DERIVATIONS

Introduction to non-associative algebra

OR

Playing havoc with the product rule?

PART IV—COHOMOLOGY OF ASSOCIATIVE ALGEBRAS

BERNARD RUSSO
University of California, Irvine

FULLERTON COLLEGE
DEPARTMENT OF MATHEMATICS
MATHEMATICS COLLOQUIUM
JULY 26, 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

OUTLINE OF TODAY'S TALK

1. **DERIVATIONS ON ALGEBRAS**
(Part I: FEBRUARY 8, 2011)

2. **DERIVATIONS ON MODULES**
(Part III: FEBRUARY 28, 2012)

3. **INTRODUCTION TO**
HOMOLOGICAL ALGEBRA

(Cohomology of associative algebras)

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.

(Today, we shall restrict ourselves to algebras only)

Part III introduced the notion of a **module**, which is usually not taught in an undergraduate curriculum.

Today, we are now ready to introduce the sophisticated subject called **homological algebra**.

(To keep things simple, we shall not consider modules and algebras will be associative)

PART 1 OF TODAY'S TALK
DERIVATIONS ON ALGEBRAS
(Review of Part I: FEBRUARY 8, 2011)

AXIOMATIC APPROACH

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

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

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

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:

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

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

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

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.

END OF PART I OF TODAY'S TALK

Part 2 of today's talk

DERIVATIONS ON MODULES

(Review of Part III: FEBRUARY 28, 2012)

WHAT IS A MODULE?

The American Heritage Dictionary of the English Language, Fourth Edition 2009 has 8 definitions.

1. A standard or unit of measurement.
2. **Architecture** The dimensions of a structural component, such as the base of a column, used as a unit of measurement or standard for determining the proportions of the rest of the construction.
3. **Visual Arts/Furniture** A standardized, often interchangeable component of a system or construction that is designed for easy assembly or flexible use: a sofa consisting of two end modules.

4. **Electronics** A self-contained assembly of electronic components and circuitry, such as a stage in a computer, that is installed as a unit.
5. **Computer Science** A portion of a program that carries out a specific function and may be used alone or combined with other modules of the same program.
6. **Astronautics** A self-contained unit of a spacecraft that performs a specific task or class of tasks in support of the major function of the craft.
7. **Education** A unit of education or instruction with a relatively low student-to-teacher ratio, in which a single topic or a small section of a broad topic is studied for a given period of time.
8. **Mathematics** A system with scalars coming from a ring.

Nine Zulu Queens Ruled China

- Mathematicians think of numbers as a set of nested Russian dolls. The inhabitants of each Russian doll are honorary inhabitants of the next one out.

$$\mathbf{N} \subset \mathbf{Z} \subset \mathbf{Q} \subset \mathbf{R} \subset \mathbf{C}$$

- In **N** you can't subtract; in **Z** you can't divide; in **Q** you can't take limits; in **R** you can't take the square root of a negative number. With the complex numbers **C**, nothing is impossible. You can even raise a number to a complex power.

- $\mathbf{Z}$ is a ring
- $\mathbf{Q}, \mathbf{R}, \mathbf{C}$ are fields
- $\mathbf{Q}^n$ is a vector space over $\mathbf{Q}$
- $\mathbf{R}^n$ is a vector space over $\mathbf{R}$
- $\mathbf{C}^n$ is a vector space over $\mathbf{C}$

A **field** is a commutative ring with identity element 1 such that for every nonzero element x, there is an element called x^{-1} such that

$$xx^{-1} = 1$$

A **vector space** over a field F (called the field of scalars) is a set V with an addition $+$ which is commutative and associative and has a zero element and for which there is a "scalar" product ax in V for each a in F and x in V, satisfying the following properties for arbitrary elements a, b in F and x, y in V:

1. $(a + b)x = ax + bx$
2. $a(x + y) = ax + ay$
3. $a(bx) = (ab)x$
4. $1x = x$

In abstract algebra, the concept of a module over a ring is a generalization of the notion of **vector space**, wherein the corresponding scalars are allowed to lie in an arbitrary ring.

Modules also generalize the notion of **abelian groups**, which are modules over the ring of integers.

Thus, a module, like a vector space, is an additive abelian group; a product is defined between elements of the ring and elements of the module, and this multiplication is associative (when used with the multiplication in the ring) and distributive.

SKIP TO PAGE 39,

NOW

(39=31+8)

Modules are very closely related to the
representation theory
of groups and of other algebraic structures.

They are also one of the central notions of

commutative algebra
and
homological algebra,

and are used widely in

algebraic geometry
and
algebraic topology.

A DIGRESSION

The traditional division of mathematics into subdisciplines:

Arithmetic (whole numbers)

Geometry (figures)

Algebra (abstract symbols)

Analysis (limits).

MATHEMATICS SUBJECT CLASSIFICATION

(AMERICAN MATHEMATICAL SOCIETY)

00-XX General
01-XX History and biography
03-XX Mathematical logic and foundations
05-XX Combinatorics
06-XX Lattices, ordered algebraic structures
08-XX General algebraic systems
11-XX Number Theory
12-XX Field theory and polynomials
13-XX **COMMUTATIVE ALGEBRA**
14-XX **ALGEBRAIC GEOMETRY**
15-XX Linear algebra; matrix theory
16-XX Associative rings and algebras
16-XX **REPRESENTATION THEORY**
17-XX Nonassociative rings and algebras
18-XX Category theory;
18-XX **HOMOLOGICAL ALGEBRA**
19-XX K-theory
20-XX Group theory and generalizations
20-XX **REPRESENTATION THEORY**
22-XX Topological groups, Lie groups

26-XX Real functions
28-XX Measure and integration
30-XX Complex Function Theory
31-XX Potential theory
32-XX Several complex variables
33-XX Special functions
34-XX Ordinary differential equations
35-XX Partial differential equations
37-XX Dynamical systems, ergodic theory
39-XX Difference and functional equations
40-XX Sequences, series, summability
41-XX Approximations and expansions
42-XX Harmonic analysis on Euclidean spaces
43-XX Abstract harmonic analysis
44-XX Integral transforms
45-XX Integral equations
46-XX Functional analysis
47-XX Operator theory
49-XX Calculus of variations, optimal control
51-XX Geometry
52-XX Convex and discrete geometry
53-XX Differential geometry
54-XX General topology

55-XX **ALGEBRAIC TOPOLOGY**
57-XX Manifolds and cell complexes
58-XX Global analysis, analysis on manifolds
60-XX Probability theory
62-XX Statistics
65-XX Numerical analysis
68-XX Computer science
70-XX Mechanics of particles and systems
74-XX Mechanics of deformable solids
76-XX Fluid mechanics
78-XX Optics, electromagnetic theory
80-XX Classical thermodynamics, heat
81-XX Quantum theory
82-XX Statistical mechanics, matter
83-XX Relativity and gravitational theory
85-XX Astronomy and astrophysics
86-XX Geophysics
90-XX Operations research
91-XX Game theory, economics
92-XX Biology and other natural sciences
93-XX Systems theory; control
94-XX Information and communication
97-XX Mathematics education

END OF DIGRESSION

MOTIVATION

In a vector space, the set of scalars forms a field and acts on the vectors by scalar multiplication, subject to certain axioms such as the distributive law. In a module, the scalars need only be a ring, so the module concept represents a significant generalization.

In commutative algebra, it is important that both ideals and quotient rings are modules, so that many arguments about ideals or quotient rings can be combined into a single argument about modules.

In non-commutative algebra the distinction between left ideals, ideals, and modules becomes more pronounced, though some important ring theoretic conditions can be expressed either about left ideals or left modules.

Much of the theory of modules consists of extending as many as possible of the desirable properties of vector spaces to the realm of modules over a "well-behaved" ring, such as a principal ideal domain.

However, modules can be quite a bit more complicated than vector spaces; for instance, not all modules have a basis, and even those that do, **free modules**, need not have a unique rank if the underlying ring does not satisfy the invariant basis number condition.

Vector spaces always have a basis whose cardinality is unique (assuming the axiom of choice).

FORMAL DEFINITION

A left R-module M over the ring R consists of an abelian group (M, $+$) and an operation $R \times M \to M$ such that for all r,s in R, x,y in M, we have:

$$r(x+y) = rx + ry$$

$$(r+s)x = rx + sx$$

$$(rs)x = r(sx)$$

$$1x = x$$

if R has multiplicative identity 1.

The operation of the ring on M is called scalar multiplication, and is usually written by juxtaposition, i.e. as rx for r in R and x in M.

EXAMPLES

1. If K is a field, then the concepts "K-vector space" (a vector space over K) and K-module are identical.
2. The concept of a Z-module agrees with the notion of an abelian group. That is, every abelian group is a module over the ring of integers Z in a unique way. For n $\geq$ 0, let nx = x + x + ... + x (n summands), 0x = 0, and (-n)x = -(nx). Such a module need not have a basis
3. The square n-by-n matrices with real entries form a ring R, and the Euclidean space R^n is a left module over this ring if we define the module operation via matrix multiplication. If R is any ring and I is any left ideal in R, then I is a left module over R. Analogously of course, right ideals are right modules.

SKIP TO PAGE 50, NOW

(50=40+10)

4. If R is any ring and n a natural number, then the cartesian product R^n is both a left and a right module over R if we use the component-wise operations. Hence when n = 1, R is an R-module, where the scalar multiplication is just ring multiplication. The case n = 0 yields the trivial R-module 0 consisting only of its identity element. Modules of this type are called free
5. If S is a nonempty set, M is a left R-module, and M^S is the collection of all functions f : S $\to$ M, then with addition and scalar multiplication in M^S defined by (f + g)(s) = f(s) + g(s) and (rf)(s) = rf(s), M^S is a left R-module. The right R-module case is analogous. In particular, if R is commutative then the collection of R-module homomorphisms h : M $\to$ N (see below) is an R-module (and in fact a submodule of N^M).
6. There are modules of a Lie algebra as well.

If one writes the scalar action as f_r so that $f_r(x) = rx$, and f for the map which takes each r to its corresponding map f_r, then the first axiom states that every f_r is a group homomorphism of M, and the other three axioms assert that the map f:R $\rightarrow$ End(M) given by $r \mapsto f_r$ is a ring homomorphism from R to the endomorphism ring End(M).

In this sense, module theory generalizes representation theory, which deals with group actions on vector spaces.

A **bimodule** is a module which is a left module and a right module such that the two multiplications are compatible.

SUBMODULES AND HOMOMORPHISMS

Suppose M is a left R-module and N is a subgroup of M. Then N is a **submodule** (or R-submodule, to be more explicit) if, for any n in N and any r in R, the product r n is in N (or nr for a right module).

If M and N are left R-modules, then a map $f : M \to N$ is a **homomorphism of R-modules** if, for any m, n in M and r, s in R, $f(rm + sn) = rf(m) + sf(n)$.

This, like any homomorphism of mathematical objects, is just a mapping which preserves the structure of the objects. Another name for a homomorphism of modules over R is an R-linear map.

A bijective module homomorphism is an **isomorphism of modules**, and the two modules are called isomorphic.

Two isomorphic modules are identical for all practical purposes, differing solely in the notation for their elements.

The kernel of a module homomorphism $f : M \to N$ is the submodule of M consisting of all elements that are sent to zero by f.

The isomorphism theorems familiar from groups and vector spaces are also valid for R-modules.

TYPES OF MODULES

(a) **Finitely generated** A module M is finitely generated if there exist finitely many elements $x_1, \ldots x_n$ in M such that every element of M is a linear combination of those elements with coefficients from the scalar ring R.

(b) **Cyclic module** A module is called a cyclic module if it is generated by one element.

(c) **Free** A free module is a module that has a basis, or equivalently, one that is isomorphic to a direct sum of copies of the scalar ring R. These are the modules that behave very much like vector spaces.

(d) **Projective** Projective modules are direct summands of free modules and share many of their desirable properties.

(e) **Injective** Injective modules are defined dually to projective modules.

(f) **Flat** A module is called flat if taking the tensor product of it with any short exact sequence of R modules preserves exactness.

(g) **Simple** A simple module S is a module that is not 0 and whose only submodules are 0 and S. Simple modules are sometimes called irreducible.

(h) **Semisimple** A semisimple module is a direct sum (finite or not) of simple modules. Historically these modules are also called completely reducible.

(i) **Indecomposable** An indecomposable module is a non-zero module that cannot be written as a direct sum of two non-zero submodules. Every simple module is indecomposable, but there are indecomposable modules which are not simple (e.g. uniform modules).

(j) **Faithful** A faithful module M is one where the action of each $r \neq 0$ in R on M is nontrivial (i.e. $rx \neq 0$ for some x in M). Equivalently, the annihilator of M is the zero ideal.

(k) **Noetherian**. A Noetherian module is a module which satisfies the ascending chain condition on submodules, that is, every increasing chain of submodules becomes stationary after finitely many steps. Equivalently, every submodule is finitely generated.

(l) **Artinian** An Artinian module is a module which satisfies the descending chain condition on submodules, that is, every decreasing chain of submodules becomes stationary after finitely many steps.

(m) **Graded** A graded module is a module decomposable as a direct sum M $= \oplus_x M_x$ over a graded ring R $= \oplus_x R_x$ such that $R_x M_y \subset M_{x+y}$ for all x and y.

(n) **Uniform** A uniform module is a module in which all pairs of nonzero submodules have nonzero intersection.

RELATION TO REPRESENTATION THEORY

If M is a left R-module, then the action of an element r in R is defined to be the map M $\rightarrow$ M that sends each x to rx (or xr in the case of a right module), and is necessarily a group endomorphism of the abelian group (M,+).

The set of all group endomorphisms of M is denoted $End_Z(M)$ and forms a ring under addition and composition, and sending a ring element r of R to its action actually defines a ring homomorphism from R to $End_Z(M)$.

Such a ring homomorphism R $\to End_Z(M)$ is called a representation of R over the abelian group M; an alternative and equivalent way of defining left R-modules is to say that a left R-module is an abelian group M together with a representation of R over it.

A representation is called faithful if and only if the map R $\to End_Z(M)$ is injective. In terms of modules, this means that if r is an element of R such that rx=0 for all x in M, then r=0.

END OF “MODULE” ON MODULES

DERIVATIONS INTO A MODULE

CONTEXTS

(i) ASSOCIATIVE ALGEBRAS
(ii) LIE ALGEBRAS
(iiI) JORDAN ALGEBRAS

Could also consider:

(i') ASSOCIATIVE TRIPLE SYSTEMS
(ii') LIE TRIPLE SYSTEMS
(iii') JORDAN TRIPLE SYSTEMS

(i) ASSOCIATIVE ALGEBRAS

derivation: $D(ab) = a \cdot Db + Da \cdot b$

inner derivation: (ad x)$(a) = x \cdot a - a \cdot x$
$(x \in M)$

THEOREM (Noether,Wedderburn) (early 20th century)) *

EVERY DERIVATION OF SEMISIMPLEASSOCIATIVE ALGEBRA IS INNER, THAT IS, OF THE FORM $x \mapsto ax - xa$ FOR SOME a IN THE ALGEBRA

THEOREM (Hochschild 1942)

EVERY DERIVATION OF SEMISIMPLE ASSOCIATIVE ALGEBRA INTO A MODULE IS INNER, THAT IS, OF THE FORM $x \mapsto ax - xa$ FOR SOME a IN THE MODULE

*The operational word here, and in all of these results is SEMISIMPLE—think primes, fundamental theorem of arithmetic

(iii) JORDAN ALGEBRAS

derivation: $D(a \circ b) = a \circ Db + Da \circ b$

inner derivation:

$\sum_i [L(x_i)L(a_i) - L(a_i)L(x_i)]$

$(x_i \in M, a_i \in A)$

$b \mapsto \sum_i [x_i \circ (a_i \circ b) - a_i \circ (x_i \circ b)]$

THEOREM (1949-Jacobson)
EVERY DERIVATION OF A FINITE DIMENSIONAL SEMISIMPLE JORDAN ALGEBRA INTO ITSELF IS INNER

THEOREM (1951-Jacobson)
EVERY DERIVATION OF A FINITE DIMENSIONAL SEMISIMPLE JORDAN ALGEBRA INTO A (JORDAN) **MODULE** IS INNER
(Lie algebras, Lie triple systems)

SKIP TO PAGE 57, SLOWLY

(57=52+5)

(iii') JORDAN TRIPLE SYSTEMS

derivation:

$$D\{a,b,c\} = \{Da.b,c\} + \{a,Db,c\} + \{a,b,Dc\}$$

$$\{x,y,z\} = (xy^*z + zy^*x)/2$$

inner derivation: $\sum_i [L(x_i,a_i) - L(a_i,x_i)]$

$$(x_i \in M, a_i \in A)$$

$$b \mapsto \sum_i [\{x_i,a_i,b\} - \{a_i,x_i,b\}]$$

THEOREM (1972 Meyberg)
EVERY DERIVATION OF A FINITE DIMENSIONAL SEMISIMPLE JORDAN TRIPLE SYSTEM IS INNER
(Lie algebras, Lie triple systems)

THEOREM (1978 Kühn-Rosendahl)
EVERY DERIVATION OF A FINITE DIMENSIONAL SEMISIMPLE JORDAN TRIPLE SYSTEM INTO A JORDAN TRIPLE MODULE IS INNER
(Lie algebras)

(i') ASSOCIATIVE TRIPLE SYSTEMS

derivation:

$$D(ab^tc) = ab^tDc + a(Db)^tc + (Da)b^tc$$

inner derivation: see Table 3

The (non-module) result can be derived from the result for Jordan triple systems. (See an exercise)

THEOREM (1976 Carlsson)
EVERY DERIVATION OF A FINITE DIMENSIONAL SEMISIMPLE ASSOCIATIVE TRIPLE SYSTEM INTO A MODULE IS INNER

(reduces to associative ALGEBRAS)

(ii) LIE ALGEBRAS

THEOREM (Zassenhaus)
(early 20th century)
EVERY DERIVATION OF A FINITE DIMENSIONAL SEMISIMPLE LIE ALGEBRA INTO ITSELF IS INNER

THEOREM (Hochschild 1942)
EVERY DERIVATION OF A FINITE DIMENSIONAL SEMISIMPLE LIE ALGEBRA INTO A MODULE IS INNER

(ii') LIE TRIPLE SYSTEMS

THEOREM (Lister 1952)
EVERY DERIVATION OF A FINITE DIMENSIONAL SEMISIMPLE LIE TRIPLE SYSTEM INTO ITSELF IS INNER

THEOREM (Harris 1961)
EVERY DERIVATION OF A FINITE DIMENSIONAL SEMISIMPLE LIE TRIPLE SYSTEM INTO A MODULE IS INNER

Table 1 $M_n(\mathbf{R})$ (ALGEBRAS)

associative	Lie	Jordan
$ab = a \times b$	$[a,b] = ab - ba$	$a \circ b = ab + ba$
Noeth,Wedd 1920	Zassenhaus 1930	Jacobson 1949
Hochschild 1942	Hochschild 1942	Jacobson 1951

Table 3 $M_{m,n}(\mathbf{R})$ (TRIPLE SYSTEMS)

associative triple	Lie triple	Jordan triple
ab^tc	$[[a,b],c]$	$ab^tc + cb^ta$
	Lister 1952	Meyberg 1972
Carlsson 1976	Harris 1961	Kühn-Rosendahl 1978

Part 3 of today's talk

COHOMOLOGY OF ASSOCIATIVE ALGEBRAS (Introduction to HOMOLOGICAL ALGEBRA)

SKIP TO PAGE 61, NOW

(61=58+3)

Let M be an associative algebra and X an M-module.

For $n \geq 1$, let

$L^n(M, X) =$ all n-linear maps

$(L^0(M, X) = X)$

Coboundary operator

$\partial : L^n \to L^{n+1}$ (for $n \geq 1$)

$$\partial\phi(a_1, \cdots, a_{n+1}) = a_1\phi(a_2, \cdots, a_{n+1})$$
$$+\sum(-1)^j\phi(a_1, \cdots, a_{j-1}, a_ja_{j+1}, \cdots, a_{n+1})$$
$$+(-1)^{n+1}\phi(a_1, \cdots, a_n)a_{n+1}$$

For $n = 0$,

$$\partial : X \to L(M, X) \qquad \partial x(a) = ax - xa$$

so

$\mathrm{Im}\partial =$ the space of inner derivations

Since $\partial \circ \partial = 0$,

$$\mathrm{Im}(\partial : L^{n-1} \to L^n) \subset \ker(\partial : L^n \to L^{n+1})$$

$H^n(M, X) = \ker\partial/\mathrm{Im}\partial$ is a vector space.

For $n = 1$, ker$\partial =$
$\{\phi : M \to X :$
$a_1\phi(a_2) - \phi(a_1 a_2) + \phi(a_1)a_2 = 0\}$
$=$ the space of continuous derivations from M to X

Thus,

$$H^1(M, X) = \frac{\text{derivations from } M \text{ to } X}{\text{inner derivations from } M \text{ to } X}$$

measures how close continuous derivations are to inner derivations.

(What do $H^2(M, X)$, $H^3(M, X)$,... measure?)

START OVER
WORK BACKWARDS

The basic formula of homological algebra

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

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

- $G : X \to Y$
- **Kernel** of G is
  $\ker G = \{x \in X : G(x) = 0\}$
- **Image** of G is
  $\operatorname{Im} G = \{G(x) : x \in X\}$

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)

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

$\underline{G = T_1}$

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

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

$\ker T_1 = \{f \in L(A) : T_1 f(x_1, x_2) = 0$ 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 $f \in L(A)$.

(we won't do the calculation for T_2)

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

FACTS:

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

Therefore

$$\operatorname{Im} T_n \subset \ker T_{n+1}$$

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

  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 $x_1, x_2, x_3 \in A$.

The cohomology groups of A are defined as follows

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

Thus

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

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

We need to know about equivalence relations and quotients of groups in order to make this definition precise.

This will have to wait for the next talk in this series, and will include an interpretation of $H^2(A)$.

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

Future talks in this series will discuss versions of cohomology involving

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