Day 1: Complex Numbers

Here I stand (here I stand)
Looked around, around, around, around, around
But you won't see me (but you won't see me)

– Queen, "Now I'm Here"

Definition 1.1. A **complex number** is a pair of real numbers (a, b), which we will write as $a + bi$.

Exercise 1.1. Thinking of $i = \sqrt{-1}$, and assuming all the standard rules of multiplication (associativity, commutativity, distributivity), define addition and multiplication laws:

$$(a + bi) + (c + di) = (?) + (?)i$$
$$(a + bi)(c + di) = (?) + (?)i$$

Definition 1.2. If $z = a + bi$ is a complex number, we define the **conjugate** of z to be $\bar{z} = a - bi$.

Exercise 1.2. Prove that $\bar{\bar{z}} = z$. Geometrically, what does the map $z \to \bar{z}$ do to the plane?

Definition 1.3. Given a complex number $z = a + bi$, we define the **real part**, $\mathrm{Re}(z) = a$, and the **imaginary part**, $\mathrm{Im}(z) = bi$.

Exercise 1.3. Write down formulas for the real and imaginary parts of a complex number z in terms of z and $\bar{z}$.

Exercise 1.4. Give a reasonable definition for the *length*, $\|z\|$, of a complex number $z = a+bi$. Can you express this purely in terms of z and $\bar{z}$ (that is, without referencing the individual components a and b)?

Exercise 1.5. Find a formula for the inverse of a nonzero complex number z (that is, the number z^{-1} such that $z^{-1}z = 1$). Again, do this without referencing individual components.

Exercise 1.6. Prove that if z and w are complex numbers, then $\|zw\| = \|z\|\|w\|$.

Exercise 1.7. If the whole numbers m and n can each be written as a sum of two squares (for example, $5 = 2^2 + 1^2$ and $13 = 3^2 + 2^2$), prove that mn can as well.

Exercise 1.8. Thinking of $a + bi$ as a vector, what is the result when you rotate it 90° counterclockwise? Find a complex number $c + di$ such that $(c + di)(a + bi)$ equals this result.

Exercise 1.9. Repeat the above problem for 180° and 270°. Can you express rotation by 45° as multiplication by some complex number? In general, given an angle θ, what complex number must we multiply by in order to rotate by θ?

Exercise 1.10. Using Exercises 1.6 and 1.9, describe multiplication of complex numbers purely in terms of geometric operations.

1.1 Follow-up Questions

Exercise 1.11. Let's get some practice with complex number arithmetic. Compute the following:

$$(2-i)\overline{(4+7i)}, \quad \frac{1}{(1+2i)}, \quad \frac{3+4i}{2+5i}, \quad \left(\frac{1+i}{\sqrt{2}}\right)^{100}$$

Exercise 1.12. Prove the triangle inequality algebraically (try to do this without referencing the components).

$$\|z+w\| \leq \|z\| + \|w\|$$

Exercise 1.13. We've seen that $z \mapsto \bar{z}$ represents a reflection across the real number line, and multiplication by a complex number can represent rotation around 0 by any angle. Come up with a formula (using only z, $\bar{z}$, and arithmetic operations) for:

- Rotation by θ around the point $2+i$ (can you generalize to any point?)
- Reflection across the line with slope 1 through i (can you generalize to any line?)

Exercise 1.14. Write 13520 as the sum of two squares. (Please do not try to do this with brute force. There is a trick!)

Exercise 1.15. Prove $\frac{\pi}{4} = \arctan\frac{1}{2} + \arctan\frac{1}{3}$ by considering $(2+i)(3+i)$.

(Historical note: since there are good algorithms for computing arctangents, a similar identity allowed John Machin to compute 100 digits of π by hand in 1706. His formula, which can be derived from $(5+i)^4(239-i)$, continued to be used well into the computer era to produce record numbers of digits)

Day 2: Quaternions: Failed Experiments

Oh yes, we'll keep on trying
Tread that fine line
Oh, we'll keep on trying, Yeah
Just passing our time

– Queen, "Innuendo"

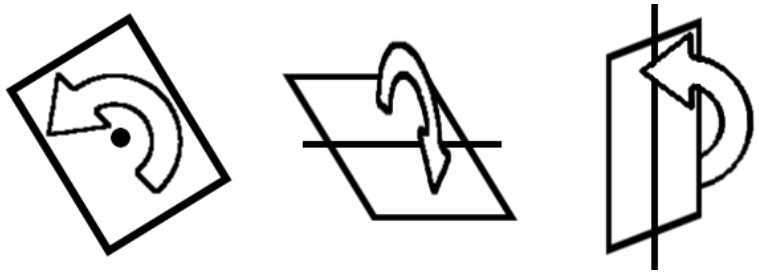
We saw yesterday that for $\mathbb{C} = \{x + yi \mid x, y \in \mathbb{R}\}$, we only had to assume $i^2 = -1$ (and the distributive law) to get a very beautiful and rich structure which allowed us to do a lot of plane geometry: rotation, reflection, lengths, scaling, etc.

Let's try to develop a number system that allows us to do 3-d geometry! We want a set $D = \{x + yi + zj : x, y, z \in \mathbb{R}\}$ with the following properties:

- D is a vector space: adding elements is done in each component separately, and multiplying anything by a real number (on either side) will scale each component.
- D contains $\mathbb{C}$; that is, $i^2 = -1$. 2-d geometry is a subset of 3-d geometry, after all!
- Multiplication by an element of D can be described as a geometric operation (e.g. scaling and rotating).

Exercise 2.1. Using the properties above, convince yourself that multiplication is associative ($(zw)v = z(wv)$ for all $v, w, z \in D$).

Exercise 2.2. Use the picture below as a guide: keep the page still, and rotate other things according to these rules. Are 3D rotations commutative?



Exercise 2.3. By expressing ij as an element of D, write $i(ij)$ in two different ways as an element of D, and show that something has gone very wrong.

So it turns out that a 3-dimensional number system is not going to work for us. But should we even expect 3 dimensions of numbers to be enough to describe 3-dimensional geometry?

Exercise 2.4. Rotations of $\mathbb{R}^2$ around the origin can be described using one number: the angle. How many numbers does it take to describe a rotation of $\mathbb{R}^3$ around the origin?

Exercise 2.5. Every rotation of the plane can be described by a complex number of length 1. If we want every rotation of 3-d space to be described by a number of length 1, what can we say about the dimension of this number system?

So it isn't going to be enough to just add a single dimension — we actually need something *four*-dimensional to describe 3-D geometry. But we built $\mathbb{C}$ using pairs of real numbers; what if we tried building a number system out of pairs of complex numbers?

Exercise 2.6. We can define multiplication on $\mathbb{C}$ as an operation on pairs of real numbers. By direct analogy, come up with a multiplication rule for pairs of complex numbers.

$$(z_1, w_1) * (z_2, w_2) = (?, ?)$$

Exercise 2.7. Show that $(1, 0)$ is a multiplicative identity.

In order to represent geometry, we want to be able to invert any nonzero element (any scaling or rotation can be undone unless it shrinks everything to zero). This means that for any (A, B) (other than $(0, 0)$), there should be (z, w) such that $(z, w) * (A, B) = (1, 0)$

Exercise 2.8. Thinking of your formula for $(z, w) * (A, B) = (1, 0)$ as a system of equations, can you always solve for z and w in terms of A and B?

Exercise 2.9. Modify the multiplication formula to ensure that you will always be able to solve for z and w in terms of A and B.

Note that if we take one of these new numbers and write it as $(a + bi, c + di)$, we can write it as

$$a(1, 0) + b(i, 0) + c(0, 1) + d(0, i).$$

In other words, if we label the elements

$$1 = (1, 0), \qquad i = (i, 0), \qquad j = (0, 1), \qquad k = (0, i),$$

then we can write this new number as $a + bi + cj + dk$.

Exercise 2.10. Using your updated definition of multiplication, fill in the following multiplication table (take the element down the left side, and multiply it by the element along the top, in that order).

	1	i	j	k
1				
i				
j				
k				

Exercise 2.11. Inscribe your results into the stone of Brougham Bridge.

2.2 Follow-up Questions

Exercise 2.12. We say that a number x is a **zero divisor** if there exists a nonzero number y such that $yx = 0$. Show that zero divisors do not have multiplicative inverses.

Exercise 2.13. Show that the multiplication you defined in Exercise 2.6 has zero divisors. Can this number system encode rotations?

Exercise 2.14. How many numbers do we need to encode a rotation of $\mathbb{R}^4$ around the origin?

Exercise 2.15. If we want every rotation of 4-D space to be described by a number of length 1, what's the dimension of this number system?

Exercise 2.16. (Challenge) Show that such a number system cannot exist.

Exercise 2.17. (Challenge) In general, how many numbers do we need to encode a rotation on $\mathbb{R}^n$?

Day 3: Exploring Quaternions

Is this the world we created?
What did we do it for
Is this the world we invaded
Against the law

– Queen, "Is This The World We Created?"

Reference and Identities

Let $\mathbb{H}$ denote the set of quaternions; elements of $\mathbb{H}$ can be thought of either as pairs of complex numbers (z, w), or in terms of four real numbers, $a + bi + cj + dk$. Given as pairs of complex numbers, they can be multiplied together as follows:

$$(z_1, w_1)(z_2, w_2) = (z_1 z_2 - w_1 \bar{w}_2, z_1 w_2 + w_1 \bar{z}_2).$$

Given in the form $a + bi + cj + dk$, they can be multiplied by expanding out and applying the multiplication table you filled out yesterday. Multiplication is not commutative.

Given a quaternion $q = (z, w) = a + bi + cj + dk \in \mathbb{H}$, we can define the following operations on it:

q	(z, w)	$a + bi + cj + dk$
$\mathrm{Re}(q)$	$(\mathrm{Re}(z), 0)$	a
$\mathrm{Im}(q)$	$(\mathrm{Im}(z), w)$	$bi + cj + dk$
$\bar{q}$	$(\bar{z}, -w)$	$a - bi - cj - dk$
$\|q\|$	$\sqrt{\|z\|^2 + \|w\|^2}$	$\sqrt{a^2 + b^2 + c^2 + d^2}$

A quaternion is **purely imaginary** if $\mathrm{Re}(q) = 0$. The set of purely imaginary quaternions (which we call $\mathrm{Im}(\mathbb{H})$) is isomorphic to $\mathbb{R}^3$ as a vector space.

Exercise 3.1. Prove the following identities.

$$q\bar{q} = \|q\|^2 \qquad \overline{qr} = \bar{r}\bar{q} \qquad \|qr\| = \|q\|\|r\| \qquad (qr)s = q(rs)$$

$$\frac{q + \bar{q}}{2} = \_\_\_\_\_ \qquad \frac{q - \bar{q}}{2} = \_\_\_\_\_ \qquad q^{-1} = \_\_\_\_\_$$

For $q \in \mathrm{Im}(\mathbb{H})$, and $\|q\| = 1$,$q^{-1} = \bar{q} = -q$.

(Hint: for some of these identities you can use the expression of a quaternion as pairs of complex numbers. For others, you can prove the identity for $1, i, j, k$ individually and then apply the distributive law. For others, you can apply identities that have already been proven.)

More on Quaternions

The way we defined quaternions, i has a special role (it is the imaginary part of the first component; j and k occur in the second component). But the next series of exercises will show that in fact, there's nothing particularly special about i.

Exercise 3.2. In $\mathbb{H}$, 1 still has two square roots, but -1 has more than two. Find them all. (Hint: do this problem in terms of pairs of complex numbers)

Exercise 3.3. Given $u, v \in \mathrm{Im}(\mathbb{H})$, expand $\mathrm{Re}(uv)$ in terms of components. Do you recognize this operation? What does it mean when this is zero (i.e. $uv \in \mathrm{Im}(\mathbb{H})$)?

Exercise 3.4. Given $u, v \in \mathrm{Im}(\mathbb{H})$, expand $\mathrm{Im}(uv)$ in terms of components. Prove that $\mathrm{Im}(uv)$ is orthogonal to u and to v. If u and v are themselves orthogonal, what is the length of $\mathrm{Im}(uv)$?

Exercise 3.5. Given any $u \in \mathrm{Im}(\mathbb{H})$ of length 1, take $v \in \mathrm{Im}(\mathbb{H})$ which is orthogonal to u and also length 1, and set $w = uv$. With this setup, make a multiplication table for $1, u, v, w$. What does this look like?

(Hint: the identities you want can all be proven from knowing u^2, v^2, w^2, and uvw).

Rotations

Exercise 3.6. Suppose r is a quaternion of length 1 (not necessarily in $\mathrm{Im}(\mathbb{H})$). Show that we can write $r = \cos\theta + u\sin\theta$ for some $\theta \in \mathbb{R}$ and some $u \in \mathrm{Im}(\mathbb{H})$. Show that this u has length 1.

Exercise 3.7. Given any $x \in \mathrm{Im}(\mathbb{H})$ and $r = \cos\theta + u\sin\theta$, prove that rxr^{-1} gives the result of rotating x by angle _____ around axis _____.

(Hint: What happens when $x = u$, when $x = v$, when $x = w$?)

Exercise 3.8. Consider 1, i, j, and k as values for r. What rotation does each give you?

Exercise 3.9. Prove that a composition of two 3-d rotations is a 3-d rotation. More concretely, if you know the axes of two rotations, how can you compute the axis of their composition?

3.3 Follow-up Questions

Exercise 3.10. Time to practice! Compute the following:

$$(i-k)(j+1) \quad (3i-5j+k)(k-j) \quad (i-2j)(1+k+i+j)$$

Exercise 3.11. Rotate $q = i$ by 120° and by 240° around the axis through 0 and $i + j + k$.

Exercise 3.12. Look at each of the Exercises from Day 1. Which of these generalize to quaternions, and how?

We've seen that we can use $r = \cos\theta + u\sin\theta$ to define an arbitrary rotation on $\mathrm{Im}(\mathbb{H})$ by $x \mapsto rxr^{-1}$. But what happens if we just consider the map $x \mapsto rx$ (as we would have if we were imitating the complex numbers)?

Exercise 3.13. Prove that for quaternions $x \in \mathrm{Im}(\mathbb{H})$, rx is orthogonal to r (i.e. left-multiplication by r takes $\mathrm{Im}(\mathbb{H})$ to the "orthogonal complement" of r).

Exercise 3.14. For which quaternions r does left-multiplication by r preserve $\mathrm{Im}(\mathbb{H})$?

Exercise 3.15. Prove that if y is orthogonal to r, then $yr^{-1} \in \mathrm{Im}(\mathbb{H})$ (this implies that performing both left-multiplication by r and right-multiplication by r^{-1} will preserve $\mathrm{Im}(\mathbb{H})$).

Exercise 3.16. (Challenge) Prove that (unlike in $\mathbb{C}$!) the conjugate of $q \in \mathbb{H}$ can be expressed solely in terms of q, addition, and multiplication.

Day 4: Topology of Rotations

Why don't you take another little piece of my life
Why don't you twist it and turn it
And cut it like a knife

– Queen, "Let Me Live"

Let S^3 denote the set of quaternions (not necessarily purely imaginary) of length 1. Yesterday, we saw that if we associate $\mathbb{R}^3$ with the space $\mathrm{Im}(\mathbb{H})$ of purely imaginary quaternions, we can encode every rotation of 3-D space by some $r \in S^3$. Given:

- An axis of rotation (determined by a point on the unit sphere in $\mathbb{R}^3$, that is, by some $u \in \mathrm{Im}(\mathbb{H})$ with length 1),
- An angle θ, and
- A vector $x \in \mathrm{Im}(\mathbb{H})$ that you want to rotate,

the rotation of x by angle θ around u is given by

$$\left(\cos\frac{\theta}{2} + u\sin\frac{\theta}{2}\right) \cdot x \cdot \left(\cos\frac{\theta}{2} - u\sin\frac{\theta}{2}\right),$$

or more simply by rxr^{-1} where $r = \cos\frac{\theta}{2} + u\sin\frac{\theta}{2}$.

Exercise 4.1. Given a fixed $r \in S^3$, find all $x \in \mathrm{Im}(\mathbb{H})$ for which $rxr^{-1} = x$.

Definition 4.1. The set of rotations of $\mathbb{R}^3$ around the origin is denoted by $SO(3)$.

Exercise 4.2. Define a map $\mathrm{Rot} : S^3 \to SO(3)$: Given $r \in S^3$, we can define a rotation $\mathrm{Rot}(r)$ of $\mathbb{R}^3$ by

$$\mathrm{Rot}(r)(b, c, d) = r(bi + cj + dk)r^{-1}$$

by thinking of the result as a point in $\mathbb{R}^3$. Prove that this map is a *homomorphism*. That is, show that:

$$\begin{aligned}
&\mathrm{Rot}(1) = \mathrm{id} \\
&\mathrm{Rot}(rs) = \mathrm{Rot}(r) \circ \mathrm{Rot}(s) \\
&\mathrm{Rot}(r) \circ \mathrm{Rot}(r^{-1}) = \mathrm{Rot}(r^{-1}) \circ \mathrm{Rot}(r) = \mathrm{id}.
\end{aligned}$$

Also show this map is surjective (that is, that every rotation is $\mathrm{Rot}(r)$ for some $r \in S^3$).

Exercise 4.3. Prove that the map Rot : $S^3 \to SO(3)$ defined above is 2-to-1. Which pairs of points will map to the same rotation?

Exercise 4.4. (Omit on first reading.) Argue that Rot is continuous, by explicitly computing what $\mathrm{Rot}(r)$ does in co-ordinates and showing that each component varies continuously as r varies.

Definition 4.2. If you take S^3 and identify every pair of points obtained in Exercise 4.3, the space that you have just defined is called the **real projective space**, often called $\mathbb{R}P(3)$.

Piecing all of the above together, we get the following theorem:

Theorem 4.3. *$SO(3)$ is topologically homeomorphic to $\mathbb{R}P(3)$.*

Exercise 4.5. Does there exist a partition of S^2 into circles? That is, every element of S^2 is in some circle, and none of the circles intersect?

Exercise 4.6. Given $x \in \mathrm{Im}(\mathbb{H})$, let C_x be the set of quaternions $q \in S^3$ such that $\mathrm{Rot}(q)(i) = x$ (for example, $C_i = \{\cos\theta + i\sin\theta : \theta \in \mathbb{R}\}$). Show that each C_x is a circle.

Exercise 4.7. Show that the sets C_x form a *partition* of S^3 into circles. This partition is called the **Hopf Fibration**.

Exercise 4.8. (Group Theory) Show that $S^3 \subset \mathbb{H}$ is a group, and use the first isomorphism theorem to show $SO(3)$ is isomorphic to a quotient group of S^3.

Number Theory Preview

Next week we're going to prove Lagrange's Four-Square Theorem, but it will help to be comfortable with a few ideas that go into Fermat's Two-Square Theorem ahead of time. Take a look at these problems over the weekend if you have time — if you've seen them before (for example if you took J-Lo's Algebraic Number Theory class) then just remind yourself of the key ideas.

Definition 4.4. The set of **Gaussian integers**, $\mathbb{Z}[i]$, is the set of complex numbers of the form $a + bi$ with $a, b \in \mathbb{Z}$.

Exercise 4.9. Prove that an integer is a sum of two perfect squares if and only if it is equal to $\|z\|^2$ for some $z \in \mathbb{Z}[i]$. If we can factor $n = a_1 \cdots a_k$ where each a_i is a sum of two squares, prove that n is a sum of two squares.

Definition 4.5. A Gaussian integer z is a **unit** if there is some $w \in \mathbb{Z}[i]$ with $zw = 1$. Suppose $z \in \mathbb{Z}[i]$ is not a unit; we say z is **irreducible** if whenever you try to write it as a product $z = \alpha\beta$ for $\alpha, \beta \in \mathbb{Z}[i]$, either α or β must be a unit.

Exercise 4.10. Let p be a prime number.

1. If there exists $z \in \mathbb{Z}[i]$ such that $z\bar{z} = p$, prove that z is irreducible.
2. If there does not exist $z \in \mathbb{Z}[i]$ such that $z\bar{z} = p$, prove that p is irreducible.

(To prove some $w \in \mathbb{Z}[i]$ is irreducible, suppose it could be written as $w = \alpha\beta$ and compute the square of the length of both sides.)

Day 5: Quaternionic Integers

Who are fools of the first division
Death on two legs
You're tearing me apart

– Queen, "Death on Two Legs"

Our goal for the next two days is to prove *Lagrange's Four Square Theorem*:

Theorem 5.1. *Any positive integer n can be written as a sum of four perfect squares.*

The main idea will be to turn this question into a question about factoring. We will use the following ideas:

Definition 5.2. Let R be a ring (a set with addition, subtraction, and multiplication). An element $z \in R$ is a **unit** if there is some $w \in R$ with $zw = wz = 1$.

Definition 5.3. Given a nonzero $z \in R$ that is not a unit, we say z is **reducible** if there exists $\alpha, \beta \in R$, neither of which are units, with $z = \alpha\beta$. z is **irreducible** if it is not reducible; that is, if whenever $z = \alpha\beta$ for some $\alpha, \beta \in R$, either α or β is a unit.

Before we dive in, let's first look at what goes into the classification of integers expressible as *two* squares, and see if we can use similar ideas for the four square case.

Flashbacks to $\mathbb{C}$

$\mathbb{Z}[i]$ is the set of complex numbers $a + bi$ with $a, b \in \mathbb{Z}$. We're going to combine a fact from modular arithmetic with a fact about greatest common divisors in $\mathbb{Z}[i]$.

Fact 5.4. *If $p \equiv 1 \pmod 4$ is a prime, then there exists an integer m such that $m^2 \equiv -1 \pmod p$ (i.e. -1 is a quadratic residue mod p).*

Fact 5.5. ***Bezout's Identity*** *holds in $\mathbb{Z}[i]$. That is, given $\alpha, \beta \in \mathbb{Z}[i]$, there exists $g \in \mathbb{Z}[i]$ such that $\alpha = gw$, $\beta = gz$, and $g = \alpha u + \beta v$ for some $u, v, w, z \in \mathbb{Z}[i]$.*

Exercise 5.1. If $p \equiv 1 \pmod 4$, show that $p \mid \beta\bar{\beta}$ for some $\beta \in \mathbb{Z}[i]$.

Exercise 5.2. Use Bezout's identity for p and β to find a factorization of p in $\mathbb{Z}[i]$, and prove that neither of the factors can be units.

Exercise 5.3. Prove (using Exercises 4.9 and 4.10 from last week) that if n is a product of primes $p \equiv 1 \pmod 4$, then n is a sum of two squares.

Returning to $\mathbb{H}$

Definition 5.6. The set of **Lipschitz integers**, L, is the set of quaternions of the form $a + bi + cj + dk$ with $a, b, c, d \in \mathbb{Z}$.

Exercise 5.4. Prove that an integer is a sum of four perfect squares if and only if it is equal to $q\bar{q}$ for some $q \in L$.

Exercise 5.5. If we could prove that every prime is a sum of four squares, show that we could conclude that every positive integer is a sum of four squares.

Unfortunately, the style of proof we used for $\mathbb{Z}[i]$ will not work for L.

Exercise 5.6. Show that the Lipschitz integers do *not* satisfy Bezout's Identity.
(Hint: consider the possibilities for g if $\alpha = 1 + i$ and $\beta = 1 + j$).

Exercise 5.7. Compute $\omega = (1 + j)^{-1}(1 + i)$. If we had a ring which included ω, would $\alpha = 1 + i$ and $\beta = 1 + j$ satisfy Bezout's Identity in this ring?

Exercise 5.8. Create a new set "Hi," the **Hurwitz integers**, by including each element of L, as well as ω plus each element of L. Describe the elements of Hi, convince yourself that Hi is closed under addition and subtraction, and show that if $q \in \mathsf{Hi}$ then $\|q\|^2$ is an integer.

Exercise 5.9. If $q \in \mathsf{Hi}$ has length 1, prove that q^{-1} is also a Hurwitz integer.

Finally, this has nothing to do with quaternions, but we'll need the following fact for tomorrow:

Exercise 5.10. Prove that for any prime p, there exist integers m, n such that $m^2 + n^2 \equiv -1 \pmod{p}$. (Compare this to Fact 5.4)

Follow-up Questions

Exercise 5.11. Prove that Hi is closed under multiplication. In particular, why won't the denominator ever get larger when you multiply two elements together?

Exercise 5.12. How many units are in L? How many units are in Hi?

Exercise 5.13. (Requires Group Theory) The units of L form a group under multiplication; describe its structure.

Exercise 5.14. (Requires Group Theory; Challenge) The units of Hi form a group under multiplication; describe its structure.

Optional: Comparing to $\mathbb{C}$ again

Exercise 5.15. Prove that you can divide with remainder in $\mathbb{Z}[i]$: that is, given any $\alpha, \beta \in \mathbb{Z}[i]$ with $\beta \neq 0$, there exist $q, r \in \mathbb{Z}[i]$ with $\alpha = q\beta + r$ and $\|r\| < \|\beta\|$.

(Hint: solve an equivalent problem by dividing everything by β, and think geometrically.)

Exercise 5.16. Use division with remainder to prove Bezout's Identity (Fact 5.5).

Exercise 5.17. Continuing from Exercise 5.3, finish off the classification of whole numbers n which can be expressed as sums of two squares.

Now let $\mathbb{Z}[\sqrt{-3}]$ be the set of complex numbers that can be written as $a + b\sqrt{-3}$ for integers a and b; note that $\|a + b\sqrt{-3}\|^2 = a^2 + 3b^2$. We can define units and irreducibles in the same way as we did for $\mathbb{Z}[i]$.

Exercise 5.18. Show that Bezout's Identity does not hold for $\mathbb{Z}[\sqrt{-3}]$. What goes wrong with division with remainder?

(Hint: consider the possibilities for g if $\alpha = 2$ and $\beta = 1 + \sqrt{-3}$.)

The **Eisenstein integers**, $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$, consists of all complex numbers of the form $\frac{a+b\sqrt{-3}}{2}$ where $a, b \in \mathbb{Z}$ with $a \equiv b \pmod 2$.

Exercise 5.19. Prove that the Eisenstein integers have division with remainder, and therefore that Bezout's Identity holds. How is the problem from Exercise 5.18 fixed?

Day 6: Lagrange's Four-Square Theorem

What do you do
To get to feel alive
You go downtown
And get some of that prime jive

– Queen, "Rock It (Prime Jive)"

Remember that we defined the following two rings:

$$L = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{Z}\},$$

$$\mathsf{Hi} = \left\{ \frac{a + bi + cj + dk}{2} \mid a, b, c, d \in \mathbb{Z}, a \equiv b \equiv c \equiv d \pmod 2 \right\}.$$

We also had the following definitions:

Definition 6.1. Let R be a ring (a set with addition, subtraction, and multiplication). An element $z \in R$ is a **unit** if there is some $w \in R$ with $zw = wz = 1$.

Definition 6.2. Given a nonzero $z \in R$ that is not a unit, we say z is **reducible** if there exists $\alpha, \beta \in \mathbb{Z}[i]$, neither of which are units, with $z = \alpha\beta$. z is **irreducible** if it is not reducible; that is, if whenever $z = \alpha\beta$ for some $\alpha, \beta \in \mathbb{Z}[i]$, either α or β is a unit.

From Geometry to GCDs

Definition 6.3. The **distance** between two quaternions q and r is $\|q - r\|$.

Exercise 6.1. Find a quaternion $\gamma \in \mathbb{H}$ such that $\|\gamma - q\| \geq 1$ for every Lipschitz integer q. What happens if you use Hi instead of L?

Exercise 6.2. Prove that we can do division with remainder on Hurwitz integers. That is, given any two $u, v \in \mathsf{Hi}$ with $v \neq 0$, there exist $q, r \in \mathsf{Hi}$ such that $u = qv + r$ and $\|r\| < \|v\|$.

(Hint: solve an equivalent problem by multiplying everything on the right by v^{-1}.)

Exercise 6.3. Given $\alpha, \beta \in \mathsf{Hi}$, show that there exists an element $g \in \mathsf{Hi}$, which we will call a **greatest common left divisor** of α and β (Compare this to Fact 5.5), that satisfies the following properties:

- $\alpha = gw$ for some $w \in \mathsf{Hi}$ (notice that g is on the left),
- $\beta = gz$ for some $z \in \mathsf{Hi}$,
- $g = \alpha u + \beta v$ for some $u, v \in \mathsf{Hi}$.

(Hint: consider the set of *all* elements of the form $\alpha u + \beta v$ with $u, v \in \mathsf{Hi}$. Is there a way to identify g in this set?)

Onward to the Finish Line

By Exercise 5.5, we only need to show that every prime number is a sum of four squares.

Exercise 6.4. Prove that every even prime can be written as a sum of four perfect squares.

From now on we will only consider odd primes p. By Exercise 5.10, we can find $m, n \in \mathbb{Z}$ such that $1 + m^2 + n^2$ is divisible by p.

Exercise 6.5. Let g be a greatest common left divisor of p and $1 + mi + nj$, so we can write $p = gw$ for $w \in \mathsf{Hi}$. If p were irreducible in Hi, conclude that p would divide $1 + mi + nj$ or $1 - mi - nj$, and derive a contradiction. (Compare this to Exercise 5.2)

Exercise 6.6. Prove that $\|g\|^2 = p$. But be careful: does this necessarily imply that p is a sum of four squares?

Exercise 6.7. If $g \in \mathsf{Hi}$ is not a Lipschitz integer, show that there exists some choice of $\omega = \frac{1}{2}(\pm 1 \pm i \pm j \pm k) \in \mathsf{Hi}$ such that the coefficients of $1, i, j$, and k in $g + \omega$ are all even integers. What is $\|\bar{\omega}(g + \omega) - 1\|^2$?

Exercise 6.8. Prove that every prime number (and hence every positive integer) is a sum of four squares.

Preparing for the Next Step

Tomorrow, we're going to try to define multiplication on pairs of quaternions. By analogy with how we originally defined quaternions, we might try to define it this way:

$$(q_1, r_1)(q_2, r_2) = (q_1 q_2 - r_1 \bar{r}_2, q_1 r_2 + r_1 \bar{q}_2).$$

Exercise 6.9. Compute $(i, j)(j, i)$ and conclude that this is bad (nonzero elements aren't invertible, length is not multiplicative, two nonzero elements multiply to give zero, etc etc)

Exercise 6.10. Remembering that $ij = -ji$, can you fix this problem by swapping some of the orders of multiplication?

Follow-up Questions

Exercise 6.11. Prove that any quaternion q is the root of a quadratic polynomial with real coefficients. If $q \in \mathsf{Hi}$, prove that it is the root of a *monic* quadratic polynomial with *integer* coefficients.

Exercise 6.12. Is there a Hurwitz integer q satisfying $q^2 + 14 = 0$? What about $q^2 + 7 = 0$?

Exercise 6.13. Which Hurwitz integers q of length 1 satisfy $q^4 = 1$? Which satisfy $q^3 = 1$? Which satisfy $q^6 = 1$?

We've encountered Fermat's Two-Square Theorem, and Lagrange's Four-Square Theorem. What we're missing is *Legendre's Three-Square Theorem*:

Theorem 6.4. *A positive integer n can be written as a sum of three perfect squares if and only if it is not of the form $n = 4^a(8b + 7)$ for integers a, b.*

Exercise 6.14. Prove one direction of the theorem: if $n = 4^a(8b + 7)$, then n is not a sum of three squares. (Hint: first prove that if $4m$ is a sum of three squares, then m is a sum of three squares.)

Exercise 6.15. Given a positive integer n, suppose there existed an element $q \in L$ satisfying $q^2 + n = 0$. Prove that in this case, n is a sum of three squares.

We don't have time to develop a proof in full, but this at least indicates a direction to explore: if we want to see which n are sums of three squares, we may want to study what possible polynomials can occur that will have elements of L as roots.

Day 7: Octonions

Is this the real life?
Is this just fantasy?
Caught in a landslide,
No escape from reality

– Queen, "Bohemian Rhapsody"

Octonions

Recall that we constructed the quaternions as pairs of complex numbers, with the **Cayley-Dickson multiplication law**[1]:

$$(z_1, w_1)(z_2, w_2) = (z_1 z_2 - \bar{w}_2 w_1, w_2 z_1 + w_1 \bar{z}_2).$$

The **octonions**, denoted $\mathbb{O}$, are constructed from the quaternions in the same way that the quaternions are constructed from the complex numbers.

Exercise 7.1. Let's get some practice! Compute:

$$((0, i)(j, 0))(i, 0)$$
$$(0, i)((j, 0)(i, 0))$$

Exercise 7.2. Given an octonion x, define $\bar{x}$, $\mathrm{Re}(x)$, $\mathrm{Im}(x)$, and $\|x\|$.

Exercise 7.3. Go back to your notes on quaternions, and prove that if $x \neq 0$, then x has an inverse.

Exercise 7.4. Prove that if $x, y \in \mathbb{O}$, then $\overline{xy} = \bar{y}\bar{x}$.

[1]There is some choice in the exact form this takes; for example, we could swap the orders of all the products in the formula, and get a multiplication law with the same properties. There are a few restrictions though; see Exercise 6.9. We'll choose this format once and for all just to be on the same page.

Exercise 7.5. We want to show that length is multiplicative. What is wrong with the following proof?

False Proof: We have $\|xy\|^2 = (xy)(\bar{y}\bar{x}) = x\|y\|^2\bar{x}$. Since real numbers commute with everything, this equals $\|y\|^2 x\bar{x} = \|y\|^2\|x\|^2$, as desired.

It turns out that length *is* multiplicative for octonions, but this takes a bit of work to verify. You can do it later as a follow-up question (Exercise 7.13). For now, we'll assume it and use it.

Exercise 7.6. Prove that two nonzero elements of $\mathbb{O}$ never multiply to 0.

Exercise 7.7. If m and n are sums of eight squares, explain how you could write mn as a sum of eight squares.

Exercise 7.8. If $x, y \in \mathrm{Im}(\mathbb{O})$, compute $\mathrm{Re}(xy)$. What is this geometrically?

Exercise 7.9. Prove that for x, y in any of $\mathbb{C}, \mathbb{H}, \mathbb{O}$, we have that

$$\mathrm{Re}(xy) = \mathrm{Re}(yx) = \mathrm{Re}(\bar{x}\bar{y}).$$

Exercise 7.10. Prove that for x in any of $\mathbb{C}, \mathbb{H}, \mathbb{O}$, $\|x\|^2 = \|\mathrm{Re}(x)\|^2 + \|\mathrm{Im}(x)\|^2$

Definition 7.1. A **cross product** on $\mathbb{R}^n$ is a bilinear map $\times : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}^n$ such that:

$$v \cdot (v \times w) = 0 = w \cdot (v \times w)$$
$$\|v\|^2\|w\|^2 = (v \cdot w)^2 + \|v \times w\|^2$$

Exercise 7.11. Prove directly from the properties that $\|v \times w\|$ is the area of the parallelogram spanned by v and w.
Hint: draw a picture

Exercise 7.12. Using $\mathbb{H}$ and $\mathbb{O}$, define a cross product on $\mathbb{R}^3$ and on $\mathbb{R}^7$.
Bonus: prove that this is indeed a cross product (come to TAU for hints).

7.4 Follow-up Questions

Exercise 7.13. Using the identity $\|x\|^2 = x\bar{x}$ and Cayley-Dickson multiplication, prove that $\|xy\|^2 = \|x\|^2\|y\|^2$ for any $x, y \in \mathbb{O}$. Be very careful about your algebra!

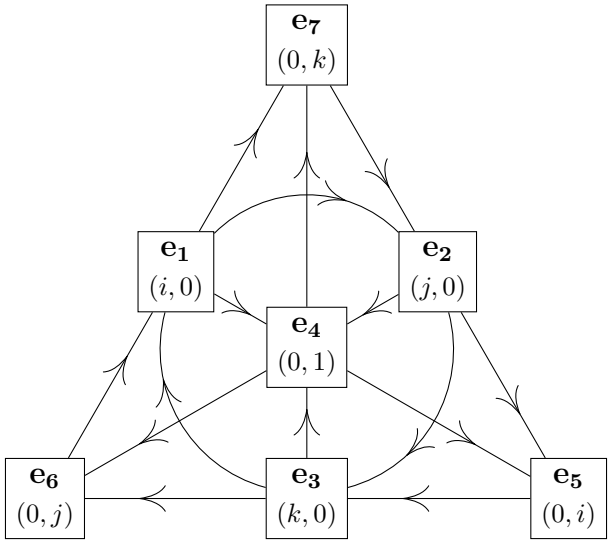
Exercise 7.14. Prove that if x is purely imaginary, then x^2 is real.

Exercise 7.15. For any v in $\mathbb{R}^3$ or $\mathbb{R}^7$, prove that $v \times v = 0$, and use this to show for any v, w in $\mathbb{R}^3$ or $\mathbb{R}^7$ that $v \times w = -w \times v$.

Exercise 7.16. We define:

$$\begin{array}{llll} e_0 = (1,0) & e_2 = (j,0) & e_4 = (0,1) & e_6 = (0,j) \\ e_1 = (i,0) & e_3 = (k,0) & e_5 = (0,i) & e_7 = (0,k) \end{array}$$

Compute some products until the following picture makes sense



Exercise 7.17. Show that if $e_k = e_i \times e_j$, then $\mathrm{Span}(e_i, e_j, e_k)$ is a copy of $\mathbb{R}^3$ in $\mathbb{R}^7$ that is closed with respect to the cross product.

Exercise 7.18. Prove that $(u \times v) \cdot w = u \cdot (v \times w)$. (Hint: compute the volume of a 3-d parallelopiped in two ways.)

Day 8: The Hop Vibrations

Tonight, I'm gonna have myself a real good time
I feel alive and the world I'll turn it inside out, yeah

– Queen, "Don't Stop me Now"

On day 4, we examined the following:

Exercise 4.6. Given $x \in \mathrm{Im}(\mathbb{H})$, let C_x be the set of quaternions $q \in S^3$ such that $qi\bar{q} = x$ (for example, $C_i = \{\cos\theta + i\sin\theta : \theta \in \mathbb{R}\}$). Show that each C_x is a circle.

Exercise 4.7. Show that the sets C_x form a *partition* of S^3 into circles. This partition is called the **Hopf Fibration**.

We'll now pick up where we left off.

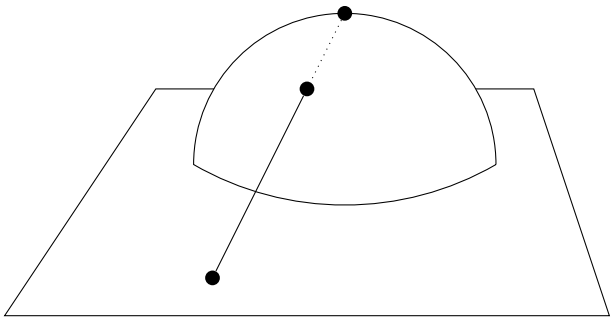
Exercise 8.1. Any point on the unit sphere in $\mathrm{Im}(\mathbb{H})$ can be rotated to any other such point. Given any $x \in \mathrm{Im}(\mathbb{H})$ of length 1, find an *explicit* $s_x \in S^3$ such that $s_x i s_x^{-1} = x$.

(Hint: use a 180° rotation.)

Exercise 8.2. Prove that $C_x = s_x C_i$. Conclude that all the circles C_x are isometric; ie, that there is a rigid motion taking any C_x to any C_y.

S^3 is hard to visualize. To understand it better, we will use **stereographic projection**.

Exercise 8.3. Consider the unit sphere in $\mathbb{R}^3$, and the $x = 0$ plane. By drawing lines through $(1, 0, 0)$, define a continuous bijection from $S^2 - \{(1, 0, 0)\}$ to $\mathbb{R}^2$. (In the picture below, the x-axis is pointing up.)



Exercise 8.4. By analogy, come up with a continuous bijection from $S^3 - \{1\}$ to $\mathbb{R}^3$.

Exercise 8.5. Prove that the circle C_i in S^3 goes to a line in $\mathbb{R}^3$, and any other C_x goes to a closed loop in $\mathbb{R}^3$.

(In fact, C_x will go to a circle in $\mathbb{R}^3$. Bonus: prove this).

Exercise 8.6. (Hard) By considering the stereographic projection, show that every C_x is linked with C_i. Use this to prove that any two circles in the Hopf fibration are linked with each other. (Two linked circles in $\mathbb{R}^3$ are called a **Hopf Link**.)

Exercise 8.7. Let $S^7 = \{(z, w) \in \mathbb{H} \times \mathbb{H} : \|z\|^2 + \|w\|^2 = 1\}$. Show that this is indeed a 7-dimensional sphere.

Exercise 8.8. We can think of S^4 as the inverse-stereographic projection of $\mathbb{H}$, where we added an extra point at ∞. We can then define $\pi : S^7 \to S^4$ by $\pi(z, w) = zw^{-1}$. Why is this map well-defined?

Exercise 8.9. Show that for any $q \in \mathbb{H}$ (considered as a subset of S^4), $\pi^{-1}(q)$ is a three-sphere lying inside S^7. What is $\pi^{-1}(\infty)$? (This partition of S^7 into disjoint copies of S^3 is called the Hopf Fibration of S^7.)

Follow-up

Exercise 8.10. (Group Theory) S^3 is a group under multiplication, and C_i is a subgroup. What is the quotient group S^3/C_i?

Exercise 8.11. Repeat Exercises 8.7 through 8.9 but replacing $\mathbb{H}$ with $\mathbb{O}$. Does everything still work? What dimensions are the spheres now?

Follow-up: Parellelizable Spheres

Over the last two weeks, we've developed the four algebras, $\mathbb{R}, \mathbb{C}, \mathbb{H}, \mathbb{O}$, and showed the geometric interpretation of their multiplication. Today we'll describe a different use of these algebras.

Definition 8.1. A **vector field** on the sphere $S^n \subset \mathbb{R}^{n+1}$ is a continuous function $f : S^n \to \mathbb{R}^{n+1}$ such that $v(x) \cdot x = 0$ (ie, $v(x)$ and x are **orthogonal**).

Exercise 8.12. Find a vector field v on S^1 such that $v(x) \neq 0$ for all x

Exercise 8.13. If $q \in \mathbb{H}$, show that $\{q, qi, qj, qk\}$ are pairwise orthogonal. Find three pairwise orthogonal vector fields on S^3.

Exercise 8.14. In 1958, using techniques from algebraic topology, characteristic classes, and differential geometry, Raoul Bott & John Milnor, and Michel Kervaire independently showed that this phenomenon of finding n perpendicular vector fields on S^n happens exclusively for $n = 1, 3, 7$. Find seven perpendicular vector fields on S^7.

Exercise 8.15. Design a t-shirt, write out the octonion multiplication table, write out the sedenion multiplication table, start riots, forge currency, and take down the government.

Preparing for Tomorrow

Definition 8.2. Given $A = \mathbb{R}^n$ for some n, we call A a **Euclidean composition algebra** if there exists a multiplication $A \times A \to A$ with the following properties:

- Multiplication on other side is distributive over addition.
- There exists a multiplicative identity $\mathbf{1}$.
- For any $c \in \mathbb{R}$ and any $x \in \mathbb{R}^n$, $(c\mathbf{1})x = x(c\mathbf{1}) = cx$ (scalar multiplication).
- Length is multiplicative: $\|xy\| = \|x\|\|y\|$ for all $x, y \in A$.

No other properties (e.g. associativity, commutativity) are assumed.

Tomorrow we will classify all Euclidean composition algebras, but we'll need a few facts. We will take these facts for granted, but if you want the satisfaction of a complete proof, you can solve the following exercises from the given axioms.

Exercise 8.16. The dot product on $\mathbb{R}^n$ satisfies the following properties:

1. $x \cdot x = \|x\|^2$.
2. $x \cdot y = \frac{1}{2}(\|x+y\|^2 - \|x\|^2 - \|y\|^2)$. (In particular, the dot product can be defined in terms of length.)
3. If $x \cdot v = y \cdot v$ for all $v \in \mathbb{R}^n$, then $x = y$.

Notice that we can use the dot product to define conjugation on any Euclidean composition algebra A: define $\bar{x} := 2(x \cdot \mathbf{1})\mathbf{1} - x$. Then we can define $\mathrm{Re}(x) := (x \cdot \mathbf{1})\mathbf{1} = \frac{1}{2}(x + \bar{x})$.

Exercise 8.17. Prove the following identities relating the dot product to multiplication:

1. $2(x \cdot y)(z \cdot w) = (xz) \cdot (yw) + (xw) \cdot (yz)$. (Hint: write $\|x+y\|^2\|v\|^2$ using dot products in two ways.)
2. $z \cdot (\bar{x}w) = (xz) \cdot w = x \cdot (w\bar{z})$. (Hint: Set $y = \mathbf{1}$ in the identity above.)
3. $\mathrm{Re}(xy) = \mathrm{Re}(yx)$.
4. $\mathrm{Re}((xy)z) = \mathrm{Re}(x(yz))$.
5. $\overline{xy} = \bar{y}\bar{x}$. (Hint: Exercise 8.16 #3.)
6. $x\bar{x} = \bar{x}x = \|x\|^2\mathbf{1}$. (Hint: set $y = x$ and $z = \mathbf{1}$ in identity #1.) As a result, every x has an inverse $\frac{\bar{x}}{\|x\|^2}$.
7. A is *alternative*; that is, $(xx)z = x(xz)$ for any $x, z \in A$. (Hint: first show $(\bar{x}x)z = \bar{x}(xz)$, then plug in the definition of $\bar{x}$.)

Day 9: 1, 2, 4, 8.

And another one gone, and another one gone
Another one bites the dust

– Queen, "Another One Bites the Dust"

Sedenions

It's only natural to try to define something that goes beyond the octonions. In the same way that we defined the octonions from the quaternions, we define the **sedenions** from the octonions.

Exercise 9.1. Construct the sedenions using the same construction as the octonions, and for a sedenion s, define $\mathrm{Re}(s), \mathrm{Im}(s), \bar{s}$

Exercise 9.2. Compute $(e_3, e_2)(e_6, -e_7)$. Conclude that length is no longer multiplicative.

Maybe we just weren't clever enough? Maybe there's a different way to define multiplication that will make the problem go away? We'll prove that in fact, the answer is no.

Hurwitz's Theorem

Our goal is to prove **Hurwitz's Theorem**.

Definition 9.1. Given $A = \mathbb{R}^n$ for some n, we call A a **Euclidean composition algebra** if there exists a multiplication $A \times A \to A$ with the following properties:

- Multiplication is distributive over addition.
- There exists a multiplicative identity $\mathbf{1}$.
- For any $c \in \mathbb{R}$ and any $x \in \mathbb{R}^n$, $(c\mathbf{1})x = x(c\mathbf{1}) = cx$ (scalar multiplication).
- Length is multiplicative: $\|xy\| = \|x\|\|y\|$ for all $x, y \in A$.

Theorem 9.2. *Every Euclidean composition algebra is isomorphic to* $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$, *or* $\mathbb{O}$.

To prove this, consider a Euclidean composition algebra B contained in A (for example, A always contains a copy of $\mathbb{R}$). If B is not equal to all of A, we will show that A must actually contain a Euclidean composition algebra of twice the dimension of B.

Exercise 9.3. Take any $j \in A$ such that $j \cdot b = 0$ for all $b \in B$. Using the definition of $\bar{j}$, prove that $j^2 = -1$. (In particular, if we take $B = \mathbb{R}$, A must contain a copy of the complex numbers.)

Exercise 9.4. With j as above, prove that $(jc) \cdot b = 0$ for all b, c in B. Conclude that $C := \{b + cj \mid b, c \in B\}$ is twice the dimension of B.

Now comes the key step. Let $a, b, c, d \in B$, and consider the elements $a + bj$ and $c + dj$ of C. If we think of these as pairs (a, b) and (c, d), we will prove that the product of these two pairs *must* obey the Cayley-Dickson multiplication law!

We need to prove a few identities. In all three cases, you can show that two desired quantities are equal by showing that their dot products with any $v \in A$ are equal. (Note: each identity is slightly trickier than the one before.)

Exercise 9.5. Given any $v \in A$, prove that $(bj) \cdot (v\bar{c}) = -(b\bar{c}) \cdot (vj)$, and use this to prove that $(bj)c = (b\bar{c})j$.

Exercise 9.6. Given any $v \in A$, prove that $(dj)\bar{v} \cdot (bj) = (b\bar{v}) \cdot d$, and use this to prove that $(bj)(dj) = -\bar{d}b$. (Hint: what is $\overline{bj}$?)

Exercise 9.7. Given any $v \in A$, prove that $a(dj) \cdot j(jv) = -a(jv) \cdot j(dj)$. Also prove that $dj = j\bar{d}$. Use these to prove that $a(dj) = (da)j$.

Exercise 9.8. Using the three identities above, prove that

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

In particular, C is closed under multiplication (and hence it is a Euclidean composition algebra).

Exercise 9.9. Prove that

- A contains a copy of the complex numbers if $n > 1$,
- A contains a copy of the quaternions if $n > 2$,
- A contains a copy of the octonions if $n > 4$,
- A contains a copy of the sedenions if $n > 8$.

Finish proving the theorem.

Follow-up

Exercise 9.10. If a cross product on $\mathbb{R}^n$ exists, show how you can use it to define a Euclidean composition algebra on $\mathbb{R}^{n+1}$ (use $\mathbb{H}$ and $\mathbb{O}$ for inspiration). Conclude that a cross product only exists for $n = 0, 1, 3, 7$.

Exercise 9.11. The sedenions aren't a Euclidean composition algebra, but why not work with them anyways? Prove that every element has a multiplicative inverse. Why doesn't this contradict the existence of nonzero elements that multiply to zero?

Exercise 9.12. (Challenge) Continue to make higher-dimensional sets with the Cayley-Dickson multiplication law until you are done.