DIVIDED POWER STRUCTURES

XINYU ZHOU

Contents

1. Divided power structures

In this note, we introduce some basic concepts about PD structures, which are the basis of the theory of crystalline cohomology. Our main reference is Chapter 3 of [BO78].

Divided power structures (PD structures for short) are a formalism that makes sense of $x^n/n!$ in an arbitary ring.

Definition 1.1 (Divided powers)**.** Let A be a ring, and $I \subset A$ an ideal. A *divided power structure* on I is a collection of maps

$$\gamma_i : I \to A \quad i \in \mathbb{Z}_{\geq 0}$$

such that

(1) $\forall x \in I$, $\gamma_0(x) = 1$, $\gamma_1(x) = x$, and $\gamma_i(x) \in I, i \geq 1$.
(2) $\forall x, y \in I$, $\gamma_k(x + y) = \sum_{i+j=k} \gamma_i(x)\gamma_j(x)$
(3) $\forall x, y \in I$, $\gamma_k(\lambda x) = \lambda^k \gamma_k(x)$

(4) $x \in I$, $\gamma_i(x)\gamma_j(x) = \binom{i+j}{j}\gamma_{i+j}(x)$, where
$$\binom{i+j}{i} = \frac{(i+j)!}{i!j!}$$
(5) $\gamma_p(\gamma_q(x)) = C_{p,q}\gamma_{pq}(x)$, where
$$C_{p,q} = \frac{(pq)!}{p!(q!)^p}$$

Example 1.2. (1) (0) is a PD ideal with $\gamma_i(0) = 0, \forall i \geq 1$.

(2) Let A be a $\mathbb{Q}$-algebra. Then there exists a unique PD structure for any ideal $I \subset A$ given by $\gamma_n(x) = x^n/n!$.

(3) Suppose A has characteristic $p > 0$ (i.e. $pA = 0$). Then an ideal I has a PD structure *only if* I is nilpotent: Axioms (1) and (4) imply
$$n!\gamma_n(x) = x^n \quad \forall n \geq 0$$
But then $p!\gamma_p(x) = 0 = x^p$.

(4) Let $A = V$ be a DVR of mixed characteristic $(0, p)$ with a uniformizer π and residue field k. Write $p = u\pi^e$, where e is called the absolute ramification index of V. Then (π) has PD if and only if $e \leq p - 1$.

Proof.

Lemma 1.3 (Legendre's formula). *Let $n = \sum a_i p^i \in \mathbb{Z}$ with $0 \leq a_i < p$. Then*
$$\mathrm{ord}_p(n!) = \frac{1}{p-1}\sum a_i(p^i - 1)$$

Thus,
$$\begin{aligned}
\mathrm{ord}_\pi(\gamma_n(\pi)) &= n - \mathrm{ord}_\pi(n!) \\
&= n - e\,\mathrm{ord}_p(n!) \\
&= \sum a_i p^i - \frac{e}{p-1}\sum a_i(p^i - 1) \\
&= \frac{1}{p-1}\sum a_i[p^i(p-1-e) + e] \\
&= \frac{p-1-e}{p-1}n + e\frac{\sum a_i}{p-1}
\end{aligned}$$

□

So $\gamma_n(\pi) \in (\pi)$ if and only if the last quantity above is greater than 0 for any a_i; this is equivalent to $p - 1 - e \geq 0$, i.e., $p - 1 \geq e$.

Some terminologies

Definition 1.4. A PD morphism $(A, I, \gamma) \to (B, I, \delta)$ is

- $f : A \to B$ a homomorphism of rings such that
- $f(I) \subset J$
- $\delta_n(f(x)) = f(\gamma_n(x)), \forall n, \forall x \in I.$

Definition 1.5. Let (A, I, γ) be a PD algebra. A sub-ideal $J \subset I$ is said to be a *sub PD ideal* if $\gamma_i(x) \in J, \forall x \in J, \forall i \geq 1$.

Lemma 1.6. *If (A, I, γ) is a PD algebra and $J \subset A$ is an ideal, then there exists a unique PD structure $\bar{\gamma}$ on $\overline{I} = I(A/J)$ such that $(A, I, \gamma) \to (A/J, \overline{I}, \bar{\gamma})$ is a PD morphism if and only if $J \cap I \subset I$ is a sub PD ideal.*

Lemma 1.7. *If I is a PD ideal, then $I^n \subset I$ is a sub PD ideal $\forall n \geq 1$.*

Lemma 1.8. *Let (I, γ) and (J, δ) be PD ideals. Suppose $I \cap J$ is a sub PD ideal of I and J and suppose γ and δ agree on $I \cap J$. Then there exists a unique PD structure on $K = I + J$ such that I and J are sub PD ideals.*

Example 1.9. $(p) \subset W$ has a unique PD structure. $(p^n) = (p)^n \subset W$ are sub PD ideals. So we have an induced PD structure on $(W_m, (p))$ for each m. We will show in later sections that W_m in general has many PD structures.

The notion of PD morphism is natural but rather restrictive. We want to introduce a more flexible notion.

Definition 1.10. Let (A, I, γ) be a PD algebra, and B an A-algebra. We say $\gamma extendstoBifthereisaPDstructu$
$(B, IB, \bar{\gamma})$ is a PD morphism.

Proposition 1.11. *If I is principal, then γ extends to any B.*

Proof. Write $I = (g)$ and $f : A \to B$. We set $\bar{\gamma}_k(b \cdot f(g)) := b^k \bar{\gamma}_k(f(g)) = b^k f(\gamma_k(g))$ for any $b \in B$. □

Proposition 1.12. *Let (A, I, γ) and B as above, and let (J, δ) be a PD ideal of B. Then the following are equivalent:*

(1) γ extends to B and $\bar{\gamma} = \delta$ on $IB \cap J$.
(2) $K = IB + J$ has a unique PD structure $\bar{\delta}$ such that $(A, I, \gamma) \to (B, K, \bar{\delta})$ and $(B, J, \bar{\delta}) \to (B, K, \delta)$ are PD morphisms.
(3) There exists an ideal $K' \supset IB + J$ with a PD structure δ' such that $(A, I, \gamma) \to (B, K', \delta')$ and $(B, J, \delta) \to (B, K', \delta')$ are PD morphisms.

Definition 1.13. PD structures γ, δ are called *compatible* if the equivalent conditions above are satisfied.

Now we discuss the main result on PD structures.

Theorem 1.14. *Let (A, I, γ) be a PD algebra, B an A-algebra, $I \subset B$ an ideal. Then there exists a B-algebra $D_{B,\gamma}(J)$ with a PD ideal $(\bar{J}, \bar{\gamma})$ such that*

(1) $JD_{B,\gamma}(J) \subset \bar{J}$
(2) $\bar{\gamma}$ is compatible with γ
(3) the following universal property is satisfied:

$$\mathrm{Hom}_{(A,I,\gamma)}\big((D_{B,\gamma}(J), \bar{J}, \bar{\gamma}), (C, K, \delta)\big) = \mathrm{Hom}_{(A,I)}\left((B, J), (C, K)\right)$$

functorially in PD algebras (C, K, δ) over (A, I, γ).

If B' is a B-algebra, then there is a natural map

$$D_{B,\gamma}(J) \otimes_B B' \to D_{B',\gamma'}(JB')$$

It is an isomorphism if B' is flat over B.

2. Globalization

We shall now discuss the globalization of the theory of PD structures. This is nothing but a sheaf-theoretic reformulation of the results above.

We also introduce the PD analogue of infinitesimal neighborhoods.

Definition 2.1. Let (A, I, γ) be a PD algebra. For $n \geq 1$, define

$$I^{[n]} := \langle \gamma_{i_1}(x_1), \cdots \gamma_{i_k}(x_k) \mid \sum i_j \geq n, x \in I \rangle$$

Example 2.2. Consider $W = W(k)$ with its canonical PD structure. Then $(p)^{[n]} = (p^\nu)$ where

$$\nu = \inf_{k \geq n} \{v_p(p^k/k!)\}.$$

Proposition 2.3. *$I^{[n]} \subset I$ is a sub PD ideal. $I^{[n]} I^{[m]} \subset I^{[n+m]}$.*

Lemma 2.4. *Let (A, I, γ) be a PD algebra, and $f \in A$ be an element. Then the localization (A_f, I_f) has a canonical PD structure γ_f and $(A, I, \gamma) \to (A_f, I_f, \gamma_f)$ is PD:*

$$\gamma_{f,n}(x/f^k) := \gamma_n(x)/f^{kn}$$

Thus, we get a sheaf of PD algebras on $\operatorname{Spec} A$ (Recall that the basic opens $\operatorname{Spec} A_f$ with $f \in A$ form a basis for the Zariski topology on $\operatorname{Spec} A$).

Let S be a scheme, and $I \subset \mathcal{O}_S$ be a quasi-coherent sheaf of ideals with PD structure γ. Let X be an S-scheme, $\mathcal{B}$ a quasi-coherent $\mathcal{O}_X$-algebra, and $\mathcal{J} \subset \mathcal{B}$ a quasi-coherent sheaf of ideals. Then $\mathcal{D}_{\mathcal{B},\gamma}(\mathcal{J})$ is a quasi-coherent $\mathcal{O}_X$-algebra.

We usually consider closed immersion $i : X \to Y$ with ideal $\mathcal{J}$ (of S-schemes). Here (S, I, γ) is as above. We have the PD envelope

$$\mathcal{D}_{X,\gamma}(Y) := \mathcal{D}_{\mathcal{O}_Y,\gamma}(J)$$

We also write

$$D_{X,\gamma}(Y) := \underline{\operatorname{Spec}}_Y \mathcal{D}_{X,\gamma}(Y).$$

Definition 2.5. Assume $X \to Y$ is a closed immersion of S-schemes.

$$\mathcal{D}^n_{X,\gamma}(Y) := \mathcal{D}_{X,\gamma}(Y)/\bar{J}^{[n+1]}$$

is called the n-th PD neighborhood of X in Y.

Example 2.6. If $X \to Y$ is a closed immersion of varieties over a char-0 field (e.g. $\mathbb{C}$), then $\mathcal{D}^n_{X,\gamma}(Y) \cong \mathcal{O}_Y / J^n$. So PD neighborhoods recover formal neighborhoods in characteristic 0.

3. Example of PD algebras and envelopes: PD polynomial algebras

We first introduce the PD polynomial algebra. Let A be a ring. Consider the following graded A-algebra

$$A\langle x_1, \ldots, x_n\rangle = \bigoplus_{i_k \geq 0} A x_1^{[i_1]} \cdots x_n^{[i_n]}$$

with the following properties:

(1) The multiplication is given by

$$x_p^{[i]} x_p^{[j]} = \frac{(i+j)!}{i!j!} x_p^{[i+j]}$$

(2) $x_p = x_p^{[1]}$

This looks like a PD structure. In fact, it comes from the augmentation ideal

$$I = \bigoplus_{\text{at least one } i_k > 0} A x_1^{[i_1]} \cdots x_n^{[i_n]}$$

in $A\langle x_1, \ldots, x_n\rangle$ with a PD structure γ such that $\gamma_n(x_i) = x_i^{[n]}$

More generally, one can construct a PD algebra $(\Gamma(M), \Gamma^+(M), \gamma_M)$ out of any A-module M (not required to be finitely generated) which satisfies a list of nice properties, and $A\langle x_1, \ldots, x_n\rangle$ is the special case where $M = A^n$ the rank-n free module.

The PD polynomial algebra $A\langle x_1, \ldots, x_n\rangle$ plays a special role in the construction of PD envelopes. Let $M = A^n$, $B = \mathrm{Sym}_A^\bullet(M) \cong A[x_1, \ldots, x_n]$. Let $\gamma = 0$ be the trivial PD structure on the ideal $(0) \subset A$, and $J = (x_1, \ldots, x_n) \subset B$ be the augmentation ideal.

The PD envelope $D_{B,0}(J)$ is just the PD polynomial algebra $A\langle x_1, \ldots, x_n\rangle$. PD envelopes in the special case (A, I, γ) with $f : (A, I) \to (B, J)$ (i.e., $f(I) \subset J$) are constructed similarly from certain $(\Gamma(M), \Gamma^+(M), \gamma_M)$. But one needs to carefully quotient out some additional relations.

Nevertheless, if (S, I, γ) is a PD scheme, and $X \to Y$ is a closed immersion of smooth S-schemes with $m\,\mathcal{O}_Y = 0$ for some positive integer m, then Zariski locally, the PD envelope $\mathcal{D}_{X,\gamma}(Y)$ is isomorphic to the PD polynomial algebra over $\mathcal{O}_X$ in $\mathrm{codim}(X, Y)$ variables. That is, if $d = \mathrm{codim}(X, Y)$ then Zariski locally,

$$\mathcal{D}_{X,\gamma}(Y) \cong \mathcal{O}_X\langle x_1, \ldots, x_d\rangle.$$

4. PD structures on rings of truncated Witt vectors

Let k be a perfect field, and let $W = W(k)$ be the ring of Witt vectors. Write $W_m = W/p^m$ for the rings of (m-)truncated Witt vectors.

Over the ideal $(p) \subset W$, there is a unique PD structure γ^{can} (the ad hoc notation stands for "canonical PD structure") given by

$$\gamma_n^{\mathrm{can}}(x) = \frac{x^n}{n!}$$

The existence is clear. To see this is unique, we again notice that Axioms 1) and 4) imply that any PD structure γ on (p) satisfies

$$n!\gamma_n(x) = x^n.$$

But then $\gamma = \gamma^{\mathrm{can}}$.

By the basic properties of PD structures, the canonical (unique) PD structure γ^{can} induces a PD structure, again denoted as γ^{can}, on W_m for any m. Our next goal is then to show there are other PD structures on W_m.

Notice again by Axioms 1) and 4), we have a unique choice for γ_n for $n < p$ given by

$$\gamma_n(x) = \frac{x^n}{n!}.$$

Assume $2 \leq m \leq p$. For $n = p$, we have

$$p!\gamma_p(p) = p^p = 0,$$

which implies $\gamma_p(p) \in (p^{m-1})$.

Lemma 4.1. *With the notations as above, for any $u \in W_m$, there is a PD structure γ on W_m with $\gamma_p(p) = u \cdot p^{m-1}$.*

The proof of this lemma is long and will be given in Section 6.

5. Maybe something/everything is wrong?

Finally, I would like to mention that some key proofs adopted from Roby's works in Berthelot's thesis may not be reliable. The reference is the blog post by Kevin Buzzard: https://xenaproject.wordpress.com/2024/12/11/fermats-last-theorem-how-its-going/

In summary, Antoine Chambert-Loir and Maria Ines de Frutos Fernandez (yes, our BU friend), with the aid of Lean, found that there is flaw in the construction in Berthelot's thesis of the PD algebra $(\Gamma(M), \Gamma^+(M), \gamma_M)$ for an A-module M. The problem seems to be that Roby's "Les algebres a puissances divisees", published in Bull Sci Math, 2ieme serie, 89, 1965, pages 75-91. Lemme 8 (on p86) is false. I have not found a copy of the paper, so I don't know what the statement actually is. But Brian Conrad pointed out that the construction of $(\Gamma(M), \Gamma^+(M), \gamma_M)$ in Berthelot-Ogus should be correct. So the crisis is resolved.

(But Ogus said there are others errors in the book, which are fixable.)

6. Proof of Lemma 4.1

We define

$$\gamma_n(p) = \begin{cases} \frac{p^n}{n!} & 0 < n < p \\ u \cdot p^{m-1} & n = p \\ 0 & n > p \end{cases}$$

For any element $x = ap \in (p)$ ($a \in W_m$), we define

$$\gamma_n(ap) = a^n \gamma_n(p)$$

The rest is to check γ satisfies the Axioms. Axioms 1) and 3) are satisfied by construction.

Axiom 2). Write $x = ap$ and $y = bp$ for $a, b \in W_m$. On one hand,

$$\gamma_k(ap+bp) = \gamma_k((a+b)p) = \begin{cases} (a+b)^k \frac{p^k}{k!} & 0 < k < p \\ (a+b)^p u p^{m-1} & k = p \\ 0 & k > p \end{cases}$$

Write $S_k := \sum_{i+j=k} \gamma_i(x)\gamma_j(y)$

If $k < p$, then

$$\begin{aligned} S_k &= \sum_{i+j=k} \frac{p^i}{i!}\frac{p^j}{j!} a^i b^j \\ &= \gamma_k(ap+bp) \end{aligned}$$

If $k = p$, then

$$S_p = \sum_{i=1}^{p-1} \frac{p^{p-1}}{(p-1)!}\frac{p!}{i!j!} a^i b^{p-i} + \gamma_p(p)(a^p + b^p)$$

So

$$\begin{aligned} S_k - \gamma_p(ap+bp) &= \left[\left(\frac{p^{p-m}}{(p-1)!} - u\right) p^{m-1}\right] \sum_{i=1}^{p-1} \frac{p!}{i!(p-i)!} a^i b^{p-i} \\ &= p^m \left(\frac{p^{p-m}}{(p-1)!} - u\right) \sum_{i=1}^{p-1} \frac{(p-1)!}{i!(p-i)!} a^i b^{p-i} \\ &= 0 \end{aligned}$$

Now assume $k > p$. In this case $\gamma_k(ap+bp) = 0$. There are three subcases.

- *Subcase 1.* $k > 2p$:
$$S_k = \sum_{i+j=k} \gamma_i(x)\gamma_j(y) = 0$$
since both $i > p$ and $j > p$.
- *Subcase 2.* $k = 2p$:
$$S_{2p} = \gamma_p(ap)\gamma_p(bp) = a^p b^p u^2 p^{2m-2}$$
where $p^{2m-2} = 0$ since $m \geq 2$.
- *Subcase 3.* $k < 2p$:
$$S_k = \gamma_{k-p}(x)\gamma_p(y) + \cdots + \gamma_p(x)\gamma_{k-p}(y)$$
The first and the last terms are:
$$\gamma_{k-p}(x)\gamma_p(y) = \frac{a^{k-p}p^{k-p}}{(k-p)!} u \cdot b^p p^{m-1} = \frac{a^{k-p}}{(k-p)!} u \cdot b^p p^{k-p+m-1} = 0$$

since $k-p+m-1 \geq m$, and

$$\gamma_p(x)\gamma_{k-p}(y) = 0$$

by "symmetry".

Each of the rest terms in the sum is of the form

$$\gamma_{k-p+i}(x)\gamma_{p-i}(y) = \frac{a^{k-p+i}p^{k-p+i}}{(k-p+i)!}\frac{b^{p-i}p^{p-i}}{(p-i)!} = 0$$

Axiom 4).

- *Subcase 1.* $i+j<p$:

$$\gamma_i(p)\gamma_j(p) = \frac{p^ip^j}{i!j!} = \binom{i+j}{i}\gamma_{i+j}(p)$$

- *Subcase 2.* $i+j>2p$:

$$\gamma_i(p)\gamma_j(p) = 0 = \binom{i+j}{i}\gamma_{i+j}(p)$$

- *Subcase 3.* $i+j=2p$:

$$\gamma_p(p)\gamma_p(p) = u^2p^{2m-2} = 0$$

  since $2m-2 \geq m$.
- *Subcase 4.* $i+j=p$: If $i \neq p$ and $j \neq p$, then

$$\gamma_i(p)\gamma_j(p) = \frac{a^ip^i}{i!}\frac{b^jp^j}{j!} = \frac{a^i}{i!}\frac{b^j}{j!}p^p = 0$$

  On the other hand

$$\binom{p}{i}\gamma_p(p) = \frac{(p-1)!}{i!(p-i)!}up^m = 0$$

  If $i=p$, then

$$\gamma_p(p)\gamma_0(p) = \gamma_p(p) = \binom{p}{0}\gamma_p(p)$$

  The case $j=0$ is similar.
- *Subcase 5.* $p<i+j<2p$: We may assume $i \leq j$. If $j>p$, then apparently, $\gamma_i(p)\gamma_j(p)=0$. So we assume $j \leq p$. Then

$$\gamma_i(p)\gamma_j(p) = \frac{p^i}{i!}\frac{p^j}{j} = 0$$

  since $i+j>p$.

Axiom 5).

$$\gamma_i(\gamma_j(p)) = \begin{cases} \gamma_i(p^j/j!) & 0 < j < p \\ \gamma_i(up^{m-1}) & j = p \\ \gamma_i(0) & j > p \end{cases}$$

Assume $0 < j < p$.

- *Subcase 1.* $i < p$:

$$\gamma_i(p^j/j!) = \frac{p^{ij}}{i!(j!)^i} = \frac{(ij)!}{i!(j!)^i}\gamma_{ij}(p) = C_{i,j}\gamma_{ij}(p)$$

- *Subcase 2.* $i = p$: If $j > 1$, then

$$\gamma_p(p^j/j!) = \frac{p^{pj-p}}{(j!)^p}u \cdot p^{m-1} = 0 = C_{p,j}\gamma_{pj}(p)$$

  since $pj - p + m - 1 \geq m$. If $j = 1$, then

$$\gamma_p(p^j/j!) = \frac{p^{p-p}}{(1!)^p}u \cdot p^{m-1} = u \cdot p^{m-1} = C_{p,1}\gamma_p(p)$$

- *Subcase 3.* $i > p$:

$$\gamma_i(p^j/j!) = 0 = C_{i,j}\gamma_{ij}(p)$$

  since both $i > p$ and $ij > p$.

Assume $j = p$.

- *Subcase 1.* $i < p$: If $i > 1$, then

$$\gamma_i(up^{m-1}) = u^i p^{(m-2)i}\frac{p^i}{i!} = 0 = C_{i,p}\gamma_{ip}(p)$$

  since $ip > p$. If $i = 1$, then

$$\gamma_1(up^{m-1}) = up^{m-1} = C_{1,p}\gamma_p(p)$$

- *Subcase 2.* $i = p$:

$$\gamma_p(up^{m-1}) = u^p p^{(m-2)p} \cdot up^{m-1} = 0 = C_{p,p}\gamma_{p^2}(p)$$

  since $(m-2)p + m - 1 \geq m$.
- *Subcase 3.* $i > p$:

$$\gamma_i(up^{m-1}) = 0 = C_{i,p}\gamma_{ip}(p)$$

The case $j > p$ is trivial.

This completes the proof of Lemma 1.

7. Determination of all possible PD structures on truncated Witt vectors

Lemma 7.1. *Assume $2 \leq m \leq p$. Let γ be a PD structure on W_m. Then $\gamma_n(p) = 0$ for any $n > p$. Therefore, the PD structures constructed in Lemma 4.1 are the only ones for W_m.*

Proof. As discussed before, we have $\gamma_k(p) = p^k/k!$ for $1 \leq k < p$. Assume $\gamma_p(p) = u \cdot p^{m-1}$ for some $u \in W_m$. We will prove the statement by induction.

By Axiom 4),

$$\gamma_p(p)\gamma_1(p) = u \cdot p^{m-1} \cdot p = 0 = \binom{p+1}{p}\gamma_{p+1}(p) = (p+1)\gamma_{p+1}(p).$$

So $\gamma_{p+1}(p) = 0$. Now assume $\gamma_k(p) = 0$ for all $p < k < n$. If $p \nmid n$, then the relation

$$\gamma_{n-1}(p)\gamma_1(p) = 0 = \binom{n}{n-1}\gamma_n(p) = n \cdot \gamma_n(p)$$

shows $\gamma_n(p) = 0$. If $p|n$, i.e., $n = mp$ for some $m > 1$, then by Axiom 5),

$$\gamma_m(\gamma_p(p)) = 0 = C_{m,p}\gamma_{mp}(p)$$

where LHS is 0 because $\gamma_m = 0$ by the induction hypothesis as $m < mp$. Observe p does not divide $C_{m,p}$. So $\gamma_{mp}(p)$. ☐

Corollary 7.2. *If $k = \mathbb{F}_p$, then there are exactly p PD structures on $W_m \cong \mathbb{Z}/p^m$ for $2 \leq m \leq p$.*

Proof. By Lemma 4.1 and Lemma 7.1, a PD structure on $W_m(\mathbb{F}_p)$ is determined by the value $\gamma_p(p) = u \cdot p^{m-1}$, where $u \in W_m(\mathbb{F}_p)$. There are exactly p possible values. ☐

References

[BO78] Pierre Berthelot and Arthur Ogus, *Notes on Crystalline Cohomology. (MN-21)*, Princeton University Press, 1978.