Quaternions and Groups

Rich Schwartz

October 16, 2014

1 What is a Quaternion ?

A *quaternion* is a symbol of the form

$$a + bi + cj + dk,$$

where a, b, c, d are real numbers and i, j, k are special symbols that obey the following algebraic rules.

$$i^2 = j^2 = k^2 = -1,$$

$$ij = k, \qquad jk = i, \qquad ki = j,$$

$$ji = -k, \qquad kj = -i, \qquad ik = -j,$$

$$ix = xi, \qquad jx = xj, \qquad kx = xk, \qquad \text{for all real } x$$

Quaternions are added componentwise, like vectors. For instance

$$(3 + 4i + j) + (7 + 2j + k) = 10 + 4i + 3j + k.$$

Quaternions are multiplied according to the foil method. Just expand everything out, and then use the rules above to simplify the expression so that it looks like a quaternion. For instance

$$(4 + j)(i + k) = 4i + 4k + ji + jk = 4i + 4k - k + i = 5i + 3k.$$

Quaternions are often denoted by single variables, like complex numbers. For instance

$$q = a + bi + cj + dj.$$

2 Other Operations on Quaternions

There are several operations on quaternions worth knowing. The *conjugate* of q is defined as

$$\overline{q} = a - bi - cj - dk.$$

The *square-norm* of q is defined as

$$|q|^2 = q\overline{q} = a^2 + b^2 + c^2 + d^2.$$

Taking square roots gives what is called the *norm*

$$|q| = \sqrt{q\overline{q}} = \sqrt{a^2 + b^2 + c^2 + d^2}.$$

Geometrically $|q|$ denotes the length of the vector (a, b, c, d) corresponding to q.

If we define

$$q^{-1} = \frac{\overline{q}}{|q|^2} = \frac{a - bi - cj - dk}{a^2 + b^2 + c^2 + d^2},$$

then

$$qq^{-1} = q^{-1}q = 1.$$

You have to be careful about defining p/q. This could mean pq^{-1} or $q^{-1}p$, and you might not get the same answer. So, it is best not to define p/q and simply to live with the fact that there are two competing notions of division, namely pq^{-1} and $q^{-1}p$.

The quaternions almost form a field. They have the basic operations of addition and multiplication, and these operations satisfy the associative laws,

$$(p + q) + r = p + (q + r), \qquad (pq)r = p(qr).$$

and the distributive law

$$p(q + r) = pq + pr.$$

Also, the addition law is commutative

$$p + q = q + p.$$

Both 0 and 1 are quaternions. Also, for any nonzero quaternion q, there is a quaternion $(-q)$ such that $q + (-q) = 0$ and a quaternion q^{-1} such that $qq^{-1} = q^{-1}q = 1$. The only thing missing is the commutative law for the multiplication. It is not always true that $pq = qp$. A set with all these properties (but without $pq = qp$) is called a *division ring* rather than a field.

3 A Basic Equation

It is not always true that $qr = rq$ for quaternions q and r. However, here is a variant which is always true.

$$\overline{rq} = (\overline{q})(\overline{r}). \tag{1}$$

Just to emphasize the order of operations, this formula says that the conjugate of rq is equal to the conjugate of q times the conjugate of r.

The proof of Equation1 is very much like the proof of the complex number angle addition formula that I did in class. Say that a pair (q, r) of quaternions is *good* if the formula holds for q and r. For example, the pair $(1, i)$ is good because

$$\overline{i \times 1} = -i, \qquad \overline{1} \times \overline{i} = -i.$$

Similarly, the pair (i, j) is good because

$$\overline{ji} = \overline{-k} = k, \qquad \overline{i} \times \overline{j} = (-i)(-j) = ij = k.$$

Similar checks show that all 16 pairs $q, r)$ are good when q is one of $1, i, j, k$ and r is one of $1, i, j, k$.

If (q, r) is good and x is any real number, then (xq, r) and (q, xr) are also good.

If (q_1, r) and (q_2, r) are good, then so is $(q_1 + q_2, r)$. To see this, just write it out and use the distributive law:

$$\overline{r(q_1 + q_2)} = \overline{rq_1} + \overline{rq_2} = (\overline{q_1})(\overline{r}) + (\overline{q_2})(\overline{r}) = (\overline{q_1 + q_2})(\overline{r}).$$

If (q, r_1) and (q, r_2) are good, then so is $(q, r_1 + r_2)$. This computation is the same as what we just did.

All these rules combine to show that any pair of quaternions is good. In other words, Equation 1 is always true.

We can use Equation 1 to prove that the norms multiply when we multiply together quaternions.

$$|qr|^2 = (qr)(\overline{qr}) =_1 (qr)(\overline{r})(\overline{q}) = q|r|^2\overline{q} =_2 (q\overline{q})||r| = |q|^2|r|^2.$$

Equality 1 uses Equation 1. Equality 2 comes from the fact that real numbers always commute with quaternions. The other equalities are basically the associative law.

Taking square roots of the equation gives $|qr| = |q||r|$.

4 Groups

One of the themes in modern mathematics is abstraction. Some familiar idea, like using addition or multiplication to combine numbers, is put in a more abstract setting. New "objects" are defined which share some of the same properties as numbers, and then these objects are studied. This approach seems a bit wierd at first – why would you want to do this? – but it turns out to reveal hidden connections between things which seemed very different. The idea of a group is an abstraction like this.

A *group* is a set, together with an operation on its members, which satisfies certain axioms. The operation is initially denoted $(*)$, and later on the notation is usually simplified. Call the set G. Here are the axioms.

1. If $a, b \in G$ are any two members, then $a * b$ is defined, and also a member of G.

2. The associative law holds: $(a*b)*c = a*(b*c)$ for every three $a, b, c \in G$.

3. There is an "identity element", called e, so that $e * a = a * e = a$ for all $a \in G$.

4. For every element $a \in G$ there is another element $b \in G$ with the property that $a*b = b*a = e$. The element b is usually written as a^{-1}.

Notice that the property $a * b = b * a$ is not listed as an axiom. When this additional property holds for all pairs of elements, G is called *commatitive* or (more commonly) *abelian*. When the property fails for at least one pair of elements, G is called *noncommutative* or (more commonly) *nonabelian*.

Why *abelian*? This terminology honors Neils Henrick Abel (1802-1829), the person who proved that you couldn't "solve" the quintic with the same kind of formula that you could use for quadratics, cubics, and quartics. This business is actually very closely related to the theory of groups.

Here are some examples of groups.

- Let $G = \boldsymbol{Z}$ be the integers and let $(*)$ be addition. Then the element e is 0 and a^{-1} is just $-a$. So, the integers form a group when you use addition.

- Let G be the set of nonzero real numbers. Let $(*)$ be multiplication. In this case, the identity element is 1, and $a^{-1} = 1/a$.

- Pick some positive integer n, and let $G = \{0, 1, ..., n-1\}$. The symbol $a * b$ is defined as follows: Add a and b and then take the remainder you get when you divide by n. For instance, if $n = 5$ then $2 * 4 = 3$. The identity element is 0 and for $a \neq 0$, we have $a^{-1} = n - a$. When $a = 0$, we have $a^{-1} = 0$. This example is often denoted $\boldsymbol{Z}/n$. It is an example of a finite abelian group.

- Let S be any set and let $A(S)$ denote the set of bijections from S to itself. The group law is the composition of bijections. For instance, if $a : S \to S$ is a bijection and so is $b : S \to S$, then $a * b$ is defined by the rule that
$$(a * b)(s) = a(b(s)),$$
for all $s \in S$. The composition of two bijections is also a bijection, so this is well defined. The identity element is the identity map, and the inverse of a bijection is again a bijection. So $A(S)$ is a group. When S is a finite set with n elements, $A(S)$ is a finite group with $n!$ elements. When $n > 2$, this group is nonabelian.

- Let G be the set of unit complex numbers, and let $*$ denote multiplication. The product of two unit complex numbers is also a unit complex number. The identity element is 1, and $z^{-1} = 1/z = \overline{z}$, which is again a unit complex number. So, G forms a group. Geometrically, we have turned the circle into a group!

How does all this relate to quaternions? Well, the last example also works for the quaternions. Let G denote the set of unit quaternions – quaternions with norm 1. Let $*$ be multiplication. If $|q| = 1$ and $|r| = 1$, then

$$|q * r| = |q||r| = 1 \times 1 = 1.$$

So the operation is well defined on G. The identity element is once again 1, and $q^{-1} = \overline{q}$. To see that this works, note that

$$qq^{-1} = q\overline{q} = 1, \qquad q^{-1}q = \overline{q}q = 1.$$

So, all the axioms hold. Geometrically, the set of unit quaternions is the set of all solutions to the equation $a^2 + b^2 + c^2 + d^2 = 1$. This is a higher dimensional version of the sphere and is often denoted S^3. What I am saying is that quaternionic multiplication turns S^3 into a group.

5 Rotations of Space

Let $\boldsymbol{R}^3$ denote ordinary three dimensional space. It is best to think of the points in $\boldsymbol{R}^3$ as vectors. Distances are measured on $\boldsymbol{R}^3$ using the dot product

$$\text{distance}(V, W) = \sqrt{(V - W) \cdot (V - W)}.$$

This is really just the pythagorean theorem. A *rotation of space* is a bijection $f : \boldsymbol{R}^3 \to \boldsymbol{R}^3$ which satisfies 3 properties:

- $f(0, 0, 0) = (0, 0, 0)$. The origin is fixed.
- f preserves dot products (and hence distances). That is

  $$f(V) \cdot f(W) = V \cdot W$$

  for all $V, W \in \boldsymbol{R}^3$.
- f is orientation preserving. This last condition is often discussed in terms of the right hand rule. If V, W, X forms a right-handed basis, then so does $f(V), f(W), f(X)$. The right hand rule means that if you curl your the fingers from V to W, then your thumb points along X (rather than along $-X$.)

If you have two rotations f and g, you can compose them. The composition $f \circ g$ is also a rotation of space. The identity element is just the rotation that "does nothing". That is $e(V) = V$ for all V. Finally, rotations are bijections, and their inverse maps are also rotations. Intuitively, if you can do a rotation, you can simply do it in reverse. In short, the set of rotations of space forms a group.

The group of rotations of space is often denoted $SO(3)$, which stands for *special orthogonal group* of rotations of $\boldsymbol{R}^3$. The latter O stands for "orthogonal", which is a name people give to maps of space which preserve the dot product. Technically "orthogonal" means "perpendicular", and the terminology derives from the fact that these kinds of maps preserve the property of perpendicularity. Finally the S stands for "special", and this is the orientation preserving property. So, $SO(3)$ stands for "group of special orthogonal maps of 3-dimensional space".

I wanted to take some time explaining the crazy notation (rather than making up my own) because sometimes this kind of mysterions notation can make a subject look incomprehensible. I wanted to demystify it.

6 The Spin Cover

Let S^3 denote the group of unit quaternions and let $SO(3)$ denote the group of rotations of space. Amazingly, there is a map from S^3 to $SO(3)$. This map is often called *the spin cover*. This terminology comes from physics. When $SO(3)$ is interpreted as the possible positions of a particle, the extra information you get by looking at S^3 is the *spin* of the particle.

Given a unit quaternion q, we want to come up with a rotation of space, and we're going to call this rotation R_q. Here's the idea. We can think of $\boldsymbol{R}^3$ as the set of pure quaternions

$$(a, b, c) \leftrightarrow 0 + ai + bj + ck.$$

(*Pure* means that there is no real component.) If V and W are pure quaterions, then the dot product $V \cdot W$ is just exactly the real component of $-VW$.

So, here's the formula

$$R_q(V) = qV\overline{q}. \tag{2}$$

On the right hand side of the equation, we're multiplying 3 quaternions together.

First, let's check that $R_q(V)$ is another pure quaternion. Note that a quaternion W is pure if $\overline{W} = -W$. So, we just have to check this for $W = R_q(V)$. The check involves several uses of Equation 1. Here goes

$$\overline{R_q(V)} = \overline{qV\overline{q}} = (\overline{V\overline{q}})q = (q\overline{V})\overline{q} = q(-V)\overline{q} = -qV\overline{q} = -R_q(V).$$

So, it works. This means that R_q is some kind of map from $\boldsymbol{R}^3$ to $\boldsymbol{R}^3$. Now we want to see that, actually, it is a rotation. Let's check the rotation properties.

Origin Fixed: Let $\boldsymbol{O}$ denote the zero quaternion. We have $R_q(\boldsymbol{O}) = q\boldsymbol{O}\overline{q} = \boldsymbol{O}$. This is the first property.

Dot Product Preserved: From what we have said about the dot product, the second property boils down to showing that WV and $R_q(V)R_q(W)$ have the same real components for any two pure quaternions V and Q. Note that

$$R_q(V)R_q(W) = (qV\overline{q})(qW\overline{q}) = qV(\overline{q}q)W\overline{q} = qVW\overline{q}.$$

This equation works because $\overline{q}q = 1$.

Let's write $X = VW$. We want to see that X and $qX\overline{q}$ have the same real component. We already know that this works in case the real component is 0. So, lets write $X = X_1 + X_2$ where X_1 is real and X_2 is pure. Since X_1 is real, it commutes with all quaternions. We have

$$qX\overline{q} = q(X_1 + X_2)\overline{q} = qX_1\overline{q} + qX_2\overline{q} = X_1(q\overline{q}) + qX_2\overline{q} = X_1 + qX_2\overline{q}.$$

The real component of $X_1 + qX_2\overline{q}$ is just X_1 because $qX_2\overline{q}$ is pure. So, the real component of $R_q(X)$ is X_1 and the real component of X is X_1. It works.

Orientation Preserved: The right hand rule can also be checked algebraically, but this is something of a pain. Here is another approach. Every dot-product preserving map of $\boldsymbol{R}^3$ either preserves orientation or reverses it. The latter cases happens when you are reflecting in a mirror. So, imagine that you continuously vary the quaternion R_q and ask the question: Does R_q preserve orientation or reverse it? The answer can't suddenly switch. So, whatever answer you get for one particular quaternion, you get for all of them. Let's ask the question when $q = 1$. In this case R_q is the identity map, which preserves orientation. Since the answer is yes for 1, it is yes for all q. That's it.

Now we know that R_q really is a rotation. This gives us a map from S^3 to $SO(3)$. What is the nature of this map? First of all $R_{-q} = R_q$, because

$$(-q)V(\overline{-q}) = (-q)V(-\overline{q}) = qV\overline{q}.$$

So, q and $-q$ give rise to the same rotation.

Now let's check how this map behaves with respect to the group laws. For instance, what does R_{qr} do? We compute

$$R_{qr}(V) = qrV(\overline{qr}) = qrV(\overline{r})(\overline{q}) = R_q(R_r(V)).$$

In short,

$$R_{qr} = R_q \circ R_r.$$

So, the map converts the one group law (quaternion multiplication) to the other one (composition.) Maps between groups which have this property are called *homomorphisms*.

Suppose that $R_q = R_r$. It turns out that $r = \pm q$ in this case. That means that the map from S^3 to $SO(3)$ is a 2-to-1 map. Each rotation of space is represented by precisely 2 quaternions.

7 The Last Word

The only thing I haven't proved is the claim that $R_r = R_q$ implies $r = \pm q$. I'll do it in this section.

Suppose that $R_q = R_r$. The quaternion $\overline{q}$ has the property that $\overline{q}q = 1$. We have

$$R_1 = R_{q\overline{q}} = R_{\overline{q}} \circ R_q = R_{\overline{q}} \circ R_r = R_{\overline{q}r}.$$

So, $R_{\overline{q}r}$ and R_1 are the same map.

It is convenient to set $s = \overline{q}r$. Now we know that R_s and R_1 are the same map. That means that

$$R_s(V) = sV\overline{s} = V,$$

for all pure quaterions V. But now we have

$$Vs = (sV\overline{s})s = sV(\overline{s}s) = sV.$$

In short $sV = Vs$ for all pure quaternions V. This implies that $s = \pm 1$. Hence

$$\overline{q}r = \pm 1.$$

But this means that

$$r = q(\overline{q}r) = qs = \pm q.$$

That's the end of the proof.

8 Exercises

Work on 4 out of 6 of these.

1. Suppose that $q = (2 - i + 3j)$ and $r = (5 + i - j - k)$. What is $qr - rq$.

2. Suppose that V and W are pure quaternions. Work out VW in terms of the dot product $V \cdot W$ and the cross product $V \times W$.

3. Consider the equation $q^2 = -1$. How many quaternion solutions does this have, and why?

4. Suppose that s is a quaternion and that $sV = Vs$ for all pure quaternions V. Prove that $s = \pm 1$. (Hint: write out $s = a + bi + cj + dk$ and try various

possibilities for V.)

5. Describe in geometrical terms what the rotation R_q does to space, when q is the quaternion $\cos(\theta) + i\sin(\theta)$.

6. An *integer quaternion* is a quaternion of the form $a + bi + cj + dk$, where a, b, c, d are all integers. Of all the prime numbers less than 20, which can be written as the form $q\overline{q}$, when q is an integer quaternion. Do you see a pattern?