DERIVATIONS
An introduction to non associative algebra
(or, Playing havoc with the product rule)

Part 9
Vanishing Theorems in dimensions 1 and 2
(Jordan algebras)

Colloquium
Fullerton College

Bernard Russo

University of California, Irvine

February 18, 2014

History of these lectures

- PART I FEBRUARY 8, 2011 **ALGEBRAS; DERIVATIONS**
- PART II JULY 21, 2011 **TRIPLE SYSTEMS; DERIVATIONS**
- PART III FEBRUARY 28, 2012 **MODULES; DERIVATIONS**
- PART IV JULY 26, 2012 **COHOMOLOGY (ASSOCIATIVE ALGEBRAS)**
- PART V OCTOBER 25, 2012 **THE SECOND COHOMOLOGY GROUP**
- PART VI MARCH 7, 2013 **COHOMOLOGY (LIE ALGEBRAS)**
- PART VII JULY 25, 2013 **COHOMOLOGY (JORDAN ALGEBRAS)**
- PART VIII SEPTEMBER 17, 2013 **VANISHING THEOREMS IN DIMENSIONS 1 AND 2 (ASSOCIATIVE ALGEBRAS)**
- PART IX FEBRUARY 18, 2014 (today) **VANISHING THEOREMS IN DIMENSIONS 1 AND 2 (JORDAN ALGEBRAS)**

Outline

- Review of Algebras

- Review of Derivations on matrix algebras

- Review of Cohomology (Associative algebras)

- Cohomology of Jordan algebras; $H^2_J(M_2, M_2) = 0$[1]

- Appendix 1—Equivalence Relations and Quotient Groups
(from pp. 23-32 of part 6 of this lecture series)

- Appendix 2—What is a module?
(from pp. 65-85 of part 3 of this lecture series)

[1] Postponed to part 10 (SUMMER 2014). The material included here will be revised in preparation for part 10

Introduction

I will present an outline of the proof of vanishing of the second (Jordan) cohomology group of a Jordan algebra, illustrating with the algebra of two by two matrices with circle multiplication.

The relevant definitions and examples from earlier talks in the series will be reviewed beforehand.

Review of Algebras—Axiomatic approach

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

ADDITION IS DENOTED BY $a+b$ AND IS REQUIRED TO BE
COMMUTATIVE $\quad a+b=b+a$
AND ASSOCIATIVE $\quad (a+b)+c=a+(b+c)$

MULTIPLICATION IS DENOTED BY ab AND IS REQUIRED TO BE DISTRIBUTIVE WITH RESPECT TO ADDITION
$(a+b)c=ac+bc, \quad a(b+c)=ab+ac$

AN ALGEBRA IS SAID TO BE ASSOCIATIVE (RESP. COMMUTATIVE) IF THE **MULTIPLICATION** IS ASSOCIATIVE (RESP. COMMUTATIVE)
(RECALL THAT ADDITION IS ALWAYS COMMUTATIVE AND ASSOCIATIVE)

Table 1 (FASHIONABLE) ALGEBRAS

commutative algebras $ab = ba$

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

Lie algebras $a^2 = 0$, $(ab)c + (bc)a + (ca)b = 0$

Jordan algebras $ab = ba$, $a(a^2b) = a^2(ab)$

We shall primarily be concerned with Jordan algebras in this talk, in fact, only the algebra of two by two matrices under circle multiplication.

DERIVATIONS ON MATRIX ALGEBRAS

THE SET $M_n(\mathbb{R})$ 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.

For the Record:

$[a_{ij}]+[b_{ij}]=[a_{ij}+b_{ij}]$ $[a_{ij}] \times [b_{ij}] = [\sum_{k=1}^n a_{ik}b_{kj}]$

DEFINITION

A DERIVATION ON $M_n(\mathbb{R})$ WITH RESPECT TO MATRIX MULTIPLICATION IS A LINEAR PROCESS δ: $\delta(A+B)=\delta(A)+\delta(B)$
WHICH SATISFIES THE PRODUCT RULE

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

.

PROPOSITION

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

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

THEN δ_A IS A DERIVATION WITH RESPECT TO MATRIX MULTIPLICATION (WHICH ARE CALLED **INNER DERIVATIONS**)

THEOREM (Noether,Wedderburn,Hochschild,Jacobson, Kaplansky,Kadison,Sakai)

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

We gave a proof of this theorem for $n = 2$ in the previous talk in this series.

THE BRACKET PRODUCT ON THE SET OF MATRICES

DEFINITION

THE **BRACKET PRODUCT** ON THE SET $M_n(\mathbb{R})$ OF MATRICES IS DEFINED BY

$$[X, Y] = X \times Y - Y \times X$$

THE SET $M_n(\mathbb{R})$ of n by n MATRICES IS AN ALGEBRA UNDER MATRIX ADDITION AND BRACKET MULTIPLICATION, WHICH IS NOT ASSOCIATIVE AND NOT COMMUTATIVE.

DEFINITION

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

$$\delta([A, B]) = [\delta(A), B] + [A, \delta(B)].$$

PROPOSITION

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

$$\delta_A(X) = [A, X] = A \times X - X \times A.$$

THEN δ_A IS A DERIVATION WITH RESPECT TO BRACKET MULTIPLICATION (STILL CALLED **INNER DERIVATION**).

THEOREM

EVERY DERIVATION ON $M_n(\mathbb{R})$ WITH RESPECT TO BRACKET MULTIPLICATION IS INNER, THAT IS, OF THE FORM δ_A FOR SOME A IN $M_n(\mathbb{R})$. [a]

[a] Full disclosure: this is actually not true. Check that the map $X \mapsto$ (trace of X)I is a derivation which is not inner (I is the identity matrix). The correct statement is that every derivation of a semisimple finite dimensional Lie algebra is inner. $M_n(\mathbb{R})$ is a semisimple associative algebra under matrix multiplication, a semisimple Jordan algebra under circle multiplication, but not a semisimple Lie algebra under bracket multiplication. Please ignore this footnote until you find out what semisimple means in each context

THE CIRCLE PRODUCT ON THE SET OF MATRICES

DEFINITION

THE **CIRCLE PRODUCT** ON THE SET $M_n(\mathbb{R})$ OF MATRICES IS DEFINED BY

$$X \circ Y = (X \times Y + Y \times X)/2$$

THE SET $M_n(\mathbb{R})$ of n by n MATRICES IS AN ALGEBRA UNDER MATRIX ADDITION AND CIRCLE MULTIPLICATION, WHICH IS COMMUTATIVE BUT NOT ASSOCIATIVE.

DEFINITION

A <u>DERIVATION</u> ON $M_n(\mathbb{R})$ WITH <u>RESPECT TO CIRCLE MULTIPLICATION</u> IS A LINEAR PROCESS δ WHICH SATISFIES THE PRODUCT RULE

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

PROPOSITION

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

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

THEN δ_A IS A DERIVATION WITH RESPECT TO CIRCLE MULTIPLICATION (ALSO CALLED AN INNER DERIVATION IN THIS CONTEXT[a])

[a] However, see the following remark. Also see some of the exercises (Dr. Gradus Ad Parnassum) in part 1 of these lectures

THEOREM (1972-Sinclair)

EVERY DERIVATION ON $M_n(\mathbb{R})$ WITH RESPECT TO CIRCLE MULTIPLICATION IS INNER, THAT IS, OF THE FORM δ_A FOR SOME A IN $M_n(\mathbb{R})$.

REMARK (1937-Jacobson)
THE ABOVE PROPOSITION AND THEOREM NEED TO BE MODIFIED FOR THE SUBALGEBRA (WITH RESPECT TO CIRCLE MULTIPLICATION) OF SYMMETRIC MATRICES, FOR EXAMPLE.

Table 2 $M_n(\mathbb{R})$ (ALGEBRAS)

matrix	bracket	circle
$ab = a \times b$	$[a, b] = ab - ba$	$a \circ b = ab + ba$
Associative	Lie	Jordan
$\delta_a(x)$ $=$ $ax - xa$	$\delta_a(x)$ $=$ $ax - xa$	$\delta_a(x)$ $=$ $ax - xa$
	or trace$(x)I$	

Review of Cohomology (Associative algebras)

NOTATION

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

The basic formula of homological algebra

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

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 constant, linear or multilinear (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, a linear function $T_0(f)$:

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

$\underline{n = 1}$

If f is a linear function from A to A, then $T_1(f)$ is a bilinear function

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

$\underline{n = 2}$

If f is a bilinear function from $A \times A$ to A, then $T_2(f)$ is a trilinear function

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

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

FIRST COHOMOLOGY GROUP

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 (also called **nullspace** 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

$\underline{G = T_0}$

$X = A$ (the algebra) $\quad Y = L(A)$ (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
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 $L(A)$
im T_1 is a subgroup of $L^2(A)$

$\underline{G = T_2}$

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

$Y = L^3(A)$ (trilinear transformations on $A \times A \times A$)

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

$\ker T_2 = \{f \in L^2(A) : T_2 f(x_1, x_2, x_3) = 0 \text{ for all } x_1, x_2, x_3 \in A\}$

$\text{im } T_2 =$ the set of all trilinear maps of $A \times A \times A$ of the form

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

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

$\ker T_2$ is a subgroup of $L^2(A)$

$\text{im } T_2$ is a subgroup of $L^3(A)$

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

FACTS: $T_1 \circ T_0 = 0$

$T_2 \circ T_1 = 0$

$\ldots$

$T_{n+1} \circ T_n = 0$

$\ldots$

Therefore

im $T_n \subset$ ker $T_{n+1} \subset L^n(A)$
and therefore
im T_n is a subgroup of ker T_{n+1}

TERMINOLOGY

im $T_{n-1} =$ the set of *n*-**coboundaries**
ker $T_n =$ the set of *n*-**cocycles**
and therefore
every *n*-coboundary is an *n*-cocycle.

im $T_0 \subset$ ker T_1
says
Every inner derivation (1-coboundary) is a derivation (1-cocycle).

im $T_1 \subset$ ker T_2
says
for every linear map f, the bilinear map Fdefined by

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

(2-coboundary) 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 $x_1, x_2, x_3 \in A$ (2-cocycle).

(Simple verification)

The cohomology groups of A are defined as the quotient groups

$$H^n(A) = \frac{\ker T_n}{\operatorname{im} T_{n-1}} = \frac{n\text{-cocycles}}{n\text{-coboundaries}} \qquad (n = 1, 2, \ldots)$$

Thus

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

$$H^2(A) = \frac{\ker T_2}{\operatorname{im} T_1} = \frac{\text{2-cocycles}}{\text{2-coboundaries}} = \frac{\text{null extensions}^{a}}{\text{split null extensions}}$$

[a] This will be explained in what follows (associative and Jordan cases)

The theorem that every derivation of $M_n(\mathbb{R})$ is inner (that is, of the form δ_a for some $a \in M_n(\mathbb{R})$, Theorem 1 below for $n = 2$) can now be restated as:
"the cohomology group $H^1(M_n(\mathbb{R}))$ is the trivial one element group"

The theorem that every null extension of $M_n(\mathbb{R})$ is a split null extension (Corollary 2 of Theorem 2 below for $n = 2$) can be stated as:
"the cohomology group $H^2(M_n(\mathbb{R}))$ is the trivial one element group"

$H^1(M_2, M_2) = 0$

Matrix units

Let $E_{11} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$, $E_{12} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$, $E_{21} = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$, $E_{22} = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$

LEMMA

- $E_{11} + E_{22} = I$
- $E_{ij}^t = E_{ji}$
- $E_{ij}E_{kl} = \delta_{jk}E_{il}$

THEOREM 1

Let $\delta : M_2 \to M_2$ be a derivation: δ is linear and $\delta(AB) = A\delta(B) + \delta(A)B$. Then there exists a matrix K such that $\delta(X) = XK - KX$ for X in M_2.

COROLLARY

$H^1(M_2, M_2) = 0$

$H^2(M_2, M_2) = 0$

THEOREM 2

Let f be a 2-cocycle: f is bilinear and

$$T_2 f(A,B,C) = Af(B,C) - f(AB,C) + f(A,BC) - f(A,B)C = 0$$

for all A, B, C in M_2. Then there exists a linear transformation ξ on M_2 such that $T_1\xi = f$, that is, f is a 2-coboundary.

COROLLARY 1

$H^2(M_2, M_2) = 0$

COROLLARY 2

It E is any associative algebra containing an ideal J such that E/J is isomorphic to M_2 (E is then said to be an **extension** of M_2), then there is a subalgebra B of E such that $E = B \oplus M_2$ (E is a **split extension**) [a]

[a] There is always a subspace B such that $E = B \oplus M_2$

Interpretation of the second cohomology group (associative algebras)

Homomorphisms of groups

$f : G_1 \to G_2$ is a homomorphism if

$f(x + y) = f(x) + f(y)$

- $f(G_1)$ is a subgroup of G_2
- $\ker f$ is a subgroup of G_1
- $G_1/\ker f$ is isomorphic to $f(G_1)$

(isomorphism =
one to one and onto homomorphism)

Homomorphisms of algebras

$h : A_1 \to A_2$ is a homomorphism if

$h(x + y) = h(x) + h(y)$

and

$h(xy) = h(x)h(y)$

- $h(A_1)$ is a subalgebra of A_2
- $\ker h$ is a subalgebra of A_1 (actually, an ideal[a] in A_1)
- $A_1/\ker h$ is isomorphic to $h(A_1)$

(isomorphism =
one to one and onto homomorphism)

[a] An **ideal** in an algebra A is a subalgebra I with the property that $AI \cup IA \subset I$, that is, $xa, ax \in I$ whenever $x \in I$ and $a \in A$

Extensions (Associative algebras)

Let A be an algebra. Let M be another algebra which contains an ideal I and let $g : M \to A$ be a homomorphism.

In symbols,

$I \overset{\subsetneq}{\to} M \overset{g}{\to} A$ This is called an **extension of** A **by** I if

- $\ker g = I$
- $\operatorname{im} g = A$

It follows that M/I is isomorphic to A

EXAMPLE 1

Let A be an algebra.

Define an algebra $M = A \oplus A$ to be the set $A \times A$ with addition

$(a, x) + (b, y) = (a + b, x + y)$

and product

$(a, x)(b, y) = (ab, xy)$

- $\{0\} \times A$ is an ideal in M
- $(\{0\} \times A)^2 \neq 0$
- $g : M \to A$ defined by $g(a, x) = a$ is a homomorphism
- M is an extension of $\{0\} \times A$ by A.

EXAMPLE 2

Let A be an algebra and let $h \in \ker T_2 \subset L^2(A)$.

Recall that this means that for all $x_1, x_2, x_3 \in A$,

$x_1 f(x_2, x_3) - f(x_1x_2, x_3)$

$+f(x_1, x_2x_3) - f(x_1, x_2)x_3 = 0$

Define an algebra M_h to be the set $A \times A$ with addition

$(a, x) + (b, y) = (a + b, x + y)$

and the product

$(a, x)(b, y) = (ab, ay + xb + h(a, b))$

Because $h \in \ker T_2$, this algebra is **ASSOCIATIVE!** whenever A is associative.

THE PLOT THICKENS (do these differ from Example 1?)

- $\{0\} \times A$ is an ideal in M_h
- $(\{0\} \times A)^2 = 0$
- $g : M_h \to A$ defined by $g(a, x) = a$ is a homomorphism
- M_h is an extension of $\{0\} \times A$ by A.

EQUIVALENCE OF EXTENSIONS

Extensions

$I \overset{\subsetneq}{\rightarrow} M \overset{g}{\rightarrow} A$ and

$I \overset{\subsetneq}{\rightarrow} M' \overset{g'}{\rightarrow} A$ are said to be equivalent if

there is an isomorphism $\psi : M \to M'$

such that

- $\psi(x) = x$ for all $x \in I$
- $g = g' \circ \psi$

(Is this an equivalence relation?)

EXAMPLE 2—continued

Let $h_1, h_2 \in \ker T_2$.

We then have two extensions of A by $\{0\} \times A$, namely

$\{0\} \times A \overset{\subsetneq}{\to} M_{h_1} \overset{g_1}{\to} A$

and

$\{0\} \times A \overset{\subsetneq}{\to} M_{h_2} \overset{g_2}{\to} A$

Now suppose that h_1 is equivalent[a] to h_2,
$h_1 - h_2 = T_1 f$ for some $f \in L(A)$

- The above two extensions are equivalent.
- We thus have a mapping from $H^2(A, A)$ into the set of equivalence classes of extensions of A by the ideal $\{0\} \times A$

[a] This is the same as saying that $[h_1] = [h_2]$ as elements of $H^2(A, A) = \ker T_2 / \operatorname{im} T_1$

GRADUS AD PARNASSUM (COHOMOLOGY)

1. Verify that there is a one to one correspondence between partitions of a set X and equivalence relations on that set. Precisely, show that

- If $X = \cup X_i$ is a partition of X, then $R := \{(x, y) \in X \times X : x, y \in X_i \text{ for some } i\}$ is an equivalence relation whose equivalence classes are the subsets X_i.
- If R is an equivalence relation on X with equivalence classes X_i, then $X = \cup X_i$ is a partition of X.

2. Verify that $T_{n+1} \circ T_n = 0$ for $n = 0, 1, 2$. Then prove it for all $n \geq 3$.

3. Show that if $f : G_1 \to G_2$ is a homomorphism of groups, then $G_1 / \ker f$ is isomorphic to $f(G_1)$
Hint: Show that the map $[x] \mapsto f(x)$ is an isomorphism of $G_1 / \ker f$ onto $f(G_1)$

4. Show that if $h : A_1 \to A_2$ is a homomorphism of algebras, then $A_1 / \ker h$ is isomorphic to $h(A_1)$
Hint: Show that the map $[x] \mapsto h(x)$ is an isomorphism of $A_1 / \ker h$ onto $h(A_1)$

5. Show that the algebra M_h in Example 2 is associative.
Hint: You use the fact that A is associative AND the fact that, since $h \in \ker T_2$, $h(a,b)c + h(ab.c) = ah(b,c) + h(a,bc)$

6. Show that equivalence of extensions is actually an equivalence relation.
Hint:

- reflexive: $\psi : M \to M$ is the identity map
- symmetric: replace $\psi : M \to M'$ by its inverse $\psi^{-1} : M' \to M$
- transitive: given $\psi : M \to M'$ and $\psi' : M' \to M''$ let $\psi'' = \psi' \circ \psi : M \to M''$

7. Show that in example 2, if h_1 and h_2 are equivalent bilinear maps, that is, $h_1 - h_2 = T_1 f$ for some linear map f, then M_{h_1} and M_{h_2} are equivalent extensions of $\{0\} \times A$ by A. **Hint:** $\psi : M_{h_1} \to M_{h_2}$ is defined by

$$\psi(a,x) = (a, x + f(a))$$

Modules (See Appendix 2 for way too much information)

Let A be an associative algebra. Let us recall that an A-**bimodule** is a vector space X, equipped with two bilinear products $(a,x) \mapsto ax$ and $(a,x) \mapsto xa$ from $A \times X$ to X satisfying, for every $a, b \in A$ and $x \in X$, the following axioms:

$$a(bx) = (ab)x, \quad a(xb) = (ax)b, \text{ and, } (xa)b = x(ab).$$

The space $A \oplus X$ is an associative algebra with respect to the product

$$(a,x)(b,y) := (ab, ay + bx).$$

Let A be a Jordan algebra. A **Jordan** A-**module** is a vector space X, equipped with two bilinear products $(a,x) \mapsto a \circ x$ and $(x,a) \mapsto x \circ a$ from $A \times X$ to X satisfying, for every $a, b \in A$ and $x \in X$, :

$$a \circ x = x \circ a, \quad a^2 \circ (x \circ a) = (a^2 \circ x) \circ a, \text{ and,}$$

$$2((x \circ a) \circ b) \circ a + x \circ (a^2 \circ b) = 2(x \circ a) \circ (a \circ b) + (x \circ b) \circ a^2.$$

The space $A \oplus X$ is a Jordan algebra with respect to the product

$$(a,x) \circ (b,y) := (a \circ b, a \circ y + b \circ x).$$

Derivations (into a module)

Let X be a A-bimodule over an (associative) Banach algebra A. A linear mapping $D : A \to X$ is said to be a **derivation** if $D(ab) = D(a)b + aD(b)$, for every a, b in A. For emphasis we call this a **binary (or associative) derivation**.

We denote the set of all binary derivations from A to X by $\mathcal{D}_b(A, X)$.

When X is a Jordan module over a Jordan algebra A, a linear mapping $D : A \to X$ is said to be a **derivation** if $D(a \circ b) = D(a) \circ b + a \circ D(b)$, for every a, b in A. For emphasis we call this a **Jordan derivation**.

We denote the set of Jordan derivations from A to X by $\mathcal{D}_J(A, X)$.

(What is a Lie-module and a Lie-derivation?)

Inner derivations

Let X be an A-bimodule over an associative algebra A. Given x_0 in X, the mapping $D_{x_0} : A \to X$, $D_{x_0}(a) = x_0 a - a x_0$ is a (associative or binary) derivation. Derivations of this form are called **inner**.

The set of all inner derivations from A to X will be denoted by $\mathcal{I}nn_b(A, X)$.

When x_0 is an element in a Jordan A-module, X, over a Jordan algebra A, for each $b \in A$, the mapping $\delta_{x_0,b} : A \to X$,

$$\delta_{x_0,b}(a) := (x_0 \circ a) \circ b - (b \circ a) \circ x_0, \ (a \in A),$$

is a derivation. Finite sums of derivations of this form are called **inner**.

The set of all inner Jordan derivations from A to X is denoted by $\mathcal{I}nn_J(A, X)$

(What is an inner Lie-derivation?)

COHOMOLOGY OF JORDAN ALGEBRAS[2]

(Comparisons) $n = 0$

ASSOCIATIVE

$f : A \to A$ is a constant function, say $f(x) = b$ for all x
$T_0(f) : A \to A$ is a linear function
$T_0(f)(x_1) = x_1 b - b x_1$

LIE

$f : A \to A$ is a constant function, say $f(x) = b$ for all x
$T_0(f) : A \to A$ is a linear function
$T_0(f)(x_1) = [b, x_1]$

JORDAN

$f \in A \times A$ is an ordered pair, say $f = (a, b)$
$T_0(f) : A \to A$ is a linear function
$T_0(f)(x_1) = a \circ (b \circ x_1) - b \circ (a \circ x_1)$

[2] For cohomology of ssociative algebras, see pp. 14-22 of this lecture; for cohomology of Lie algebras, see part 6 (pp. 57-74) of this series of lectures

$n = 1$

ASSOCIATIVE

$f : A \to A$ is a linear function
$T_1(f) : A \times A \to A$ is a bilinear function
$T_1(f)(x_1, x_2) = x_1 f(x_2) - f(x_1 x_2) + f(x_1) x_2$

LIE

$f : A \to A$ is a linear function
$T_1(f) : A \times A \to A$ is a skew-symmetric bilinear function
$T_1(f)(x_1, x_2) = -[f(x_2), x_1] + [f(x_1), x_2] - f([x_1, x_2])$

JORDAN

$f : A \to A$ is a linear function
$T_1(f) : A \times A \to A$ is a symmetric bilinear function
$T_1(f)(x_1, x_2) = x_1 \circ f(x_2) - f(x_1 \circ x_2) + f(x_1) \circ x_2$

$n = 2$

ASSOCIATIVE

$f : A \times A \to A$ is a bilinear function
$T_2(f) : A \times A \times A \to A$ is a trilinear function
$T_2(f)(x_1, x_2, x_3) = x_1 f(x_2, x_3) - f(x_1 x_2, x_3) - f(x_1, x_2 x_3) + f(x_1, x_2) x_3$

LIE

$f : A \times A \to A$ is a skew-symmetric bilinear function
$T_2(f) : A \times A \times A \to A$ is a skew-symmetric trilinear function

$$\begin{array}{rcl} T_2(f)(x_1, x_2, x_3) & = & [f(x_2, x_3), x_1] - [f(x_1, x_3), x_2] + [f(x_1, x_2), x_3] \\ & - & f(x_3, [x_1, x_2]) + f(x_2, [x_1, x_3]) - f(x_1, [x_2, x_3]) \end{array}$$

JORDAN

Postponed from part 7 (SUMMER 2013) to part 8 (FALL 2013) and again from part 8 to part 9 (today SPRING 2014) and again to part 10 (SUMMER 2014)

THE BIG PICTURE

INTERPRETATION OF COHOMOLOGY GROUPS

FIRST COHOMOLOGY GROUP
DERIVATIONS (AND INNER DERIVATIONS)

SECOND COHOMOLOGY GROUP
EXTENSIONS (AND SPLIT EXTENSIONS)

VANISHING THEOREMS

FOR EACH CLASS OF ALGEBRAS (ASSOCIATIVE, LIE, JORDAN), UNDER WHAT CONDITIONS IS $H^n(A) = 0$, ESPECIALLY FOR $n = 1, 2$

Extensions of Jordan algebras[3] [4] (pp.91-92)[5]

Let A and M be Jordan algebras. We shall denote Jordan products by juxtaposition. An **extension of A by M** is a short exact sequence

$$0 \to M \overset{\alpha}{\to} E \overset{\beta}{\to} A \to 0.$$

Thus α is an injective homomorphism and β is a surjective homorphism.

Extensions

$$0 \to M \overset{\alpha}{\to} E \overset{\beta}{\to} A \to 0 \text{ and } 0 \to M \overset{\alpha'}{\to} E' \overset{\beta'}{\to} A \to 0$$

are **equivalent** if there exists a homomorphism $\gamma : E \to E'$ such that $\alpha' = \gamma \circ \alpha$ and $\beta = \beta' \circ \gamma$. Thus γ is an isomorphism of E onto E'.

[3] The material which follows (not including Appendices 1 and 2) will be revised and presented in part 10 (SUMMER 2014)

[4] For extensions of associative algebras, see pp. 27-33 of this lecture

[5] Page numbers refer to the masterpiece "Structure and Representation of Jordan Algebras", by Nathan Jacobson 1968

An extension

$$0 \to M \overset{\alpha}{\to} E \overset{\beta}{\to} A \to 0.$$

is **split** (or **inessential**) is there exists a homomorphism $\delta : A \to E$ with $\beta \circ \delta = 1_A$. Thus $E = \delta(A) \oplus \alpha(M)$ as vector spaces and $\delta(A)$ is a subalgebra of E isomorphic to A.

Exercise 1

Prove the last statement.

An extension

$$0 \to M \overset{\alpha}{\to} E \overset{\beta}{\to} A \to 0.$$

is **null** if $M^2 = 0$, that is, all products in M are zero.

Let

$$0 \to M \overset{\alpha}{\to} E \overset{\beta}{\to} A \to 0.$$

be any extension and identify M with $\alpha(M) \subset E$. Then we may write $E = M \oplus \delta(A)$, a vector space direct sum, for some linear map $\delta : A \to E$ such that $\beta \circ \delta = 1_A$.

Exercise 2

Prove the last statement.

For $a, b \in A$, $h(a,b) := \delta(a)\delta(b) - \delta(ab) \in \ker \beta = M$ so $h : A \times A \to M$ is a bilinear map.

Exercise 3

M is a Jordan A-module under the module actions $a \cdot u = \delta(a)u$, $u \cdot a = u\delta(a)$ for $a \in A$ and $u \in M \subset E$. (Multiplication in E)

Outline of proof: E is an E-module and since M is an ideal in E, it is a submodule. If $M^2 = 0$ then[a] M is an E/M-module via $(e + M) \cdot u = eu$, $u \cdot (e + M) = ue$. Now use the isomorphism $\beta(e) \to e + M$ of A with E/M.

[a] Why is the assumption $M^2 = 0$ needed?

DEFINITION

Let M be a Jordan A-module. A bilinear map $h : A \times A \to M$ is a (Jordan) **2-cocycle** if it is symmetric and satisfies

$$(h(a,a)\cdot b)\cdot a + h(a^2,b)\cdot a + h(a^2 b,a) = a^2 \cdot h(b,a) + h(a,a)\cdot(ba) + h(a^2,ba).$$

A map $h : A \times A \to M$ is a (Jordan) **2-coboundary** if it is of the form

$$h(a,b) = \mu(ab) - a\cdot\mu(b) - \mu(a)\cdot b$$

for some linear map $\mu : A \to M$.

Exercise 4

Every Jordan 2-coboundary in a Jordan 2-cocycle.

DEFINITION

The vector space of all 2-cocycles modulo 2-coboundaries is denoted $H^2(A,M)$. (For emphasis, we can write $H^2_J(A,M)$)

THEOREM 12, p.94 of Jacobson's book

Let M be a Jordan A-module. Then there is a bijection of $H^2(A, M)$ and the set of equivalence classes of null extensions of A by M such that the associated bimodule structure on M given by Exercise 3 is the given one. In this correspondence the equivalence class of 0 in $H^2(A, M)$ corresponds to the isomorphism class of inessential extensions.

Outline of proof: Given a 2-cocycle h, $M \times A$ becomes a Jordan algebra with the product

$$(u_1, a_1)(u_2, a_2) = (u_1 \cdot a_2 + u_2 \cdot a_1 + h(a_1, a_2), a_1 a_2).$$

giving rise to the bijection.

Exercise 5

Fill in the calculations in the above outlined proof.

Jordan Matrix Algebras (pp.125-131)

Let D be a unital algebra with involution $j(d) = \overline{d}$. Then D_n denotes the algebra of n by n matrices with entries from D, with involution $X \mapsto X^J = \overline{X}^t$, and $H(D_n) \subset D_n^+$ denotes the subalgebra of symmetric elements.

Let e_{ij} be the usual matrix units in D_n and if $x \in D$, we identify x with the diagonal matrix in D_n all of whose diagonal entries are x. Then xe_{ij} is the matrix with x in the (i,j)-position and zeros elsewhere. We set $x[ij] = xe_{ij} + (xe_{ij})^J$.

Definition

Algebras of the form $H(D_n)$ which are Jordan algebras are called **Jordan matrix algebras**.

Theorem (THEOREM 1, p.127)

For $n \geq 3$, $H(D_n)$ is a Jordan algebra if and only if D is associative, or $n = 3$ and D is alternative with symmetric elements in the nucleus[a].

[a] At this time we shall not define alternative algebra or nucleus of an algebra

Solvable ideals and the radical (pp.192-196)

The powers J^{2^k} of a Jordan algebra J are $J^{2^0} = J$ and $J^{2^k} = (J^{2^{k-1}})^2$. J^2 is an ideal and J^{2^k} is a subalgebra. J is **solvable** if there exists an integer N with $J^{2^N} = 0$.

$$J^2 = 0,\ J^2J^2 = 0,\ (J^2J^2)(J^2J^2) = 0,\ ((J^2J^2)(J^2J^2))((J^2J^2)(J^2J^2)) = 0, \ldots$$

Lemma (Lemma 1, p.192)

For a Jordan algebra J,

- *If J contains a solvable ideal B such that J/B is solvable, then J is solvable.*
- *If B_1 and B_2 are solvable ideals, then $B_1 + B_2$ is a solvable ideal.*

If J is finite dimensional (more generally, if J satisfies the maximum condition for ideals), then it contains a solvable ideal R, the **radical** ($= \operatorname{rad} J$), such that R contains every solvable ideal of J. J is **semisimple** if $R = 0$ (J has no nonzero solvable ideals). Note that $J/\operatorname{rad} J$ is semisimple. (Proof: If S_1 is the radical of J/R, then $S_1 = S/R$ for some ideal S in J. Since S/R and R are solvable, so is S, so $S \subset R$ and $S_1 = 0$.)

The next two theorems are included for their intrinsic interest.

An algebra is **nilpotent** if there exists an integer N such that every product (in any association) of N elements is zero. A nilpotent Jordan algebra is solvable.

$$J^2 = 0,\ J^2J = 0.\ (J^2J)J = J^2J^2 = 0, \dots$$

$$ab = 0,\ (ab)c = 0,\ ((ab)c)d = (ab)(cd) = 0, \dots$$

Theorem (COROLLARY 1, p.195, Albert)

Any finite dimensional solvable Jordan algebra is nilpotent.

An algebra is **nil** if every element a in the algebra is nilpotent ($a^n = 0$ for some n depending on a)[a]. A solvable Jordan algebra is nil.

[a] A Jordan algebra is **power associative**, $a^k(a^m a^n) = (a^k a^m)a^n$

Theorem (THEOREM 3, p.196, Albert)

Any finite dimensional nil algebra is solvable.

$H_J^2(H(\mathbb{C}_n), M) = 0$

Theorem (Theorem 13, p. 292 (Albert-Penico-Taft))

Let E be a finite dimensional Jordan algebra, M an ideal in E such that $E/M \sim H(\mathbb{C}_n)$. Then there is a subalgebra R of E such that $E = R \oplus M$ as vector spaces. (Actually, you can replace $H(\mathbb{C}_n)$ by any semisimple algebra.)

Corollary (Corollary, p 292)

If M is a finite dimensional bimodule for $H(\mathbb{C}_n)$, then $H_J^2(H(\mathbb{C}_n), M) = 0$. In particular, $H_J^2(H(\mathbb{C}_n), H(\mathbb{C}_n)) = 0$.

Theorem (THEOREM 10, p.151)

Let J be a Jordan algebra with 1, N a nil ideal such that J/N is isomorphic to a Jordan matrix algebra $H(F_n)$ of order $n \geq 3$. Then J is isomorphic to a Jordan matrix algebra $H(D_n)$ where the ideal in $H(D_n)$ corresponding to N has the form $M_n \cap H(D_n)$ where M is an ideal in D and D/M is isomorphic to F as algebras with involution.

Lemma (Lemma 1, p 287)

Let J be a finite dimensional Jordan algebra with radical (= maximal solvable ideal) $\mathit{rad}\, J$. Then

1. *If B is an ideal in J, then $\mathit{rad}\, B = \mathit{rad}\, J \cap B$*
2. *If B is an ideal in J such that J/B is semisimple, then $\mathit{rad}\, B = \mathit{rad}\, J$*

Proof.

(1) $(\text{rad}\, J) \cap B$ is a solvable ideal in B, so $(\text{rad}\, J) \cap B \subset \text{rad}\, B$. Also,

$$B/(\text{rad}\, J \cap B) \sim (B + \text{rad}\, J)/\text{rad}\, J$$

is an ideal in the semisimple algebra $J/\text{rad}\, J$ and is therefore a direct summand and hence semisimple[a]. Then $B/(\text{rad}\, J \cap B)$ is semisimple and since $\text{rad}\, J \cap B \subset \text{rad}\, B$, $\text{rad}\, J \cap B = \text{rad}\, B$.
(2) Since $(B + \text{rad}\, J)/B \sim \text{rad}\, J/(B \cap \text{rad}\, J)$, $(B + \text{rad}\, J)/B$ is a solvable ideal in J/B, hence it is zero. Thus $B \supset \text{rad}\, J$. □

[a] See Kevin McCrimmon's book "A Taste of Jordan algebras" 2004, p. 502

Lemma (Reduction I, p.288)

If Theorem 13, page 292 is true for solvable M, then it is true for arbitrary M.

Proof.

Let E be a finite dimensional Jordan algebra, M an ideal in E such that $E/M \sim H(\mathbb{C}_n)$. If R_1 is the radical of M, then by (2) of Lemma 1 page 287 (see the previous page), R_1 is the radical of E and E/R_1 is semisimple. Now M/R_1 is an ideal in E/R_1 and so $E/R_1 = M/R_1 \oplus F/R_1$, where F/R_1 is an ideal isomorphic to $(E/R_1)/(M/R_1) \sim E/M$, which is semisimple, so R_1 is solvable. By assumption, there is a subalgebra R_2 of F with $F = R_1 \oplus R_2$ as vector spaces. Then $R_2 \sim F/R_1 \sim E/M$ and $R_2 \cap M \subset F \cap M \subset R_1$ since $M/R_1 \cap F/R_1 = 0$. So $R_2 \cap M \subset R_2 \cap R_1 = 0$ and by counting dimensions, $E = R_2 \oplus M$ as vector spaces. □

Lemma (Reduction II, p.288)

If Theorem 13, page 292 is true for solvable M with $M^2 = 0$, then it is true for arbitrary solvable M.

Proof.

Suppose that $M^2 \neq 0$. Then by Lemma 2, page 192 (see below), there is a nonzero solvable ideal $N \subset M$ with $N \neq M$. Then E/N has the solvable ideal M/N and $(E/N)/(M/N) \sim E/M \sim H(\mathbb{C}_n)$. By induction on the dimension, there is a subalgebra F/N of E/N with $E/N = (F/N) \oplus (M/N)$, where F is a subalgebra E containing N and $F/N \sim (E/N)/(M/N) \sim E/M \sim H(\mathbb{C}_n)$. Since $\dim F = \dim(E/M) + \dim N < \dim E$, by induction on the dimension there is a subalgebra $R \subset F$ with $F = R \oplus N$ and $R \sim F/N \sim H(\mathbb{C}_n)$ is semisimple. Since M is solvable we have $E = M \oplus R$. □

Lemma (Lemma 2, p.192, Penico)

For a finite dimensional Jordan algebra J with a solvable ideal B, define $B^{(k)}$ by $B^{(0)} = B$, $B^{(k)} = B^{(k-1)}B^{(k-1)} + (B^{(k-1)}B^{(k-1)})J$. Then the $B^{(k)}$ are ideals, $(B^{(k)})^2 \subset B^{(k+1)} \subset B^{(k)}$, and there exists an integer M such that $B^{(M)} = 0$.

Lemma (Reduction III, p.288)

If Theorem 13, page 292 is true for algebras E with a unit, then it is true for arbitrary E.

Proof.

Let E contain an ideal M such that $M^2 = 0$ and $E/M \sim H(\mathbb{C}_n)$. Let $E' = \Phi 1 \oplus E$ be the algebra obtained by adjoining a unit to E. (Φ is the underlying field.) Then M is a solvable ideal in E' and $E'/M \sim \Phi 1 \oplus (E/M)$ is semisimple. By our assumption, there is a subalgebra R' of E' such that $E' = R' \oplus M$. Since $M \subset E$, $E = E' \cap E = (E \cap R') \oplus M$ and $R := E \cap R'$ is a subalgebra. □

Lemma (Reduction IV, p.288-289)

If Theorem 13, page 292 is true for algebras E over an algebraically closed field[a]*, then it is true for arbitrary E*

[a] $\mathbb{R}$ is not algebraically closed, $\mathbb{C}$ is algebraically closed (fundamental theorem of algebra!)

Proof:

Theorem 13, page 292 is a statement about algebras over the real field. We shall show that if we complexify the short exact sequence

$$0 \to M \to E \to H(\mathbb{C}_n) \to 0, \tag{1}$$

and this complexified sequence splits, then so does the original one. For this we shall use the equivalence given by Theorem 12, page 94. Accordingly, let $h : H(\mathbb{C}_n) \times H(\mathbb{C}_n) \to M$ be a Jordan 2-cocycle (over the real field). We need to show that there is a linear map $\mu : H(\mathbb{C}_n) \to M$ such that

$$h(a, b) = \mu(ab) - \mu(a) \cdot b - \mu(b) \cdot a. \tag{2}$$

Let $u_1, \ldots, u_n$ be a basis for $H(\mathbb{C}_n)$ over $\mathbb{R}$ and $v_1, \ldots, v_r$ a basis for M over $\mathbb{R}$. Then (2) holds if and only if it holds for $a, b \in \{u_1, \ldots, u_n\}$. With μ provisionally defined by $\mu(u_i) = \sum_p \mu_{ip} v_p$, define the quantities $\eta_{ijq}, \ \ \gamma_{ijk}, \ \ \delta_{piq}$ by the formulas

$$h(u_i, u_j) = \sum_q \eta_{ijq} v_q, \quad u_i u_j = \sum_k \gamma_{ijk} u_k; \quad v_p \cdot u_i = \sum_q \delta_{piq} v_q.$$

Then (2) for $a = u_i$ and $b = u_j$ is equivalent to the set of linear equations

$$\eta_{ijk} = \sum_k \gamma_{ijk} \mu_{kq} - \sum_p \mu_{ip} \delta_{pjq} - \sum_p \mu_{jp} \delta_{piq}. \tag{3}$$

for the μ's in $\mathbb{R}$.

The solvability of (3) for the μ's in $\mathbb{R}$ is a necessary and sufficient condition that the extension splits. If we complexity the sequence (1), and extend the maps α, β, and h, we still have $(M^{\mathbb{C}})^2 = 0$, $H(\mathbb{C}_n)^{\mathbb{C}} = M_n(\mathbb{C})$ is semisimple, and $h^{\mathbb{C}}$ is a Jordan 2-cocycle. The bases $\{u_i\}$ and $\{v_j\}$ remain bases over the complex field. Assuming the theorem holds in the algebraically closed case, the equations (3) have a solution $\{\mu_{ip}\}$ in $\mathbb{C}$. Since these are linear equations with coefficients in $\mathbb{R}$, it follows that they have a solution in $\mathbb{R}$. **Q.E.D.**

We shall skip the proof of the following lemma, since $H(\mathbb{C}_n)$ is simple.

Lemma (Reduction V, p.289-290)

If Theorem 13, page 292 is true for algebras E with E/M simple, then it is true for arbitrary E (with E/M semisimple, that is).

The proof of Theorem 13, page 292, is now reduced to the following lemma!!

Lemma (Lemma 4, p 291)

Let E be a finite dimensional Jordan algebra with unit over an algebraically closed field and let M be an ideal in E such that $M^2 = 0$ and E/M is isomorphic to $H(\mathbb{C}_n)$. Then E contains a subalgebra isomorphic to $H(\mathbb{C}_n)$.

Proof.

Put $F = \mathbb{C}$ in Theorem 10, page 151. Thus E is isomorphic to a Jordan matrix algebra $H(D_n)$ where D has a unit and contains an ideal N with $D/N \sim \mathbb{C}$. Further, D contains a subalgebra $L = \mathbb{C}1$ isomorphic to $\mathbb{C}$. Thus $E \sim H(D_n)$ contains a subalgebra $H(L_n)$ isomorphic to $H(\mathbb{C}_n)$. □

THE END

Appendix 1–Equivalence classes and quotient groups

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

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

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 $(x,y) \in R$.

- $R = \{(x,y) \in \mathbb{R} \times \mathbb{R} : x < y\}$
- $R = \{(x,y) \in \mathbb{R} \times \mathbb{R} : y = \sin x\}$
- 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

$$\begin{aligned} \text{reflexive} \quad & (x,x) \in R \\ \text{symmetric} \quad & (x,y) \in R \Rightarrow (y,x) \in R \\ \text{transitive} \quad & (x,y),(y,z) \in R \Rightarrow (x,z) \in R \end{aligned}$$

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:

$$R = \{(\frac{a}{b}, \frac{c}{d}) : a, b, c, d \in \mathbb{Z}, b \neq 0, d \neq 0, ad = bc\}$$

- 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:
  $R = \{(x,y) \in \mathbb{R} \times \mathbb{R} : x - y$ is an integer$\}$
- integers modulo n:
  $R = \{(x,y) \in \mathbb{N} \times \mathbb{N} : x - y$ is divisible by $n\}$

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. $\mathbb{R}, +, 0, x^{-1} = -x$
2. positive real numbers, $\times, 1, x^{-1} = 1/x$
3. $\mathbb{R}^n$,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. $M_n(\mathbb{R}), +, 0, A^{-1} = [-a_{ij}]$
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. $G = \mathbb{R}, +, 0, x^{-1} = -x$;
   $H = \mathbb{Z}$ or $H = \mathbb{Q}$
2. $\mathbb{R}^n$,vector addition,$(0, \cdots, 0)$,
   $(x_1, \cdots, x_n)^{-1} = (-x_1, \cdots, -x_n)$;
   $H = \mathbb{Z}^n$ or $H = \mathbb{Q}^n$
3. $\mathcal{C}, +, 0, f^{-1} = -f$;
   $H = \mathcal{D}$ or $H =$ polynomials
4. $M_n(\mathbb{R}), +, 0, A^{-1} = [-a_{ij}]$;
   $H =$symmetric matrices, or
   $H =$anti-symmetric matrices

Appendix 2—What is a module?

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.

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 $\rightarrow$ 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.

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. 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

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 $\mathsf{f}: \mathsf{M} \rightarrow \mathsf{N}$ 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

1. **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.

2. **Cyclic module** A module is called a cyclic module if it is generated by one element.

3. **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.

4.**Projective** Projective modules are direct summands of free modules and share many of their desirable properties.

5. **Injective** Injective modules are defined dually to projective modules.

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

7. **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.

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

9. **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).

10. **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.

11. **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.

12.**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.

13. **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.

14. **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.