An introduction to δ-rings

Definition, examples and properties

Anneloes Viergever

Universität Duisburg-Essen

06-01-2021

Goal: Prismatic Cohomology

In the second half of the seminar, we want to define and study *prismatic cohomology*, for which we will need the definition of a *prism*. Very roughly speaking, these are pairs (R, I) where R is a δ*-ring* and $I \subset R$ an ideal satisfying certain conditions.

So...

We will have to define δ-rings.

A bit of history

δ-rings were introduced by Joyal [3] in 1985. Later on, the concept was explored by Buium [4] in 1997 as an arithmetic analogue of the algebraic concept of derivations.

General idea

Let p be a prime number and let R be a commutative ring. We have the Frobenius map

$$R/(p) \to R/(p), x \mapsto x^p$$

which is a ring homomorphism.

Intuitive idea

A *δ-structure* on R is a map $\delta_R : R \to R$ such that the associated morphism

$$\phi_R : R \to R, x \mapsto x^p + p\delta_R(x)$$

is a ring homomorphism, i.e. a lift for the Frobenius map.

In the literature, δ-structures are often referred to as *p-derivations*.

Table of contents

Table of Contents

Definition of a δ-ring

Throughout, we fix a prime number p.

Definition

A *δ-ring* is a pair (R, δ) where R is a commutative ring and $\delta : R \to R$ is a map of sets satisfying $\delta(0) = \delta(1) = 0$, $\delta(xy) = x^p\delta(y) + y^p\delta(x) + p\delta(x)\delta(y)$ for all $x, y \in R$ and

$$\begin{aligned} \delta(x+y) &= \delta(x) + \delta(y) + \frac{x^p + y^p - (x+y)^p}{p} \\ &= \delta(x) + \delta(y) - \sum_{i=1}^{p-1} \frac{1}{p} \binom{p}{i} x^i y^{p-i} \end{aligned}$$

for all $x, y \in R$.

δ-rings give Frobenius lifts

Now let (R, δ) be a δ-ring, and consider the map

$$\phi : R \to R, x \mapsto x^p + p\delta(x).$$

Note: This is a ring homomorphism, inducing Frobenius on $R/(p)$, as

$$\begin{aligned}\phi(x+y) &= (x+y)^p + p\delta(x) + p\delta(y) + x^p + y^p - (x+y)^p \\ &= \phi(x) + \phi(y)\end{aligned}$$

and

$$\begin{aligned}\phi(xy) &= x^p y^p + px^p\delta(y) + py^p\delta(x) + p^2\delta(x)\delta(y) \\ &= \phi(x)\phi(y)\end{aligned}$$

and $\phi(1) = 1 + p\delta(1) = 1$.

Frobenius lifts give δ-structures in the torsionfree case

If R is now a commutative ring without p-torsion, then for any lift $\phi : R \to R$ of the Frobenius morphism on $R/(p)$, we obtain a unique δ-structure given by

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

There is a bijective correspondence between δ-structures on R and Frobenius lifts on R.

Note

If p is invertible, the condition of being a lift of the Frobenius map doesn't make much sense. For example, a δ-ring over $\mathbb{Q}$ just means to give a $\mathbb{Q}$-algebra together with an endomorphism.

Some first examples

The integers

The ring $\mathbb{Z}$ is p-torsionfree, and the identity map gives rise to a δ-structure given by $\delta(n) = \frac{n-n^p}{p}$. This is the initial object in the category of δ-rings. Note that this structure is the unique one!

Another example

Consider the ring $\mathbb{Z}[x]$ and take any $g \in \mathbb{Z}[x]$. Then we find an attached δ-structure for the endomorphism defined by $\phi(1) = 1$ and

$$\phi(x) = x^p + pg(x).$$

So there are quite a lot of δ-structures on $\mathbb{Z}[x]$.

An important example

Slight variant on previous example: The ring $\mathbb{Z}_{(p)}$ has no p-torsion and the identity morphism is its unique endomorphism, and so we find a unique δ-structure given by $\delta(x) = \frac{x - x^p}{p}$.

Some remarks

- Considering the category of δ-rings over $\mathbb{Z}_{(p)}$-algebras, we have that this is the initial object.
- δ lowers the p-adic valuation of a nonunit by one.
- $\delta^n(p^n)$ is a unit for all n (see also [2], Lemma 1.5 for this).

Can also define a δ-structure on $\mathbb{Z}_p$ (so the p-adic integers) by using the identity map and the fact that $\mathbb{Z}_p$ has no p-torsion.

Galois extensions

Situation.

Assume $p \neq 2$ for a moment. Consider the Galois extension $\mathbb{Q}_p \subset \mathbb{Q}_p(\zeta_p)$ where ζ_p is a primitive p'th root of unity. Consider the subring $\mathbb{Z}_p[\zeta_p] \subset \mathbb{Q}_p(\zeta_p)$.

We note that:

- $\mathbb{Z}_p[\zeta_p]$ is a discrete valuation ring and p is a uniformizer.
- $\mathbb{Z}_p/(p) \cong \mathbb{F}_p$ and also $\mathbb{Z}_p[\zeta_p]/(p) \cong \mathbb{F}_p$. That is, this is a totally ramified extension of degree $p-1$.
- The Galois group can be identified with $(\mathbb{Z}/p\mathbb{Z})^*$, by using $t \mapsto (\zeta_p \mapsto \zeta_p^t)$.

Any automorphism in here gives rise to a δ-structure on $\mathbb{Z}_p[\zeta_p]$ as before ($\mathbb{Q}_p$ has no p-torsion). See [6] for more information.

More general: Let $K \subset L$ be a Galois extension of fields and let $B \subset L$ be a discrete valuation ring. Let $A = B \cap K$. Suppose that p is a uniformizer for B and that $A/(p) = \mathbb{F}_p$.

Can show:

Then there is an element $\sigma \in \mathrm{Gal}(L/K)$ such that σ fixes B and $\sigma(x) = x^p$ modulo the ideal generated by p in B. That is, there is a δ-structure given by $\delta(x) = \frac{\sigma(x) - x^p}{p}$.

This is proven in [[5], chapter V, 11]. Example taken from [3].

p-typical length 2 Witt vectors

Let R be a ring then we define the ring $W_2(R)$ of *p-typical length 2 Witt vectors* to be the set $R \times R$ equipped with the addition

$$(x, y) + (x', y') = \left(x + x', y + y' + \frac{x^p + (x')^p - (x + x')^p}{p}\right)$$

which has identity element $(0, 0)$ and the multiplication

$$(x, y) \cdot (x', y') = (xx', x^p y' + x'^p y + pyy')$$

with unit $(1, 0)$.

Can check:

This data gives a ring.

Relation to Witt vectors

Projection onto the first factor gives a natural ring homomorphism $\epsilon : W_2(R) \to R$.

Observe:

If we have a δ-structure δ on R, then this gives a ring homomorphism

$$w : R \to W_2(R), x \mapsto (x, \delta(x))$$

and we have that $\epsilon \circ w$ is the identity on R. On the other hand, a morphism $w : R \to W_2(R)$ such that $\epsilon \circ w$ is the identity on R defines a δ-structure by defining δ as the composition of w and the projection onto the second coordinate.

Table of Contents

Limits and colimits

Lemma ([2], Lemma 2.3)

The category of δ-rings admits all limits and colimits, and these are computed on the level of the underlying rings.

Proof.

Let $\{(R_i, \delta_i)_i, (v_{ij} : R_i \to R_j)_{ij}\}$ be a diagram of δ-rings. The limit of the R_i can be constructed very explicitly: define the set

$$R = \left(\bigsqcup_i R_i \right) / \sim$$

where $r_i \sim r_j$ for $r_i \in R_i, r_j \in R_j$ if and only if $v_{ik}(r_i) = v_{jk}(r_j)$ for some $k \geq i, j$. This has a ring structure and it is the direct limit!

Proof (continued).

The δ_i give a map δ on $\bigsqcup_i R_i$.
Note: If $r_i \sim r_j$ then $\delta(r_i) \sim \delta(r_j)$. Namely, there is a $k \geq i, j$ such that $v_{ik}(r_i) = v_{jk}(r_j)$ so

$$\begin{aligned} v_{ik}(\delta(r_i)) &= v_{ik}(\delta_i(r_i)) = \delta_k(v_{ik}(r_i)) \\ &= \delta_k(v_{jk}(r_j)) = v_{jk}(\delta_j(r_j)) \\ &= v_{jk}(\delta(r_j)) \end{aligned}$$

So δ gives a well defined map of sets on $R \to R$. One can show that it gives a δ-structure. Now for the colimits, we note that the maps $R_i \to W_2(R_i)$ are compatible in i. Taking colimits gives a map

$$\mathrm{colim}_i R_i \to \mathrm{colim}_i(W_2(R_i)).$$

Proof (continued).

As $W_2(-)$ is functorial, the maps $R_i \to \mathrm{colim}_i R_i$ give rise to maps $W_2(R_i) \to W_2(\mathrm{colim}_i R_i)$. Using the universal property of the colimit, there is a map

$$\mathrm{colim}_i(W_2(R_i)) \to W_2(\mathrm{colim}_i R_i)$$

and composing with the map we had gives a map

$$\mathrm{colim}_i R_i \to W_2(\mathrm{colim}_i(R_i)).$$

One can check: If we now compose with the natural projection $W_2(\mathrm{colim}_i(R_i)) \to \mathrm{colim}_i(R_i)$ we get the identity.
And so: We find a δ-structure on $\mathrm{colim}_i(R_i)$. This yields the desired result. □

Free elements and quotients

By the previous lemma: The forgetful functor from δ-rings to rings has a left and right adjoint!

Observe

The left adjoint gives a formal notion of free δ-rings. We can therefore talk about $\mathbb{Z}_{(p)}\{x\}$ as the free δ-ring on one generator, and $\mathbb{Z}_{(p)}\{x, y\}$ and so on.

Also: Using limits and colimits, we can define quotients. For example, $\mathbb{Z}_{(p)}\{x, y\}/(f)_\delta$ is now defined by the pushout square

$$\begin{array}{ccc} \mathbb{Z}_{(p)}\{t\} & \xrightarrow{t \mapsto f} & \mathbb{Z}_{(p)}\{x, y\} \\ \downarrow{\scriptstyle t \mapsto 0} & & \downarrow \\ \mathbb{Z}_{(p)} & \longrightarrow & \mathbb{Z}_{(p)}\{x, y\}/(f)_\delta \end{array}$$

A δ-structure on a quotient ring

Lemma ([1], Lemma 2.9)

Let (R, δ) be a δ-ring and $I \subset R$ an ideal. Then I is stable under δ if and only if there exists a δ-structure on R/I compatible with the one on R.

Proof.

$\implies$: Suppose that $r \in R$ and $f \in I$ then we have that

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

and clearly, all terms except for $\delta(r)$ are in I. So $\delta(r) = \delta(r+f)$ modulo I and we get our δ-structure on R/I.
$\impliedby$: Clear now. □

Quotients in general

Now let (R, δ) be a δ-ring and $I \subset R$ an ideal. Then we can form the ideal J generated by $\bigcup_n \delta^n(I)$.

Note:

J is the smallest ideal containing I which is stable under δ.

Using the lemma: There is a δ-structure on the quotient $B = R/J$ which is compatible with the one on R.

Free δ-rings

There is also a nice result on free δ-rings. We omit the proof here.

Lemma ([1], Lemma 2.11)

The ring $\mathbb{Z}_{(p)}\{x\}$ is a polynomial ring on $\{x, \delta(x), \delta^2(x), \ldots\}$ and its Frobenius endomorphism (i.e. the lift that we have from the δ-structure) is faithfully flat. The ring $\mathbb{Q}\{x\} = \mathbb{Z}_{(p)}\{x\}[\frac{1}{p}]$ is also a polynomial ring on the set $\{x, \phi(x), \phi^2(x), \ldots\}$.

Idea: The assertion for $\mathbb{Q}$ follows from the rest. To prove it for $\mathbb{Z}_{(p)}$, one uses uniqueness and universal properties.

Table of Contents

Extending a δ-ring structure in a localization

Lemma ([1], Lemma 2.15)

Let R be a $\delta - \mathbb{Z}_{(p)}$-algebra and let $S \subset R$ be a multiplicative subset such that $\phi_R(S) \subset S$. Then $S^{-1}R$ admits a unique δ-structure which is compatible with the map $R \to S^{-1}R$. Moreover, $R \to S^{-1}R$ is initial amongst all δ-R-algebras B such that each element of S is invertible in B (i.e. satisfies the usual universal property).

Proof.

First step: Suppose that R is p-torsionfree. Then $S^{-1}R$ is also p-torsionfree and as $\phi_R : R \to R$ sends S to S, we get a map $\phi_{S^{-1}R} : S^{-1}R \to S^{-1}R$. This is a lift of the Frobenius morphism, giving the first part of the lemma, and the second part is clear.

Proof (continued).

Second step: Now let R be a general δ-ring and let $S \subset R$ be a multiplicative subset such that $\phi(S) \subset S$. Choose a surjection $\alpha : F \to R$ where F is a free δ-ring. Then:

- F is p-torsionfree (by the previous lemma).
- $T = \alpha^{-1}(S) \subset F$ is a multiplicatively closed subset of F which satisfies $\phi_F(T) \subset T$, as α commutes with ϕ.

By Step 1, $T^{-1}F$ has a unique δ-structure compatible with the one on F, and as $S^{-1}R = T^{-1}F \otimes_F R$ we have that $S^{-1}R$ also has a unique δ-structure compatible with the one on R. The second part of the statement is also clear now. □

Note that we used that colimits of δ-rings are the same as those of the underlying rings here.

Some recap on completions

For a ring R and an ideal $I \subset R$, there is a descending filtration

$$\cdots \subset I^n \subset I^{n-1} \subset \cdots \subset I \subset R$$

giving rise to the inverse limit

$$\hat{R} = \varprojlim (R/I^n)$$

which is called the *I-adic completion*.

Associated topology

This gives rise to the *I-adic topology* on R with basis $x + I^n$ for $x \in R$, $n \geq 1$. The completion is also the completion in the topological sense.

Any continuous map in this topology gives rise to a morphism on completions.

Important note

Note: We have that $\hat{I}$ is in the Jacobson radical J-rad$(\hat{R}) = \{x \in \hat{R} : 1 + \hat{R}x\hat{R} \subset \hat{R}^*\}$ of $\hat{R}$. Namely, for $a \in I$, we have that:

- $1 - a^n \in 1 + I^n$ for all n so for every basic open neighborhood of 1, the sequence $(1 - a^n)_n$ is eventually in it, i.e. this sequence converges to 1.
- $(f_n)_n = (1 + a + \cdots + a^n)_n$ is a Cauchy sequence, which in this case means that for every m, we have that there is an N_m such that $f_{n_1} - f_{n_2} \in I^m$ for all $n_1, n_2 \geq N_m$. So the sequence converges in the completion.
- $(1 - a)(1 + a + \cdots + a^n) = 1 - a^{n+1}$.

And so taking limits in $\hat{R}$, we see that $(1 - a)b = 1$ for b the limit of $(1 + a + \cdots + a^n)_n$ in $\hat{R}$, i.e. $1 - a$ becomes a unit there. See also [7], chapter 10.

Extension of δ-structures with respect to completions

We will now see that we can extend a δ-structure to completions.

Lemma ([1], Lemma 2.17)

Let R be a δ-ring and let $I \subset R$ be a finitely generated ideal containing p. Then:

1. *The map $\delta : R \to R$ is I-adically continuous. More precisely: for all $n \geq 0$ there is an m such that for all $x \in R$, we have that $\delta(x + I^m) \subset \delta(x) + I^n$.*
2. *The I-adic completion $\hat{R}$ of R admits a unique δ-structure compatible with the one on R.*

Proof.

First step: for proving 1, it suffices to see that for any n, there is some $m \geq n$ such that $\delta(I^m) \subset I^n$.

By the addition formula, we have for $m \geq 1$, $i \in I^m$ and $x \in R$ that

$$\delta(x+i) = \delta(x) + \delta(i) + \frac{x^p + i^p - (x+i)^p}{p}.$$

Note that the final factor is in I^m, as it is equal to

$$\sum_{i=1}^{p-1} \frac{1}{p} \binom{p}{i} x^i i^{p-i}.$$

We see that $\delta(x + I^m) - \delta(x) \subset \delta(I^m) + I^m$.

So: for a given n, if there is an $m \geq n$ such that $\delta(I^m) \subset I^n$ then $\delta(x + I^m) \subset \delta(x) + I^n$ as desired.

Proof (continued).

Second step: prove 1 using this reduction.
Consider two ideals $J_1, J_2 \subset R$. For $x \in J_1, y \in J_2$, by the product formula, we see that

$$\delta(xy) = x^p\delta(y) + y^p\delta(x) + p\delta(x)\delta(y) \in J_1 + J_2 + p\delta(J_1)\delta(J_2)$$

and by the addition formula $\delta(z) \in J_1 + J_2 + p\delta(J_1)\delta(J_2)$ for any z in the ideal J_1J_2. So:

$$\delta(J_1J_2) \subset J_1 + J_2 + p\delta(J_1)\delta(J_2).$$

Now taking $J_1 = J_2 = I$ we find that $\delta(I^2) \subset I$, because $p \in I$ by assumption. Now we use induction to see that $\delta(I^{2^{n+1}}) \subset I^{2^n}$ for all n, as desired. This proves 1.

Proof (continued).

Step three: Prove part 2.

Need to show two things:

- Existence of a δ-structure on $\hat{R}$: Part 1 implies that δ extends to a continuous map on the I-adic completion $\hat{R}$ of R. By continuity, this is still a δ-structure.
- Uniqueness. This is because the δ-structure on $\hat{R}$ must be $\hat{I}$-adically continuous by the first part of the result applied to $\hat{R}$.

This completes the proof. □

Table of Contents

Distinguished elements

In examples of prisms (R, I) which we will see later, e.g. crystalline prisms, the ideal I in the δ-ring R will be principal, so $I = (d)$ for some $d \in R$. It turns out that in order for this to be a prism, we will need that $\delta(d) \in R^*$.

Definition

An element d of a δ-ring R is a *distinguished element* if $\delta(d)$ is a unit.

Some examples of distinguished elements

- "Crystalline cohomology": $R = \mathbb{Z}_p$, $d = p$, δ-structure defined by the identity, i.e. $\delta(x) = \frac{x - x^p}{p}$. We see indeed that $\delta(p) = 1 - p^{p-1} \in \mathbb{Z}_p^*$ so p is distinguished.
- $R = \mathbb{Z}_{(p)}$, $d = p$ works too because we have already seen that $\delta(p)$ is a unit. In fact, this implies that p is distinguished in any δ- $\mathbb{Z}_{(p)}$-algebra.
- "q-de Rham cohomology": $R = \mathbb{Z}_p[q]$, $d = \frac{q^p - 1}{q - 1}$ with the δ-structure determined by $\phi(q) = q^p$ as before. Can see that $\delta(d)$ is a unit by direct computation.
- Consider the free δ-ring $\mathbb{Z}_{(p)}\{d, \delta(d)^{-1}\}$ then by our previous results, we have that this ring is actually $S^{-1}\mathbb{Z}_{(p)}\{d\}$ where $S = \{\delta(d), \phi(\delta(d)), \cdots\}$. In particular, d is now a distinguished element.

Lemma ([1], Lemma 2.23)

Let R be a δ-ring and let $d \in R$ be a distinguished element and let $u \in R^*$ be a unit. If $d, p \in J\text{-rad}(R)$, we have that ud is distinguished.

Proof.

We have that

$$\delta(ud) = u^p\delta(d) + d^p\delta(u) + p\delta(u)\delta(d).$$

Note that:

- $u^p\delta(d)$ is a unit.
- $d^p\delta(u)$ and $p\delta(u)\delta(d)$ are in the Jacobson radical of R.

So $\delta(ud)$ is indeed a unit. □

Lemma ([1], Lemma 2.24)

Let R be a δ-ring and let $d \in R$ be a distinguished element. Assume that $d = fh$ for some $f, h \in R$ such that $f, p \in$ J-rad(R). Then f is distinguished and h is a unit.

Proof.

We have that

$$\delta(d) = f^p\delta(h) + h^p\delta(f) + p\delta(f)\delta(h).$$

Note that:

- $f^p\delta(h)$ and $p\delta(f)\delta(h)$ are in J-rad(R).
- $\delta(d)$ is a unit.

So $h^p\delta(f)$ is a unit too, implying the statement. □

Distinguishedness only depends on the ideal (d)

We can now prove the following important result.

Lemma ([1], Lemma 2.25)

Let R be a δ-$\mathbb{Z}_{(p)}$-algebra and $d \in R$ be such that $d, p \in J\text{-rad}(R)$. Then d is distinguished if and only if $p \in (d, \phi(d))$.

Proof.

For $\implies$, suppose that d is distinguished. Then $\delta(d)$ is a unit and $\phi(d) = d^p + p\delta(d)$ so $p \in (d, \phi(d))$.
Now for $\impliedby$, suppose that $p = ad + b\phi(d)$ for some $a, b \in R$.
We want to show that $\delta(d)$ is a unit.
Note: As $d, p \in \text{J-rad}(R)$, it will suffice to show that $R/(p, d, \delta(d)) = 0$, by similar arguments as before.

Proof (continued).

We can therefore replace R by its $(p, d, \delta(d))$-adic completion and assume that $p, d, \delta(d) \in$ J-rad(R). We then find that

$$p = ad + b\phi(d) = ad + bd^p + bp\delta(d)$$

and so

$$p(1 - b\delta(d)) = d(a + bd^{p-1}).$$

Now as p is distinguished and $\delta(d) \in$ J-rad(R), we have that the left hand side is distinguished by the first previous lemma. But then we can apply the second lemma to see that d is distinguished, which completes the proof. □

Table of Contents

Sources and further reading I

- Bhargav Bhatt and Peter Scholze, *Prisms and Prismatic Cohomology*, 2019.
  See https://arxiv.org/abs/1905.08229.
- Bhargav Bhatt, *Prismatic Cohomology (Eilenberg Lectures at Columbia University)*, 2018.
  See http://www-personal.umich.edu/~bhattb/teaching/prismatic-columbia/.
- Andre Joyal, *δ-anneaux et vecteurs de Witt*, C. R. Math. Rep. Acad. Sci. Canada Vol. 7 (3) 1985, pp. 177 182.
  See https://mr.math.ca/article/%F0%9D%9B%BF-anneaux-et-vecteurs-de-witt/.

Sources and further reading II

- Alexandru Buium, *Arithmetic Analogues of Derivations*, Journal of Algebra 198, pages 290-299, 1997.
- Nicolas Bourbaki, *Algebra*, Original French edition published by Masson, Paris, 1981.
- Peter Stevenhagen, *Voortgezette getaltheorie*, Leiden, 2017 (course notes).
  See: `http://www.math.leidenuniv.nl/~psh/VGT.pdf`.
- Micheal Atiyah and Ian G. MacDonald, *Introduction to Commutative Algebra*, Addison-Wesley Publishing Company, 1969.

Thank you so much for listening!

Any questions/comments/remarks...?