A Formalization of Divided Powers in Lean

María Inés de Frutos-Fernández

University of Bonn

joint work with

Antoine Chambert-Loir

Université Paris Cité

1 October 2025

ITP 2025, Reykjavik University

Outline

Motivation: $\{x \mapsto \frac{x^n}{n!}\}_{n \in \mathbb{N}}$

A primitive of a polynomial $\displaystyle\sum_{n=0}^{N} a_n X^n \in \mathbb{R}[X]$ is given by $\displaystyle\sum_{n=0}^{N} \frac{a_n}{n+1} X^{n+1}$.

Motivation: $\{x \mapsto \frac{x^n}{n!}\}_{n\in\mathbb{N}}$

A primitive of a polynomial $\sum_{n=0}^{N} a_n X^n \in \mathbb{R}[X]$ is given by $\sum_{n=0}^{N} \frac{a_n}{n+1} X^{n+1}$.

Exponential power series: $\forall a \in \mathbb{R}, \exp(aX) = \sum_{n=0}^{\infty} \frac{a^n}{n!} X^n$.

Motivation: $\{x \mapsto \frac{x^n}{n!}\}_{n\in\mathbb{N}}$

A primitive of a polynomial $\sum_{n=0}^{N} a_n X^n \in \mathbb{R}[X]$ is given by $\sum_{n=0}^{N} \frac{a_n}{n+1} X^{n+1}$.

Exponential power series: $\forall a \in \mathbb{R}, \exp(aX) = \sum_{n=0}^{\infty} \frac{a^n}{n!} X^n$.

Both related to the family of maps $\{x \mapsto \frac{x^n}{n!} : \mathbb{R} \to \mathbb{R}\}_{n\in\mathbb{N}}$.

Motivation: $\{x \mapsto \frac{x^n}{n!}\}_{n \in \mathbb{N}}$

The family $\{x \mapsto \frac{x^n}{n!} : \mathbb{R} \to \mathbb{R}\}_{n \in \mathbb{N}}$ still makes sense if $\mathbb{R}$ is replaced by any $\mathbb{Q}$-algebra (e.g., $\mathbb{Q}, \mathbb{C}, \mathbb{Q}[X], \dots$).

What happens if we work over a ring where division by nonzero integers is not always possible (e.g., $\mathbb{Z}, \mathbb{Z}[X], \mathbb{Z}_p, \dots$)?

Motivation: $\{x \mapsto \frac{x^n}{n!}\}_{n\in\mathbb{N}}$

The family $\{x \mapsto \frac{x^n}{n!} : \mathbb{R} \to \mathbb{R}\}_{n\in\mathbb{N}}$ still makes sense if $\mathbb{R}$ is replaced by any $\mathbb{Q}$-algebra (e.g., $\mathbb{Q}, \mathbb{C}, \mathbb{Q}[X], \dots$).

What happens if we work over a ring where division by nonzero integers is not always possible (e.g., $\mathbb{Z}, \mathbb{Z}[X], \mathbb{Z}_p, \dots$)?

Cartan (1950s) observed that, in some contexts, there are families of 'divided powers' $\{x \mapsto \gamma_n(x)\}_{n\in\mathbb{N}}$ that 'behave like' $\{x \mapsto \frac{x^n}{n!}\}_{n\in\mathbb{N}}$, even when division by nonzero integers is not defined.

Motivation from number theory: The ring B_{cris}

B_{cris} is a ring used in current arithmetic geometry research:

- In p-adic Hodge theory to detect "crystalline" Galois representations.
- In a comparison theorem between cohomology theories.

Motivation from number theory: The ring B_{cris}

B_{cris} is a ring used in current arithmetic geometry research:

- In p-adic Hodge theory to detect “crystalline” Galois representations.
- In a comparison theorem between cohomology theories.

The definition of B_{cris} is very hard (>100 pages of math. research).

- One step is to take the divided power envelope of a certain ring.
- This universal construction relies on the theory of divided powers.

History of divided powers

Divided powers were introduced by Cartan (1950s) in the context of algebraic topology (homology of Eilenberg–MacLane spaces).

The main proofs are due to Roby (1960s).

The divided power envelope is due to Berthelot (1970s), who developed crystalline cohomology.

History of divided powers

Divided powers were introduced by Cartan (1950s) in the context of algebraic topology (homology of Eilenberg–MacLane spaces).

The main proofs are due to Roby (1960s).

The divided power envelope is due to Berthelot (1970s), who developed crystalline cohomology.

Now, we are formalizing the theory in Lean (2020s).

Outline

Divided powers (I)

Let I be an ideal in a commutative ring A. A divided power structure on I is a collection of maps $\gamma_n : I \to A$ for $n \in \mathbb{N}$ such that

i. $\forall x \in I,\ \gamma_0(x) = 1.$
ii. $\forall x \in I,\ \gamma_1(x) = x.$
iii. $\forall x \in I, \forall n > 0, \gamma_n(x) \in I.$
iv. $\forall x, y \in I, \gamma_n(x + y) = \sum_{i+j=n} \gamma_i(x) \cdot \gamma_j(y).$
v. $\forall a \in A, \forall x \in I, \gamma_n(a \cdot x) = a^n \cdot \gamma_n(x).$
vi. $\forall x \in I, \forall m, n \in \mathbb{N}, \gamma_m(x) \cdot \gamma_n(x) = \binom{m+n}{m} \cdot \gamma_{m+n}(x).$
vii. $\forall x \in I, \forall m \in \mathbb{N}, \forall n > 0, \gamma_m(\gamma_n(x)) = \frac{(m \cdot n)!}{m!(n!)^m} \cdot \gamma_{m \cdot n}(x).$

We call (A, I, γ) a divided power algebra.

Divided powers (II)

```
structure DividedPowers {A : Type*} [CommSemiring A] (I : Ideal A)
    where
  dpow : ℕ → A → A
  dpow_null : ∀ {n x} (_ : x ∉ I), dpow n x = 0
  dpow_zero : ∀ {x} (_ : x ∈ I), dpow 0 x = 1
  dpow_one : ∀ {x} (_ : x ∈ I), dpow 1 x = x
  dpow_mem : ∀ {n x} (_ : n ≠ 0) (_ : x ∈ I), dpow n x ∈ I
  dpow_add : ∀ {n x y} (_ : x ∈ I) (_ : y ∈ I), dpow n (x + y) =
    (antidiagonal n).sum fun k => dpow k.1 x * dpow k.2 y
  dpow_mul : ∀ {n} {a : A} {x} (_ : x ∈ I),
    dpow n (a * x) = a ^ n * dpow n x
  mul_dpow : ∀ {m n} {x} (_ : x ∈ I),
    dpow m x * dpow n x = choose (m + n) m * dpow (m + n) x
  dpow_comp : ∀ {m n x} (_ : n ≠ 0) (_ : x ∈ I),
    dpow m (dpow n x) = uniformBell m n * dpow (m * n) x
```

Implementation remarks.

- We allow commutative semirings in the definition.
- We define `dpow : ℕ → A → A`, by imposing `dpow n x = 0` if `x ∉ I`.
- `antidiagonal n` is the finite set of tuples $(i, j) \in \mathbb{N}^2$ with $i + j = n$.
- `uniformBell m n` is the number of partitions of a set with mn elements into m subsets of size n.
- We prove `n! * dpow n a = a ^ n` for all $a \in I$.

Examples

Let I be an ideal in a commutative ring A.

- If A is a $\mathbb{Q}$-algebra, $\gamma_n(x) = \frac{x^n}{n!}$ is the unique DP structure on I.
- If $A = \mathbb{Z}_p$, the ideal $I := (p)$ admits a unique DP structure, since $\frac{p^n}{n!} \in (p)$ for all $n \geq 1$.
- If $(n-1)!$ is invertible in A and $I^n = 0$, then I admits a DP structure $(x^n/n!)$. In particular:
  - if $I^p = 0$ in a ring of characteristic p.
  - if $I^p = 0$ in a ring where the prime p is nilpotent.
  - if $I^2 = 0$.

Divided power morphisms

A DP morphism $f : (A, I, \gamma) \to (B, J, \delta)$ is a ring homomorphism $f : A \to B$ such that $f(I) \subseteq J$ and such that $\delta_n(f(x)) = f(\gamma_n(x))$ for all $n \in \mathbb{N}, x \in I$.

```
def IsDPMorphism {A B : Type*} [CommSemiring A] [CommSemiring B]
    {I : Ideal A} {J : Ideal B} (hI : DividedPowers I)
    (hJ : DividedPowers J) (f : A →+* B) : Prop where
  ideal_comp : I.map f ≤ J
  dpow_comp : ∀ {n : ℕ}, ∀ a ∈ I, hJ.dpow n (f a) = f (hI.dpow n a)
```

- The composition of DP morphisms is a DP morphism.
- If $I = \text{span}(S)$ and $f : A \to B$ is a ring homomorphism such that $f(I) \subseteq J$, and $\forall n \in \mathbb{N}, x \in S$ the equality $\delta_n(f(x)) = f(\gamma_n(x))$ holds, then f is a DP morphism.

Sub-DP-Ideals (I)

Let (A, I, γ) be a divided power algebra. A subideal $J \leq I$ is a sub-DP-ideal of I if $\gamma_n(x) \in J$ for all $n > 0, x \in J$.

```
structure IsSubDPIdeal {A : Type*} [CommSemiring A] {I : Ideal A}
    (hI : DividedPowers I) (J : Ideal A) : Prop where
  isSubideal : J ≤ I
  dpow_mem : ∀ {n : ℕ} (_: n ≠ 0) {j : A} (_ : j ∈ J), hI.dpow n j ∈ J

structure SubDPIdeal {A : Type*} [CommSemiring A] {I : Ideal A}
    (hI : DividedPowers I) where
  carrier : Ideal A
  isSubideal : carrier ≤ I
  dpow_mem : ∀ {n : ℕ} (_ : n ≠ 0), ∀ j ∈ carrier, hI.dpow n j ∈ carrier
```

Sub-DP-Ideals (II)

Let (A, I, γ) be a divided power algebra, $J \leq I$ be a sub-ideal.

- To check whether $\mathrm{span}(S)$ is a sub-DP-ideal of (I, γ), it suffices to check the condition on the generators.
- $J \cap I$ is a sub-DP-ideal of I iff there is a DP structure on $I \cdot A/J$ such that the quotient map is a DP morphism.
- Sub-DP-ideals of I form a complete lattice.
- Let $f : (A, I, \gamma) \to (B, K, \delta)$ be a DP morphism. Then $\mathrm{span}(f(I))$ is a sub-DP-ideal of K and $\ker f \cap I$ is a sub-DP-ideal of I.

Divided powers on a sum of ideals

Given divided powers (A, I, γ_I), (A, J, γ_J) that agree on $I \cap J$, $I + J$ has a unique divided power structure γ_{I+J} extending those on I and J.

First implementation:

$$\gamma_{I+J}(x + y) = \sum_{k=0}^{n} \gamma_{I,k}(x)\gamma_{J,n-k}(y) \quad \text{for } x \in I, y \in J.$$

Preferred implementation: Unique linear map $I + J \to \mathscr{E}(A)$ that extends $I \to \mathscr{E}(A)$ and $J \to \mathscr{E}(A)$, where $\mathscr{E}(A)$ is the exponential module of A $\rightsquigarrow$ requires topology of power series rings.

Outline

The exponential module

- A power series $f \in A[\![X]\!]$ is of exponential type if $f(0) = 1$ and $f(X+Y) = f(X) \cdot f(Y)$.
- The exponential module $\mathscr{E}(A)$ is the set of power series of exponential type (with addition given by product of power series, and external law given by rescaling).
- If (A, I, γ) is a divided power algebra, then for every $a \in I$, the power series $\exp_I(aX) = \sum \gamma_n(a) X^n$ is of exponential type.
- The map $a \mapsto \exp_I(aX) : I \to \mathscr{E}(A)$ is a morphism of A-modules.

The exponential module

- A power series $f \in A[\![X]\!]$ is of exponential type if $f(0) = 1$ and $f(X+Y) = f(X) \cdot f(Y)$.

- The exponential module $\mathscr{E}(A)$ is the set of power series of exponential type.

- If (A, I, γ) is a divided power ideal, then for every $a \in I$, the power series $\exp_I(aX) = \sum \gamma_n(a) X^n$ is of exponential type.

- The map $a \mapsto \exp_I(aX) : I \to \mathscr{E}(A)$ is a morphism of A-modules.

Topology on multivariate power series rings

Let A be a ring with a topology, σ a set.

The ring $A[\![(X_s)_{s\in\sigma}]\!]$ of multivariate power series is naturally induced with the product topology, provided as scoped instance.

```
open scoped MvPowerSeries.WithPiTopology
```

With the product topology on $A[\![(X_s)_{s\in\sigma}]\!]$:

- If A is Hausdorff, then so is $A[\![(X_s)_{s\in\sigma}]\!]$.
- If A is a topological (semi)ring, then so is $A[\![(X_s)_{s\in\sigma}]\!]$.
- If A is a complete uniform space, then so is $A[\![(X_s)_{s\in\sigma}]\!]$, and $A[(X_s)_{s\in\sigma}]$ is dense in $A[\![(X_s)_{s\in\sigma}]\!]$.

Evaluation and substitution of multivariate power series

Let A be a topological ring, B an A-algebra, σ a set.

Assume that the topology on A is linear (i.e., zero has a basis of open neighborhoods consisting of two-sided ideals).

- Evaluation of polynomials $f \in A[(X_s)_{s\in\sigma}]$ is possible $\forall\, (b_s)_{s\in\sigma} \subseteq B$.
- Evaluation of power series $f \in A[\![(X_s)_{s\in\sigma}]\!]$ at $(b_s)_{s\in\sigma} \subseteq B$ is possible e.g. when σ is finite and the b_s are topologically nilpotent.
- Substitution of multivariate power series, under certain conditions.
  - E.g., if σ is finite, and $(b_s)_{s\in\sigma} \subseteq B[\![(X_s)_{s\in\sigma}]\!]$, it suffices that the constant coefficient of b_s is zero (or nilpotent) for each $s \in \sigma$.

Questions

Thanks for listening! Questions?

https://doi.org/10.4230/LIPIcs.ITP.2025.4

https://github.com/mariainesdff/divided_powers_journal