THE BAKER-CAMPBELL-HAUSDORFF FORMULA

DEFORMATION THEORY 2011-12; M. M.

1. Review of terminology about algebras

Let R be a commutative ring, by a nonassociative (= not necessarily associative) R-algebra we mean a R-module M endowed with a R-bilinear map $M \times M \to M$.

A nonassociative algebra M is called **unitary** if there exist a "unity" $1 \in M$ such that $1m = m1 = m$ for every $m \in M$. A **left ideal** (resp.: **right ideal**) of M is a submodule $I \subset M$ such that $MI \subset I$ (resp.: $IM \subset I$). A submodule is called an **ideal** if it is both a left and right ideal. A homomorphism of R-modules $d\colon M \to M$ is called a **derivation** if satisfies the Leibnitz rule $d(ab) = d(a)b + ad(b)$. A derivation d is called a **differential** if $d^2 = d \circ d = 0$. A R-algebra M is **associative** if $(ab)c = a(bc)$ for every $a, b, c \in M$. Unless otherwise specified, we reserve the simple term **algebra** only to associative algebra.

For every associative $\mathbb{K}$-algebra R we denote by R_L the associated Lie algebra with bracket $[a, b] = ab - ba$; we have seen that the adjoint operator

$$\mathrm{ad} : : R_L \to \mathrm{End}(R), \qquad \mathrm{ad}\, x(y) = [x, y] = xy - yx,$$

is a morphism of Lie algebras. Notice that if $I \subset R$ is an ideal then I is also a Lie ideal of R_L.

2. Exponential and logarithm

Let $\mathbb{K}$ be a field of characteristic 0, R a unitary associative $\mathbb{K}$-algebra and $I \subset R$ a nilpotent ideal. We may define the **exponential**

$$e\colon I \to 1 + I \subset R, \quad e^a = \sum_{n\geq 0} \frac{a^n}{n!},$$

and the invertible operator

$$e^{\mathrm{ad}\, a} = \sum_{n\geq 0} \frac{(\mathrm{ad}\, a)^n}{n!} \in \mathrm{End}(R).$$

For later use we also note that the operator

$$\frac{e^{\mathrm{ad}\, a} - 1}{\mathrm{ad}\, a} = \sum_{n\geq 0} \frac{(\mathrm{ad}\, a)^n}{(n+1)!} \in \mathrm{End}(R)$$

is still invertible: its inverse is

$$\frac{\mathrm{ad}\, a}{e^{\mathrm{ad}\, a} - 1} = \sum_{n\geq 0} \frac{B_n}{n!} (\mathrm{ad}\, a)^n,$$

where $B_0 = 1, B_1 = -1/2, B_2 = 1/6, B_3 = 0, \dots$ are the Bernoulli numbers.

We can also define the **logarithm**

$$\log\colon 1+I\to I,\quad \log(1+a)=\sum_{n=1}^{\infty}(-1)^{n-1}\frac{a^n}{n}.$$

Lemma 2.1. *Exponential and logarithm are one the inverse of the other, i.e. for every $a,b\in I$ we have*

$$\log(e^a)=a,\qquad e^{\log(1+b)}=1+b.$$

Proof. We may reduce to the classical theory by using the algebra morphism

$$\mathbb{Q}[[t]]\to R,\qquad p(t)\mapsto p(a).$$

□

Proposition 2.2. *In the notation above:*

(1) *for every $a,b\in R$ and $n\ge 0$*

$$(\operatorname{ad} a)^n b=\sum_{i=0}^{n}(-1)^i\binom{n}{i}a^{n-i}ba^i=\sum_{i=0}^{n}\binom{n}{i}a^{n-i}b(-a)^i.$$

(2) *If a is nilpotent in R then also $\operatorname{ad} a$ is nilpotent in $\operatorname{End}(R)$.*

(3) *For every $a\in I$ and $b\in R$*

$$e^{\operatorname{ad} a}b:=\sum_{n\ge 0}\frac{(\operatorname{ad} a)^n}{n!}b=e^a b e^{-a}.$$

(4) *For every $a\in I$ and $b\in R$ we have $ab=ba$ if and only if $e^a b=be^a$.*

(5) *For every $a,b\in I$ we have $e^a b=be^a$ if and only if $e^a e^b=e^b e^a$.*

(6) *Given $a,b\in I$ such that $ab=ba$, then*

$$e^{a+b}=e^a e^b=e^b e^a,\qquad \log((1+a)(1+b))=\log(1+a)+\log(1+b).$$

Proof. [1] We have

$$(\operatorname{ad} a)^n b=a(\operatorname{ad} a)^{n-1}(b)-(\operatorname{ad} a)^{n-1}(b)a$$

By induction

$$(\operatorname{ad} a)^n b=\sum_{i=0}^{n-1}(-1)^i\binom{n-1}{i}a^{n-i}ba^i-\sum_{j=0}^{n-1}(-1)^j\binom{n-1}{i}a^{n-1-j}ba^{j+1}.$$

Setting $j=i-1$ on the second summand we get

$$(\operatorname{ad} a)^n b=\sum_{i=0}^{n-1}(-1)^i\binom{n-1}{i}a^{n-i}ba^i+\sum_{i=1}^{n}(-1)^i\binom{n-1}{i-1}a^{n-i}ba^i=$$

$$=\sum_{i=0}^{n}(-1)^i\left(\binom{n-1}{i}+\binom{n-1}{i-1}\right)a^{n-i}ba^i=\sum_{i=0}^{n}(-1)^i\binom{n}{i}a^{n-i}ba^i.$$

[2] If $a^n=0$ then $(\operatorname{ad} a)^{2n}=0$.

[3] Using item 1 we get

$$e^{\operatorname{ad} a}b:=\sum_{n\ge 0}\frac{(\operatorname{ad} a)^n}{n!}b=\sum_{n\ge 0}\sum_{i=0}^{n}\frac{1}{n!}\binom{n}{i}a^{n-i}b(-a)^i$$

Setting $j=n-i$ we get

$$e^{\operatorname{ad} a}b:=\sum_{i,j\ge 0}\frac{1}{i!j!}a^j b(-a)^i=e^a be^{-a}.$$

[4] We have $e^a b = b e^a$ if and only if $e^a b e^{-a} - b = 0$ and by the above formula

$$e^a b e^{-a} - b = e^{\operatorname{ad} a} b - b = \frac{e^{\operatorname{ad} a} - 1}{\operatorname{ad} a}([a, b]).$$

[5] Setting $x = e^b$ we have by item 4 applied twice

$$e^a e^b = e^b e^a \iff x e^a = e^a x \iff ax = xa \iff a e^b = e^b a \iff ab = ba.$$

[6] Since $ab = ba$ we have for every $n \geq 0$

$$(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i},$$

$$e^{a+b} = \sum_{n\geq 0} \frac{(a+b)^n}{n!} = \sum_{n\geq 0}\sum_{i=0}^{n} \frac{1}{n!}\binom{n}{i} a^i b^{n-i} = \sum_{n\geq 0}\sum_{i=0}^{n} \frac{1}{i!(n-i)!} a^i b^{n-i}.$$

Setting $j = n - i$ we get

$$e^{a+b} = \sum_{i,j\geq 0} \frac{1}{i!j!} a^i b^j = e^a e^b.$$

Setting $x = \log(1+a)$, $y = \log(1+b)$ we have $e^x e^y = e^y e^x$: therefore $xy = yx$ and

$$\log((1+a)(1+b)) = \log(e^x e^y) = \log(e^{x+y}) = x + y = \log(1+a) + y = \log(1+b).$$

□

Let t be an indeterminate and denote by $d\colon R[t] \to R[t]$, $d(a) = a'$, the derivation operator. Multiplication on the left give an injective morphism of algebras

$$\phi\colon R[t] \to \operatorname{End}(R[t], R[t]), \qquad \phi(a)b = ab$$

and Leibniz formula can be written as

$$\phi(a') = [d, \phi(a)], \qquad a \in R[t].$$

Given $a \in I[t]$ we have $\phi(e^a) = e^{\phi(a)}$ and

$$\phi((e^a)') = d e^{\phi(a)} - e^{\phi(a)} d$$

By the above proposition

$$-\phi((e^a)' e^{-a}) = e^{\phi(a)} d e^{-\phi(a)} - d = \frac{e^{\operatorname{ad}\phi(a)} - 1}{\operatorname{ad}\phi(a)}([\phi(a), d]) = -\frac{e^{\operatorname{ad}\phi(a)} - 1}{\operatorname{ad}\phi(a)}(\phi(a')),$$

and then, since ϕ is injective

$$(e^a)' e^{-a} = \frac{e^{\operatorname{ad} a} - 1}{\operatorname{ad} a}(a').$$

Now, let $a, b \in I$ and define

$$Z = \log(e^{ta} e^b) \in I[t].$$

We have $Z = Z_0 + tZ_1 + \cdots + t^n Z_n + \cdots$, with $Z_0 = b$ and $Z_n \in I^n$. By derivation formula we have

$$(e^Z)' e^{-Z} = \frac{e^{\operatorname{ad} Z} - 1}{\operatorname{ad} Z}(Z'),$$

$$(e^Z)' e^{-Z} = (e^{ta} e^b)' e^{-b} e^{-ta} = (e^{ta})' e^{-ta} = a.$$

Therefore Z is the solution of the Cauchy problem

$$Z' = \sum_{n\geq 0} \frac{B_n}{n!} (\operatorname{ad} Z)^n (a), \qquad Z(0) = Z_0 = b.$$

The coefficients Z_n can be computed recursively

$$Z_{r+1} = \frac{1}{r+1}\sum_{m\geq 0}\frac{B_m}{m!}\sum_{i_1+\cdots+i_m=r}(\operatorname{ad} Z_{i_1})(\operatorname{ad} Z_{i_2})\cdots(\operatorname{ad} Z_{i_m})a$$

Theorem 2.3. *Given $a, b \in I$ we have*

$$e^a e^b = e^{a\bullet b}, \quad \textit{where} \quad a\bullet b = \sum_{n\geq 0} Z_n,$$

and

$$Z_0 = b, \qquad Z_{r+1} = \frac{1}{r+1}\sum_{m\geq 0}\frac{B_m}{m!}\sum_{i_1+\cdots+i_m=r}(\operatorname{ad} Z_{i_1})(\operatorname{ad} Z_{i_2})\cdots(\operatorname{ad} Z_{i_m})a.$$

The first terms of the above series are

$$a\bullet b = a + b + \frac{1}{2}[a,b] + \frac{1}{12}[a,[a,b]] + \frac{1}{12}[b,[a,b]] + \cdots$$

Since $(e^a e^b)e^c = e^a(e^b e^c)$ the product $I\times I\xrightarrow{\bullet} I$ is associative. If L is a Lie subalgebra of I and $a, b \in L$, then $a\bullet b \in L$ and $a\bullet b - a - b$ belongs to the Lie ideal generated by $[a, b]$.

The formula of the theorem allow to define for every nilpotent Lie algebra L a map

$$L\times L\to L, \qquad (a,b)\mapsto a\bullet b$$

commuting with morphisms of Lie algebras. Notice that $-(a\bullet b) = (-b)\bullet(-a)$, $a\bullet(-a) = 0$ and, if $[a, b] = 0$ then $a\bullet b = a + b$.

If L is a Lie subalgebra of a nilpotent ideal of a unitary associative algebra R then

$$e^{a\bullet b} = e^a e^b.$$

We define $\exp(L) = \{e^a \mid a \in L\}$ as the set of formal exponents of elements of L and the "product"

$$\exp(L)\times\exp(L)\to\exp(L), \qquad e^a e^b = e^{a\bullet b}.$$

We will prove later, using free Lie algebras, that **every nilpotent Lie algebra is a quotient of a Lie algebra contained in a nilpotent ideal of an associative algebra.** This implies that $\bullet$ is always associative and gives a group structure on $\exp(L)$.

We have the functorial properties:

(1) If $f\colon L\to M$ is a morphism of nilpotent Lie algebras, then the map

$$f\colon \exp(L)\to\exp(M), \qquad f(e^a) = e^{f(a)},$$

is a homomorphism of groups.

(2) Let V be a vector space and $f\colon L\to \operatorname{End}(V)$ a Lie algebra morphism. If the image of L is contained in a nilpotent ideal, then the maps

$$\exp(L)\times V\to V, \qquad (e^a, v)\mapsto e^{f(a)}v,$$

$$\exp(L)\times\operatorname{End}(V)\to\operatorname{End}(V), \qquad (e^a, g)\mapsto e^{f(a)}ge^{-f(a)} = e^{\operatorname{ad} f}(g),$$

are right actions.