1 Fields

From calculus we should be used to working with the real numbers, which we denote $\mathbb{R}$. We're used enough to them that we don't really think about them a lot, honestly. But the real numbers aren't the only kind of numbers out there, and we want flexibility to consider other kinds as well. So we want to describe the important properties of the real numbers that we use frequently, and then see what else has those properties.

1.1 Introduction to Fields

Definition 1.1. Suppose $\mathbb{F}$ is a set with two binary operations, $+$ and $\times$. We say $\mathbb{F}$ is a *field* if it satisfies the following axioms:

1. (Closure) If $x, y \in \mathbb{F}$ then $x + y, xy \in \mathbb{F}$.
2. (Commutativity) $x + y = y + x$ and $xy = yx$ for all $x, y \in \mathbb{F}$.
3. (Associativity) $(x + y) + z = x + (y + z)$ and $(xy)z = x(yz)$ for all $x, y, z \in \mathbb{F}$.
4. (Identities) There is an element $0 \in \mathbb{F}$ such that $x + 0 = x$ for all $x \in \mathbb{F}$. There is an element $1 \in \mathbb{F}$ such that $1x = x$ for all $x \in \mathbb{F}$.
5. (Inverses) For every $x \in \mathbb{F}$ there is a $-x \in \mathbb{F}$ such that $x + (-x) = 0$. For every non-zero $x \in \mathbb{F}$ there is an element $x^{-1} \in \mathbb{F}$ such that $xx^{-1} = 1$.
6. (Distributivity) $x(y + z) = xy + xz$ for all $x, y, z \in \mathbb{F}$.

Remark 1.2. The real numbers, of course, have more properties than this—barely. The real numbers are the unique *complete ordered* field. "Ordered" means that if we have two distinct real numbers, we can say which one is bigger. "Complete" means that it's good for doing calculus. Neither of those properties will be important in this course very often, so we will be able to do almost everything over "fields" in general.

Example 1.3. The set $\mathbb{Q}$ of rational numbers is a field. The sets $\mathbb{R}$ and $\mathbb{C}$ of real and complex numbers are fields.

The set $\mathbb{Z}$ of integers is not a field, because it does not have multiplicative inverses. (We call this set a *ring*).

The set $\mathbb{N}$ of natural numbers is not a field. It does not have multiplicative or additive inverses.

The set $\mathbb{Z}/n\mathbb{Z}$ of integers modulo n is is a field if n is prime, and is not a field if n is composite. We sometimes call these the *finite fields* $\mathbb{Z}/p\mathbb{Z}$ or $\mathbb{F}_p$. These may come up from time to time in this course.

Example 1.4. Consider specifically the set $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z} = \{0, 1\}$, the integers mod 2. We have the operations

$$0+0=0 \qquad 0+1=1+0=1 \qquad 1+1=0$$
$$0\times 0=0 \qquad 0\times 1=1\times 0=0 \qquad 1\times 1=1.$$

We can check the field axioms and see this is a field.

Proposition 1.5. *Let $\mathbb{F}$ be a field. For all $a, b, c \in \mathbb{F}$, we have*

1. *(Cancellation of addition) If $a + b = a + c$, then $b = c$.*
2. *(Cancellation of multiplication) If $a \cdot b = a \cdot c$ and $a \neq 0$, then $b = c$.*
3. *$a \cdot 0 = 0$.*
4. *$(-a) \cdot b = a \cdot (-b) = -(a \cdot b)$.*
5. *$(-a) \cdot (-b) = a \cdot b$.*

But the two main examples we will see in this course are the *real numbers* and the *complex numbers*. We'll assume you're familiar with the real numbers from calculus, so we won't talk to much more about their specific properties. But we do need to do a quick overview of the complex numbers.

1.2 The complex numbers

Definition 1.6. A *complex number* is a number $z = a + bi$ where $a, b \in \mathbb{R}$. We say that $a = \mathcal{R}(z)$ is the *real part* and $b = \mathcal{I}(z)$ is the *imaginary part*. The set of all complex numbers is $\mathbb{C} = \{a + bi : a, bin\mathbb{R}\}$.

We can add complex numbers in the obvious way. We can also multiply them, once we take the rule that $i^2 = -1$.

$$\begin{aligned}(a+bi)+(c+di) &= (a+c)+(b+d)i \\ (a+bi)(c+di) &= ac+adi+bci+bdi^2 \\ &= ac+adi+bci+bd(-1) \\ &= (ac-bd)+(ad+bc)i\end{aligned}$$

Example 1.7. Let $z = 3-i$ and $w = \pi+4i$. Then $z+w = 3+pi+3i$, and

$$zw = (3-i)(\pi+4i) = 3\pi+4+(12-\pi)i.$$

We want to check that $\mathbb{C}$ is also a field, which means we need to check the six properties in definition 1.1. We just showed that addition and multiplication are closed; most of the properties are very easy to check, given that we know that the *real numbers* have those properties.

Proposition 1.8 (Commutativity of complex numbers)**.** *If $z, w \in \mathbb{C}$, then $z+w = w+z$ and $zw = wz$.*

Proof. Let $z = a+bi$ and $w = c+di$. Then

$$\begin{aligned}z+w &= (a+bi)+(c+di) = (a+c)+(b+d)i \\ w+z &= (c+di)+(a+bi) = (c+a)+(d+b)i \\ &= (a+c)+(b+d)i && \text{by additive commutatitivity}\end{aligned}$$

Similarly,

$$\begin{aligned}zw &= (a+bi)(c+di) = (ac-bd)+(ad+bc)i \\ wz &= (c+di)(a+bi) = (ca-db)+(cb+da)i \\ &= (ac-bd)+(bc+ad)i && \text{by multiplicative commutativity} \\ &= (ac-bd)+(ad+bc)i && \text{by additive commutativity.}\end{aligned}$$

□

The important thing to notice about this proof, as a matter of proof technique, is that we don't need to do anything weird and fancy, or special to the complex numbers, to check these properties. We're just using the fact that the complex numbers are made up of real numbers, and we know the real numbers are a field. We'll use this approach constantly throughout the semester.

But there's one property that isn't trivial: multiplicative inverses. How do we *divide* by a complex number? We can start by defining a useful operation:

Definition 1.9. Let $z = a + bi$. Then the *complex conjugate* of z is the complex number $\overline{z} = a - bi$.

This complex conjugate has a number of useful properties, but the one we're interested in here is that

$$z\overline{z} = (a+bi)(a-bi) = a^2 + b^2 + (ab - ab)i = a^2 + b^2,$$

which is a real number. And we know how to divide by real numbers!

So if $z = a + bi \in \mathbb{C}$ is not zero, then we can define a new number

$$w = \frac{\overline{z}}{z\overline{z}} = \frac{a-bi}{a^2+b^2} = \frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}i.$$

This is a complex number since $\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2} \in \mathbb{R}$, and we can check that

$$\begin{aligned} zw &= (a+bi)\left(\frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}i\right) \\ &= \left(\frac{a^2}{a^2+b^2} + \frac{b^2}{a^2+b^2}\right) + \left(\frac{ab}{a^2+b^2} - \frac{ab}{a^2+b^2}\right)i \\ &= \frac{a^2+b^2}{a^2+b^2} + 0i = 1 + 0i. \end{aligned}$$

Example 1.10. We'll still take $z = 3 - i$ and $w = \pi + 4i$. Then $\overline{z} = 3 + i$, and

$$z^{-1} = \frac{\overline{z}}{z\overline{z}} = \frac{3+i}{3^2+1^1} = \frac{3}{10} + \frac{i}{10}.$$

So we can compute

$$\begin{aligned} \frac{w}{z} &= (\pi + 4i)\left(\frac{3}{10} + \frac{i}{10}\right) \\ &= \frac{3\pi}{10} - \frac{4}{10} + \left(\frac{12}{10} + \frac{\pi}{10}\right)i \\ &= \frac{3\pi - 4}{10} + \frac{12-\pi}{10}i. \end{aligned}$$

Proposition 1.11 (Properties of the complex conjugate)**.** *Let $z, w \in \mathbb{C}$. Then:*

(a) $\overline{\overline{z}} = z$.

(b) $\overline{z+w} = \overline{z} + \overline{w}$.

(c) $\overline{zw} = \overline{z} \cdot \overline{w}$.

(d) $\overline{\left(\frac{z}{w}\right)} = \frac{\overline{z}}{\overline{w}}$ *if* $w \neq 0$.

(e) z *is a real number if and only if* $\overline{z} = z$.

Proof. The proofs of (b) and (c) are in the book, so we'll prove the other parts.

(a) Let $z = a + bi$. Then $\overline{z} = a - bi$ and so $\overline{\overline{z}} = a - (-b)i = a + bi = z$.

(d) Let $z = a + bi$ and $w = c + di$ where $w \neq 0$. Then we can compute

$$\begin{aligned}\overline{\left(\frac{z}{w}\right)} &= \overline{\left(\frac{a+bi}{c+di}\right)} = \overline{\left(\frac{(a+bi)(c-di)}{c^2+d^2}\right)} \\ &= \overline{\left(\frac{ac+bd}{c^2+d^2} + \frac{-ad+bc}{c^2+d^2}i\right)} \\ &= \frac{ac+bd}{c^2+d^2} + \frac{ad-bc}{c^2+d^2}i.\end{aligned}$$

But we can also compute out the other side, and see

$$\begin{aligned}\frac{\overline{z}}{\overline{w}} &= \frac{a-bi}{c-di} = \frac{(a-bi)(c+di)}{c^2+d^2} \\ &= \frac{(ac+bd)+(ad-bc)i}{c^2+d^2}.\end{aligned}$$

and so $\overline{\left(\frac{z}{w}\right)} = \frac{\overline{z}}{\overline{w}}$.

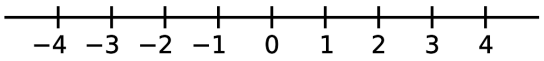
(e) If z is real, then $z = a + 0i$ for some $c \in \mathbb{R}$. Then $\overline{z} = a - 0i = a + 0i = z$.

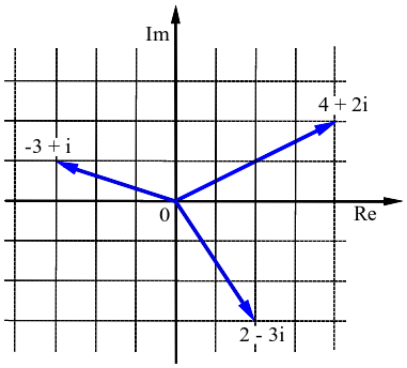
Conversely, suppose $z = a + bi$ and $z = \overline{z}$. We know that $\overline{z} = a - bi$, so we have $a + bi = a - bi$. This implies that $bi = -bi$ and thus that $b = -b$, so $b = 0$. Thus $z = a + 0i \in \mathbb{R}$.

□

One of the lenses this course will keep returning to is the idea of geometry, and a little of that can help us right now. If we have a pair of real numbers, we can graph it on a plane, using the first number for the horizontal coordinate and the second number for the vertical coordinate. But a complex number $z = a + bi$ is a pair of real numbers. And that means that, just like we can think of the real numbers as forming a line:

we can think of the complex numbers as forming a plane:





We'll return to this geometric picture soon, but for right now I want to think about distance. You can see each complex number implies a right triangle, so we can find the distance from the origin $0 + 0i$ with the Pythagorean Theorem. If $z = a + bi$ the lengths of these sides are just a and b, so we have

Definition 1.12. Let $z = a + bi$ where $a, b \in \mathbb{R}$. The *absolute value* or *modulus* of z is

$$|z| = \sqrt{a^2 + b^2}.$$

Conveniently we can compute this in terms of more fundamental operations, because we saw that $z \cdot \overline{z} = a^2 + b^2$. Thus $|z| = \sqrt{z\overline{z}}$.

We can derive the following properties for the complex absolute value:

Proposition 1.13. *Let $z, w \in \mathbb{C}$. Then*

(a) $|zw| = |z| \cdot |w|$.

(b) $\left|\frac{z}{w}\right| = \frac{|z|}{|w|}$ *if* $w \neq 0$.

(c) $|z + w| \leq |z| + |w|$ *(Triangle Inequality).*

(d) $|z| - |w| \leq |z + w|$ *(Reverse Triangle Inequality).*