(A)) = 1 + T.N[[T]]$).

Théorème 7.— *Soit A un p-anneau commutatif unitaire fini. Le groupe $\mathbf{P}(A)$ est isomorphe en tant que groupe profini au produit direct $\mathbf{Tors}(\mathbf{P}(A)) \times \widehat{F}_\omega(\mathcal{C}_p^{ab})$.*

Preuve : La proposition 5 prouve que $\mathbf{Tors}(\mathbf{P}(A))$ est fermé dans $\mathbf{P}(A)$ et donc la propriété 1 prouve que $\mathbf{P}(A)$ est isomorphe à un produit $\widehat{F}_\alpha(\mathcal{C}_p^{ab}) \times \mathbf{Tors}(\mathbf{P}(A))$. Il s'agit donc de déterminer le cardinal α pour conclure.

On sait déjà que $\alpha \leq \aleph_0$. Considérons un idéal maximal M de A. Comme A est unitaire, $K = A/M$ est un corps fini. L'épimorphisme canonique $s : A \longrightarrow A/M$ induit un épimorphisme $A[[T]] \longrightarrow K[[T]]$ et, par suite, un épimorphisme continu $\tilde{s} : \mathbf{P}(A) \longrightarrow \mathbf{P}(K)$. Dans la section 3.1. on a vu que $\mathbf{P}(K) = \widehat{F}_\omega(\mathcal{C}_p^{ab})$ et donc que $\mathbf{P}(K)$ est sans torsion. Il s'ensuit que la restriction de $\tilde{s}$ à $\mathbf{Tors}(\mathbf{P}(A))$ est triviale et donc que $\tilde{s}$ induit un épimorphisme continu de $\widehat{F}_\alpha(\mathcal{C}_p^{ab})$ sur $\widehat{F}_\omega(\mathcal{C}_p^{ab})$. On en déduit que $\alpha \geq \aleph_0$ et, par suite, que $\alpha = \aleph_0$.

4.— Le groupe $\mathbf{Tors}(\mathbf{P}(A))$.

On vient de montrer que si A est un p-anneau commutatif unitaire fini alors le groupe $\mathbf{Tors}(\mathbf{P}(A))$ est un pro-p-groupe abélien d'exposant $p^{\alpha+g-1}$ où $p^\alpha = \mathrm{car}(A)$ et $p^g = \sharp A$. Le théorème de structure des groupes profinis abéliens de torsion (cf [RZ, p.136 theorem 4.3.8]) montre qu'il existe une suite $\lambda_1, \cdots, \lambda_{\alpha+g-1}$ de cardinaux au plus dénombrable dont au moins un est infini, telle que

$$\mathbf{Tors}(\mathbf{P}(A)) \simeq \prod_{i=1}^{\alpha+g-1} \left(\frac{\mathbf{Z}}{p^i\mathbf{Z}}\right)^{\lambda_i}$$

Nous avons, par ailleurs, aussi vu que

$$\mathbf{Tors}(\mathbf{P}(A)) = 1 + T.N[[T]]$$

(attention, écrire $1 + T.N[[T]] = \mathbf{P}(N)$ ne serait pas pertinent car N n'est pas unitaire!) et donc $\mathbf{Tors}(\mathbf{P}(A))$ s'identifie à la limite projective

$$\lim_{\longleftarrow} \frac{1 + T.N[[T]]}{1 + T^{n+1}.N[[T]]}$$

Il est donc assez naturel d'essayer de faire le lien entre le groupe $\mathbf{Tors}(\mathbf{P}(A)) = 1 + T.N[[T]]$ et le groupe N.

On note dans la suite $V_n = 1 + T^{n+1}.N[[T]]$, $\Gamma_n = 1 + T.N[[T]]/V_n$ et $F_n = \{1 + a_1T + \cdots + a_nT^n/\ a_1, \cdots, a_n \in N\}$ (qui est une classe de représentants de Γ_n dans $1 + T.N[[T]]$). L'épimorphisme de groupe $\varphi_n : \Gamma_{n+1} \longrightarrow \Gamma_n$ a pour noyau

$$\mathrm{Ker}(\varphi_n) = \left\{1 + aT^{n+1}/a \in N\right\} \simeq N$$

On est donc amené à comparer le système projectif $(\Gamma_n, \varphi_n)_n$ au système $(N^n, \pi_n)_n$ où $\pi_n : N^{n+1} \longrightarrow N^n$ est l'épimorphisme canonique qui "oublie" le dernier facteur du produit cartésien. Affirmer que ces deux systèmes projectifs sont isomorphes (c'est-à-dire affirmer pour tout $n \geq 1$ l'existence d'isomorphismes $\mu_n : \Gamma_n \longrightarrow N^n$ tels que le diagramme suivant

$$\begin{array}{ccc} \Gamma_{n+1} & \xrightarrow{\mu_{n+1}} & N^{n+1} \\ \Big\downarrow{\scriptstyle \varphi_n} & & \Big\downarrow{\scriptstyle \pi_n} \\ \Gamma_n & \xrightarrow{\mu_n} & N^n \end{array}$$

soit commutatif pour tout $n \geq 1$) revient à montrer que pour tout entier $n \geq 1$ et tout $f \in \Gamma_n$, il existe un relevé $\tilde{f}$ de f dans Γ_{n+1} de même ordre que f. La condition est visiblement nécessaire, elle est suffisante en vertu du lemme suivant :

Lemme 8.— *Soit* $1 \longrightarrow A \longrightarrow G \longrightarrow B \longrightarrow 1$ *une suite exacte de groupes abéliens finis. Les propositions suivantes sont équivalentes :*

i) la suite est scindée,

ii) tout élément x *de* B *admet un relevé dans* G *de même ordre que* x*.*

Preuve : *i)* $\Rightarrow$ *ii)* Evident.

ii) $\Rightarrow$ *i)* Soit $B = C_1 \oplus \cdots \oplus C_n$ une décomposition en sous-groupes cycliques de B et pour tout $i = 1, \cdots, n$ des éléments $x_i \in B$ tels que $< x_i >= C_i$. Notons $\tilde{x_i}$

un relevé de x_i dans G et $\widetilde{C_i} =< \tilde{x_i} >$. Les sous-groupes $\widetilde{C_i}$ sont alors en somme directe, car si $\alpha_1, \cdots, \alpha_n$ sont des entiers tels que

$$\tilde{x_1}^{\alpha_1} \cdots \tilde{x_n}^{\alpha_n} = e$$

alors

$$x_1^{\alpha_1} \cdots x_n^{\alpha_n} = e$$

et donc $x_i^{\alpha_i} = e$ pour tout $i = 1, \cdots, n$, mais comme x_i et $\tilde{x_i}$ sont de même ordre, on a $\tilde{x_i}^{\alpha_i} = e$. Le sous-groupe $\widetilde{C_1} \oplus \cdots \oplus \widetilde{C_n}$ permet alors de définir une section à la suite exacte.

On voit donc que si tout élément $f \in \Gamma_n$ se relève en un élément de $\mathbf{Tors}(\mathbf{P}(A))$ de même ordre, alors les systèmes projectifs $(\Gamma_n, \varphi_n)_n$ et $(N^n, \pi_n)_n$ sont isomorphes et donc que, par suite, on a

$$\mathbf{Tors}(\mathbf{P}(A)) \simeq \varprojlim \Gamma_n \simeq \varprojlim N^n \simeq N^{\aleph_0}$$

En toute généralité sur A, un élément $f \in \Gamma_n$ ne se relève pas forcément en un élément de $\mathbf{Tors}(\mathbf{P}(A))$ de même ordre. En effet, considérons par exemple l'anneau

$$A = \frac{\mathbf{F}_p[X]}{(X^{p+1})}$$

On voit que

$$N = A - A^* = \frac{X\mathbf{F}_p[X]}{(X^{p+1})} \simeq \left(\frac{\mathbf{Z}}{p\mathbf{Z}}\right)^p$$

Dans Γ_1, l'élément $f(T) = 1 + XT$ est d'ordre p. S'il existait un relevé de f dans Γ_p (de même ordre que f) alors il existerait des éléments $P_2(X), \cdots, P_p(X) \in N$ tels que $(f(T) + P_2(X)T^2 + \cdots + P_p(X)T^p)^p = 1$ dans Γ_p. Or, dans Γ_p, on a

$$\begin{array}{rcl} (f(T) + P_2(X)T^2 + \cdots + P_p(X)T^p)^p & = & f(T)^p + P_2^p(X)T^{2p} + \cdots + P_p^p(X)T^{p^2} \\ & = & 1 + X^pT^p \neq 1 \end{array}$$

Il existe donc des éléments d'ordre p^2 dans $\mathbf{Tors}(\mathbf{P}(A))$, ce qui montre bien que $\mathbf{Tors}(\mathbf{P}(A))$ ne peut être isomorphe à $N^{\aleph_0} \simeq (\mathbf{Z}/p)^{\aleph_0}$.

On a toutefois, pour le relèvement, la condition suffisante suivante :

Proposition 9.— *Si A est un p-anneau commutatif unitaire fini vérifiant la propriété*

$$(*) \quad \forall a \in N, \forall \alpha \geq 1,\ p^\alpha a = 0 \Longrightarrow \forall s = 0, \cdots, \alpha,\ p^{\alpha - s} a^{p^s} = 0$$

alors les systèmes projectifs $(\Gamma_n, \varphi_n)_n$ et $(N^n, \pi_n)_n$ sont isomorphes et, en particulier, on a

$$\mathbf{Tors}(\mathbf{P}(A)) \simeq N^{\aleph_0}$$

Preuve : Remarquons que si A satisfait $(*)$ alors pour tout $a \in N$, tout $\alpha \geq 1$ tel que $p^\alpha a = 0$ et tout $n \geq 1$ on a

$$(1 + aT^n)^{p^\alpha} = \sum_{k=0}^{p^\alpha} C_{p^\alpha}^k a^k T^{nk} = 1$$

car le lemme 6 permet d'assurer que pour tout $k = 1, \cdots, p^\alpha$ on a $C^k_{p^\alpha} a^k = mp^{\alpha - v_p(k)} a^k = 0$ $(m \geq 1)$.

Considérons $a_1, \cdots, a_h$ une base du $\mathbf{Z}$-module additif N. On sait que le noyau de l'épimorphisme canonique $\varphi_n : \Gamma_{n+1} \longrightarrow \Gamma_n$ est isomorphe à N. Plus exactement, on a

$$\mathrm{Ker}(\varphi_n) = < 1 + a_1 T^{n+1} > \oplus \cdots \oplus < 1 + a_h T^{n+1} >$$

Puisque l'élément $(1 + aT^n) \in \Gamma_n$ se relève à Γ_{n+1} en un élément de même ordre, l'argument utilisé dans le lemme 8 permet alors de montrer par récurrence que pour $n \geq 1$ on a la décomposition suivante :

$$\Gamma_n = \bigoplus_{i=1}^{i=h} < 1 + a_i T > \oplus \cdots \oplus \bigoplus_{i=1}^{i=h} < 1 + a_i T^n >$$

Cette décomposition fournit alors des isomorphismes $\mu_n : \Gamma_n \longrightarrow N^n$ qui font commuter les diagrammes.

La condition $(*)$ bien qu'*a priori* non nécéssaire couvre quand même une classe assez large d'anneaux. Elle englobe en particulier le cas des anneaux A vérifiant $\sqrt{\{0\}} = pA$, donc par exemple le cas des anneaux produits $\mathbf{Z}/p^{\alpha_1}\mathbf{Z} \times \cdots \times \mathbf{Z}/p^{\alpha_n}\mathbf{Z}$. Elle englobe aussi le cas d'anneaux A ne vérifiant pas $\sqrt{\{0\}} = pA$. Par exemple si l'on prend l'anneau $A = \dfrac{\mathbf{F}_p[X]}{(X^n)}$ avec $2 \leq n \leq p$ alors $N = A - A^*$ et donc $\sqrt{\{0\}} \neq pA$ et, pour tout $P \in N$, on a $P^p = 0$ ce qui justifie que A satisfait $(*)$.

En combinant les remarques de structure de l'introduction ainsi que les résultats établis précédemment, on trouve :

Théorème 10.— *Soit A un anneau commutatif unitaire fini et $N = \sqrt{\{0\}}$ son nilradical. Si A satisfait la condition*

$$\forall a \in N,\ \forall p \text{ premier},\ \forall \alpha \geq 1,\ p^\alpha a = 0 \Longrightarrow \forall s = 0, \cdots, \alpha,\ p^{\alpha - s} a^{p^s} = 0$$

alors on a

$$\mathbf{U}(A) \simeq A^* \times N^{\aleph_0} \times \left(\prod_{p \mid \sharp A} \mathbf{Z}_p \right)^{\aleph_0}$$

Par exemple, si $n = p_1^{\alpha_1}.\cdots.p_k^{\alpha_k}$ est la décomposition en facteurs premiers de l'entier n, on a :

$$\begin{aligned} \mathbf{U}(\mathbf{Z}/n\mathbf{Z}) &\simeq \left(\frac{\mathbf{Z}}{n\mathbf{Z}}\right)^* \times \left(\prod_{i=1}^{k} \frac{p_i \mathbf{Z}}{p_i^{\alpha_i}\mathbf{Z}} \right)^{\aleph_0} \times \left(\prod_{i=1}^{k} \mathbf{Z}_{p_i} \right)^{\aleph_0} \\ &\simeq \left(\frac{\mathbf{Z}}{n\mathbf{Z}}\right)^* \times \left(\frac{\mathbf{Z}}{m\mathbf{Z}}\right)^{\aleph_0} \times \left(\prod_{p \mid n} \mathbf{Z}_p \right)^{\aleph_0} \end{aligned}$$

où $m = \dfrac{n}{\prod_{p \mid n} p}$.

Bibliographie

[**FJ**] Mike Fried and Moshe Jarden, *Field arithmetic*, Ergeb. der Math. 11, Springer-Verlag (1985).

[**G**] K.W. Gruenberg, *Projective profinite groups*, Journal of London Math. Society 42, p. 155-165 (1967).

[**RZ**] Luis Ribes and Pavel Zalesskii, *Profinite groups*, Ergeb. der Math. 40, Springer (2000).

[**S**] Jean-Pierre Serre, *Cohomologie galoisienne*, Lect. note in math. 5, 5ème édition, Springer-Verlag (1994).

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