Math Circles: A Run Through Some Fields

M. Victor Wickerhauser

Sunday, October 8th, 2017

1 Stuff to Read

A *field* (denoted $\mathbb{F}$) is a set of numbers that can be added, subtracted, multiplied and divided. It must contain 0 (the unique *additive identity*) and 1 (the unique *multiplicative identity*), with $0 \neq 1$, and must satisfy these nine *axioms*:

Add.ID: Adding 0 leaves a number unchanged so, (for all $x \in \mathbb{F}$) $x + 0 = 0 + x = x$.

Mult.ID: Multiplying by 1 leaves a number unchanged, so $(\forall x \in \mathbb{F})\ 1 * x = x * 1 = x$.

Add.Inv: Every number x has a (unique) additive inverse $-x$ such that $x + (-x) = (-x) + x = 0$.

Mult.Inv: Every number $x \neq 0$ has a (unique) multiplicative inverse x^{-1} such that $x * x^{-1} = x^{-1} * x = 1$.

Thus $1^{-1} = 1$. There is no 0^{-1}.

Two examples of fields are the *real numbers* $\mathbb{R}$, and the *rational numbers* $\mathbb{Q}$ which comprise the subset of $\mathbb{R}$ that can be written as quotients a/b, or ratios of integers a, b.

The simplest possible field is the set $\{0, 1\}$ of integers mod 2, where $-1 = 1$ and only 1 has a multiplicative inverse (which is also 1).

In a field $\mathbb{F}$, addition must be commutative and associative:

Add.Comm: $(\forall x, y \in \mathbb{F})\ x + y = y + x$.

Add.Assoc: $(\forall x, y, z \in \mathbb{F})\ x + (y + z) = (x + y) + z$.

Also, multiplication from either side must distribute over addition:

Distrib: $(\forall x, y, z \in \mathbb{F})\ x * (y + z) = x * y + x * z$ and $(\forall x, y, z \in \mathbb{F})\ (x + y) * z = x * z + y * z$.

The eighth and ninth axioms will be violated by things called quaternions and octonions that are similar to fields, but not quite:

Mult.Comm: $(\forall x, y \in \mathbb{F})\ x * y = y * x$.

Mult.Assoc: $(\forall x, y, z \in \mathbb{F})\ x * (y * z) = (x * y) * z$.

Both $\mathbb{R}$ and $\mathbb{Q}$ satisfy these additional axioms, of course.

Some other axioms are useful when the numbers are used to model physical measurements like position or size:

Order1: For any $x, y \in \mathbb{F}$, either $x < y$, or $x > y$, or $x = y$.

Order2: For any $x, y, z \in \mathbb{F}$, if $x < y$ then $x + z < y + z$.

Order3: For any $x, y \in \mathbb{F}$ and $a \in \mathbb{F}$ with $a > 0$, if $x < y$ then $a * x < a * y$.

Abs.Val1: There is a nonnegative $\mathbb{R}$-valued function $x \mapsto |x|$ satisfying $|x| = 0 \iff x = 0$.

Abs.Val2: $(\forall x, y \in \mathbb{F})\ |x + y| \leq |x| + |y|$.

Abs.Val3: $(\forall x, y \in \mathbb{F})\ |x * y| = |x||y|$.

Again, both $\mathbb{R}$ and $\mathbb{Q}$ satisfy these six additional axioms. But not all fields are ordered, nor have absolute values. Likewise, some sets that aren't fields satisfy some or all of these six axioms.

2 Stuff to Do

1. Prove that $0 * 1 = 0$ using just Add.ID, Mult.ID, and Distrib as follows:

   - Which axiom implies $1 + 0 * 1 = 1 * 1 + 0 * 1$?
   - Which axiom implies $1 * 1 + 0 * 1 = (1 + 0) * 1$?
   - Which axiom implies $(1 + 0) * 1 = 1 * 1$?
   - Which axiom implies $1 * 1 = 1$?

   Stringing these equalities together gives $1+0*1 = 1$. Conclude that $0*1$ must be the (unique) additive identity, namely $0 * 1 = 0$.

2. Start with $1 * 0 + 1$ and prove that $1 * 0 = 0$ using just Add.ID, Mult.ID, and Distrib.

3. Write -1 for the additive inverse of 1, so $1 + (-1) = (-1) + 1 = 0$. Which axiom implies $1 * (-1) = (-1) * 1 = -1$?

4. Start with $-1 + (-1) * 0$ and prove that $(-1) * 0 = 0$ using just Add.ID, Mult.ID, and Distrib.

5. Start with $x + x * 0$ and prove that $(\forall x \in \mathbb{F})\ x * 0 = 0$ using just Add.ID, Mult.ID, and Distrib.

6. Prove that $(-1) * (-1) = 1$ in any field using just Add.ID, Mult.ID, and Distrib as follows:

   - Which axiom implies $-1 + (-1) * (-1) = (-1) * 1 + (-1) * (-1)$?
   - Which axiom implies $(-1) * 1 + (-1) * (-1) = (-1) * (1 + (-1))$?
   - Which axiom implies $(-1) * (1 + (-1)) = (-1) * 0$?
   - Which previous result implies $(-1) * 0 = 0$? (Did it use just Add.ID, Mult.ID, and Distrib?)

   Stringing these equalities together gives $(-1) + (-1) * (-1) = 0$. Conclude that $(-1) * (-1)$ must be the (unique) additive inverse of (-1), namely $(-1) * (-1) = 1$.

7. Exactly one of $0 = 1$, $0 < 1$, or $0 > 1$ must be true. But $0 = 1$ is prohibited, and we may exclude $0 > 1$ as follows:

   - If $0 > 1$, which axiom implies $(-1) > 0$?
   - If $(-1) > 0$, which axiom implies $(-1) * (-1) > (-1) * 0$?
   - Evaluating both sides implies $1 > 0$ which contradicts $0 > 1$.

   Thus $0 < 1$ is the only possible case.

8. Prove that $|1| = 1$ using Abs.Val3.

9. A finite field can be specified by its addition table and its multiplication table. For the field $\{0, 1\}$, these are

$+$	0	1
0	0	1
1	1	0

$*$	0	1
0	0	0
1	0	1

Can you complete these addition and multiplication tables for the set $\{0, 1, 2\}$ to make it a field? (Hint: consider the integers mod 3.)

$+$	0	1	2
0	0	1	2
1	1		
2	2		

$*$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	

Use your tables to find -2 and 2^{-1} in this field.

10. Can you make the set $\{0, 1, 2, 3\}$ into a field by completing these tables? (Hint: it is possible, but addition and multiplication like the integers mod 4 will not work.)

$+$	0	1	2	3
0	0	1	2	3
1	1			
2	2			
3	3			

$*$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2		
3	0	3		

11. Can you find multiplication and addition tables that make the 5-element set $\{0, 1, 2, 3, 4\}$ into a field? (Hint: consider the integers mod 5.)

12. Can you find multiplication and addition tables that make the 6-element set $\{0, 1, 2, 3, 4, 5\}$ into a field? (Hint: it is not possible. A field exists with n elements if and only if n is a power of a prime number. Integers mod n give examples when n is prime. When $n = p^k$ for prime p and integer $k > 1$, the examples are called *Galois fields* after Evariste Galois and are constructed from polynomials over the field with p elements.)

3 Stuff to Read About Complex Numbers

Fields are places to find solutions to polynomial equations. For example, in $ax+b=0$ where x is the unknown variable and integers a, b are given with $a \neq 0$, there is a unique solution $x = -b/a \in \mathbb{Q}$. This works if $a, b \in \mathbb{Q}$ as well, since the ratio of two fractions is again a fraction.

But the polynomial equation $x^2 - 2 = 0$ does not have a solution in $\mathbb{Q}$, since its two solutions $\sqrt{2}$ and $-\sqrt{2}$ cannot be written as ratios of integers (this was proved centuries ago by Pythagoras, who kept it secret). But this equation can be solved by successive approximation, and so it has a solution in $\mathbb{R}$.

The similar-looking polynomial equation $x^2 + 1 = 0$ cannot have a solution in the ordered field $\mathbb{R}$ because the square of any real number must be nonnegative. The workaround is to enlarge $\mathbb{R}$ with an "imaginary" number $\sqrt{-1}$, usually called i, so $i^2 = -1$. Then to get a field we need to have all multiples of i, including its additive inverse $-i$ and all combinations with elements of $\mathbb{R}$. This produces a new set called the *complex numbers*:

$$\mathbb{C} \stackrel{\text{def}}{=} \{a + ib : a, b \in \mathbb{R}\}.$$

Both i and $-i$ are solutions to $x^2 = -1$, so they should be interchangeable in many formulas. The interchange, when extended to all complex numbers, is called *complex conjugation* and is denoted by a bar over the number:

$$\overline{a + ib} \stackrel{\text{def}}{=} a - ib.$$

Addition in this set may be defined "componentwise" assuming Add.Comm, Add.Assoc and Distrib for i and $\mathbb{R}$:

$$(a + ib) + (c + id) = (a + c) + i(b + d).$$

The unique additive inverse of $a + ib$ is $(-a) + i(-b) = -a - ib$. The unique additive identity is still $0 = 0 + 0i$.

Multiplication in this set may be defined via binomial expansion, assuming Add.Comm, Add.Assoc, Mult.Comm, Mult.Assoc, and Distrib for i and $\mathbb{R}$:

$$(a + ib) * (c + id) = ac + (ib)(id) + (ib)c + a(id) = (ac - bd) + i(ad + bc).$$

The unique multiplicative identity is still $1 = 1 + 0i$. The unique multiplicative inverse of $a + ib$ is

$$(a + ib)^{-1} = \frac{a}{\sqrt{a^2 + b^2}} + i\frac{(-b)}{\sqrt{a^2 + b^2}} = \frac{\overline{a + ib}}{\sqrt{a^2 + b^2}},$$

using the complex conjugation operator. Note that this exists whenever $a + ib \neq 0 + i0$. But also,

$$(a + ib) * (\overline{a + ib}) = (a + ib) * (a - ib) = a^2 + b^2 \stackrel{\text{def}}{=} |a + ib|^2,$$

which defines an absolute value function $|a + ib| \stackrel{\text{def}}{=} \sqrt{(a + ib) * (\overline{a + ib})} = \sqrt{a^2 + b^2}$, so the multiplicative inverse can be written more simply as

$$(a + ib)^{-1} = \frac{\overline{a + ib}}{|a + ib|^2},$$

from which it is obvious that $(a + ib)^{-1} * (a + ib) = (a + ib) * (a + ib)^{-1} = |a + ib|^2/|a + ib|^2 = 1$.

4 Stuff to Do With Complex Numbers

1. Prove that $\mathbb{C}$ is not an ordered field by excluding all three possibilities $i = 0$, $i < 0$, and $i > 0$:
   - What prohibits $i = 0$?
   - If $i > 0$, which axiom implies that $(-1) > 0$? Which previous result does this contradict?
   - If $i < 0$, which axiom implies $0 < (-i)$? Which axiom then implies $0 < (-1)$, and how does this lead to a contradiction?
2. Prove that multiplication in $\mathbb{C}$ is commutative:
   - Compute $(a + ib) * (c + id)$.
   - Compute $(c + id) * (a + ib)$.
   - Which axioms for $\mathbb{R}$ are needed to show that the two results above are equal?
3. Find the multiplicative inverse of i in $\mathbb{C}$. Then find $(2i)^{-1}$.
4. Let $z \in \mathbb{C}$ and write $z = a + ib$ for $a, b \in \mathbb{R}$. Show that the *real part* of z is $a = \frac{1}{2}(z + \bar{z})$ and the *imaginary part* of z is $b = \frac{1}{2i}(z - \bar{z})$. (Here $\frac{1}{2i}$ means $(2i)^{-1}$.)
5. Prove that complex conjugation is an *involution*: $(\forall z \in \mathbb{C})\ \overline{\bar{z}} = z$.
6. Prove that $(\forall z \in \mathbb{C})\ |\bar{z}| = |z|$.
7. Prove that Abs.Val1, Abs.Val2, and Abs.Val3 are true in $\mathbb{C}$.

8. For an angle θ, let $z_\theta \stackrel{\text{def}}{=} \cos\theta + i\sin\theta$ be a complex number.
   - Prove that $z_\theta^{-1} = \cos\theta - i\sin\theta = \bar{z}_\theta$.
   - Since $z_\theta^{-1} = \bar{z}_\theta$, prove that $|z_\theta| = 1$.
   - Prove that $z_\theta^{-1} = z_{-\theta}$.
   - Suppose ϕ and θ are two angles. Prove that $z_\phi * z_\theta = z_{\phi+\theta}$.

9. Extend this multiplication table for 1 and i in $\mathbb{C}$ by including -1 and $-i$ to get a set that is closed under multiplication.

$*$	1	i
1	1	i
i	i	-1

5 Stuff to Read About Quaternions and Octonions

Complex numbers are like points in the plane: the point at coordinates (x, y) corresponds to $x+iy \in \mathbb{C}$. Then we may convert geometry to algebra by such formulas as distance$(P_1, P_2) = |P_1 + P_2|$, where $P_1 = (x_1, y_1) = x_1 + iy_1$ and $P_2 = (x_2, y_2) = x_2 + iy_2$. We already know how to add points together (the parallelogram rule) but since $\mathbb{C}$ is a field we can now multiply points together, which is a way to compute angles and perform rotations and other transformations. For example, given an angle θ, multiplication by the complex number $\cos\theta + i\sin\theta$ rotates a point around the origin by an angle θ.

It occurred to William Rowan Hamilton in 1843 that there might be a field of numbers bigger than $\mathbb{C}$ that are like points in space-time: given 3 spacial coordinates (x, y, z) and a time coordinate t, with $x, y, z, t \in \mathbb{R}$, identify

$$(t, x, y, z) \;\leftrightarrow\; t + ix + jy + kz$$

Hamilton called the set of such numbers *quaternions*. They are denoted by $\mathbb{H}$ in his honor. Their addition is defined componentwise:

$$(t_1 + ix_1 + jy_1 + kz_1) + (t_2 + ix_2 + jy_2 + kz_2) = [t_1 + t_2] + [x_1 + x_2]i + [y_1 + y_2]j + [z_1 + z_2]k,$$

using Add.Assoc, Add.Comm, Distrib, Mult.Assoc, and Mult.Comm in $\mathbb{R}$. He found a multiplication table for i, j, k which gives every nonzero quaternion a multiplicative inverse:

$*$	1	i	j	k
1	1	i	j	k
i	i	-1	k	$-j$
j	j	$-k$	-1	i
k	k	j	$-i$	-1

That is because it permits writing the absolute value of a quaternion in terms of conjugates. Define

$$h \stackrel{\text{def}}{=} t + ix + jy + kz; \qquad \bar{h} = \overline{t + ix + jy + kz} \stackrel{\text{def}}{=} t - ix - jy - kz;$$

then $h * \bar{h} = \bar{h} * h = t^2 + x^2 + y^2 + z^2$ and we may put

$$|h| \stackrel{\text{def}}{=} \sqrt{h * \bar{h}} = \sqrt{t^2 + x^2 + y^2 + z^2}.$$

This is the distance formula in 4 dimensions and we know it satisfies Abs.Val1 and Abs.Val2. As for $\mathbb{C}$, we get multiplicative inverses from

$$h^{-1} = \frac{\bar{h}}{|h|}.$$

This table also makes $\mathbb{H}$ satisfy Mult.Assoc.

Unfortunately, that multiplication table is not symmetric: $i * j = k$ but $j * i = -k$, and $-k \neq k$ for otherwise $k = 0$. Thus quaternion multiplication does not satisfy Mult.Comm. ($\mathbb{H}$, like $\mathbb{C}$, does not satisfy the Order axioms.) $\mathbb{H}$ was the first example of an almost-field but with noncommutative multiplication. It is actually called a *skew field*. One consequence is that the properly-defined conjugate, though it splits across sums as usual, must reverse order across products:

$$(\forall h, g \in \mathbb{H})\ \overline{h + g} = \bar{h} + \bar{g}; \qquad (\forall h, g \in \mathbb{H})\ \overline{h * g} = \bar{g} * \bar{h}.$$

The same year, 1843, John T. Graves and Arthur Cayley discovered an 8-dimensional system they named *octonions*, denoted $\mathbb{O}$. It has 7 different imaginary components $\{e_1, \ldots, e_7\}$ plus a real component e_0 (which is just 1). The following multiplication table permits defining conjugates and absolute values, so every nonzero element has a multiplicative inverse:

$*$	e_0	e_1	e_2	e_3	e_4	e_5	e_6	e_7
e_0	e_0	e_1	e_2	e_3	e_4	e_5	e_6	e_7
e_1	e_1	$-e_0$	e_3	$-e_2$	e_5	$-e_4$	e_7	$-e_6$
e_2	e_2	$-e_3$	$-e_0$	e_1	e_6	e_7	$-e_4$	$-e_5$
e_3	e_3	e_2	$-e_1$	$-e_0$	e_7	$-e_6$	e_5	$-e_4$
e_4	e_4	$-e_5$	$-e_6$	$-e_7$	$-e_0$	e_1	e_2	e_3
e_5	e_5	e_4	$-e_7$	e_6	$-e_1$	$-e_0$	$-e_3$	e_2
e_6	e_6	e_7	e_4	$-e_5$	$-e_2$	e_3	$-e_0$	$-e_1$
e_7	e_7	$-e_6$	e_5	e_4	$-e_3$	$-e_2$	e_1	$-e_0$

For $o = x_0e_0 + x_1e_1 + \cdots + x_7e_7$, conjugation $o \mapsto \bar{o} = x_0e_0 - x_1e_1 - \cdots - x_7e_7$ sends every component except e_0 to its negative. Absolute value is defined by

$$|o| = \sqrt{o * \bar{o}} = \sqrt{x_0^2 + x_1^2 + \cdots + x_7^2},$$

where the choice of table insures that the second equation holds. Then

$$o^{-1} = \frac{\bar{o}}{|o|^2}$$

exists for every nonzero $o \in \mathbb{O}$.

This multiplication table is not the only one that works: there are 480 equivalent versions. All of them, however, violate Mult.Assoc (as well as Mult.Comm), so $\mathbb{O}$ is missing yet another field axiom satisfied by $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, and $\mathbb{H}$.

6 Stuff to Do With Quaternions and Octonions

1. Let i, j, k be the imaginary components in $\mathbb{H}$. Prove that $i * j * k = -1$.

2. Quaternions can be written as pairs of complex numbers:

   $$(t, x, y, z) \;\leftrightarrow\; t + ix + jy + kz \;\leftrightarrow\; (t + ix) + (y + iz)j,$$

   using the multiplication fact $i * j = k$. Compute the conjugate $\overline{t + ix + jy + kz}$ with this formula to see that we must have

   $$\overline{i * j} = \bar{k} = -k = j * i = (-j) * (-i) = \bar{j} * \bar{i}.$$

3. Conjugation for octonions also reverses over multiplication:

   $$(\forall p, q \in \mathbb{O})\ \overline{p * q} = \bar{q} * \bar{p}.$$

   Given $p, q, r \in \mathbb{O}$, compute $\overline{(p * q) * r}$ and $\overline{p * (q * r)}$ in terms of $\bar{p}, \bar{q}, \bar{r}$.

4. Find some triplet e_i, e_j, and e_j in the octonion multiplication table for which

$$(e_i * e_j) * e_k \neq e_i * (e_j * e_k).$$

This proves that octonion multiplication is not associative (Mult.Assoc doesn't hold in $\mathbb{O}$).

5. Octonions can be written as pairs of quaternions:

$$(x_0, x_1, \ldots, x_7) \;\leftrightarrow\; (x_0 + ix_1 + jx_2 + kx_3) + (x_4 + ix_5 + jx_6 + kx_7)\ell,$$

putting $e_1 = i$, $e_2 = j$, $e_3 = k$, and $e_4 = \ell$. The remaining imaginary components e_5, e_6, e_7 come from the e_4 column of the octonion multiplication table.

Suppose $a, b, c, d \in \mathbb{H}$ are quaternions and we form octonions $a + b\ell$ and $c + d\ell$. Show that octonion multiplication may be expressed as

$$(a + b\ell) * (c + d\ell) = (ac - \bar{d}b) + (da + b\bar{c})\ell,$$

where the multiplications and conjugations on the right-hand side are those for quaternions.

6. Prove that Abs.Val3 holds in $\mathbb{O}$, namely $(\forall h, g \in \mathbb{O})\ |h * g| = |h||g|$.