UN ANNEAU DE PRÜFER

H. LOMBARDI

Résumé. Notons **E** l'anneau des polynômes à valeurs entières sur $\mathbb{Z}$. On sait que cet anneau est un anneau de Prüfer. Mais il semble qu'il n'existe pas d'algorithme connu pour inverser un idéal de type fini non nul de **E**. Dans cette note, nous montrons comment obtenir un tel algorithme en déchiffrant une démonstration abstraite qui utilise les localisations de **E** en ses idéaux maximaux. Ceci confirme le programme général de décryptage des démonstrations classiques pour en extraire des preuve constructives.

Abstract. Let **E** be the ring of integer valued polynomials over $\mathbb{Z}$. This ring is known to be a Prüfer domain. But it seems there does not exist an algorithm for inverting a nonzero finitely generated ideal of **E**. In this note we show how to obtain such an algorithm by deciphering a classical abstract proof that uses localisations of **E** at all prime ideals of **E**. This confirms a general program of deciphering abstract classical proofs in order to obtain algorithmic proofs.

Décembre 2012. Version légèrement étendue de l'article original
lequel se trouve à :
http://acirm.cedram.org/cgi-bin/browse?id=ACIRM_2010__2_2

Introduction

Nous nous situons dans la tradition constructive de Bishop [1, 2], Bridges et Richman [3, 21, 22].

Nous notons **E** l'anneau des polynômes à valeurs entières (en une variable) sur $\mathbb{Z}$. Il est connu que cet anneau est un anneau de Prüfer, par exemple parce que l'on a étudié ses idéaux premiers et que les localisés correspondants sont des anneaux de valuation [4, 5, Chabert]. Cependant, il ne semble pas que l'on connaisse d'algorithme pour inverser un idéal de type fini non nul de **E**. Nous montrons dans cette note comment le décryptage de la preuve classique évoquée ci-dessus permet de résoudre le problème algorithmique correspondant. Ceci confirme la faisabilité du programme général de réécriture sous le slogan : les mathématiques classiques sont constructives, si l'on veut bien se donner la peine de regarder en détail ce qui se cache derrière les raccourcis audacieux usuellement pratiqués.

Pour prendre connaissance de quelques succès déjà obtenus dans ce programme, on pourra consulter les articles [6–15, 18, 23] et le livre [20].

1. Préliminaires

Dans cet article tous les anneaux sont commutatifs et unitaires.

Anneaux arithmétiques et de Prüfer. Un anneau de Prüfer peut être défini comme un anneau arithmétique intègre [17], ou comme un anneau intègre dans lequel les idéaux de type fini non nuls sont inversibles [16], ou comme un anneau intègre dont tous les localisés en ses idéaux premiers (on peut se limiter aux idéaux maximaux) sont des anneaux de valuation.

La première ou la seconde définition a l'avantage d'être plus simple (notamment du point de vue de la complexité logique des énoncés) et de pouvoir servir à établir des résultats dans un cadre algorithmique

Date: June 2011.
2000 *Mathematics Subject Classification.* 13F05, 13F20, 13A15, 03F65.
Key words and phrases. Prüfer rings, Integer valued polynomials, Constructive mathematics.

et constructif. La troisième définition n'implique la première qu'en mathématiques classiques, avec le secours du principe du tiers exclu et de l'axiome du choix[1].

Un anneau arithmétique est un anneau dans lequel les idéaux de type fini sont localement principaux. En pratique il suffit d'établir la propriété pour les idéaux à deux générateurs et cela donne la définition très élémentaire suivante [15]. Un anneau $\mathbf{A}$ est arithmétique si, pour tous $x, y \in \mathbf{A}$, il existe u, v, s, t dans $\mathbf{A}$ tels que soient satisfaites les égalités

$$s+t=1, \quad sx=uy, \quad ty=vx. \tag{1}$$

Ainsi dans $\mathbf{A}[1/s]$ l'idéal $\langle x, y\rangle$ est égal à $\langle y\rangle$ et dans $\mathbf{A}[1/t]$ il est égal à $\langle x\rangle$. En outre $\langle x, y\rangle \langle t, u\rangle = \langle x\rangle$ et $\langle x, y\rangle \langle s, v\rangle = \langle y\rangle$. Plus généralement dans un anneau arithmétique, tout idéal de type fini contenant un élément régulier est inversible.

La matrice $M = \begin{bmatrix} t & v \\ u & s \end{bmatrix}$ est appelée *une matrice de localisation principale pour* (x, y) : ses lignes sont « proportionnelles » à (x, y), et sa trace est égale à 1 :

$$\begin{vmatrix} u & s \\ x & y \end{vmatrix} = \begin{vmatrix} t & v \\ x & y \end{vmatrix} = 0, \quad \mathrm{Tr}(M) = 1. \tag{2}$$

La notion de matrice de localisation principale s'étend pour un système $(x_1, \ldots, x_n)$ de n éléments. Les matrices de localisation principale pour n éléments peuvent être construites à partir des matrices de localisation principale pour deux éléments ([15]).

$\mathbb{Z}$-bases et automorphismes de l'anneau des polynômes à valeurs entières sur $\mathbb{Z}$. Si $\mathbf{A}$ est un anneau intègre de corps de fractions $\mathbf{K}$, l'anneau des polynômes à valeurs entières sur $\mathbf{A}$ (en une variable) est le sous-anneau de $\mathbf{K}[x]$ fomé par les polynômes f qui envoient $\mathbf{A}$ dans $\mathbf{A}$ ($\forall \xi \in \mathbf{A},\ f(\xi) \in \mathbf{A}$).

Nous notons $\mathbf{E}$ l'anneau des polynômes à valeurs entières (en une variable) sur $\mathbb{Z}$. Pour tout $r \in \mathbb{Z}$, l'application $f(x) \mapsto f(x-r)$ est un automorphisme de $\mathbf{E}$.

Une $\mathbb{Z}$-base de $\mathbf{E}$ est formée par les polynômes combinatoires $C_n = \binom{x}{n}$. La base des C_n est triangulaire par rapport à la $\mathbb{Q}$-base des monômes de $\mathbb{Q}[x]$.

D'autres bases triangulaires de $\mathbf{E}$ sont obtenues par translation : pour $r \in \mathbb{Z}$ fixé les $C_n(x-r)$ forment une base triangulaire.

Si p est un nombre premier, nous notons $\mathbb{Z}_{(p)} = \mathbb{Z}_{1+p\mathbb{Z}}$ le localisé de $\mathbb{Z}$ en l'idéal maximal $p\mathbb{Z}$ et $\mathbf{E}_p$ l'anneau des polynômes à valeurs entières (en une variable) sur $\mathbb{Z}_{(p)}$. Les C_n forment une $\mathbb{Z}_{(p)}$-base triangulaire de $\mathbf{E}_p$, de même que tous les systèmes obtenus par translation. Ainsi $\mathbf{E}_p \simeq \mathbb{Z}_{(p)} \otimes_{\mathbb{Z}} \mathbf{E}$.

Le principe local-global de base. Le reste de la section 1 est un rappel, pour la commodité du lecteur, de la méthode générale de décryptage des démonstrations classiques basées sur les localisations en des idéaux premiers arbitraires [10, 15, 18–20].

Un *anneau local* est un anneau $\mathbf{A}$ où est vérifié l'axiome suivant :

$$\forall x, y \in \mathbf{A},\ x+y \in \mathbf{A}^\times \ \Rightarrow\ (x \in \mathbf{A}^\times \text{ ou } y \in \mathbf{A}^\times)$$

Il revient au même de demander : $\forall x \in \mathbf{A},\ x \in \mathbf{A}^\times$ ou $1-x \in \mathbf{A}^\times$.

Notez que selon cette définition l'anneau trivial est local. Par ailleurs, les « ou » doivent être compris dans leur sens constructif : l'alternative doit être explicite. La plupart des anneaux locaux avec lesquels on travaille usuellement en mathématiques classiques vérifient en fait la définition précédente si on les regarde d'un point de vue constructif.

Pour un anneau commutatif arbitraire, le *radical de Jacobson* de $\mathbf{A}$ est défini comme

$$\mathrm{Rad}(\mathbf{A}) = \{\, a \in \mathbf{A} \mid \forall y \in \mathbf{A},\ \ 1+ay \in \mathbf{A}^\times \,\}$$

En mathématiques classiques le radical de Jacobson est l'intersection des idéaux maximaux.

Par définition un *anneau local résiduellement discret* est un anneau local qui satisfait l'axiome suivant

$$\forall x \in \mathbf{A} \qquad x \in \mathbf{A}^\times \ \text{ ou } \ 1+x\mathbf{A} \subseteq \mathbf{A}^\times \tag{3}$$

de sorte que dans le quotient $\mathbf{A}/\mathrm{Rad}(\mathbf{A})$, tout élément est nul ou inversible (avec un « ou » explicite). En mathématiques classiques tous les anneaux locaux sont résiduellement discrets.

1. Ces principes, surtout le premier, constituent la raison du caractère non explicite des démonstrations en mathématiques classiques.

Nous appelons *monoïde de* $\mathbf{A}$ toute partie S stable par multiplication. Le monoïde S est dit *saturé* si $xy \in S$ implique x et $y \in S$. Un monoïde saturé est appelé un *filtre*. Un monoïde est dit *trivial* s'il contient 0, c'est-à-dire si le filtre obtenu par saturation est égal à $\mathbf{A}$. C'est le cas où $\mathbf{A}_S$ est l'anneau trivial.

Définition 1.1.

(1) *Des monoïdes $S_1, \ldots, S_n$ de l'anneau $\mathbf{A}$ sont dits* comaximaux *si un idéal de $\mathbf{A}$ qui coupe chacun des S_i contient toujours* 1*, autrement dit si on a :*

$$\forall s_1 \in S_1 \ \cdots \ \forall s_n \in S_n \ \ \exists a_1, \ldots, a_n \in \mathbf{A} \quad \sum\nolimits_{i=1}^{n} a_i s_i = 1$$

(2) *On dit que* les monoïdes $S_1, \ldots, S_n$ de l'anneau $\mathbf{A}$ recouvrent le monoïde S *si S est contenu dans les S_i et si un idéal de $\mathbf{A}$ qui coupe chacun des S_i coupe toujours S, autrement dit si on a :*

$$\forall s_1 \in S_1 \ \cdots \ \forall s_n \in S_n \ \ \exists a_1, \ldots, a_n \in \mathbf{A} \quad \sum\nolimits_{i=1}^{n} a_i s_i \in S$$

(3) *Nous noterons $\mathcal{M}(U)$ le monoïde engendré par l'élément ou la partie U de $\mathbf{A}$, $\mathcal{I}_{\mathbf{A}}(I)$ ou $\mathcal{I}(I)$ ou $\langle I \rangle$ l'idéal de $\mathbf{A}$ engendré par I, et $\mathcal{S}(I;U)$ le monoïde :*

$$\mathcal{S}(I;U) = \{v \ ; \ \exists u \in \mathcal{M}(U) \ \exists a \in \mathcal{I}(I) \quad v = u + a \ \}$$

et de la même manière :

$$\mathcal{S}(a_1, \ldots, a_k; u_1, \ldots, u_\ell) = \{v \ ; \ \exists u \in \mathcal{M}(u_1, \ldots, u_\ell) \ \exists a \in \mathcal{I}(a_1, \ldots, a_k) \quad v = u + a \ \}.$$

Nous disons qu'un tel monoïde admet une description finie*.*

Notez que lorsqu'on localise en $S = \mathcal{S}(I;U)$, les éléments de U deviennent inversibles et ceux de I se retrouvent dans le radical de Jacobson de $\mathbf{A}_S$. Dans la suite « radical de $\mathbf{A}$ » signifiera toujours radical de Jacobson de $\mathbf{A}$.

Lemme 1.2. (lemme fondamental)
Soit U et I des parties de l'anneau $\mathbf{A}$ et $a \in \mathbf{A}$, alors les monoïdes $\mathcal{S}(I;U,a)$ et $\mathcal{S}(I,a;U)$ recouvrent le monoïde $\mathcal{S}(I;U)$.

En particulier les monoïdes $S = \mathcal{M}(a) = \mathcal{S}(0;a)$ et $S' = \mathcal{S}(a;1) = 1 + a\mathbf{A}$ sont comaximaux.
De même les monoïdes $\mathcal{S}(a_1;1)$, $\mathcal{S}(a_2;a_1)$ et $\mathcal{S}(0;a_1a_2)$ sont comaximaux. Donc a fortiori $\mathcal{S}(a_1;1)$, $\mathcal{S}(a_2;1)$ et $\mathcal{S}(0;a_1a_2)$ sont comaximaux.
On a aussi facilement le lemme suivant, que l'on peut voir comme un corollaire du lemme fondamental en suivant l'exemple précédent.

Lemme 1.3. *Soient U et I des parties de l'anneau $\mathbf{A}$ et $a_1, \ldots, a_k \in \mathbf{A}$ qui satisfont une appartenance*

$$u \textstyle\prod_{i \in [\![1..k]\!]} a_i \in \langle I \rangle_{\mathbf{A}}$$

pour un $u \in \mathcal{S}(I;U)$. Alors $\mathcal{S}(I;U)$ est recouvert par les $\mathcal{S}(I,a_i;U)$.

Principe local-global concret 1. (principe local-global de base)
Soient $S_1, \ldots, S_n$ des monoïdes comaximaux de $\mathbf{A}$. Soit B une matrice $\in \mathbf{A}^{m \times p}$ et C un vecteur colonne dans $\mathbf{A}^{m \times 1}$. Les propriétés suivantes sont équivalentes.

(1) *Le système linéaire $BX = C$ admet une solution dans $\mathbf{A}^{p \times 1}$.*

(2) *Pour chaque $i \in [\![1..n]\!]$ le système linéaire $BX = C$ admet une solution dans $\mathbf{A}_{S_i}^{p \times 1}$.*

Comme conséquence immédiate on a le lemme suivant.

Lemme 1.4. (Principe local-global pour les idéaux localement principaux)
Soient $S_1, \ldots, S_n$ des monoïdes comaximaux et $\mathfrak{a}$ un idéal de type fini de $\mathbf{A}$. Alors $\mathfrak{a}$ est localement principal si, et seulement si, il est localement principal après localisation en chaque S_i.

Le décryptage des démonstrations basées sur la localisation en un idéal premier arbitraire. Un argument de localisation typique fonctionne comme suit en mathématiques classiques. Lorsque l'anneau est local une certaine propriété P est vérifiée en vertu d'une démonstration assez concrète. Lorsque l'anneau n'est pas local, la même propriété est encore vraie (d'un point de vue classique non constructif) car il suffit de la vérifier localement.

Nous examinons avec un peu d'attention la première preuve. Nous voyons alors apparaître certains calculs qui sont faisables en vertu du principe suivant :

$$\forall x \in \mathbf{A} \quad x \in \mathbf{A}^\times \ \vee \ x \in \mathrm{Rad}(\mathbf{A}),$$

principe qui est appliqué à des éléments x provenant de la preuve elle-même. Autrement dit, la preuve classique donnée dans le cas local nous fournit une preuve constructive sous l'hypothèse d'un anneau local résiduellement discret. Voici maintenant notre décryptage dynamique constructif. Dans le cas d'un anneau arbitraire, nous répétons la même preuve, en remplaçant chaque disjonction « x est inversible ou x est dans le radical », par la considération des deux anneaux $\mathbf{A}_{\mathcal{S}(I,x;U)}$ et $\mathbf{A}_{\mathcal{S}(I;x,U)}$, où $\mathbf{A}_{\mathcal{S}(I,U)}$ est la localisation "courante" de l'anneau $\mathbf{A}$ de départ, à l'endroit de la preuve où l'on se trouve. Lorsque la preuve initiale est ainsi déployée, on a construit à la fin un certain nombre, fini parce que la preuve est finie, de localisés $\mathbf{A}_{S_i}$, pour lesquels la propriété est vraie. D'un point de vue constructif, nous obtenons au moins le résultat « quasi global », c'est-à-dire que la propriété P est vérifiée après localisation en des monoïdes comaximaux, en vertu du lemme 1.2. On fait alors appel à un principe local-global concret pour conclure. Dans cet article ce sera le lemme 1.4 pour les idéaux de type fini localement principaux.

La méthode indiquée ci-dessus donne donc, comme corollaire du lemme 1.2 le principe général de décryptage suivant, qui *permet d'obtenir automatiquement une version constructive globale (ou au moins quasi globale) d'un théorème à partir de sa version locale.*

Machinerie locale-globale à idéaux premiers.
Lorsque l'on relit une preuve constructive, donnée pour le cas d'un anneau local résiduellement discret, avec un anneau $\mathbf{A}$ arbitraire, que l'on considère au départ comme $\mathbf{A} = \mathbf{A}_{\mathcal{S}(0;1)}$ et qu'à chaque disjonction (pour un élément a qui se présente au cours du calcul dans le cas local)

$$a \in \mathbf{A}^\times \ \vee \ a \in \mathrm{Rad}(\mathbf{A}),$$

on remplace l'anneau « en cours » $\mathbf{A}_{\mathcal{S}(I;U)}$ par les deux anneaux $\mathbf{A}_{\mathcal{S}(I;U,a)}$ et $\mathbf{A}_{\mathcal{S}(I,a;U)}$ (dans chacun desquels le calcul peut se poursuivre), on obtient à la fin de la relecture, une famille finie d'anneaux $\mathbf{A}_{\mathcal{S}(I_j;U_j)}$ avec les monoïdes $\mathcal{S}(I_j;U_j)$ comaximaux et I_j, U_j finis. Dans chacun de ces anneaux, le calcul a été poursuivi avec succès et a donné le résultat souhaité.

On notera que si « l'anneau en cours » est $\mathbf{A}' = \mathbf{A}_{\mathcal{S}(I;U)}$ et si la disjonction porte sur

$$b \in \mathbf{A}'^\times \ \vee \ b \in \mathrm{Rad}(\mathbf{A}'),$$

avec $b = a/(u+i)$, $a \in \mathbf{A}$, $u \in \mathcal{M}(U)$ et $i \in \langle I \rangle_{\mathbf{A}}$, alors il faut considérer les localisés $\mathbf{A}_{\mathcal{S}(I;U,a)}$ et $\mathbf{A}_{\mathcal{S}(I,a;U)}$.

2. Des idéaux maximaux de l'anneau des polynômes à valeurs entières

Soit p un nombre premier fixé. Notons $\mathbf{B} = \mathbf{E}_p \subseteq \mathbb{Q}[x]$ l'anneau des polynômes à valeurs entières sur l'anneau $\mathbb{Z}_{(p)} = \mathbb{Z}_{1+p\mathbb{Z}}$. On s'intéresse ici aux idéaux maximaux *détachables*[2] de $\mathbf{E}_p$. Notez que l'on a une inclusion stricte $\mathbf{E}_p \subsetneq \mathbf{E}[1/p]$ et ne vous laissez donc pas abuser par la notation $\mathbf{E}_p$.

En mathématiques classiques, un anneau intègre est un anneau de Prüfer si, et seulement si, tous les localisés en les idéaux premiers sont des anneaux de valuation (on peut aussi considérer seulement les idéaux maximaux). On va démontrer dans cette section que c'est bien le cas, au moins pour les idéaux premiers de $\mathbf{E}_p$ qui contiennent p.

Il existe des idéaux premiers $\mathfrak{p}$ de $\mathbf{E}_p$ qui intersectent $\mathbb{Z}_{(p)}$ en $\{0\}$. Dans ce cas le corps $\mathrm{Frac}(\mathbf{E}_p/\mathfrak{p})$ est de la forme $\mathbb{Q}(\overline{x})$ où $\overline{x}$ est la classe de x dans le quotient. Si $\mathfrak{p}$ est maximal, $\overline{x}$ est algébrique sur $\mathbb{Q}$. L'exemple le plus simple est celui de l'idéal maximal $\langle 3x-1\rangle$ de $\mathbf{E}_3$, l'anneau quotient étant isomorphe à $\mathbb{Z}_{(3)}[\frac{1}{3}] = \mathbb{Q}$.

Il se trouve que dans la situation présente, il suffit de considérer les idéaux premiers contenant p pour montrer que $\mathbf{E}_p$ est un anneau de Prüfer, comme on le verra lorsqu'on prouvera le théorème 2.

2. Une partie M d'un ensemble E est dite détachable lorsque l'on dispose d'un test pour $f \in M$? lorsque $f \in E$.

On note

$$B_k = c_k \binom{x}{p^k}$$

où l'entier c_k est choisi de façon à ce qu'il ne reste plus que la puissance de p au dénominateur de B_k. Par exemple avec $p = 3$ on obtient

$$B_0 = x,\ B_1 = \tfrac{x(x-1)(x-2)}{3},\ B_2 = \tfrac{B_1(x)B_1(x-3)B_1(x-6)}{3},\ B_3 = \tfrac{B_2(x)B_2(x-9)B_2(x-18)}{3},\ \dots$$

Proposition et définition 2.1. *(Avec les notations précédentes)*

(1) *Prenons par exemple $p = 3$. On a alors une $\mathbb{Z}_{(3)}$-base triangulaire de $\mathbf{B}$, $(A_n)_{n\in\mathbb{N}}$ formée comme suit*

A_0	A_1	A_2	A_3	A_4	A_5	A_6	A_7	A_8	A_9	A_{10}	A_{11}	A_{12}	A_{13}	$\dots$
1	x	x^2	B_1	xB_1	x^2B_1	B_1^2	xB_1^2	$x^2B_1^2$	B_2	xB_2	x^2B_2	B_1B_2	xB_1B_2	$\dots$

(2) *Plus généralement si $n = \sum_k a_k p^k$ avec $a_k \in [\![0..p-1]\!]$ pour tout k, on pose*

$$A_n = x^{a_0}\, B_1^{a_1}\, B_2^{a_2}\, \cdots = \prod_{k=0}^{N} B_k^{a_k} \quad (N \textit{ assez grand}),$$

et la famille $(A_n)_{n\in\mathbb{N}}$ est une $\mathbb{Z}_{(p)}$-base de $\mathbf{E}_p$.

Remarque. Au lieu des polynômes B_k on aurait pu prendre les polynômes D_k définis par récurrence comme suit : $D_0 = x$, puis $D_{k+1} = ({D_k}^p - D_k)/p$. ∎

Notre but est maintenant d'étudier un idéal maximal de $\mathbf{B}$ qui contient p. Nous reprenons sans perte de généralité le cas $p = 3$ et nous supposons avoir à notre disposition un idéal maximal $\mathfrak{m}$ de $\mathbf{B} = \mathbf{E}_p$ qui soit détachable et qui contienne p.

L'anneau $\mathbf{V} = \mathbf{B}_{1+\mathfrak{m}} \subseteq \mathbb{Q}(x)$, autrement dit le localisé de $\mathbf{B}$ en $\mathfrak{m}$, est « l'anneau qui intéresse le mathématicien classique », celui qui doit être un anneau de valuation, condition nécessaire pour que $\mathbf{B}$ soit un anneau de Prüfer.

Rappelons qu'en toute généralité, pour un idéal $\mathfrak{a} \subseteq \mathbf{A}$ en posant $\mathbf{V} = \mathbf{A}_{1+\mathfrak{a}}$, on a pour un entier $k > 0$ et un $f \in \mathbf{A}$ arbitraires l'équivalence de $f \in \mathfrak{a}^k$ avec $f \in (\mathfrak{a}\mathbf{V})^k$.

En fait nous supposerons seulement au départ que $\mathfrak{m}$ est premier et détachable, et dans ce contexte l'anneau $\mathbf{V} = \mathbf{B}_{1+\mathfrak{m}}$ n'est pas a priori un anneau local, car on ne suppose pas $\mathfrak{m}$ maximal. Nous verrons à l'arrivée que $\mathfrak{m}$ est en fait maximal.

L'idée générale pour étudier un idéal premier de $\mathbf{B} = \mathbf{E}_p$ contenant p est la suivante, énoncée de façon très informelle.
À translation près, *si l'on ne désire qu'une information de précision finie concernant l'idéal $\mathfrak{m}$, en se limitant à un exposant k donné et à des A_n pour $n \le d$ où d est donné, on peut toujours supposer que les A_n sont tous dans $\mathfrak{m}^k$, à l'exception de $A_0 = 1$.*

Nous allons au cours de l'étude de $\mathfrak{m}$ expliquer les approximations successives de $\mathfrak{m}$ que nous pouvons considérer au fur et à mesure que nous accumulons des informations concernant $\mathfrak{m}$. Nous allons voir que des approximations finies de $\mathfrak{m}$ suffisent pour obtenir les résultats souhaités.

Voyons comment cela se passe en détail.

Au départ la seule information concernant $\mathfrak{m}$ est que $3 \in \mathfrak{m}$. On dispose donc de l'approximation $\mathbf{B}_{\mathcal{S}(3;1)}$ de $\mathbf{V}$.

Pour alléger la notation dans la suite, nous noterons $\mathbf{B}_{3;1}$ à la place de $\mathbf{B}_{\mathcal{S}(3;1)}$.

Les localisations de $\mathbf{B}_{3;1}$ que nous allons introduire comme approximations de $\mathbf{V}$ seront toutes non triviales du type $\mathbf{B}_{3,I;1}$, et 3 ne sera jamais une unité : la localisation ne sera jamais l'anneau trivial.

Puisque le produit $x(x-1)(x-2) = 3B_1(x) \in 3\mathbf{B} \subseteq \mathfrak{m}$, on a nécessairement $x \in \mathfrak{m}$ ou $x - 1 \in \mathfrak{m}$ ou $x - 2 \in \mathfrak{m}$. Comme 1 et 2 sont des unités modulo 3, ce sont des unités modulo $\mathfrak{m}$ et les trois cas sont exclusifs l'un de l'autre :

- Si $x \in \mathfrak{m}$, alors $x - 1$ et $x - 2$ sont des unités modulo $\mathfrak{m}$.
- Si $x - 1 \in \mathfrak{m}$, alors x et $x - 2$ sont des unités modulo $\mathfrak{m}$.
- Si $x - 2 \in \mathfrak{m}$, alors x et $x - 1$ sont des unités modulo $\mathfrak{m}$.

Vu les automorphismes de $\mathbf{E}_3$ par translations, l'étude des trois cas est inutile. Il suffit d'étudier le premier.

Supposons $x \in \mathfrak{m}$. Pour les premiers éléments de la $\mathbb{Z}_{(p)}$-base des A_n, on obtient les résultats suivants :

A_0	A_1	A_2	A_3	A_4	A_5	A_6	A_7	A_8	A_9	A_{10}	A_{11}	A_{12}	A_{13}	$\dots$
1	x	x^2	B_1	xB_1	x^2B_1	B_1^2	xB_1^2	$x^2B_1^2$	B_2	xB_2	x^2B_2	B_1B_2	xB_1B_2	$\dots$
$=0$	≥ 1	≥ 2	≥ 0	≥ 1	≥ 2	≥ 0	≥ 1	≥ 2	≥ 0	≥ 1	≥ 2	≥ 0	≥ 1	$\dots$

où l'on a fait figurer sur la dernière ligne l'exposant k de $\mathfrak{m}$ pour lequel on sait que $A_n \in \mathfrak{m}^k$.
Ainsi l'indication ≥ 0 signifie que nous ne savons rien concernant la question $A_k \in \mathfrak{m}$ (on sait seulement que A_k est dans $\mathbf{B}$).
On en déduit que si $f \in \mathbf{B}$ est de degré ≤ 2 avec $f(0) \not\equiv 0 \bmod 3$ alors f est une unité modulo $\mathfrak{m}$, tandis que dans le cas contraire $f \in \mathfrak{m}$. Par contre on ne sait pas si $B_1 \in \mathfrak{m}$ ou $\notin \mathfrak{m}$. De même si $\deg(f) = 5$ on aura une information sur f (à savoir $f \in \mathfrak{m}$) seulement dans le cas où le coefficient de f sur A_3 est nul modulo 3.

Du point de vue des approximations, les mêmes raisonnements (en utilisant le lemme 1.3) nous apprennent que le monoïde $\mathcal{S}(3;1)$ est recouvert par les 3 monoïdes

$$\mathcal{S}(3, x; 1), \quad \mathcal{S}(3, x-1; 1) \text{ et } \mathcal{S}(3, x-2; 1).$$

Comme ces monoïdes se déduisent les uns des autres par translation, nous savons qu'ils sont non triviaux (ils ne contiennent pas 0), car si l'un était trivial les trois le seraient et $\mathcal{S}(3;1)$ serait lui-même trivial.

Dans l'anneau $\mathbf{B}_{3,x;1}$, l'élément x est dans le radical tandis que $x-1$ et $x-2$ sont des unités. Donc, puisque $x(x-1)(x-2) \in 3\mathbf{B}_{3,x;1}$, on obtient $\langle 3, x\rangle = \langle 3\rangle$ dans $\mathbf{B}_{3,x;1}$.

Soit $f \in \mathbf{B}$ de degré ≤ 2. Si $f(0) \not\equiv 0 \bmod 3$ alors f est une unité dans $\mathbf{B}_{3,x;1}$, tandis que dans le cas contraire f est dans le radical. Autrement dit, les informations que nous avons indiquées concernant le localisé $\mathbf{B}_{1+\mathfrak{m}}$ lorsque $x \in \mathfrak{m}$ sont déjà correctes pour l'anneau $\mathbf{B}_{3,x;1}$.

Poursuivons notre étude de $\mathfrak{m}$ sous l'hypothèse que $x \in \mathfrak{m}$[3].

Puisque le produit $B_1(x)B_1(x-3)B_1(x-6) = 3B_2(x) \in 3\mathbf{B} \subseteq \mathfrak{m}$, on a nécessairement $B_1(x) \in \mathfrak{m}$ ou $B_1(x-3) \in \mathfrak{m}$ ou $B_1(x-6) \in \mathfrak{m}$. Vu les automorphisme de $\mathbf{B}$ par translations, l'étude des trois cas est inutile. Il suffit d'étudier le premier.

Supposons $B_1(x) \in \mathfrak{m}$, alors puisque $(x-1)(x-2)$ est une unité modulo $\mathfrak{m}$, on a $\frac{x}{3} \in \mathfrak{m}\mathbf{V}$.
Donc $x \in 3\mathfrak{m} \subseteq \mathfrak{m}^2$.
Puisque $\frac{x-3}{3} = -1 + \frac{x}{3} \in -1 + \mathfrak{m}\mathbf{V}$, on obtient $\frac{x-3}{3} \in \mathbf{V}^\times$, c'est-à-dire $(x-3) \sim 3$ (cette notation signifie que 3 et $x-3$ sont associés dans $\mathbf{V}$). De même $\frac{x-6}{3} \in \mathbf{V}^\times$ et $(x-6) \sim 3$ dans $\mathbf{V}$.
On en déduit que si l'on considère $B_1(x-a)$ pour les 9 valeurs possibles de l'entier a modulo 9, seul $B_1(x)$ est dans $\mathfrak{m}$. Les 8 autres $B_1(x-a)$ sont des unités modulo $\mathfrak{m}$[4]. Concernant les $(x-a)$, on a $x \in \mathfrak{m}^2$, $(x-3) \sim (x-6) \sim 3$, et les 6 autres sont des unités.

Pour les premiers éléments de la $\mathbb{Z}_{(p)}$-base des A_n, on obtient les résultats suivants :

A_0	A_1	A_2	A_3	A_4	A_5	A_6	A_7	A_8	A_9	A_{10}	A_{11}	A_{12}	A_{13}	$\dots$
1	x	x^2	B_1	xB_1	x^2B_1	B_1^2	xB_1^2	$x^2B_1^2$	B_2	xB_2	x^2B_2	B_1B_2	xB_1B_2	$\dots$
$=0$	≥ 2	≥ 4	≥ 1	≥ 3	≥ 5	≥ 2	≥ 4	≥ 6	≥ 0	≥ 2	≥ 4	≥ 1	≥ 3	$\dots$

Soit $f \in \mathbf{B}$ de degré ≤ 2.
- Si $f(0) \not\equiv 0 \bmod 3$ alors $f \in \mathbf{V}^\times$.
- Si $f(0) \equiv 3$ ou $6 \bmod 9$ alors $f \sim 3$ dans $\mathbf{V}$.
- Si $f(0) \equiv 0 \bmod 9$ alors $f \in \mathfrak{m}^2$.

Soit maintenant g de degré ≤ 8 et ≥ 3.
- Si $g(0) \not\equiv 0 \bmod 3$ alors $g \in \mathbf{V}^\times$.
- Si $g(0) \equiv 0 \bmod 3$ alors $g \in \mathfrak{m}$.

3. Comme nous l'avons déjà indiqué, on ne perd pas de généralité en supposant $x \in \mathfrak{m}$: par exemple si $x-1 \in \mathfrak{m}$ on peut faire la translation $x \mapsto x+1$ qui nous ramène au cas précédent.

4. De la même manière, dans le cas où $B_1(x-3) \in \mathfrak{m}$, la translation $x \mapsto x+3$ qui nous ramène au cas précédent : on a alors $x-3 \in \mathfrak{m}^2$ et si l'on considère les $B_1(x-a)$ pour les 9 valeurs possibles de l'entier a modulo 9, seul $B_1(x-3)$ est dans $\mathfrak{m}$.
Notons cependant que $B_1(x) \in \mathfrak{m}$ n'implique pas $x \in \mathfrak{m}$. On peut avoir par exemple $x-1 \in \mathfrak{m}$ et $B_1(x) \in \mathfrak{m}$ avec x et $x-2$ des unités modulo $\mathfrak{m}$, et $x-1 \in \mathfrak{m}^2$.

Du point de vue des approximations, les mêmes raisonnements (en utilisant le lemme 1.3) nous apprennent que le monoïde $\mathcal{S}(3,x;1)$ est recouvert par les 3 monoïdes

$$\mathcal{S}(3,x,B_1(x);1),\ \ \mathcal{S}(3,x,B_1(x-3);1)\ \text{ et }\ \mathcal{S}(3,x,B_1(x-6);1).$$

Comme ces monoïdes se déduisent les uns des autres par translation, nous savons qu'ils sont non triviaux, car si l'un était trival les trois le seraient et $\mathcal{S}(3,x;1)$ serait lui-même trivial([5]).

Dans l'anneau $\mathbf{C}=\mathbf{B}_{3,x,B_1(x);1}$, notons $\mathfrak{b}=\langle 3,x,B_1(x)\rangle$. Alors
- $x\in\mathfrak{b}^2$,
- $x-3\sim x-6\sim 3$ dans $\mathbf{C}$,
- $x-1$, $x-2$, $x-4$, $x-5$, $x-7$ et $x-8\in\mathbf{C}^\times$,
- $B_1(x)\in 3\mathbf{C}$, et
- $B_1(x-1),\ldots,B_1(x-8)\in\mathbf{C}^\times$,
- $\mathfrak{b}=\langle 3\rangle$.

On en déduit quelques informations partielles. Soit $f\in\mathbf{B}$ de degré ≤ 2.
- Si $f(0)\not\equiv 0 \bmod 3$ alors $f\in\mathbf{C}^\times$.
- Si $f(0)\equiv 3$ ou $6 \bmod 9$ alors $f\sim 3$ dans $\mathbf{C}$.
- Si $f(0)\equiv 0 \bmod 9$ alors $f\in\mathfrak{b}^2$.

Soit maintenant g de degré ≤ 8.
- Si $g(0)\not\equiv 0 \bmod 3$ alors $g\in\mathbf{C}^\times$.
- Si $g(0)\equiv 0 \bmod 3$, alors $g\in\mathfrak{b}$.

Autrement dit, les informations que nous avons indiquées concernant le localisé $\mathbf{B}_{1+\mathfrak{m}}$ lorsque x et $B_1\in\mathfrak{m}$ sont déjà correctes pour l'anneau $\mathbf{C}=\mathbf{B}_{3,x,B_1;1}=\mathbf{B}_{1+\langle 3,x,B_1\rangle}$.

Poursuivons notre étude de $\mathfrak{m}$. De nouveau sans perte de généralité (grâce aux translations) nous pouvons supposer être dans le cas où x et $B_1(x)$ sont dans $\mathfrak{m}$.
Puisque le produit $B_2(x)B_2(x-9)B_2(x-18)=3B_3(x)\in 3\mathbf{B}\subseteq\mathfrak{m}$, on a nécessairement $B_2(x)\in\mathfrak{m}$ ou $B_2(x-9)\in\mathfrak{m}$ ou $B_2(x-18)\in\mathfrak{m}$. Vu les automorphisme de $\mathbf{B}$ par translations, l'étude des trois cas est inutile. Il suffit d'étudier le premier.

Supposons que $B_2(x)\in\mathfrak{m}$. On a $3B_2(x)=B_1(x)B_1(x-3)B_1(x-6)$. On sait déjà que $B_1(x)\in\mathfrak{m}$, et que $B_1(x-3)$ et $B_1(x-6)$ sont des unités. Donc $B_1(x)\in 3\mathfrak{m}\subseteq\mathfrak{m}^2$ et par suite $x\in 3\mathfrak{m}^2\subseteq\mathfrak{m}^3$.
Puisque $\frac{x-9}{9}=-1+\frac{x}{9}\in -1+\mathfrak{m}\mathbf{V}$, on obtient $\frac{x-9}{9}\in\mathbf{V}^\times$, c'est-à-dire $(x-9)\sim 9$ dans $\mathbf{V}$.

En raisonnant comme précédemment, on obtient que si l'on considère $B_2(x-a)$, pour les 27 valeurs possibles de l'entier a modulo 27, seul $B_2(x)$ est dans $\mathfrak{m}$. On obtient les résultats certifiés pour les premiers éléments de la base (A_n) indiqués dans le tableau qui suit.

A_0	A_1	A_2	A_3	A_4	A_5	A_6	A_7	A_8	A_9	A_{10}	A_{11}	A_{12}	A_{13}	$\ldots$
1	x	x^2	B_1	xB_1	x^2B_1	B_1^2	xB_1^2	$x^2B_1^2$	B_2	xB_2	x^2B_2	B_1B_2	xB_1B_2	$\ldots$
$=0$	≥ 3	≥ 6	≥ 2	≥ 5	≥ 8	≥ 4	≥ 7	≥ 10	≥ 1	≥ 4	≥ 7	≥ 3	≥ 6	$\ldots$

Du point de vue des approximations, les mêmes raisonnements nous apprennent que le monoïde $\mathcal{S}(3,x,B_1(x);1)$ est recouvert par les 3 monoïdes

$$\mathcal{S}(3,x,B_1(x),B_2(x);1),\ \ \mathcal{S}(3,x,B_1(x),B_2(x-9);1)\ \text{ et }\ \mathcal{S}(3,x,B_1(x),B_2(x-18);1).$$

Nous savons aussi qu'ils sont non triviaux.

Considérons l'anneau $\mathbf{D}=\mathbf{B}_{3,x,B_1(x),B_2(x);1}$ et l'idéal $\mathfrak{c}=\langle 3,x,B_1(x),B_2(x)\rangle$. Les mêmes raisonnements que précédemment montrent que $\mathfrak{c}=\langle 3\rangle$. Le tableau ci-dessus implique les précisions suivantes concernant un élément $f\in\mathbf{B}$ de degré ≤ 2.
- Si $f(0)\not\equiv 0 \bmod 3$ alors $f\in\mathbf{D}^\times$.
- Si $f(0)\equiv 3$ ou $6 \bmod 9$ alors $f\sim 3$ dans $\mathbf{D}$.
- Si $f(0)\equiv 9$ ou $18 \bmod 27$ alors $f\sim 9$ dans $\mathbf{D}$.
- Si $f(0)\equiv 0 \bmod 27$ alors $f\in\mathfrak{c}^3$.

Soit maintenant g de degré ≤ 8.
- Si $g(0)\not\equiv 0 \bmod 3$ alors $g\in\mathbf{D}^\times$.
- Si $g(0)\equiv 3$ ou $6 \bmod 9$ alors $g\sim 3$ dans $\mathbf{D}$.

5. De même, par translation, le monoïde $\mathcal{S}(3,x-1;1)$ est recouvert par les 3 monoïdes non triviaux $\mathcal{S}(3,x-1,B_1(x-1);1)$, $\mathcal{S}(3,x-1,B_1(x-4);1)$ et $\mathcal{S}(3,x-1,B_1(x-7);1)$.

– Si $g(0) \equiv 0 \bmod 9$ alors $g \in \mathfrak{c}^2$.

Ces informations sont les mêmes que celles concernant le localisé $\mathbf{V} = \mathbf{B}_{1+\mathfrak{m}}$ lorsque x, B_1 et $B_2 \in \mathfrak{m}$: elles sont déjà correctes pour l'anneau $\mathbf{D} = \mathbf{B}_{3,x,B_1,B_2;1}$.

Plus généralement le même type de raisonnement conduit aux propositions suivantes.

Proposition 2.2. *Soit $\mathfrak{m}$ un idéal premier détachable de $\mathbf{E}_p$ avec $p \in \mathfrak{m}$ et $\mathbf{V}$ le localisé de $\mathbf{E}_p$ en $\mathfrak{m}$.*

1. *Pour tout $k > 0$ il existe un unique entier a_k modulo p^k tel que $B_\ell(x - a_k) \in \mathfrak{m}$ pour $\ell < k$. En outre $a_k \equiv a_{k+r} \bmod p^k$ pour $r > 0$.*
2. *On a alors pour $\ell < k$, $B_\ell(x - a_k) \in \mathfrak{m}^{k-\ell}$. En particulier $x - a_k \in \mathfrak{m}^k$.*
3. *Pour un f donné dans $\mathbf{E}_p$ et un exposant r donné, on a l'alternative suivante :*
   – *$f \in p^r\mathbf{V} \subseteq \mathfrak{m}^r$, ou bien*
   – *il existe $s \in [\![0..r-1]\!]$ tel que f est associé à p^s dans $\mathbf{V}$.*
4. *L'idéal $\mathfrak{m}$ est maximal, avec corps résiduel $\mathbb{F}_p$.*

Le dernier point découle du fait que tous les éléments de la $\mathbb{Z}_{(p)}$-base de $\mathbf{E}_p$ construite à partir des $B_k(x - a_k)$ $(k \geq 1)$, sont dans $\mathfrak{m}$, à l'exception de A_0.

Pour donner l'analogue de la proposition précédente en termes d'approximations, nous avons besoin de notations supplémentaires. On considère un nombre premier p fixé et le monoïde $S_0 = \mathcal{S}(p; 1)$ de $\mathbf{E}_p$. Soit un entier $k \geq 0$ et un entier a_k modulo p^k. On définit de manière récursive le monoïde $S_{k,a_k} = \mathcal{S}(I_{k,a_k}; 1)$ de $\mathbf{E}_p$ comme suit.

– Tout d'abord $S_{1,r} = \mathcal{S}(p, x - r; 1) = \mathcal{S}\big(p, B_0(x - r); 1\big)$ $(0 \leq r < p)$.
– Ensuite, pour $k \geq 2$ si $a_{k-1} \equiv a_k \bmod p^{k-1}$ on pose $I_{k,a_k} = I_{k-1,a_{k-1}}, B_{k-1}(x - a_k)$.

Par exemple avec $p = 3$,

– $S_{2,5} = \mathcal{S}\big(3, x - 2, B_1(x - 5); 1\big) = \mathcal{S}\big(3, x - 5, B_1(x - 5); 1\big)$.
  C'est un translaté de $S_{2,0} = \mathcal{S}(3, x, B_1(x); 1)$.
– $S_{3,14} = \mathcal{S}\big(3, x - 2, B_1(x - 5), B_2(x - 14); 1\big) = \mathcal{S}\big(3, x - 14, B_1(x - 14), B_2(x - 14); 1\big)$.
  C'est un translaté de $S_{3,0} = \mathcal{S}(3, x, B_1(x), B_2(x); 1)$.

Proposition 2.3. *Avec les notations précédentes (et $\mathbf{E}_p = \mathbf{B}$).*

1. *Le monoïde S_{k,a_k} est recouvert par les p monoïdes $S_{k+1,b}$ pour les $b \bmod p^{k+1}$ qui vérifient $b \equiv a_k \bmod p^k$.*
2. *En conséquence le monoïde S_0 est recouvert par les p^k monoïdes S_{k,a_k} où a_k parcourt tous les entiers modulo p^k.*
3. *On a alors pour $\ell < k$, $B_\ell(x - a_k) \in p^{k-\ell}\mathbf{B}_{S_{k,b}}$. En particulier $x - a_k \in p^k\mathbf{B}_{S_{k,b}}$.*
4. *Pour un f fixé dans $\mathbf{E}_p$ et un exposant r donné, il existe un entier k tel que pour chaque b modulo p^k, on a l'alternative suivante :*
   – *$f \in p^r\mathbf{B}_{S_{k,b}}$, ou bien*
   – *il existe $s \in [\![0..r-1]\!]$ tel que f est associé à p^s dans $\mathbf{B}_{S_{k,b}}$.*

On termine cette section en donnant la description complète de tous les idéaux premiers détachables de $\mathbf{E}_p$ qui contiennent p (nous savons maintenant qu'ils sont maximaux).

Ce résultat est mis ici pour satisfaire la curiosité de la lectrice concernant ce que l'on peut traiter de manière entièrement constructive, mais nous ne l'utiliserons pas dans la suite.

Nous utilisons la notation usuelle

$$\mathbb{Z}_p = \varprojlim(\mathbb{Z}/p^k\mathbb{Z})$$

pour l'anneau des entiers p-adiques. On remarque que tout $f \in \mathbf{E}_p$ peut être évalué en n'importe quel $\xi \in \mathbb{Z}_p$. Cela tient à ce que si $\deg(f) < p^k$ alors $f(x)$ modulo p^r ne dépend que de x modulo p^{k+r}.

Si pour chaque k on sélectionne l'entier a_k modulo p^k tel que $B_\ell(x - a_k) \in \mathfrak{m}$ pour $0 < \ell \leq k$, on obtient une suite qui détermine un entier p-adique ξ. Cet entier p-adique jouira de la propriété suivante : en évaluant un $f \in \mathbf{E}_p$ arbitraire en ξ, on obtient que $f \in \mathfrak{m}^k$ dans $\mathbf{E}_p$ si, et seulement si, $f(\xi) \in p^k\mathbb{Z}_p$. En effet, pour $\xi = 0$ cela se voit clairement en écrivant f sur la $\mathbb{Z}_{(p)}$-base $(A_n)_{n\in\mathbb{N}}$. Et le cas général s'en déduit par translations.

Proposition 2.4. *Soit $\mathfrak{m}$ un idéal premier détachable de $\mathbf{E}_p$ avec $p \in \mathfrak{m}$ (donc $\mathfrak{m}$ est maximal).*

(1) *Il existe un unique entier p-adique* ξ *tel que* $\mathfrak{m} = \{\, f \in \mathbf{E}_p \mid f(\xi) \in p\mathbb{Z}_p \,\}$.
En outre, pour tout $k > 0$ *on a* $f \in \mathfrak{m}^k$ *si, et seulement si,* $f(\xi) \in p^k\mathbb{Z}_p$.

On note $\mathfrak{m} = \mathfrak{m}_\xi$ *et* $\mathbf{V}_\xi = (1+\mathfrak{m}_\xi)^{-1}\mathbf{E}_p$.

(2) *L'application* $f \mapsto f(\xi)$ *de* $\mathbf{E}_p$ *dans* $\mathbb{Z}_p$ *se prolonge en un homomorphisme local* $\theta_\xi : \mathbf{V}_\xi \to \mathbb{Z}_p$.

(3) *Si* ξ *est transcendant sur* $\mathbb{Z}_{(p)}$, θ_ξ *est injectif, l'intersection des* $\mathfrak{m}^k$ *est réduite à* 0 *et* $\mathbf{V}_\xi$ *est un anneau de valuation discrète d'uniformisante* p.

(4) *Si* ξ *est entier sur* $\mathbb{Z}_{(p)}$, $\operatorname{Ker}\theta_\xi$ *est un idéal premier non nul strictement contenu dans* $\mathfrak{m}_\xi$, *et* $\mathbf{V}_\xi$ *est de dimension de Krull* 2.

Notez cependant que l'on n'a pas moyen de tester la transcendance de ξ sous la seule l'hypothèse concernant $\mathfrak{m}$ qu'il s'agit d'un idéal premier détachable contenant p.

3. Des anneaux de Prüfer

De la proposition 2.2 on déduit que l'anneau $\mathbf{V}$ (localisé de $\mathbf{E}_p$ en $\mathfrak{m}$) est un anneau de valuation.

Théorème 1. *Soit* $\mathfrak{m}$ *un idéal premier détachable de* $\mathbf{E}_p$ *avec* $p \in \mathfrak{m}$ *et* $\mathbf{V}$ *le localisé de* $\mathbf{E}_p$ *en* $\mathfrak{m}$. *Alors* $\mathbf{V}$ *est un anneau de valuation.*

▷ Soient f, $g \neq 0$ dans $\mathbf{E}_p$. Dans l'anneau de Bezout $\mathbb{Q}[x]$ on a des polynômes h, F, G, u, v tels que

$$g = hG,\ f = hF,\ uF + vG = 1$$

En multipliant par des puissances de p convenables, on obtient des exposants r, $m \geq 0$ et des polynômes h_1, F_1, G_1, u_1, $v_1 \in \mathbf{E}_p$ tels que

$$p^m g = h_1 G_1,\ p^m f = h_1 F_1,\ u_1 F_1 + v_1 G_1 = p^r.$$

On doit montrer que g divise f ou f divise g dans $\mathbf{V}$, ou, ce qui revient au même, que G_1 divise F_1 ou F_1 divise G_1 dans $\mathbf{V}$. L'égalité $u_1F_1 + v_1G_1 = p^r$ interdit que F_1 et G_1 soient tous deux dans $p^{r+1}\mathbf{V}$. La proposition 2.2 appliquée avec F_1 et G_1 nous permet donc d'affirmer que
- ou bien F_1 et G_1 sont associés à p^s et p^t pour deux entiers s et $t \in [\![0..r]\!]$,
- ou bien F_1 est associé à p^s pour un entier $s \in [\![0..r]\!]$ et $G_1 \in p^{r+1}\mathbf{V}$,
- ou bien G_1 est associé à p^s pour un entier $s \in [\![0..r]\!]$ et $F_1 \in p^{r+1}\mathbf{V}$.

Dans chaque cas l'un des deux divise l'autre. ◁

Essentiellement la même démonstration nous donne de façon constructive le résultat souhaité pour les anneaux des polynômes à valeurs entières $\mathbf{E}_p$ et $\mathbf{E}$.

Théorème 2. *Les anneaux des polynômes à valeurs entières* $\mathbf{E}$ *et* $\mathbf{E}_p$ *sont des anneaux de Prüfer au sens constructif : tout idéal de type fini est de façon explicite localement principal.*

▷ Nous faisons la démonstration pour $\mathbf{E}$ qui est plus générale. Soient f, g non nuls arbitraires dans $\mathbf{E}$. Nous devons construire une matrice de localisation principale pour (f, g) dans $\mathbf{E}$ (voir les équations (1) et (2)). Dans l'anneau de Bezout $\mathbb{Q}[x]$ on calcule une relation de Bezout fournissant le pgcd h de f et g, donnée par des polynômes h, F, G, u, v tels que

$$g = hG,\ f = hF,\ uF + vG = 1$$

Avec des entiers convenables μ et $\rho > 0$, on obtient des polynômes h_1, F_1, G_1, u_1, $v_1 \in \mathbf{E}$ tels que

$$\mu g = h_1 G_1,\ \mu f = h_1 F_1,\ u_1 F_1 + v_1 G_1 = \rho.$$

On note qu'une matrice de localisation principale pour (f, g) est la même chose qu'une matrice de localisation principale pour (F_1, G_1).
Il suffit de montrer que l'on peut construire une matrice de localisation principale pour (F_1, G_1) sur $\mathbf{E}_{\mathcal{S}(0;\rho)} = \mathbf{E}[1/\rho]$ et une autre sur $\mathbf{E}_{\mathcal{S}(\rho;1)} = \mathbf{E}_{1+\rho\mathbf{E}}$ (lemmes 1.4 et 1.2).
Sur $\mathbf{E}[1/\rho]$ on a la matrice de localisation principale

$$\frac{1}{\rho}\begin{bmatrix} u_1F_1 & u_1G_1 \\ v_1F_1 & v_1G_1 \end{bmatrix}$$

Le monoïde $\mathcal{S}(\rho;1)$ est recouvert par les monoïdes $\mathcal{S}(q_i;1)$ où $\rho = \prod_i q_i$ (lemme 1.3), et chaque q_i est la puissance d'un nombre premier p_i. Les monoïdes $\mathcal{S}(q_i;1)$ et $\mathcal{S}(p_i;1)$ donnent la même localisation (ils définissent les mêmes filtres). Il suffit donc de construire une matrice de localisation principale pour (F_1, G_1) sur chacun des $\mathbf{E}_{\mathcal{S}(p_i;1)}$ (lemme 1.4). On note que l'on a sur $\mathbf{E}_{p_i}$ (qui est une localisation beaucoup moins poussée de $\mathbf{E}$) une égalité

$$u_1F_1 + v_1G_1 = c_i\, p_i^{r_i} \quad (c_i \in \mathbb{Z}_{(p)}{}^{\times}).$$

Pour construire une matrice de localisation principale sur $\mathbf{E}_{\mathcal{S}(p_i;1)}$ il suffit de le faire pour des localisations plus poussées en des monoïdes qui recouvrent $\mathbf{E}_{\mathcal{S}(p_i;1)}$. La proposition 2.3 nous dit que pour une famille finie de monoïdes non triviaux qui recouvrent $\mathcal{S}(p_i;1)$, vue l'égalité $u_1F_1 + v_1G_1 = c_i\, p_i^{r_i}$ qui interdit que F_1 et G_1 soient tous deux multiples de $p_i^{r_i+1}$, on est certain de pouvoir expliciter que F_1 divise G_1 ou G_1 divise F_1 dans chaque localisé. Et naturellement si dans un anneau on a $ax = y$ cela donne la matrice de localisation principale $\begin{bmatrix} 1 & a \\ 0 & 0 \end{bmatrix}$ pour (x, y). ◁

Un exemple. Nous traitons un exemple simple qui montre qu'il est sans doute possible d'optimiser l'algorithme sous-jacent à la démonstration constructive du théorème 2 en tenant compte du fait que de nombreuses branches de l'arbre peuvent être regroupées en utilisant judicieusement le lemme 1.2.

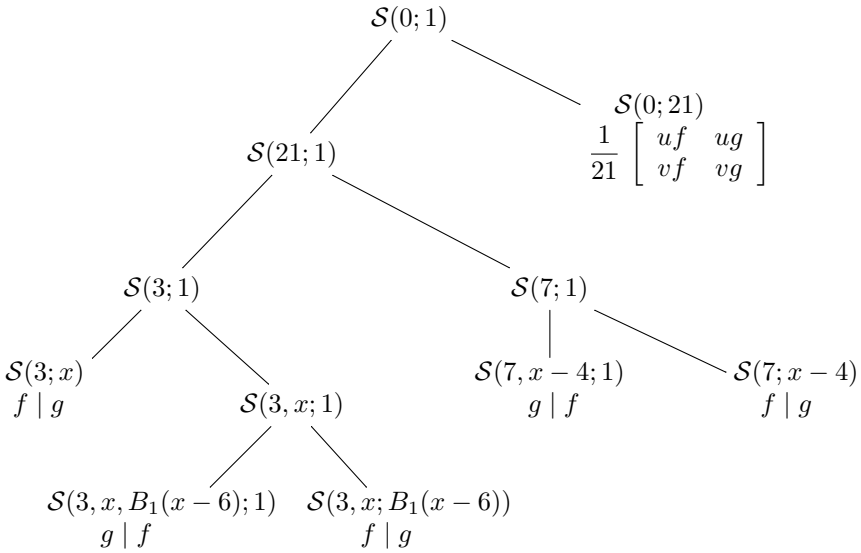
Nous considérons les polynômes

$$f = 3 + x, \qquad g = -3 + 2x(x-1).$$

On obtient en calculant leur résultant

$$uf + vg = 21 \quad \text{avec} \quad u = 8 - 2x \text{ et } v = 1.$$

L'arbre des localisations que l'on construit est alors le suivant.



(1) En $\mathcal{S}(0;21)$, la matrice de localisation principale est

$$\frac{1}{21}\,M_{0;21} \quad \text{avec} \quad M_{0;21} = \begin{bmatrix} uf & ug \\ vf & vg \end{bmatrix}.$$

(2) En $\mathcal{S}(3;x)$, $f = 3 + x$ est une unité, ce qui donne la matrice de localisation principale

$$\frac{1}{f}\,M_{3;x} \quad \text{avec} \quad M_{3;x} = \begin{bmatrix} f & g \\ 0 & 0 \end{bmatrix}$$

(3) La feuille $\mathcal{S}(7;x-4)$ peut être comprise comme regroupant les 6 feuilles $\mathcal{S}(7,x-i;1)$ ($i \not\equiv 4 \bmod 7$) pour lesquelles f est une unité. Ici $f = 7 + (x-4)$ est une unité, ce qui donne la matrice de localisation principale

$$\frac{1}{f}\,M_{7;x-4} \quad \text{avec} \quad M_{7;x-4} = \begin{bmatrix} f & g \\ 0 & 0 \end{bmatrix}$$

(4) En $\mathcal{S}(7, x-4; 1)$ on écrit $g(x) = 21+14(x-4)+2(x-4)^2$ qui montre que $g \sim 7$. Plus précisément $(x-4)U(x) = 7V(x)$ avec $V(x) = \frac{1}{7}\prod_{i=0}^{6}(x-i)$ et donc

$$U^2 g = 7 \times (3U + 7(2UV + 2V^2)), \quad U^2 f = 7 \times U(U+V)$$

ce qui donne la matrice de localisation principale $\frac{1}{g}\begin{bmatrix} 0 & 0 \\ f & g \end{bmatrix}$ ou, mieux

$$\frac{1}{W} M_{7,x-4;1} \quad \text{avec} \quad M_{7,x-4;1} = \begin{bmatrix} 0 & 0 \\ U(U+V) & W \end{bmatrix}$$

et $W = 3U + 7(2UV + 2V^2)$. Posons $y = x - 4$. Puisque

$$U = \prod\nolimits_{i\in[\![0..6]\!], i\neq 4}(y+4-i) \;\equiv\; 48 \bmod y \;\equiv\; -1 \bmod \langle 7, y\rangle,$$

U et W sont des unités, en particulier nous pouvons écrire dans $\mathbf{E}$,

$$2W = 1 + 7\,W_1 + (x-4)\,W_2 \in \mathcal{S}(7, x-4; 1).$$

(5) Nous calculons maintenant une matrice de localisation principale en $\mathcal{S}(7;1)$ en combinant celles obtenues en $\mathcal{S}(7; x-4)$ et $\mathcal{S}(7, x-4; 1)$. En posant

$$M_{7;1} = 2M_{7,(x-4);1} - W_2 M_{7;x-4},$$

nous trouvons une matrice à coefficients dans $\mathbf{E}$ dont les lignes sont proportionnelles à (f, g) et dont la trace est égale à

$$1 + 7W_1 + (x-4)\,W_2 - (7 + (x-4))\,W_2 = 1 + 7\,(W_1 - W_2) = 1 + 7\,W_3$$

ce qui donne la matrice de localisation principale

$$\frac{1}{1+7W_3} M_{7;1}$$

(6) En $\mathcal{S}(3, x; 1)$, f et g sont dans le radical, mais aucun n'a une « valuation » fixée. L'élément $x - 2 = 1 - 3 + x$ est une unité et $(x-2)g = -3 + 6B_1 = 3(2B_1 - 1)$.
Nous devons a priori ouvrir les trois branches $\mathcal{S}(3, x, B_1(x-3i); 1)$ $(i = 0, 1, 2)$. En fait f est associé à 3 dans les deux premières, nous notons $Q = B_1(x-6)$ et nous ouvrons seulement deux branches $\mathcal{S}(3, x; Q)$ et $\mathcal{S}(3, x, Q; 1)$. Nous écrivons

$$f = 9 + (x-6), \quad g = 3 + 54 + 22(x-6) + 2(x-6)^2.$$

(7) Dans la branche $\mathcal{S}(3, x; Q)$, $x-6$ est associé à 3, f est associé à 3 et f divise g.
Écrivons ceci dans $\mathbf{E}$. Notons $P = (x-7)(x-8)$ avec $-P \in \mathcal{S}(3, x; 1)$ et $(x-6)P = 3Q$. Alors

$$\begin{aligned} Pf &= 3 \times (Q + 3P) \\ Pg &= (x-7)(x-2-6)g = (x-7)(x-2)g - 6(x-7)g \\ &= 3(x-7)(2B_1 - 1 - 4g) = 3R \end{aligned}$$

ce qui donne la matrice de localisation principale $\frac{1}{f}\begin{bmatrix} f & g \\ 0 & 0 \end{bmatrix}$ ou mieux

$$\frac{1}{Q+3P} M_{3,x;Q} \quad \text{avec} \quad M_{3,x;Q} = \begin{bmatrix} Q+3P & R \\ 0 & 0 \end{bmatrix}$$

(8) Dans la branche $\mathcal{S}(3, x, Q; 1)$, $x-6$ est multiple de 9, g est associé à 3 et divise f. Écrivons ceci dans $\mathbf{E}$. On a $B_1(x)B_1(x-3)Q = 3B_2$, et en posant $z = x - 6$ on obtient que

$$\begin{aligned} B_1(x-3) &= 2 + 3z + 3z^2 + Q \quad \equiv \; 2 \bmod \langle 3, x, Q\rangle \\ B_1(x) &= 40 + 24z + 6z^2 + Q \quad \equiv \; 1 \bmod \langle 3, x, Q\rangle \end{aligned}$$

sont des unités. Enfin en posant $b = (x-7)(x-8)B_1(x)B_1(x-3)$ on obtient $b \times (x-6) = 9B_2$ avec $b \equiv 1 \bmod \langle 3, x, Q\rangle$, c'est-à-dire $b = 1 + 3b_1 + xb_2 + Qb_3$. Donc

$$\begin{aligned} bg &= 3 \times (b + 3 \times (6b + 22B_2 + 2(x-6)B_2)) \\ &= 3 \times (1 + 3b_4 + xb_2 + Qb_3) = 3 \times (1 + b_5) \\ bf &= 9 \times (b + B_2) = 3 \times b_6 \end{aligned}$$

ce qui donne la matrice de localisation principale en $\mathcal{S}(3, x, Q; 1)$

$$\frac{1}{1+b_5}\, M_{3,x,Q;1} \quad \text{avec} \quad M_{3,x,Q;1} = \begin{bmatrix} 0 & 0 \\ b_6 & 1+b_5 \end{bmatrix}$$

(9) On utilise les résultats de 7. et 8. pour obtenir une matrice de localisation principale en $\mathcal{S}(3, x; 1)$: la matrice $M_{3,x;1} = -b_3\, M_{3,x;Q} + M_{3,x,Q;1}$ a ses lignes proportionnelles à (f, g) et sa trace est égale à $1 + 3b_4 + xb_2 - 3Pb_3 = 1 + 3b_7 + xb_2 \in \mathcal{S}(3, x; 1)$.

(10) On utilise les résultats de 2. et 9. pour obtenir une matrice de localisation principale en $\mathcal{S}(3; 1)$: la matrice $M_{3;1} = M_{3,x;1} - b_2\, M_{3;x}$ a ses lignes proportionnelles à (f, g) et sa trace est égale à $1 + 3b_7 - 3b_2 = 1 + 3b_8 \in \mathcal{S}(3; 1)$.

(11) On utilise les résultats de 5. et 10. pour obtenir une matrice de localisation principale en $\mathcal{S}(21; 1)$: la matrice $M_{21;1} = 7\, M_{3;1} - 6\, M_{7;1}$ a ses lignes proportionnelles à (f, g) et sa trace est égale à $1 + 21(b_8 - 2W_3) = 1 + 21b_9 \in \mathcal{S}(21; 1)$

(12) On utilise les résultats de 1. et 11. pour obtenir une matrice de localisation principale sur $\mathbf{E}$: la matrice $M_{0;1} = M_{21;1} - b_9\, M_{0;21}$ a ses lignes proportionnelles à (f, g) et sa trace est égale à 1.

Références

[1] Bishop E. *Foundations of Constructive Analysis.* McGraw Hill, (1967).

[2] Bishop E., Bridges D. *Constructive Analysis.* Springer-Verlag, (1985).

[3] Bridges D., Richman F. *Varieties of Constructive Mathematics.* London Math. Soc. LNS 97. Cambridge University Press (1987).

[4] Chabert J.-L. *Anneaux de polynômes à valeurs entières et anneaux de Fatou.* Bull. soc. math. France, **99**, (1971), 273–283.

[5] Chabert J.-L. *Un anneau de Prüfer.* Journal of Algebra, **107**, (1987), 1–16.

[6] Coquand T. *Sur un théorème de Kronecker concernant les variétés algébriques.* C. R. Acad. Sci. Paris, Ser. I, **338**, (2004), 291–294.

[7] Coquand T. *On seminormality.* Journal of Algebra, **305**, (2006), 585–602.

[8] Coquand T. *Space of valuations*, Annals of Pure and Applied Logic, **157**, (2009), 97-109.

[9] Coquand T., Lombardi H. *A logical approach to abstract algebra.* (survey) Math. Struct. in Comput. Science, **16**, (2006), 885–900.

[10] Coquand T., Lombardi H., Quitté C. *Generating non-Nœtherian modules constructively.* Manuscripta mathematica, **115**, (2004), 513–520.

[11] Coquand T., Lombardi H., Schuster P. *Spectral Schemes as Ringed Lattices.* Annals of Mathematics and Artificial Intelligence. **56**, (2009), 339–360.

[12] Coquand T., Quitté C. *Constructive Finite Free Resolutions.* Preprint 2011.

[13] Coste M., Lombardi H., Roy M.-F. *Dynamical method in algebra : Effective Nullstellensätze.* Annals of Pure and Applied Logic **111**, (2001) 203–256.

[14] Díaz-Toca G., Lombardi H. *Dynamic Galois Theory.* Journal of Symbolic Computation. **45**, (2010) 1316–1329.

[15] Ducos L., Lombardi H., Quitté C., Salou M. *Théorie algorithmique des anneaux arithmétiques, des anneaux de Prüfer et des anneaux de Dedekind.* Journal of Algebra, **281**, (2004), 604–650.

[16] Gilmer R. *Multiplicative Ideal Theory.* Queens papers in pure and applied Math, vol. 90, 1992.

[17] Jensen C. *Arithmetical rings.* Acta Mathematica Academiae Scientiarum Hungaricae, **17**, (1966) 115–123. Birkhäuser, (1991).

[18] Lombardi H. *Algèbre dynamique, espaces topologiques sans points et programme de Hilbert.* Annals of Pure and Applied Logic, **137**, (2006), 256–290.

[19] Lombardi H., Quitté C. *Constructions cachées en algèbre abstraite (2) Le principe local global*, dans : Commutative ring theory and applications, eds. Fontana M., Kabbaj S.-E., Wiegand S. Lecture notes in pure and applied mathematics vol 231. M. Dekker, (2002). p. 461–476.
[20] Lombardi H., Quitté C. *Algèbre commutative. Méthodes constructives.* Calvage & Mounet, (2011).
[21] Mines R., Richman F., Ruitenburg W. *A Course in Constructive Algebra.* Universitext. Springer-Verlag, (1988).
[22] Richman F. *Non trivial uses of trivial rings.* Proc. Amer. Math. Soc., **103**, (1988), 1012–1014.
[23] Yengui I. *Making the use of maximal ideals constructive.* Theoretical Computer Science, **392**, (2008) 174–178.

Current address: Équipe de Mathématiques, UMR CNRS 6623, UFR des Sciences et Techniques, Université de Franche-Comté, 25030 BESANCON cedex, FRANCE

E-mail address: henri.lombardi@univ-fcomte.fr