DERIVATIONS

Introduction to non-associative algebra

OR

Playing havoc with the product rule?

PART V—THE MEANING OF THE SECOND COHOMOLOGY GROUP

BERNARD RUSSO
University of California, Irvine

FULLERTON COLLEGE
DEPARTMENT OF MATHEMATICS
MATHEMATICS COLLOQUIUM
OCTOBER 25, 2012

HISTORY OF THESE LECTURES

PART I

ALGEBRAS

FEBRUARY 8, 2011

PART II

TRIPLE SYSTEMS

JULY 21, 2011

PART III

MODULES AND DERIVATIONS

FEBRUARY 28, 2012

PART IV

COHOMOLOGY OF ASSOCIATIVE ALGEBRAS

JULY 26, 2012

PART V

MEANING OF THE SECOND COHOMOLOGY GROUP

OCTOBER 25, 2012

OUTLINE OF TODAY'S TALK

1. SOME SET THEORY
(EQUIVALENCE CLASSES)

2. GROUPS AND THEIR QUOTIENT
GROUPS

3. DERIVATIONS ON ALGEBRAS
(FROM FEBRUARY 8, 2011)

4. FIRST COHOMOLOGY GROUP
(FROM JULY 26, 2012)

5. SECOND COHOMOLOGY GROUP

Note: PART 5 WILL BE POSTPONED TO
PART VI (MARCH 7, 2013)

PREAMBLE

Much of the algebra taught in the undergraduate curriculum, such as linear algebra (**vector spaces, matrices**), modern algebra (**groups, rings, fields**), number theory (**primes, congruences**) is concerned with systems with one or more associative binary products.

For example, addition and multiplication of matrices is associative:

$$A+(B+C)=(A+B)+C$$

and

$$A(BC)=(AB)C.$$

In the early 20th century, physicists started using the product A.B for matrices, defined by

$$A.B = AB + BA,$$

and called the Jordan product (after the physicist **Pascual Jordan 1902-1980**), to model the observables in quantum mechanics.

Also in the early 20th century both mathematicians and physicists used the product [A,B], defined by

$$[A, B] = AB - BA$$

and called the Lie product (after the mathematician **Sophus Lie 1842-1899**), to study differential equations.

Neither one of these products is associative, so they each give rise to what is called a nonassociative algebra, in these cases, called **Jordan algebras** and **Lie algebras** respectively.

Abstract theories of these algebras and other nonassociative algebras were subsequently developed and have many other applications, for example to **cryptography** and **genetics**, to name just two.

Lie algebras are especially important in **particle physics**.

Using only the product rule for differentiation, which every calculus student knows, part I introduced the subject of **nonassociative algebras** as the natural context for derivations.

Part II introduced derivations on other algebraic systems which have a **ternary** rather than a binary product, with special emphasis on Jordan and Lie structures.

Part III introduced the notion of **module** and was concerned with derivations from an algebra, not into itself, but into a module over the algebra. This is the appropriate setting for the study of cohomology and homological algebra

Part IV introduced the cohomology groups of an algebra and rephrased the theory of derivations on an algebra into a statement on the first cohomology group.

In this talk, we shall give the background on **equivalence relations** and **quotient groups** of abelian groups in order to define rigorously the cohomology groups of an associative algebra.

Then we shall give an interpretation* of the statement that the second cohomology group vanishes

*This will be deferred to the next talk in the series, Part VI on March 7, 2013

PART 1 OF TODAY'S TALK

A **partition** of a set X is a disjoint class $\{X_i\}$ of non-empty subsets of X whose union is X

- $\{1, 2, 3, 4, 5\} = \{1, 3, 5\} \cup \{2, 4\}$
- $\{1, 2, 3, 4, 5\} = \{1\} \cup \{2\} \cup \{3, 5\} \cup \{4\}$
- $\mathbf{R} = \mathbf{Q} \cup (\mathbf{R} - \mathbf{Q})$
- $\mathbf{R} = \cdots \cup [-2, -1) \cup [-1, 0) \cup [0, 1) \cup \cdots$

A **binary relation** on the set X is a subset R of $X \times X$. For each ordered pair

$$(x, y) \in X \times X,$$

x is said to be related to y if $(x, y) \in R$.

- $R = \{(x, y) \in \mathbf{R} \times \mathbf{R} : x < y\}$
- $R = \{(x, y) \in \mathbf{R} \times \mathbf{R} : y = \sin x\}$
- For a partition $X = \cup_i X_i$ of a set X, let $R = \{(x, y) \in X \times X : x, y \in X_i \text{ for some } i\}$

An **equivalence relation** on a set X is a relation $R \subset X \times X$ satisfying

reflexive $(x, x) \in R$
symmetric $(x, y) \in R \Rightarrow (y, x) \in R$
transitive $(x, y), (y, z) \in R \Rightarrow (x, z) \in R$

There is a one to one correspondence between equivalence relations on a set X and partitions of that set.

NOTATION

- If R is an equivalence relation we denote $(x, y) \in R$ by $x \sim y$.
- The equivalence class containing x is denoted by $[x]$. Thus

$$[x] = \{y \in X : x \sim y\}.$$

EXAMPLES

- equality: $R = \{(x, x) : x \in X\}$
- equivalence class of fractions
  = rational number:

  $R = \{(\frac{a}{b}, \frac{c}{d}) : a, b, c, d \in \mathbf{Z}, b \neq 0, d \neq 0, ad = bc\}$
- equipotent sets: X and Y are equivalent if there exists a function $f : X \to Y$ which is one to one and onto.
- half open interval of length one:
  $R = \{(x, y) \in \mathbf{R} \times \mathbf{R} : x - y \text{ is an integer}\}$
- integers modulo n:

$R = \{(x, y) \in \mathbf{N} \times \mathbf{N} : x - y \text{ is divisible by } n\}$

PART 2 OF TODAY'S TALK

A **group** is a set G together with an operation (called *multiplication*) which associates with each ordered pair x, y of elements of G a third element in G (called their *product* and written xy) in such a manner that

- multiplication is *associative*: $(xy)z = x(yz)$
- there exists an element e in G, called the *identity* element with the property that
$$xe = ex = x \text{ for all } x$$
- to each element x, there corresponds another element in G, called the *inverse* of x and written x^{-1}, with the property that
$$xx^{-1} = x^{-1}x = e$$

TYPES OF GROUPS

- commutative groups: $xy = yx$
- finite groups $\{g_1, g_2, \cdots, g_n\}$
- infinite groups $\{g_1, g_2, \cdots, g_n, \cdots\}$
- cyclic groups $\{e, a, a^2, a^3, \ldots\}$

EXAMPLES

1. $\mathbf{R}, +, 0, x^{-1} = -x$
2. positive real numbers, $\times, 1, x^{-1} = 1/x$
3. $\mathbf{R}^n$,vector addition,$(0, \cdots, 0)$, $(x_1, \cdots, x_n)^{-1} = (-x_1, \cdots, -x_n)$
4. $\mathcal{C}, +, 0, f^{-1} = -f$
5. $\{0, 1, 2, \cdots, m-1\}$, addition modulo m, 0, $k^{-1} = m - k$
6. permutations (=one to one onto functions), composition, identity permutation, inverse permutation
7. $M_n(\mathbf{R})$,+,0,$A^{-1} = [-a_{ij}]$
8. non-singular matrices, matrix multiplication, identity matrix, matrix inverse

Which of these are commutative, finite, infinite?

We shall consider only commutative groups and we shall denote the multiplication by $+$, the identity by 0, and inverse by -. No confusion should result.

ALERT

Counterintuitively, a very important (commutative) group is a group with one element

Let H be a subgroup of a commutative group G. That is, H is a subset of G and is a group under the same $+$,0,- as G.

Define an equivalence relations on G as follows: $x \sim y$ if $x - y \in H$.

The set of equivalence classes is a group under the definition of addition given by

$$[x] + [y] = [x + y].$$

This group is denoted by G/H and is called the **quotient group** of G by H.

Special cases:

$H = \{e\}$; $G/H = G$ (isomorphic)

$H = G$; $G/H = \{e\}$ (isomorphic)

EXAMPLES

1. $G = \mathbf{R}, +, 0, x^{-1} = -x$;

   $H = \mathbf{Z}$ or $H = \mathbf{Q}$

2. $\mathbf{R}^n$,vector addition,$(0, \cdots, 0)$,
   $(x_1, \cdots, x_n)^{-1} = (-x_1, \cdots, -x_n)$;

   $H = \mathbf{Z}^n$ or $H = \mathbf{Q}^n$

3. $\mathcal{C}, +, 0, f^{-1} = -f$;

   $H = \mathcal{D}$ or $H =$ polynomials

4. $M_n(\mathbf{R})$,+,0,$A^{-1} = [-a_{ij}]$;

   $H =$symmetric matrices, or
   $H =$anti-symmetric matrices

PART 3 OF TODAY'S TALK
DERIVATIONS ON ALGEBRAS
(Review of Part I: FEBRUARY 8, 2011)

AXIOMATIC APPROACH

AN <u>ALGEBRA</u> IS DEFINED TO BE A SET (ACTUALLY A VECTOR SPACE) WITH TWO BINARY OPERATIONS, CALLED <u>ADDITION</u> AND <u>MULTIPLICATION</u>

ACTUALLY, IF YOU FORGET ABOUT THE VECTOR SPACE, THIS DEFINES A

RING

ADDITION IS DENOTED BY

$$a + b$$

AND IS REQUIRED TO BE COMMUTATIVE AND ASSOCIATIVE

$$a + b = b + a, \quad (a + b) + c = a + (b + c)$$

THERE IS ALSO AN ELEMENT 0 WITH THE PROPERTY THAT FOR EACH a,

$$a + 0 = a$$

AND THERE IS AN ELEMENT CALLED $-a$ SUCH THAT

$$a + (-a) = 0$$

SO FAR, WE HAVE A COMMUTATIVE GROUP

MULTIPLICATION IS DENOTED BY

$$ab$$

AND IS REQUIRED TO BE DISTRIBUTIVE WITH RESPECT TO ADDITION

$$(a+b)c = ac + bc, \quad a(b+c) = ab + ac$$

IMPORTANT: A RING MAY OR MAY NOT HAVE AN IDENTITY ELEMENT (FOR MULTIPLICATION)

$$1x = x1 = x$$

AN ALGEBRA (or RING) IS SAID TO BE <u>ASSOCIATIVE</u> (RESP. <u>COMMUTATIVE</u>) IF THE **MULTIPLICATION** IS ASSOCIATIVE (RESP. COMMUTATIVE)

(RECALL THAT ADDITION IS ALWAYS COMMUTATIVE AND ASSOCIATIVE)

Table 2

ALGEBRAS (OR RINGS)

commutative algebras

$$ab = ba$$

associative algebras

$$a(bc) = (ab)c$$

Lie algebras

$$a^2 = 0$$

$$(ab)c + (bc)a + (ca)b = 0$$

Jordan algebras

$$ab = ba$$

$$a(a^2b) = a^2(ab)$$

Sophus Lie (1842–1899)

Marius Sophus Lie was a Norwegian mathematician. He largely created the theory of continuous symmetry, and applied it to the study of geometry and differential equations.

Pascual Jordan (1902–1980)

Pascual Jordan was a German theoretical and mathematical physicist who made significant contributions to quantum mechanics and quantum field theory.

THE DERIVATIVE

$$f'(x) = \lim_{h \to 0} \frac{f(x+h) - f(x)}{h}$$

DIFFERENTIATION IS A LINEAR PROCESS

$$(f+g)' = f' + g'$$

$$(cf)' = cf'$$

THE SET OF DIFFERENTIABLE FUNCTIONS FORMS AN ALGEBRA $\mathcal{D}$

$$(fg)' = fg' + f'g$$

(product rule)

CONTINUITY

$$x_n \to x \Rightarrow f(x_n) \to f(x)$$

THE SET OF CONTINUOUS FUNCTIONS FORMS AN ALGEBRA $\mathcal{C}$

(sums, constant multiples and products of continuous functions are continuous)

$\mathcal{D}$ and $\mathcal{C}$ ARE EXAMPLES OF ALGEBRAS WHICH ARE BOTH **ASSOCIATIVE** AND **COMMUTATIVE**

PROPOSITION 1

EVERY DIFFERENTIABLE FUNCTION IS CONTINUOUS

$\mathcal{D}$ is a subalgebra of $\mathcal{C}$; $\mathcal{D} \subset \mathcal{C}$

$$\mathcal{D} \neq \mathcal{C}$$

$$(f(x) = |x|)$$

DIFFERENTIATION IS A LINEAR PROCESS

LET US DENOTE IT BY D AND WRITE Df for f'

$$D(f+g) = Df + Dg$$

$$D(cf) = cDf$$

$$D(fg) = (Df)g + f(Dg)$$

$$D(f/g) = \frac{g(Df) - f(Dg)}{g^2}$$

DEFINITION 1

A DERIVATION ON $\mathcal{C}$ IS A LINEAR PROCESS SATISFYING THE LEIBNIZ RULE:

$$\delta(f+g) = \delta(f) + \delta(g)$$

$$\delta(cf) = c\delta(f)$$

$$\overline{\underline{\delta(fg) = \delta(f)g + f\delta(g)}}$$

DEFINITION 2

A DERIVATION ON AN ALGEBRA $\mathcal{A}$ IS A LINEAR PROCESS δ SATISFYING THE LEIBNIZ RULE:

$$\delta(ab) = \delta(a)b + a\delta(b)$$

THEOREM 1

(1955 Singer-Wermer, 1960 Sakai)

There are no (non-zero) derivations on $\mathcal{C}$.

In other words,

Every derivation of $\mathcal{C}$ is identically zero

Just to be clear,

The linear transformation which sends every function to the zero function, is the only derivation on $\mathcal{C}$.

DERIVATIONS ON THE SET OF MATRICES

THE SET $M_n(\mathbf{R})$ of n by n MATRICES IS AN ALGEBRA UNDER

MATRIX ADDITION

$$A+B$$

AND

MATRIX MULTIPLICATION

$$A\times B$$

WHICH IS ASSOCIATIVE BUT NOT COMMUTATIVE.

(PREVIOUSLY WE DEFINED TWO MORE MULTIPLICATIONS)

DEFINITION 3

A DERIVATION ON $M_n(\mathbf{R})$ WITH RESPECT TO MATRIX MULTIPLICATION IS A LINEAR PROCESS δ WHICH SATISFIES THE PRODUCT RULE

$$\delta(A \times B) = \delta(A) \times B + A \times \delta(B)$$

.

PROPOSITION 2

FIX A MATRIX A in $M_n(\mathbf{R})$ AND DEFINE

$$\delta_A(X) = A \times X - X \times A.$$

THEN δ_A IS A DERIVATION WITH RESPECT TO MATRIX MULTIPLICATION (WHICH CAN BE NON-ZERO)

THEOREM 2

(1942 Hochschild)

EVERY DERIVATION ON $M_n(\mathbf{R})$ WITH RESPECT TO MATRIX MULTIPLICATION IS OF THE FORM δ_A FOR SOME A IN $M_n(\mathbf{R})$.

Gerhard Hochschild (1915–2010)

(Photo 1968)

Gerhard Paul Hochschild was an American mathematician who worked on Lie groups, algebraic groups, homological algebra and algebraic number theory.

Joseph Henry Maclagan Wedderburn
(1882–1948)

Scottish mathematician, who taught at Princeton University for most of his career. A significant algebraist, he proved that a finite division algebra is a field, and part of the Artin–Wedderburn theorem on simple algebras. He also worked on group theory and matrix algebra.

Amalie Emmy Noether (1882–1935)

Amalie Emmy Noether was an influential German mathematician known for her groundbreaking contributions to abstract algebra and theoretical physics. Described as the most important woman in the history of mathematics, she revolutionized the theories of rings, fields, and algebras. In physics, Noether's theorem explains the fundamental connection between symmetry and conservation laws.

PROOF OF THEOREM 2 (Jacobson 1937)

If δ is a derivation, consider the two representations of $M_n(\mathbf{C})$

$$z \mapsto \begin{bmatrix} z & 0 \\ 0 & z \end{bmatrix} \text{ and } z \mapsto \begin{bmatrix} z & 0 \\ \delta(z) & z \end{bmatrix}$$

The first is a direct sum of two copies of the identity representation; but so is the second, since

$$\begin{bmatrix} 0 & 0 \\ \delta(z) & z \end{bmatrix} \text{ is equivalent to } \begin{bmatrix} 0 & 0 \\ 0 & z \end{bmatrix}$$

$$\text{so } \begin{bmatrix} z & 0 \\ \delta(z) & 0 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} z & 0 \\ 0 & z \end{bmatrix}$$

Thus $az = za,\ bz = zb$

$\delta(z)a = cz - zc$ and $\delta(z)b = dz - zd.$

a and b are multiples of I and can't both be zero. QED

Part 4 of today's talk

COHOMOLOGY OF ASSOCIATIVE ALGEBRAS

(FIRST COHOMOLOGY GROUP)

(Review of Part IV: JULY 26, 2012)

Now that we know what a quotient group is, we can better understand this material from July 26, 2012

The basic formula of homological algebra

$$F(x_1,\ldots,x_n,x_{n+1}) =$$
$$x_1 f(x_2,\ldots,x_{n+1})$$
$$-f(x_1x_2,x_3,\ldots,x_{n+1})$$
$$+f(x_1,x_2x_3,x_4,\ldots,x_{n+1})$$
$$-\cdots$$
$$\pm f(x_1,x_2,\ldots,x_nx_{n+1})$$
$$\mp f(x_1,\ldots,x_n)x_{n+1}$$

OBSERVATIONS

- n is a positive integer, $n = 1, 2, \cdots$
- f is a function of n variables
- F is a function of $n+1$ variables
- $x_1, x_2, \cdots, x_{n+1}$ belong an algebra A
- $f(y_1,\ldots,y_n)$ and $F(y_1,\cdots,y_{n+1})$ also belong to A

HIERARCHY

- $x_1, x_2, \ldots, x_n$ are points (or vectors)
- f and F are functions—they take points to points
- T, defined by $T(f) = F$ is a transformation—takes functions to functions

- points $x_1, \ldots, x_{n+1}$ and $f(y_1, \ldots, y_n)$ will belong to an algebra A
- functions f will be either <u>constant</u>, <u>linear</u> or <u>multilinear</u> (hence so will F)
- transformation T is linear

SHORT FORM OF THE FORMULA

$$(Tf)(x_1, \ldots, x_n, x_{n+1})$$

$$= x_1 f(x_2, \ldots, x_{n+1})$$

$$+ \sum_{j=1}^{n} (-1)^j f(x_1, \ldots, x_j x_{j+1}, \ldots, x_{n+1})$$

$$+(-1)^{n+1} f(x_1, \ldots, x_n) x_{n+1}$$

FIRST CASES

$\underline{n = 0}$

If f is any constant function from A to A, say, $f(x) = b$ for all x in A, where b is a fixed element of A, we have, consistent with the basic formula,

$$T_0(f)(x_1) = x_1 b - b x_1$$

$\underline{n = 1}$

If f is a linear map from A to A, then

$$T_1(f)(x_1, x_2) = x_1 f(x_2) - f(x_1 x_2) + f(x_1) x_2$$

$\underline{n = 2}$

If f is a bilinear map from $A \times A$ to A, then

$$T_2(f)(x_1, x_2, x_3) =$$

$$x_1 f(x_2, x_3) - f(x_1 x_2, x_3)$$

$$+ f(x_1, x_2 x_3) - f(x_1, x_2) x_3$$

Kernel and Image of a linear transformation

- $G : X \to Y$

  Since X and Y are vector spaces, they are in particular, commutative groups.

- **Kernel** of G is
  $\ker G = \{x \in X : G(x) = 0\}$

  This is a subgroup of X

- **Image** of G is
  $\operatorname{im} G = \{G(x) : x \in X\}$

  This is a subgroup of Y

What is the kernel of D on $\mathcal{D}$?

What is the image of D on $\mathcal{D}$?

(Hint: Second Fundamental theorem of calculus)

We now let $G = T_0, T_1, T_2$

$\underline{G = T_0}$

$X = A$ (the algebra)

$Y = L(A)$ (all linear transformations on A)

$$T_0(f)(x_1) = x_1 b - b x_1$$

$\ker T_0 = \{b \in A : xb - bx = 0 \text{ for all } x \in A\}$ (center of A)

$\operatorname{im} T_0 =$ the set of all linear maps of A of the form $x \mapsto xb - bx$,

in other words, the set of all inner derivations of A

$\ker T_0$ is a subgroup of A

$\operatorname{im} T_0$ is a subgroup of $L(A)$

$\underline{G = T_1}$

$X = L(A)$ (linear transformations on A)

$Y = L^2(A)$ (bilinear transformations on $A \times A$)

$$T_1(f)(x_1, x_2) = x_1 f(x_2) - f(x_1 x_2) + f(x_1) x_2$$

$\ker T_1 = \{f \in L(A) : T_1 f(x_1, x_2) =$ 0 for all $x_1, x_2 \in A\}$ = the set of all derivations of A

$\operatorname{im} T_1$ = the set of all bilinear maps of $A \times A$ of the form

$$(x_1, x_2) \mapsto x_1 f(x_2) - f(x_1 x_2) + f(x_1) x_2,$$

for some linear function $f \in L(A)$.

$\ker T_1$ is a subgroup of $L(A)$

$\operatorname{im} T_1$ is a subgroup of $L^2(A)$

$$L^0(A) \xrightarrow{T_0} L(A) \xrightarrow{T_1} L^2(A) \xrightarrow{T_2} L^3(A) \cdots$$

FACTS:

- $T_1 \circ T_0 = 0$
- $T_2 \circ T_1 = 0$
- $\cdots$
- $T_{n+1} \circ T_n = 0$
- $\cdots$

Therefore

$$\operatorname{im} T_n \subset \ker T_{n+1} \subset L^n(A)$$

and

$\operatorname{im} T_n$ is a subgroup of $\ker T_{n+1}$

The cohomology groups of A are defined as the quotient groups

$$H^n(A) = \frac{\ker T_n}{\operatorname{im} T_{n-1}}$$

$$(n = 1, 2, \ldots)$$

Thus

$$H^1(A) = \frac{\ker T_1}{\operatorname{im} T_0} = \frac{\text{derivations}}{\text{inner derivations}}$$

$$H^2(A) = \frac{\ker T_2}{\operatorname{im} T_1} = \frac{?}{?}$$

The theorem that every derivation of $M_n(\mathbf{R})$ is inner (that is, of the form δ_a for some $a \in M_n(\mathbf{R})$) can now be restated as:

"the cohomology group $H^1(M_n(\mathbf{R}))$ is the trivial one element group"

- $\operatorname{im} T_0 \subset \ker T_1$

  says

  Every inner derivation is a derivation

- $\operatorname{im} T_1 \subset \ker T_2$

  says

  for every linear map f, the bilinear map F defined by

  $$F(x_1, x_2) = x_1 f(x_2) - f(x_1 x_2) + f(x_1) x_2$$

  satisfies the equation

  $$x_1 F(x_2, x_3) - F(x_1 x_2, x_3) +$$

  $$F(x_1, x_2 x_3) - F(x_1, x_2) x_3 = 0$$

  for every $x_1, x_2, x_3 \in A$.

Some facts which may be discussed later on
(M is a module)

- $H^1(\mathcal{C}) = 0$, $H^2(\mathcal{C}) = 0$
- $H^1(\mathcal{C}, M) = 0$, $H^2(\mathcal{C}, M) = 0$
- $H^n(M_k(\mathbf{R}), M) = 0 \; \forall n \geq 1, k \geq 2$
- $H^n(A) = H^1(A, L(A))$ for $n \geq 2$

Cohomology groups were defined in various contexts as follows

- associative algebras (1945)
- Lie algebras (1952)
- Lie triple systems (1961,2002)
- Jordan algebras (1971)
- associative triple systems (1976)
- Jordan triple systems (1982)

Part 5 of today's talk

THIS IS POSTPONED TO THE NEXT TALK IN THE SERIES (MARCH 7, 2013)