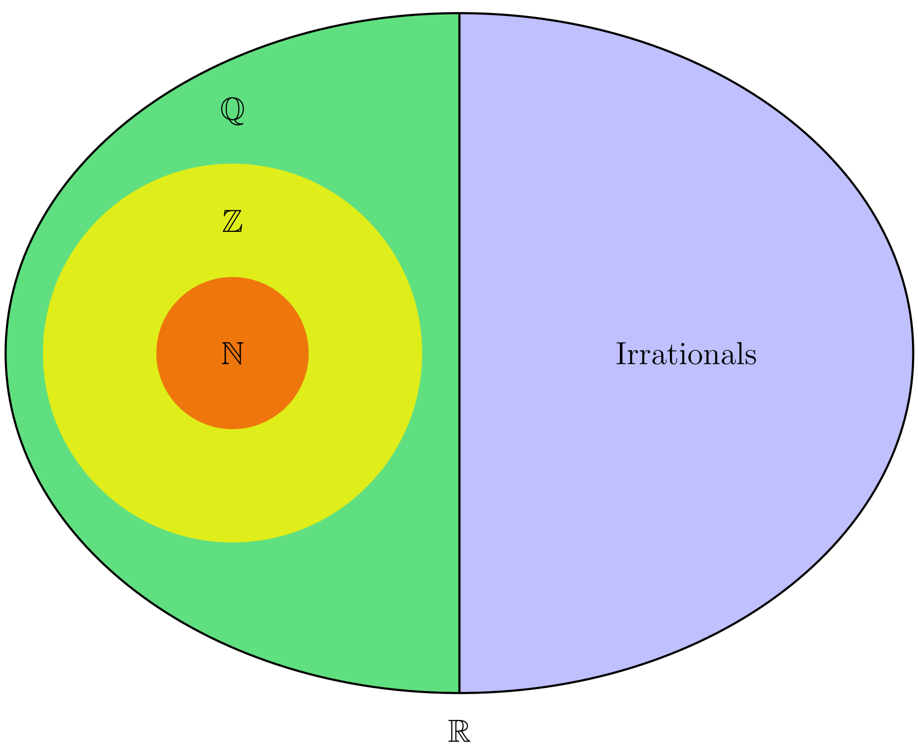
Some Notes on the Real Numbers and other Division Algebras

August 21, 2018

1 The Real Numbers

Here is the standard classification of the real numbers (which I will denote by $\mathbb{R}$).



I personally think of the natural numbers as

$$\mathbb{N} = \{0, 1, 2, 3, \cdots\}.$$

Of course, not everyone agrees with this particular definition. From a modern perspective, 0 is the "most natural" number since all other numbers can be built out of it using machinery from set theory. Also, I have never used (or even seen) a symbol for the whole numbers in any mathematical paper.

No one disagrees on the definition of the integers

$$\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \cdots\}.$$

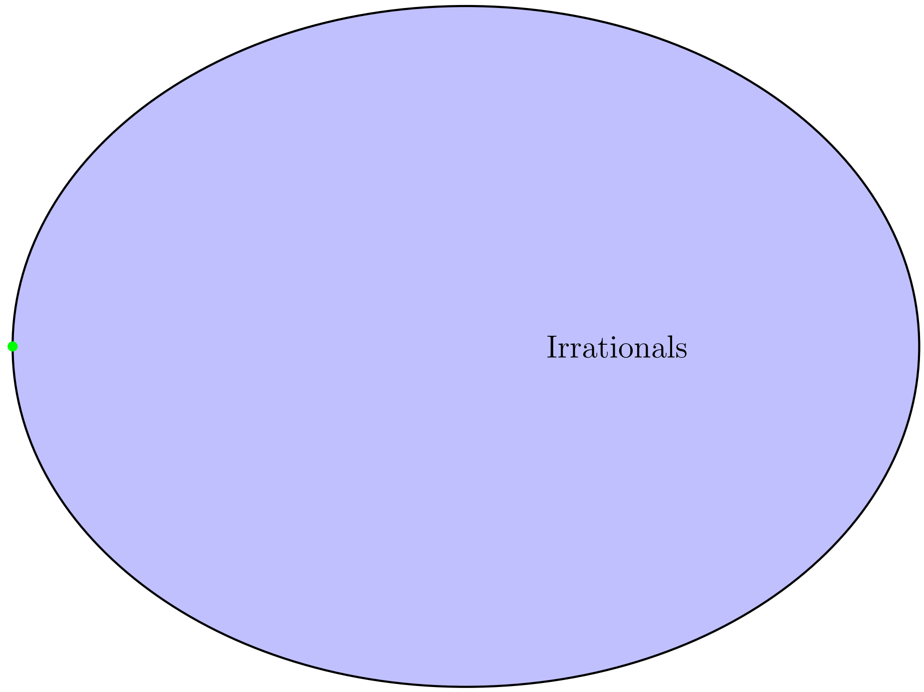
The fancy $\mathbb{Z}$ stands for the German word "Zahlen" which means "numbers." To avoid the controversy over what exactly constitutes the natural numbers, many mathematicians will use $\mathbb{Z}_{\geq 0}$ to stand for the non-negative integers and $\mathbb{Z}_{>0}$ to stand for the positive integers.

The rational numbers are given the fancy symbol $\mathbb{Q}$ (for Quotient):

$$\mathbb{Q} = \left\{ \frac{a}{b} \middle| \, a, b \in \mathbb{Z};\ b > 0;\ a \text{ and } b \text{ share no common prime factors} \right\}.$$

The set of irrationals is not given any special symbol that I know of and is rather difficult to define rigorously. The usual notion that a number is irrational if it has a non-terminating, non-repeating decimal expansion is the easiest characterization, but that actually entails a lot of baggage about representations of numbers. For example, if a number has a non-terminating, non-repeating decimal expansion, will its expansion in base 7 also be non-terminating and non-repeating? The answer is yes, but it takes some work to prove that. Notice that the Venn diagram for $\mathbb{R}$ is completely filled by the rationals and irrationals. This is because all real numbers are either rational or irrational!

The curious thing is that this representation of the reals is horribly misleading. From above, you might conclude that the reals are sort of half rational and half irrational. But that is totally untrue! While both sets are infinitely large, the infinity of irrational numbers completely overwhelms the infinity of rational numbers. In more technical language, we say that the rationals are *countably infinite* while the irrationals (and the reals as a whole) are *uncountably infinite* (or just *uncountable*). A more realistic diagram would be

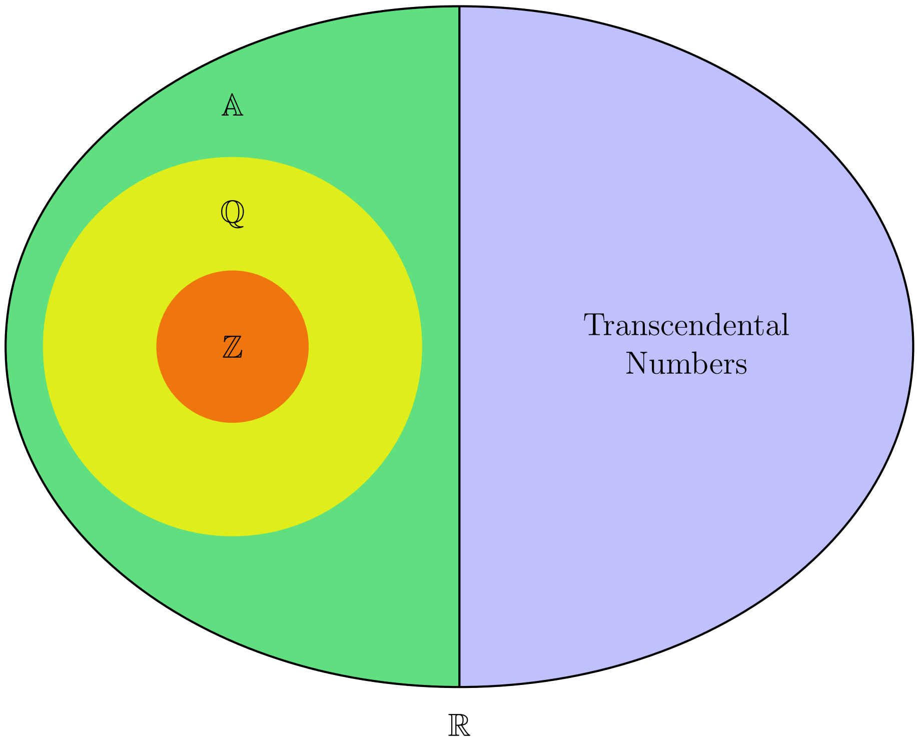


$\mathbb{R}$

The tiny green dot on the boundary is the entirety of $\mathbb{Q}$! In fact, if we were to be completely accurate, then you shouldn't be able to see the dot representing the rationals at all! If you could somehow pick a real number at random (which is physically impossible), then the probability that you would pick an irrational number is 100% even though it is possible to pick a rational number (probabilities become a little strange when you're dealing with sets like the reals)! The Reader's Digest version is that the vast majority of all real numbers are irrational.

This Venn diagram is still a little misleading. Even though the rational numbers, as a set, are insignificant as compared to the irrationals, the rationals and irrationals are mixed up in a complicated way along the real number line. A better mental image would be that the real number line is mostly comprised of irrational numbers with an almost imperceptible dusting of rational numbers over the whole thing. But any relatively simple analogy is going to misrepresent some aspect of the real numbers.

Actually, there is a slightly more interesting classification of the real numbers that is even more bewildering!



The sets of integers, $\mathbb{Z}$, and rationals, $\mathbb{Q}$, are the same as before (I omitted the circle for $\mathbb{N}$ to keep the diagram from being too crowded). $\mathbb{A}$ is the set of real algebraic numbers. These are all of the real numbers that are the zeros of polynomials with integer coefficients. For example, $\sqrt{2}$ is algebraic since it is the solution to $x^2 - 2 = 0$ (the other solution to this equation, $-\sqrt{2}$, is also algebraic). All rational numbers are algebraic since they are the solutions to equations like $bx - a = 0$. The number $\sqrt[3]{3} + \sqrt{2}$ is algebraic since it solves

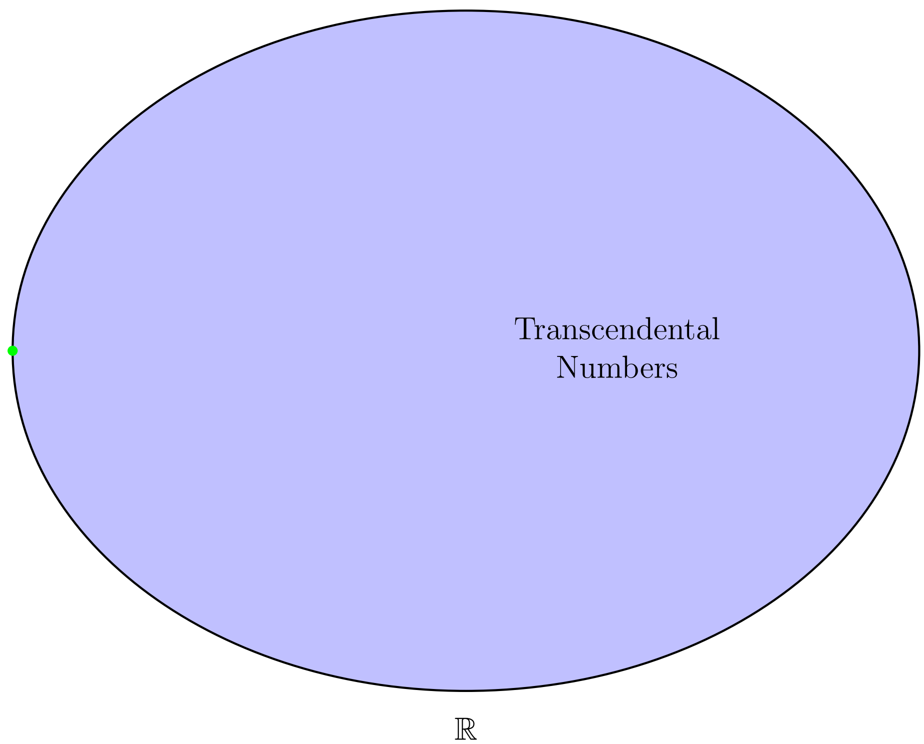
$$x^6 - 6x^4 - 6x^3 + 12x^2 - 36x + 1 = 0.$$

Basically, any number built out of rational numbers and square roots, cube roots, etc. will be algebraic. Curiously, there are algebraic numbers which cannot be expressed using roots! This is one of the conclusions from a branch of mathematics called Galois Theory. You can think of the algebraic numbers as the set of real numbers that have simple descriptions (e.g. $\sqrt{2}$ is a number such that when you square it and subtract 2 you get 0).

The set of transcendental numbers is the set of all real numbers which are not the roots of polynomials with integer coefficients. Proving a number is transcendental is hard work, but we know that π and e are definitely transcendental. One of the first numbers definitely proved to be transcendental is the Liouville Number

$$\sum_{k=1}^{\infty} 10^{-k!} = 0.110001000000000000000001000 \cdots .$$

Loosely, transcendental numbers are the real numbers which lack a simple (algebraic) description. What is so bewildering is that the set of algebraic numbers is still countably infinite while the set of transcendentals is uncountable! In other words, the actual diagram is more like the following.



Now, the tiny green dot (which should actually be invisible if we were completely accurate) is the entirety of $\mathbb{A}$. Since the vast majority of numbers we are familiar with are algebraic, and most of us only know a handful of transcendental numbers (like π and e), we are left with the very uncomfortable reality that the vast majority of real numbers are totally mysterious!

2 Division Algebras over the Real Numbers

We can generalize the notion of number a bit by considering *division algebras* over the real numbers. Essentially, these are extensions of the real numbers that retain the property that for any element a and any non-zero element b there is precisely one element x so that $a = bx$ and precisely one element y so that $a = yb$ (it could be that $x = y$). In this case, you can think of these numbers as

$$x = \frac{1}{b} \cdot a \text{ and } y = a \cdot \frac{1}{b}.$$

In other words, division algebras have a notion of division!

The real numbers themselves are the simplest division algebra over the reals. Since multiplication is commutative in the real number system, we have

$$\frac{1}{b} \cdot a = a \cdot \frac{1}{b} = \frac{a}{b}$$

so long as $b \neq 0$.

2.1 The Complex Numbers

The next simplest division algebra over the reals is the set of complex numbers,

$$\mathbb{C} = \{x + iy \mid x, y \in \mathbb{R}\},$$

where i is the imaginary unit ($i^2 = -1$). Addition/subtraction of complex numbers is defined component–wise:

$$(a + ib) + (x + iy) = (a + x) + i(b + y).$$

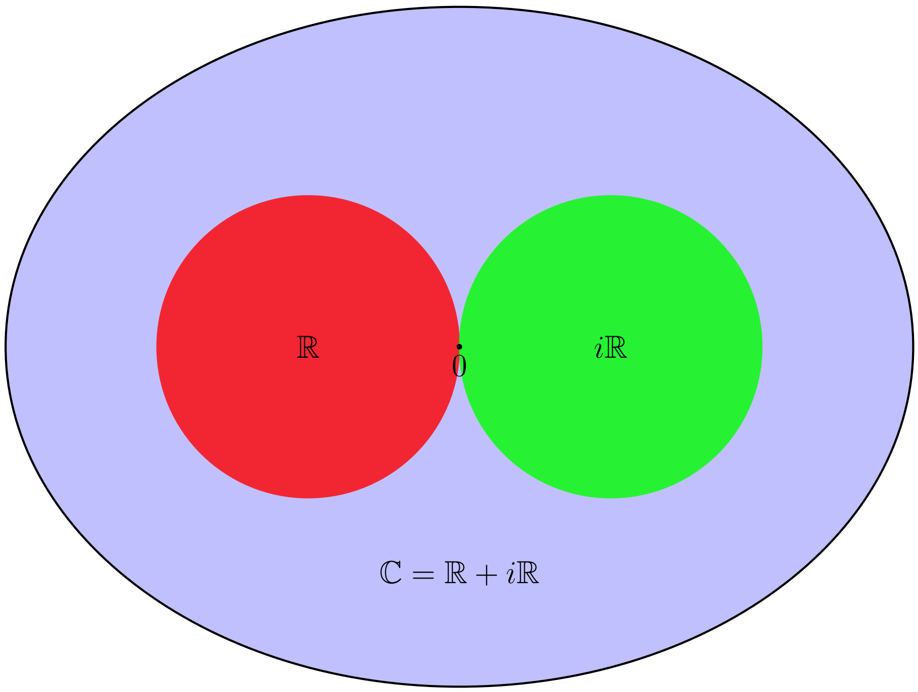
Multiplication is defined by extending the distributive property (and remembering the defining property of i):

$$(a + ib) \cdot (x + iy) = ax + iay + ibx + i^2by = (ax - by) + i(ay + bx).$$

We can show that multiplication is commutative for complex numbers. So, there is a unique multiplicative inverse for every non-zero complex number:

$$\frac{1}{x + iy} = \frac{1}{x + iy} \cdot \frac{x - iy}{x - iy} = \frac{x - iy}{x^2 + y^2} = \left(\frac{x}{x^2 + y^2}\right) - i\left(\frac{y}{x^2 + y^2}\right).$$

Since every complex number is the combination of a purely real part together with i times another real number (the imaginary part of the complex number), we can think $\mathbb{C} = \mathbb{R} + i\mathbb{R}$. Notice that the two sets $\mathbb{R}$ and $i\mathbb{R}$ intersect in exactly one point – namely 0.



It turns out that whenever we move from a less complicated division algebra to a more complicated one, some nice property of the original division algebra is lost. In the case of the complex numbers, it's a little difficult to see what nice property we lose. As it turns out, the complex numbers are no longer *totally ordered*. For two real numbers x and y, either $x < y, x = y$, or $x > y$. Basically, the real numbers can be totally ordered because they all lie along a line. Once you move to the complex numbers (which are two–dimensional), it is no longer possible to say that one complex number is smaller than another in any reasonable way.

2.2 The Quaternions

In 1843, William Hamilton discovered a four–dimensional division algebra over the reals, the quaternions:

$$\mathbb{H} = \{a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} \mid a, b, c, d \in \mathbb{R}\}.$$

The symbol $\mathbb{H}$ is for Hamilton (and because $\mathbb{Q}$ is already used for the rationals). Given our discussion for the complex numbers, it's no surprise that we can think of

$$\mathbb{H} = \mathbb{R} + \mathbf{i}\mathbb{R} + \mathbf{j}\mathbb{R} + \mathbf{k}\mathbb{R}.$$

The three imaginary units $\mathbf{i}, \mathbf{j}$, and $\mathbf{k}$ each satisfy $\mathbf{i}^2 = -1$, $\mathbf{j}^2 = -1$, and $\mathbf{k}^2 = -1$. Products of these three numbers are given by

$$\begin{aligned} \mathbf{i} \cdot \mathbf{j} &= \mathbf{k}, & \mathbf{j} \cdot \mathbf{i} &= -\mathbf{k}, \\ \mathbf{j} \cdot \mathbf{k} &= \mathbf{i}, & \mathbf{k} \cdot \mathbf{j} &= -\mathbf{i}, \\ \mathbf{k} \cdot \mathbf{i} &= \mathbf{j}, & \mathbf{i} \cdot \mathbf{k} &= -\mathbf{j}. \end{aligned}$$

Notice that $\mathbb{C}$ is a subset of $\mathbb{H}$ (just take the $\mathbf{j}$ and $\mathbf{k}$ terms to have coefficients of 0). The property that we lose in passing from the complex numbers to the quaternions is clear in the list above: quaternion multiplication is *non-commutative*! The product of two quaternions depends on the order you multiply them. In general, for two quaternions q_1 and q_2,

$$q_1 \cdot q_2 \neq q_2 \cdot q_1.$$

Just like with the complex numbers, addition of quaternions is defined by adding like components:

$$(a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}) + (x + y\mathbf{i} + z\mathbf{j} + w\mathbf{k}) = (a + x) + (b + y)\mathbf{i} + (c + z)\mathbf{j} + (d + w)\mathbf{k}.$$

Multiplication is defined by extending the distributive property (using the rules above for products of the imaginary units). Even though multiplication is not commutative, every quaternion has a unique multiplicative inverse:

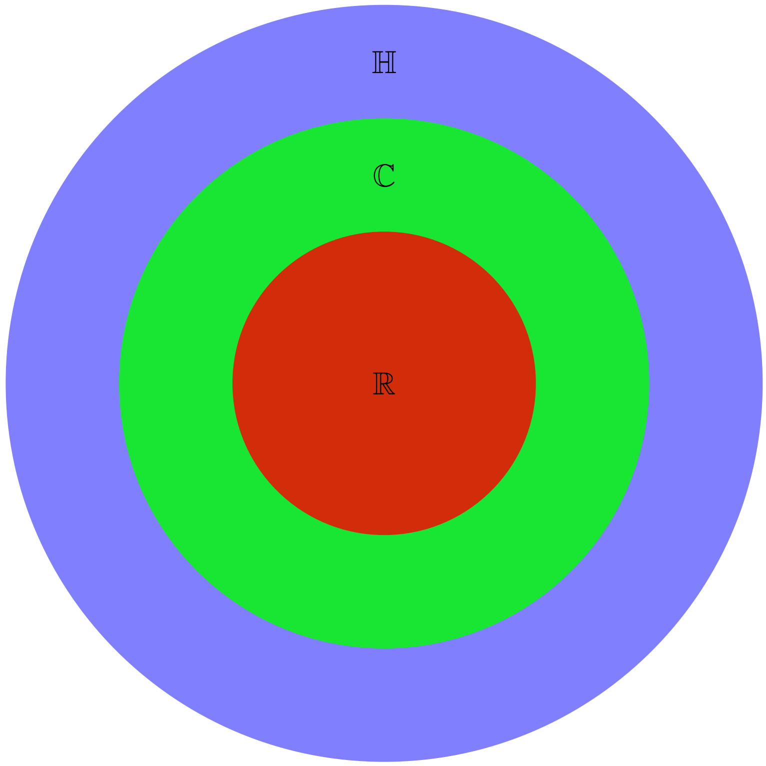
$$\frac{1}{a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}} = \frac{a - b\mathbf{i} - c\mathbf{j} - d\mathbf{k}}{a^2 + b^2 + c^2 + d^2}.$$

However, if q_1 and q_2 are two quaternions, the notation $\frac{q_1}{q_2}$ is ambiguous in general. Since multiplication is non-commutative,

$$\frac{1}{q_2} \cdot q_1 \neq q_1 \cdot \frac{1}{q_2},$$

for generic quaternions.

We now have expanded our notion of number to include three increasingly complex number systems.

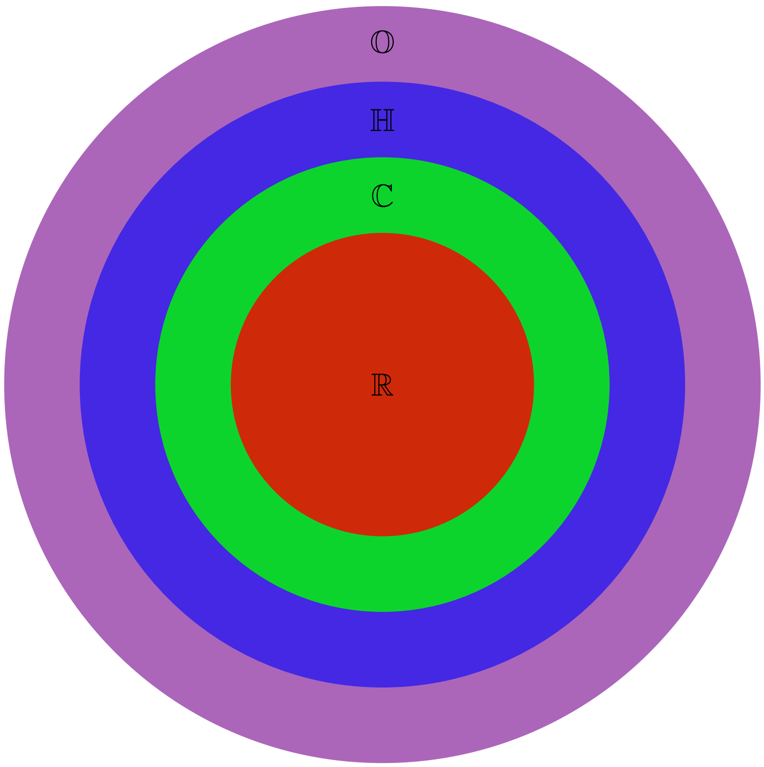


By the way, despite seeming rather abstract, quaternions are used extensively in many applications. In particular, the algebra of quaternions gives a rather fast algorithm for computing rotations in three dimensions. So, many graphics processors will use quaternions when dynamically rendering three–dimensional images.

2.3 The Octonions

We have a one–dimensional division algebra over the reals (namely $\mathbb{R}$ itself), a two–dimensional one ($\mathbb{C}$), and a four–dimensional one ($\mathbb{H}$). A natural question to ask is whether there is a three–dimensional division algebra over $\mathbb{R}$. In fact, this was what Hamilton initially set out to find. Try as he might, he could not make a three-dimensional version work, and this eventually led him to discover the four–dimensional quaternions discussed above. The fact that there is no division algebra of dimension three is a deep result. In fact, it was shown in the late 1950s that the only finite–dimensional division algebras over the reals are:

- $\mathbb{R}$ (the real numbers, one–dimensional)
- $\mathbb{C}$ (the complex numbers, two–dimensional)
- $\mathbb{H}$ (the quaternions, four–dimensional)
- $\mathbb{O}$ (the octonions, eight–dimensional)



It turns out that you have to double the dimension in order to have a consistent notion of division, but after the octonions, you lose too many nice algebraic properties.

The octonions are defined by

$$\mathbb{O} = \{a + b\mathbf{e_1} + c\mathbf{e_2} + d\mathbf{e_3} + f\mathbf{e_4} + g\mathbf{e_5} + h\mathbf{e_6} + k\mathbf{e_7} \mid a, b, \cdots, k \in \mathbb{R}\}\,.$$

Addition, as always, is defined by adding up like components. Just as before, we define multiplication by extending the distributive property in the usual way. All we really need to know is how to multiply the imaginary units $\mathbf{e_1}, \mathbf{e_2}, \cdots, \mathbf{e_7}$. This is difficult to summarize nicely. The best way is to give a multiplication table for these numbers.

$\cdot$	1	$\mathbf{e_1}$	$\mathbf{e_2}$	$\mathbf{e_3}$	$\mathbf{e_4}$	$\mathbf{e_5}$	$\mathbf{e_6}$	$\mathbf{e_7}$
1	1	$\mathbf{e_1}$	$\mathbf{e_2}$	$\mathbf{e_3}$	$\mathbf{e_4}$	$\mathbf{e_5}$	$\mathbf{e_6}$	$\mathbf{e_7}$
$\mathbf{e_1}$	$\mathbf{e_1}$	-1	$\mathbf{e_3}$	$-\mathbf{e_2}$	$\mathbf{e_5}$	$-\mathbf{e_4}$	$-\mathbf{e_7}$	$\mathbf{e_6}$
$\mathbf{e_2}$	$\mathbf{e_2}$	$-\mathbf{e_3}$	-1	$\mathbf{e_1}$	$\mathbf{e_6}$	$\mathbf{e_7}$	$-\mathbf{e_4}$	$-\mathbf{e_5}$
$\mathbf{e_3}$	$\mathbf{e_3}$	$\mathbf{e_2}$	$-\mathbf{e_1}$	-1	$\mathbf{e_7}$	$-\mathbf{e_6}$	$\mathbf{e_5}$	$-\mathbf{e_4}$
$\mathbf{e_4}$	$\mathbf{e_4}$	$-\mathbf{e_5}$	$-\mathbf{e_6}$	$-\mathbf{e_7}$	-1	$\mathbf{e_1}$	$\mathbf{e_2}$	$\mathbf{e_3}$
$\mathbf{e_5}$	$\mathbf{e_5}$	$\mathbf{e_4}$	$-\mathbf{e_7}$	$\mathbf{e_6}$	$-\mathbf{e_1}$	-1	$-\mathbf{e_3}$	$\mathbf{e_2}$
$\mathbf{e_6}$	$\mathbf{e_6}$	$\mathbf{e_7}$	$\mathbf{e_4}$	$-\mathbf{e_5}$	$-\mathbf{e_2}$	$\mathbf{e_3}$	-1	$-\mathbf{e_1}$
$\mathbf{e_7}$	$\mathbf{e_7}$	$-\mathbf{e_6}$	$\mathbf{e_5}$	$\mathbf{e_4}$	$-\mathbf{e_3}$	$-\mathbf{e_2}$	$\mathbf{e_1}$	-1

If we think of $\mathbf{e_1} = \mathbf{i}$, $\mathbf{e_2} = \mathbf{j}$, and $\mathbf{e_3} = \mathbf{k}$, then we can see that the quaternions sit inside of the octonions (as they should). The use of $\mathbf{e_i}$ for the imaginary units is simply for convenience.

Since octonion multiplication is not commutative (as the quaternions are not commutative), you have to read this table carefully. For example, to find $\mathbf{e_1} \cdot \mathbf{e_5}$, you find $\mathbf{e_1}$ in the left–hand column and $\mathbf{e_5}$ in the top row. Following the table gives

$$\mathbf{e_1} \cdot \mathbf{e_5} = -\mathbf{e_4}.$$

On the other hand $\mathbf{e_5} \cdot \mathbf{e_1} = \mathbf{e_4}$. The nice property we lose upon passing from the quaternions to the octonions is *associativity of multiplication.* For real numbers, complex numbers, and quaternions, multiplication satisfies

$$(x \cdot y) \cdot z = x \cdot (y \cdot z).$$

This means we can simply write $x \cdot y \cdot z$ for these numbers without any ambiguity. However, octonions do not have this property. For example,

$$(\mathbf{e_1} \cdot \mathbf{e_3}) \cdot \mathbf{e_5} = -\mathbf{e_7} \text{ but } \mathbf{e_1} \cdot (\mathbf{e_3} \cdot \mathbf{e_5}) = \mathbf{e_7}.$$

Octonions do enjoy a weaker version of associativity known as *alternativity*:

$$x \cdot (x \cdot y) = (x \cdot x) \cdot y \text{ and } y \cdot (x \cdot x) = (y \cdot x) \cdot x.$$

Finally, the multiplicative inverse of an octonion is very similar to the ones for complex numbers and quaternions:

$$\frac{1}{a + b\mathbf{e_1} + c\mathbf{e_2} + d\mathbf{e_3} + f\mathbf{e_4} + g\mathbf{e_5} + h\mathbf{e_6} + k\mathbf{e_7}}$$

$$= \frac{a - b\mathbf{e_1} - c\mathbf{e_2} - d\mathbf{e_3} - f\mathbf{e_4} - g\mathbf{e_5} - h\mathbf{e_6} - k\mathbf{e_7}}{a^2 + b^2 + c^2 + d^2 + f^2 + g^2 + h^2 + k^2}.$$

2.4 Beyond the Octonions

The process of doubling dimensions can actually be continued indefinitely. This leads to a sequence of higher and higher dimensional algebras over the reals. After the octonions, however, it becomes impossible to have a consistent notion of division. For example, doubling the octonions leads to the 16–dimensional algebra $\mathbb{S}$, known as the sedenions (you would now have imaginary units $\mathbf{e_1}$ up to $\mathbf{e_{15}}$). You can still add and multiply sedenions together, but it turns out that you can multiply two non-zero sedenions together and obtain zero! As an example,

$$(\mathbf{e_3} + \mathbf{e_{10}}) \cdot (\mathbf{e_6} - \mathbf{e_{15}}) = 0.$$

The loss of the Zero Product Property is disastrous for the notion of divisibility (though you can still define multiplicative inverses for the sedenions)! If you're curious, the multiplication table for the sedenions can be found on Wikipedia.