**Complex numbers, modular arithmetic, binary operations, and fields**
9/30/05

These notes are a noncomprehensive summary to supplement your own notes on what we have covered in the first two and a half weeks.

## 1. Complex numbers

Appendix G in Stewart is on complex numbers. If you need more details or more exercises, look there. Or if you don't have Stewart, most calculus books will have some introductory level discussion on complex numbers.

### 1.1. Complex arithmetic.

**Definition 1.** *The set of* complex numbers $\mathbb{C}$ *is*

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

*where* $i^2 = -1$.

For $x + yi$, $x$ is called the real part and $y$ is called the imaginary part. If $y = 0$, then $x + 0i = x$ is just a real number. If $x = 0$, we say $0 + yi = yi$ is an imaginary number. To do arithmetic on the complex numbers, you to treat $i$ as if it were a variable, and you can replace $i^2$ with $-1$.

**Example 1.**

$$(4 + 2i) + (5 + 3i) = 4 + 2i + 5 + 3i = 9 + 5i$$
$$(2 - 7i) - (6 - 4i) = 2 - 7i - 6 + 4i = -4 - 3i$$
$$(4 + 2i)(5 - 3i) = 20 - 12i + 10i - 6i^2 = 20 - 12i + 10i - 6(-1) = 26 - 2i$$

Division is a little trickier. We first need to introduce complex conjugates.

**Definition 2.** *The* complex conjugate *of the complex number* $x + yi$ *is* $x - yi$ *and is denoted by* $\overline{x + yi}$.

For example, $\overline{2 - 3i} = 2 + 3i$. That is you conjugate a complex number by multiplying its imaginary coordinate by $-1$. Obviously, the conjugate of a real number is itself.

**Proposition 1.** *Let* $z, z_1, z_2 \in \mathbb{C}$.

1. $\overline{\overline{z}} = z$
2. $\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$
3. $\overline{z_1 z_2} = \overline{z_1}\,\overline{z_2}$

*Proof:* Let $z = x + yi$.

$$\overline{\overline{z}} = \overline{\overline{x + yi}} = \overline{x - yi} = x + yi = z$$

The rest is left as an (easy) exercise for the reader. □

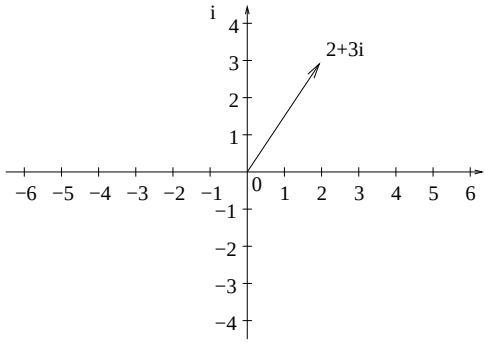
Notice that $(x + yi)(\overline{x + yi}) = (x + yi)(x - yi) = x^2 - y^2 i^2 = x^2 + y^2$, which is a real number. In fact, it is a nonnegative real number and is only 0 if $x = y = 0$.

Now we are ready to do division:

$$\frac{x + yi}{s + ti} = \frac{x + yi}{s + ti}\frac{(\overline{s + ti})}{(\overline{s + ti})} = \frac{x + yi}{s + ti}\frac{s - ti}{s - ti}$$
$$= \frac{(x + yi)(s - ti)}{s^2 + t^2} = \frac{xs + yt - xti + ysi}{s^2 + t^2} = \frac{xs + yt}{s^2 + t^2} + \frac{ys - xt}{s^2 + t^2}i$$

**Exercise:** Pick some random complex numbers and do all kinds of arithmetic (add, subtract, multiply, divide) on them until you are comfortable with complex numbers and you can do the computation efficiently.

1.2. **The complex plane.** Complex numbers can be represented as points or vectors in a 2-dimensional Cartesian plane. The horizontal axis serves as the real line, and the vertical axis has the imaginary numbers on it. E.g.



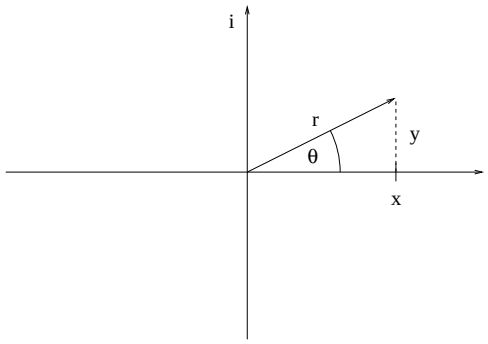

The nice thing is that adding and subtracting of complex numbers correspond to adding and subtracting them as vectors in this plane. Conjugation is reflection across the real axis. Notice that $z\overline{z} = (x+yi)(\overline{x+yi}) = (x+yi)(x-yi) = x^2+y^2$, which is the square of the length of the vector $z$. This motivates the following definition.

**Definition 3.** *The* magnitude *or* absolute value *of a complex number $z$ is defined as $|z| = \sqrt{z\overline{z}}$.*

Notice that we are taking the square root of a nonnegative real number here, so $|z|$ is also a nonnegative real number and is 0 if and only if $x = y = 0$.

Multiplication and division are a little more complicated, but we will return to them later.

1.3. **Polar coordinates.** Just like points in the plane, complex numbers can also be written in polar coordinates.




We can set $x + yi = r(\cos(\theta) + i\sin(\theta))$ where we can require without loss of generality that $r \geq 0$. In fact, you can see from the picture

$$r^2 = x^2 + y^2$$
$$\tan(\theta) = \frac{y}{x}$$

These formulas are the same ones you are familiar with from your calculus/precalculus classes and can be used the same way to convert between Cartesian and polar coordinates. You can see $r = |z|$ is just the magnitude of $z$. $\theta$ is called the argument.

Be careful when converting from Cartesian coordinates to polar coordinates. You may be tempted to say $\theta = \arctan(y/x)$, but this is not quite true. Recall that tan has period $\pi$, so arctan has range $(-\pi/2, \pi/2)$. Therefore $\arctan(y/x)$ will never give you an angle in the 2nd and 3rd quadrants. For example, $1+i$ and $-1-i$ would both give you $\theta = \arctan(1) = \pi/4$, but the argument of $-1-i$ is

$5\pi/4$. To compensate for this deficiency, you should always visualize which quadrant the complex number lies in and correct the angle arctan returns by adding $\pi$ if necessary.

**Example 2.** *Let's convert* $5(\cos(3\pi/4)+i\sin(3\pi/4))$ *to Cartesian coordinates. This is really easy:*

$$5(\cos(3\pi/4)+i\sin(3\pi/4)) = 5(-\frac{1}{\sqrt{2}}+\frac{1}{\sqrt{2}}i) = -\frac{5}{\sqrt{2}}+\frac{5}{\sqrt{2}}i$$

**Example 3.** *Let's convert* $-1+\sqrt{3}i$ *to polar coordinates.*

$$r = \sqrt{(-1)^2+\sqrt{3}^2} = 2$$

*You should be able to figure out without a calculator that* $\arctan(-\sqrt{3}/1) = -\pi/3$*, but you can easily see that* $-1+\sqrt{3}i$ *is in the 2nd quadrant. So* $\theta = 2\pi/3$ *and*

$$-1+\sqrt{3}i = 2(\cos(2\pi/3)+i\sin(2\pi/3))$$

Another way to write $r(\cos(\theta)+i\sin(\theta))$ is $re^{i\theta}$. This makes multiplication and division really easy. Conjugation is also quite simple:

$$(r_1e^{i\theta_1})(r_2e^{i\theta_2}) = r_1r_2e^{i(\theta_1+\theta_2)}$$

$$\frac{r_1e^{i\theta_1}}{r_2e^{i\theta_2}} = \frac{r_1}{r_2}\,e^{i(\theta_1-\theta_2)}$$

$$\overline{re^{i\theta}} = re^{-i\theta}$$

If these equations are not obvious to you, substitute $e^{i\theta} = \cos(\theta)+i\sin(\theta)$ and verify them.

Thinking in terms of vectors in the complex plane, this shows that the length of the product of two vectors is the product of the length of the vectors, while the angle is the sum of the angles. Similarly, the length of the quotient of two vectors is the quotient of the length of the vectors, while the angle is the difference of the angles.

The equation $e^{i\theta} = \cos(\theta)+i\sin(\theta)$ is not just clever notation. There is some serious mathematical content behind it. If you are curious, do the following exercises.

**Exercises:**

1. Find the Taylor series expansion of $f(x) = e^x$ about $x = 0$. What is the radius of convergence?
2. Find the Taylor series expansion of $f(x) = \sin(x)$ about $x = 0$. What is the radius of convergence?
3. Find the Taylor series expansion of $f(x) = \cos(x)$ about $x = 0$. What is the radius of convergence?
4. Substitute $i\theta$ for $x$ and verify that

   $$e^{i\theta} = \cos(\theta)+i\sin(\theta)$$

   Of course, $i\theta$ is not a real number, so what you are doing here is purely formal manipulation. But it can be shown this is meaningful even in the context of complex numbers. You can find out how by taking complex analysis.

1.4. **The Fundamental Theorem of Algebra.** Complex numbers have many nice properties. You can solve linear equations over complex numbers the same way you solve them over real numbers. You can even use the quadratic formula to find roots of quadratic polynomials, although you may end up with a complex number under the square root, which you would need to know how to interpret. (It is not difficult, but we have not talked about it.)

One particularly nice property of $\mathbb{C}$ is the following:

**Theorem 1.** (The Fundamental Theorem of Algebra) *Let* $p(x)$ *be a polynomial of degree at least* 1 *with complex coefficients. Then* $p(x)$ *has a root among the complex numbers.*

In other words, the polynomial equation $p(x) = 0$ always has at least one complex solution. Contrast this with the real numbers, where the equation $x^2 + 1 = 0$ has no solutions. The proof of this theorem is well beyond our reach at this point, so we will just believe it. Despite its name, it has more to do with complex analysis than algebra.

Actually, if $p(x)$ has a root $z_1$, then we can write it as $p(x) = (x - z)p_1(x)$ where $\deg(p_1) = \deg(p) - 1$. Now you can repeat this for $p_1$, find a root $z_2$, and write it as $p_1(x) = (x - z_2)p_2(x)$. And so on, until you get down to degree 1. If a number appears more than once as a root in this process, we say it is a multiple root. Its multiplicity is the number of times it appears. We have just proved the following corollary.

**Corollary 1.** *A polynomial of degree $n \geq 1$ over the complex numbers has exactly $n$ roots if the roots are counted with multiplicity, and factors into $n$ linear factors.*

Again, contrast this with working over the real numbers, where $x^2 + 1$ cannot be factored into linear factors.

Many things can be done over the complex numbers that can be done over the reals. For example, you can differentiate and integrate functions $\mathbb{C} \to \mathbb{C}$ (not all of them). In fact, doing it over the complex numbers is in many ways easier. (In other ways, it is harder.)

**Exercise:** Find $x, y \in \mathbb{C}$ to solve the following system of linear equations over the complex numbers:

$$\begin{aligned}(2 - i)x + (3 + i)y + 9 &= \frac{9i}{2} \\ 5ix + (2i - 5)y &= 12 - 12i\end{aligned}$$

## 2. Modular arithmetic

2.1. **The set $\mathbb{Z}_n$.** For a formal definition of $\mathbb{Z}_n$, you will have to wait until you take algebra, if you choose to pursue math further in that direction. It uses some concepts we don't have at this point. But we can give a good intuitive description which will suffice for our purposes. Think of $\mathbb{Z}_n$ as the set you get if you group integers together based on their remainder after integer division by $n$. E.g. if $n = 3$, you would get three groups:

$$\{\ldots, -6, -3, 0, 3, 6, \ldots\}$$
$$\{\ldots, -5, -2, 1, 4, 7, \ldots\}$$
$$\{\ldots, -4, -1, 2, 5, 8, \ldots\}$$

It should be immediately obvious from this definition that $\mathbb{Z}_n$ has $n$ distinct elements.

The numbers within a group are considered the same when you work modulo $n$. So $k$ and $m$ are the same modulo $n$, if they give the same remainder after division by $n$, or equivalently, if $k - m$ is a multiple on $n$. (Why are these two conditions equivalent?) This is denoted as $k \equiv m \mod n$. In the example above, $1 \equiv 7 \mod 3$. Each member of a remainder group can stand for the whole group. It's a bit like dividing up a state into voting districts and then letting anyone represent their entire district. There is another notation which really captures this idea: for each integer $k$, let $\overline{k}$ mean the entire group of numbers that $k$ belongs to modulo $n$. In the above example, $\overline{1} = \overline{7}$. This is usually the more convenient notation, but can only be used if it is clear from context what $n$ is.

2.2. **Addition.** We can define addition on the elements of $\mathbb{Z}_n$ as follows:

$$\overline{k} + \overline{m} = \overline{k + m}$$

Since $k$ and $m$ here could be any representatives of their remainder groups, it is not immediately clear that this definition is good. It could happen that for different representatives $k'$ and $m'$ instead of $k$ and $m$, $k + m$ and $k' + m'$ are not in the same remainder group. This would be bad because different people may choose different numbers from the remainder group of $k$ and $m$ to represent

the whole groups, and they would then end up with different results. But if you think about what is really going on here, you will see that such a thing fortunately cannot happen. $k$ and $k'$ have the same remainder after division by $n$ and so do $m$ and $m'$. Then $k+m$ and $k'+m'$ must also have the same remainder after division by $n$.

Here is a more formal argument. If $\overline{k} = \overline{k'}$ then $k - k'$ is a multiple of $n$. Let's say $k - k' = ns$ for some $s \in \mathbb{Z}$. Similarly, $\overline{m} = \overline{m'}$ implies $m - m' = nt$ for some $t \in \mathbb{Z}$. Hence

$$(k+m) - (k'+m') = k - k' + m - m' = ns + nt = n(s+t)$$

So $(k+m) - (k'+m')$ is also a multiple of $n$ and therefore $\overline{k+m} = \overline{k'+m'}$.

2.3. **Subtraction.** Similarly, we can define subtraction on $\mathbb{Z}_n$ as

$$\overline{k} + \overline{m} = \overline{k+m}$$

Again, we should check that this definition is good. The check is essentially the same as for addition, so I will leave it to the exercises. Notice that by these definitions:

$$\overline{k} + \overline{0} = \overline{k+0} = \overline{k}$$
$$\overline{k} + \overline{-k} = \overline{k+(-k)} = \overline{0}$$

The first equation says $\overline{0}$ works much like the number 0 in that adding it to something does nothing. It is an additive identity. (See the next chapter for the formal definition of identity.) The second equation says that every element of $\mathbb{Z}_n$ has an inverse with respect to addition, and this inverse is exactly what you would expect it to be. (See the next chapter for more on inverses.)

2.4. **Multiplication.** We can even define multiplication on $\mathbb{Z}_n$ by

$$\overline{k}\,\overline{m} = \overline{km}$$

Again, I will leave it as an exercise to show that this definition is good. Notice that

$$\overline{k}\,\overline{1} = \overline{k \cdot 1} = \overline{k}$$

so $\overline{1}$ works as an identity with respect to multiplication.

2.5. **Division.** Something interesting happens to division. We will not define it in term of division on $\mathbb{Z}$ because you usually cannot divide two integer numbers and get an integer. But in $\mathbb{Z}_n$ you can often, although not always, divide $\overline{k}$ by $\overline{m}$ even when $k$ is not divisible by $m$ as integers.

Consider for example $\mathbb{Z}_5$. What would $\overline{1}/\overline{2}$ be? Whatever it is, it must be such that when we multiply it by $\overline{2}$ we get $\overline{1}$. Let's call it $x$ for now. So

$$\overline{2}x = \overline{1}$$

If you try all five possibilities, you find that $x = \overline{3}$ does the job and nothing else works. So we can say $\overline{1}/\overline{2} = \overline{3}$. What about $\overline{3}/\overline{4}$? If it exists, it must be such that when we multiply it by $\overline{4}$ we get $\overline{3}$. So call it $x$ and see what element of $\mathbb{Z}_5$ solves the equation

$$\overline{4}x = \overline{3}$$

Again, it is easy to try all five possibilities. (Do so.) You will find $\overline{2}$ works and nothing else does. So we can say $\overline{3}/\overline{4} = \overline{2}$.

Let us now look in $\mathbb{Z}_6$. What is $\overline{1}/\overline{2}$? If you try to solve

$$\overline{2}x = \overline{1}$$

by trial and error, you find no solution. In fact, there is a good reason why there is no solution. Suppose there were an element of $x$ satisfying the above equation. Then we multiply both sides by $\overline{3}$ and we would get

$$\overline{3} = \overline{3}\,\overline{1} = \overline{3}(\overline{2}x) = (\overline{3}\,\overline{2})x = \overline{0}x = \overline{0}.$$

But we know $\overline{3} \neq \overline{0}$. What about $\overline{1}/\overline{5}$? If you try to solve

$$\overline{5}x = \overline{1}$$

you find that $\overline{5}$ works and nothing else does, so $\overline{1}/\overline{5} = \overline{5}$. Actually, this is not surprising if you realize that $\overline{5} = \overline{-1}$.

Here we found $\overline{k}/\overline{m}$ by trial and error, whenever we could. In fact, it is possible to give an algorithm to do it more efficiently, but this is beyond the scope of this class. If you stay tuned, you can find out about it in algebra or number theory.

**Exercises:**

1. Pick a number $n$. Now pick some random numbers and do all kinds of computations adding, subtracting, and multiplying them modulo $n$ until you are comfortable with modular arithmetic. Do some divisions too, whenever you can.
2. Notice that you can find a correspondence between the days of the week and $\mathbb{Z}_7$. (E.g. let Sun $\leftrightarrow \overline{0}$, Mon $\leftrightarrow \overline{1}$, etc.) Use arithmetic modulo 7 to compute what day of the week it will be a month from today. What about a year from today? What about 10 years ago? Compute on what day of the week your birthday was.
3. Show that the way we defined subtraction on $\mathbb{Z}_n$ does not depend on the choice of representatives for $\overline{k}$ and $\overline{m}$.
4. Show that the way we defined multiplication on $\mathbb{Z}_n$ does not depend on the choice of representatives for $\overline{k}$ and $\overline{m}$.

2.6. **Zero divisors and inverses.** Being able to divide is a very useful thing because it allows you to solve linear equations. So we will further investigate what elements of $\mathbb{Z}_n$ we can divide by and which ones we cannot divide by. First observe that if we can do $\overline{1}/\overline{m}$, we can also do $\overline{k}/\overline{m}$ because we can just multiply $\overline{1}/\overline{m}$ by $\overline{k}$. So what we really need to know is which elements of $\mathbb{Z}_n$ have reciprocals, or in other words multiplicative inverses.

In the example above, we saw that $\overline{2}$ in $\mathbb{Z}_6$ does not have a multiplicative inverse. Then I showed you that $\overline{2}$ must not have a multiplicative inverse because if it did $\overline{3}$ would have to be $\overline{0}$. The crux of the argument was that $\overline{2}\,\overline{3} = \overline{0}$ in $\mathbb{Z}_6$. This is very strange indeed. We multiply two things neither of which is $\overline{0}$, and yet we get $\overline{0}$. This deserves a definition:

**Definition 4.** *In $\mathbb{Z}_n$, we say that a nonzero element $x$ is a* zero divisor *if there exists another nonzero element $y$ such that*

$$xy = \overline{0}$$

Zero divisors are bad because

**Proposition 2.** *An element $x \in \mathbb{Z}_n$ that is a zero divisor cannot have a multiplicative inverse.*

*Proof:* Since $x$ is a zero divisor there must exist $y \neq \overline{0}$ such that $xy = \overline{0}$. If $x$ had an inverse $z \in \mathbb{Z}_n$, then

$$y = \overline{1}y = (zx)y = z(xy) = z\overline{0} = \overline{0}$$

But that is a contradiction. □

Actually, the converse is also true, although it is a little more difficult to prove:

**Proposition 3.** *An element $x \in \mathbb{Z}_n$ that is not a zero divisor has a multiplicative inverse.*

*Proof:* Let $x \in \mathbb{Z}_n$ be a nonzero divisor. Define the function $f : \mathbb{Z}_n \to \mathbb{Z}_n$ by $f(y) = xy$. First, we will show that $f$ is one-to-one. Let $y, z \in \mathbb{Z}_n$. If $f(y) = f(z)$, then

$$\begin{aligned} xy &= xz \\ xy - xz &= 0 \\ x(y - z) &= 0 \end{aligned}$$

Since $x$ is not a zero divisor, $y - z$ must be 0. That is $y = z$. So $f$ is indeed one-to-one. This means $f$ sends different elements of $\mathbb{Z}_n$ to different elements of $\mathbb{Z}_n$. Hence just like $\mathbb{Z}_n$, the image of $f$ has exactly $n$ elements in it. But $\text{im}(f) \subseteq \mathbb{Z}_n$. The only way it fits in there is if $\text{im}(f) = \mathbb{Z}_n$.

So $f$ is also onto. Hence there must exist some element $y \in \mathbb{Z}_n$ such that $f(y) = 1$. But this $y$ is then a multiplicative inverse of $x$. □

Hence the elements of $\mathbb{Z}_n$ which have inverses are exactly the ones which are not zero divisors.

**Theorem 2.** *$\mathbb{Z}_n$ has no zero divisors if and only if $n$ is prime.*

*Proof:* First, suppose $n$ is prime. Let $\overline{k}, \overline{m} \in \mathbb{Z}_n$ such that $\overline{k}\overline{m} = \overline{0}$. That is $km$ is a multiple of $n$. Since $n$ is prime, it must divide either $k$ or $m$. But then either $\overline{k} = \overline{0}$ or $\overline{m} = \overline{0}$. So there cannot exist nonzero elements in $\mathbb{Z}_n$ whose product is $\overline{0}$.

Now, suppose $n$ is composite. Then we can find a proper factorization $n = km$. Since $1 < k, m < n$, $\overline{k} \neq \overline{0}$ and $\overline{m} \neq \overline{0}$. But $\overline{k}\overline{m} = \overline{n} = \overline{0}$. So $\overline{k}$ (or $\overline{m}$ for that matter) is a zero divisor. □

**Corollary 2.** *Every nonzero element of $\mathbb{Z}_n$ has a multiplicative inverse if and only if $n$ is prime.*

*Proof:* By Propositions 2 and 3, we know that an element of $\mathbb{Z}_n$ has an inverse if and only if it is not a zero divisor.

If $n$ is prime, then $\mathbb{Z}_n$ contains no zero divisors, therefore every element has an inverse.

If $n$ is composite, then $\mathbb{Z}_n$ contains some zero divisors, and those have no inverses. □

2.7. **Zero divisors and polynomials.** We know that a polynomial of degree $k$ in the complex numbers has exactly $k$ roots when counting with multiplicity. A polynomial of degree $n$ in the real numbers has at most $k$ roots. (The same polynomial when viewed over the complex numbers will have $k$ roots, but some of them may not be real.)

In $\mathbb{Z}_n$, where there may be zero divisors around, a polynomial of degree $k$ can have more than $k$ roots. E.g. let's look for the roots of the polynomial $x^2 - x$ in $\mathbb{Z}_6$. We immediately notice we can factor $x^2 - x = x(x - \overline{1})$. This may lead us to believe that

$$x^2 - x = \overline{0}$$
$$x(x - \overline{1}) = \overline{0}$$

has roots $x = \overline{0}$ and $x = \overline{1}$. But $x = \overline{3}$ and $x = \overline{4}$ are also roots. Why does this happen? When you look at the factorization $x(x - \overline{1})$, you conclude $x = \overline{0}$ and $x = \overline{1}$ are roots because you are used to the fact that when a product is zero, at least one of its factors must be zero. But this is not the case in $\mathbb{Z}_6$ where there are zero divisors. $x(x - \overline{1})$ could be equal to $\overline{0}$ without either $x$ or $x - \overline{1}$ being equal to $\overline{0}$.

Another thing you may notice is that $x^2 - x$ in fact also factors as $(x - \overline{3})(x - \overline{4})$ over $\mathbb{Z}_6$. This is also unusual. Over the real numbers or the complex numbers, every polynomial factors uniquely into irreducible factors. But the presence of zero divisors in $\mathbb{Z}_6$ makes it possible to factor the same polynomial into irreducible factors in several ways.

## 3. Operations and their properties

3.1. **Binary operations.**

**Definition 5.** *A* (binary) operation *on the set $S$ is a function $\circ : S \times S \to S$.*

The customary notation is to write $x \circ y$ instead of $\circ(x, y)$.

So the criterion for $\circ$ to be an operation on $S$ is that for all $x, y \in S$, $x \circ y$ is an element of $S$. Another way to say $x \circ y \in S$ for all $x, y \in S$ is that $S$ is *closed* under $\circ$. Notice that being an operation is a property of $\circ$ with respect to $S$, while being closed is a property of $S$ with respect to $\circ$. Which is more convenient to say depends on the context. You can use either, but don't confuse them. Again, saying things like $\circ$ is closed makes no sense.

**Example 4.** $\circ$ *defined by* $x \circ y = x - y$ *is an operation on* $\mathbb{R}$ *because* $x - y$ *is a real number whenever* $x, y \in \mathbb{R}$.

**Example 5.** $\circ$ *defined by* $x \circ y = x/y$ *is not an operation on* $\mathbb{R}$ *because* $x/y$ *is not always a real number if* $x, y \in \mathbb{R}$. *E.g.* $1 \circ 0 = 1/0$ *does not even exist.*

**Example 6.** $\circ$ *defined by* $x \circ y = \sqrt{xy}$ *is not operation on* $\mathbb{Q}$ *because* $\sqrt{xy}$ *is not always a rational number if* $x, y \in \mathbb{Q}$. *E.g.* $1 \circ 2 = \sqrt{(1)(2)}$ *is well-known to be irrational.*

**Exercises:** Prove that the following are operations:

1. $+$ on $\mathbb{N}$
2. $+$ on $\mathbb{Q}$
3. $+$ on $\mathbb{Z}_n$
4. $+$ on $\mathbb{C}$
5. $\cdot$ on $\mathbb{N}$
6. $\cdot$ on $\mathbb{Q}$
7. $\cdot$ on $\mathbb{C}$
8. $-$ on $\mathbb{Z}$
9. $/$ on $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$
10. $x \circ y = (x + 1)(y - 1)$ on $\mathbb{C}$.
11. Composition of functions on the set of functions $\mathbb{R} \to \mathbb{R}$.
12. Composition of functions on $\mathbb{Q}[x]$, which is the set of all polynomials with rational coefficients.

Prove that the following are not operations:

1. $-$ on $\mathbb{N}$
2. $/$ on $\mathbb{Q}$
3. $/$ on $\mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$
4. $x \circ y = \sqrt{xy}$ on $\mathbb{R}$.
5. Dot product of vectors on $\mathbb{R}^2$.

### 3.2. **Commutativity.**

**Definition 6.** *An operation* $\circ$ *on the set* $S$ *is* commutative *if* $x \circ y = y \circ x$ *for all* $x, y \in S$.

The "for all" part in this definition is crucial. Given any operation on any set, it's easy to find two elements $x, y \in S$ such that $x \circ y = y \circ x$. E.g. you could just take $y = x$. The real question is whether you can find $x, y \in S$ such that $x \circ y \neq y \circ x$. If not, $\circ$ is commutative.

**Example 7.** $+$ *on* $\mathbb{Z}$ *is commutative because* $x + y = y + x$ *for any integers* $x, y$.

**Example 8.** $-$ *on* $\mathbb{Z}$ *is not commutative because* $x - y \neq y - x$ *in general, e.g.* $0 - 1 \neq 1 - 0$.

**Example 9.** *Composition of functions on the set of functions* $\mathbb{R} \to \mathbb{R}$ *is not commutative because* $f \circ g \neq g \circ f$ *in general. E.g. let* $f(x) = -x$ *and* $g(x) = x^2$. *Then* $f \circ g(x) = f(g(x)) = -x^2$ *and* $g \circ f(x) = g(f(x)) = (-x)^2 = x^2$ *are not the same.*

**Exercises:** Which of the following operations are commutative?

1. $\cdot$ on $\mathbb{R}$
2. $\cdot$ on $\mathbb{C}$
3. $-$ on $\mathbb{Z}_2$
4. $/$ on $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$
5. $x \circ y = x^y$ on $\mathbb{R}^+ = \{x \in \mathbb{R} \mid x > 0\}$.

3.3. **Associativity.**

**Definition 7.** *An operation $\circ$ on the set $S$ is* associative *if $(x \circ y) \circ z = x \circ (y \circ z)$ for all $x, y, z \in S$.*

Notice that commutativity and associativity are properties of the operation $\circ$ and not of the set $S$. Saying things like $\mathbb{R}$ is associative makes about as much sense as claiming that the temperature is purple today.

**Example 10.** *$\cdot$ on $\mathbb{Z}$ is associative because $(xy)z) = x(yz)$ for any integers $x, y$.*

**Example 11.** *$-$ on $\mathbb{Z}$ is not associative because $(x-y)-z \neq y-(x-z)$ in general, e.g. $(0-1)-1 \neq 0-(1-1)$.*

**Example 12.** *Composition of functions on the set of functions $\mathbb{R} \to \mathbb{R}$ is associative. To see this we need to convince ourselves that $(f \circ g) \circ h = f \circ (g \circ h)$ for any functions $f, g, h$. We are comparing two functions here. Two functions are equal if they have the same domain and codomain and their values agree on all elements of this common domain. Both $(f \circ g) \circ h$ and $f \circ (g \circ h)$ have $\mathbb{R}$ for the domain and the codomain. So let's see if they agree for all $x \in \mathbb{R}$.*

$$(f \circ g) \circ h(x) = f \circ g(h(x)) = f(g(h(x)))$$
$$f \circ (g \circ h)(x) = f(g \circ h(x)) = f(g(h(x)))$$

*These are indeed the same for all $x$.*

**Exercises:** Which of the following operations are associative?

1. $\cdot$ on $\mathbb{Z}_n$
2. $\cdot$ on $\mathbb{C}$
3. $/$ on $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$
4. $x \circ y = (x+1)(y-1)$ on $\mathbb{C}$
5. $x \circ y = x^y$ on $\mathbb{R}^+ = \{x \in \mathbb{R} \mid x > 0\}$.

3.4. **Identity.**

**Definition 8.** *Given an operation $\circ$ on a set $S$, we say $x \in S$ is an* identity *if $x \circ s = s$ for all $s \in S$ and $s \circ x = s$ for all $s \in S$.*

**Example 13.** *For $+$ on $\mathbb{Z}$, $0$ is an identity because $0 + x = x = x + 0$ for all $x \in \mathbb{Z}$.*

**Example 14.** *For $\cdot$ on $\mathbb{Z}_n$, $\overline{1}$ is an identity because $\overline{1} \cdot x = x = x \cdot \overline{1}$ for all $x \in \mathbb{R}$.*

**Example 15.** *For composition on the set of functions $\mathbb{R} \to \mathbb{R}$, the identity function $f(x) = x$ is an identity since $f \circ g(x) = f(g(x)) = g(x)$ and $g \circ f(x) = g(f(x)) = g(x)$ for every function $g$.*

**Example 16.** *The operation $x \circ y = xy - 1$ on $\mathbb{Z}$ has no identity. If $y \in \mathbb{Z}$ were an identity, it would have to satisfy $x = x \circ y = xy - 1$ for all $x$. In particular, if $x = 1$, we get $y = 2$ and if $x = 2$ we get $y = 3/2$, and $y$ cannot be both at the same time, not to mention that $3/2$ is not even in $\mathbb{Z}$.*

**Example 17.** *The operation $x \circ y = x\overline{y}$ on $\mathbb{C}$ does not have an identity either. If $y \in \mathbb{C}$ were an identity, it would have to satisfy $x = x \circ y = x\overline{y}$ for all $x \in \mathbb{C}$, which suggests $\overline{y} = 1$ and hence $y = 1$. But $1 \circ x = 1\overline{x} \neq x$ in general. E.g. $\overline{i} \neq i$.*

**Exercises:** Which of the following operations have identities and what are they?

1. $\cdot$ on $\mathbb{Z}_n$
2. $x \circ y = x^4 y$ on $\mathbb{Z}_5$
3. $-$ on $\mathbb{Z}$
4. $+$ on the set of all functions $\mathbb{R} \to \mathbb{R}$ (recall $f + g$ is defined by $(f + g)(x) = f(x) + g(x)$)
5. $/$ on $\mathbb{R}^*$
6. $x \circ y = (x+1)(y-1)$ on $\mathbb{C}$

7. $x \circ y = x^y$ on $\mathbb{R}^+$.

**Proposition 4.** *If an operation $\circ$ on the set $S$ has an identity, this identity is unique.*

The proof of this was a homework problem.

3.5. **Inverses.**

**Definition 9.** *Let $\circ$ be an operation on the set $S$ and assume $\circ$ has an identity $e$. We say that $x \in S$ has an* inverse *if there exists a $y \in S$ such that $x \circ y = e$ and $y \circ x = e$.*

**Example 18.** *Consider $+$ on $\mathbb{Z}$. We know $0$ is the identity (we can say "the" identity because we now know there can only be one). Every $x \in \mathbb{Z}$ has an inverse, namely $-x$ because $x + (-x) = 0$ and $(-x) + x = 0$.*

**Example 19.** *Consider $\cdot$ on $\mathbb{R}$. We know $1$ is the identity. The element $2$ then has inverse $1/2$. The element $0$ has no inverse because no matter what you multiply $0$ by, you never get $1$. In fact, if $x \in \mathbb{R}$ and $x \neq 0$, then $x$ has inverse $1/x$ with respect to this operation.*

**Example 20.** *Consider composition on all functions $\mathbb{R} \to \mathbb{R}$. We know that the identity is $f(x) = x$. The function $g(x) = x - 1$ has inverse $g^{-1}(x) = x + 1$. The function $g(x) = 3x$ has inverse $g^{-1}(x) = x/3$. The function $g(x) = x^2$ has no inverse because it is not one-to-one. (Why can't a function that is not one-to-one have an inverse?) The function $f(x) = e^x$ has no inverse either because it is not onto. You might now say, but wait, I learned in precalculus that the inverse of $e^x$ is $\log(x)$. But the problem is that $\log(x)$ is not a function $\mathbb{R} \to \mathbb{R}$ because its domain only includes the positive real numbers. So the way we defined our operation, $e^x$ has no inverse. In fact, the function has an inverse with respect to our operation iff it is both one-to-one and onto.*

**Exercises:** Which of the following operations are such that every element of the underlying set has an inverse?

1. $\cdot$ on $\mathbb{Z}^+ = \{x \in \mathbb{Z} \mid x > 0\}$
2. $\cdot$ on $\mathbb{Z}_n$
3. $\cdot$ on $\mathbb{Z}_p$
4. $\cdot$ on $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{\overline{0}\}$
5. Composition of functions on $\mathbb{Q}[x]$, which is the set of all polynomials with rational coefficients.
6. $\cdot$ on the set of all functions $\mathbb{R} \to \mathbb{R}$ (recall $fg$ is defined by $(fg)(x) = f(x)g(x)$)
7. $\cdot$ on $\mathbb{R}[x]$, the set of all polynomials with real coefficients
8. $\cdot$ on $\mathbb{R}(x)$, which is the set of all rational functions with real coefficients.

**Proposition 5.** *Let $\circ$ be an associative operation on the set $S$ and assume that it has an identity $e$. If $x \in S$ has an inverse, then this inverse is unique.*

In other words, an element can have no inverse, or one inverse, but it cannot have two distinct inverses. The proof was a homework exercise. Can you find an example of an operation with an identity for which inverses don't have to be unique? By the above theorem, such an operation would have to be nonassociative. (Finding such an example may be quite hard.)

## 4. Fields

**Definition 10.** *A* field *is a set $F$ with two operations $+$ and $\cdot$ such that*

1. *$+$ and $\cdot$ are both commutative and associative*
2. *$+$ has an identity denoted by $0 \in F$*
3. *$\cdot$ has an identity denoted by $1 \in F$*
4. *Every element has an inverse with respect to $+$*
5. *Every element except $0$ has an inverse with respect to $\cdot$*

6. $+$ *and* $\cdot$ *are distributive, which means* $x \cdot (y + z) = x \cdot y + x \cdot z$ *for all* $x, y, z \in F$
7. $0 \neq 1$

Note that $+$ and $\cdot$ may have nothing to do with the addition and multiplication of numbers you are familiar with. But their properties indeed mimic those of usual addition and multiplication. The operation $+$ is referred to as addition and $\cdot$ is referred to as multiplication. $\cdot$ is usually omitted in formulas, just like multiplication of numbers. 0 is called zero and 1 is called one, although they may have nothing to do with the real numbers 0 and 1. The rules about additive and multiplicative inverses in essence say that you can subtract any element from any element and you can divide any element by any nonzero element (0 has no multiplicative inverse).

**Example 21.** $\mathbb{R}$ *with ordinary addition and multiplication is a field. In this case the additive identity and the multiplicative identity are the numbers* 0 *and* 1 *you are familiar with. The additive inverse of a number is its usual negative and the multiplicative inverse is the usual reciprocal. (Notice* 0 *has no reciprocal, but it doesn't have to have a multiplicative inverse.) Commutativity, associativity, and distributivity are properties you learned about long ago.*

**Example 22.** $\mathbb{Z}$ *with ordinary addition and multiplication is not a field because not every nonzero element has a multiplicative inverse. E.g.* 2 *does not.*

**Example 23.** $\mathbb{Z}_p$ *where* $p$ *is prime is a field. We showed in class that* $+$ *and* $\cdot$ *are operations. They are commutative and associative on* $\mathbb{Z}_p$ *because they are commutative and associative on* $\mathbb{Z}$ *and* $+$ *and* $\cdot$ *on* $\mathbb{Z}_p$ *is defined in terms of* $+$ *and* $\cdot$ *on* $\mathbb{Z}$*. (If this last statement doesn't make sense to you, you should verify* $+$ *and* $\cdot$ *are indeed commutative and associative on* $\mathbb{Z}_p$ *by writing down the four equalities that must hold.) We saw in class that* $\overline{0}$ *is an additive identity, and* $\overline{1}$ *is a multiplicative identity. We also saw that* $\overline{k}$ *has additive inverse* $\overline{-k}$ *(this should be obvious). We proved that every* $\overline{k} \neq \overline{0}$ *has a multiplicative inverse (this is not obvious, but we proved it in Corollary 2). Distributivity holds for the same reason as commutativity and associativity.*

**Example 24.** $\mathbb{Z}_n$ *is not a field if* $n$ *is not prime. This is because* $n$ *has a proper divisor, which is then a zero divisor, hence cannot have a multiplicative inverse. All the other field axioms are satisfied.*

**Example 25.** *The subset* $\mathbb{Q}[\sqrt{2}] = \left\{x + y\sqrt{2} \mid x, y \in \mathbb{Q}\right\}$ *of* $\mathbb{R}$ *is a field with usual addition and multiplication. In fact, we can say it is a subfield of* $\mathbb{R}$*. It is closed under* $+$ *because*

$$(x + y\sqrt{2}) + (x' + y'\sqrt{2}) = (x + x') + (y + y')\sqrt{2}) \in \mathbb{Q}[\sqrt{2}]$$

*It is closed under* $\cdot$ *because*

$$(x + y\sqrt{2})(x' + y'\sqrt{2}) = (xx' + 2yy') + (xy' + x'y)\sqrt{2}) \in \mathbb{Q}[\sqrt{2}]$$

*It has additive and multiplicative identities* $0 = 0 + 0\sqrt{2}$ *and* $1 = 1 + 0\sqrt{2}$*. The element* $x + y\sqrt{2}$ *has an additive inverse because*

$$-(x + y\sqrt{2}) = -x + (-y)\sqrt{2} \in \mathbb{Q}[\sqrt{2}$$

*If* $x + y\sqrt{2} \neq 0$*, that is at least one of* $x$ *or* $y$ *is not* 0*, then it has multiplicative inverse because*

$$\frac{1}{x + y\sqrt{2}} = \frac{1}{x + y\sqrt{2}} \frac{x - y\sqrt{2}}{x - y\sqrt{2}} = \frac{x - y\sqrt{2}}{x^2 - 2y^2} = \frac{x}{x^2 - 2y^2} + \frac{-y}{x^2 - 2y^2}\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$$

*(Why can't* $x^2 - 2y^2 = 0$*? Remember* $x, y$ *are rational numbers.) The two commutativity and associativity axioms and the distributivity axiom hold because they hold for* $+$ *and* $\cdot$ *on* $\mathbb{R}$*, which contains* $\mathbb{Q}[\sqrt{2}]$*.*

**Example 26.** *Consider the set of all functions $\mathbb{R} \to \mathbb{R}$ with addition defined by $(f+g)(x) = f(x) + g(x)$ and multiplication $fg(x) = f(g(x))$. In other words, multiplication is composition here. Is this a field? You can easily check that addition is indeed an operation, is commutative and associative, has the zero function $f(x) = 0$ for identity, and every function $f$ has an inverse $-f$ defined by $(-f)(x) = -f(x)$. The multiplication (which is composition in this case) is an operation, is associative, and has the identity function $f(x) = x$ for an identity. But it is not commutative, and not every nonzero function has a multiplicative inverse. For example, $f(x) = x^2$ is not invertible because it is not one-to-one. Distributivity also fails:*

$$[f(g+h)](x) = f(g(x) + h(x))$$
$$(fg + fh)(x) = f(g(x)) + f(h(x))$$

*which are in general not equal. E.g. try $f(x) = x^2$, $g(x) = x$, and $h(x) = x$.*

**Example 27.** *The set $\{1\}$ with addition defined as $1 + 1 = 1$, and multiplication $1 \cdot 1 = 1$ is not a field. Actually, it satisfies almost all axioms. It even has an additive identity and a multiplicative identity. But they are the same thing, so it fails the axiom $0 \neq 1$.*

**Exercises:** Which of the following are fields?

1. $\mathbb{C}$ with usual addition and multiplication.
2. $\mathbb{Q}$ with usual addition and multiplication.
3. $\mathbb{Z}_p[x]$, the set of all polynomials with coefficients in $\mathbb{Z}_p$ with usual polynomial addition and multiplication.
4. The set of all functions $\mathbb{R} \to \mathbb{R}$ with usual addition and multiplication of functions.
5. The set of all functions $f : \mathbb{R} \to \mathbb{R}$ such that $f(x) \neq 0$ for any $x \in \mathbb{R}$ with usual addition and multiplication of functions.
6. $\mathbb{R}(x)$, the set of all (formal) rational functions with real coefficients with usual addition and multiplication of functions. That they are formal rational functions means you don't have to worry about what the domain is when you add and multiply them.
7. The subset $\mathbb{Z}[i] = \{x + yi \mid x, y \in \mathbb{Z}\}$ of $\mathbb{C}$ with ordinary addition and multiplication.
8. The subset $\mathbb{Q}[i] = \{x + yi \mid x, y \in \mathbb{Q}\}$ of $\mathbb{C}$ with ordinary addition and multiplication.