Lambda-Divided Power Hopf Algebras

Nigel Byott

University of Exeter, UK

Omaha, 26 May 2017

Joint work with Griff Elder and Alan Koch

The (standard) divided power Hopf algebra

The **divided power Hopf algebra** A over a commutative ring R has basis $(a_n)_{n \geq 0}$ where

$$a_m a_n = \binom{m+n}{m} a_{m+n} \quad (\text{so } a_0 = 1);$$

$$\Delta(a_n) = \sum_{j=0}^{n} a_j \otimes a_{n-j};$$

$$\epsilon(a_n) = \delta_{n0}; \qquad S(a_n) = (-1)^n a_n.$$

This acts on the polynomial ring $R[X]$ by

$$a_m \cdot X^k = \binom{k}{m} X^{k-m},$$

making $R[X]$ into an A-module algebra.

$$\left(\text{Think of } a_m \text{ as } \frac{1}{m!} \, \frac{d^m}{dX^m} . \right)$$

Remarks:

(1) “Basis” means “algebraic basis”: each element of A is a **finite** R-linear combination of the a_m.

(2) If R has characteristic p (prime) then $(a_n)_{n<p^m}$ span a sub-Hopf algebra of A, which is free of rank p^m as an R-module.
In the preprint

[BCE] Nigel Byott, Lindsay Childs, Griff Elder:
Scaffolds and Generalized Integral Galois Modules Structure
[arXiv:1308.2088v3]

we used **scaffolds** in such Hopf algebras (with R a local field of characteristic p) to investigate “Galois module structure” in inseparable field extensions.

The λ-divided power Hopf algebra

In the paper

> [AGKO] George Andrews, Li Guo, William Keigher, Ken Ono: *Baxter Algebras and Hopf Algebras,* (Trans. A.M.S, 2003)

the authors define the λ-**divided power Hopf algebra** $\mathcal{A}_\lambda$ for $\lambda \in R$. This has basis $(a_n)_{n \geq 0}$ where

$$a_m a_n = \sum_{k=0}^{m} \lambda^k \binom{m+n-k}{m} \binom{m}{k} a_{m+n-k};$$

$$\Delta(a_n) = \sum_{k=0}^{n} \sum_{i=0}^{n-k} (-\lambda)^k a_i \otimes a_{n-k-i} \in A \otimes_R A;$$

$$\epsilon(a_n) = \begin{cases} 1 & \text{if } n = 0, \\ \lambda & \text{if } n = 1, ; \\ 0 & \text{if } n \geq 2; \end{cases} \qquad S(a_n) = (-1)^n \sum_{v=0}^{n} \binom{n-3}{n-v} \lambda^{n-v} a_v.$$

Taking $\lambda = 0$ gives the usual divided power Hopf algebra.

The λ-divided power Hopf algebra

In [AGKO], the Hopf algebra axioms are shown to hold by a combination of routine verification and clever manipulations of non-obvious identities involving binomial coefficients.

The algebra structure of $\mathcal{A}_\lambda$ is explained by previous work of Keigher and Guo on Baxter algebras, but no motivation is given for the formulae defining Δ, ϵ and S.

The authors also investigate when $\mathcal{A}_\lambda \cong \mathcal{A}_\nu$ (but get it wrong!)

The aim of this talk is to explain what $\mathcal{A}_\lambda$ really is, and what it is good for.

One-dimensional formal groups

A (one-dimensional) **formal group** over an arbitrary commutative ring R is a formal power series $F(X,Y) \in R[[X,Y]]$ such that

$$F(X,0) = X; \qquad F(0,Y) = Y;$$

$$F(X,F(Y,Z)) = F(F(X,Y),Z);$$

$$F(X,Y) \equiv X + Y \text{ mod deg } 2.$$

Then there is a unique series $i(X) \in R[[X]]$ with

$$F(X,i(X)) = 0 = F(i(X),X).$$

We can make the set $XR[[X]]$ into a group with the operation $+_F$ where

$$a(X) +_F b(X) = F(a(X),b(X)).$$

A **homomorphism** $h : F \to G$ of formal groups is a power series $h(X) \in R[[X]]$ such that

$$h(0) = 0 \text{ and } h(F(X,Y)) = G(h(X),h(Y)).$$

One-dimensional formal groups

A formal group F gives the ring $R[[X]]$ the structure of a **topological** Hopf algebra with

$$\Delta(X) \mapsto F(Y,Z) \in R[[Y,Z]] = R[[X]] \widehat{\otimes} R[[X]]$$

(where $Y = X \otimes 1$, $Z = 1 \otimes X$);

$$\epsilon(X) = 0, \qquad S(X) = -X.$$

Note that Δ takes values in the **completed** tensor product $R[[X]] \widehat{\otimes} R[[X]]$ (not just in $R[[X]] \otimes R[[X]]$), and Δ, ϵ, S are **continuous** R-algebra homomorphisms (i.e. they respect infinite sums).

Polynomial formal groups

We say a formal group $F(X, Y)$ is a **polynomial formal group** if

$$F(X, Y) \in R[X, Y].$$

This can only happen if

$$F(X, Y) = F_\lambda(X, Y) := X + Y + \lambda XY \text{ for some } \lambda \in R.$$

Examples: $\lambda = 0$ gives the additive formal group

$$F_0(X, Y) = X + Y.$$

$\lambda = 1$ gives the multiplicative formal group

$$F_1(X, Y) = X + Y + XY = (1 + X)(1 + Y) - 1.$$

For F_λ, the inverse is

$$i(X) = -X(1 + \lambda X)^{-1} = \sum_{n=1}^{\infty} (-1)^n \lambda^{n-1} X^n$$

which is (usually) not in $R[X]$. So we need to work with $R[[X]]$ (not just $R[X]$) even for polynomial formal groups.

The topology on $R[[X]]$

The power series ring $R[[X]]$ comes equipped with a topology: the ideals $X^n R[[X]]$ are a basis of neighbourhoods of 0 (so R itself has the discrete topology).

This is precisely the topology in which all infinite sums of the form

$$\sum_{n=0}^{\infty} r_n X^n, \qquad r_n \in R$$

converge.

Thus the monomials $(X^n)_{n \geq 0}$ are a **topological basis** for $R[[X]]$ (infinite sums allowed!)

Duality

Now consider topological R-modules M of the following special type:

- either M has a countably infinite topological basis m_0, m_1, m_2, ...,

  $$\text{i.e.} \qquad M = \left\{ \sum_{n=0}^{\infty} r_n m_m \ : \ r_n \in R \right\}$$

  where all these sums converge and the submodules

  $$M_k = \left\{ \sum_{j=k}^{\infty} r_j m_j : r_j \in R \right\}$$

  for $k \geq 0$ form a basis of neighbourhoods of 0.

- or M is free on a finite basis $m_1, \ldots, m_n$ (and has the discrete topology).

Duality

Examples:
(1) $R[[X]]$ with topological basis 1, X, X^2, $\ldots$;
(2) $R[[Y,Z]]$ with topological basis 1, Y, Z, Y^2, YZ, Z^2, $\ldots$;
(3) R itself.

Define the **continuous dual** of M to be

$$M^* = \mathrm{Hom}_{R-\mathrm{cts}}(M, R),$$

the module of continuous R-module homomorphisms from M to R.

As R has the discrete topology, continuity means that for $f : M \to R$ we have

$$f \in M^* \Leftrightarrow f(m_k) = 0 \text{ for all but finitely many } k.$$

(In particular, if M has a finite basis then M^* is the usual R-linear dual.)

Duality

Define $e_j \in M^*$ by

$$e_j(m_k) = \delta_{jk}.$$

Then the e_j form an *algebraic* basis of M^*: we have

$$M = \prod_{j \geq 0} Rm_j \text{ and } M^* = \bigoplus_{j \geq 0} Re_j.$$

The duality functor is contravariant and fully faithful: the obvious map

$$\mathrm{Hom}_{R-\mathrm{cts}}(M, N) \to \mathrm{Hom}_R(N^*, M^*), \qquad g \mapsto g^*$$

is bijective.

Back to polynomial formal groups

The polynomial formal group

$$F_\lambda(X, Y) = X + Y + \lambda XY$$

makes $R[[X]]$ into a topological Hopf algebra H_λ, with

$$\Delta(X^r) = F_\lambda(Y, Z)^r = \sum_{i=0}^{r} \sum_{j=0}^{r-i} \lambda^{r-i-j} \binom{r}{j} \binom{r-i}{j} Y^{r-i} Z^{r-j}.$$

Let

$$A_\lambda = H_\lambda^*$$

be the continuous dual of H_λ. Then A_λ has an (algebraic) basis $(e_j)_{n \geq 0}$ dual to the topological basis $(X^j)_{j \geq 0}$ of H_λ.

The multiplication (resp. comultiplication) on H_λ induces a comultiplication (resp. multiplication) on A_λ. Thus A_λ becomes a Hopf algebra (not a topological one!)

Operations on the dual A_λ of H_λ

It is a routine calculation to express the Hopf algebra operations on A_λ in terms of the basis elements e_n.

$$e_n e_m = \sum_{k=0}^{m+n} \lambda^k \binom{m+n-k}{m} \binom{m}{k} e_{m+n-k}.$$

$$\Delta(e_n) = \sum_{i=0}^{n} e_i \otimes e_{n-i}, \qquad \epsilon(e_n) = \delta_{n0},$$

$$S(e_n) = (-1)^n \sum_{r=0}^{n} \lambda^{n-r} \binom{n-1}{n-r} e_r.$$

Taking $\lambda = 0$ gives usual divided power Hopf algebra.

The algebra structure on our Hopf algebra A_λ is the same as for the λ-divided power Hopf algebra $\mathcal{A}_\lambda$ (replacing a_j by e_j). However, the formulae for the comultiplication/counit/antipode are different . . .

. . . because [AGKO] uses the wrong basis!

Operations on the dual A_λ of H_λ

Consider the map $\theta : H_\lambda \to H_\lambda$ given by $\theta(f(X)) = (1+\lambda X)f(X)$.

This is a coalgebra homomorphism since

$$(1+\lambda Y)(1+\lambda Z) = 1 + \lambda(Y + Z + \lambda YZ) = 1 + \lambda F(Y, Z).$$

Dualising gives an algebra homomorphism $\theta^* : A_\lambda \to A_\lambda$, so changing to the basis

$$a_n = \theta^*(e_n) = \begin{cases} e_0 & \text{if } n = 0, \\ \lambda e_{n-1} + e_n & \text{if } n \geq 0, \end{cases}$$

does not change the formula for multiplication in A_λ.
But it changes the formulae for comultiplication/counit/antipode to those in [AGKO].
So we have proved

Theorem: Over any commutative ring R, the λ-divided power Hopf algebra $\mathcal{A}_\lambda$ constructed in [AGKO] is just the continuous dual of the formal Hopf algebra H_λ associated to the polynomial formal group F_λ.

Isomorphisms

"Theorem" [AGKO]: Suppose that R is a $\mathbb{Q}$-algebra. Then

$$\mathcal{A}_\lambda \cong \mathcal{A}_\nu \Leftrightarrow R\lambda = R\nu.$$

Disproof: Over a $\mathbb{Q}$-algebra, *any* one-dimensional formal group is isomorphic to the additive formal group via its logarithm. So we *always* have $\mathcal{A}_\lambda \cong \mathcal{A}_\nu$. □

In fact we have

Theorem:
(i) [AGKO] Over any R, if $R\lambda = R\nu$ then $\mathcal{A}_\lambda \cong \mathcal{A}_\nu$.
(ii) If R has characteristic p (prime), then

$$\mathcal{A}_\lambda \cong \mathcal{A}_\nu \Leftrightarrow \lambda^{p-1} = \alpha^{p-1}\nu^{p-1} \text{ for some } \alpha \in R^\times.$$

In particular, if R is an integral domain of characteristic p then

$$\mathcal{A}_\lambda \cong \mathcal{A}_\nu \Leftrightarrow \lambda R = \nu R.$$

Proof: Check when there is an isomorphism $F_\lambda \cong F_\nu$ of formal groups.

Actions and coactions

The formal Hopf algebra H_λ is a right (formal) comodule algebra over itself via comultiplication.

Relabel one copy of $R_\lambda[[X]]$ as $R[[[Z]]$. We have

$$R[[Z]] \to R[[Z]] \widehat{\otimes}_R H_\lambda, \qquad Z \mapsto F_\lambda(Z, X).$$

By the usual duality considerations, this makes $R[[Z]]$ into a left A_λ-module algebra, with action

$$e_n \cdot Z^r = \binom{r}{n} Z^{r-n}(1+\lambda Z)^n.$$

This also makes the polynomial ring $R[Z]$ into a left A_λ-module algebra.

Truncations

Now let R have characteristic p, let $m \geq 1$, and set

$$A_{\lambda,m} = \bigoplus_{n<p^m} R \cdot e_n.$$

Then $A_{\lambda,m}$ is sub-Hopf algebra of A_λ which is free of rank p^m over R.

$A_{\lambda,m}$ represents the finite affine group scheme $\mathcal{G}_{\lambda,m}$ which is the kernel of the homomorphism of formal groups

$$F_\lambda \to F_{\lambda^{p^m}}, \qquad X \mapsto X^{p^m}$$

and is dual to the Hopf algebra

$$H_{\lambda,m} = \frac{R[[X]]}{(X^{p^m})}, \qquad \Delta(x) = F_\lambda(x \otimes 1, 1 \otimes x)$$

where $x = X + (X^{p^m})$.

Two arithmetic applications: (1)

Now suppose that R is a PID of characteristic p.

Following work of David Moss, we can construct principal homogeneous spaces over $\mathcal{G}_{\lambda,m}$ as follows.

Pick $c \in R$ and let

$$S_c = \frac{R[[Z]]}{(Z^{p^m} - c)}.$$

Then S_c is a comodule algebra over $H_{\lambda,m}$ with

$$z \mapsto F_\lambda(z, x),$$

where $z = Z + (Z^{p^m} - c)$.

Two arithmetic applications: (1)

Proposition: S_c is a principal homogenous space over $\mathcal{G}_{\lambda,m}$ if and only if $1 + \lambda^{p^m} c \in R^\times$.

Each such S_c is then free as an $A_{\lambda,m}$-module.

However, if S_c is an integral domain (i.e. if $Z^{p^m} - c$ is irreducible over the field of fractions of R) then S_c is in general not integrally closed in its field of fractions.

Question: If R is a PID of characteristic p, does *every* principal homogeneous space over $\mathcal{G}_{\lambda,m}$ arise this way?

(Moss proves a result of this type over finite extensions of $\mathbb{Z}_p$ using sheaf cohomology.)

Two arithmetic applications: (2)

Now let $K = k((T))$, where k is some field of characteristic p.

Let L be a purely inseparable and totally ramified extension of K of degree p^m. Let x be a uniformising parameter. Then

$$L = K(x) \text{ with } x^{p^m} \in K, \quad x^{p^{m-1}} \notin K.$$

Choose an integer $b > 0$ with $p \nmid b$, and let $y = x^b$. Then $v_L(y) = b$ and we also have $L = K[y]$.

Two arithmetic applications: (2)

Up to isomorphism, there are two possible λ-divided power Hopf algebras over K, with $\lambda = 0$ and $\lambda = 1$.

In either case, we can form the truncated λ-divided power Hopf algebra $A_{\lambda,m}$ and make it act on L in many ways.
We choose the action with

$$e_n \cdot y^r = \binom{r}{n} y^{r-n}(1+\lambda y)^n.$$

This gives L an $A_{\lambda,m}$ Hopf-Galois structure, which depends on the choice of y (and hence of b).

For $0 \leq i \leq m-1$, define $\Psi_{m-i} = e_{p^i}$.

Two arithmetic applications: (2)

Write

$$r = r_0 + pr_1 + \cdots p^{m-1} r_{m-1} \text{ with } 0 \le r_0, \ldots, r_{m-1} \le p-1,$$

When $\lambda = 0$, we have

$$\Psi_{m-i} \cdot y^r = \binom{r}{p^i} y^{r-p^i}(1 + \lambda^{p^i} y^{p^i}) = \begin{cases} u_{i,r} y^{r-p^i} & \text{if } r_i \neq 0 \\ 0 & \text{otherwise,} \end{cases}$$

where $u_{i,r} \in \mathbb{F}_p^\times$. In this case, we get a scaffold with infinite precision and with (unique) shift parameter $-b$. This is the same situation as in [BCE] (but described in a different way).

Two arithmetic applications: (2)

When $\lambda = 1$, we have

$$\Psi_{m-i} \cdot y^r = \begin{cases} u_{i,r}(y^{r-p^i} + y^r) & \text{if } r_i \neq 0 \\ 0 & \text{otherwise,} \end{cases}$$

We now get an "error term" y^r with valuation $p^i b$ more than the "main term". This gives a new example of a scaffold, with shift parameter $-b$ and with precision b.

So, provided $b \geq 2p^m - 1$, [BCE] tells us, for example:

- if $m = 2$ then the valuation ring $\mathfrak{O}_L$ in L is free over its associated order in $A_{\lambda,m} = A_{1,2}$ if and only if $(-b \bmod p^2)$ divides $p^2 - 1$;
- if $-b \equiv 1 \pmod{p^m}$ then, writing $\mathfrak{P}$ for the maximal ideal in $\mathfrak{O}_L$,

$$\mathfrak{P}^j \text{ is free over its associated order in } A_{1,m}$$

$$\Leftrightarrow j \equiv 1, 0, -1, \ldots, \left\lfloor \frac{2 - p^m}{2} \right\rfloor \pmod{p^m}.$$