Abstract Algebra for Physicists[†]

J. Zeman

Department of Physics, The Johns Hopkins University

Baltimore, Maryland, 21218

Abstract. Certain recent models of composite hardons involve concepts and theorems from abstract algebra which are unfamiliar to most theoretical physicists. We summarize the algebraic apparatus needed for an understanding of these models. Particular emphasis is given to algebraic structures which are not assumed to be associative.

MASTER

[†] Research supported by the U. S. Energy Research and Development Administration under Contract No. E(11-1)3285.

NOTICE
This report was prepared as an account of work sponsored by the United States Government. Neither the United States nor the United States Energy Research and Development Administration, nor any of their employees, nor any of their contractors, subcontractors, or their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness or usefulness of any information, apparatus, product or process disclosed, or represents that its use would not infringe privately owned rights.

DISTRIBUTION OF THIS DOCUMENT UNLIMITED

See

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency Thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

DISCLAIMER

Portions of this document may be illegible in electronic image products. Images are produced from the best available original document.

I. Introduction

It has been proposed¹ that the somewhat mysterious composite nature of hadrons (supposedly made up of constituents which are themselves unobservable) may be understood through a suitable algebraic generalization of quantum theory.

The algebraic concepts involved in the papers of ref. 1, though well-known to most mathematicians, are generally unfamiliar to particle theorists, primarily because most algebraic structures previously encountered in physics are associative (Lie algebras being an important exception).

The purpose of these notes is to present the basic mathematical background needed for an understanding of non-associative algebras, thus making the ideas involved in ref. 1 accessible to a larger group of physicists.

II. Abstract Algebra

The basic algebraic structure in our discussion is a group, which is a non-empty set G and a binary operation, "+" which satisfies

- 1.) for every a, b in G , there exists a unique c such that $a + b = c$.
- 2.) for every a, b, c in G , $(a + b) + c = a + (b + c)$ (the associative law)
- 3.) There is an element 0 in G such that $a + 0 = 0 + a = a$ for a in G
(such an element is called an identity)
- 4.) for every a in G there is an element, $(-a)$ in G such that $a + (-a) = -a + a = 0$ (the inverse).

A group is commutative if in addition to 1) through 4),

- 5.) $a + b = b + a$ for all a, b in G .

We don't pause to review the basic results of group theory, but only remark that a good deal is known about the structure of groups, especially those of finite order.

In part because of the fruitfulness of the group axioms, a number of systems with weakened axioms have been defined. Four of these systems are of

interest to us.

The weakest structure is that of a groupoid, where we assume only that a binary operation is defined (property (1) of a group) with no further restrictions. An associative groupoid is called a semigroup.

Before we consider the remaining two structures, we point out that the existence of the inverse and the associative law for groups guarantees that for every $a, b \in G$ there is a unique x, y such that

$$a + x = b \quad (\text{let } x = -a + b)$$

$$y + a = b \quad (\text{let } y = b - a).$$

We choose this property as the defining property of a quasigroup. That is, a quasigroup Q is a set endowed with a binary operation (i.e., it is a groupoid) such that the two equations above have unique solutions for every a, b in Q . A quasigroup with identity is called a loop. Since a loop has identity, each element a has a left (right) inverse, which is the solution to the equation $x + a = 0$ ($a + y = 0$). Finally an associative loop is a group (Fig. 1). As an illustrative exercise, we show that an associative quasigroup is a group. We show first that an associative quasigroup Q possesses a right identity. Let a be any element of Q . There is a unique 0 in Q such that

$$a + 0 = a$$

Let b be any other element of Q , and let c be the unique element of Q such that

$$b = c + a. \quad \text{Then}$$

$$b + 0 = (c + a) + 0 = c + (a + 0) = c + a = b$$

and 0 is a right identity. Thus $0 + 0 = 0$. In fact, 0 is the only element with this property. Let $x + x = x$. There is some x^* in Q such that $x + x^* = 0$.

We have

$$0 = x + x^* = (x + x) + x^* = x + (x + x^*) = x + 0 = x$$

We now verify that if $a + a^* = 0$, then $a^* + a = 0$ by computing

$$\begin{aligned}
 (a^* + a) + (a^* + a) &= [(a^* + a) + a^*] + a \\
 &= [a^* + (a + a^*)] + a \\
 &= [a^* + 0] + a \\
 &= a^* + a
 \end{aligned}$$

Thus, $a^* + a = 0$ as 0 is the only idempotent. Finally, we show that 0 is also a left identity, $0 + a = a$. Proof: Let $a + a^* = 0$. Then $a^* + a = 0$, so

$$a = a + 0 = a + (a^* + a) = (a + a^*) + a = 0 + a$$

and we have verified all the axioms of a group.

We next consider sets with two operations $\langle R, +, \cdot \rangle$ and define a Ring as a set with two operations such that

- 1.) $\langle R, + \rangle$ is a commutative group
- 2.) $\langle R, \cdot \rangle$ is a groupoid
- 3.) $a \cdot (b + c) = a \cdot b + a \cdot c$, and $(a + b) \cdot c = a \cdot c + b \cdot c$ for all a, b, c in R

Examples of rings abound: let R be any commutative group, and define $ab = 0$ for every a, b in R . Then $\langle R, +, \cdot \rangle$ is a ring, called the zero ring. A non-trivial example is the integers under the usual addition and multiplication.

Note that our definition is not that found in most introductory texts, especially older ones, which consider only associative rings (i.e., ones in which $\langle R, \cdot \rangle$ is a semigroup). In the literature, rings which are not assumed to be associative are sometimes termed non-associative.

We define a useful function of three variables x, y, z , the associator

$$A(x, y, z) = (xy)z - x(yz)$$

which measures the amount by which the three elements "miss" being associative.

(Similarly, define the commutator of two elements $[x, y] = xy - yx$). The nucleus N is the set of all elements n which associate with every other pair of elements: $A(n, x, y) = A(x, n, y) = A(x, y, n) = 0$. The center C is the set of all elements of the nucleus which commute with every element of the ring. If $N = R$, the ring

is associative; if $C = R$, it is associative and commutative.

A division ring is a ring whose non-zero elements form a loop under multiplication. Thus, if $a \neq 0$, both

$$ax = b$$

$$ya = b$$

have unique solutions. In the case of interest to us (finite dimensional division algebras) this is equivalent to the statement that $ab = 0$ only if $a = 0$ or $b = 0$. In general, an associative commutative division ring is a field; in other words, a field is a ring whose non-zero elements form a group under multiplication.

(Fig. 2)

Actually, the study of non-associative rings per se is inessential in that any simple non-associative ring is actually a non-associative algebra, a fact we do not prove here².

As an aside, we note that each element of a ring defines two homomorphisms of the additive group of a ring into itself. (A homomorphism of a group is a mapping of the group into another group which preserves the group operation.

I. e., if a is in G , then $f(a)$ is in G' and

$$f(a+b) = f(a) + f(b)$$

for all a, b in G .) One of these homomorphisms is left multiplication $l_a: x \mapsto l_a(x)$ where $l_a(x) = ax$. This is a homomorphism by the distributive property of the ring: $l_a(x + y) = a(x + y) = ax + ay = l_a(x) + l_a(y)$. Similarly, we define $r_a: x \mapsto r_a(x) = xa$. In addition, we have

$$(l_a + l_b)(x) = l_a(x) + l_b(x)$$

and, if R is associative

$$(l_a l_b)(x) = l_a(l_b(x)).$$

A module is an additive commutative group G and a ring of operators R on the group such that if a, b , are elements of G and f, g elements of R

- 1.) $f(a + b) = f(a) + f(b)$
- 2.) $(f + g)(a) = f(a) + g(a)$
- 3.) $(fg)(a) = f(g(a)).$

Thus we have seen that any associative ring is a module. Similarly, if R is a ring and R' is a subring (a subset that is itself a ring) of the nucleus, then R' is a module over the additive group $\langle R, + \rangle$. Another (trivial) example is the following: let R be any ring, G any group, and let the operator associated with any element a of R map every element x of G into the identity of G ; $a(x) = 0$.

An important class of modules are those in which the operators map the group onto itself. Thus, for any x in G , there is an a in R and an f in G such that $f(a) = x$. Such modules are called unitary. A unitary module where the ring is an (associative) division ring is called a vector space.

The vector spaces with which physicists are most familiar are vector spaces over the fields of real and complex numbers. However, upon a little reflection, one realizes that the commutativity of the multiplication of the coefficients of vectors is rarely used in an essential way, thus we have relaxed this requirement in the definition.

We will deal only with finite dimensional vector spaces. If $\{e_i\}_1^n$ is a basis, we may write any vector as

$$\xi = \sum \xi_i e_i$$

and the componentwise addition and multiplication of scalars is equivalent to that of the system of n -tuples (we identify $e_1 = (1, 0, 0 \dots 0)$, etc.) that physicists ususally think of when dealing with vectors.

For our last definition, an algebra A is a vector space that is itself a ring, whose multiplication satisfies

$$\alpha(xy) = (\alpha x)y = x(\alpha y)$$

for each x, y in A , and every coefficient α . Thus multiplication between any two vectors is defined (and is a vector). If two vectors are expanded in terms

of a basis $x = \sum_{i=1}^n \xi_i e_i$, $y = \sum_{j=1}^n \eta_j e_j$, then

$$\begin{aligned} xy &= \left(\sum_{i=1}^n \xi_i e_i \right) \left(\sum_{j=1}^n \eta_j e_j \right) \\ &= \sum_{ij} (\xi_i e_i) (\eta_j e_j) \text{ by distributive law} \\ &= \sum_{ij} (\xi_i \eta_j) (e_i e_j) \text{ by def. algebra} \end{aligned}$$

since $\xi_i \eta_j$ is an element of the coefficient division ring, we see that we need only specify the multiplication of basis vectors to determine the entire algebra. For finite algebras, it is convenient to do so by means of a Cayley table,

$$\begin{array}{c|ccc} & e_1 & e_2 & e_3 \dots \\ \hline e_1 & \sum \gamma_{11k} e_k & \dots & \\ e_2 & \vdots & & \\ e_3 & & & \end{array}$$

where the γ_{ijk} are elements of the coefficient ring. An algebra is termed associative, commutative, etc. as its multiplication is associative, etc. Clearly, we need verify these properties for the basis elements only.

Once the Cayley table is specified, a whole class of algebras is defined with different division rings as the coordinates of the vector space (as long as all the γ_{ijk} are in the ring itself). In particular, we examine the following tables:

	1
1	1

	1	i
1	1	i
i	i	-1

	1	i	j	k
1	1	i	j	k
i	i	-1	k	-j
j	j	-k	-1	i
k	k	j	-i	-1

	1	e ₁	e ₂	e ₃	e ₄	e ₅	e ₆	e ₇
1	1	e ₁	e ₂	e ₃	e ₄	e ₅	e ₆	e ₇
e ₁	e ₁	-1	-e ₃	e ₂	-e ₅	e ₄	e ₇	-e ₆
e ₂	e ₂	e ₃	-1	-e ₁	-e ₆	-e ₇	e ₄	e ₅
e ₃	e ₃	-e ₂	e ₁	-1	-e ₇	e ₆	-e ₅	e ₄
e ₄	e ₄	e ₅	e ₆	e ₇	-1	-e ₁	-e ₂	-e ₃
e ₅	e ₅	-e ₄	e ₇	-e ₆	e ₁	-1	e ₃	-e ₂
e ₆	e ₆	-e ₇	-e ₄	e ₅	e ₂	-e ₃	-1	e ₁
e ₇	e ₇	e ₆	-e ₅	-e ₄	e ₃	e ₂	-e ₁	-1

These are the tables of the reals, complexes, quaternions, and octonions, respectively. (The quaternions are associative, and therefore can be represented by matrices. In fact, $-i\sigma_1$, where σ_1 is the Pauli spin matrix, has the correct algebra. Thus, quaternions have been used in physics for some time. Octonions are non-associative, and therefore not representable in terms of real or complex matrices.) It is a remarkable fact that these algebras are the only finite dimensional division algebras over the reals³. They are also the only finite normed algebras over the reals, which we shall show in the next section.

III. Non-Associative Algebras

Modern mathematics is almost relentlessly axiomatic. As Wigner states⁴, "mathematics is the science of skillful operations with concepts and rules invented just for this purpose". However, the motivation for much of the developments of mathematics has been interesting special problems, frequently of a physical nature. We here consider two such problems that motivated research into non-associative algebras.

As is well known, complex numbers may be associated with points in a plane, addition of complex numbers being equivalent to component-wise addition of points. Then complex multiplication is equivalent to defining

$$(a,b) (c,d) = (ac - bd, ad + bc).$$

The points of the plane under these definitions thus form a field.

To any complex number z (or point) we define a conjugate $\bar{z}$ (the conjugate of (a,b) is $(a, -b)$). Then

$$z\bar{z} = a^2 + b^2$$

is the square of the length of z . We define the norm of z

$$|z| \equiv \sqrt{z\bar{z}}$$

we have $\overline{(z_1 z_2)} = \bar{z}_1 \bar{z}_2$, so

$$\begin{aligned} |z_1| |z_2| &= (z_1 \bar{z}_1) (z_2 \bar{z}_2) \\ &= [(z_1 \bar{z}_1) z_2] \bar{z}_2 \\ &= [z_1 (\bar{z}_1 z_2)] \bar{z}_2 \\ &= [z_1 (z_2 \bar{z}_1)] \bar{z}_2 \\ &= [(z_1 z_2) \bar{z}_1] \bar{z}_2 \\ &= (z_1 z_2) (\bar{z}_1 \bar{z}_2) = (z_1 z_2) \overline{(z_1 z_2)} = |z_1 z_2| \end{aligned}$$

where we have used the associativity and commutativity of complex numbers. The

norm of the product is equal to the product of the norms is thus responsible for the following identity for real numbers

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2.$$

The question we wish to consider is the generalization of these observations. When can multiplication of points be defined to give a field? When can the product of sums of squares be given by sums of squares?

Hamilton⁵ showed that the quaternions solved both problems for $n = 4$.

In the notation of points

$$(a_1, a_2, a_3, a_4) (b_1, b_2, b_3, b_4) = (A_1, A_2, A_3, A_4)$$

where

$$A_1 = a_1 b_1 - a_2 b_2 - a_3 b_3 - a_4 b_4$$

$$A_2 = a_1 b_2 + a_2 b_1 + a_3 b_4 - a_4 b_3$$

$$A_3 = a_1 b_3 - a_2 b_4 + a_3 b_1 + a_4 b_2$$

$$A_4 = a_1 b_4 + a_2 b_3 - a_3 b_2 + a_4 b_1.$$

The quaternions, being a division ring, satisfy all the properties of a field, except commutativity of multiplication. (These observations follow quickly from the representation of quaternions as spin matrices.) Turning to the second question, we define

$$\bar{q} = (a_1, -a_2, -a_3, -a_4).$$

Then $q\bar{q} = a_1^2 + a_2^2 + a_3^2 + a_4^2 \equiv |q|$, and

$$\begin{aligned} |q_1| |q_2| &= (q_1 \bar{q}_1) |q_2| = q_1 (\bar{q}_1 |q_2|) = q_1 (|q_2| \bar{q}_1) = q_1 ((q_2 \bar{q}_2) \bar{q}_1) \\ &= q_1 (q_2 (\bar{q}_2 \bar{q}_1)) = (q_1 q_2) (\bar{q}_2 \bar{q}_1) = (q_1 q_2) \overline{(q_1 q_2)} = |q_1 q_2| \end{aligned}$$

where we have used associativity, the fact that the norm is a real number and

therefore commutes with every quaternion, and the fact that $\overline{q_1 q_2} = \overline{q_2} \overline{q_1}$, which follows from the usual $(AB)^{-1} = B^{-1} A^{-1}$ for matrices, and the fact that $\overline{q} = |q| q^{-1}$. Thus we have the relation

$$(a_1^2 + a_2^2 + a_3^2 + a_4^2)(b_1^2 + b_2^2 + b_3^2 + b_4^2) = A_1^2 + A_2^2 + A_3^2 + A_4^2$$

with A_i given above. This relation, discovered by Euler some 70 years before, was used to prove the fact that any positive integer may be written as the sum of four squares⁶.

Recalling the definitions given earlier, we can rephrase our problems. For the second question, we need the concept of a normed algebra. If we consider any finite algebra, we can define the norm of a vector with respect to that basis as the sum of the coefficients squared of the vector in question. An algebra is normed if there exists a basis in which the product of norms is the norm of the product. Thus, with axiomatic hindsight, we wish to find all division algebras, and all normed algebras, over the reals⁷.

We notice first that a normed algebra over the reals is necessarily a division algebra. We have seen that the multiplication by an element of a ring is an operation which maps the additive group of the ring onto a subgroup. Similarly, the multiplication by an element of an algebra maps the vector space of the algebra onto a subvector space. Thus, the left and right multiplications by a fixed element are linear transformations of a vector space, L_a and R_a .

In a normed algebra,

$$|ab| = |a| |b|.$$

Thus $ab = 0$ implies $|a| = 0$ or $|b| = 0$. In a real algebra $0 = |a| = \sum_{i=1}^n a_i^2$ implies $a_i \equiv 0$. So, $ab = 0$ implies $a = 0$ or $b = 0$. Thus, if $a \neq 0$,

$L_a(b) = 0$ implies $b = 0$. Therefore, the inverse vector space transformation exists, and $ax = b$ has a unique solution $L_a^{-1}(b)$. Similarly for $ya = b$. Thus, a normed algebra over the reals is a division algebra. (Note: for fields other than the reals this proof fails as it is not necessarily true that $\sum_{i=1}^n a_i^2 = 0$

implies $a_1 \equiv 0$.)

At about the same time as Hamilton discussed quaternions, Cayley⁸ showed that there was a solution for $n = 8$. The octonions are neither commutative nor associative, but in a sense they are "almost" associative. The octonions are alternative, which means that

$$A(a, a, b) = A(a, b, b) = 0$$

for any a, b . These identities can be shown to imply that the subalgebra generated by any two elements of an alternative algebra is associative.

A number of erroneous solutions were published⁹ for $n = 16$, until Hurwitz showed that the only normed algebras over the reals are the ones we have described. The more general case of arbitrary fields has been solved in two papers by Albert¹⁰. With slight variations in the tables, they are again complex, quaternion, and octonion algebras.

The problem of determining all finite dimensional division rings over the reals has recently yielded to very powerful techniques of algebraic topology. In 1958 it was shown¹¹ that such an algebra must be of dimension 1, 2, 4, or 8. Although we have division algebras of these dimensions, they are not the only ones; however, they are the only alternative ones¹².

We give a proof of Hurwitz's theorem. This serves two purposes: first, it is an interesting theorem in itself, and second, the proof is similar in style to many of the purely algebraic proofs in the theory of non-associative algebras. We do not prove the more difficult results on division algebras because, as we have noted above, the necessary techniques would take us far afield.

First we show that any normed algebra may be taken to possess an identity. Let e be an element whose norm is 1. Then

$$|ex| = |e| |x| = |x| = |x| |e| = |xe|,$$

and R_e and L_e are length preserving. Obviously, $e \neq 0$, so R_e^{-1} and L_e^{-1} exist

and are length preserving. We define a new multiplication $*$ such that

$$x * y = (R_e^{-1}(x)) (L_e^{-1}(y)).$$

and define a new element $1 \equiv e^2$. Then

$$1 * y = e^2 * y = (R_e^{-1}(e^2)) (L_e^{-1}(y))$$

$$= (e) (L_e^{-1}(y))$$

$$= y$$

and $y * 1 = y * e^2 = (R_e^{-1}(y)) (L_e^{-1}(e^2))$

$$= (R_e^{-1}(y)) (e)$$

$$= y$$

Finally, we show that the algebra is still normed

$$|x * y| = |(R_e^{-1}(x)) (L_e^{-1}(y))|$$

$$= |R_e^{-1}(x)| |L_e^{-1}(y)|$$

$$= |x| |y|.$$

Henceforth, without loss of generality, we consider only algebras with identity.

Algebras are vector spaces, so we introduce the familiar dot product of two vectors

$$(a, b) = \sum_{i=1}^n a_i b_i.$$

Obviously $|a| = (a, a)$. Also we have $(a, b) = \frac{1}{2} (|a + b| - |a| - |b|)$. I

By using $|(a + a') b| = |a + a'| |b|$ we have $(ab, a'b) = (a, a') |b|$. II

Similarly, $(ab, a'b') + (ab', a'b) = 2 (a, a') (b, b')$ III

$(ab, ab') = |a| (b, b')$. IV

In any algebra, we use the notation $[x]$ for the one-dimensional subspace generated by the element x . $[x] = \{\alpha x, \alpha \text{ in } F\}$. For any subspace W ,

$$W \oplus W^\perp = A$$

where $\oplus$ denotes the vector space direct sum, and $W^\perp$ is $\{a \text{ in } A \text{ such that } (a, w) = 0 \text{ for every } w \text{ in } W\}$.

In particular, in a normed algebra A ,

$$A = [1] \oplus [1]^\perp.$$

I. e., if a is any element of A

$$a = \alpha \cdot 1 + b$$

where α is real, b is in $[1]^\perp$, and both α and b are unique (this is what we mean by a vector space direct sum). Define

$$\bar{a} = \alpha \cdot 1 - b,$$

and note that $\bar{\bar{a}} = a$. We wish to show that

$$\overline{ab} = \bar{b} \bar{a}$$

(this is the relation we had for quaternions.)

We use formula III, in the special case that $a' = 1$ and $a \in [1]^\perp$. Then

$$(ab, b') + (ab', b) = 0, \text{ for any } b, b'. \quad (A)$$

Similarly, for $b' = 1$, b in $[1]^\perp$ we have $(ab, a') + (a, a'b) = 0$, for any a, a' .

(B)

Next, for γ real number, b, b' arbitrary,

$$((\gamma \cdot 1) b, b') - (b, (\gamma \cdot 1) b') = 0.$$

Adding (A) to this we have

$$(ab, b') - (b, \bar{a} b') = 0$$

for any a, b, b' . Similarly, using (B)

$$(ab, a') - (a, a' \bar{b}) = 0.$$

Thus

$$(ab, b') = (b, \bar{a} b') = (b \bar{b}', \bar{a}) = (\bar{b}', \bar{b} \bar{a}).$$

Letting $a = 1$ implies $(b, b') = (\bar{b}', \bar{b})$, so $(ab, b') = (\bar{b}', \bar{ab})$.

But we have

$$(ab, b') = (\bar{b}', \bar{b} \bar{a}).$$

Since $(\ , \)$ is non-degenerate, and b' is arbitrary, we have

$$\overline{ab} = \overline{b} \overline{a} \text{ for any } a, b,$$

as we wished to show.

Obviously, those elements left fixed by the map $a \rightarrow \overline{a}$ (called an involution) are just $[1]$. Thus, since

$$\overline{a \overline{a}} = \overline{\overline{a} a} = a \overline{a}$$

is left fixed, $a \overline{a} = \gamma \cdot 1$, γ some real number. Then

$$\gamma = (\gamma \cdot 1, 1) = (a \overline{a}, 1) = (a, a) = |a|$$

shows

$$a \overline{a} = |a| \cdot 1,$$

a fact most physicists would take for granted. Also, $a + \overline{a} = T(a) \cdot 1$, where $T(a)$ is a real linear function on the algebra A .

We have proved the last part of the following

Theorem: Let A be a normed algebra with identity (1) over the reals. Then A is an alternative algebra with an involution $a \rightarrow \overline{a}$ such that for all a in A ,

$$a \overline{a} = |a| \cdot 1$$

$$a + \overline{a} = T(a) \cdot 1, T(a) \text{ real}$$

$[1]$ is unchanged by the involution, while $[1]^\perp$ is the set of elements such that $\overline{a} = -a$.

We complete the proof by showing that A is alternative. We have seen that

$$(ax, ab) = (x, \overline{a} (ab)).$$

On the other hand, IV implies

$$(ax, ab) = |a| (x, b) = (x, |a| b) = (x, (\overline{a} a) b)$$

Thus,

$$\overline{a} (ab) = (\overline{a} a)b.$$

By the definition of an algebra

$$\alpha(ab) = (\alpha a) b$$

for any real number α . In particular, let $\alpha = a + \overline{a}$, and subtract the

previous relation to obtain

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

This may be written $A(a, a, b) = 0$. By a similar process, we show $A(a, b, b) = 0$.

We prove next a partial converse to the above theorem.

Theorem: Let A be an alternative algebra with identity over the reals with an involution $a \rightarrow \bar{a}$ such that for all a in A

$$a\bar{a} = |a| \cdot 1$$

$$a + \bar{a} = T(a) \cdot 1, T(a) \text{ real.}$$

Then $|ab| = |a| |b|$. (I.e., then A is a normed algebra).

This is just the procedure we used to prove that the quaternions are a normed algebra; this time we assume only alternativity, instead of associativity.

The alternative laws are:

$$A(a, a, b) = 0$$

$$A(a, b, b) = 0.$$

Substituting $a = x + y$ in first and $b = x + y$ in the second gives

$$A(x, y, b) = -A(x, b, y) \text{ and } A(a, y, x) = -A(a, x, y).$$

(These relations supply the reason for the term alternative: the associator "alternates". I.e., if σ is a permutation of 1, 2, 3, $A(x_{1\sigma}, x_{2\sigma}, x_{3\sigma}) = (\text{sign } \sigma) (x_1, x_2, x_3)$.)

Combining the last two relations, we have

$$A(x, y, b) = A(b, x, y),$$

V

which implies

$$A(b, y, b) = A(b, b, y) = 0.$$

VI

Writing V out we have

$$x(yb) + (bx)y = (xy)b + b(xy).$$

Replace x by bx , and replace y by yb , and add the two equations to give

$$\begin{aligned}
 & (bx)(yb) + (b(bx))y + x((yb)b) + (bx)(yb) \\
 &= ((bx)y)b + b((bx)y) + (x(yb))b + b(x(yb)) \\
 &= b((bx)y + x(yb)) + ((bx)y + x(yb))b
 \end{aligned}$$

VII

Now VI implies $b((xy)b) = (b(xy))b$, so there is no ambiguity in writing $b(xy)b$ for both. Then VII becomes

$$(b^2 x)y + 2(bx)(yb) + x(yb^2) = b^2(xy) + 2b(xy)b + (xy)b^2.$$

If we let $b \rightarrow b^2$ in V and subtract from the last relation, we have

$$(bx)(yb) = b(xy)b$$

This important result is called the Moufang identity. With this result, we can prove the above theorem, that any alternative algebra with involution such that $a\bar{a} = |a| \cdot 1$, $a + \bar{a} = T(a) \cdot 1$, is normed. As before, alternativity and the fact that $a + \bar{a} \in [1]$ implies that

$$(a\bar{a})b = a(\bar{a}b) \quad \text{and} \quad a(b\bar{b}) = (ab)\bar{b}.$$

So

$$\begin{aligned}
 |a|b \cdot 1 &= (ab)(\bar{b}\bar{a}) \\
 &= (ab)(\bar{b}(T(a) \cdot 1 - a)) \\
 &= T(a)(ab)\bar{b} - (ab)(\bar{b}a) \\
 &= T(a)(a(b\bar{b})) - a(b\bar{b})a \\
 &= T(a)(a|b|) - a|b|a \\
 &= a(T(a) - a)|b| \\
 &= a(\bar{a})|b| = |a||b|
 \end{aligned}$$

We can now construct all normed algebras over the reals. To do this, we use a generalization of the procedure used to create the complexes from the reals. Let A be a normed algebra. Then consider pairs of elements of A and define

$$(a, b)(c, d) = (ac - \bar{d}b, da + \bar{b}c).$$

The algebra B so generated has dimension twice that of A . The element $(1, 0)$

is the identity in B, and if $j \equiv (0, 1)$, then

$$j^2 = -1$$

Every element may be written in the form $a + bj$, where a and b are elements of A.

In this notation

$$(a + bj)(c + dj) = ac - \bar{d}b + (da + \bar{b}c)j.$$

B is associative if and only if A is commutative, as may be easily verified.

For $x = a + bj$, define $\bar{x} = \bar{a} - bj$. Then $\bar{\bar{x}} = x$, and

$$\overline{xy} = \bar{y} \bar{x}$$

follows from the definition of multiplication.

$$\begin{aligned} \bar{xx} &= (a + bj)(\bar{a} - bj) \\ &= (a\bar{a} + b\bar{b}) \cdot 1 = |x| \cdot 1 \end{aligned}$$

Also $x + \bar{x} = a + \bar{a} = T(a) \cdot 1$. Thus, if B is alternative, then it is normed.

Since $x + \bar{x}$ is in [1], we need again show only

$$A(x, \bar{x}, y) = A(y, x, \bar{x}) = 0.$$

But

$$\begin{aligned} \overline{A(y, x, \bar{x})} &= \overline{(yx)\bar{x} - y(xx)} \\ &= x(\bar{xy}) - (\bar{xx})\bar{y} \\ &= -A(x, \bar{x}, y) \end{aligned}$$

shows that the second associator is zero if the first is.

Calculating, we have (for $x = a + bj$, $y = c + dj$)

$$\begin{aligned} x(\bar{xy}) &= x[(\bar{a}c + \bar{d}b) + (\bar{d}a - \bar{b}c)j] \\ &= a(\bar{a}c + \bar{d}b) - (\bar{a}d - \bar{c}b)b + [(\bar{d}a - \bar{b}c)a + b(\bar{c}a + \bar{b}d)]j \\ &= (|a| + |b|)(c + dj) - A(a, \bar{d}, b) - A(b, \bar{c}, a)j \\ &= (\bar{xx})y - A(a, \bar{d}, b) - A(b, \bar{c}, a)j \end{aligned}$$

Since a, b, c, d are arbitrary, B is alternative if and only if A is associative. Thus, if we apply this procedure to the reals we get complexes, then quaternions, then octonions. The 16-dimensional algebra generated by this method

is not alternative, and therefore not normed.

Parenthetically, we note that we can generalize this procedure somewhat by defining the multiplication in B to be

$$(a, b)(c, d) = (ac + \mu \bar{d}b, ca + \bar{b}c)$$

where μ is some element of the underlying coefficient division ring (in the present case, a real number). Once again, $(1, 0)$ is the identity, but if $v = (0, 1)$, then

$$v^2 = \mu 1.$$

Again, the conjugate of $a + vb$ is

$$\bar{a} - vb,$$

and $\overline{xy} = \bar{y} \bar{x}$. B is associative if A is commutative, and alternative if A is associative. The eight-dimensional algebras constructed in this way are called Cayley-Dickson algebras. They are all alternative, and depend on three constants μ_1, μ_2, μ_3 . For $\mu_1 = \mu_2 = \mu_3 = -1$ we have the octonions. $\mu_1 = \mu_2 = -\mu_3 = -1$ is the split Cayley algebra discussed in the papers of footnote 1.

We can now complete the proof of Hurwitz's theorem, that is, that the complexes, quaternions, and octonions are the only normed algebras over the reals. To do so, we will use the notion of a subalgebra containing the identity. Such an algebra is sent into itself by the involution $a \rightarrow \bar{a}$.

Let A be any normed algebra, A_1 a subalgebra (containing 1). Then

$$A = A_1 \oplus A_1^\perp.$$

Suppose $A_1 \neq A$. Then there is some j in $A_1^\perp$ such that $|j| = 1$. $[1] \subset A_1 \Rightarrow A_1^\perp \subset [1]^\perp$, so

$$\bar{j} = -j,$$

and $j^2 = -1$. If we substitute $x \rightarrow x + y$ in

$$x\bar{x} = |x| \cdot 1$$

we get

$$\overline{xy} + \overline{yx} = 2(x, y) \cdot 1.$$

For a in A_1 , this reads

$$aj = j\overline{a}.$$

If a and b are in A_1

$$(a, bj) = (\overline{ba}, j) = 0$$

shows that A_1j is in $A_1^\perp$. Also

$$(aj, bj) = ((aj)\overline{j}, b) = (a(j\overline{j}), b) = (a, b)$$

shows that $a \mapsto aj$ is a 1 - 1 linear transformation. Thus A_1 and A_1j have the same dimension as vector spaces.

From the relation

$$a(\overline{a}x) = (a\overline{a})x = |a|^2x,$$

we have, replacing a by $a + b$,

$$a(\overline{b}x) + b(\overline{a}x) = 2(a, b)x.$$

With $b = j$, and a and x in A_1 , this gives

$$a(\overline{j}x) + j(\overline{a}x) = 0,$$

or $a(jx) = j(\overline{a}x)$; which in turn implies $a(\overline{x}j) = (\overline{x}a)j$.

Thus, we have

$$a(bj) = (ba)j$$

VIII

Taking conjugates gives

$$(ja)b = j(ba)$$

IX

Finally, using the Moufang identity at the appropriate step

$$\begin{aligned} (aj)(bj) &= (j\overline{a})(bj) = j(\overline{a}b)j = (\overline{b}a)j^2 \\ &= -\overline{ba}. \end{aligned}$$

X

VIII, IX and X show that $A_1 + A_1j$ is a subvector space of A closed under multiplication. Thus, it is a subalgebra itself. In fact, it is the algebra

we would generate from A_1 using the construction given previously. Thus, consider [1]. This is a subalgebra. If $A = [1]$, we are done. If not, A contains the complexes. If $A \neq \mathbb{C}$, then A contains the quaternions. If $A \neq \mathbb{Q}$, then A contains the octonions. Finally, if $A \neq 0$, it contains the 16 dimensional algebra generated by the octonions. But this algebra is not alternative, therefore A is not normed, a contradiction. Thus, the only normed algebras over the reals are the ones whose Cayley tables are given in the second section.

Throughout our proofs, we have made extensive use of the identities satisfied by the multiplication in an algebra. More generally, identities have become a crucial tool in the study of non-associative algebras. Their importance can be traced to two facts. First, any subalgebra, any homomorphic algebra, and the direct sum of any number of algebras satisfying the same identities, satisfy the same identities as the original algebra (s). More surprisingly, the converse is also true: any class of algebras which is closed under the processes of direct summation, homomorphic mappings and contains all the subalgebras of its members is uniquely defined by a set of identities¹⁴.

The algebras which are most well understood are the associative algebras (which satisfy $A(x, y, z) = 0$), Lie algebras ($x^2 = 0$, $(xy)z + (yz)x + (zx)y = 0$), alternative algebras ($A(x, y, y) = A(x, x, y) = 0$), and Jordan algebras ($xy = yx$, $A(x, y, x^2) = 0$).

Of course, the structure theory of Lie algebras is fairly well known. Here we pause to point out the following facts. If A is any associative algebra, redefine the product to be antisymmetric, i.e.

$$x \cdot y = xy - yx$$

Then the associativity of the original algebra implies that the Jacobi identity is satisfied in the new algebra A^- . A^- is therefore a Lie algebra. The Birkhoff-Witt theorem states that any Lie algebra is isomorphic to a subalgebra of some A^- .

Similarly, if A is any associative algebra we may define a new product

$$x * y = xy + yx$$

This gives a commutative, though not associative algebra. However, the identity $(x * y) * (x * x) = x * [y * (x * x)]$ is satisfied, i. e. A^+ is a Jordan algebra. Jordan introduced these algebras in 1933 because of his dissatisfaction with matrix formulation of QM. As opposed to the case in Lie algebras, not all Jordan algebras may be derived from associative algebras; those that can are called special. For his purposes Jordan needed a large class of non-special Jordan algebras. Jordan algebra theory is closely related to Lie theory, all non-special Jordan algebras, like the exceptional Lie groups, being closely related to alternative non-associative algebras, i.e., to the Cayley-Dickson algebras¹⁵.

In the alternative theory itself, the octonions and closely related algebras play a dominant role. For instance, any alternative division ring is either associative or a Cayley-Dickson algebra¹⁶. In fact, it is not unfair to say that the study of alternative algebras begins and ends with Cayley numbers, as alternative rings were defined to study them, and they are the only distinguished member of the class.

Of course, the study of other identities is ongoing, but one is impressed by the coherence of the non-associative algebras we have discussed, and its strong impact on other branches of mathematics, for example, projective geometry. Because of their close inter-relations in mathematics, one is perhaps justified in wondering if the Jordan and alternative algebras have as important a role to play in physics as the Lie algebras.

Footnotes and References

The bulk of these notes comes from the books by Albert and Schafer, footnotes 3 and 2. Schafer's is the more authoritative of the two, however the other is more pleasant, being descriptive. Schafer requires more background. Extensive references to the original literature are given in Albert.

1. M. Gunaydin and F. Gursey, Lett. Nuovo Cimento G, 49 (1973).
M. Gunaydin and F. Gursey, Jour. Math. Phys. 14, 1651 (1973).
M. Gunaydin and F. Gursey, Phys. Rev. D9, 3387 (1974).
F. Gursey in Proc. Johns Hopkins University Workshop, (ed. by G. Domokos and S. K. Domokos), Johns Hopkins University, Baltimore, 1974.
F. Gursey, invited talk at the Kyoto Conference 1975; Yale University preprint (1975), unpublished.
R. Casalbuoni, G. Domokos and S. K. Domokos, Algebraic Approach to the Quark Problem, to be published.
2. See R. D. Schafer, An Introduction to Nonassociative Algebras, Academic Press, 1966; pg. 15.
3. For a detailed proof of this and some similar interesting results see E. Kleinfeld's article in A. A. Albert, Studies in Modern Algebra, Mathematical Association of America, 1963.
4. E. P. Wigner, The Unreasonable Effectiveness of Mathematics in the Natural Sciences, Communications on Pure and Applied Mathematics, Vol. 13 (1960) pp. 1-14.
5. W. R. Hamilton, Lectures on Quaternions, Dublin, 1853.
6. For a playful account of sums of cubes, etc. see H. Rademacher and O. Tóth, The Enjoyment of Mathematics, Princeton University Press, 1956.
7. The more general case of normed and division algebras over arbitrary fields are discussed in the references of the article by C. W. Curtis in A. A. Albert, op. cit.

8. A. Cayley, On Jacobi's Elliptic Functions, in Reply to the Rev. Brice Bronwin and on Quaternions, Philosophical Magazine and Journal of Science, Vol. 3 (1845), pp. 210-213.
9. L. E. Dickson, On Quaternions and their Generalization and the History of the Eight Square Problem, Annals of Mathematics, Vol. 20 (1919), pp. 155-171.
10. A. A. Albert, Quadratic Forms Permitting Composition, Annals of Mathematics, Vol. 43 (1942), pp. 161-177, and Absolute-Valued Algebraic Algebras, Bulletin of the American Mathematical Society, Vol. 55 (1949), pp. 763-768.
11. R. Bott and J. Milnor, On the Parallelizability of the Spheres, Bulletin American Mathematical Society Vol. 64 (1958) 86-89; and M. Kervaire, Non-Parallelizability of the N-Sphere for $N \geq 7$, Proceedings of the National Academy of Science of the United States, Vol. 44 (1958), pp. 280-283.
12. Examples of other division algebras are given in R. H. Bruck, Some Results in the Theory of Linear Nonassociative Algebras, Transactions American Mathematical Society Vol. 56 (1944), 141-199; and J. M. Osborn, Quadratic Division Algebras, Transactions American Mathematical Society Vol. 105 (1962), pg. 202-221.
13. A more complete discussion of this procedure for arbitrary field is given in R. D. Schafer, op. cit., pp. 45-50.
14. G. Birkhoff, Universal Algebras, Proceedings of the Canadian Mathematical Congress (1946).
15. A discussion of Jordan algebras and their relation to the alternative algebras and to the exceptional semi-simple Lie groups is given in R. D. Schafer, op. cit., Chapter IV.
16. R. D. Schafer, op. cit., pg. 48.

(fig. 1)

(fig. 2)