Sur la formalisation des puissances divisées

Colloque *Formalisation des mathématiques et types dépendants*
Collège de France, 2 juin 2025

Antoine Chambert-Loir (Université Paris Cité, IMJ-PRG)

Travail en commun avec María Inés de Frutos Fernández (Universität Bonn)

Puissances divisées

Années 1950 — Topologie algébrique

Structure algébrique inventée par Henri Cartan (1954) : opérations supplémentaires sur l'homologie des espaces d'Eilenberg-MacLane (Séminaire 1954/55, 7e année, exposé 3)

Années 1960 — Algèbre commutative

Développée par Norbert Roby (1963, 1965, 1968). Il se restreint au cas des anneaux commutatifs.

Années 1970 — Géométrie algébrique

Brique fondamentale pour l'invention par Alexandre Grothendieck (1968) du **topos cristallin** d'un schéma et le développement par Pierre Berthelot (1974) de la cohomologie cristalline.

Puissances divisées

Années 1950 — Topologie algébrique

Structure algébrique inventée par Henri Cartan (1954) : opérations supplémentaires sur l'homologie des espaces d'Eilenberg-MacLane (Séminaire 1954/55, 7^{e} année, exposé 3)

Années 1960 — Algèbre commutative

Développée par Norbert Roby (1963, 1965, 1968). Il se restreint au cas des anneaux commutatifs.

Années 1970 — Géométrie algébrique

Brique fondamentale pour l'invention par Alexandre Grothendieck (1968) du **topos cristallin** d'un schéma et le développement par Pierre Berthelot (1974) de la cohomologie cristalline.

Années 2020 — Formalisation en `Lean/mathlib`

Puissances divisées

Définition

Soit A un anneau (commutatif, unitaire) et I un idéal de A.
*Une **structure de puissances divisées** sur I est une suite d'applications $x \mapsto x^{[n]}$ de I dans A telles que pour tous $x, y \in I$, on ait :*

1. $x^{[0]} = 1$, $x^{[1]} = x$; *si* $n \geqslant 1$, $x^{[n]} \in I$;
2. $x^{[m]}x^{[n]} = \binom{m+n}{m} x^{[m+n]}$;
3. $(x+y)^{[n]} = \sum_{p+q=n} x^{[p]}y^{[q]}$ *(formule du binôme sans coefficients binomiaux);*
4. $(xy)^{[m]} = x^m y^{[m]} = x^{[m]}y^m = m!x^m y^m$;
5. $(x^{[m]})^{[n]} = (\!(m,n)\!)x^{[mn]}$, *où* $(\!(m,n)\!) = (mn)!/n!m!^n$ *est le nombre de partitions d'un ensemble à mn éléments en n parties de m élements.*

Formalisation

```
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
```

Formalisation

Remarques sur le code :

- On a choisi de permettre cette définition pour tout *semi*-anneau, mais on n'a pas supprimé l'hypothèse *commutatif* car on ne connaît apparemment pas de bonne axiomatique dans le cas non commutatif.
- On définit `dpow` : $\mathbb{N} \to$ `A` $\to$ `A` sur tout l'anneau, en imposant `dpow_null` : `dpow n x = 0` si `x` $\notin$ `I`.
- C'est une `structure` et non une `class` car Lean ne peut pas deviner de quel idéal il s'agit. Mathématiquement, on veut aussi pouvoir considérer plusieurs structures de puissances divisées sur un même idéal.
- `antidiagonal n` est l'ensemble fini des couples (p, q) tels que $p + q = n$.
- `uniformBell m n` est le nombre de partitions d'un ensemble à mn éléments en m parties de cardinal n; il est défini par un produit explicite qui montre que c'est un entier, plutôt que par la formule $(mn)!/m!n!^m$.
- Ces axiomes permettent de démontrer `factorial_mul_dpow_eq_pow : n ! * dpow n x = x ^ n`.

Exemples

- Si les entiers non nuls sont réguliers dans A, la formule $n!x^{[n]} = x^n$ montre qu'il existe au plus une structure de puissance divisée sur un idéal I de A.
- Si A est une $\mathbf{Q}$-algèbre, tout idéal possède une (unique) structure de puissances divisées.
- Si $A = \mathbf{Z}_p$, l'idéal $I = \langle p \rangle$ possède une unique structure de puissances divisées (car $p^n/n! \in \langle p \rangle$ pour tout $n \geqslant 1$).
- Si $(p-1)!$ est inversible dans A et $I^p = 0$, alors $x^{[n]} = n!^{-1}x^n$ pour $n < p$, et $x^{[n]} = 0$ pour $n \geqslant p$, fournit une structure de puissances divisées.
- Si p est un nombre premier et $p \cdot 1_A = 0$, toute structure de puissances divisées est déterminée par l'application $x \mapsto x^{[p]}$ de I dans I.

Constructions universelles

Au delà de ces exemples explicites, deux constructions universelles sont importantes en pratique :

- L'**algèbre à puissances divisées** d'un module (Roby, 1965) : si M est un A-module, c'est une A-algèbre $\Gamma_A(M)$ munie d'un idéal à puissances divisées $\Gamma_A^+(M)$ et d'un morphisme de A-modules $M \to \Gamma_A(M)$ dont l'image engendre $\Gamma_A^+(M)$ comme idéal à puissances divisées, universelle pour cette propriété.
- L'**enveloppe à puissances divisées** d'un idéal (Berthelot, 1974) : si I est un idéal d'un anneau A, c'est une A-algèbre $\widetilde{A}$ munie d'un idéal $\widetilde{I}$ à puissances divisées contenant l'image de I, universel pour cette propriété.

L'existence de tels objets est plus ou moins formelle, il suffit de prouver qu'un foncteur d'oubli convenable possède un adjoint à gauche, mais cela ne donne aucune information sur la structure de ces objets.

L'algèbre à puissances divisées : définition

Soit A un anneau (commutatif, unitaire) et M un A-module. Roby (1963) définit l'algèbre à puissances divisées $\Gamma_A(M)$ de M par générateurs et relations.

Les générateurs sont les symboles $x^{[n]}$, pour $x \in M$ et $n \in \mathbf{N}$.

Les relations sont les suivantes, pour $x, y \in M$ et $n \in \mathbf{N}$:

- $(ax)^{[m]} = a^m x^{[m]}$;
- $x^{[m]} x^{[n]} = \binom{m+n}{n} x^{[m+n]}$;
- $(x+y)^{[n]} = \sum_{p+q=n} x^{[p]} y^{[q]}$.

Algèbre à puissances divisées : formalisation

```
variable (R M : Type*) [CommSemiring R] [AddCommMonoid M] [Module R M]

inductive Rel : (MvPolynomial (ℕ × M) R) → (MvPolynomial (ℕ × M) R) → Prop
  | rfl_zero : Rel 0 0 -- Needed for technical reasons.
  | zero {a : M} : Rel (X (0, a)) 1
  | smul {r : R} {n : ℕ} {a : M} : Rel (X (n, r • a)) (r ^ n • X (n, a))
  | mul {m n : ℕ} {a : M} : Rel (X (m, a) * X (n, a)) (Nat.choose (m + n) m •
    X (m + n, a))
  | add {n : ℕ} {a b : M} :
    Rel (X (n, a + b)) ((Finset.antidiagonal n).sum fun k => X (k.1, a) * X
    (k.2, b))

abbrev DividedPowerAlgebra : Type _ := RingQuot (DividedPowerAlgebra.Rel R M)
```

Algèbre à puissances divisées : premières propriétés

Si $x^{[m]}$ a degré m, ces relations sont homogènes, si bien que $\Gamma_A(M)$ est une algèbre graduée.

On prouve $\Gamma_A^0(M) = A$ et $\Gamma_A^1(M) = M$.

L'idéal d'augmentation $\Gamma_A^+(M)$ de $\Gamma_A(M)$ est engendré par les classes des symboles $x^{[n]}$ pour $x \in M$ et $n \geqslant 1$.

```
DividedPowerAlgebra.augIdeal : Ideal (DividedPowerAlgebra R M) : Type _ :=
  RingHom.ker (algebraMapInv R M)
```

où `algebraMapInv` représente le morphisme d'algèbres de $\Gamma_A(M)$ dans A qui applique $x^{[n]}$ sur 1 si $n = 0$ et sur 0 sinon.

Pourquoi possède-t-il des puissances divisées ?

Algèbre à puissances divisées : unicité

Par construction, tout élément de $\Gamma_A^+(M)$ se décompose sous la forme d'une somme finie

$$\xi = \sum_{i=1}^{p} x_i^{[m_i]} y_i \qquad \text{où } x_i \in M,\ m_i \geqslant 1 \text{ et } y_i \in \Gamma_A(M).$$

Si $\Gamma_A^+(M)$ possède une structure de puissances divisées pour laquelle $x^{[m]}$ est effectivement la puissance divisée m-ième de x, elle est prescrite par la « formule du multinôme » (sans coefficients multinomiaux) :

$$\xi^{[n]} = \sum_{n_1+\cdots+n_p=n} \prod (x_i^{[m_i]})^{[n_i]} \prod_{y_i}^{n_i} = \sum_{n_1+\cdots+n_p=n} \prod (\!(m_i, n_i)\!) \prod x_i^{[m_i+n_i]} \prod {y_i}^{n_i}.$$

L'idéal d'augmentation possède donc au plus une structure de puissances divisées ; mais en possède-t-il une ?

Algèbre à puissances divisées : existence

La démonstration proposée par Roby (1965) de l'existence est compliquée, et en fait un peu bancale car la preuve du lemme 8 ne fait pas sens.

On peut la réparer (ACL/MIdFF) en généralisant les arguments de son lemme 12 ; la preuve qui en résulte est plus simple.

Roby (1968) en propose une seconde, également plus simple.

Dans tous les cas, la clé est une compréhension duale de l'algèbre à puissances divisées, c'est-à-dire de prouver qu'elle est également un adjoint à droite — plus exactement chacun de sous-modules homogènes.

Penser au fait que l'algèbre de polynômes est un module **libre**, mais que ça ne se voit pas sur sa définition par générateurs (sans relations).

Théorème (Roby, 1963)

Pour tout entier n, l'application $x \mapsto x^{[n]}$ de M dans $\Gamma_A^n(M)$ est la loi polynomiale homogène de degré n universelle.

Si M et N sont des A-modules, une **loi polynomiale** $p \in P_A(M; N)$ est la donnée d'applications $p_R \colon R \otimes_A M \to R \otimes_A N$, pour toute A-algèbre R, de façon fonctorielle en R.

(Pour donner sens au théorème précédent, il faut promouvoir l'application indiquée en une loi polynomiale.)

La terminologie vient de ce que pour toute suite finie $\mu = (m_i)$ dans M, il existe un unique polynôme $p^\mu \in N[T_i]$ tel que $p_R(\sum r_i \otimes m_i) = p^\mu(r)$ pour toute A-algèbre R et toute famille (r_i) dans R.

Une loi polynomiale p est homogène de degré n si les polynômes p^μ sont homogènes de degré n.

Lois polynomiales : formalisation

```
structure PolynomialLaw (R : Type u) [CommSemiring R]
    (M : Type*) [AddCommMonoid M] [Module R M]
    (N : Type*) [AddCommMonoid N] [Module R N] where
  /-- The functions `S ⊗[R] M → S ⊗[R] N` underlying a polynomial law -/
  toFun' (S : Type u) [CommSemiring S] [Algebra R S] : S ⊗[R] M → S ⊗[R] N
  /-- The compatibility relations between the functions underlying a
    polynomial law -/
  isCompat' {S : Type u} [CommSemiring S] [Algebra R S]
    {S' : Type u} [CommSemiring S'] [Algebra R S'] (φ : S →ₐ[R] S') :
    φ.toLinearMap.rTensor N ∘ toFun' S = toFun' S' ∘ φ.toLinearMap.rTensor M
    := by aesop
```

Noter que pour `toFun'` et `isCompat'`, l'algèbre `S` est restreinte au même **univers** que `R`, mais on peut ensuite *construire* leurs extensions `PolynomialLaw.toFun` et `PolynomialLaw.isCompat` à tout univers.

Algèbre à puissances divisées

Deux applications importantes du théorème précédent.

Corollaire (Roby, 1963)

Soit M un A-module libre, de base (e_i). Pour tout entier n, le A-module $\Gamma_A^n(M)$ est libre, de base la famille des $\prod e_i^{[n_i]}$, où (n_i) est une famille finie d'entiers, de somme n.

Corollaire (Roby, 1963)

Soit M un A-module et N un sous-module de M. Le morphisme d'algèbres canonique $\Gamma_A(M) \to \Gamma_A(M/N)$ est surjectif; son noyau est l'idéal engendré par les $x^{[n]}$, pour $x \in N$ et $n \geqslant 1$.

Nous n'avons pas encore formalisés ces corollaires (ni le théorème, d'ailleurs).

Algèbre à puissances divisées : construction

Soit R une $\mathbf{Z}$-algèbre intègre et fidèle munie d'un homomorphisme surjectif $\varphi\colon R \to A$; nous prenons l'anneau des polynômes à coefficients entiers sur $A - \{0\}$.

Soit F le corps des fractions de R.

Soit L le R-module libre de base une famille génératrice (m_i) de M.

Notre preuve de l'existence des puissances divisées sur l'idéal $\Gamma_A^+(M)$ de $\Gamma_A(M)$ consiste à contempler le diagramme d'anneaux, de modules et d'algèbres

$$F \hookleftarrow R \twoheadrightarrow A = A$$

$$F \otimes_R L \hookleftarrow L \twoheadrightarrow A \otimes_R L \twoheadrightarrow M$$

$$\Gamma_F(F \otimes_R L) \hookleftarrow \Gamma_R(L) \twoheadrightarrow \Gamma_A(A \otimes_R L) \twoheadrightarrow \Gamma_A(M)$$

Algèbre à puissances divisées : construction

1. L'idéal d'augmentation de l'algèbre à puissances divisées $\Gamma_F(F \otimes L)$ possède des puissances divisées ($\mathbf{Q}$-algèbre).
2. En utilisant la liberté de $\Gamma_R(L)$, on voit que c'est une sous-algèbre de $\Gamma_F(F \otimes L)$; les puissances divisées de cette dernière se restreignent en une structure de puissances divisées sur l'idéal d'augmentation de $\Gamma_R(L)$.
3. Elle fournit, par passage au quotient, une structure de puissances divisées sur l'idéal d'augmentation de $\Gamma_A(A \otimes L)$.
4. On vérifie que le noyau de l'homomorphisme surjectif $\Gamma_R(A \otimes_R L) \to \Gamma_A(M)$ est stable par les puissances divisées, d'où, par quotient, la structure voulue sur $\Gamma_A(M)$.

Perspectives

- Adjonction à `mathlib` des résultats déjà prouvés.
- Nous avons formalisé la construction des puissances divisées *modulo* les résultats de Roby sur la structure de l'algèbre à puissances divisées.
- La formalisation de ces résultats requiert de formaliser à peu près toute la première partie de l'article (Roby, 1963).
- Nous avons commencé à formaliser la construction de l'enveloppe à puissances divisées et sa propriété universelle.
- Une application sera la définition de l'anneau de Fontaine $\mathbf{A}_{\text{cris}}$ des périodes cristallines, avec en vue la définition des représentations galoisiennes cristallines et leurs propriétés.

Bibliographie

P. Berthelot (1974). *Cohomologie cristalline des schémas de caractéristique $p > 0$*. Lecture Notes in Mathematics **407**. Springer-Verlag

H. Cartan (1954). « Puissances divisées ». Séminaire Henri Cartan **7**, exposé 3

A. Grothendieck (1968). « Crystals and the de Rham cohomology of schemes ». In *Dix exposés sur la cohomologie des schémas*. Adv. Stud. in pure Math. North-Holland

N. Roby (1963). « Lois polynomes et lois formelles en théorie des modules ». *Annales scientifiques de l'École Normale Supérieure* **80** (3), p. 213-348

— (1965). « Les algèbres à puissances divisées ». *Bulletin des Sciences Mathématiques*. Deuxième Série **89**, p. 75-91

— (1968). « Construction de certaines algèbres à puissances divisées ». *Bulletin de la Société Mathématique de France* **96**, p. 97-113