Multiplication on $\mathbb{R}^n$

1. Division Algebra and Vector Product

Basudeb Datta

Basudeb Datta received his Ph D degree from the Indian Statistical Institute in 1988. Since July 1992 he has been at the Indian Institute of Science, Bangalore. His areas of interest are Topology and Geometry.

In 1843 Hamilton discovered the quaternions and in the same year Graves found an algebra with 8 basis elements. So, mathematicians knew the division algebra structures (over $\mathbb{R}$) on $\mathbb{R}$, $\mathbb{R}^2$, $\mathbb{R}^4$ and $\mathbb{R}^8$ in the first half of the 19th century itself. It took more than 100 years to prove that these are all the division algebras over $\mathbb{R}$. This follows from a theorem of Adams (which we will discuss in Part 2). In this part we also discuss 'vector products' on $\mathbb{R}^3$ and $\mathbb{R}^7$ and Hurwitz's theorem on 'sums of squares formulae'.

Division Algebra

Let $\mathbb{R}$ and $\mathbb{C}$ denote the set of real and complex numbers respectively. Recall the multiplication rule of complex numbers:

$$(a + bi)\ \ (c + di) = (ac - db) + (da + bc)i. \qquad (1)$$

Identifying $\mathbb{R}^2$ with $\mathbb{C}$ (by $(a, b) \mapsto a + bi$) we get a multiplication on $\mathbb{R}^2$ namely,

$$(a, b)\ \ (c, d) = (ac - db, da + bc). \qquad (1')$$

Gerolamo Cardano, a famous medical doctor, philosopher and mathematician, who lived in Milan, was the first person to define complex numbers in 1539.

With this multiplication, $\mathbb{R}^2$ becomes an associative division algebra [1] over $\mathbb{R}$. In this case $1 = (1, 0)$ is the unity for the multiplication and $x^{-1} = \overline{x}/\|x\|$ for all $x \neq (0, 0)$, where $\overline{(x_1, x_2)} = (x_1, -x_2)$ and $\|(x_1, x_2)\| = (x_1^2 + x_2^2)^{1/2}$.

We also know (!) that $\mathbb{R}^4$ has a multiplication given by:

$$\begin{aligned} i^2 = j^2 = k^2 = -1, \qquad & i \cdot j = k = -j\ \ i, \\ j\ \ k = i = -k \cdot j, \qquad & k \cdot i = j = -i\ \ k, \end{aligned} \qquad (2)$$

where $1 = (1,0,0,0)$, $i = (0,1,0,0)$, $j = (0,0,1,0)$ and $k = (0,0,0,1)$. In this case also $x^{-1} = \overline{x}/\|x\|$, where $(x_1, x_2, x_3, x_4) = (x_1, -x_2, -x_3, -x_4)$. With this multiplication and the usual vector space structure, $\mathbb{R}^4$ is an associative division algebra over $\mathbb{R}$. But you have to be careful about dividing a by b on the left or on the right! This algebra is called the *algebra of quaternions* and is denoted by $\mathbb{H}$.

Observe that multiplication in $\mathbb{H}$ is not commutative, whereas multiplication in reals or complex numbers is commutative. So you know why it took 304 years to define quaternions. Also, a polynomial may have infinitely many zeros in $\mathbb{H}$. Find the zeros of $x^2 + 1$ in $\mathbb{H}$ (exercise).

If we identify $\mathbb{H}$ with $\mathbb{C} \times \mathbb{C}$ via

$$x + yi + zj + wk = (x + yi) + (z + wi)j \mapsto (x + yi, z + wi),$$

then the multiplication in (2) can be obtained from the formula

$$(x, y)\ \ (z, w) = (xz - \overline{w}y, wx + y\overline{z}). \qquad (2')$$

where here x, y, z and w are elements of $\mathbb{C}$.

Now, if we take $x, y, z, w \in \mathbb{H}$ in $(2')$, then we get a multiplication on $\mathbb{R}^8$ Therefore, for $n \in \{1, 2, 4\}$ we have the following:

> Multiplication in $\mathbb{R}^{2n}$ can be obtained from that of $\mathbb{R}^n$ by the formula: $(x, y) \cdot (z, w) = (xz - \overline{w}y, wx + y\overline{z})$.

There is another way to remember the multiplication in $\mathbb{R}^8$ by the following rule:

$$(e_1 \cdot e_2) \cdot e_4 = e_1 \cdot (e_2 \cdot e_4) = (e_2 \cdot e_3) \cdot e_5 = e_2 \cdot (e_3 \cdot e_5) = (e_3 \cdot e_4) \cdot e_6$$

$$= e_3 \cdot (e_4 \cdot e_6) = (e_4 \cdot e_5) \cdot e_7 = e_4 \cdot (e_5 \cdot e_7) = (e_5 \cdot e_6) \cdot e_1 = e_5 \cdot (e_6 \cdot e_1)$$

$$= (e_6 \cdot e_7) \cdot e_2 = e_6 \cdot (e_7 \cdot e_2) = (e_7 \cdot e_1) \cdot e_3 = e_7 \cdot (e_1 \cdot e_3) = e_r^2 =$$

$$-1 = -e_0 \quad \text{and} \quad (e_r\ \ e_s)\ \ e_s = e_s\ \ (e_s\ \ e_r) = -e_r$$

[1] An *algebra* over $\mathbb{R}$ consists of a vector space V over $\mathbb{R}$, together with a binary operation of multiplication ('$\cdot$') on the set V of vectors, such that for all a in $\mathbb{R}$ and α, β, γ in V, the following conditions are satisfied: (i) $(a\alpha)\ \beta = a(\alpha \cdot \beta) = \alpha\ \ (a\beta)$, (ii) $(\alpha + \beta) \cdot \gamma = (\alpha \cdot \gamma) + (\beta \cdot \gamma)$ and (iii) $\alpha \cdot (\beta + \gamma) = (\alpha \cdot \beta) + (\alpha \cdot \gamma)$. If moreover V satisfies (iv) $(\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma)$ for all α, β, γ in V, then V is called an *associative algebra* over $\mathbb{R}$. An algebra V over $\mathbb{R}$ is a *division algebra* over $\mathbb{R}$ if V has a unity for multiplication and each nonzero element x has a unique left inverse x_L, a unique right inverse x_R, with $x_L = x_R$.This is denoted by x^{-1}.

An easy way to remember multiplication in $\mathbb{R}^8$ is: $e_p e_{p+1} e_{p+3} = e_q^2 = -1$ for $p,\ q \in \{1, ..., 7\}$ (addition in the suffix is modulo 7).

In a letter to John Graves, written on October 17, 1843, W R Hamilton announced the discovery of quaternions one day after the discovery.

John Graves found an algebra with 8 basis elements in December 1843. In 1848 he published his discovery in the Transactions of the Irish Academy, 21, p.388. Octonions were rediscovered by Arthur Cayley in 1845 (Collected Papers I, p.127 and XI, p.368–371). Because of this the octonions are known as Cayley numbers!

for $r, s \in \{1, 2, . \quad 7\}$, where the identification between $\mathbb{R}^8$ and $\mathbb{H} \times \mathbb{H}$ is given by $e_0 = (1, 0, . \quad , 0) \mapsto (1, 0)$, $e_1 = (0, 1, 0, \quad , 0) \mapsto (i, 0)$, $e_2 \mapsto (j, 0)$, $e_3 \mapsto (0, 1)$, $e_4 \mapsto (k, 0)$, $e_5 \mapsto (0, j)$, $e_6 \mapsto (0, -k)$ and $e_7 = (0, . \quad , 0, 1) \mapsto (0, i)$.

Now, $(e_1 \quad e_2) \quad e_5 = e_7 \neq -e_7 = e_1 \quad (e_2 \quad e_5)$. Therefore, this multiplication in $\mathbb{R}^8$ is non-associative. However, in $\mathbb{R}^8$ also each non-zero x has unique inverse, namely, $x^{-1} = \overline{x}/\|x\|$, where $\overline{(h_1, h_2)} = (\overline{h_1}, -h_2)$, i.e., $\overline{(x_1, \quad , x_8)} = (x_1, -x_2, -x_8)$. $\mathbb{R}^8$ with this multiplication forms a non-associative division algebra, denoted by $\mathbb{O}$, called the *algebra of octonions* or *Cayley numbers.*

Observation 1 : *Any two octonions generate an associative sub-algebra of* $\mathbb{O}$.

If we continue further with the formula (2′) to define a multiplication on $\mathbb{R}^{16}$ then we get $(e_1, e_2) \quad (e_5, -e_7) = (0, 0)$. Thus we get 'divisors of zero'. So we better stop here! (If x and y are two nonzero elements such that $xy = 0$, then they are called divisors of zero. A division algebra does not have divisors of zero (exercise).)

All these four algebras $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$ and $\mathbb{O}$ are normed algebras, i.e., $\|x \cdot y\| = \|x\| \cdot \|y\|$, where $\| \ \|$ denotes the usual Euclidean length. $\mathbb{R}$ and $\mathbb{C}$ are commutative algebras. $\mathbb{R}$, $\mathbb{C}$ and $\mathbb{H}$ are associative algebras.

Thus, $\mathbb{R}^n$ has a division algebra structure if $n \in \{1, 2, 4, 8\}$.

Question : Does there exist n, other than 1, 2, 4 and 8, for which $\mathbb{R}^n$ has a division algebra structure over $\mathbb{R}$? This question is resolved by the following theorem.

Theorem A : $\mathbb{R}^n$ *has a division algebra structure over* $\mathbb{R}$ *if and only if* $n \in \{1, 2, 4, 8\}$.

Remark: An examination of the proof of Theorem A (which

will be given in Part 2) will show that we have actually proved the following statement: $\mathbb{R}^n$ has an algebra structure over $\mathbb{R}$ without divisors of zero if and only if $n \in \{1, 2, 4, 8\}$.

Vector Product

Recall the cross product (or vector product) on $\mathbb{R}^3$. It is given by

$$i \times j = k = -j \times i, \qquad j \times k = i = -k \times j,$$
$$k \times i = j = -i \times k, \qquad i \times i = j \times j = k \times k = 0$$

where i, j, k here are the usual basis vectors in $\mathbb{R}^3$ and bilinearity (or distributive property)is assumed. Is it in any way related to $\mathbb{H}$? Yes!

If we take $\mathbb{R}^3 = \text{Span}_{\mathbb{R}}(\{i, j, k\}) \subseteq \mathbb{H}$, then [2]

$$x \times y = \text{ imaginary part of } x\ \ y.$$

This cross product has the following properties

$$(x \times y) \perp x, \quad (x \times y) \perp y \quad \text{and} \ [3] \tag{3}$$

$$\|x \times y\|^2 = \langle x, x\rangle\langle y, y\rangle - \langle x, y\rangle^2 \tag{4}$$

[4]for all x, y in $\mathbb{R}^3$

By a vector product on $\mathbb{R}^n$ we mean a continuous mapping $\nu : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}^n$ with the properties (3) and (4). More precisely, we have the following definition.

Vector product: A continuous map $\nu : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}^n$ is called a vector product on $\mathbb{R}^n$ if $\nu(x, y) \perp x$, $\nu(x, y) \perp y$ and $\|\nu(x, y)\|^2 = \langle x, x\rangle\langle y, y\rangle - \langle x, y\rangle^2$ for all $x, y \in \mathbb{R}^n$.

Thus, the usual 'cross product' on $\mathbb{R}^3$ is a vector product in this sense. The map $\nu : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$, given by $\nu(x, y) = 0$ for all x, $y \in \mathbb{R}$, is clearly a vector product on $\mathbb{R}$. It is also not difficult to see that this is the only vector product on $\mathbb{R}$. Consider $\mathbb{R}^7$ as the 'imaginary' subspace of $\mathbb{R}^8 = \mathbb{O}$, i.e.,

[2] For $\alpha_1, \ldots, \alpha_p$ in $\mathbb{R}^n$ $\text{Span}_{\mathbb{R}}(\{\alpha_1, \ldots, \alpha_p\})$ denotes the subspace generated by $\{\alpha_1, \ldots, \alpha_p\}$.

[3] If $\langle z, w\rangle = 0$ then we say z is orthogonal to w and we write $z \perp w$.

[4] Here $\langle , \rangle$ denotes the usual inner product (also known as 'dot product') in $\mathbb{R}^n$, namely, $\langle (x_1, \ldots, x_n), (y_1, \ldots, y_n)\rangle = x_1y_1 + \cdots + x_ny_n$. In this article '$\cdot$' corresponds to multiplication in the algebra sense, **not** the inner product.

$\mathbf{R}^7$ also has a vector product like $\mathbf{R}^3$

$\mathbb{R}^7 = \text{Span}_{\mathbb{R}}(\{e_1, \ldots, e_7\})$. Define $\nu(x,y)$ $(= x \times y)$:= the imaginary part of $x \cdot y$. Then ν satisfies (3) and (4). So, we have a vector product on $\mathbb{R}^7$ also. These vector products on $\mathbb{R}^3$ and $\mathbb{R}^7$ have the following properties:

$$x \times y = -y \times x, \tag{5}$$

$$x \times (ay+bz) = (ax) \times y + (bx) \times z = x \times (ay) + x \times (bz), \tag{6}$$

$$\|x\|^2 = \langle x, x \rangle = -x \quad x, \tag{7}$$

$$\langle x, y \rangle = - \text{ real part of } x \quad y \quad \text{and} \tag{8}$$

$$x \cdot y = -\langle x, y \rangle + x \times y \tag{9}$$

for all $a, b \in \mathbb{R}$ and $x, y, z \in \mathbb{R}^n$ where $n = 3$ or 7.

When we replace $\mathbf{R}$ by $\mathbf{C}$ we lose the ordering but we gain the Fundamental Theorem of Algebra, namely, "every non-constant polynomial over $\mathbf{C}$ has a zero in $\mathbf{C}$". And hence (thanks to the commutative property), a polynomial of degree n has exactly (if you count properly) n zeros. When we consider $\mathbf{R}^4$ we lose commutative property but we gain something. A polynomial may have infinitely many zeros. What a gain!

Here is the vector product table on $\mathbb{R}^7$

$\times$	e_1	e_2	e_3	e_4	e_5	e_6	e_7
e_1	0	e_4	e_7	$-e_2$	e_6	$-e_5$	$-e_3$
e_2	$-e_4$	0	e_5	e_1	$-e_3$	e_7	$-e_6$
e_3	$-e_7$	$-e_5$	0	e_6	e_2	$-e_4$	e_1
e_4	e_2	$-e_1$	$-e_6$	0	e_7	e_3	$-e_5$
e_5	$-e_6$	e_3	$-e_2$	$-e_7$	0	e_1	e_4
e_6	e_5	$-e_7$	e_4	$-e_3$	$-e_1$	0	e_2
e_7	e_3	e_6	$-e_1$	e_5	$-e_4$	$-e_2$	0

This table also gives (see (9)) the multiplication in $\mathbb{O}$.

Question : Does there exist integer n other than 1, 3 and 7 for which $\mathbb{R}^n$ has a vector product? This question is again answered by the following theorem.

Theorem L: *$\mathbb{R}^p$ has a vector product if and only if $p \in \{1, 3, 7\}$.*

Sums of Squares Formulae

We all know the sums of squares formulae

$$(a_1^2 + a_2^2)(\alpha_1^2 + \alpha_2^2) = A_1^2 + A_2^2, \quad \text{where}$$
$$A_1 = a_1\alpha_1 - a_2\alpha_2 \quad \text{and} \quad A_2 = a_1\alpha_2 + a_2\alpha_1. \tag{10}$$

So, product of sums of squares of integers is a sum of square of two integers. (10) follows from the fact that

$$\|z\|^2 \ \ \|w\|^2 = \|z \ \ w\|^2 \tag{11}$$

for any two complex numbers z and w. As the multiplication in $\mathbb{H}$ is also norm preserving, if we take quaternions in place of complex numbers in (11) we get[5]

$$\begin{aligned}(a_1^2+a_2^2+a_3^2+a_4^2) \quad & (\alpha_1^2+\alpha_2^2+\alpha_3^2+\alpha_4^2) \\ & = \ A_1^2+A_2^2+A_3^2+A_4^2, \\ \text{where} \quad A_1 &= a_1\alpha_1 \ - \ a_2\alpha_2 - a_3\alpha_3 - a_4\alpha_4 \\ A_2 &= a_1\alpha_2 \ + \ a_2\alpha_1 + a_3\alpha_4 - a_4\alpha_3 \\ A_3 &= a_1\alpha_3 \ - \ a_2\alpha_4 + a_3\alpha_1 + a_4\alpha_2 \\ A_4 &= a_1\alpha_4 \ + \ a_2\alpha_3 - a_3\alpha_2 + a_4\alpha_1. \end{aligned} \tag{12}$$

Similarly, from norm preserving octonian multiplication we get

$$\left(\sum_{r=1}^{8} a_r^2\right) \ \ \left(\sum_{r=1}^{8} \alpha_r^2\right) = \sum_{r=1}^{8} A_r^2,$$

where $A_1, \quad , A_8$ are given by

$$[A_1 \quad \cdot A_8] = [a_1 \quad \cdot a_8]\,[M] \tag{13}$$

$$[M] = \begin{bmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 & \alpha_5 & \alpha_6 & \alpha_7 & \alpha_8 \\ -\alpha_2 & \alpha_1 & -\alpha_5 & -\alpha_8 & \alpha_3 & -\alpha_7 & \alpha_6 & \alpha_4 \\ -\alpha_3 & \alpha_5 & \alpha_1 & -\alpha_6 & -\alpha_2 & \alpha_4 & -\alpha_8 & \alpha_7 \\ -\alpha_4 & \alpha_8 & \alpha_6 & \alpha_1 & -\alpha_7 & -\alpha_3 & \alpha_5 & -\alpha_2 \\ -\alpha_5 & -\alpha_3 & \alpha_2 & \alpha_7 & \alpha_1 & -\alpha_8 & -\alpha_4 & \alpha_6 \\ -\alpha_6 & \alpha_7 & -\alpha_4 & \alpha_3 & \alpha_8 & \alpha_1 & -\alpha_2 & -\alpha_5 \\ -\alpha_7 & -\alpha_6 & \alpha_8 & -\alpha_5 & \alpha_4 & \alpha_2 & \alpha_1 & -\alpha_3 \\ -\alpha_8 & -\alpha_4 & -\alpha_7 & \alpha_2 & -\alpha_6 & \alpha_5 & \alpha_3 & \alpha_1 \end{bmatrix}$$

Observe that, for $n = 2, 4$ and 8, $A_1, \ldots, A_n$ are linear in $a_1, \ldots, a_n$ and also in $\alpha_1, \ldots, \alpha_n$ in (10), (12) and (13) respectively. So, it is natural to ask for the values of n for which there exists an identity of the form $(a_1^2+\cdots+a_n^2)(\alpha_1^2+\cdots+\alpha_n^2) = A_1^2+\cdots+A_n^2$, where $A_1, \ldots, A_n$ are linear in

[5] Euler discovered formula (12) in 1748, much earlier than Hamilton's invention of quaternions, while investigating the theorem (later proved by Lagrange in 1869) that 'every positive integer is a sum of four integral squares'. Euler showed, by proving formula (12), that it is sufficient to prove the theorem for every prime. So, Euler knew quaternion multiplication!

$a_1, \ldots, a_n$ and also in $\alpha_1, \ldots, \alpha_n$. In 1896, A Hurwitz proved the following:

Theorem S: *If there exists an identity of the form* $(a_1^2 + \cdots + a_n^2)(\alpha_1^2 + \cdots + \alpha_n^2) = A_1^2 + \cdots + A_n^2$, *where* $A_1, \ldots, A_n$ *are linear functions of* $a_1, \ldots, a_n$ *and* $\alpha_1, \ldots, \alpha_n$ *then* $n = 1, 2, 4$ *or 8.*

In 1923, A Hurwitz proved the following stronger result (Theorem N). Any positive integer n can be expressed uniquely as: $n = 2^{4\alpha+\beta}(2\gamma+1)$, where $0 \leq \beta \leq 3$. Let $k(n) := 8\alpha + 2^\beta$ for that n.

Theorem N: *If there exists a bilinear* [6] *map such that* $f : \mathbb{R}^m \times \mathbb{R}^n \to \mathbb{R}^n$ *such that* $\|f(y,x)\| = \|y\| \cdot \|x\|$ *for all* $y \in \mathbb{R}^m$ *and* $x \in \mathbb{R}^n$ *then* $m \leq k(n)$.

Remark: In fact, Hurwitz showed (for a different proof see pages 140 and 156 in Husemoller) that for each n there is a bilinear map $f : \mathbb{R}^m \times \mathbb{R}^n \to \mathbb{R}^n$ satisfying $\|f(y,x)\| = \|y\| \ \|x\|$ for $m = k(n)$ but not for bigger m.

Theorem N also follows from another theorem of Adams. We will discuss all the proofs in Part 2 of this article.

[6] A map $f : \mathbb{R}^m \times \mathbb{R}^n \to \mathbb{R}^p$ is called bilinear if $f(a_1\alpha_1 + a_2\alpha_2, \beta) = a_1 f(\alpha_1, \beta) + a_2 f(\alpha_2, \beta)$ and $f(\alpha, b_1\beta_1 + b_2\beta_2) = b_1 f(\alpha, \beta_1) + b_2 f(\alpha, \beta_2)$ for all $\alpha, \alpha_1, \alpha_2 \in \mathbb{R}^m$ $\beta, \beta_1, \beta_2 \in \mathbb{R}^n$ and $a_1, a_2, b_1, b_2 \in \mathbb{R}$.

Address for Correspondence
Basudeb Datta
Department of Mathematics
Indian Institute of Science
Bangalore 560 012, India.
dattab@math.iisc.ernet.in

Suggested Reading

- **D Husemoller.** ***Fibre Bundles.*** **Springer-Verlag, 1966.**

Nowadays superelastic alloys are available that behave like rubber and are able to endure huge elastic deformations – two orders of magnitude greater than ordinary metals. On the other hand, many kinds of alloys can be brought to a super-elastic state, when they flow under very low pressure like heated glues.

Quantum Kaleidoscope. pp.33. Sept-Oct, 1995.