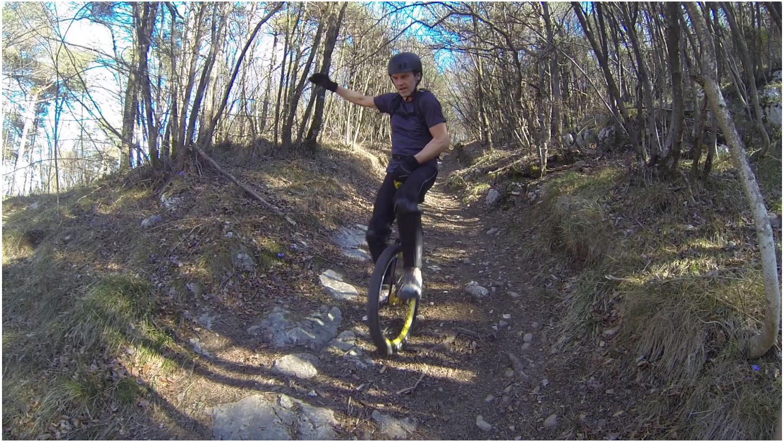
Exponentials of derivations in prime characteristic

Sandro Mattarei

University of Lincoln

Bath, February 2016

Taking a break from maths:



Summary

1. Traditional exponentials in characteristic zero
2. Truncated exponentials
3. Application to gradings of algebras
4. Artin-Hasse exponentials
5. Laguerre polynomials

Derivations and automorphisms

Let A be a non-associative algebra over a field F.

- A derivation of A is a linear map $D : A \to A$ such that

$$D(a \cdot b) = (Da) \cdot b + a \cdot (Db), \quad \text{for } a, b \in A.$$

Lemma

Assume $\operatorname{char}(F) = 0$. *If D is a nilpotent derivation of A, then* $\exp D = \sum_{k=0}^{\infty} D^k/k!$ *is an automorphism of A.*

- D being a derivation is equivalent to

$$D \circ m = m \circ (D \otimes \mathrm{id} + \mathrm{id} \otimes D),$$

where $m : A \otimes A \to A$ is the multiplication map.
- The Lemma follows from

$$\exp(X + Y) = \exp(X) \cdot \exp(Y)$$

after setting $X = D \otimes \mathrm{id}$ and $Y = \mathrm{id} \otimes D$.

Proof of the Lemma

Proof.

Because
$$D^k \circ m = m \circ (D \otimes \mathrm{id} + \mathrm{id} \otimes D)^k$$
for $k \geq 0$, we have

$$\begin{aligned}(\exp D) \circ m &= m \circ \exp(D \otimes \mathrm{id} + \mathrm{id} \otimes D) \\ &= m \circ \exp(D \otimes \mathrm{id}) \circ \exp(\mathrm{id} \otimes D) \\ &= m \circ \big((\exp D) \otimes \mathrm{id}\big) \circ \big(\mathrm{id} \otimes (\exp D)\big)\end{aligned}$$

Evaluating on $x \otimes y$, for $x, y \in A$, we get

$$(\exp D)(x \cdot y) = (\exp D)(x) \cdot (\exp D)(y)$$

and hence $\exp D$ is an automorphism of A. □

Example: A polynomial algebra

Example

Let $A = F[X]$, $D = d/dX$, $\alpha, \beta \in F$. Then

- $\exp(\beta D) f(X) = f(X + \beta)$ (Taylor's formula);
- $\exp(\alpha X D) f(X) = f(e^\alpha X)$ (if e^α makes sense).

- In fact, all automorphisms of $F[X]$ as an F-algebra are given by substitutions $X \mapsto aX + b$, for $a \in F^*$, $b \in F$.
- The derivation algebra is much larger,

$$W_1 = \mathrm{Der}(F[X]) = \bigoplus_{k \geq -1} \mathrm{Der}(F[X])_k = \bigoplus_{k \geq -1} F \cdot X^{k+1} D,$$

but exp does not apply to derivations of positive degree.

Example: The Lie algebra W_1

- $W_1 = \mathrm{Der}(F[X])$ is the Lie algebra *of polynomial vector fields on the line* (usually with $F = \mathbb{R}$ or $\mathbb{C}$).
- W_1 has a $\mathbb{Z}$-graded basis given by the $X^{i+1}D$, where $D = d/dX$, this element having degree i, for $i \geq -1$.
- Lie bracket:

$$[X^{i+1}D, X^{j+1}D] = (j-i)X^{i+j+1}D.$$

In particular, consider the inner derivation $\operatorname{ad} D = [D, \cdot]$.

Example

Lie algebra $W_1 = \mathrm{Der}(F[X])$.
Then $\exp(\operatorname{ad} D)$ is an automorphism of W_1. Explicitly:

$$\exp(\operatorname{ad} D)X^{i+1}D = (X+1)^{i+1}D$$

Exponentials in positive characteristic

From now on assume $\mathrm{char}(F) = p > 0$.

- For $\exp(D)$ to make sense we need at least $D^p = 0$, but then what we really apply is the *truncated exponential*

$$E(D) = \sum_{k=0}^{p-1} D^k/k!$$

- This is defined for any derivation D but it *need not* be an automorphism, even when $D^p = 0$.
- In the theory of modular Lie algebras, this is *good*: certain $E(D)$ can be used to pass from some torus to another torus with more desirable properties (*toral switching:* [Winter 1969], [Block-Wilson 1982], [Premet 1986/89]).

What fails with the truncated exponential

We compute $E(X) \cdot E(Y)$,

$$
\begin{array}{ccccccc}
1 & Y & \frac{Y^2}{2!} & \frac{Y^3}{3!} & \cdots & \cdots & \frac{Y^{p-1}}{(p-1)!} \\
X & XY & \frac{XY^2}{2!} & & & \frac{XY^{p-2}}{(p-2)!} & \frac{XY^{p-1}}{(p-1)!} \\
\frac{X^2}{2!} & \frac{X^2Y}{2!} & & & \frac{X^2Y^{p-3}}{2!(p-3)!} & \frac{X^2Y^{p-2}}{2!(p-2)!} & \frac{X^2Y^{p-1}}{2!(p-1)!} \\
\frac{X^3}{3!} & & & & & & \vdots \\
\vdots & & \frac{X^{p-3}Y^2}{(p-3)!2!} & & & & \\
\vdots & \frac{X^{p-2}Y}{(p-2)!} & \frac{X^{p-2}Y^2}{(p-2)!2!} & & & & \vdots \\
\frac{X^{p-1}}{(p-1)!} & \frac{X^{p-1}Y}{(p-1)!} & \frac{X^{p-1}Y^2}{(p-1)!2!} & \cdots & & \cdots & \frac{X^{p-1}Y^{p-1}}{(p-1)!(p-1)!}
\end{array}
$$

and find

$$E(X) \cdot E(Y) - E(X+Y) = \sum_{k=p}^{2p-2} \sum_{i=k+1-p}^{p-1} \frac{X^i Y^{k-i}}{i!(k-i)!}.$$

A closer look at the term of degree p

- The term with $k = p$ in $E(X) \cdot E(Y) - E(X+Y)$ is

$$\frac{1}{p!}\sum_{i=1}^{p-1}\binom{p}{i}X^iY^{p-i} = \frac{(X+Y)^p - X^p - Y^p}{p!}.$$

- Modulo p it can also be written as

$$\sum_{i=1}^{p-1}\frac{(-1)^i}{i}X^iY^{p-i}.$$

The obstruction formula

- Setting $X = D \otimes \mathrm{id}$ and $Y = \mathrm{id} \otimes D$ yields the *obstruction formula*

$$E(D)x \cdot E(D)y - E(D)(xy) = \sum_{k=p}^{2p-2} \sum_{i=k+1-p}^{p-1} \frac{(D^i x)(D^{k-i} y)}{i!(k-i)!},$$

  for D any derivation of A, and $x, y \in A$.
- In particular, if p is odd and $D^{(p+1)/2} = 0$, then $E(D)$ is an automorphism of A.

Example: A truncated polynomial ring

Example

If $A = F[X]/(X^p)$ and $D = d/dX$, then $D^p = 0$, and

$$E(D)X^k = (X+1)^k \qquad \text{for } 0 \leq k < p.$$

Here $X^p = 0$, but $(X+1)^p = 1$, and hence $E(D)$ *is not* an automorphism of A.

- However,

$$A = F1 \oplus FX \oplus \cdots \oplus FX^{p-1}$$

is a $\mathbb{Z}$-grading of A, and $E(D)$ maps it to

$$A = F1 \oplus F(X+1) \oplus \cdots \oplus F(X+1)^{p-1},$$

which is a (*genuine*) $\mathbb{Z}/p\mathbb{Z}$-grading of A.

Why did $E(D)$ turn a grading into another?

Lemma

If D is a derivation of A with $D^p = 0$, for $x, y \in A$ we have

$$E(D)x \cdot E(D)y - E(D)(xy) = E(D) \sum_{i=1}^{p-1} \frac{(-1)^i}{i} (D^i x)(D^{p-i} y).$$

- The sum at the RHS equals the term with $k = p$ of the obstruction formula. That is the *primary obstruction cocycle*

$$\mathrm{Sq}_p(D) = \sum_{i=1}^{p-1} \frac{D^i}{i!} \smile \frac{D^{p-i}}{(p-i)!} \in Z^2(A, A)$$

which arises in Gerstenhaber's *deformation theory*.

Truncated exponentials and gradings

Theorem (grading switching with $D^p = 0$)

- *Let $A = \bigoplus_k A_k$ be a $\mathbb{Z}/m\mathbb{Z}$-grading of A;*
- *let D be a derivation of A, homogeneous of degree d, with $m \mid pd$, such that $D^p = 0$.*

Then

$$A = \bigoplus_k E(D)A_k$$

is a $\mathbb{Z}/m\mathbb{Z}$-grading of A.

- In our example with $A = F[X]/(X^p)$, its derivation $D = d/dX$ had degree -1, and A was graded over $\mathbb{Z}$, but then also over $\mathbb{Z}/m\mathbb{Z}$ with $m = p$.
- Less trivial application: construction of gradings over a group having elements of order p^2.

Two basic methods to produce gradings

- If $D \in \mathrm{Der}(A)$ and $$A_\alpha = \bigcup_{i>0} \ker\big((D - \alpha \cdot \mathrm{id})^i\big),$$ then $A = \bigoplus_{\alpha \in F} A_\alpha$ is a grading over the *additive* group of F (or a subgroup).
- With $\psi \in \mathrm{Aut}(A)$ in place of D we get a grading $A = \bigoplus_{\alpha \in F^*} A_\alpha$ over the *multiplicative* group of F.
- Combining the two methods one can get gradings over any f.g. abelian group with no elements of order p^2.
- These methods alone are unable to produce *genuine* $\mathbb{Z}/p^s\mathbb{Z}$-gradings with $s > 1$, which do occur in practice.
- *'genuine'* means that the grading does not simply come from a $\mathbb{Z}/m\mathbb{Z}$-grading with $m = 0$ or a larger power of p by viewing the degrees modulo p^s.

Weakening the condition $D^p = 0$

- The Artin-Hasse exponential series

$$E_p(X) = \exp\left(X + \frac{X^p}{p} + \frac{X^{p^2}}{p^2} + \cdots\right) = \prod_{i=0}^{\infty} \exp\left(\frac{X^{p^i}}{p^i}\right)$$

has coefficients in the (rational) p-adic integers.
- For example, the term of degree p is $\frac{(p-1)!+1}{p!}X^p$.

Lemma

There exist integers a_{ij}, with $a_{ij} = 0$ if $p \nmid i+j$, such that for D a nilpotent derivation of A, and for $x, y \in A$, we have

$$E_p(D)x \cdot E_p(D)y - E_p(D)(xy) = E_p(D) \sum_{i,j>0} a_{ij} D^i x \cdot D^j y.$$

- Proof: $\boxed{E_p(X) \cdot E_p(Y) = E_p(X+Y) \cdot \left(1 + \sum a_{ij} X^i Y^j\right)}$.

Artin-Hasse exponentials and gradings

Theorem (grading switching for nilpotent D)

- *Let* $A = \bigoplus_k A_k$ *be a* $\mathbb{Z}/m\mathbb{Z}$*-grading of* A*;*
- *let* D *be a nilpotent derivation of* A*, homogeneous of degree* d*, with* $m \mid pd$*.*

Then

$$A = \bigoplus_k E_p(D) A_k$$

is a $\mathbb{Z}/m\mathbb{Z}$*-grading of* A*.*

S. Mattarei
Artin-Hasse exponentials of derivations
J. Algebra **294** (2005), 1–18

Application: gradings of a Zassenhaus algebra

- $W(1:n) = \bigoplus_{i=-1}^{p^n-2} FE_i$, with

$$[E_i, E_j] = \left(\binom{i+j+1}{j} - \binom{i+j+1}{i}\right) E_{i+j}.$$

- Because $[E_{-1}, E_j] = E_{j-1}$ we have $(\operatorname{ad} E_{-1})^{p^n} = 0$.

Theorem

$W(1:n)$ has a genuine $\mathbb{Z}/p^r\mathbb{Z}$-grading, for each $1 \leq r \leq n$.

- Proof: Apply grading switching to $A = W(1:n)$ with the $\mathbb{Z}$-grading viewed modulo p^r, and $D = (\operatorname{ad} E_{-1})^{p^{r-1}}$. Then $E_p(D)$ maps that grading to a $\mathbb{Z}/p^r\mathbb{Z}$-grading.

Application: a grading of a Block algebra

Theorem (M. Avitabile and SM, 2005)

The simple Lie algebra $H(2;\mathbf{n};\Phi(\tau))^{(1)}$ has a grading over a finite cyclic group, for which

'the corresponding infinite dimensional loop algebra is a thin Lie algebra with certain properties.'

- The grading is produced from some known grading by applying the Artin-Hasse exponential of a derivation D which satisfies only $D^{2p} = 0$.

An approximate functional equation for $E_p(X)$

- If $F(X) \in 1 + X\mathbb{C}[[X]]$ satisfies $F(X+Y) = F(X)F(Y)$, then $F(X) = \exp(cX)$, for some $c \in \mathbb{C}$.
- Recall that $(E_p(X+Y))^{-1}E_p(X)E_p(Y)$ has only terms of total degree a multiple of p.

Theorem (SM, 2006)

Let $F(X) \in 1 + X\mathbb{F}_p[[X]]$, such that $(F(X+Y))^{-1}F(X)F(Y)$ has only terms of total degree a multiple of p. Then

$$F(X) = E_p(cX) \cdot G(X^p),$$

for some $c \in \mathbb{F}_p$ and $G(X) \in 1 + X\mathbb{F}_p[[X]]$, where $E_p(X)$ is the Artin-Hasse exponential.

Motivation

- What follows appears in

  M. Avitabile and S. Mattarei
  Laguerre polynomials of derivations
  Israel J. Math. **205** (2015), 109–126

- It finds one application (to *thin Lie algebras*) in

  M. Avitabile and S. Mattarei
  Nottingham Lie algebras with diamonds of finite and infinite type
  J. Lie Theory **24** (2014), 268–274

- There we need a cyclic grading of $H(2; \mathbf{n}; \Phi(1))$, an Albert-Zassenhaus algebra, obtained from a standard grading by grading switching with a derivation which is not nilpotent.

Laguerre polynomials

- The (generalized) Laguerre polynomial of degree $n \geq 0$ and parameter α is

$$L_n^{(\alpha)}(X) = \sum_{k=0}^{n} \binom{\alpha+n}{n-k} \frac{(-X)^k}{k!} \in \mathbb{Q}[\alpha, X].$$

- In the classical setting, $\alpha \in \mathbb{R}$ and > -1, and then

$$\int_0^\infty e^{-X} X^\alpha \cdot L_n^{(\alpha)}(X) L_m^{(\alpha)}(X)\, dX = 0 \qquad \text{iff } n \neq m.$$

- $Y = L_n^{(\alpha)}(X) \in \mathbb{R}[X]$ satisfies the differential equation

$$\boxed{XY'' + (\alpha + 1 - X)Y' + nY = 0.}$$

Laguerre polynomials modulo p

Letting p be a prime and $n = p - 1$, we find

$$L_{p-1}^{(\alpha)}(X) \equiv (1 - \alpha^{p-1}) \sum_{k=0}^{p-1} \frac{X^k}{(\alpha + k)(\alpha + k - 1) \cdots (\alpha + 1)}$$

modulo p, with its special case

$$L_{p-1}^{(0)}(X) \equiv E(X) = \sum_{k=0}^{p-1} X^k / k! \pmod{p}.$$

A modular differential equation for $L_{p-1}^{(\alpha)}(X)$

$$X\frac{d}{dX}L_{p-1}^{(\alpha)}(X) \equiv (X-\alpha)L_{p-1}^{(\alpha)}(X) + X^p - (\alpha^p - \alpha) \pmod p$$

- This is an analogue modulo p of the differential equation $\exp'(X) = \exp(X)$. For $\alpha = 0$ it reads

$$XE'(X) \equiv XE(X) + X^p \pmod p.$$

- Taking a further derivative we would get

$$XY'' + (\alpha + 1 - X)Y' - Y \equiv 0 \pmod p$$

for $Y = L_{p-1}^{(\alpha)}(X)$, which is the classical differential equation read modulo p.

A modular functional equation for $L_{p-1}^{(\alpha)}(X)$

Now we turn the differential equation into an analogue of the functional equation $\exp(X) \cdot \exp(Y) = \exp(X + Y)$.

Theorem

Let α, β, X, Y be indeterminates, and consider the subring $R = \mathbb{F}_p[\alpha, \beta, ((\alpha + \beta)^{p-1} - 1)^{-1}]$ of $\mathbb{F}_p(\alpha, \beta)$. Then there exists rational expressions $c_i(\alpha, \beta) \in R$ such that

$$L_{p-1}^{(\alpha)}(X) L_{p-1}^{(\beta)}(Y) \equiv L_{p-1}^{(\alpha+\beta)}(X + Y) \cdot \\ \cdot \left(c_0(\alpha, \beta) + \sum_{i=1}^{p-1} c_i(\alpha, \beta) X^i Y^{p-i} \right)$$

in $R[X, Y]$, modulo the ideal generated by $X^p - (\alpha^p - \alpha)$ and $Y^p - (\beta^p - \beta)$.

Laguerre polynomials and gradings (a model special case)

Theorem (grading switching with $D^{p^2} = D^p$)

- *Let* $A = \bigoplus_k A_k$ *be a* $\mathbb{Z}/m\mathbb{Z}$*-grading of* A*;*
- *let* $D \in \mathrm{Der}(A)$*, homogeneous of degree* d*, with* $m \mid pd$*, such that* $D^{p^2} = D^p$*;*
- *let* $A = \bigoplus_{a \in \mathbb{F}_p} A^{(a)}$ *be the decomposition of* A *into generalized eigenspaces for* D*;*
- *assuming* $\mathbb{F}_{p^p} \subseteq F$*, fix* $\gamma \in F$ *with* $\gamma^p - \gamma = 1$*;*
- *let* $\mathcal{L}_{\mathcal{D}} : A \to A$ *be the linear map on* A *whose restriction to* $A^{(a)}$ *coincides with* $L_{p-1}^{(a\gamma)}(D)$*.*

Then $A = \bigoplus_k \mathcal{L}_{\mathcal{D}}(A_k)$ *is a* $\mathbb{Z}/m\mathbb{Z}$*-grading of* A*.*

Laguerre polynomials and gradings

Theorem (general grading switching)

- *Let* $A = \bigoplus_k A_k$ *be a* $\mathbb{Z}/m\mathbb{Z}$*-grading of* A*;*
- *let* $D \in \mathrm{Der}(A)$*, homogeneous of degree* d*, with* $m \mid pd$*, such that* D^{p^r} *is diagonalizable over* F*;*
- *let* $A = \bigoplus_{\rho \in \mathbb{F}} A^{(\rho)}$ *be the decomposition of* A *into generalized eigenspaces for* D*;*
- *assuming* F *large enough, there is a* p*-polynomial* $g(T) \in F[T]$*, such that* $g(D)^p - g(D) = D^{p^r}$*; set* $h(T) = \sum_{i=1}^{r-1} T^{p^i}$*;*
- *let* $\mathcal{L_D} : A \to A$ *be the linear map on* A *whose restriction to* $A^{(\rho)}$ *coincides with* $L_{p-1}^{((g(\rho)-h(D))}(D)$*.*

Then $A = \bigoplus_k \mathcal{L_D}(A_k)$ *is a* $\mathbb{Z}/m\mathbb{Z}$*-grading of* A*.*

Comparison with toral switching

- On the subalgebra $A^{(0)}$ the map $\mathcal{L}_{\mathcal{D}}$ coincides with (a variation of) the Artin-Hasse exponential.
- When specialising to the toral switching setting we recover the formulas used there to map the old root spaces to the new ones.
- Toral switching
  - applies some $E(\operatorname{ad} x)$ to a torus T to get a new torus (as the maximal torus in the centralizer of $E(\operatorname{ad} x)T$),
  - and leaves to that the job of recovering the whole grading as a root space decomposition;
  - hence the grading group has exponent p.
- Grading switching
  - produces the whole grading at the same time (over a cyclic group, but this is not restrictive);
  - applies to nonassociative algebras;
  - is not restricted to gradings over groups of exponent p.