Divulgaciones Matemáticas Vol. 10 No. 2(2002), pp. 161–169

Alternative Real Division Algebras of Finite Dimension

Algebras de División Alternativas Reales de Dimensión Finita

Angel Oneto (angeloneto@hotmail.com)
Departamento de Matemática
Facultad Exp. de Ciencias, Universidad del Zulia,
Maracaibo, Venezuela.

Abstract

An elementary and self contained proof of the theorem which asserts that the only alternative,finite dimensional division algebras over the real numbers are the reals, the complex numbers, the quaternions and the octonions is given. Moreover, as a corollary, a theorem of Hurwitz which gives the classification of the real normed algebras of finite dimension is derived.
Key words and phrases: division algebra, quaternions, real normed algebra.

Resumen

Se prueba de manera elemental y autocontenida que las únicas álgebras de división alternativas de dimensión finita sobre los reales, son los números reales, los complejos, los cuaternios y los octonios. Asimismo, como corolario se deriva un teorema de Hurwitz que clasifica las R-álgebras normadas de dimensión finita.
Palabras y frases clave: álgebra de división, cuaternios, álgebra real normada.

Introduction

In 1843, Hamilton trying to extend to three dimensions the nice properties (those of a normed algebra) of the complex numbers, realized that instead of triples he consider quadruples of real numbers, the desired generalization is

Recibido 2001/12/12. Aceptado 2002/06/12.
MSC (2000): Primary 17D05.

possible although at the cost of abandoning the commutativity of the product, creating in this way the quaternions.

Soon after, in 1845, Cayley extends that construction to eight dimensions, this time he should not only abandon the commutativity but also the associativity of the product, building the octonions or Cayley numbers. In these octonions the lack of associativity is compensed in part by a sort of weak associativity, the alternative laws:

$$x(xy) = x^2y, \qquad (yx)x = yx^2$$

In 1877 Frobenius showed the singularity of the quaternions, proving the theorem that classifies the associative division finite dimensional algebras over the reals.

The singularity of the Cayley numbers was also proved: a theorem due to Bruck and Kleinfeld (1957) asserts that an alternative division ring is necessarily a division algebra of Cayley - Dickson (a generalization of the Cayley numbers to an arbitrary field) or an associative division algebra [1].

The purpose of this article is to give an elementary and self contained proof, in the spirit of the proof of Frobenius theorem given in [2], of the following generalized Frobenius:

Main Theorem: An alternative division algebra of finite dimension over the reals is isomorphic to the field of real numbers, to the complex one, to the quaternion algebra or to the algebra of Cayley numbers.

This will be proved in section 2 where also the definition of the Cayley numbers is given. In section 1 a few lemmas on general alternative algebras needed in the proof are stablished, and in the last section a famous theorem of Hurwitz (1898), which gives the classification of the real normed algebras of finite dimension, is derived.

1 Lemmas

In a nonassociative algebra it is convenient to introduce the *associator* of x, y, z, defined by:

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

Then the associativity is expressed by: $A(x, y, z) = 0$, and the alternative laws become: $A(x, x, y) = A(y, x, x) = 0$. The associator is clearly linear in each variable.

Throughout this section we assume that we work with an alternative algebra (which satisfies the alternative laws above) over a field K, and x, y, z, are elements of this algebra.

(a) The associator is antisymmetric:

$$A(x,y,z) = -A(y,x,z) = -A(x,z,y) = -A(z,y,x).$$

We shall prove only the first identity, the others follow in a similar way. By the left alternative law we have:

$$0 = A(x+y,x+y,z) = A(x,x,z)+A(x,y,z)+A(y,x,z)+A(y,y,z) = A(x,y,z)+A(y,x,z).$$

From (a) we have $A(x,y,x) = -A(y,x,x)$, then:

(b) The so called *flexible law* is valid: $x(yx) = (xy)x$, and this common value will be denoted then by xyx.

By (a) we have $A(x,y,z) + A(y,x,z) = 0$, and if $xy + yx = 0$:

$$0 = A(x,y,z) + A(y,x,z) + (xy + yx)z = x(yz) + y(xz).$$

Or $x(yz) = -y(xz)$. In a similar fashion we have: $(zx)y = -(zy)x$, hence:

(c) If x, y anticommute, that is if $xy = -yx$, then:

$$x(yz) = -y(xz), \quad (zx)y = -(zy)x.$$

(d) The following *Moufang identity* holds:

$$(zx)(yz) = z(xy)z$$

Proof:

$$\begin{aligned}(zx)(yz) - ((zx)y)z &= A(zx,y,z) = A(y,z,zx) = y(z^2x) - (yz)(zx) = \\ &= y(z^2x) - A(yz,z,x) - (yz^2)x = A(y,z^2,x) - A(yz,z,x) = \\ &= A(y,z^2,x) - A(x,yz,z) = A(y,z^2,x) - x(yz^2) + (x(yz))z = \\ &= A(y,z^2,x) + A(x,y,z)z - A(x,y,z^2) = A(x,y,z)z,\end{aligned}$$

then

$$\begin{aligned}(zx)(yz) &= A(x,y,z)z + ((zx)y)z = \\ &= A(x,y,z)z - A(z,x,y)z + z(xy)z = z(xy)z.\end{aligned}$$

(e) If we define inductively: $x^1 = x$, $x^{n+1} = x^n x$ for natural n, we have:

$$x^n x^m = x^{n+m} \quad (*)$$

Proof: By induction on m using the flexible law one shows: $xx^m = x^{m+1}$. Then by induction on n, as $(*)$ is obvious for $m = 1$, we can assume $m > 1$ and the inductive step follows from Moufang identity:

$$x^{n+1}x^m = (xx^n)(x^{m-1}x) = xx^{n+m-1}x = x^{n+m+1}.$$

2 Main theorem

In what follows D denotes a finite dimensional alternative division algebra over the field R of real numbers.

By lemma (e) the specialization: $R[X] \longrightarrow D : X \longmapsto x$ is an algebra morphism.

The set of powers: $1, x, x^2, \ldots$ of an element x in D is linearly dependent (if it is finite there is a dependence relation of the form $x^n = x^m$ for $n \neq m$ and if it is infinite it follows from the finite dimensionality of D). As a polynomial in $R[X]$ is a product of polynomials of degree one or two, and as D has no nonzero divisor we deduce that x satisfies a second degree equation with real coefficients, That is:

(1) If $x \in D$ then $x^2 \in R + Rx$.

Explicitly $x^2 = ax + b$ for real a, b and so $\left(x - \frac{a}{2}\right)^2 \in R$. Then if $x \notin R$ we must have $\left(x - \frac{a}{2}\right)^2 = -c^2$ with $c \in R$. From this we obtain on one hand, if $D \neq R$, the existence of $i \in D$ such that $i^2 = -1$, and on the other if $x \in D$ and $xi = ix$ then $x \in R + Ri$, since if $x \notin R$ then $\left(x - \frac{a}{2}\right)^2 = (ic)^2$, but from $xi = ix$ we have

$$\left(x - \frac{a}{2}\right)^2 - (ic)^2 = \left(x - \frac{a}{2} + ic\right)\left(x - \frac{a}{2} - ic\right) = 0$$

and so $x \in R + Ri$. We have proved:

(2) If $D \neq R$ then there exists $i \in D$ such that $i^2 = -1$; $C = R + Ri$ is a field isomorphic to the field of complex numbers and $C = \{x \in D \,/\, xi = ix\}$.

Set $C^- = \{x \in D \,/\, xi = -ix\}$. Obviously C^- is a subspace of D such that $C \cap C^- = 0$. Moreover:

(3) $D = C \oplus C^-$.

It only remains to prove that $D = C + C^-$ but this is a consequence of the identity:

$$x = \frac{1}{2}(x - ixi) + \frac{1}{2}(x + ixi) \quad (\#)$$

since in virtue of the alternative and flexible laws $x - ixi \in C$ and $x + ixi \in C^-$ (for example: $(x+ixi)i = xi - ix$ and $i(x+ixi) = ix - xi$ and so $x + ixi \in C^-$).

The next observation also follows from the alternative and flexible laws.

(4) If $x, u \in D$ anticommute, then x^2 and u commute.

In fact, from $xu = -ux$ it follows $x^2u = x(xu) = -x(ux) = -(xu)x = (ux)x = ux^2$.

Now let $x \in C^-, x \neq 0$. By (4), (2) and (1) we have $x \in C \cap (R + Rx)$ but $Rx \subset C^-$ and so by (3), $x^2 \in R$. If $x^2 > 0$ then $x \in R$, which contradicts (3), hence: $x^2 = -c^2$ with $c \in R$ and if we define $j = c^{-1}x$, we obtain $j^2 = -1$ and $ji = -ij$. Setting $k = ij$ we deduce the defining relations of the quaternions:

$$i^2 = j^2 = k^2 = -1;\ ij = -ji = k;\ jk = -kj = i;\ ki = -ik = j$$

For example, by Moufang identity we have: $k^2 = (ij)(ij) = -(ij)(ji) = -ij^2i = i^2 = -1$. Then,

(5) If $D \nsubseteq C$ then there exists $j \in C^-$ such that $j^2 = -1$ and the 4-dimensional subspace $C + Cj$ is an associative division algebra (over R) isomorphic to the Hamilton quaternions.

Inasmuch as $C + Cj$ is associative, setting $H = \{x \in D \,/\, xk = (xi)j\}$ it follows that H is a subspace such that $C + Cj \subset H$. In order to establish the opposite inclusion we first note:

(6) $H = C \oplus (C^- \cap H)$.

By (2) and (#) it suffices to verify that if $x \in H$ then $x + ixi \in H$. From lemma (c) and Moufang identity we have:

$$(x + ixi)k = xk - i(xk)i = xk - (ix)(ki) = xk - (ix)j,$$

and by the right alternative law:

$$((x + ixi)i)j = (xi)j - (ix)j.$$

But if $x \in H$ then $xk = (xi)j$ and so $x + ixi \in H$ and (6) is proved.

Multiplication on the right by j defines an R-linear transformation $T(x) = xj$ that maps H into itself. In fact if $x \in H$ then by lemma (c):

$$\begin{aligned} (xj)k &= -(xk)j = -((xi)j)j = xi \\ ((xj)i)j &= -((xj)j)i = xi, \end{aligned}$$

hence $xj \in H$. Also T interchanges C and $C^- \cap H$, for if $x \in C$ $(xi = ix)$ we have:

$$(xj)i = -(xi)j = -(ix)j = -i(xj)$$

where the last equality results from:

$$0 = A(x, i, j) = -A(i, x, j) = -i(xj) + (ix)j.$$

Hence, if $x \in C$ then $xj \in C^- \cap H$. In the same way one obtains: if $x \in C^- \cap H$ then $xj \in C$. But T is an automorphism (its inverse is the right multiplication by $-j$) then $\dim(C' \cap H) = \dim C = 2$ and, by (6), H is a 4-dimensional subspace. As was observed above $C + Cj \subset H$ and so:

(7) $H = C + Cj$.

By analogy with (3) we define $H^- = \{x \in D \,/\, xk = -(xi)j\}$ which is obviously a subspace such that $H \cap H^- = 0$. Moreover we shall prove:

(8) $D = H \oplus H^-$.

To show that $D = H + H^-$ we use the identity:

$$x = \frac{1}{2}(x - xijk) + \frac{1}{2}(x + xijk)$$

where to avoid the proliferation of parenthesis we write $xijk$ for $((xi)j)k$ and so in similar cases. This notation will be maintained along the proof of (8) and only in it. Due to the above identity it only remains to verify that $x - xijk \in H$ and $x + xijk \in H^-$. We have by lemma (c) and the alternative laws:

$$\begin{aligned} (x + xijk)k &= xk - xij \\ (x + xijk)ij &= xij + xi^2jkj = xij - xjkj = xij - xk \end{aligned}$$

then $x + xijk \in H^-$. Similarly one verifies that $x - xijk \in H$.

(9) If $x \in H^-$ then x anticommutes with i, j and k.

As $x \in H^-$ we have $xk = \frac{1}{2}A(x, i, j)$. But $xk = -(xi)j$ implies $x = [(xi)j]k$. Now, by Moufang identity:

$$kx = [k(xi)](jk) = [k(xi)]i = [(ij)(xi)]i = \{[i(jx)]i\}i = -i(jx)$$

and so $kx = -\frac{1}{2}As(i, j, x) = -\frac{1}{2}As(x, i, j) = -xk$.

Similarly, since by lemma (c) we have $x = -[(xi)k]j$ $(x \in H^-)$, then we have:

$$jx = -[j(xi)](kj) = [j(xi)]i = -[(ik)(xi)]i = -[i(kx)i]i = i(kx).$$

Hence $jx = \frac{1}{2}A(i, k, x) = \frac{1}{2}A(x, i, k) = -\frac{1}{2}xj - \frac{1}{2}(xi)k = -xj$ (since $x = -[(xi)k]j$, thus $xj = (xi)k$).

One can prove that x anticommutes with i in a similar way or, more simply, as it anticommutes with k and j we have:

$$xi = (xk)j = -(kx)j = (kj)x = -ix.$$

(10) If $D \not\subseteq H$ then there exists $h \in H^-$ such that $h^2 = -1$.

Let $x \in H^-$, $x \neq 0$. By (9), $x \in C^-$ and from (4), (2) and (1) we obtain: $x^2 \in C \cap (R + Rx) = R$. But $x \notin R$ ($x \in H^-$), thus $x^2 = -c^2$ with $c \in R$, $c \neq 0$. Setting $h = c^{-1}x$, (10) follows.

We are now in a position to end the proof:

(11) If $D \not\subseteq H$, then D is an 8-dimensional algebra isomorphic to the algebra of Cayley numbers.

The mapping defined by $T(x) = xh$ is a linear automorphism of D over R (its inverse is right multiplication by $-h$) and interchanges H and H^-, for if $x \in H$ we have:

$$(xh)k = -(xk)h = -((xi)j)h = -((xh)i)j$$

and so $xh \in H^-$. Similarly if $x \in H^-$ then $xh \in H$.

Now, by (7), $\dim H^- = \dim H = 4$ and, by (8), $\dim D = 8$. It also follows that $H^- = Hh$ and $\{h, ih, jh, kh\}$ is a basis of H^-. Hence $\{1, i, j, k, h, ih, jh, kh\}$ is a basis of D and we have:

$$\begin{aligned} (ih)(kh) &= -(hi)(kh) = -h(ik)h = hjh = -(jh)h = j, \\ (ih)(ih) &= -(ih)(hi) = -ih^2i = i^2 = -1. \end{aligned}$$

In the same way one can obtain all the entries of the following table, whose (r, s)-th element is the product $x_r x_s$ (in that order) and where we use the following notation:

$$x_1 = i,\ x_2 = j,\ x_3 = k,\ x_4 = h,\ x_5 = ih,\ x_6 = jh,\ x_7 = kh$$

$\cdot$	x_1	x_2	x_3	x_4	x_5	x_6	x_7
x_1	-1	x_3	$-x_2$	x_5	$-x_4$	$-x_7$	x_6
x_2	$-x_3$	-1	x_1	x_6	x_7	$-x_4$	$-x_5$
x_3	x_2	$-x_1$	-1	x_7	$-x_6$	x_5	$-x_4$
x_4	$-x_5$	$-x_6$	$-x_7$	-1	x_1	x_2	x_3
x_5	x_4	$-x_7$	x_6	$-x_1$	1	$-x_3$	x_2
x_6	x_7	x_4	$-x_5$	$-x_2$	x_3	-1	$-x_1$
x_7	$-x_6$	$-x_6$	x_4	$-x_3$	$-x_2$	x_1	-1

The relations in this table are the definitory relations of the Cayley numbers and (11) follows. As we have not defined yet the Cayley numbers, we cannot verify the last assertion, but now it is clear how to define them: take an 8-dimensional vector space over R and an ordered basis $\{x_0, x_1, x_2, x_3, x_4, x_5, x_6, x_7\}$.

Define a product of the elements of this basis in such way that x_0 will be a neutral element: $x_0x_r = x_rx_0$ $(r = 0, \ldots, 7)$ and for $r, s = 1, \ldots, 7$ define x_rx_s by the above table and extend by bilinearity:

$$\left(\sum_{r=0}^{7} a_r x_r\right)\left(\sum_{r=0}^{7} b_r x_r\right) = \sum_{0\leq r,s\leq 7} a_r b_s (x_r x_s)$$

where x_rx_s is to be replaced by its value given in the table. In this way we obtain an alternative algebra (the alternative laws are valid for the elements of the basis and then for arbitrary elements). To see that it is a division algebra we proceed as in the case of the quaternions or of the complex numbers: the conjugate of $x = a_0 + \sum_{r\geq 1} a_r x_r$ is defined by $\overline{x} = a_0 - \sum_{r\geq 1} a_r x_r$. Then:

$$x\overline{x} = \overline{x}x = a_0^2 - \sum_{r\geq 1} a_r^2 x_r^2 - \sum_{1\leq r<s} a_r a_s (x_r x_s + x_s s_r) = \sum_{r\geq o} a_r^2.$$

Setting $N(x) = \sum_{r\geq 0} a_r^2$ it follows that $N(x) = 0$ if and only if $x = 0$, and if $x \neq 0$ then $N(x)^{-1}\overline{x}$ is the inverse of x.

3 A corollary

If one takes the definitory basis $\{x_r\}$ as ortonormal, the complex numbers, the quaternions and the Cayley numbers become real vector spaces with scalar product $\langle , \rangle$ such that $N(x) = \langle x, x\rangle$. Also in these algebras one have $\overline{xy} = \overline{yx}$ and then $N(xy) = N(x)N(y)$.

In general, a *normed algebra* is an algebra over the reals with a scalar product $\langle , \rangle$ such that the norm defined by $N(x) = \langle x, x\rangle$ is multiplicative: $N(xy) = N(x)N(y)$. In a normed algebra each element x can be writen univocally as $x = a + x'$ where $a \in R$ and $x' \in S$, being S the ortogonal complement of the subspace generated by the identity element, and its *conjugate* is defined by: $\overline{x} = a - x'$. It is clear that $x\overline{x} = \overline{x}x$ and $\overline{\overline{x}} = x$. As we will see also in this general situation one have $N(x) = \overline{x}x$, this will follow from the next lemma:

Lemma In a normed algebra with scalar product $\langle , \rangle$ we have:

$$\langle xu, v\rangle = \langle u, \overline{x}v\rangle$$

Proof: From the basic relation between the scalar product and the norm:

$$\langle x, y\rangle = \frac{1}{2}\{N(x + y) - N(x) - N(y)\}$$

and the multiplicative property of the norm we obtain:

$$\langle xy, y\rangle = N(y)\,\langle x, 1\rangle$$

then if $x' \in S$ we have $\langle x'y, y\rangle = 0$ and if we put $y = u + v$ it follows: $\langle x'u, v\rangle = -\langle u, x'v\rangle$. From this, if $x = a + x'$ with $a \in R$ and $x' \in S$ it results:

$$\langle xu, v\rangle = a\,\langle u, v\rangle + \langle x'u, v\rangle = \langle u, av\rangle - \langle u, x'v\rangle = \langle u, \overline{x}v\rangle$$

□

Lemma Every normed algebra is an alternative division algebra.

Proof: From the previous lemma we have:

$$\langle \overline{x}x, y\rangle = \langle x, xy\rangle = N(x)\,\langle 1, y\rangle = \langle N(x), y\rangle$$

then $N(x) = \overline{x}x$. As $N(x) = 0 \iff x = 0$, it follows that $N(x)^{-1}\overline{x}$ is the inverse of $x \neq 0$.

To prove the alternative laws consider $\langle xz, xy\rangle$. On one hand we have $\langle xz, xy\rangle = N(x)\,\langle z, y\rangle = \langle z, (\overline{x}x)y\rangle$ and on the other hand, by the previous lemma, $\langle xz, xy\rangle = \langle z, \overline{x}(xy)\rangle$ and so:

$$(\overline{x}x)y = \overline{x}(xy),$$

but $x + \overline{x} \in R$, then $[(x + \overline{x})x]y = x[(x + \overline{x})y]$ and we have: $x^2y = x(xy)$. The other alternative law follows similarly. □

As a corollary of the main theorem and the lemma just proved, it follows the famous Hurwitz's theorem (1898):

Theorem A finite dimensional normed algebra is isomorphic to the real numbers, to the complex numbers, to the quaternions or to the Cayley numbers.

References

[1] Kleinfeld E. *A Characterization of the Cayley Numbers*, Studies in Modern Algebra, MAA Studies in Mathematics, Vol. 2 (1963).

[2] Palais R. S. *The Classification of Real Division Algebras*, Amer. Math. Monthly **75**(1968) 366–368.