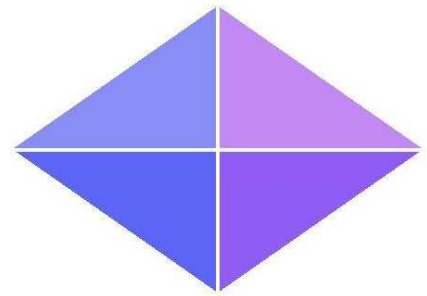


DFG-Forschergruppe
Regensburg/Freiburg

Algebraische Zyklen und
L-Funktionen



Problème inverse de Galois sur
quelques extensions de $\mathbb{Q}(T)$

Jérôme Poineau

Preprint Nr. 13/2008

PROBLÈME INVERSE DE GALOIS SUR QUELQUES EXTENSIONS DE $\mathbf{Q}(T)$

par

Jérôme Poineau

Résumé. — Nous présentons ici quelques résultats autour du problème inverse de Galois. Nous commençons par rappeler les résultats classiques selon lesquels tout groupe fini est groupe de Galois d’une extension de $\mathbf{C}(T)$ ou $\mathbf{Q}_p(T)$ et indiquons la stratégie mise en œuvre dans la démonstration. En utilisant une méthode similaire, nous proposons une nouvelle preuve, purement géométrique, dans le langage des espaces de Berkovich sur $\mathbf{Z}$, d’un résultat de D. Harbater assurant que tout groupe fini peut être réalisé comme groupe de Galois d’une extension d’un corps de séries arithmétiques convergentes, ainsi que quelques généralisations.

Dans le but que ce texte puisse être lu sans connaissances préalables, nous n’avons pas hésité à inclure rappels et détails.

Table des matières

Introduction	3
1. Stratégie de recollement	5
2. La droite de Berkovich sur $\mathbf{Z}$	9
2.1. Définitions	9
2.2. Dimension 0	10
2.3. Dimension 1	11
3. Démonstration du théorème 1	15
3.1. Construction locale de revêtements cycliques ..	15
3.2. Recollement	20

Classification mathématique par sujets (2000). — 12F12, 14G22, 14G25.

Mots clefs. — Problème inverse de Galois, espaces de Berkovich, séries arithmétiques convergentes.

3.3. Retour à l'algèbre	23
3.4. Généralisations	26
Références	29

Introduction

Le problème inverse de Galois consiste à montrer que tout groupe fini peut être réalisé comme groupe de Galois d'une extension du corps des nombres rationnels $\mathbf{Q}$. La simplicité de l'énoncé n'augure en rien de la difficulté de la question et sa réponse nous échappe encore à ce jour.

Une stratégie due à D. Hilbert consiste à chercher à réaliser, tout d'abord, un groupe fini G donné comme groupe de Galois d'une extension du corps $\mathbf{Q}(T)$. Ce second problème se prête à une approche géométrique. En effet, supposons que nous sachions construire un revêtement (ramifié) galoisien X de la droite projective $\mathbf{P}_{\mathbf{Q}}^1$ de groupe de Galois G . L'extension

$$\mathcal{M}(\mathbf{P}_{\mathbf{Q}}^1) = \mathbf{Q}(T) \rightarrow \mathcal{M}(X)$$

induite entre les corps de fonctions fournirait alors une réponse au problème. Fait remarquable, il est possible de spécialiser une telle extension en un nombre rationnel $T = t \in \mathbf{Q}$ de façon à obtenir une extension du corps $\mathbf{Q}$ dont le groupe de Galois est encore G . Ce dernier résultat est connu sous le nom de théorème d'irréductibilité de Hilbert (*cf.* [2], theorem 5.9.7).

Le problème précédent, dit problème inverse de Galois géométrique, présente également l'avantage d'admettre une généralisation en remplaçant le corps $\mathbf{Q}$ par n'importe quel autre corps. Signalons que ce n'est pas le cas du premier problème, dont l'énoncé tombe en défaut pour bon nombre de corps, ceux qui sont algébriquement clos ou finis, par exemple. Nous renvoyons le lecteur intéressé par ces problèmes et leurs généralisations au texte [3] de P. Dèbes.

Dans la section 1, nous nous intéresserons au problème inverse de Galois géométrique dans le cas du corps des nombres complexes $\mathbf{C}$ et rappellerons les grandes lignes d'une preuve classique. Nous mentionnons également le cas d'un corps valué complet arbitraire.

Le reste du texte est consacré à un résultat proche du problème inverse de Galois géométrique sur $\mathbf{Q}$. Pour tout $r \in \mathbf{R}_+$, notons $\mathbf{Z}_r\llbracket T \rrbracket$ l'anneau formé des séries en une variable à coefficients entiers dont le rayon de convergence complexe est supérieur ou égal à r . Dans l'article [8], D. Harbater énonce le résultat suivant (corollary 3.8) :

Théorème 1 (D. Harbater). — *Tout groupe fini est le groupe de Galois d'une extension du corps $\text{Frac}(\mathbf{Z}_1\llbracket T \rrbracket)$.*

Remarquons, dès à présent, que pour tout $r > 1$, l'anneau $\mathbf{Z}_{r-}\llbracket T \rrbracket$ est réduit à l'anneau de polynômes $\mathbf{Z}[T]$. Si nous disposions du théorème précédent pour un certain nombre réel $r > 1$, nous aurions donc résolu le problème inverse de Galois géométrique sur $\mathbf{Q}$.

La démonstration originale de ce résultat, aboutissement de la série d'articles [5], [6], [4] et [8], est ardue et technique ; elle basée sur des manipulations algébriques des anneaux de séries du type précédent. Nous en proposons une nouvelle, purement géométrique et remarquablement proche de la démonstration dans le cadre complexe. La seule difficulté réside dans le fait que le cadre géométrique adapté à ce problème est celui, fort naturel mais sans doute encore un peu exotique, des espaces de Berkovich sur $\mathbf{Z}$. Nous consacrons la section 2 à des rappels sur ces espaces et la section 3 à la démonstration annoncée.

La majeure partie de ce texte a été rédigée au cours de l'année que j'ai passée à l'université de Ratisbonne. Je souhaite remercier Klaus Künnemann, qui m'a permis d'y séjourner, pour son accueil et ses encouragements.

1. Stratégie de recollement

Commençons par nous intéresser au problème inverse de Galois géométrique sur le corps $\mathbf{C}$. Nous cherchons donc à construire un revêtement ramifié galoisien de $\mathbf{P}^1_{\mathbf{C}}$ ayant pour groupe de Galois un certain groupe fini fixé au préalable. En réalité, nous n'allons pas travailler avec la variété algébrique $\mathbf{P}^1_{\mathbf{C}}$, mais plutôt avec la variété analytique complexe $\mathbf{P}^1(\mathbf{C})$.

Considérons tout d'abord le cas des groupes cycliques. Soit $m \in \mathbf{N}^*$. Il est aisé de construire localement un revêtement galoisien de groupe $\mathbf{Z}/k\mathbf{Z}$. En effet, choisissons un point P de $\mathbf{P}^1(\mathbf{C})$, z une coordonnée locale au voisinage de ce point et D_P un disque ouvert centré en P sur lequel elle est définie. Considérons le revêtement X_P du disque D_P donné par l'équation

$$t^k = z.$$

Il vérifie les propriétés attendues. En outre, il est connexe, lisse et trivial au-dessus du complémentaire du point P . Remarquons que, pour déterminer le groupe de Galois, nous avons utilisé le fait que le corps $\mathbf{C}$ contienne exactement k racines $k^{\text{èmes}}$ de l'unité.

Nous allons maintenant recoller des revêtement du type précédent afin d'en construire qui possèdent d'autres groupes de Galois. Fixons un groupe fini G . Notons n son ordre et $g_1, \dots, g_n$ ses éléments. Soit $i \in \llbracket 1, n \rrbracket$. Notons n_i l'ordre de l'élément g_i dans le groupe G et $d_i = n/n_i$. Choisissons des représentants $h_{i,0}, \dots, h_{i,d_i-1}$ des éléments du quotient $G/\langle g_i \rangle$ dans G . Choisissons un point P_i de $\mathbf{P}^1(\mathbf{C})$ et construisons un revêtement X_{P_i} au-dessus d'un disque D_{P_i} comme précédemment. Indexons les feuilles de ce revêtement par les entiers de 0 à n_i-1 de façon compatible avec l'action du groupe $\mathbf{Z}/n_i\mathbf{Z}$. Considérons, à présent, d_i copies de X_{P_i} indexées par les entiers de 0 à $d_i - 1$. Notons Y_{P_i} le revêtement de D_{P_i} ainsi obtenu.

Notons D' le complémentaire des points $P_1, \dots, P_n$ dans $\mathbf{P}^1(\mathbf{C})$ et Y' le revêtement trivial à n feuillets au-dessus de D' . Indexons ces feuillets par les éléments du groupe G . Nous allons, maintenant, recoller les revêtements précédents. Nous supposons que les disques D_{P_i} , avec $i \in \llbracket 1, n \rrbracket$, sont deux à deux disjoints. Nous pouvons facilement nous ramener à ce cas en les réduisant, si besoin est. Soit $i \in \llbracket 1, n \rrbracket$. Au-dessus de $D_{P_i} \cap D'$, nous recollons la feuille indexée par l'élément k de la copie de X_{P_i} indexée par l du revêtement Y_{P_i} avec la feuille indexée par l'élément $a_{i,l}g_i^k$ du revêtement Y' (cf. figure 1). Nous obtenons ainsi

un revêtement Y de $\mathbf{P}^1(\mathbf{C})$ dont on vérifie facilement qu'il est connexe, lisse et galoisien de groupe G .

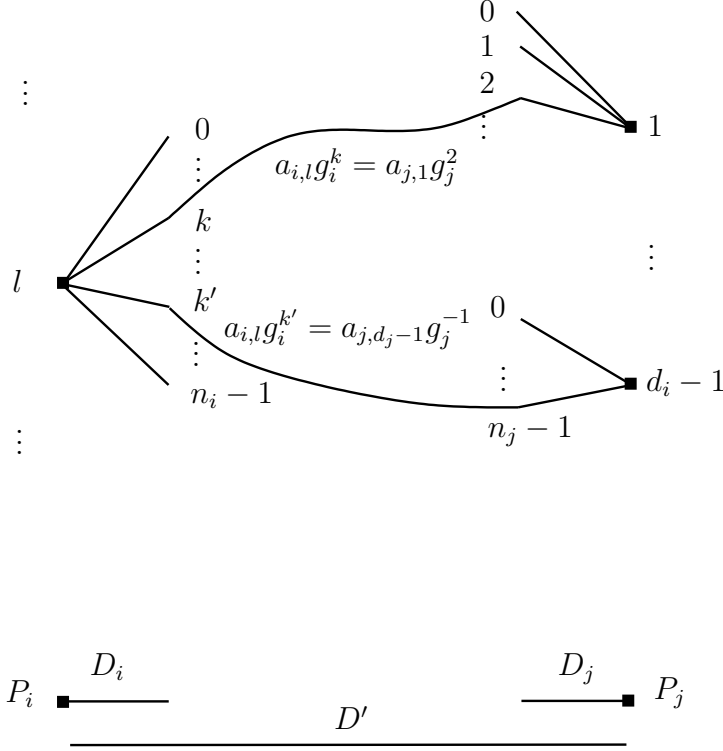


FIG. 1. Recollement de revêtements cycliques.

Ainsi avons-nous obtenu une variété analytique complexe Y vérifiant les propriétés requises. Il nous reste à montrer que c'est, en réalité, une variété algébrique. Ce résultat découle du théorème d'existence de B. Riemann ou, si l'on veut, des théorèmes GAGA de J.-P. Serre. Nous avons finalement obtenu le résultat suivant :

Théorème 1.1. — *Tout groupe fini est groupe de Galois d'une extension du corps $\mathbf{C}(T)$.*

Pour résumer, rappelons en quelques mots la stratégie de la preuve :

1. Construire des revêtements cycliques sur de petits ouverts.
2. Recoller les revêtements précédents.
3. Montrer que l'extension induite sur les corps de fonctions est algébrique.

Elle est due à D. Harbater, qui l'a développée dans plusieurs contextes et utilisée pour démontrer de nombreux résultats. Nous renvoyons le lecteur désireux d'en savoir plus au texte [9], où il trouvera une introduction élémentaire au sujet comme les détails des résultats les plus poussés.

La simplicité de la stratégie d'Harbater invite à l'appliquer dans de nombreux contextes géométriques, pour peu que l'on dispose d'une bonne notion de « petits ouverts » et de théorèmes d'algébricité du type GAGA. Ce n'est pas le cas de la géométrie algébrique, où deux ouverts non-vides de la droite projective se coupent toujours, interdisant d'utiliser les techniques précédentes. Ce devrait, en revanche, être le cas de toute géométrie analytique raisonnable. L'on peut ainsi obtenir le théorème suivant.

Théorème 1.2. — *Soit K un corps muni d'une valeur absolue ultramétrique non-triviale pour laquelle il est complet. Tout groupe fini est groupe de Galois d'une extension du corps $K(T)$. L'extension peut être choisie régulière, c'est-à-dire que le corps K y est algébriquement fermé.*

La démonstration originale est due à D. Harbater (cf. [7]) ; elle est écrite dans le cadre de la géométrie formelle et s'écarte un peu de la stratégie précédente (le recollement se fait à l'aide de « mock covers »). Il existe également une preuve dans le cadre de la géométrie rigide, rédigée par Q. Liu dans [10] en suivant une idée de J.-P. Serre, qui suit de très près la stratégie indiquée. Signalons, cependant, que l'absence, en général, de racines primitives de l'unité de tout ordre complique la première étape.

Dans ce qui suit, nous allons appliquer la stratégie de recollement dans le cadre des espaces de Berkovich sur $\mathbf{Z}$ afin de démontrer le théorème 1.

2. La droite de Berkovich sur $\mathbf{Z}$

Dans cette section, nous présentons succinctement la droite de Berkovich sur $\mathbf{Z}$. Nous en donnons une description rapide et nous concentrons sur les propriétés dont nous aurons besoin par la suite. Nous invitons le lecteur dont ces prémices auront éveillé la curiosité à parcourir l'ouvrage [11] pour de ce vaste et passionnant sujet.

2.1. Définitions

Commençons par rappeler la définition d'espace affine analytique sur $\mathbf{Z}$. Elle est due à V. Berkovich (*cf.* [1], §1.5). Soit $n \in \mathbf{N}$. L'espace affine analytique de dimension n sur $\mathbf{Z}$, noté $\mathbf{A}_{\mathbf{Z}}^{n,\text{an}}$, est l'ensemble des semi-normes multiplicatives sur $\mathbf{Z}[T_1, \dots, T_n]$, c'est-à-dire l'ensemble des applications

$$|\cdot| : \mathbf{Z}[T_1, \dots, T_n] \rightarrow \mathbf{R}_+$$

qui vérifient les propriétés suivantes :

- i) $|0| = 0$ et $|1| = 1$;
- ii) $\forall P, Q \in \mathbf{Z}[T_1, \dots, T_n], |P + Q| \leq |P| + |Q|$;
- iii) $\forall P, Q \in \mathbf{Z}[T_1, \dots, T_n], |PQ| = |P||Q|$.

Soit x un point de $\mathbf{A}_{\mathbf{Z}}^{n,\text{an}}$. Il lui est associé une semi-norme multiplicative $|\cdot|_x$ sur $\mathbf{Z}[T_1, \dots, T_n]$. L'ensemble $\mathfrak{p}_x$ des éléments sur lesquels elle s'annule est un idéal premier de $\mathbf{Z}[T_1, \dots, T_n]$. Le quotient est un anneau intègre sur lequel la semi-norme $|\cdot|_x$ induit une valeur absolue. Nous noterons $\mathcal{H}(x)$ le complété du corps des fractions de cet anneau pour cette valeur absolue. Nous noterons simplement $|\cdot|$ la valeur absolue sur le corps $\mathcal{H}(x)$, cela n'entraînant pas de confusion. La construction fournit un morphisme

$$\mathbf{Z}[T_1, \dots, T_n] \rightarrow \mathcal{H}(x).$$

L'image d'un élément P de $\mathbf{Z}[T_1, \dots, T_n]$ par ce morphisme sera notée $P(x)$. Avec ces notations, nous avons donc $|P(x)| = |P|_x$.

Munissons, à présent, l'espace analytique $\mathbf{A}_{\mathbf{Z}}^{n,\text{an}}$ d'une topologie : celle engendrée par les ensembles de la forme

$$\{x \in \mathbf{A}_{\mathbf{Z}}^{n,\text{an}} \mid r < |P(x)| < s\},$$

pour $P \in \mathbf{Z}[T_1, \dots, T_n]$ et $r, s \in \mathbf{R}$.

Pour finir, nous définissons un faisceau d'anneaux $\mathcal{O}$ sur $\mathbf{A}_{\mathbf{Z}}^{n,\text{an}}$ de la façon suivante : pour tout ouvert U de $\mathbf{A}_{\mathbf{Z}}^{n,\text{an}}$, l'anneau $\mathcal{O}(U)$ est constitué des applications

$$f : U \rightarrow \bigsqcup_{x \in U} \mathcal{H}(x)$$

qui vérifient les deux conditions suivantes :

- i) $\forall x \in U, f(x) \in \mathcal{H}(x)$;
- ii) f est localement limite uniforme de fractions rationnelles sans pôles.

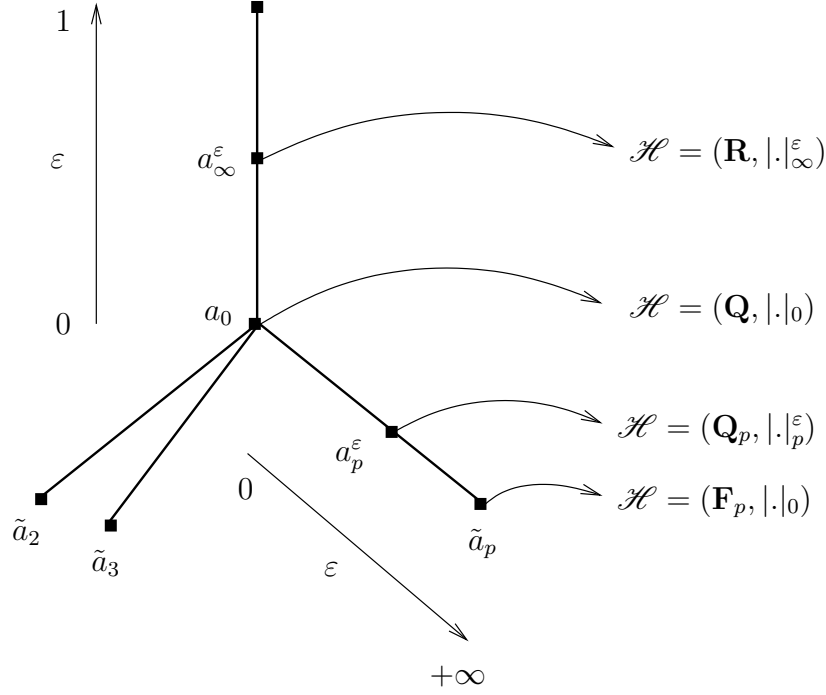
2.2. Dimension 0

Afin de rendre plus palpables les définitions précédentes, nous allons décrire explicitement l'espace $\mathbf{A}_0^{\text{an}}\mathbf{Z}$, l'espace affine analytique de dimension 0 sur $\mathbf{Z}$, que nous noterons plus volontiers $\mathcal{M}(\mathbf{Z})$. Nous noterons $|\cdot|_{\infty}$ la valeur absolue usuelle et, pour tout nombre premier p , $|\cdot|_p$ la valeur absolue p -adique usuelle. Du théorème d'Ostrowski, l'on déduit que les points de $\mathcal{M}(\mathbf{Z})$ sont exactement

- i) la valeur absolue triviale $|\cdot|_0$ (nous noterons a_0 le point associé) ;
- ii) les valeurs absolues archimédiennes $|\cdot|_{\infty}^{\varepsilon}$ (nous noterons a_{∞}^{ε} le point associé), avec $\varepsilon \in]0, 1]$;
- iii) pour tout nombre premier p , les valeurs absolues p -adiques $|\cdot|_p^{\varepsilon}$ (nous noterons a_{∞}^{ε} le point associé), avec $\varepsilon \in]0, +\infty[$;
- iv) pour tout nombre premier p , la semi-norme $|\cdot|_p^{+\infty}$ induite par la valeur absolue triviale sur $\mathbf{F}_p$ (nous noterons $\tilde{a}_p$ le point associé).

Topologiquement, nous disposons également d'une description explicite. Tout d'abord, chacune des branches tracée sur la figure 2 est homéomorphe à un segment réel. Il nous reste à décrire les voisinages du point central a_0 : ce sont les parties qui contiennent entièrement toutes les branches à l'exception d'un nombre fini, et qui contiennent un voisinage de a_0 dans chacune des branches restantes. Si l'on préfère, l'espace $\mathcal{M}(\mathbf{Z})$ a la topologie du compactifié d'Alexandrov de la réunion disjointe de ses branches privées de a_0 , le point a_0 jouant le rôle du point à l'infini.

Nous pouvons également décrire explicitement les sections du faisceau structural sur les ouverts de $\mathcal{M}(\mathbf{Z})$. Nous avons représenté les différents cas à la figure 3.

FIG. 2. L'espace $\mathcal{M}(\mathbf{Z})$.

2.3. Dimension 1

Venons-en, à présent, à l'espace affine analytique de dimension 1 sur $\mathbf{Z}$. Nous noterons T la coordonnée sur cet espace. Remarquons, tout d'abord, que le morphisme $\mathbf{Z} \rightarrow \mathbf{Z}[T]$ induit un morphisme de projection

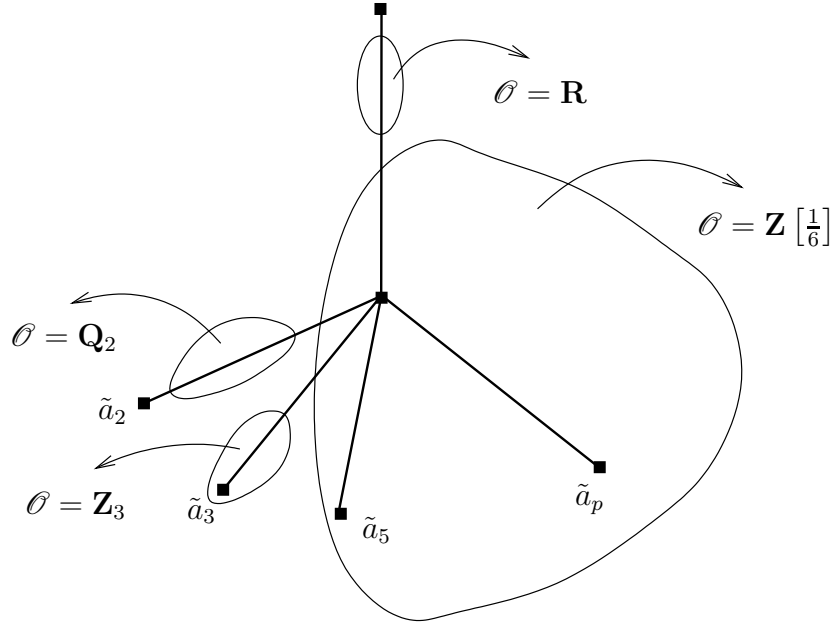
$$\pi : \mathbf{A}_{\mathbf{Z}}^{1,\text{an}} \rightarrow \mathcal{M}(\mathbf{Z}).$$

Cela nous permet d'obtenir une description topologique de la droite de Berkovich sur $\mathbf{Z}$: la fibre de π au-dessus d'un point x de $\mathcal{M}(\mathbf{Z})$ est isomorphe à la droite de Berkovich sur le corps $\mathcal{H}(x)$. Si $\mathcal{H}(x) = \mathbf{R}$, cette droite est isomorphe au quotient de l'espace $\mathbf{C}$ par la conjugaison complexe. Nous ne chercherons pas à obtenir de description plus précise et nous contenterons d'indiquer quelques propriétés (cf. [11], théorèmes 4.4.1 et 4.5.5).

Théorème 2.1. — *i) L'espace $\mathbf{A}_{\mathbf{Z}}^{1,\text{an}}$ est localement compact, métrisable et de dimension topologique 3.*

ii) L'espace $\mathbf{A}_{\mathbf{Z}}^{1,\text{an}}$ est localement connexe par arcs.

iii) Le morphisme de projection $\pi : \mathbf{A}_{\mathbf{Z}}^{1,\text{an}} \rightarrow \mathcal{M}(\mathbf{Z})$ est ouvert.

FIG. 3. Le faisceau structural sur $\mathcal{M}(\mathbf{Z})$.

- iv) En tout point x de $\mathbf{A}_{\mathbf{Z}}^{1,\text{an}}$, l'anneau local $\mathcal{O}_x$ est hensélien, noethérien, régulier, de dimension inférieure à 2 et le corps résiduel $\kappa(x)$ est hensélien.
- v) Le faisceau structural $\mathcal{O}$ est cohérent.

Dans la section qui suit, nous aurons besoin d'autres propriétés liées au principe du prolongement analytique (cf. [11] théorèmes 4.4.2 et 7.1.9, corollaire 4.4.5).

Théorème 2.2. — Soit U une partie connexe de $\mathbf{A}_{\mathbf{Z}}^{1,\text{an}}$.

- i) Le principe du prolongement analytique vaut sur U . En particulier, l'anneau $\mathcal{O}(U)$ est intègre.
- ii) L'anneau des sections méromorphes $\mathcal{M}(U)$ est un corps.
- iii) Si U est de Stein, le morphisme naturel $\text{Frac}(\mathcal{O}(U)) \rightarrow \mathcal{M}(U)$ est un isomorphisme.

Rappelons ici ce que nous entendons par espace de Stein. Nous dirons qu'un espace localement annelé $(X, \mathcal{O}_X)$ est de Stein s'il satisfait les conclusions des théorèmes de H. Cartan :

- A) pour tout faisceau de $\mathcal{O}_X$ -modules cohérent $\mathcal{F}$ et tout point x de X , la fibre $\mathcal{F}_x$ est engendrée par l'ensemble des sections globales $\mathcal{F}(X)$;

B) pour tout faisceau de $\mathcal{O}_X$ -modules cohérent $\mathcal{F}$ et tout entier $q \in \mathbf{N}^*$, nous avons $H^q(X, \mathcal{F}) = 0$.

Donnons quelques exemples de sous-espaces de la droite analytique $\mathbf{A}_{\mathbf{Z}}^{1,\text{an}}$ qui sont des espaces de Stein (cf. [11], théorème 6.6.29).

Théorème 2.3. — *Soient V une partie ouverte et connexe de l'espace $\mathcal{M}(\mathbf{Z})$ et $s, t \in \mathbf{R}$. Les parties suivantes de la droite analytique $\mathbf{A}_{\mathbf{Z}}^{1,\text{an}}$ sont des espaces de Stein :*

- i) $\{x \in \pi^{-1}(V) \mid s < |T(x)| < t\}$;
- ii) $\{x \in \pi^{-1}(V) \mid |T(x)| > s\}$.

Pour terminer, disons quelques mots des sections globales sur les parties de la droite analytique $\mathbf{A}_{\mathbf{Z}}^{1,\text{an}}$. Sur les disques, elles s'expriment essentiellement en termes de séries dont les coefficients sont des fonctions sur $\mathcal{M}(\mathbf{Z})$. Considérons, par exemple, le disque ouvert relatif de rayon 1 :

$$\mathbf{D} = \left\{ x \in \mathbf{A}_{\mathbf{Z}}^{1,\text{an}} \mid |T(x)| < 1 \right\}.$$

Le morphisme naturel $\mathbf{Z}[T] \rightarrow \mathcal{O}(\mathbf{D})$ induit un isomorphisme

$$\mathbf{Z}_1\text{-}[T] \xrightarrow{\sim} \mathcal{O}(\mathbf{D}),$$

où $\mathbf{Z}_1\text{-}[T]$ désigne l'anneau constitué des séries de la forme

$$\sum_{i \geq 0} a_i T^i \in \mathbf{Z}[[T]]$$

telles que le rayon de convergence de la série

$$\sum_{i \geq 0} |a_i|_{\infty} T^i$$

soit supérieur à 1. On déduit cette description du théorème 3.2.16 de [11].

À partir de la description des anneaux de sections sur les disques, nous pouvons en déduire celle des anneaux locaux en certains points. Nous nous contenterons de deux exemples. Soit p un nombre premier. Notons z_p le point 0 de la fibre de π au-dessus du point $\tilde{a}_p$. D'après le corollaire 3.2.5 de [11], le morphisme naturel $\mathbf{Z}[T] \rightarrow \mathcal{O}_{z_p}$ induit un isomorphisme

$$\mathbf{Z}_p\text{-}[T] \xrightarrow{\sim} \mathcal{O}_{z_p}.$$

Notons z_0 le point 0 de la fibre de π au-dessus du point a_0 . D'après le corollaire 3.2.8 de [11], le morphisme naturel $\mathbf{Z}[T] \rightarrow \mathcal{O}_{z_0}$ induit un isomorphisme

$$E \xrightarrow{\sim} \mathcal{O}_{z_0},$$

où E désigne l'anneau constitué des éléments f de $\mathbf{Q}[[T]]$ qui vérifient les propriétés suivantes :

- i)* $\exists a \in \mathbf{N}^*, f(aT) \in \mathbf{Z}[[T]]$;
- ii)* le rayon de convergence complexe de la série f est strictement positif ;
- iii)* pour tout nombre premier p , le rayon de convergence p -adique de la série f est strictement positif.

3. Démonstration du théorème 1

Nous allons maintenant appliquer la stratégie de recollement décrite à la section 1 dans le cadre des espaces de Berkovich sur $\mathbf{Z}$ afin de démontrer le théorème 1. Plus précisément, un groupe fini G étant donné, nous allons construire un revêtement galoisien de groupe G du disque

$$\mathbf{D} = \left\{ x \in \mathbf{A}_{\mathbf{Z}}^{1,\text{an}} \mid |T(x)| < 1 \right\}.$$

Cela indique que la troisième étape de notre démonstration différera fondamentalement de la troisième étape de la démonstration du cas complexe. En effet, le disque $\mathbf{D}$ est un espace affine et non plus projectif comme l'était $\mathbf{P}^1(\mathbf{C})$. En particulier, les théorèmes GAGA n'y sont pas valables. Nous utiliserons à leur place le caractère Stein du disque $\mathbf{D}$ afin de terminer la démonstration.

Mentionnons, pour finir, que nous allons en fait construire des faisceaux d'algèbres cohérents ayant pour groupe d'automorphismes un groupe fini prescrit. Bien entendu, ces faisceaux sont les images directes de faisceaux structuraux de revêtements ramifiés de la droite analytique sur $\mathbf{Z}$ et il y aurait tout intérêt à mener plutôt nos constructions dans ce langage. Nous nous en abstenons uniquement parce qu'aucune référence concernant ces espaces n'est disponible. Nous indiquerons cependant en remarque les traductions dans ce cadre ; elles sont immédiates pour qui dispose d'une bonne théorie des courbes analytiques sur $\mathbf{Z}$.

Nous noterons $X = \mathbf{A}_{\mathbf{Z}}^{1,\text{an}}$ et, pour tout nombre premier p ,

$$\begin{aligned} \mathbf{D}_p &= \mathbf{D} \cap \pi^{-1}([a_0, \tilde{a}_p]), \\ \mathbf{D}'_p &= \mathbf{D} \cap \pi^{-1}(]a_0, \tilde{a}_p]), \\ \text{et } \mathbf{D}''_p &= \mathbf{D} \cap \pi^{-1}(]a_0, \tilde{a}_p[). \end{aligned}$$

Ces trois parties sont connexes.

3.1. Construction locale de revêtements cycliques

Dans le cas complexe, la construction locale était particulièrement simple car nous disposions de racines primitives de l'unité de tout ordre. Elle ne sera guère plus difficile ici puisque, comme nous allons l'expliquer, un entier n étant donné, il existe toujours une branche de $\mathcal{M}(\mathbf{Z})$, et même une infinité, sur laquelle existe une racine primitive $n^{\text{ème}}$ de l'unité.

Soient V une partie ouverte de X et P un polynôme unitaire à coefficients dans $\mathcal{O}(V)$. Notons n son degré. On définit un préfaisceau $\mathcal{F}_P$ sur V en posant,

pour toute partie ouverte U de V ,

$$\mathcal{F}_P(U) = \mathcal{O}(U)[S]/(P(S))$$

et en utilisant les morphismes de restriction induits par ceux du faisceau $\mathcal{O}$.

Lemme 3.1. — *Le préfaisceau $\mathcal{F}_P$ est un faisceau de $\mathcal{O}_V$ -algèbres cohérent.*

Démonstration. — On constate immédiatement que le préfaisceau $\mathcal{F}_P$ est un préfaisceau de $\mathcal{O}_V$ -algèbres. Il nous suffit donc de montrer que c'est un faisceau et un faisceau de $\mathcal{O}_V$ -modules cohérent. Puisque le polynôme P est unitaire, le morphisme de $\mathcal{O}_V$ -modules

$$\begin{aligned} \mathcal{O}_V^n &\rightarrow \mathcal{F} \\ (a_0, \dots, a_{n-1}) &\mapsto \sum_{i=0}^{n-1} a_i S^i \end{aligned}$$

est un isomorphisme. On en déduit que le préfaisceau $\mathcal{F}$ est un faisceau, puis qu'il est cohérent, car le faisceau structural $\mathcal{O}$ l'est, en vertu du théorème 2.1. $\square$

Remarque 3.2. — Le faisceau $\mathcal{F}_P$ est l'image directe du faisceau structural d'une courbe analytique sur $\mathbf{Z}$. Celle-ci nous est donnée comme un revêtement ramifié, de degré inférieur à n , de la partie V de la droite analytique $\mathbf{A}_{\mathbf{Z}}^{1,\text{an}}$.

Nous allons, à présent, restreindre notre étude aux faisceaux $\mathcal{F}_P$ pour une classe de polynômes P particuliers. Soient n un entier supérieur à 1 et p un nombre premier congru à 1 modulo n . Posons

$$Q(S) = S^n - p^n - T \in \mathcal{O}(\mathbf{D}_p'')[S].$$

Le résultat du lemme suivant donne la raison du choix des entiers n et p .

Lemme 3.3. — *L'anneau $\mathbf{Z}_p$ contient n racines $n^{\text{èmes}}$ de l'unité.*

Démonstration. — Il suffit de montrer que le polynôme $U^n - 1$ possède n racines dans $\mathbf{Z}_p$. Le groupe multiplicatif $\mathbf{F}_p^*$ du corps résiduel $\mathbf{F}_p$ de $\mathbf{Z}_p$ est cyclique et d'ordre $p - 1$. Puisque n divise $p - 1$, le groupe $\mathbf{F}_p^*$ contient un élément d'ordre exactement n et le polynôme $U^n - 1$ est scindé à racines simples sur $\mathbf{F}_p$. Le lemme de Hensel assure qu'il l'est encore sur $\mathbf{Z}_p$. $\square$

Pour tout entier positif i et tout nombre rationnel k , posons

$$C_k^i = \frac{k(k-1) \cdots (k-i+1)}{i!} \in \mathbf{Q}.$$

Rappelons que nous avons l'égalité

$$\left(\sum_{i \geq 0} C_{1/n}^i Z^i \right)^n = 1 + Z \text{ dans } \mathbf{Q}[[Z]].$$

Lemme 3.4. — *Pour tout élément x de $\mathbf{D}'_p$ et tout entier positif i , nous avons*

$$\left| C_{1/n}^i(x) \right| \leq 1.$$

Démonstration. — Soient x un élément de $\mathbf{D}'_p$ et i un entier positif. Notons $|\cdot|_x$ la valeur absolue sur le corps $\mathcal{H}(x)$. Remarquons que l'application

$$C_k^i : \mathbf{Q} \rightarrow \mathbf{Q}$$

est polynomiale, et donc continue lorsque l'on munit le corps $\mathbf{Q}$ de la valeur absolue $|\cdot|_x$. Nous savons que, pour tout entier l , l'élément C_l^i est entier. Il vérifie donc l'inégalité

$$\left| C_l^i \right|_x \leq 1,$$

puisque la valeur absolue $|\cdot|_x$ est ultramétrique. En outre, le nombre premier p ne divise pas l'entier n . Par conséquent, le nombre rationnel $1/n$ appartient à $\mathbf{Z}_p$ et il est donc limite d'éléments de $\mathbf{Z}$ pour la valeur absolue $|\cdot|_x$. On en déduit le résultat voulu. $\square$

Fixons ζ une racine primitive $n^{\text{ème}}$ de l'unité. Notons τ la permutation cyclique $(1\ 2\ \cdots\ n)$ de l'ensemble $\llbracket 1, n \rrbracket$. Posons

$$U = \{x \in D'_p \mid |T(x)| < |p(x)|^n\}.$$

Proposition 3.5. — *Il existe un isomorphisme de $\mathcal{O}_U$ -algèbres*

$$\varphi : \mathcal{F}_Q \rightarrow \mathcal{O}^n$$

tel que, pour tout ouvert V de U et tout élément s de $\mathcal{F}(V)$, nous ayons

$$\varphi(\zeta s) = \tau(\varphi(s)).$$

Démonstration. — Considérons la fonction

$$f = p^{-n} T$$

définie sur X'_p . Pour tout élément r de $]0, 1[$, considérons la partie V_r de $\mathbf{D}'_p$ définie par

$$V_r = \{x \in \mathbf{D}'_p \mid |T(x)| \leq r|p(x)|^n\}.$$

Pour tout élément x de V_r et tous entiers $a \geq 0$ et $b \geq a$, nous avons

$$\left| \sum_{i=a}^b C_{1/n}(x)^i f(x)^i \right| \leq r^a.$$

On en déduit que la série $\sum_{i \geq 0} C_{1/n}^i f^i$ converge uniformément sur V_r . Puisque tout point de U possède un voisinage de la forme V_r , pour un certain élément r

de $]0, 1[$, la série $\sum_{i \geq 0} C_{1/n}^i f^i$ définit une fonction g sur U . Cette fonction vérifie l'égalité

$$g^n = 1 + f = 1 + p^{-n} T \text{ dans } \mathcal{O}(U).$$

On en déduit que nous avons l'égalité

$$Q(S) = S^n - p^n - T = \prod_{j=0}^n (S - p\zeta^j g) \text{ dans } \mathcal{O}(U)[S].$$

Par conséquent, le morphisme

$$\begin{array}{ccc} \mathcal{F}_Q & \rightarrow & \mathcal{O}^n \\ F(S) & \mapsto & (F(pg), F(p\zeta^{-1}g), \dots, F(p\zeta^{-(n-1)}g)) \end{array}$$

est un isomorphisme. On vérifie immédiatement qu'il satisfait la condition requise. $\square$

Remarque 3.6. — La première partie du résultat signifie que le revêtement associé au faisceau $\mathcal{F}_Q$ est trivial au-dessus de l'ouvert U . La seconde assure que le groupe $\langle \zeta \rangle \simeq \mathbf{Z}/n\mathbf{Z}$ agit sur le revêtement par une permutation cyclique des feuillets du lieu trivial.

Lemme 3.7. — *Le polynôme $Q(S) = S^n - p^n - T$ est irréductible sur le corps $\text{Frac}(\mathcal{O}(\mathbf{D}_p''))$. En particulier, l'anneau $\mathcal{F}_Q(\mathbf{D}_p'')$ est intègre.*

Démonstration. — Notons z_p le point 0 de la fibre $\pi^{-1}(\tilde{a}_p)$. D'après la discussion menée à la fin de la section 2, l'anneau local en ce point est isomorphe à l'anneau $\mathbf{Z}_p[[T]]$. Montrons que le polynôme $Q(S)$ est irréductible sur son corps des fractions $\mathbf{Q}_p((T))$. En effet, il n'y a aucune racine, pour des raisons de valuation T -adique, est séparable et le groupe de Galois de son extension de décomposition agit transitivement sur ses racines.

D'après le principe du prolongement analytique (*cf.* théorème 2.2), le morphisme naturel $\mathcal{O}(\mathbf{D}_p'') \rightarrow \mathcal{O}_{z_p}$ est injectif. Par conséquent, le corps $\text{Frac}(\mathcal{O}(\mathbf{D}_p''))$ est un sous-corps de $\mathbf{Q}_p((T))$. On en déduit que le polynôme $Q(S)$ est irréductible sur le corps $\text{Frac}(\mathcal{O}(\mathbf{D}_p''))$.

Puisque le polynôme $Q(S)$ est unitaire, l'unicité de la division euclidienne assure que le morphisme

$$\mathcal{O}(\mathbf{D}_p'')[S]/(Q(S)) \rightarrow \text{Frac}(\mathcal{O}(\mathbf{D}_p''))[S]/(Q(S))$$

est injectif. Puisque l'anneau au but est intègre, celui à la source, qui n'est autre que l'anneau $\mathcal{F}_Q(\mathbf{D}_p'')$, l'est également. $\square$

Remarque 3.8. — Ce résultat signifie que la courbe associée au faisceau $\mathcal{F}_Q$ est intègre, c'est-à-dire réduite et irréductible.

Nous pouvons être encore plus précis.

Lemme 3.9. — *Soient x un point de U et i un élément de $\llbracket 1, n \rrbracket$. Le morphisme*

$$\rho : \mathcal{F}_Q(\mathbf{D}_p'') \rightarrow \mathcal{F}_x \xrightarrow[\sim]{\varphi_x} \mathcal{O}_x^n \xrightarrow{p_i} \mathcal{O}_x,$$

où p_i est la projection sur le $i^{\text{ème}}$ facteur, est injectif.

Démonstration. — Soit s un élément de l'anneau $\mathcal{F}_Q(\mathbf{D}_p'') = \mathcal{O}(\mathbf{D}_p'')/(Q(S))$ dont l'image par le morphisme ρ est nulle. Choisissons un élément $F(S)$ de $\mathcal{O}(\mathbf{D}_p'')[S]$ qui représente la section s . Reprenons les notations de la preuve de la proposition 3.5. Par hypothèse, nous avons

$$R(p\zeta^{-i}g) = 0 \text{ dans } \mathcal{O}_x.$$

Pour montrer que l'élément s est nul, il suffit de montrer que le polynôme $Q(S)$ est le polynôme minimal de l'élément $p\zeta^{-i}g$ sur le corps $\text{Frac}(\mathcal{O}(\mathbf{D}_p''))$. C'est bien le cas, puisque le lemme précédent assure que le polynôme Q est irréductible sur le corps $\text{Frac}(\mathcal{O}(\mathbf{D}_p''))$. $\square$

Remarque 3.10. — Ce résultat est une sorte de principe du prolongement analytique sur la courbe associée au faisceau $\mathcal{F}_Q$: si une fonction holomorphe sur la courbe est nulle au voisinage d'un point de l'un des feuillettes du revêtement, alors elle est nulle partout. On attend que ce principe vaille pour toute courbe irréductible.

Terminons par un résultat topologique.

Lemme 3.11. — *La partie*

$$F = \mathbf{D}_p'' \setminus U = \{x \in \mathbf{D}_p'' \mid |T(x)| \geq |p(x)|^n\}$$

est fermée dans le disque $\mathbf{D}$.

Démonstration. — Il suffit de montrer que F est fermée dans $\mathbf{D}_p$ puisque cette dernière partie est elle-même fermée dans $\mathbf{D}$. En d'autres termes, nous souhaitons montrer que la partie

$$V = U \cup (\mathbf{D} \cap \pi^{-1}(a_0))$$

est ouverte dans $\mathbf{D}_p$. Puisque U est une partie ouverte de $\mathbf{D}_p$, il suffit de montrer que V est voisinage dans $\mathbf{D}_p$ de chacun des points de $\mathbf{D} \cap \pi^{-1}(a_0)$.

Soit x un point de $\mathbf{D} \cap \pi^{-1}(a_0)$. Posons $r = |T(x)|$. C'est un élément de l'intervalle $]0, 1[$. Soient s un élément de $]r, 1[$ et ε un élément de $]0, 1[$ tels que l'on ait $p^{-n\varepsilon} > s$. La partie

$$\{y \in \pi^{-1}([a_0, a_p^\varepsilon]) \mid |T(y)| < s\}$$

est un voisinage ouvert du point x dans $\mathbf{D}_p$ qui est contenu dans V . $\square$

3.2. Recollement

Soit G un groupe fini. Notons n son ordre et $g_1, \dots, g_n$ ses éléments. Chacun de ces éléments engendre un sous-groupe cyclique de G . Nous allons construire, par la méthode mise en place au numéro précédent, un revêtement galoisien cyclique associé à chacun des éléments du groupe G . Il ne nous restera plus ensuite qu'à les recoller convenablement.

En termes géométriques, nous allons recoller les revêtements au-dessus de leur lieu de trivialité en tenant compte des relations entre les éléments du groupe G . Ce procédé est simple et naturel et l'on ne doit pas se laisser rebuter par la technicité apparente de la construction qui suit. Ce n'est rien de plus qu'une traduction en termes mathématiques précis de la méthode représentée à la figure 1.

Soit i un élément de $\llbracket 1, n \rrbracket$. Notons n_i l'ordre de l'élément g_i dans le groupe G . C'est un diviseur de n et nous noterons d_i le quotient. Soit p_i un nombre premier congru à 1 modulo n_i . Soit ζ_i une racine primitive $n_i^{\text{ème}}$ de l'unité dans $\mathbf{Z}_{p_i}$. Notons $\mathcal{F}_i$ le faisceau $\mathcal{F}_{S^{n_i} - p_i^{n_i} - T}$ sur $\mathbf{D}_{p_i}''$ et $\mathcal{G}_i$ le faisceau $\mathcal{F}_i^{d_i}$. Posons

$$U_i = \{x \in \mathbf{D}_{p_i}'' \mid |T(x)| < |p_i(x)|^{n_i}\} \text{ et } F_i = \mathbf{D}_{p_i}'' \setminus U_i.$$

Notons τ_i la permutation cyclique $(1 \ 2 \ \dots \ n_i)$ de l'ensemble $\llbracket 1, n_i \rrbracket$. D'après la proposition 3.5, il existe un isomorphisme de $\mathcal{O}_{U_i}$ -algèbres

$$\varphi_i : \mathcal{F}_i \xrightarrow{\sim} \mathcal{O}^{n_i}$$

qui vérifie la condition suivante : pour tout ouvert V de U_i et toute section s de $\mathcal{F}_i$ sur V , nous ayons

$$\varphi_i(\zeta_i s) = \tau_i(\varphi_i(s)).$$

Choisissons des éléments $a_{i,0}, \dots, a_{i,d_i-1}$ de $\llbracket 1, n \rrbracket$ de sorte que tout élément du quotient $G/\langle g_i \rangle$ possède un représentant et un seul parmi les éléments $g_{a_{i,0}}, \dots, g_{a_{i,d_i-1}}$. Notons σ_i la permutation de l'ensemble $\llbracket 1, n \rrbracket$ telle que

$$\forall u \in \llbracket 0, d_i - 1 \rrbracket, \forall v \in \llbracket 1, n_i \rrbracket, g_{a_{i,u}} g_i^{v-1} = g_{\sigma_i(un_i+v)}.$$

D'après le lemme 3.11, pour tout élément i de $\llbracket 1, n \rrbracket$, la partie F_i est fermée dans $\mathbf{D}$. Définissons une partie ouverte de $\mathbf{D}$ par

$$U_0 = \mathbf{D} \setminus \bigcup_{1 \leq i \leq n} F_i.$$

Notons $\mathcal{G}_0$ le faisceau $\mathcal{O}^n$ sur U_0 .

Lemme 3.12. — *L'ouvert U_0 de la droite X est connexe.*

Démonstration. — Notons $\mathcal{P}$ l'ensemble des nombres premiers et $\mathcal{P}_0 = \{p_1, \dots, p_n\}$. Par définition, nous avons

$$U_0 = \bigcup_{1 \leq i \leq n} \{x \in \mathbf{D}_{p_i}'' \mid |T(x)| < |p_i(x)|\} \cup \bigcup_{p \in \mathcal{P} \setminus \mathcal{P}_0} [a_0, \tilde{a}_p] \cup [a_0, a_\infty^1].$$

La projection de cette partie est

$$V_0 = \mathcal{M}(\mathbf{Z}) \setminus \bigcup_{1 \leq i \leq n} \{\tilde{a}_{p_i}\},$$

qui est connexe. En outre, la section nulle définit une section continue de l'application $\pi : U_0 \rightarrow V_0$ et, pour tout élément b de V_0 , la partie $\pi^{-1}(b) \cap U_0$ est connexe. On en déduit que la partie U_0 est connexe. $\square$

La famille $(U_0, \mathbf{D}_{p_1}'', \dots, \mathbf{D}_{p_n}'')$ définit un recouvrement ouvert du disque $\mathbf{D}$. Les seules intersections de deux éléments de cette famille à n'être pas vides sont celles de la forme $\mathbf{D}_{p_i}'' \cap \mathbf{D}_{p_i}''$, pour $i \in \llbracket 0, n \rrbracket$, et $\mathbf{D}_{p_i}'' \cap U_0 = U_i$, pour $i \in \llbracket 1, n \rrbracket$. Pour définir un faisceau d'algèbres $\mathcal{G}$ en recollant les faisceaux $\mathcal{G}_0, \dots, \mathcal{G}_n$, il nous suffit de choisir un isomorphisme de $\mathcal{O}$ -algèbres entre $\mathcal{G}_i$ et $\mathcal{G}_0$ au-dessus de l'ouvert U_i , pour tout élément i de $\llbracket 1, n \rrbracket$. Nous utiliserons l'isomorphisme

$$\psi_i : \mathcal{G}_i \xrightarrow[\sim]{(\varphi_i, \dots, \varphi_i)} \mathcal{O}^n \xrightarrow[\sim]{\sigma_i^{-1}} \mathcal{O}^n = \mathcal{G}_0.$$

Remarquons que le faisceau $\mathcal{G}$ est cohérent, car nous l'avons construit en recollant des faisceaux cohérents (cf. lemme 3.1).

Proposition 3.13. — *Il existe un morphisme de groupes injectif du groupe G dans le groupe des automorphismes de $\mathcal{O}$ -algèbres du faisceau $\mathcal{F}$.*

Démonstration. — Soit h un élément du groupe G . Notons α_h la permutation de l'ensemble $\llbracket 1, n \rrbracket$ telle que

$$\forall j \in \llbracket 1, n \rrbracket, hg_j = g_{\alpha_h(j)}.$$

On définit à l'aide de cette permutation un automorphisme de $\mathcal{O}_{U_0}$ -algèbres μ_h de $\mathcal{G}_0$:

$$\mu_h : \mathcal{G}_0 = \mathcal{O}^n \xrightarrow[\sim]{\alpha_h} \mathcal{O}^n = \mathcal{G}_0.$$

Soit i un élément de $\llbracket 1, n \rrbracket$. Notons β_h la permutation de l'ensemble $\llbracket 0, d_i - 1 \rrbracket$ telle que

$$\forall u \in \llbracket 0, d_i - 1 \rrbracket, hg_{a_{i,u}} = g_{a_{i,\beta_h(u)}} \text{ dans } G/\langle g_i \rangle.$$

Notons β'_h la permutation de l'ensemble $\llbracket 1, d_i \rrbracket$ définie par

$$\forall u \in \llbracket 1, d_i \rrbracket, \beta'_h(u) = \beta_h(u - 1) + 1.$$

Elle induit un automorphisme de $\mathcal{O}_{U_i}$ -algèbres de $\mathcal{G}_i$:

$$\mathcal{G}_i = \mathcal{F}_i^{d_i} \xrightarrow[\sim]{\beta'_h} \mathcal{F}_i^{d_i} = \mathcal{G}_i.$$

Soit u un élément de $\llbracket 0, d_i - 1 \rrbracket$. Il existe un élément $m_{i,u}$ de $\llbracket 0, n_i - 1 \rrbracket$ tel que

$$hg_{a_i,u} = g_{a_i,\beta_h(u)} g_i^{m_{i,u}} \text{ dans } G.$$

On définit alors un automorphisme γ_h de $\mathcal{O}_{U_i}$ -algèbres de $\mathcal{G}_i$:

$$\mathcal{G}_i = \mathcal{F}_i^{d_i} \xrightarrow[\sim]{(\varphi_i^{m_{i,1}}, \dots, \varphi_i^{m_{i,d_i}})} \mathcal{F}_i^{d_i} = \mathcal{G}_i.$$

Un simple calcul montre qu'au-dessus de l'ouvert U_i , les automorphismes μ_h et $\gamma_h \circ \beta'_h$ de $\mathcal{G}$ coïncident.

Nous avons donc construit une application

$$\mu : \begin{array}{ccc} G & \rightarrow & \text{Aut}_{\mathcal{O}}(\mathcal{G}) \\ h & \mapsto & \mu_h \end{array}.$$

Montrons que c'est un morphisme de groupes. Soient h_1 et h_2 deux éléments de G . Pour tout élément j de $\llbracket 1, n \rrbracket$, nous avons

$$\begin{aligned} g_{\alpha_{h_1 h_2}(j)} &= h_1 h_2 g_j \\ &= h_1 g_{\alpha_{h_2}(j)} \\ &= g_{\alpha_{h_1}(\alpha_{h_2}(j))}. \end{aligned}$$

Par conséquent, nous avons $\alpha_{h_1 h_2} = \alpha_{h_1} \circ \alpha_{h_2}$ et donc $\mu_{h_1 h_2} = \mu_{h_1} \circ \mu_{h_2}$. Par conséquent, l'application μ est un morphisme de groupes.

Montrons finalement que le morphisme μ est injectif. Soient h_1 et h_2 deux éléments de G tels que $\alpha_{h_1} = \alpha_{h_2}$. Nous avons alors

$$h_1 g_1 = g_{\alpha_{h_1}(1)} = g_{\alpha_{h_2}(1)} = h_2 g_1.$$

On en déduit que $h_1 = h_2$. Par conséquent, le morphisme μ est injectif. $\square$

Remarque 3.14. — Il n'est guère difficile de montrer que le morphisme μ construit précédemment est en fait un isomorphisme de groupes. Nous n'aurons pas besoin de ce fait par la suite et ne nous attarderons donc pas à le démontrer.

3.3. Retour à l'algèbre

Nous disposons, à présent, d'un revêtement du disque $\mathbf{D}$ possédant le groupe de Galois voulu G . Il nous reste à montrer que l'extension induite entre les corps de fonctions est galoisienne de même groupe. Nous utiliserons, pour ce faire, le caractère Stein du disque $\mathbf{D}$ (cf. théorème 2.3).

Corollaire 3.15. — *Il existe un morphisme de groupes injectif du groupe G dans le groupe des automorphismes de $\mathcal{O}(\mathbf{D})$ -algèbres du faisceau $\mathcal{G}(\mathbf{D})$.*

Démonstration. — Soient $\mathcal{A}$ et $\mathcal{B}$ deux faisceaux de $\mathcal{O}_{\mathbf{D}}$ -algèbres cohérents. Considérons l'application surjective

$$\mathrm{Mor}_{\mathcal{O}}(\mathcal{A}, \mathcal{B}) \rightarrow \mathrm{Mor}_{\mathcal{O}(\mathbf{D})}(\mathcal{A}(\mathbf{D}), \mathcal{B}(\mathbf{D})).$$

Elle est injective car les faisceaux $\mathcal{A}$ et $\mathcal{B}$ satisfont le théorème A.

On en déduit que le morphisme de groupes injectif

$$\mu : G \rightarrow \mathrm{Aut}_{\mathcal{O}}(\mathcal{G})$$

construit précédemment induit un morphisme de groupes injectif

$$\mu_{\mathbf{D}} : G \rightarrow \mathrm{Aut}_{\mathcal{O}(\mathbf{D})}(\mathcal{G}(\mathbf{D})).$$

□

Lemme 3.16. — *Tout élément de $\mathcal{G}(\mathbf{D})$ annule un polynôme unitaire à coefficients dans $\mathcal{M}(\mathbf{D})$ de degré inférieur à n .*

Démonstration. — Soit s un élément de $\mathcal{G}(\mathbf{D})$. Nous supposons, tout d'abord, qu'il existe un point x_0 de U_0 tel que toutes les coordonnées de son image s_{x_0} dans $\mathcal{G}_{x_0} = \mathcal{O}_{X, x_0}^n$ soient distinctes. Puisque l'ouvert U_0 est connexe, le principe du prolongement analytique (cf. théorème 2.2) assure qu'en tout point x de U_0 , toutes les coordonnées du germe s_x sont distinctes. Notons $a_1, \dots, a_n$ les coordonnées de l'image de s dans $\mathcal{G}(U_0) = \mathcal{O}(U_0)^n$. Posons

$$M(Z) = \prod_{j=1}^n (Z - a_j) \in \mathcal{O}(U_0)[Z].$$

En tout point x de U_0 , l'image du polynôme M est l'unique polynôme unitaire de degré inférieur à n à coefficients dans $\mathcal{M}_x$ qui annule le germe s_x .

Pour tout élément j de $\llbracket 0, n \rrbracket$, posons $V_j = U_0 \cup \bigcup_{1 \leq i \leq j} \mathbf{D}_{p_i}''$. Montrons, par récurrence, que pour tout élément j de $\llbracket 0, n \rrbracket$, il existe un polynôme unitaire N_j de degré n à coefficients dans $\mathcal{M}(V_j)$ qui annule l'élément $s|_{V_j}$ de $\mathcal{G}(V_j)$. Nous avons déjà traité le cas $j = 0$. Soit maintenant un élément j de $\llbracket 0, n-1 \rrbracket$ pour

lequel l'hypothèse de récurrence est vérifiée. Puisque l'ouvert $\mathbf{D}_{p_{j+1}}''$ est connexe, l'anneau $\mathcal{M}(\mathbf{D}_{p_i}'')$ est un corps, d'après le théorème 2.2, et tout élément de l'anneau $\mathcal{O}(\mathbf{D}_{p_i}'')/(S^{n_{j+1}} - p_{j+1}^{n_{j+1}} - T)$ est annulé par un polynôme unitaire de degré inférieur à n_{j+1} à coefficients dans le corps $\mathcal{M}(\mathbf{D}_{p_i}'')$. On en déduit que l'élément $s|_{U_{j+1}}$ de $\mathcal{G}(\mathbf{D}_{p_i}'')$ est annulé par un polynôme unitaire M_{j+1} de degré inférieur à n à coefficients dans le corps $\mathcal{M}(\mathbf{D}_{p_i}'')$. Soit x un élément de $\mathbf{D}_{p_i}'' \cap U_0 = U_{j+1}$. Nous avons démontré qu'il existe un unique polynôme unitaire de degré inférieur à n à coefficients dans $\mathcal{M}_x$ qui annule le germe s_x . On en déduit que les images des polynômes N_j et M_{j+1} dans $\mathcal{M}_x[Z]$ coïncident. Par conséquent, les images de ces polynômes dans $\mathcal{M}(U_{j+1})[Z]$ coïncident. On en déduit que le polynôme N_j se prolonge en un polynôme unitaire N_{j+1} de degré inférieur à n à coefficients dans $\mathcal{M}(V_{j+1})$ qui annule l'élément $s|_{V_{j+1}}$ de $\mathcal{G}(V_{j+1})$.

On déduit finalement le résultat attendu du cas $j = n$.

Soit x_0 un point de l'ouvert U_0 . La fibre du faisceau $\mathcal{F}$ au point x_0 est isomorphe à l'algèbre $\mathcal{O}_{x_0}^n$. D'après le théorème 2.3, le faisceau $\mathcal{G}$ vérifie le théorème A sur le disque $\mathbf{D}$. On en déduit qu'il existe un élément s_0 de $\mathcal{G}(\mathbf{D})$ dont toutes les coordonnées de l'image dans la fibre $\mathcal{G}_{x_0} = \mathcal{O}_{x_0}^n$ sont distinctes.

Soit s un élément de $\mathcal{O}(\mathbf{D})$. Il existe un élément λ de $\mathcal{O}(\mathbf{D})$ tel que toutes les coordonnées du germe de la section $s_1 = s + \lambda s_0$ au point x_0 soient distinctes. Le raisonnement qui précède montre qu'il existe deux polynômes unitaires P_0 et P_1 de degré inférieur à n à coefficients dans $\mathcal{M}(\mathbf{D})$ qui annulent respectivement les sections s_0 et s_1 . D'après le théorème 2.2, l'anneau $\mathcal{M}(\mathbf{D})$ est un corps. On en déduit qu'il existe un polynôme unitaire P de degré inférieur à n à coefficients dans $\mathcal{M}(\mathbf{D})$ qui annule la section s . $\square$

Lemme 3.17. — *L'algèbre $\mathcal{G}(\mathbf{D})$ est intègre.*

Démonstration. — Soient s et t deux éléments de $\mathcal{G}(\mathbf{D})$ dont le produit est nul. Au-dessus de l'ouvert U_0 , le faisceau $\mathcal{G}$ n'est autre que le faisceau $\mathcal{O}^n$. D'après le lemme 3.12 et le théorème 2.2, l'anneau $\mathcal{O}(U_0)$ est intègre. Par conséquent, la première coordonnée de l'une des deux sections doit être nulle. Supposons que ce soit celle de s . Notons

$$s = (s_1, \dots, s_n) \text{ dans } \mathcal{O}(U_0)^n.$$

Nous supposons donc que $s_1 = 0$.

Soit i un élément de $\llbracket 1, n \rrbracket$. Il existe un élément j de $\llbracket 1, n \rrbracket$ tel que $g_j = g_i g_1^{-1}$ dans le groupe G . Notons

$$s = (t_1, \dots, t_{d_j}) \text{ dans } \mathcal{F}_j(\mathbf{D}_{p_j}'')^{d_j}.$$

Il existe des éléments u de $\llbracket 0, d_j - 1 \rrbracket$ et v de $\llbracket 1, n_j \rrbracket$ tels que

$$g_1 = g_{a_{j,u}} g_j^{v-1}.$$

Par définition du morphisme ψ_j , nous avons alors

$$\varphi_j(t_{u+1}) = \begin{pmatrix} s_{\sigma_j(un_j+1)} \\ \vdots \\ s_{\sigma_j(un_j+n_j)} \end{pmatrix} \text{ dans } \mathcal{O}(U_j)^{n_j}.$$

Par définition de σ_j , nous avons $\sigma_j(un_j+v) = 1$. Par conséquent, l'élément $s_{\sigma_j(un_j+v)}$ de $\mathcal{O}(U_j)$ est nul. Le lemme 3.9 assure que l'élément t_{u+1} de $\mathcal{F}_j(\mathbf{D}_{p_j}'')$ est également nul. Nous avons choisi l'élément j de façon à avoir l'égalité $g_1 = g_i$ dans $G/\langle g_j \rangle$. On en déduit qu'il existe un élément w de $\llbracket 1, n_j \rrbracket$ tel que $s_i = s_{\sigma_j(un_j+w)}$ dans $\mathcal{O}(U_j)$. Par conséquent, l'élément s_i est nul dans $\mathcal{O}(U_j)$ et donc dans $\mathcal{O}(U_0)$, par le principe du prolongement analytique.

Nous avons montré que l'élément $s|_{U_0}$ de $\mathcal{G}_0(U_0)$ est nul. En utilisant de façon répétée le lemme 3.9, on en déduit que l'élément s de $\mathcal{G}(\mathbf{D})$ est nul. Par conséquent, l'algèbre $\mathcal{G}(\mathbf{D})$ est intègre. $\square$

Lemme 3.18. — *L'anneau $\mathbf{Z}$ est algébriquement fermé dans l'anneau $\mathcal{G}(\mathbf{D})$.*

Démonstration. — Soit P un polynôme unitaire à coefficients dans $\mathbf{Z}$ sans racines dans $\mathbf{Z}$. Supposons, par l'absurde, qu'il existe une section s de $\mathcal{G}(\mathbf{D})$ qui est racine du polynôme P . Notons z_0 le point 0 de la fibre $\pi^{-1}(a_0)$ de l'espace X . C'est un point de l'ouvert U_0 . Notons a la première coordonnée de l'image du germe s_{z_0} par l'isomorphisme $\mathcal{G}_{z_0} \xrightarrow{\sim} \mathcal{O}_{z_0}^n$. C'est un élément de $\mathcal{O}_{z_0}$ qui vérifie l'égalité $P(a) = 0$. D'après la discussion menée à la fin de la section 2, l'anneau local $\mathcal{O}_{z_0}$ se plonge dans l'anneau $\mathbf{Q}[[T]]$. On en déduit que le polynôme P possède une racine dans l'anneau $\mathbf{Q}[[T]]$ et donc dans le corps $\mathbf{Q}$. Puisque l'anneau $\mathbf{Z}$ est algébriquement fermé dans le corps $\mathbf{Q}$, cette racine doit appartenir à $\mathbf{Z}$. Nous avons abouti à une contradiction. On en déduit le résultat annoncé. $\square$

Introduisons une définition correspondant à cette propriété.

Définition 3.19. — *Une extension L du corps $\mathcal{M}(\mathbf{D})$ est dite régulière si le corps $\mathbf{Q}$ est algébriquement fermé dans L .*

Regroupons, à présent, les résultats obtenus.

Proposition 3.20. — *L'extension de corps*

$$\mathcal{M}(\mathbf{D}) \rightarrow \text{Frac}(\mathcal{G}(\mathbf{D}))$$

est finie de degré n , régulière et galoisienne de groupe de Galois G .

Démonstration. — L'extension $\mathcal{M}(\mathbf{D}) \rightarrow \text{Frac}(\mathcal{G}(\mathbf{D}))$ est finie et de degré inférieur à n d'après le lemme 3.16. Elle est régulière d'après le lemme 3.18. On déduit du corollaire 3.15 que le groupe G s'injecte dans le groupe des $\mathcal{M}(\mathbf{D})$ -automorphismes du corps $\text{Frac}(\mathcal{G}(\mathbf{D}))$. Or le groupe G a pour cardinal n . On en déduit que l'extension $\mathcal{M}(\mathbf{D}) \rightarrow \text{Frac}(\mathcal{G}(\mathbf{D}))$ est exactement de degré n , qu'elle est galoisienne et que son groupe de Galois est isomorphe au groupe G . $\square$

Puisque nous sommes partis d'un groupe fini G arbitraire, nous avons finalement démontré que tout groupe fini est le groupe de Galois d'une extension finie, galoisienne et régulière du corps $\mathcal{M}(\mathbf{D})$. D'après les théorèmes 2.2 et 2.3 et la description de l'anneau $\mathcal{O}(\mathbf{D})$ donnée à la fin de la section 2, ce dernier est isomorphe au corps $\text{Frac}(\mathbf{Z}_1 - \llbracket T \rrbracket)$. Ceci conclut la démonstration du théorème 1.

3.4. Généralisations

Dans ce dernier numéro, nous regroupons quelques résultats proches de celui du théorème 1. Signalons, tout d'abord, qu'il existe une théorie des espaces de Berkovich au-dessus d'un anneau d'entiers de corps de nombres quelconque, complètement analogue à la théorie sur $\mathbf{Z}$. C'est d'ailleurs dans ce cadre qu'est rédigé le mémoire [11]. Soient K un corps de nombres et A l'anneau de ses entiers. Notons Σ_∞ l'ensemble des plongements complexes du corps K dans $\mathbf{C}$ et définissons une norme $\|\cdot\|$ sur l'anneau A par

$$\forall f \in A, \|f\| = \max_{\sigma \in \Sigma_\infty} (|\sigma(f)|_\infty).$$

Notons $A_1 - \llbracket T \rrbracket$ le sous-anneau de $A \llbracket T \rrbracket$ constitué des séries de la forme

$$\sum_{k \geq 0} a_k T^k$$

qui vérifient la condition suivante :

$$\forall r < 1, \lim_{k \rightarrow +\infty} \|a_k\| r^k = 0.$$

En reprenant exactement le raisonnement suivi dans cette section dans le cadre des espaces de Berkovich sur A , nous obtenons le résultat suivant (cf. [11], théorème 7.3.21) :

Théorème 3.21. — *Tout groupe fini est le groupe de Galois d'une extension finie, galoisienne et régulière du corps $\text{Frac}(A_1 - \llbracket T \rrbracket)$.*

Changeons à présent de cadre et passons des corps de nombres aux corps de fonctions. Nous nous placerons dans le cadre de la théorie de Berkovich classique, c'est-à-dire au-dessus d'un corps valué (cf. [1]). Soit k un corps de caractéristique nulle. Munissons-le de la valeur absolue triviale $|\cdot|_0$. La droite analytique $\mathbf{A}_k^{1,\text{an}}$ présente alors de nombreuses analogies avec l'espace $\mathcal{M}(\mathbf{Z})$, bien que ce dernier soit compact, phénomène curieux sur lequel nous ne nous attarderons pas ici.

Considérons, maintenant, l'espace $\mathbf{A}_k^{2,\text{an}}$, analogue de $\mathbf{A}_{\mathbf{Z}}^{1,\text{an}}$. Nous noterons U et T les coordonnées sur cet espace. Pour tout entier strictement positif n , il existe une infinité de branches de $\mathbf{A}_k^{1,\text{an}}$ sur lesquels il existe exactement n racines $n^{\text{èmes}}$ de l'unité : celles associées aux facteurs irréductibles des polynômes cyclotomiques (en la variable U) dont l'ordre est multiple de n . Posons

$$\mathbf{D}_k = \left\{ x \in \mathbf{A}_k^{2,\text{an}} \mid |T(x)| < 1 \right\}.$$

En appliquant le raisonnement suivi dans de cette section, nous démontrons que tout groupe fini est le groupe de Galois d'une extension finie, galoisienne et régulière du corps $\text{Frac}(\mathcal{O}(\mathbf{D}_k))$. Par régulière, nous entendons ici que le corps $k(U)$ est algébriquement fermé dans l'extension en question.

Afin de rendre ce résultat plus explicite, décrivons l'anneau $\mathcal{O}(\mathbf{D}_k)$. Il est constitué des séries de la forme

$$\sum_{n \geq 0} a_n(U) T^n \in k[U][[T]]$$

qui vérifient la condition suivante :

$$\forall s > 1, \forall r \in]0, 1[, \lim_{n \rightarrow +\infty} (s^{\deg(a_n)} r^n) = 0.$$

Cette description vaut d'ailleurs indépendamment de la caractéristique du corps k .

Supposons, à présent, que le corps k est de caractéristique p , où p est un nombre premier. Dans ce cas, la construction des revêtements cycliques locaux est plus complexe. Remarquons, tout d'abord, qu'il n'est pas nécessaire de construire un revêtement cyclique associé à chaque élément du groupe, mais que nous pouvons nous contenter d'un système de générateurs. Quitte à choisir convenablement ce système, nous pouvons supposer que chaque élément qui le compose a pour ordre un entier premier à p ou une puissance de p . Si un élément a pour ordre un entier n premier à p , nous construisons un revêtement

local cyclique de degré n par la même méthode que dans le cas d'un corps de caractéristique nulle.

Supposons, maintenant, que l'ordre d'un élément soit p^r , avec $r \geq 1$. Choisissons une branche quelconque B de la droite $\mathbf{A}_k^{1,\text{an}}$. Elle est associée à un polynôme irréductible $P(U) \in k[U]$. Notons W_r l'anneau des vecteurs de Witt de longueur r sur $k[U, T, S_0, \dots, S_{r-1}]$. Posons

$$S = (S_0, \dots, S_{r-1}) \in W_r$$

et, pour tout élément α de $k[U, T, S_0, \dots, S_{r-1}]$,

$$\{\alpha\} = (\alpha, 0, \dots, 0) \in W_r.$$

Pour tout $i \in \llbracket 0, r-1 \rrbracket$, définissons un polynôme $Q_i(S_0, \dots, S_{r-1})$ à coefficients dans $k[T, U]$ par la formule

$$(Q_0, \dots, Q_{r-1}) = F(S) - \{P(U)\}^{p-1}S - \{T\} \text{ dans } W_r.$$

Le groupe $\mathbf{Z}/p^r\mathbf{Z}$ agit sur l'anneau $k[T, U, S_0, \dots, S_{r-1}]/(Q_0, \dots, Q_{r-1})$ en laissant stable $k[T, U]$ et en envoyant S_i , pour $i \in \llbracket 0, r-1 \rrbracket$, sur la $(i+1)^{\text{ème}}$ coordonnée du vecteur $S + \{P(U)\}$ dans W_r . En fait, d'après la théorie d'Artin-Schreier-Witt, l'extension

$$k(T, U) \rightarrow k(T, U)[S_0, \dots, S_{r-1}]/(Q_0, \dots, Q_{r-1})$$

est galoisienne de groupe $\mathbf{Z}/p^r\mathbf{Z}$. Par analogie avec la construction du numéro 3.1, nous définissons un faisceau sur le disque ouvert de rayon 1 au-dessus de la branche B privé du point central, noté $\mathbf{D}_{k,B}''$, par

$$\mathcal{F}_{Q_0, \dots, Q_r} = \mathcal{O}[S_0, \dots, S_{r-1}]/(Q_0, \dots, Q_{r-1}).$$

Les propriétés des vecteurs de Witt montrent que, pour tout $i \in \llbracket 0, r-1 \rrbracket$, nous avons

$$Q_i = S_i^p - P(U)^{(p-1)p^i} S_i \mod (T, Q_0, \dots, Q_{i-1}).$$

Considérons un point x situé sur la section nulle au-dessus de la branche B privée de ses deux extrémités. L'image $S_0^p - P(U)^{p-1}S_0$ du polynôme $Q_0(S_0)$ dans le corps résiduel $\kappa(x)$ de l'anneau local $\mathcal{O}_x$ est scindé à racines simples. Puisque cet anneau local est hensélien, le polynôme $P_0(S_0)$ possède p racines simples dans $\mathcal{O}_x$.

En raisonnant par récurrence sur le nombre de variables, on montre ainsi que le système d'équations polynomiales donné par $Q_0, \dots, Q_{r-1}$ possède exactement p^r racines $\alpha_1, \dots, \alpha_{p^r}$ dans $\mathcal{O}_x^r$ et que le morphisme

$$\begin{aligned} \varphi : \mathcal{O}_x[S_0, \dots, S_{r-1}] / (Q_0, \dots, Q_{r-1}) &\rightarrow \mathcal{O}_x^{p^r} \\ R(S_0, \dots, S_{r-1}) &\mapsto (R(\alpha_i))_{1 \leq i \leq p^r} \end{aligned}$$

est un isomorphisme. On utilise ensuite les propriétés du flot (à toute semi-norme multiplicative $|\cdot|_x$ sur $k[T]$ est associée une application de $\mathbf{R}_+^*$ dans $\mathbf{A}_k^{1, \text{an}}$ qui envoie ε sur le point associé à $|\cdot|_x^\varepsilon$, cf. [11], numéro 1.3) pour en déduire que cet isomorphisme se prolonge en dehors d'une partie fermée du disque $\mathbf{D}_{k, B}''$ qui est encore fermée dans $\mathbf{D}_k$ (cf. lemme 3.11).

Il nous faut encore prouver que l'anneau $\mathcal{F}_{Q_0, \dots, Q_{r-1}}(\mathbf{D}_B'')$ est intègre. On démontre cette propriété par récurrence sur le nombre de variables en raisonnant comme dans la preuve du lemme 3.7.

Les arguments des numéros 3.2 et 3.3 s'adaptent alors exactement. On en déduit le résultat suivant :

Théorème 3.22. — *Soit k un corps. Tout groupe fini est le groupe de Galois d'une extension finie, galoisienne et régulière du corps $\text{Frac}(\mathcal{O}(\mathbf{D}_k))$.*

Références

- [1] Vladimir G. Berkovich. *Spectral theory and analytic geometry over non-Archimedean fields*, volume 33 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 1990.
- [2] Antoine Chambert-Loir. *A field guide to algebra*. Undergraduate Texts in Mathematics. Springer-Verlag, New York, 2005.
- [3] Pierre Dèbes. Théorie de Galois et géométrie : une introduction. In *Arithmétique de revêtements algébriques (Saint-Étienne, 2000)*, volume 5 of *Sémin. Congr.*, pages 1–26. Soc. Math. France, Paris, 2001.
- [4] David Harbater. Algebraic rings of arithmetic power series. *J. Algebra*, 91(2) :294–319, 1984.
- [5] David Harbater. Convergent arithmetic power series. *Amer. J. Math.*, 106(4) :801–846, 1984.
- [6] David Harbater. Mock covers and Galois extensions. *J. Algebra*, 91(2) :281–293, 1984.
- [7] David Harbater. Galois coverings of the arithmetic line. In *Number theory (New York, 1984–1985)*, volume 1240 of *Lecture Notes in Math.*, pages 165–195. Springer, Berlin, 1987.
- [8] David Harbater. Galois covers of an arithmetic surface. *Amer. J. Math.*, 110(5) :849–885, 1988.

- [9] David Harbater. Patching and Galois theory. In *Galois groups and fundamental groups*, volume 41 of *Math. Sci. Res. Inst. Publ.*, pages 313–424. Cambridge Univ. Press, Cambridge, 2003.
- [10] Qing Liu. Tout groupe fini est un groupe de Galois sur $\mathbf{Q}_p(T)$, d’après Harbater. In *Recent developments in the inverse Galois problem (Seattle, WA, 1993)*, volume 186 of *Contemp. Math.*, pages 261–265. Amer. Math. Soc., Providence, RI, 1995.
- [11] Jérôme Poineau. La droite de Berkovich sur $\mathbf{Z}$. Soumis.

11 septembre 2008

JÉRÔME POINEAU, Institut de recherche mathématique avancée, 7, rue René Descartes, 67084
Strasbourg, France • *E-mail* : `jerome.poineau@math.u-strasbg.fr`