DERIVATIONS

Introduction to non-associative algebra

OR

Playing havoc with the product rule?

BERNARD RUSSO
UNIVERSITY OF CALIFORNIA, IRVINE
DEPARTMENT OF MATHEMATICS

UNIVERSITY STUDIES 4
TRANSFER SEMINAR

FALL 2012

Fifth Meeting: October 25, 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.

1. REVIEW OF ALGEBRAS (SEPT 27,OCT 4,OCT 11)

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

$$1x = x1 = x$$

AN ALGEBRA (or RING) IS SAID TO BE ASSOCIATIVE (RESP. COMMUTATIVE) 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 $\mathcal{C}$; $\mathcal{D} \subset \mathcal{C}$

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:

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

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

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

THEOREM 1

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

In other words,
Every derivation of $\mathcal{C}$ is identically zero

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.

(WE DEFINED TWO MORE MULTIPLICATIONS)

DEFINITION 2

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.

DISCUSSION OF EXERCISE 7

7. **PROBLEM** Let us write $\delta_{a,b}$ for the linear process $\delta_{a,b}(x) = a(bx) - b(ax)$ in a Jordan algebra. Show that $\delta_{a,b}$ is a derivation of the Jordan algebra by following the outline below.

SOLUTION

(a) In the Jordan algebra axiom

$$u(u^2v) = u^2(uv),$$

replace u by $u+w$ to obtain the two equations

$$2u((uw)v)+w(u^2v) = 2(uw)(uv)+u^2(wv) \quad (1)$$

and

$$u(w^2v) + 2w((uw)v) = w^2(uv) + 2(uw)(wv).$$

(Hint: Consider the "degree" of w on each side of the equation resulting from the substitution)

(b) In (1), interchange v and w and subtract the resulting equation from (1) to obtain the equation

$$2u(\delta_{v,w}(u)) = \delta_{v,w}(u^2). \qquad (2)$$

(c) In (2), replace u by $x + y$ to obtain the equation

$$\delta_{v,w}(xy) = y\delta_{v,w}(x) + x\delta_{v,w}(y),$$

which is the desired result.

WE NOW RETURN TO MODULES
(the mathematical definition #8)

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

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.

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.

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.

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 $\to$ 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.

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 $nx = x + x + \ldots + x$ (n summands), $0x = 0$, and $(-n)x = -(nx)$. Such a module need not have a basis
3. 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

Note: THE NEXT 8 PAGES MAY BE SKIPPED AT THIS TIME

4. 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).
5. 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.
6. There are modules of a Lie algebra as well.

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 $\rightarrow$ 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 $\rightarrow$ 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 $\rightarrow End_Z(M)$ 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 $\rightarrow End_Z(M)$ 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

So far we have defined a module over an associative algebra. One can also define modules over Lie algebras and modules over Jordan algebras.

We now recall the earlier theorems on derivations and restate them in the case of a derivation into a module

(i) ASSOCIATIVE ALGEBRAS

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

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

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

EVERY DERIVATION OF SEMISIMPLE ASSOCIATIVE 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 $x \mapsto a \cdot x - x \cdot a$ FOR SOME a IN THE MODULE

(ii) LIE ALGEBRAS

derivation: $D([a,b]) = [a, Db] + [Da, b]$

inner derivation: $\delta_x(a) = [a, x]$ $(x \in M)$

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

(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)