Dérivation arithmétique

Marie CALCAGNO

Décembre 2020

Professeur encadrant : Bernard LE STUM

Table des matières

Introduction :

La dérivation arithmétique est une notion qui a été introduite par André Joyal dans les années 1980. Nous pouvons construire à partir de cette notion ce que l'on appelle les δ-anneaux, que nous allons introduire et étudier dans la première partie de ce document. L'idée de Joyal est d'obtenir la théorie des λ-anneaux à partir de celle des δ-anneaux, et pour cela il construit les P-anneaux (où P est un ensemble de nombres premiers) à partir des δ-anneaux puis il montre que les concepts de P-anneaux et de λ-anneaux sont équivalents lorsque P est l'ensemble de tous les nombres premiers. La notion de dérivation arithmétique a ensuite été reprise et développée par Alexandru Buium dans les années 2000. Les travaux de Buium sur la dérivation arithmétique, que nous allons étudier dans une seconde partie, ont pour but de développer un analogue arithmétique de la dérivation. Enfin, ces dernières années, de nouveaux travaux sur ce sujet ont été effectués par Bhargav Bhatt et Peter Scholze. Ces derniers s'appuient notamment sur la notion de Frobenius et l'utilisent pour la théorie de Hodge p-adique.

1 δ-structures

1.1 Définitions

Soit A un anneau commutatif unitaire et soit p un nombre premier.

Définition 1.1. *Un **vecteur de Witt** à coefficients dans A est une suite infinie de la forme $(f_0, \dots, f_m, \dots)$ avec $f_0, \dots, f_m, \dots \in A$. Pour tout $n \in \mathbb{N}$, le **n-ième polynôme de Witt** est :*

$$W_n(f_0, \dots, f_m, \dots) = f_0^{p^n} + pf_1^{p^{n-1}} + \cdots + p^n f_n.$$

Nous allons nous intéresser au cas où $n = 1$. Nous avons alors $W_1(f, g) = f^p + pg$ pour $f, g \in A$. L'**anneau des vecteurs de Witt** (de type p) de longueur 2 sur l'anneau commutatif A est $W_1(A) = A \times A$ muni des lois suivantes : pour $f, g, f', g' \in A$,

- $(f, g) + (f', g') = \left(f + f', g + g' - \sum_{k=1}^{p-1} \frac{1}{p}\binom{p}{k} f^{p-k} f'^k\right)$,

- $(f,g) \times (f',g') = (ff', f^p g' + g f'^p + p g g')$.

L'élément neutre pour l'addition (resp. la multiplication) est $(0,0)$ (resp. $(1,0)$).

Avant d'introduire les δ-structures, donnons la définition d'une p-dérivation :

Définition 1.2. *Une p-**dérivation** est une application $\delta : A \to A$ telle que :*

1. $\delta(0) = \delta(1) = 0$,
2. $\forall f,g \in A, \delta(f+g) = \delta(f) + \delta(g) - \sum_{k=1}^{p-1} \frac{1}{p}\binom{p}{k} f^{p-k} g^k$,
3. $\forall f,g \in A, \delta(fg) = f^p \delta(g) + \delta(f) g^p + p\delta(f)\delta(g)$.

Définition 1.3. *On considère le 0-ième polynôme de Witt W_0. Une δ-**structure** est une section de W_0 :*

$$\begin{aligned} A \to\ & W_1(A)\ . \\ f \mapsto\ & (f, \delta(f)) \end{aligned}$$

Lemme 1.4. *Se donner une δ-structure équivaut à se donner une p-dérivation.*

Démonstration : Soit δ une p-dérivation. Pour $f, f' \in A$, l'application $f \in A \mapsto (f, \delta(f)) \in W_1(A)$ vérifie :

- $(0, \delta(0)) = (0,0)$,
- $(1, \delta(1)) = (1,0)$,
- $(f,\delta(f)) + (f', \delta(f')) = \left(f + f', \delta(f) + \delta(f') - \sum_{k=1}^{p-1} \frac{1}{p}\binom{p}{k} f^{p-k} f'^k\right) = (f+f', \delta(f+f'))$,
- $(f,\delta(f))(f',\delta(f')) = (ff', f^p\delta(f') + \delta(f)f'^p + p\delta(f)\delta(f')) = (ff', \delta(ff'))$

donc c'est un morphisme d'anneaux. Comme $W_0(f,\delta(f)) = f$, le morphisme $f \in A \mapsto (f,\delta(f)) \in W_1(A)$ est une section de W_0 et donc une δ-structure. Réciproquement, soit

$$\begin{aligned} \sigma : A \to\ & W_1(A) \\ f \mapsto\ & (f, \delta(f)) \end{aligned}$$

une δ-structure. Par définition σ est une section de W_0 et on a $W_0(f,\delta(f)) = W_0 \circ \sigma(f) = f$. Vérifions que δ est une p-dérivation. Comme σ est à valeurs dans $W_1(A)$, il vient pour $f, f' \in A$:

$$(f,\delta(f)) + (f', \delta(f')) = \left(f + f', \delta(f) + \delta(f') - \sum_{k=1}^{p-1} \frac{1}{p}\binom{p}{k} f^{p-k} f'^k\right)$$

puis

$$W_0\left((f,\delta(f)) + (f', \delta(f'))\right) = W_0\left(f + f', \delta(f) + \delta(f') - \sum_{k=1}^{p-1} \frac{1}{p}\binom{p}{k} f^{p-k} f'^k\right) = f + f'$$

d'où $\delta(f+f') = \delta(f) + \delta(f') - \sum_{k=1}^{p-1} \frac{1}{p}\binom{p}{k} f^{p-k} f'^k$. On a de même que :

$$W_0((f,\delta(f)) \times (f',\delta(f'))) = W_0(ff', f^p\delta(f') + \delta(f)f'^p + p\delta(f)\delta(f')) = ff'$$

d'où $\delta(ff') = f^p\delta(f') + \delta(f)f'^p + p\delta(f)\delta(f')$. Enfin, on obtient que $\delta(0) = 0$ (resp. $\delta(1) = 0$) en considérant l'élément neutre pour l'addition (resp. multiplication) de $W_1(A)$. $\square$

Définition 1.5. *Un δ-**anneau** est un anneau commutatif doté d'une δ-structure. Autrement dit, c'est un couple (A, δ) composé d'un anneau commutatif A et d'une p-dérivation $\delta : A \to A$. Si le contexte est clair, on peut seulement noter A au lieu de (A,δ). Un δ-**sous-anneau** d'un δ-anneau A est un sous-anneau B de A tel que $\delta B \subset B$.*

Définition 1.6. *Un **morphisme de δ-anneaux** (ou δ-morphisme) est un morphisme d'anneaux qui préserve δ. Autrement dit, si A, B sont deux δ-anneaux, un morphisme d'anneaux $u : A \to B$ est un morphisme de δ-anneaux si $u \circ \delta = \delta \circ u$.*

Remarque 1.7. *On obtient la catégorie $\underline{\delta A}$ des δ-anneaux : les objets sont les δ-anneaux, les flèches sont les morphismes de δ-anneaux. On dispose alors du foncteur oubliant $G : \underline{\delta A} \to \underline{A}$ où $\underline{A}$ désigne la catégorie des anneaux.*

Définition 1.8. *Soit R un δ-anneau fixé. Un **δ-anneau sur** R (ou $\delta - R$-algèbre) est un δ-anneau A muni d'un morphisme de δ-anneaux $R \to A$. Un **morphisme de δ-anneaux sur** R est un morphisme de δ-anneaux qui est un morphisme de R-algèbres. On obtient la catégorie $\underline{R_\delta}$ des δ-anneaux sur R.*

Proposition 1.9. *Soit R un δ-anneau fixé et soit A un δ-anneau sur R. Notons f_i pour $i \in E$ les générateurs de A sur R (on notera alors $A = R[(f_i)_{i \in E}]$). Une δ-structure sur A est déterminée de manière unique par l'action de δ sur les f_i.*

Démonstration : D'après le lemme 1.4, se donner une δ-structure revient à se donner une p-dérivation δ. La proposition découle alors directement des axiomes de la définition de la p-dérivation δ (définition 1.2). □

Définition 1.10. *Un **Frobenius** sur A est un endomorphisme ϕ de A qui vérifie :*

$$\forall f \in A, \phi(f) \equiv f^p \mod p.$$

Donnons un exemple de Frobenius : soit A un δ-anneau, l'application $\phi : \begin{array}{rcl} A & \to & A \\ f & \mapsto & f^p + p\delta(f) \end{array}$ est un Frobenius sur A. En effet, il est clair que $\phi(f) \equiv f^p \mod p$ pour tout $f \in A$ et on a la proposition suivante :

Proposition 1.11. *Soit A un δ-anneau. L'application $\phi : f \in A \mapsto f^p + p\delta(f) \in A$ est un endomorphisme de A.*

Démonstration : Pour $f, f' \in A$, par définition d'une p-dérivation on a :

$$\begin{aligned}
\phi(f + f') &= (f + f')^p + p\delta(f + f') \\
&= (f + f')^p + p\left(\delta(f) + \delta(f') - \sum_{k=1}^{p-1} \frac{1}{p}\binom{p}{k} f^{p-k} f'^k\right) \\
&= f^p + p\delta(f) + f'^p + \delta(f') \\
&= \phi(f) + \phi(f'),
\end{aligned}$$

$$\begin{aligned}
\phi(ff') = (ff')^p + p\delta(ff') &= f^p f'^p + p(f^p\delta(f') + \delta(f)f'^p + p\delta(f)\delta(f')) \\
&= (f^p + p\delta(f))(f'^p + p\delta(f')) \\
&= \phi(f)\phi(f'),
\end{aligned}$$

$\phi(0) = p\delta(0) = 0$ et $\phi(1) = 1 + p\delta(1) = 1$. □

Remarque 1.12.

1. *ϕ est obtenue par composition de la section $f \mapsto (f, \delta(f))$ avec le polynôme de Witt W_1.*
2. *La condition multiplicative d'une p-dérivation se réécrit alors :*

$$\forall f, g \in A, \delta(fg) = f^p\delta(g) + \delta(f)\phi(g) = \delta(f)g^p + \phi(f)\delta(g).$$

ϕ est appelé l'**endomorphisme de Frobenius** de A. On a ainsi montré qu'à partir d'une δ-structure sur A, on obtient un endomorphisme de A. Il existe une réciproque partielle :

Proposition 1.13. *On suppose que A est un anneau sans p-torsion. Soit ϕ un endomorphisme de A. On suppose que ϕ est un Frobenius sur A. En posant :*

$$\delta(f) = \frac{\phi(f) - f^p}{p}$$

pour tout $f \in A$, on obtient une structure de δ-anneau sur A.

Démonstration : ϕ est un Frobenius donc on a bien $\delta(f) \in A$ pour tout $f \in A$. En utilisant le fait que ϕ est un morphisme, on montre facilement que δ vérifie les axiomes de la définition 1.2, donc δ est une p-dérivation. □

1.2 Exemples

Nous allons commencer par regarder le cas où $A = \mathbb{Z}$.

Proposition 1.14. *Il existe une unique δ-structure sur $\mathbb{Z}$.*

Démonstration : Le seul endomorphisme de $\mathbb{Z}$ est l'identité et c'est un Frobenius sur A car pour $n \in \mathbb{Z}$, ou bien p divise n et dans ce cas n et n^p sont tous les deux congrus à 0 modulo p, ou bien p ne divise pas n et le petit théorème de Fermat nous donne que $n^{p-1} \equiv 1 \mod p$ d'où $n \equiv n^p \mod p$. De plus, l'anneau $\mathbb{Z}$ est sans torsion donc a fortiori sans p-torsion pour p premier. D'après la proposition 1.13, il existe une unique structure de δ-anneau sur $\mathbb{Z}$, c'est-à-dire une unique δ-structure. □

D'après la proposition 1.13, l'unique δ-structure sur $\mathbb{Z}$ est donnée par :

$$\forall n \in \mathbb{Z}, \delta(n) = \frac{n - n^p}{p}.$$

Intéressons-nous maintenant au cas où $A = \mathbb{Z}[X]$.

Proposition 1.15. *Il existe une unique δ-structure sur $\mathbb{Z}[X]$ pour laquelle $\delta(X) = f$ (où $f \in \mathbb{Z}[X]$).*

Démonstration : On considère l'endomorphisme ϕ de $A = \mathbb{Z}[X]$ défini par $\phi(n) = n$ pour $n \in \mathbb{Z}$ et $\phi(X) = X^p + pf$ avec $f \in A$. Il est clair que ϕ est un Frobenius sur $\mathbb{Z}[X]$. $\mathbb{Z}[X]$ est un anneau sans p-torsion donc, par la proposition 1.13, on obtient l'existence d'une δ-structure sur $\mathbb{Z}[X]$ qui est définie par $\delta(n) = \frac{n-n^p}{p}$ pour $n \in \mathbb{Z}$ et $\delta(X) = f$. D'après la proposition 1.9, une δ-structure sur $\mathbb{Z}[X]$ est déterminée de manière unique par l'action de δ sur X, ce qui nous donne l'unicité. □

Théorème 1.16. *Il existe une unique δ-structure sur $\mathbb{Z}[X_0, \ldots, X_m, \ldots]$ pour laquelle $\delta(X_m) = X_{m+1}$ pour tout $m \in \mathbb{N}$.*

Démonstration : La démonstration est analogue à la preuve de la proposition 1.15 : on considère l'endomorphisme ϕ de $A = \mathbb{Z}[X_0, \ldots, X_m, \ldots]$ défini par $\phi(n) = n$ pour $n \in \mathbb{Z}$ et $\phi(X_m) = X_m^p + pX_{m+1}$ pour tout $m \in \mathbb{N}$. Il est clair que ϕ est un Frobenius sur A. A est un anneau sans p-torsion donc, par la proposition 1.13, on obtient l'existence d'une δ-structure sur A qui est définie par $\delta(n) = \frac{n-n^p}{p}$ pour $n \in \mathbb{Z}$ et $\delta(X_m) = X_{m+1}$ pour $m \in \mathbb{N}$. D'après la proposition 1.9, on a unicité de cette δ-structure. □

Il peut arriver qu'un anneau A ne possède pas de δ-structure même s'il ne contient pas d'élément de p-torsion. On a l'exemple suivant :

Proposition 1.17. *Lorsque $p = 2$, l'anneau des entiers de Gauss $A = \mathbb{Z}[i]$ ne possède pas de δ-structure.*

Démonstration : $\mathbb{Z}[i]$ est sans élément de 2-torsion et on a deux endomorphismes de $\mathbb{Z}[i]$: l'identité et la conjugaison. Mais aucun de ces deux endomorphismes n'est un Frobenius de $\mathbb{Z}[i]$. En effet, soit $a+ib \in \mathbb{Z}[i]$ (avec $a, b \in \mathbb{Z}$). On a :

$$(a+ib)^2 = a^2 + 2iab - b^2 \equiv a^2 - b^2 \mod 2$$

mais $a+ib \not\equiv a^2-b^2 \mod 2$, donc le morphisme identité n'est pas un Frobenius. De même, $a-ib \not\equiv a^2-b^2 \mod 2$, donc le morphisme conjugaison n'est pas un Frobenius. $\square$

Regardons à présent le cas où $R = \mathbb{Z}/p^k\mathbb{Z}$ avec $k \in \mathbb{N}\backslash\{0\}$ et A est une R-algèbre. On a le résultat suivant :

Proposition 1.18. *A possède une δ-structure si et seulement si $A = \{0\}$.*

Démonstration :

- Si $A = \{0\}$, alors A possède une δ-structure, il s'agit de la δ-structure associée à la p-dérivation $\delta : A \to A, 0 \mapsto 0$.
- Supposons que $A \neq \{0\}$. On suppose par l'absurde que A possède une δ-structure. Pour $n \in \mathbb{Z}$, on a :

  $$v_p(\delta(n)) = v_p\left(\frac{n-n^p}{p}\right) = v_p(n-n^p) - v_p(p) = v_p(n) + v_p(1-n^{p-1}) - 1 = v_p(n) - 1.$$

  Par une récurrence immédiate, il vient que $v_p(\delta^j(n)) = v_p(n) - j$ pour tout $j \in \mathbb{N}$. En particulier pour $n = p^k$, on obtient $v_p(\delta^k(p^k)) = v_p(p^k) - k = k - k = 0$. Dans $\mathbb{Z}/p^k\mathbb{Z}$, on a que $p^k = 0$ d'où $\delta^k(p^k) = 0$ puis p^k divise $\delta^k(p^k)$: contradiction avec $v_p(\delta^k(p^k)) = 0$.

$\square$

1.3 δ-enveloppe et δ-idéal

Définition 1.19. *Soit R un δ-anneau et soit A une R-algèbre. La **δ-enveloppe** A^δ de A est un δ-anneau qui est universel pour les morphismes de R-algèbres dans les $\delta - R$-algèbres. Autrement dit, il existe un δ-anneau A^δ sur R et un morphisme de R-algèbres $j : A \to A^\delta$ tels que si on se donne un morphisme de R-algèbres $u : A \to T$ où T est une $\delta - R$-algèbre, alors il existe un unique morphisme $u' : A^\delta \to T$ de δ-anneaux sur R tel que $u = u' \circ j$.*

Exemple 1.20. *On a $\mathbb{Z}[X]^\delta = \mathbb{Z}[(X_i)_{i\in\mathbb{N}}]$ avec l'unique δ-structure telle que $\delta(X_i) = X_{i+1}$ pour tout $i \in \mathbb{N}$ (théorème 1.16). Plus généralement, pour un anneau R qui possède une unique δ-structure, on a $R[(X_k)_{k\in F}]^\delta = R[(X_{k,i})_{k\in F, i\in\mathbb{N}}]$ avec l'unique δ-structure telle que $\delta(X_{k,i}) = X_{k,i+1}$ pour $k \in F$ et $i \in \mathbb{N}$.*

Définition 1.21. *Un **δ-idéal** dans un δ-anneau A est un idéal I de A qui est stable sous δ. La **δ-clôture** I_δ d'un idéal I de A est le plus petit δ-idéal de A qui contient I.*

Remarque 1.22. *La δ-clôture d'un idéal I de A existe toujours car A est un δ-idéal de lui même et il contient I.*

Lemme 1.23. *Le noyau d'un morphisme de δ-anneaux $u : A \to B$ est stable par δ.*

Démonstration : u est un morphisme de δ-anneaux donc par définition $u \circ \delta = \delta \circ u$. Pour $a \in \ker(u)$, on a : $u \circ \delta(a) = \delta \circ u(a) = \delta(0) = 0$, donc $\delta(\ker(u)) \subset \ker(u)$. $\square$

Proposition 1.24. *Un δ-idéal est le noyau d'un morphisme de δ-anneaux.*

Démonstration : Soient A un δ-anneau et I un idéal de A.

- Supposons que I est un δ-idéal. Alors $\delta(I) \subset I$. On considère l'anneau quotient A/I et le morphisme d'anneaux $r : A \to A/I$. On a $I = \ker(r)$. On définit δ sur A/I par $\delta : f + I \in A/I \mapsto \delta(f) + I \in A/I$. On vérifie facilement que c'est une p-dérivation sur A/I car δ est une p-dérivation sur A. Alors A/I est un δ-anneau. r est donc un morphisme de δ-anneaux et I est le noyau du morphisme de δ-anneaux r.

- Réciproquement, supposons que I est le noyau d'un morphisme de δ-anneaux. Soient B un δ-anneau et $u : A \to B$ un morphisme de δ-anneaux tels que $\ker(u) = I$. Comme $\ker(u)$ est stable par δ d'après le lemme 1.23, alors I est stable par δ et c'est un δ-idéal de A.

$\square$

Proposition 1.25. *Un idéal I d'un δ-anneau A est un δ-idéal de A si et seulement si pour tout générateur f de I on a $\delta(f) \subset I$.*

Démonstration : Le sens direct est évident. La réciproque découle directement des assertions 2. et 3. de la définition d'une p-dérivation (définition 1.2). $\square$

Proposition 1.26. *Si $I = \langle f_i \rangle_{i \in E}$, alors $I_\delta = \langle \delta^j(f_i) \rangle_{i \in E, j \in \mathbb{N}}$.*

Démonstration : Notons $J = \langle \delta^j(f_i) \rangle_{i \in E, j \in \mathbb{N}}$.

- J contient I (il suffit de regarder les $\delta^j(f_i)$ avec $j = 0$).
- Pour tout $(i', j') \in E \times \mathbb{N}$, on a $\delta(\delta^{j'}(f_{i'})) = \delta^{j'+1}(f_{i'}) \in J$ donc J est un δ-idéal par la proposition 1.25.
- Soit K un δ-idéal contenant I. Pour tout $i \in E$, on a $\delta(f_i) \in K$ car $f_i \in I \subset K$ et K est un δ-idéal. Comme $\delta(f_i) \in K$ et K est un δ-idéal, il vient $\delta^2(f_i) \in K$, puis en itérant on obtient $\delta^j(f_i)$ pour tout $j \in \mathbb{N}$. Ceci étant vrai pour tout $i \in E$, on en déduit que $J \subset K$.

Ainsi, J est un δ-idéal qui contient I et c'est le plus petit au sens de l'inclusion, donc $I_\delta = J$. $\square$

Proposition 1.27. *Soit R un δ-anneau, notons $\underline{A_R}$ la catégorie des R-algèbres.*
Le foncteur $F : \underline{A_R} \to \underline{R_\delta}, A \mapsto A^\delta$ est adjoint au foncteur oubliant $G : \underline{R_\delta} \to \underline{A_R}, (A, \delta) \mapsto A$.

Démonstration : Commençons par montrer l'existence de la δ-enveloppe. Soit A une R-algèbre. On peut écrire $A = R[(X_k)_{k \in F}]/I$ avec $I = \langle f_i \rangle_{i \in E}$. Comme à l'exemple 1.20, on a :

$$R[(X_k)_{k \in F}]^\delta = R[(X_{k,l})_{k \in F, l \in \mathbb{N}}]$$

avec l'unique δ-structure telle que $\delta(X_{k,l}) = X_{k,l+1}$ pour $k \in F$ et $l \in \mathbb{N}$. De plus, d'après la proposition 1.26, on a $I_\delta = \langle \delta^j(f_i) \rangle_{i \in E, j \in \mathbb{N}}$. Donc $R[(X_{k,l})_{k \in F, l \in \mathbb{N}}]/\langle \delta^j(f_i) \rangle_{i \in E, j \in \mathbb{N}}$ est un δ-anneau et il s'agit de la δ-enveloppe A^δ de A. Montrons à présent l'existence d'un isomorphisme :

$$\forall A \in \underline{A_R}, \forall (B, \delta) \in \underline{R_\delta},\ \alpha_{A,B} : \mathrm{Hom}(A^\delta, (B, \delta)) \simeq \mathrm{Hom}(A, B).$$

Soit j un morphisme de A dans $B = G(B, \delta)$ où $A \in \underline{A_R}$ est une R-algèbre et où $(B, \delta) \in \underline{R_\delta}$ est une $\delta - R$-algèbre. Par définition de la δ-enveloppe, il existe un morphisme $F_A : A \to A^\delta = F(A)$. On considère aussi la restriction $G_B : (B, \delta) \to B = G(B, \delta)$. Par définition de la δ-enveloppe, A^δ est un δ-anneau tel que si on se donne un morphisme $u : A \to (B, \delta)$, alors il existe un unique isomorphisme $u' : A^\delta \to (B, \delta)$ tel que $u = u' \circ F_A$. Comme $j = G_B \circ u$, il existe donc un unique morphisme (et même isomorphisme) $u' : A^\delta \to (B, \delta)$ tel que $j = G_B \circ u' \circ F_A$. $\square$

2 Travaux de Buium

Les travaux de Buium sur la dérivation arithmétique ont pour but de développer un analogue arithmétique de la dérivation. La variable temporelle t est remplacée par un nombre premier p fixé. Les fonctions à valeurs réelles lisses sont remplacées par des entiers relatifs, ou plus généralement par des entiers de corps de nombres. L'opérateur de dérivation sur les fonctions $f(t) \mapsto \frac{df}{dt}(t)$ est remplacé par la p-dérivation que l'on a défini sur $\mathbb{Z}$ à la section 1.2. Buium introduit ainsi un analogue arithmétique des dérivations, appelé π-dérivations. La question est de savoir à quel point ces opérateurs de π-dérivation paraissent « naturels » et quels autres choix nous avons pour définir des analogues arithmétiques des dérivations « usuelles ».

Soit A un anneau commutatif unitaire.

Définition 2.1.

1. *Une application* $\delta : A \to A$ *est appelée un* ***opérateur*** *sur* A *s'il existe deux polynômes* S, P *dans* $A[X_0, X_1, Y_0, Y_1]$ *tels que pour tous* $x, y \in A$ *on a :*

$$\delta(x+y) = S(x, y, \delta(x), \delta(y)),$$

$$\delta(xy) = P(x, y, \delta(x), \delta(y)).$$

   Dans ce cas, on dit que δ *et le couple* (S, P) *correspondent l'un à l'autre.*

2. *Soit* δ *un opérateur sur* A*. On dit que* δ *est* ***générique*** *sur* A *si, pour tout polynôme* $F \in A[X_0, X_1]$ *vérifiant* $F(x, \delta(x)) = 0$ *pour tout* $x \in A$*, on a* $F = 0$*.*
3. *Soit* δ *un opérateur sur* A*. Une* ***extension générique*** *de* δ *est un opérateur* $\tilde{\delta}$ *sur une extension d'anneau* $\tilde{A}$ *de* A *tel que :* $\tilde{\delta}$ *coïncide avec* δ *sur* A*, il existe un couple* (S, P) *qui correspond à* δ *et* $\tilde{\delta}$*, et* $\tilde{\delta}$ *est générique sur* $\tilde{A}$*.*
4. *Un opérateur* δ *sur* A *est appelé un* ***opérateur de jet*** *si* $\delta(0) = \delta(1) = 0$ *et s'il admet une extension générique.*
5. *Deux opérateurs* δ_1 *et* δ_2 *sur* A *sont dits* ***équivalents*** *s'il existe un élément inversible* $\lambda \in A^\times$ *et un polynôme* $f \in A[X]$ *vérifiant* $f(0) = f(1) = 0$ *et :*

$$\forall x \in A, \delta_1(x) = \lambda\delta_2(x) + f(x).$$

Proposition 2.2. *Soient* δ_1 *et* δ_2 *deux opérateurs équivalents sur* A*. Alors* δ_1 *est un opérateur de jet si et seulement si* δ_2 *en est un.*

Démonstration : Supposons que δ_2 est un opérateur de jet. On a :

$$\delta_1(0) = \lambda\delta_2(0) + f(0) = 0 \text{ et } \delta_1(1) = \lambda\delta_2(1) + f(1) = 0.$$

Soit $\tilde{\delta_2}$ une extension générique de δ_2 sur une extension d'anneau $\tilde{A}$ de A. On pose $\tilde{\delta_1}(x) = \lambda\tilde{\delta_2}(x) + f(x)$ pour tout $x \in \tilde{A}$.

- Comme $\tilde{\delta_2}$ coïncide avec δ_2 sur A, il en découle directement que $\tilde{\delta_1}$ coïncide avec δ_1 sur A.
- Soit (S_2, P_2) un couple qui correspond à $\tilde{\delta_2}$ et à δ_2. On considère les polynômes $F, G \in A[X_0, X_1, Y_0, Y_1]$ définis pas $F(X_0, X_1, Y_0, Y_1) = X_0 + X_1$ et $G(X_0, X_1, Y_0, Y_1) = X_0X_1$. En posant :

$$S_1(X_0, X_1, Y_0, Y_1) = \lambda S_2\left(X_0, X_1, \lambda^{-1}(Y_0 - f(X_0)), \lambda^{-1}(Y_1 - f(X_1))\right) + f(F(X_0, X_1, Y_0, Y_1)),$$

$$P_1(X_0, X_1, Y_0, Y_1) = \lambda P_2\left(X_0, X_1, \lambda^{-1}(Y_0 - f(X_0)), \lambda^{-1}(Y_1 - f(X_1))\right) + f(G(X_0, X_1, Y_0, Y_1)),$$

  on a $S_1, P_1 \in A[X_0, X_1, Y_0, Y_1]$ et le couple (S_1, P_1) correspond à $\tilde{\delta_1}$ et à δ_1.
- Il reste à montrer que $\tilde{\delta_1}$ est générique sur $\tilde{A}$. Soit $F \in \tilde{A}[X_0, X_1]$ un polynôme tel que $F(x, \tilde{\delta_1}(x)) = 0$ pour tout $x \in \tilde{A}$. On considère l'application : $G : (X_0, X_1) \mapsto (X_0, \lambda X_1 + f(X_0))$. Alors on a $F \circ G \in \tilde{A}[X_0, X_1]$ et pour tout $x \in \tilde{A}$ il vient :

$$(F \circ G)(x, \tilde{\delta_2}(x)) = F(x, \lambda\tilde{\delta_2}(x) + f(x)) = F(x, \tilde{\delta_1}(x)) = 0.$$

  Comme $\tilde{\delta_2}$ est générique sur $\tilde{A}$, on en déduit que $F \circ G = 0$, puis $F = 0$.

La réciproque se démontre de manière similaire. □

Exemple 2.3. *On a les quatre opérateurs sur* A *suivants :*

1. *Une application* $\delta : A \to A$ *qui vérifie*

$$\delta(x+y) = \delta(x) + \delta(y), \delta(xy) = x\delta(y) + y\delta(x) + \delta(x)\delta(y) \text{ et } \delta(1) = 0$$

   pour tous $x, y \in A$ *est un opérateur sur* A *(découle directement de la définition d'un opérateur sur* A*) appelé* ***opérateur de différence****.*

2. *Une application $\delta : A \to A$ qui satisfait*

$$\delta(x+y) = \delta(x) + \delta(y) \text{ et } \delta(xy) = x\delta(y) + y\delta(x)$$

*est appelée une **dérivation**. Une dérivation sur A est clairement un opérateur sur A. Les dérivations sont les bases de l'algèbre différentielle.*

3. *Soit π un élément non inversible de A. Une application $\delta : A \to A$ qui vérifie*

$$\delta(x+y) = \delta(x) + \delta(y) \text{ et } \delta(xy) = x\delta(y) + y\delta(x) + \pi\delta(x)\delta(y)$$

*pour tous $x, y \in A$ est un opérateur (découle de la définition d'un opérateur) sur A appelé **opérateur de π-différence**.*

4. *Soit π un élément non inversible de A. On suppose qu'il existe un élément $\pi^* \in A$ tel que $\pi\pi^* = p$ où p est un entier premier. Soit $q \neq 1$ une puissance de p. On considère le polynôme à coefficients entiers*

$$C_q(X,Y) = \frac{X^q + Y^q - (X+Y)^q}{p}.$$

*Une application $\delta : A \to A$ est appelée une **π-dérivation** si elle satisfait*

$$\delta(x+y) = \delta(x) + \delta(y) + \pi^* C_q(x,y) \text{ et } \delta(xy) = x^q\delta(y) + y^q\delta(x) + \pi\delta(x)\delta(y).$$

Une π-dérivation sur A est clairement un opérateur sur A. Dans le cas où $q = p$ et $\pi^* = 1$, on retrouve la notion de p-dérivation (définition 1.2).

Lemme 2.4. *Reprenons les notations de l'exemple 2.3. On suppose que l'anneau A n'a pas d'idempotents non triviaux.*

- *L'application $\delta : A \to A$ est un opérateur de différence si et seulement si l'application*

$$\phi : x \in A \mapsto x + \delta(x) \in A$$

est un morphisme d'anneaux.

- *L'application $\delta : A \to A$ est un opérateur de π-différence si et seulement si l'application*

$$\phi : x \in A \mapsto x + \pi\delta(x) \in A$$

est un morphisme d'anneaux.

- *L'application $\delta : A \to A$ est une π-dérivation si et seulement si l'application*

$$\phi : x \in A \mapsto x^q + \pi\delta(x) \in A$$

est un morphisme d'anneaux.

Démonstration : Immédiat. □

Proposition 2.5. *Reprenons les notations de l'exemple 2.3. Si l'anneau A n'a pas d'idempotents non triviaux et si π n'est pas un diviseur de 0, alors les quatre opérateurs de l'exemple 2.3 sont des opérateurs de jet.*

Démonstration : On suppose que A n'a pas d'idempotents non triviaux et que π n'est pas un diviseur de 0. Comme $C_q(0,0) = 0$, on a dans les quatre cas $\delta(0+0) = \delta(0) + \delta(0)$ d'où $\delta(0) = 0$. Dans le cas 2, $\delta(1 \times 1) = \delta(1) + \delta(1)$ ce qui nous donne $\delta(1) = 0$. Dans les cas 3 et 4, on a :

$$\delta(1) = \delta(1 \times 1) = 2\delta(1) + \pi\delta(1)^2,$$

d'où $-\delta(1) = \pi\delta(1)^2$ puis $-\pi\delta(1) = (-\pi\delta(1))^2$. Comme A ne possède pas d'idempotents non triviaux, on en déduit que $-\pi\delta(1) \in \{0,1\}$. Comme π n'est pas inversible dans A, on ne peut pas avoir que $-\pi\delta(1) = \pi(-\delta(1)) = 1$, d'où $-\pi\delta(1) = 0$. De plus, π n'est pas un diviseur de 0, d'où $\delta(1) = 0$.

Montrons à présent que dans les quatre cas, δ admet une extension générique. Nous allons commencer par faire la démonstration pour un opérateur de π-différence, les preuves pour un opérateur de différence ou une π-dérivation sont similaires. Soit donc δ un opérateur de π-différence sur A. On considère l'anneau $\tilde{A} = A[T_0, T_1, \ldots, T_n, \ldots]$. Nous allons montrer que l'on peut étendre δ en un opérateur $\tilde{\delta}$ sur $\tilde{A}$ en posant $\tilde{\delta}(T_n) = T_{n+1}$ pour tout $n \in \mathbb{N}$. D'après le lemme 2.4, l'application $\phi : x \in A \mapsto x + \pi\delta(x) \in A$ est un morphisme. On étend ϕ en un endomorphisme de $\tilde{A}$ en posant $\tilde{\phi}(T_n) = T_n + \pi T_{n+1}$ pour tout $n \in \mathbb{N}$. On définit $\tilde{\delta} : x \in \tilde{A} \mapsto \frac{\tilde{\phi}(x)-x}{\pi} \in \tilde{A}$. C'est un opérateur de π-différence par le lemme 2.4, donc il existe un couple $(\tilde{S}, \tilde{P})$ qui correspond à $\tilde{\delta}$. On a bien que $\tilde{\delta}$ coïncide avec δ sur A et que $(\tilde{S}, \tilde{P})$ correspond à δ et $\tilde{\delta}$. Il reste à vérifier que $\tilde{\delta}$ est générique sur $\tilde{A}$. Soit $F \in \tilde{A}[X_0, X_1]$ tel que $F(\tilde{x}, \tilde{\delta}(\tilde{x})) = 0$ pour tout $\tilde{x} \in \tilde{A}$ et soit $n \in \mathbb{N}$ tel que $F \in A[T_0, T_1, \ldots, T_n][X_0, X_1]$. En prenant $\tilde{x} = T_{n+1}$, il vient :

$$0 = F(T_{n+1}, \tilde{\delta}(T_{n+1})) = F(T_{n+1}, T_{n+2})$$

d'où $F = 0$.

Intéressons-nous à présent au cas où δ est une dérivation. On définit $\tilde{\delta}$ sur $\tilde{A}$ par $\tilde{\delta} := \delta$ sur A et $\tilde{\delta}(T_n) = T_{n+1}$ pour tout $n \in \mathbb{N}$, et on définit $S, P \in \tilde{A}[X_0, X_1, Y_0, Y_1]$ par $S(X_0, X_1, Y_0, Y_1) = Y_0 + Y_1$ et $P(X_0, X_1, Y_0, Y_1) = X_0Y_1 + X_1Y_0$. Le couple (S, P) correspond à δ et $\tilde{\delta}$. On montre que $\tilde{\delta}$ est générique sur $\tilde{A}$ comme au cas précédent, et on obtient alors que $\tilde{\delta}$ est une extension générique de δ. □

L'idée à présent est de classifier les opérateurs de jets, ce qui est fait dans le théorème suivant :

Théorème 2.6. ***(Théorème de classification de Buium)***
On suppose que A est un anneau local intègre de caractéristique 0. Tout opérateur de jet sur A est équivalent à l'un des opérateurs suivants : un opérateur de différence, un opérateur de dérivation, un opérateur de π-différence, ou un opérateur de π-dérivation.

La démonstration du théorème de classification de Buium étant assez longue, nous allons voir les principales étapes de la preuve. Nous avons besoin des résultats suivants :

Lemme 2.7. *Soit A un anneau. On suppose que $\delta : A \to A$ est un opérateur et $\tilde{\delta} : \tilde{A} \to \tilde{A}$ une extension générique de δ. Soit $F \in \tilde{A}[X_{1,0}, \ldots, X_{m,0}, X_{1,1}, \ldots, X_{m,1}]$ un polynôme en $2m$ variables tel que $F(\tilde{x}_1, \ldots, \tilde{x}_m, \tilde{\delta}(\tilde{x}_1), \ldots, \tilde{\delta}(\tilde{x}_m)) = 0$ pour tous $\tilde{x}_1, \ldots, \tilde{x}_m \in \tilde{A}$. Alors $F = 0$.*

Démonstration : Immédiat par récurrence sur $m \in \mathbb{N}\backslash\{0\}$. □

Corollaire 2.8. *Avec les notations du lemme 2.7, il existe un unique couple (S, P) qui correspond à δ et $\tilde{\delta}$.*

Démonstration : Il existe au moins un couple (S, P) qui correspond à δ et $\tilde{\delta}$ car $\tilde{\delta}$ est une extension générique de δ. Si (S_1, P_1) et (S_2, P_2) sont deux couples qui correspondent à δ et $\tilde{\delta}$, en appliquant le lemme 2.7 à $F = S_1 - S_2$ (resp. $F = P_1 - P_2$), on obtient que $S_1 = S_2$ (resp. $P_1 = P_2$). □

Lemme 2.9. *Soit A un anneau. On suppose que $\delta : A \to A$ est un opérateur et $\tilde{\delta} : \tilde{A} \to \tilde{A}$ une extension générique de δ. Soit (S, P) l'unique couple qui correspond à δ et $\tilde{\delta}$. Pour toute A-algèbre B, les formules*

$$(x_0, x_1) + (y_0, y_1) = (x_0 + y_0, S(x_0, y_0, x_1, y_1)),$$

$$(x_0, x_1).(y_0, y_1) = (x_0y_0, P(x_0, y_0, x_1, y_1)),$$

définissent une structure d'anneau sur $B \times B$ telle que l'élément neutre pour l'addition soit $(0, 0)$ et l'élément neutre pour la multiplication soit $(1, 0)$.

Notons $\Sigma(A)$ l'ensemble de tous les couples $(S, P) \in A[X_0, X_1, Y_0, Y_1]$ tels que les deux formules du lemme 2.9 définissent, pour toute A-algèbre B, une structure d'anneau sur $B \times B$ dont l'élément neutre pour l'addition (respectivement la multiplication) est $(0, 0)$ (resp. $(1, 0)$). Par ailleurs, notons $\Gamma(A)$ le groupe $A^\times \times X(X-1)A[X]$ muni du produit semi-direct $(\lambda_1, f_1).(\lambda_2, f_2) = (\lambda_1\lambda_2, f_1 + \lambda_1 f_2)$. Le groupe $\Gamma(A)$ agit sur $\Sigma(A)$, l'action est donnée par $(\lambda, f).(S, P) = (S', P')$ pour $(\lambda, f) \in \Gamma(A), (S, P) \in \Sigma(A)$ avec

$$S' = \lambda S\left(X_0, \lambda^{-1}(X_1 - f(X_0)), Y_0, \lambda^{-1}(Y_1 - f(Y_0))\right) + f(X_0 + Y_0),$$

$$P' = \lambda P\left(X_0, \lambda^{-1}(X_1 - f(X_0)), Y_0, \lambda^{-1}(Y_1 - f(Y_0))\right) + f(X_0Y_0).$$

Le lemme suivant découle directement du lemme 2.9 :

Lemme 2.10. *Si (S, P) est un couple qui correspond à un opérateur de jet δ sur A et à une extension générique de δ, alors $(S, P) \in \Sigma(A)$ et l'application $x \in A \mapsto (x, \delta(x)) \in A \times A$ est un morphisme d'anneaux (où la structure d'anneau sur $A \times A$ est définie par (S, P) comme dans le lemme 2.9). Réciproquement, si on a un opérateur ∂ sur A tel que l'application $x \in A \mapsto (x, \partial(x)) \in A \times A$ est un morphisme d'anneaux (où la structure d'anneau sur $A \times A$ est définie par un couple (S, P) comme dans le lemme 2.9), alors ∂ correspond à (S, P).*

On déduit du lemme 2.10 que démontrer le théorème de classification de Buium revient à démontrer la proposition suivante :

Proposition 2.11. *On suppose que A est un anneau local intègre de caractéristique 0. Tout élément de $\Sigma(A)$ appartient à l'orbite sous l'action de $\Gamma(A)$ de l'un des quatre couples (S, P) suivants :*

$S = X_1 + Y_1, P = X_0Y_1 + Y_0X_1 + X_1Y_1$ *(correspond à un opérateur de différence),*
$S = X_1 + Y_1, P = X_0Y_1 + Y_0X_1$ *(correspond à une dérivation),*
$S = X_1 + Y_1, P = X_0Y_1 + Y_0X_1 + \pi X_1Y_1$ *(correspond à un opérateur de π-différence),*
$S = X_1 + Y_1 + \pi^* C_q(X_0, Y_0), P = X_0^qY_1 + Y_0^qX_1 + \pi X_1Y_1$ *(correspond à une π-dérivation),*

où π est défini comme dans les exemples 2.3-3 et 2.3-4 respectivement.

Pour démontrer la proposition 2.11, une première étape est donnée par le lemme suivant (que nous allons admettre) :

Lemme 2.12. *On suppose que A est un anneau local intègre de caractéristique 0, notons K son corps des fractions. Tout élément de $\Sigma(K)$ appartient à l'orbite sous l'action de $\Gamma(K)$ de l'un des deux couples (S, P) suivants :*

$$S = X_1 + Y_1, P = X_0Y_1 + Y_0X_1 + X_1Y_1,$$
$$S = X_1 + Y_1, P = X_0Y_1 + Y_0X_1.$$

On se donne un élément $(S, P) \in \Sigma(A)$ (où A vérifie les hypothèses de la proposition 2.11). D'après le lemme 2.12, nous avons les deux cas suivants :

1. (S, P) est dans l'orbite de $(X_1 + Y_1, X_0Y_1 + Y_0X_1)$ sous l'action de $\Gamma(K)$,
2. (S, P) est dans l'orbite de $(X_1 + Y_1, X_0Y_1 + Y_0X_1 + X_1Y_1)$ sous l'action de $\Gamma(K)$.

Nous allons faire la preuve ici uniquement pour le premier cas. On suppose ainsi que (S, P) est dans l'orbite de $(X_1 + Y_1, X_0Y_1 + Y_0X_1)$ sous l'action de $\Gamma(K)$. On peut écrire

$$(S, P) = (\lambda, f).(X_1 + Y_1, X_0Y_1 + Y_0X_1)$$

où $\lambda \in K^\times$ et $f \in X(X-1)K[X]$. On obtient :

$$S = X_1 + Y_1 + f(X_0 + Y_0) - f(X_0) - f(Y_0),$$
$$P = X_0Y_1 + Y_0X_1 + f(X_0Y_0) - X_0f(Y_0) - Y_0f(X_0).$$

On peut alors supposer que $\lambda = 1$. Comme P est à coefficients dans A, la deuxième égalité ci-dessus nous donne que f est aussi à coefficients dans A. D'où $(\lambda, f) \in \Gamma(A)$. On a ainsi démontré que (S, P) est dans l'orbite du couple $(X_1 + Y_1, X_0Y_1 + Y_0X_1)$ sous l'action de $\Gamma(A)$, ce qui termine la preuve de ce cas.

3 Références

[B1] *Arithmetic Analogues of Derivations* d'Alexandru BUIUM, 31 janvier 1997.

[B2] *Arithmetic Differential Equations* d'Alexandru BUIUM, American Mathematical Society, 2005.

[BS] *Prisms and prismatic cohomology* de Bhargav BHATT et Peter SCHOLZE, 27 août 2019.

[J1] *δ-anneaux et λ-anneaux* d'André JOYAL, 4 août 1985.

[J2] *δ-anneaux et vecteurs de Witt* d'André JOYAL, juin 1985.

[LS] *Twisted differential operators and q-crystal* de Michel GROS, Bernard LE STUM et Adolfo QUIROS, versions du 29 avril 2020 et du 17 décembre 2020.

[Bo] Conférence sur le sujet *Introduction to Witt vectors, delta-rings, and prisms* de James BORGER, septembre 2019, disponible à l'adresse Internet suivante :
https ://www.youtube.com/watch ?v=_ y2Tcu-iJV4