Lecture Notes for MAT 4170

Lily Silverstein

Contents

1 Preliminaries

1.1 Some notation for common sets

- $\mathbb{N} :=$ the set of natural numbers, $\{1, 2, 3, \ldots\}$
- $\mathbb{Z} :=$ the set of integers, $\{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$
- $\mathbb{Q} :=$ the set of rational numbers, $\{p/q : p, q \in \mathbb{Z}, q \neq 0\}$
- $\mathbb{R} :=$ the set of real numbers
- $\mathbb{C} :=$ the set of complex numbers, $\{a + bi : a, b \in \mathbb{R}\}$ where $i = \sqrt{-1}$

Also, you might see:

- $\mathbb{R}_{\geq 0}$, shorthand for $\{r \in \mathbb{R} : r \geq 0\}$, i.e. all non-negative real numbers (includes 0)
- $\mathbb{R}_{>0}$, shorthand for $\{r \in \mathbb{R} : r > 0\}$, i.e. all positive real numbers (not including 0)
- Or $\mathbb{Q}_{\geq 0}$, $\mathbb{Q}_{>0}$, etc.

1.2 Domain, codomain, ~~range~~, and image

Let $f : \mathbb{R} \to \mathbb{R}$ be defined by $f(x) = x^2$. We know that the domain of the function f is $\mathbb{R}$. But what is its range? Is it $\mathbb{R}$, the "target space" of the function? Or is it $\mathbb{R}_{\geq 0}$, the set of output values that the function takes? *"Range" is ambiguous because both of these different meanings are in use.* So we will not use the word range. Instead we will use codomain and image.

If f is a function from a set A to a set B, then A is its **domain** and B is its **codomain**.

$$f : \underset{\text{domain}}{\boxed{A}} \longrightarrow \underset{\text{codomain}}{\boxed{B}}$$

The **image** of f is the set $\{f(a) : a \in A\}$, the set of output values. There are two ways you'll seen this written: $\text{Im}(f)$ and $f(A)$. You should be familiar with both.

So in the example $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^2$, the codomain of f is $\mathbb{R}$, while the image of f is $\mathbb{R}_{\geq 0}$.

1.3 Well-defined maps

Often Judson uses the word **map** or **mapping** instead of function. They mean exactly the same thing. Sometimes when Judson says "map," he is emphasizing that the function is **well-defined**, meaning that for each input value, there is one and only one output value. This is part of the definition of function so we usually take it for granted, but in 4170 there will be times when it is critical to check that a function is well-defined.

Here are some examples of functions that are *not* well-defined:

- Define $\phi : \mathbb{R} \to \mathbb{R}$ by $\phi(x) = \sqrt{x}$. This is not well-defined because $\phi(-4)$ doesn't exist.

- Define $\psi : \mathbb{Q} \to \mathbb{Z}$ by $\psi\left(\frac{a}{b}\right) = a + b$. This is not well-defined for a different reason. The problem is that there is more than one way to represent elements of the domain. For instance 1/2 and 5/10 are two equivalent ways to write the same rational number. But $\psi\left(\frac{1}{2}\right) = 3$ while $\psi\left(\frac{5}{10}\right) = 15$. So this "function" does not assign a unique output to every rational number.

The second kind of problem is the one you most need to watch out for in 4170, and it's a concern whenever there is more than one way to represent the elements of a set. (Like how rational numbers can be represented by fractions in more than one way.)

To prove that a given function is well-defined, therefore, you need to show that this can't happen; that the choice of representation doesn't matter. To do this, you have to:

1. Assume that two *arbitrary* elements of the domain are equal.

2. Prove that they are mapped to the same element of the codomain.

In symbols: to show that $f : A \to B$ is well-defined, let $x, y \in A$ such that $x = y$, then prove that $f(x) = f(y) \in B$.

Example: Define $g : \mathbb{Q} \to \mathbb{Q}$ by $g\left(\frac{a}{b}\right) = \frac{a^2}{b^2}$. Suppose that $\frac{a}{b} = \frac{c}{d} \in \mathbb{Q}$. Then

$$g\left(\frac{a}{b}\right) = \frac{a^2}{b^2} = \left(\frac{a}{b}\right)^2 = \left(\frac{c}{d}\right)^2 = \left(\frac{c}{d}\right) = g\left(\frac{c}{d}\right).$$

Therefore g is well-defined.

1.4 One-to-one (injective) and onto (surjective)

You might notice that proving a map is well-defined is sort of the "opposite" of proving that it is **one-to-one**. Remember that to prove that a given map is one-to-one, you have to

1. Assume that two *arbitrary* elements of the domain are mapped to the same element of the codomain.

2. Prove that those two elements are equal.

In symbols: to prove that $f : A \to B$ is one-to-one, let $x, y \in A$ such that $f(x) = f(y)$, then prove that $x = y$.

The word **injective** is a synonym for one-to-one. Sometimes an injective function is simply called an **injection**.

Finally, recall that to prove that a map is **onto**, you have to show that every element of the codomain is also an element of the image. The way to do this is:

1. Choose an *arbitrary* element of the codomain.

2. Show that there is an element in the domain that maps to it.

In symbols: to prove that $f : A \to B$ is onto, let $y \in B$, then show that there exists an $x \in A$ such that $f(x) = y$.

The word **surjective** is a synonym for onto. Sometimes a surjective function is simply called a **surjection**.

Important: all three of these proof methods (well-defined, one-to-one, and onto) only work if you start with arbitrary elements. That is, designate the elements by variables and do *not* choose specific members of the set! That is the only way to show that the statement holds for *all* elements.

1.5 Problems

1. For each of the following functions, determine: (i) if it is well-defined, (ii) the domain, (iii) the codomain, (iv) the image, (v) if the function is injective, and (vi) if the function is surjective.

a. $g : \mathbb{R} \to \mathbb{R}$ by $g(x) = x^2$.

b. $T : \mathbb{R}^3 \to \mathbb{R}^2$ by

$$T\left(\begin{bmatrix} a \\ b \\ c \end{bmatrix}\right) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} a \\ b \\ c \end{bmatrix}$$

c. $U : \mathbb{R}^2 \to \mathbb{R}^3$ by

$$U\left(\begin{bmatrix} a \\ b \end{bmatrix}\right) = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix}$$

d. $f : M_2(\mathbb{R}) \to \mathbb{R}$ by $f(A) = \det(A)$

e. $f : \mathbb{R} \to M_2(\mathbb{R})$ defined by

$$f(x) = \begin{bmatrix} \cos(x) & -\sin(x) \\ \sin(x) & \cos(x) \end{bmatrix}$$

f. $f : [0, 2\pi) \to M_2(\mathbb{R})$ defined by

$$f(x) = \begin{bmatrix} \cos(x) & -\sin(x) \\ \sin(x) & \cos(x) \end{bmatrix}$$

1.6 GCD's, the Euclidean Algorithm, and the extended Euclidean algorithm

The greatest common divisor of two natural numbers is the largest natural number that divides both of them. More formally,

Definition. Let $a, b \in \mathbb{N}$. The **greatest common divisor** of a and b, written $\gcd(a, b)$, is the natural number d such that:

1. $d | a$ and $d | b$, and

2. if c is any natural number that divides a and b, then $c \leq d$.

Example. $\gcd(18, 30) = 6$

Example. We use the concept of greatest common divisor, though not necessary the name, when we reduce fractions. For instance to reduce $\frac{18}{30}$, we divide both numerator and denominator by $\gcd(18, 30) = 6$ to get $\frac{3}{5}$. Now the fraction is reduced because 3 and 5 are relatively prime.

Definition. For $a, b \in \mathbb{N}$, we call a and b **relatively prime** if $\gcd(a, b) = 1$.

There are three methods for finding the greatest common divisor of two numbers.

Method 1. List all the divisors of each number. The gcd is the largest number that appears in both lists.

$$18 : 1, 2, 3, \boxed{6}, 9, 18.$$

$$30 : 1, 2, 3, 5, \boxed{6}, 10, 15, 30$$

Method 2. Factor both numbers into a product of primes and take the smallest power of each prime.

$$8232 = 2^3 \cdot 3 \cdot 7^3$$

$$3920 = 2^4 \cdot 5 \cdot 7^2$$

So $\gcd(8232, 3920) = 2^3 \cdot 7^2 = 392$.

These methods don't scale very well, because it's hard to find the divisors/prime divisors of very large integers. Luckily there is a better way.

Method 3. The Euclidean Algorithm. This method works by using the Division Algorithm repeatedly. Before stating the definition, let's see an example where we find $\gcd(1960, 1008)$.

$$\begin{aligned} 1960 &= 1 \cdot 1008 + 952 \\ 1008 &= 1 \cdot 952 + 56 \\ 952 &= 17 \cdot 56 + 0 \end{aligned}$$

Therefore $\gcd(1960, 1008) = 56$.

And in general,

Definition. Euclidean Algorithm.
Let a and b be integers with $a \geq b > 0$. Applying the division algorithm repeatedly, we obtain integers $q_1, q_2, \ldots, q_{n+1}$ and $r_1, r_2, \ldots, r_n$ such that

$$\begin{aligned} a &= q_1 b + r_1, & 0 &\leq r_1 < b \\ b &= q_2 r_1 + r_2, & 0 &\leq r_2 < r_1 \\ r_1 &= q_3 r_2 + r_3, & 0 &\leq r_3 < r_2 \\ &\vdots \\ r_{n-1} &= q_{n+1} r_n + 0 \end{aligned}$$

Then $\gcd(a, b) = r_n$.

Before we prove that the Euclidean Algorithm works, we will prove an important lemma.

Theorem. If $a = qb + r$, then $\gcd(a, b) = \gcd(b, r)$.

Proof. Let $d = \gcd(a, b)$. By definition, $d|a$ and $d|b$, and if $c|a$ and $c|b$ then $c \leq d$. We need to show that

1. $d|b$ and $d|r$, and

2. if $c|b$ and $c|r$, then $c \leq d$.

We already know that $d|b$. To see that $d|r$, note that $r = a - qb$. Since $a = dm$ for some $m \in \mathbb{Z}$, and $b = dn$ for some $n \in \mathbb{Z}$, we have $r = dm - qdn = d(m - qn)$ where $m - qn \in \mathbb{Z}$ and therefore $d|r$. This proves **1.**

Now suppose that $c|b$ and $c|r$. Again, since $a = qb + r$ and both b and r are multiples of c, this shows $c|a$. Since $c|a$ and $c|b$, but $d = \gcd(a, b)$, we know $c \leq d$. Therefore **2.** is true, so $\gcd(b, r) = d = \gcd(a, b)$. □

Now let's prove that the Euclidean Algorithm works.

Proof. Suppose we perform the Euclidean Algorithm on $a \geq b > 0$ and get the following sequence:

$$\begin{aligned} a &= q_1 b + r_1, & 0 \leq r_1 < b \\ b &= q_2 r_1 + r_2, & 0 \leq r_2 < r_1 \\ r_1 &= q_3 r_2 + r_3, & 0 \leq r_3 < r_2 \\ &\vdots \\ r_{n-1} &= q_{n+1} r_n + 0 \end{aligned}$$

Then by the lemma, $\gcd(a, b) = \gcd(b, r_1) = \gcd(r_1, r_2) = \cdots = \gcd(r_{n-1}, r_n)$. Now note that $\gcd(r_{n-1}, r_n) = r_n$, because $r_n | r_n$ and $r_n | r_{n-1}$, and r_n is the largest integer that can divide r_n. Therefore $\gcd(a, b) = r_n$. □

The Extended Euclidean Algorithm

Now we know that there always *exists* a linear combination $ax + by = \gcd(a, b)$. But how do we *find* x and y? One way is to use the Euclidean Algorithm "backwards."

Example. Find x and y satisfying $18x + 30y = \gcd(18, 30)$.

First we perform the Euclidean Algorithm to find $\gcd(18, 30)$. Even if you can see by inspection that the gcd is 6, you should write out the steps because we will use them in the next part.

$$\begin{aligned} 30 =& 1 \cdot 18 + 12 \\ 18 =& 1 \cdot 12 + 6 \\ 12 =& 2 \cdot 6 + 0 \end{aligned}$$

Notice that every line with a non-zero remainder can be rewritten to express the remainder as a linear combination of previous integers. In this case, we rewrite the second line as $6 = 18 - 1 \cdot 12$, and rewrite the first line as $12 = 30 - 1 \cdot 18$.

Starting with the gcd (the last nonzero remainder), we go backwards through the lines and make these substitutions.

$$\begin{aligned} 6 &= 18 - 1 \cdot 12 \\ 6 &= 18 - 1 \cdot (30 - 1 \cdot 18) = 2 \cdot 18 - 1 \cdot 30 \end{aligned}$$

So $x = 2, y = -1$ is a solution to $18x + 30y = 6$.

Example. Find x and y satisfying $112x + 241y = \gcd(112, 241)$.

First we perform the Euclidean Algorithm.

$$\begin{aligned} 241 &= 2 \cdot 112 + 17 \\ 112 &= 6 \cdot 17 + 10 \\ 17 &= 1 \cdot 10 + 7 \\ 10 &= 1 \cdot 7 + 3 \\ 7 &= 2 \cdot 3 + 1 \\ 3 &= 1 \cdot 3 + 0 \end{aligned}$$

So $1 = \gcd(112, 241)$.

Now we go backwards, starting with the second-to-last line with the gcd as the remainder:

$$1 = 7 - 2 \cdot 3$$

Make the next substitution, $3 = 10 - 1 \cdot 7$, then collect like terms:

$$\begin{aligned} &= 7 - 2(10 - 1 \cdot 7) \\ &= -2 \cdot 10 + 3 \cdot 7 \end{aligned}$$

The next substitution is $7 = 17 - 1 \cdot 10$.

$$\begin{aligned} &= -2 \cdot 10 + 3(17 - 1 \cdot 10) \\ &= 3 \cdot 17 - 5 \cdot 10 \end{aligned}$$

Continuing this process:

$$\begin{aligned} &= 3 \cdot 17 - 5(112 - 6 \cdot 17) \\ &= -5 \cdot 112 + 33 \cdot 17 \\ &= -5 \cdot 112 + 33(241 - 2 \cdot 112) \\ &= 33 \cdot 241 - 71 \cdot 112 \end{aligned}$$

So $x = -71, y = 33$ is a solution to $112x + 241y = 1$.

1.7 Material from Chapters 1 and 2 to add to this section

that y'all requested... will be updated...

- identity mapping
- bijective, inverse mapping
- mathematical induction
- equivalence relations, equivalence classes, partitions
- examples of equivalence relations, equivalence classes, partitions
- prime, relatively prime, composite, fundamental theorem of arithmetic

2 Binary operations

2.1 Definition

Definition. A **binary operation** $\circ$ on a set S is a function $S \times S \to S$ that assigns each pair $(a, b) \in S \times S$ to a unique element $a \circ b \in S$.

We will write $(S, \circ)$ to refer to a set S together with a binary operation $\circ$ on S.

When Judson says "assigns each pair... to a unique element" he is saying that the binary operation must be well-defined. He is *not* saying it must be one-to-one.

Non-example. In Python, the function `random.randint` takes an input of two integers a and b, and outputs a random integer x such that $a \leq x \leq b$. So you might run it several times and see:

```
>>> random.randint(1,10)
4
>>> random.randint(1,10)
9
>>> random.randint(1,10)
1
```

Even though this is a reasonable rule for taking two integers and outputting a new integer, it is not a binary operation on the integers, because there is not a *unique* output assigned to each pair of inputs. It is not a well-defined map.

Furthermore, this Python function won't work if the first integer is greater than the second:

```
>>> random.randint(10,1)
ValueError:...
```

This violates the requirement that a binary function needs to assign an output to *each* pair of inputs.

Definition. A binary operation $\circ$ on a set S is called **commutative** if $a \circ b = b \circ a$ for all $a, b \in S$.

Example. $(\mathbb{Z}, +)$ is a commutative binary operation.

Non-example. Subtraction is a binary operation on the integers, but $(\mathbb{Z}, -)$ is not commutative, since $5 - 3 \neq 3 - 5$.

2.2 Associativity

Definition. A binary operation $\circ$ on a set S is called **associative** if

$$a \circ (b \circ c) = (a \circ b) \circ c$$

for all a, b, and c in S.

Example. Many familiar binary operations are associative, such as addition and multiplication of real numbers, addition and multiplication of and complex numbers, addition and multiplication of integers modulo n for any n, and addition and multiplication of matrices.

Non-example. $(\mathbb{Z}, -)$ is not associative, since $(5 - 3) - 1 = 2 - 1 = 1$, while $5 - (3 - 1) = 5 - 2 = 3$.

2.3 Identity element

Definition. An **identity element** for $(S, \circ)$ is an element $e \in S$ satisfying:

$$e \circ a = a$$

and

$$a \circ e = a$$

for all a in S.

Example. The identity element of $(\mathbb{R}, +)$ is 0, since $0 + r = r = r + 0$ for all $r \in \mathbb{R}$.

Example. The identity element of $(\mathbb{R}, \cdot)$ is 1, since $1 \cdot r = r = r \cdot 1$ for all $r \in \mathbb{R}$.

Non-example. Not every binary operation has an identity element. For example, let $2\mathbb{Z}$ denote the set of even integers. Multiplication is a binary operation on $2\mathbb{Z}$, since the product of two even integers is always an even integer. But $(2\mathbb{Z}, \cdot)$ does not have an identity element since $1 \notin 2\mathbb{Z}$.

Non-example. Define the binary operation $*$ on $\mathbb{R}$ by $a*b = a+ab$. Then, for every $r \in \mathbb{R}$, $r*0 = r+r\cdot 0 = r$, but $0 * r = 0 + 0 \cdot r = 0$ for all r, so 0 is not the identity element of $(\mathbb{R}, *)$. This shows why you need to check *both* parts of the definition.

However, if the binary operation is commutative, then "checking one side" is enough to prove something is the identity—as long as you explicitly mention that you are using commutativity.

2.4 Inverses

Definition. An element $a \in S$ has an **inverse** in $(S, \circ)$ if there exists $b \in S$ such that

$$a \circ b = e$$

and

$$b \circ a = e,$$

where e is the identity of $(S, \circ)$.

Note that the definition of inverse makes no sense unless the binary operation in question has an identity.

Example. In $(\mathbb{R}, +)$, the inverse of 5 is -5, since $5 + (-5) = 0 = (-5) + 5$ and 0 is the identity of $(\mathbb{R}, +)$. In fact, every element of $(\mathbb{R}, +)$ has an inverse.

Example. In $(\mathbb{R}, \cdot)$, the inverse of 5 is 0.2, since $5 \cdot 0.2 = 1 = 0.2 \cdot 5$ and 1 is the identity of $(\mathbb{R}, \cdot)$. Every nonzero element of $(\mathbb{R}, \cdot)$ has an inverse, but 0 doesn't have an inverse.

Non-example. In $(\mathbb{Z}, \cdot)$, 5 doesn't have an inverse. (Remember that inverses must belong to the set in question!) The only elements of In $(\mathbb{Z}, \cdot)$ that have inverses are 1 and -1.

Again, if the binary operation is commutative, then it suffices to check only one of the equations—as long as you state that's what you're doing.

3 Groups

3.1 Definitions and examples

Definition. A **group** $(G, \circ)$ is a set G together with a binary operation $\circ : G \times G \to G$ that satisfies three properties:

1. The operation $\circ$ is associative.

$$(a \circ b) \circ c = a \circ (b \circ c) \;\; \forall\, a, b, c \in G$$

2. There is an identity element.

$$\exists\, e \in G \text{ such that } e \circ a = a \circ e = a \;\; \forall\, a \in G$$

3. Every element has an inverse.

$$\forall\, g \in G, \exists\, h \text{ such that } g \circ h = h \circ g = e$$

If the operation is commutative ($a \circ b = b \circ a \;\; \forall\, a, b \in G$), we call G an **abelian** group. Otherwise it is a nonabelian group.

Example. $(\mathbb{Z}_6, +_6)$, the set of congruence classes of integers modulo 6 ("integers mod 6" for short), under the operation of addition modulo 6, is an abelian group. Below is its operation table, or **Cayley table**.

$+_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

If you have a finite set of elements, you can use a Cayley table to determine whether it forms a group under the operation.

- In order to have a binary operation, every entry of the table must match one of the row/column headings.
- Existence of an identity = existence of an element whose row *and* column match the row and column headings.

  Example. The identity of $(\mathbb{Z}_6, +_6)$ is 0 because the "0 row" matches the header row, showing that $0 +_6 a = a \;\; \forall\, a \in \mathbb{Z}_6$, and the "0 column" matches the header column, showing that $a +_6 0 = a \;\; \forall\, a \in \mathbb{Z}_6$.

$+_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

- To find the inverse of an element, look at where the identity appears in that element's row *and* column.

Example. In $(\mathbb{Z}_6, +_6)$, to find the inverse of 2, look for the identity (in this case 0) in the "2 row" and then in the "2 column". We find that $2 +_6 4 = 0$ and $4 +_6 2 = 0$ and therefore 4 is the inverse of 2.

$+_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$+_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

- There isn't a quick visual way to check for associativity, but the Cayley table is a reference that can make it easier to do computations in group.
- If the group is abelian, its Cayley table will be symmetric along the diagonal:

$+_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Non-example. Let's look at the Cayley table for $(\mathbb{Z}_6, \cdot_6)$ now. We can see that $\cdot_6$ is a binary operation on this set, and that 1 functions as an identity element using the row/column trick.

$\cdot_6$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

However, not every element of the set has an inverse under $\cdot_6$. For instance, in the "2 row" we never see 1 (the identity) appear, so there is no $a \in \mathbb{Z}_6$ such that $2 \cdot_6 a = 1$. Therefore $(\mathbb{Z}_6, \cdot_6)$ is not a group.

3.2 Some general hints when proving/disproving something is a group.

1. Don't forget to check that the set is closed under the operation.
2. If you already know the operation is associative *in general*, it follows that it is associative on a particular set.

   You can state without proof that the following are associative:
   - Addition and multiplication of real and complex numbers (and therefore any subset).
   - Addition and multiplication of integers modulo n for any n.
   - Addition and multiplication of matrices.
   - We will prove next time that function composition is associative in general.
3. If you have already shown that an operation is commutative, then you only have to prove "one side" for identity and inverses.
   - $\exists\, e \in G$ such that $e \circ a = a \;\; \forall\, a \in G$
   - $\forall\, a \in G$, $\exists\, b \in G$ such that $a \circ b = e$
4. If G is finite, you can prove that an element a does or doesn't have an identity/inverse by explicitly checking $a \circ b$ and/or $b \circ a$ for every $b \in G$.

3.3 More Cayley table examples

- Suppose $G = \{a, b, c, d\}$ has a binary operation $\Box$ with the following Cayley table.

$\Box$	a	b	c	d
a	a	c	d	a
b	b	b	c	d
c	c	d	a	b
d	d	a	b	c

  Then $(G, \Box)$ does not have an identity element, so it is not a group.

- Suppose $G = \{a, b, c, d\}$ has a binary operation $\triangle$ with the following Cayley table.

$\triangle$	a	b	c	d
a	a	b	c	d
b	b	d	a	c
c	c	a	d	b
d	d	c	b	a

  Then $(G, \triangle)$ is an abelian group.

- Suppose $G = \{a, b, c, d\}$ has a binary operation $\heartsuit$ with the following Cayley table.

$\heartsuit$	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

  Then $(G, \heartsuit)$ is an abelian group. Notice that $(G, \heartsuit)$ and $(G, \triangle)$ are "fundamentally different" groups. In other words, not only are the Cayley tables different as drawn, there is no way we could ever "relabel" the elements of one group to obtain the other group. You can see this from the fact that $(G, \triangle)$ has two elements which are their own inverses, whereas $(G, \heartsuit)$ has four elements which are their own inverses. So, even if we changed the names of the elements, this fundamental difference could never be overcome. We will talk more about this idea when we learn about **isomorphisms**.

- Suppose $G = \{a, b, c, d\}$ has a binary operation $\diamondsuit$ with the following Cayley table.

$\diamondsuit$	a	b	c	d
a	a	b	c	d
b	b	a	c	d
c	c	b	a	d
d	d	d	b	c

  The element a is the identity of the operation $\diamondsuit$. This means that d has no inverse because there is no $x \in G$ satisfying $d \diamondsuit x = x \diamondsuit d = a$. Therefore $(G, \diamondsuit)$ is not a group.

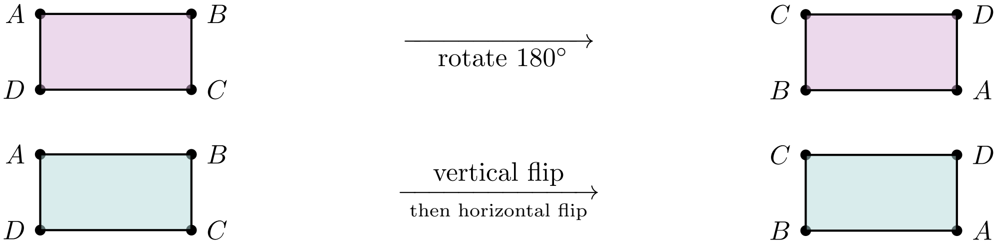
3.4 Symmetry groups and permutations

Definition. (Judson) A **symmetry** of a geometric figure is a rearrangement of the figure preserving the arrangement of its sides and vertices as well as its distances and angles.

Alternatively: A **transformation** in the plane is a function that maps points in the plane to other points in the plane. A transformation is also called a mapping or a function from the plane to itself. An **isometry** or **rigid motion** is a transformation that preserves angles and distances. A **symmetry** is a rigid motion of the plane that maps a figure to itself.

Definition. Two symmetries of a figure are said to be **equivalent** if they have the same effect on every point in the figure. Since symmetries are really functions of the plane, equivalence of symmetries is a special case of equivalence of functions.

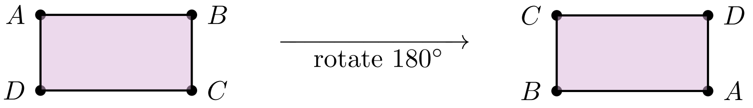
Example. Rotating a rectangle 180° is equivalent to a vertical reflection followed by a horizontal reflection.

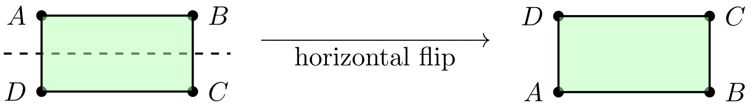


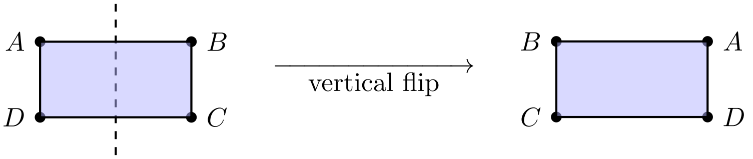
A **permutation** of a set S is a bijective map $\pi : S \to S$. To write this function in double-decker notation, the general form is:

$$\pi = \begin{pmatrix} x_1 & x_2 & \cdots & x_n \\ \pi(x_1) & \pi(x_2) & \cdots & \pi(x_n) \end{pmatrix}$$

Examples.

- 

$\begin{pmatrix} A & B & C & D \\ C & D & A & B \end{pmatrix}$
- 

$\begin{pmatrix} A & B & C & D \\ D & C & B & A \end{pmatrix}$
- 

$\begin{pmatrix} A & B & C & D \\ B & A & D & C \end{pmatrix}$

To **compose** permutations, remember that they are functions, so we compose from right to left.

Examples.

- $\begin{pmatrix} A & B & C & D \\ B & A & C & D \end{pmatrix} \circ \begin{pmatrix} A & B & C & D \\ A & C & D & B \end{pmatrix} = \begin{pmatrix} A & B & C & D \\ B & C & D & A \end{pmatrix}$
- $\begin{pmatrix} A & B & C & D \\ A & C & D & B \end{pmatrix} \circ \begin{pmatrix} A & B & C & D \\ B & A & C & D \end{pmatrix} = \begin{pmatrix} A & B & C & D \\ C & A & D & B \end{pmatrix}$

Proposition. The symmetries of a rectangle form a group under the binary operation of composition.

Proof. Let's use the following notation: I = identity, V = vertical flip, H = horizontal flip, R_{180} = rotate

180°. Then the Cayley table for the symmetries of a rectangle is:

$\circ$	I	V	H	R_{180}
I	I	V	H	R_{180}
V	V	I	R_{180}	H
H	H	R_{180}	I	V
R_{180}	R_{180}	H	V	I

The only group property we can't check by looking at the table is **associativity**. We will take care of this by proving in the next theorem that function composition is associative in general (therefore associative in this case). □

Theorem. Let $f : A \to B$, $g : B \to C$, and $h : C \to D$. Then $h \circ (g \circ f) = (h \circ g) \circ f$.

Proof. Remember that two functions are equal if they agree on every element in the domain. Let $a \in A$. Then

$$\begin{aligned}(h \circ (g \circ f))(a) &= h((g \circ f)(a)) \\ &= h(g(f(a))) \\ &= (h \circ g)(f(a)) \\ &= ((h \circ g) \circ f)(a).\end{aligned}$$

Therefore $h \circ (g \circ f) = (h \circ g) \circ f$. □

3.5 Uniqueness of identity and inverses in groups

Theorem. Let $(G, *)$ be a group. Then G has a unique identity element.

Proof. Since $(G, *)$ is a group, we know it has at least one identity. Now suppose a and b are both identity elements of the group $(G, *)$. Then by definition,

1. $a * x = x * a = x$ for all $x \in G$, and

2. $b * x = x * b = x$ for all $x \in G$.

Therefore $a * b = b$, by **1.**, and $a * b = a$, by **2.** Since $*$ is a binary operation, $a = a * b = b$ so the identity is unique. □

Theorem. Let $(G, *)$ be a group. For every $x \in G$, x has a unique inverse in G.

Proof. Suppose $(G, *)$ is a group with identity element e, and let $x \in G$. Since G is a group, we know x has at least one inverse. Now suppose y and z are both inverses of x. Then by definition,

1. $x * y = y * x = e$, and

2. $x * z = z * x = e$.

Therefore $x * y = x * z$. Multiply both sides of this equation on the left by y to obtain $y * (x * y) = y * (x * z)$. By associativity, $(y * x) * y = (y * x) * z$. And since $y * x = e$, this becomes $e * y = e * z$. From the definition of identity element, $e * a = a$ for all $a \in G$. Therefore $y = e * y = e * z = z$.

Therefore x has a unique inverse for all $x \in G$. □

3.6 Examples of checking group axioms

Example. Let $G = \{a + b\sqrt{2} : a, b \in \mathbb{Q}$ and a, b are not both $0\}$. Is G a group under multiplication?

Proof. First, let's check that multiplication is a binary operation on G. Let $a + b\sqrt{2}$ and $c + d\sqrt{2}$ be two arbitrary elements of G. Then

$$(a + b\sqrt{2})(c + d\sqrt{2}) = ac + ad\sqrt{2} + bc\sqrt{2} + 2bd = (ac + 2bd) + (ad + bc)\sqrt{2}.$$

Now $ac + 2bd$ and $ad + bc$ are both rational numbers. And since neither $a + b\sqrt{2}$ nor $c + d\sqrt{2}$ is zero, their product is not zero. Thus G is closed under multiplication.

Next, we need to know if the operation is associative. Since every element of G is a real number, and multiplication of real numbers is associative, we can see that multiplication in G is associative.

Now let's check for an identity. We know that 1 is the identity for multiplication of real numbers, so it should be an identity here, but we need to check whether 1 is an element of G. Since we can write $1 = 1 + 0\sqrt{2}$, and $1, 0 \in \mathbb{Q}$, then $1 \in G$ and satisfies $1 \cdot (a + b\sqrt{2}) = (a + b\sqrt{2}) \cdot 1 = a + b\sqrt{2}$ for all $a + b\sqrt{2} \in G$.

Finally, we need to show that every element of G has an inverse under multiplication. Let $a + b\sqrt{2} \in G$ be an arbitrary element. Since $a + b\sqrt{2}$ is a nonzero real number we know that the real number $\dfrac{1}{a + b\sqrt{2}}$ is its multiplicative inverse, but the question is whether or not this number can be written in the form $c + d\sqrt{2}$ where $c, d \in \mathbb{Q}$. To do this, rationalize the denominator:

$$\frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{(a + b\sqrt{2})(a - b\sqrt{2})} = \frac{a - b\sqrt{2}}{a - 2b^2}.$$

So the rational numbers

$$c = \frac{a}{a - 2b^2} \qquad \text{and} \qquad d = \frac{-b}{a - 2b^2}$$

will work. So every element of G has a multiplicative inverse *that belongs to* G. Therefore G is a group. □

Example. Let $X = \mathbb{R}\backslash\{1\}$, and define the operation $*$ by $a * b = a + b - ab$. Is $(X, *)$ a group?

Proof. To check closure under the operation: let $a, b \in X$. Then $a * b = a + b - ab$ is a real number. We need to show that it's not equal to 1 in order to show the operation is a binary operation on X.

Suppose that $a + b - ab = 1$. If $a = 0$, then $b = 1$ is the only solution, so suppose $a \neq 0$. Then $1 + b/a - b = 1/a$, which implies $1 - b = (1 - b) \wedge a$, which implies $a = 1$. Therefore $(a \neq 1) \wedge (b \neq 1) \implies (a + b - ab \neq 1)$. So X is closed under $*$.

Associativity: let $a, b, c \in X$. Then

$$\begin{aligned} a * (b * c) &= a * (b + c - bc) \\ &= a + (b + c - bc) - a(b + c - bc) \\ &= a + b + c - bc - ab - ac + abc. \end{aligned}$$

On the other hand,

$$\begin{aligned}(a * b) * c &= (a + b - ab) * c \\ &= (a + b - ab) + c - (a + b - ab)c \\ &= a + b + c - ab - ac - bc + abc.\end{aligned}$$

Therefore $a * (b * c) = (a * b) * c$.

Now let's try to find an identity element. Notice that this operation is commutative, because

$$a * b = a + b - ab = b + a - ba = b * a$$

for all $a, b \in X$. So we only need to check one direction in the definition of identity. We want to find an element $e \in X$ such that $a * e = a$ for all $a \in X$. We need e to satisfy $a = a * e = a + e - ae$, which implies $0 = e - ae$, which implies $ae = e$. Since $a \neq 1$, this implies $e = 0$. So $e = 0$ is the identity element since it satisfies (double-checking)

$$a * 0 = a + 0 - a0 = a$$

for all $a \in X$.

Since 0 is the identity, we can now try to show that every element of X has an inverse. Let $a \in X$. We want to find an element a^{-1} such that $a * a^{-1} = 0$. Again, we only need to check one direction because $*$ is commutative. We need $0 = a * a^{-1} = a + a^{-1} - aa^{-1}$. If $a = 0$, then $a^{-1} = 0$ since the identity is always its own inverse. So suppose $a \neq 0$. Then $a^{-1} \neq 0$, so $0 = a/a^{-1} + 1 - a$, which implies $a - 1 = a/a^{-1}$, which implies $a^{-1} = a/(a - 1)$. Since $a \neq 1$, $a^{-1} \in X$. So every $a \in X$ has an inverse element in the set X. □

3.7 Multiplicative vs. additive notation in groups

	multiplicative (most groups)	additive (e.g., $\mathbb{Z}$ and $\mathbb{Z}_n$)
operation	$a \cdot b$ or ab	$a + b$
identity	id or e or 1	id or 0
inverse of a	a^{-1}	$-a$
	powers of a: $a^n = \underbrace{a \cdot a \cdot \cdots \cdot a}_{n}$ $a^{-n} = \underbrace{a^{-1} \cdot a^{-1} \cdot \cdots \cdot a^{-1}}_{n}$ $a^0 = id$	multiples of a $na = \underbrace{a + a + \cdots + a}_{n}$ $-na = \underbrace{(-a) + (-a) + \cdots + (-a)}_{n}$ $0a = id$
	"quotient", $a \cdot b^{-1}$	"difference", $a + (-b)$

3.8 Rules of exponents in groups

Proposition. Let G be a group. Then $(ab)^{-1} = b^{-1}a^{-1}$.

Proof. Let e denote the identity of G. Then

$$(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = a(e)a^{-1} = (ae)a^{-1} = aa^{-1} = e,$$

and

$$(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b = b^{-1}(e)b = (b^{-1}e)b = b^{-1}b = e.$$

So by definition $b^{-1}a^{-1}$ is the inverse of ab. □

Example. In D_3, $(sr)^{-1} = r^{-1}s^{-1} = r^2 s = sr$. Notice that $(sr)^{-1} \neq s^{-1}r^{-1} = sr^2$.

Note: Some people call Proposition 13 the "socks and shoes rule". To get dressed you put your socks on first, then your shoes. To do the inverse, you have to go in reverse order: shoes off first, then socks off.

Theorem. Let G be a group. Then the following familiar laws of exponents hold for all $g, h \in G$, and for all $m, n \in \mathbb{Z}$:

1. $g^m g^n = g^{m+n}$,

2. $(g^m)^n = g^{mn}$,

3. $(gh)^n = (h^{-1}g^{-1})^{-n}$.

If G is abelian, then the following also holds:

4. $(gh)^n = g^n h^n$.

Note: This theorem is stated using multiplicative notation. The same statements hold for groups written with additive notation, but you have to "translate" them. For example, the first statement becomes $mg+ng = (m+n)g$.

3.9 The Sudoku rule

Informally, the "Sudoku rule" says that in a finite group, every element of the group appears exactly once per column, and exactly once per row, in the Cayley table.

Visually, this means that the following situations cannot happen:

	$\cdots$	a	b	$\cdots$
$\vdots$				
c		x	x	
$\vdots$				

	$\cdots$	c	$\cdots$
$\vdots$			
a		x	
b		x	
$\vdots$			

This helps us come up with a formal statement of the Sudoku rule:

1. For all $a, b, c \in G$, if $a \neq b$ then $ca \neq cb$.

2. For all $a, b, c \in G$, if $a \neq b$ then $ac \neq bc$.

Notice that the conditions above guarantee there are no repeats in any row or column of the table. They do not guarantee that each element actually appears once per column and once per row. So we have two more conditions to add:

3. For all $x \in G$, and for all $a \in G$, there exists $b \in G$ such that $ab = x$.

4. For all $x \in G$, and for all $a \in G$, there exists $b \in G$ such that $ba = x$.

Notice that condition **3** can be interpreted as: if x is an element of G, then x must appear somewhere in the "a row" for every $a \in G$. Similarly condition **4** says that x must appear somewhere in the "a column" for every $a \in G$.

I will leave it to you to prove the four pieces of the Sudoku rule follow from the group axioms.

3.10 Groups to know by name

From now on, we will refer to the following groups without explicitly saying the operation, because in each case there is only one familiar operation that makes the set a group.

- $\mathbb{Z}$, integers under addition
- $\mathbb{Z}_n$, integers mod n under addition mod n
- $U(n)$, invertible elements of the integers mod n under multiplication mod n
- $\mathbb{Q}$, rational numbers under addition
- $\mathbb{Q}^*$, nonzero rationals under multiplication
- $\mathbb{R}$, real numbers under addition
- $\mathbb{R}^*$, nonzero reals under multiplication
- $\mathbb{C}$, complex numbers under addition
- $\mathbb{C}^*$, nonzero complex numbers under multiplication
- D_3, symmetries of an equilateral triangle under composition
- D_4, symmetries of a square under composition

4 Subgroups

4.1 Order of a group, order of an element

Definition. Let G be a group. The **order of** G, written $|G|$, is the number of elements in G.

- If G has finitely many elements (i.e., $|G| < \infty$), then G is a **finite group**.
- Otherwise we say G is an infinite group. Sometimes we abuse notation and write $|G| = \infty$.

Examples. $|D_3| = 6$. $|\mathbb{Z}| = \infty$. $|\mathbb{Z}_5| = 5$ and in general, $|\mathbb{Z}_n| = n$.

Definition. Let G be a group with identity e. For $a \in G$, the **order of** a is the smallest positive integer n such that $a^n = e$. We write $|a| = n$.

If there is no n so that $a^n = e$, then we say a has infinite order. Sometimes we abuse notation and write $|a| = \infty$.

Examples. In D_3, $|r| = 3$, $|s| = 2$, and $|1| = 1$. In $\mathbb{Z}_5$, $|0| = 1$, $|1| = 5$, and $|2| = 5$. In $\mathbb{Z}$, $|0| = 1$, $|1| = \infty$ and $|2| = \infty$.

It may seem strange that we use the same word, and the same notation, for these two different definitions. However, there is a connection via subgroups that we will see soon.

4.2 Subgroup definition and examples

Definition. Let $(G, \circ)$ be a group and let H be a subset of G. We say that H is a **subgroup** of G if $(H, \circ)$ is a group.

Examples.

- $\mathbb{Z}$ is a subgroup of $\mathbb{Q}$
- $3\mathbb{Z}$ is a subgroup of $\mathbb{Z}$
- $\{1, r, r^2\}$ and $\{1, s\}$ are subgroups of D_3
- $\{1, i, -1, -i\}$ is a subgroup of $\mathbb{C}^*$

Non-examples.

- Even though $\mathbb{R}^* = \mathbb{R}\backslash\{0\}$ is a sub*set* of $\mathbb{R}$, the group $\mathbb{R}^*$ is not a sub*group* of $\mathbb{R}$, because the operation in $\mathbb{R}$ is addition and $\mathbb{R}^*$ is not a group under addition.
- Similarly, $\mathbb{Z}_6$ is not a subgroup of $\mathbb{Z}$ because addition mod 6 is not the same operation as addition in $\mathbb{Z}$. To convince yourself of this, consider that $1 + 5 = 0$ is true in $\mathbb{Z}_6$ but not true in $\mathbb{Z}$, so these operations can't be the same.
- $\{1, r, s\}$ is not a subgroup of D_3 because it isn't a group under composition. For instance, it is not closed under the operation.

Proposition. Three-Step Subgroup Test. A subset H of a group G is a subgroup of G if and only if:

1. The identity of G belongs to H. (In symbols, $e_G \in H$.)

2. H is closed under the operation of G. (If $a, b \in H$, then $ab \in H$.)

3. H is closed under inverses. (If $a \in H$, then $a^{-1} \in H$.)

Proof. See Judson Section 3.3. □

Proposition. One-Step Subgroup Test. A subset H of a group G is a subgroup of G if and only if H is non-empty and:

1. If $a, b \in H$, then $ab^{-1} \in H$.

Note: Besides the "one step," there is a very important additional assumption to check here, namely that H is non-empty.

Proof. See Judson Section 3.3. □

5 Cyclic subgroups and cyclic groups

Theorem. Let G be a group, and let $a \in G$. The set $\langle a \rangle = \{a^k : k \in \mathbb{Z}\}$ is a subgroup of G.

Proof. We will use the 3-step subgroup test. First, since $0 \in \mathbb{Z}$, $a^0 \in \langle a \rangle$, and $a^0 = e$ where e is the identity element of G. Therefore $\langle a \rangle$ contains the identity.

Second, we want to show that $\langle a \rangle$ is closed under the operation of G. Suppose $x, y \in G$. Then there exist $j, k \in \mathbb{Z}$ so that $x = a^j$ and $y = a^k$. Now $xy = a^j a^k = a^{j+k}$, and since $j + k \in \langle a \rangle$, this shows $xy \in \langle a \rangle$.

Third, we want to show that $\langle a \rangle$ is closed under inverses. Suppose $x = a^j \in \langle a \rangle$. Since G is a group, x has an inverse $x^{-1} = (a^j)^{-1} = a^{-j}$ in G. We need to check that the inverse belongs to $\langle a \rangle$. But since j was an integer, $-j$ is also an integer, so $x^{-1} = a^{-j} \in \langle a \rangle$. □

This theorem justifies the following definition:

Definition. Let G be a group, and let $a \in G$. We call

$$\langle a \rangle = \{a^k : k \in \mathbb{Z}\}$$

the **cyclic subgroup generated by** a and sometimes simply the **subgroup generated by** a.

If G is a group written with additive notation, then $\langle a \rangle = \{ka : k \in \mathbb{Z}\}$.

Examples.

- In $\mathbb{Z}_8$,
  - $\langle 2 \rangle = \{0, 2, 4, 6\}$
  - $\langle 4 \rangle = \{0, 4\}$
  - $\langle 6 \rangle = \{0, 3, 6, 1, 4, 7, 2, 5\} = \mathbb{Z}_8$
  - $\langle 0 \rangle = \{0\}$
- In D_3,
  - $\langle r \rangle = \{id, r, r^2\}$
  - $\langle s \rangle = \{id, s\}$
  - $\langle id \rangle = \{id\}$
- In $\mathbb{Q}^*$, $\left\langle \frac{1}{2} \right\rangle = \left\{ \left(\frac{1}{2}\right)^k : k \in \mathbb{Z} \right\} = \left\{ 1, \frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \frac{1}{16}, \cdots, 2, 4, 8, 16, \dots \right\}$

Definition. A group G is **cyclic** if there exists some $a \in G$ such that $G = \langle a \rangle$.

Example. $\mathbb{Z}_8$ is a cyclic group because $\mathbb{Z}_8 = \langle 3 \rangle$.

Notice cyclic generators are not unique. We also have $\mathbb{Z}_8 = \langle 1 \rangle$, $\mathbb{Z}_8 = \langle 5 \rangle$, and $\mathbb{Z}_8 = \langle 7 \rangle$.

Proposition.

1. For all $n \in \mathbb{N}$, $\mathbb{Z}_n$ is a cyclic group.

2. $\mathbb{Z}$ is a cyclic group.

Proof. In each of these groups, the element 1 is a generator. □

Theorem. Every cyclic group is abelian.

Proof. We did this proof in class. If you missed it, try it as an exercise. □

5.1 The $U(n)$ groups

Definition. An element $a \in \mathbb{Z}_n$ has a multiplicative inverse if there exists $b \in \mathbb{Z}_n$ such that $ab \equiv 1 \bmod n$. The elements of $\mathbb{Z}_n$ with multiplicative inverses are called the **units** (or **invertible elements**) of $\mathbb{Z}_n$.

Example. In $\mathbb{Z}_{10}$, 3 is a unit because $3 \cdot 7 \equiv 1 \bmod 10$. This also shows that 7 is a unit of $\mathbb{Z}_{10}$. On the other hand, 5 is not a unit of $\mathbb{Z}_{10}$ because there is no multiple of 5 congruent to 1 mod 10.

Proposition. For all $n \in \mathbb{N}$, the set

$$U(n) = \{a \in \mathbb{Z}_n : a \text{ is a unit}\}$$

is a group under multiplication mod n.

Example. $U(10) = \{1, 3, 7, 9\}$ is a group with Cayley table:

$\cdot_{10}$	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

Notice that $U(10)$ is cyclic because $3^0 = 1$, $3^1 = 3$, $3^2 = 9$, and $3^3 = 7$, so $U(10) = \langle 3 \rangle$.

Example. $U(8) = \{1, 3, 5, 7\}$ is a group with Cayley table:

$\cdot_8$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

$U(8)$ is not cyclic because $\langle 1 \rangle = \{1\}$, $\langle 3 \rangle = \{1, 3\}$, $\langle 5 \rangle = \{1, 5\}$, and $\langle 7 \rangle = \{1, 7\}$. So there is no element that generates the entire group.

Proposition. For each n, the elements of $U(n)$ are the integers $a \in \{0, 1, \ldots, n-1\}$ such that $\gcd(a, n) = 1$.

Proposition. For each n, the elements of $\mathbb{Z}_n$ that are cyclic generators of $\mathbb{Z}_n$ (under addition!) are also the elements $a \in \mathbb{Z}_n$ such that $\gcd(a, n) = 1$.

6 The symmetric group S_n

Recall that a *permutation* of a set X is a bijective map $\pi : X \to X$.

Definition. The set of all permutations of n elements forms a group under composition. We write this group as S_n and call it the **symmetric group** on n elements (or n letters).

For every n, $|S_n| = n!$. Any subgroup of S_n is called a **permutation group.**

6.1 Cycle notation for permutations

Previously we have used "double-decker notation" to describe permutations of a finite set. For example,

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 2 & 3 & 5 & 6 \end{pmatrix}$$

is the permutation that sends $1 \mapsto 1$, $2 \mapsto 4$, etc. Notice that the elements 1, 5, and 6 are fixed by the permutation τ. Meanwhile we have 2 maps to 4, 4 maps to 3, and 3 maps to 2 in a single cycle. The motivation behind cycle notation is to condense this information by expressing τ as:

$$\tau = (243) \in S_6.$$

The notation (243) represents the cycle where each element is sent to the element immediately following it inside the parentheses, and the last element "wraps around" and is sent back to the start of the list. We include the $\in S_6$ part to indicate that τ is still a function of 6 elements, even though in this case only three of them are actually affected by τ.

As another example, consider the permutation

$$\rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 1 & 3 & 6 & 5 \end{pmatrix}$$

Here there are two separate cycles of elements under ρ: the cycle $1 \mapsto 2 \mapsto 4 \mapsto 3 \mapsto 1$ and the cycle $5 \mapsto 6 \mapsto 5$. In cycle notation, we write

$$\rho = (1243)(56) \in S_6.$$

We might leave out the $\in S_6$ part if it is clear from the context.

Notice that we could have written ρ in several different ways: (2431)(56), (4312)(65), (56)(1243), etc., are all mathematically equivalent to (1243)(56). We also could have written $\tau = (243)(1)(5)(6)$ or $\tau = (6)(5)(432)(1)$ etc., to indicate the fixed points which are like cycles of length one. To make our notation consistent, however, we will agree on some conventions so we have a canonical way to write permutations in cycle notation.

Definition. (Conventions for cycle notation)

- The identity permutation, which fixes every element in the set, is written ().
- Write every cycle with its smallest element first.

  For instance, write (1243) instead of (2431), and write (56) instead of (65).
- Write every product of cycles as a product of disjoint cycles.

  For instance, (165)(2743) is the same function as (15)(16)(2743)(17)(17), but the latter notation is not as nice because we see some elements multiple times, so it isn't clear from a glance where each element goes.
- Write the disjoint cycles in a product of disjoint cycles in order of their smallest elements.

  For instance, write (1243)(56) instead of (56)(1243), and write (165)(2743) instead of (2743)(165).

Let's talk a bit more about the last two conventions.

Definition. Two cycles $(a_1 a_2 \cdots a_j)$ and $(b_1 b_2 \cdots b_k)$ are called **disjoint** if

$$\{a_1, a_2, \ldots, a_j\} \cap \{b_1, b_2, \ldots, b_k\} = \emptyset.$$

Proposition. If $(a_1 a_2 \cdots a_j)$ and $(b_1 b_2 \cdots b_k)$ are disjoint cycles, then

$$(a_1 a_2 \cdots a_j)(b_1 b_2 \cdots b_k) = (b_1 b_2 \cdots b_k)(a_1 a_2 \cdots a_j).$$

In words, disjoint cycles commute with each other. This justifies our last convention for cycle notation, which says we can choose the order of the disjoint cycles in a product of disjoint cycles. Remember that in general composition of permutations is not commutative, so your cycles *must* be disjoint to change the order of composition!

Proposition. Every permutation of S_n can be written as a product of disjoint cycles.

There is a proof of this proposition in Judson, but it is not very enlightening. In fact, it is really just a proof of the correctness of the method for composing cycles that we learned in class. Using this method, no matter how many cycles you are composing, you only ever write down each element once.

6.2 Transpositions, even and odd permutations

The simplest permutation is a cycle of length 2. Such a cycle is called a **transposition**. There is a straightforward way to write any longer cycle as a product of transpositions: In general,

$$(a_1 a_2 \ldots a_n) = (a_1 a_n)(a_1 a_{n-1}) \cdots (a_1 a_3)(a_1 a_2).$$

For example, (132765) = (15)(16)(17)(12)(13).

In this way, any cycle can be written as the product of transpositions, leading to the following proposition.

Proposition. Any permutation of S_n, for $n \geq 2$, can be written as the product of transpositions.

Notice that when we wrote (132765) as a product of transpositions, it was a product of an *odd* number (five) of transpositions. A permutation can be written as a product of transpositions in more than one way, for instance it's also true that

$$(132765) = (15)(16)(17)(12)(13)(35)(35).$$

However, whether or not the product has an even or odd number of transpositions is unique for each permutation. This leads to the following definition.

Definition. A permutation is called **even** if it can be expressed as an even number of transpositions, and called **odd** if it can be expressed as an odd number of transpositions.

Note: The identity permutation can be expressed $() = (12)(21)$ so the identity is even.

6.3 Cycle notation practice

We did some more examples with a worksheet called "cycle notation practice," which you can find on Canvas. Here are the answers to that worksheet.

1. Write the following permutations in cycle notation.

a. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 1 & 5 & 3 \end{pmatrix}$ Solution: (12453)

b. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 5 & 1 & 3 \end{pmatrix}$ Solution: (14)(35)

c. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 1 & 4 & 2 \end{pmatrix}$ Solution: (13)(25)

d. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 2 & 5 \end{pmatrix}$ Solution: (24)

2. Compute each of the following.

e. $(1254)^{-1}$ Solution: (1452)

f. $(13)^3(25)^2$ Solution: (13)

g. $(1254)^2$ Solution: (15)(24)

h. $(1254)^2(123)(45)$ Solution: $(1452)^2(123)(45) = (15)(24)(123)(45) = (14)(235)$

i. $((123)(45))^{10}$ Solution: Since (123) and (45) are disjoint, $((123)(45))^{10} = (123)^{10}(45)^{10}$.

And since (123) has order 3 and (45) has order 2, $(123)^{10}(45)^{10} = (123)$.

j. $(1254)^{100}$ Solution: Since $(1254)^4 = ()$, we have $(1254)^{100} = \left((1254)^4\right)^{25} = ()^{25} = ()$.

k. $|(1254)|$ Solution: 4

l. $|(1254)^2|$ Solution: 2

m. $|(123)(45)|$ Solution: 6

3. Express the following permutations as products of transpositions and identify them as even or odd.

a. (14356) Solution: $(14356) = (16)(15)(13)(14)$, even

b. $(156)(234)$ Solution: $(156)(234) = (16)(15)(24)(23)$, even

c. $(1426)(142)$ Solution: $(1426)(142) = (16)(12)(14)(12)(14)$, odd

d. $(17254)(1423)(154632)$ Solution: $(14)(15)(12)(17)(13)(12)(14)(12)(13)(16)(14)(15)$, even

e. (142637) Solution: $(142637) = (17)(13)(16)(12)(14)$, odd

6.4 The alternating group A_n

Definition. The **alternating group** A_n is the subset of S_n containing all the even permutations of S_n.

Example. $A_3 = \{(), (123), (132)\}$.

Theorem. (Thm 5.16 and Prop 5.17 in Judson) The set A_n is a subgroup of S_n, with $|A_n| = \dfrac{n!}{2}$.

7 Cosets

7.1 Definitions and examples

Definition. Let G be a group and H a subgroup of G. The **left coset of** H **containing** a is

$$aH = \{ah : h \in H\}.$$

Another name for aH is the **left coset of** H **with representative** a.) The **right coset of** H **containing** a is

$$Ha = \{ha : h \in H\}.$$

Another name for Ha is the **right coset of** H **with representative** a.

Examples.

- Let $G = S_3$, $H = \{(), (23)\}$.
  There are three distinct left cosets of H in G:

$$()H = (23)H = \{(), (23)\}$$

$$(12)H = (123)H = \{(12), (123)\}$$

$$(13)H = (132)H = \{(13), (132)\}$$

Notice that these left cosets partition the six elements of S_3 into three subsets with two elements each.

There are also three distinct right cosets of H in G:

$$H() = H(23) = \{(), (23)\}$$
$$H(12) = H(132) = \{(12), (132)\}$$
$$H(13) = H(123) = \{(13), (123)\}$$

The right cosets also partition S_3 into three sets of two elements each. But notice that we get a *different partition.* For instance, the elements (12) and (132) are in the same right coset of H, but they belong to two different left cosets of H.

- Let $G = \mathbb{Z}_{12}$, $H = \langle 8 \rangle$.

  Remember that $\langle 8 \rangle = \{0, 4, 8\} \leq G$. Since G is a group written with additive notation, we will use additive notation for the cosets, too. In this example I will write each left coset with only one representative:

$$0 + H = \{0, 4, 8\}$$
$$1 + H = \{1, 5, 9\}$$
$$2 + H = \{2, 6, 10\}$$
$$3 + H = \{3, 7, 11\}$$

  However it is important to understand that $7 + H$ is the same coset as $3 + H$, and $10 + H$ is the same as $2 + H$, etc.

  What about the right cosets of $\langle 8 \rangle$ in $\mathbb{Z}_{12}$? We get the same four:

$$H + 0 = \{0, 4, 8\}$$
$$H + 1 = \{1, 5, 9\}$$
$$H + 2 = \{2, 6, 10\}$$
$$H + 3 = \{3, 7, 11\}$$

  And in fact, this always happens when the group G is abelian, as the next proposition shows.

Proposition. Suppose G is an abelian group, and $H \leq G$. Then the left cosets and the right cosets of H are the same; that is, $aH = Ha$ for all $a \in G$.

Proof. Suppose G is abelian, $H \leq G$, and let $a \in G$. Then

$$\begin{aligned} aH &= \{ah : h \in H\} \\ &= \{ha : h \in H\} \text{ (since } G \text{ is abelian)} \\ &= Ha. \end{aligned}$$

□

Definition. Let G be a group and H a subgroup of G. The **index of H in G**, written $[G : H]$, is the number of left cosets of H in G.

Examples.

- $[S_3 : \{(), (23)\}] = 3$
- $[S_3 : A_3] = 2$
- $[\mathbb{Z}_{12} : \langle 8 \rangle] = 4$
- $[\mathbb{Z}_{12} : \langle 6 \rangle] = 6.$

7.2 Properties of cosets

Theorem. (The Coset Theorem) Let G be a group, H a subgroup of G, and $a, b \in G$. Then

1. $a \in aH$

2. $aH = H$ if and only if $a \in H$

3. $aH = bH$ or $aH \cap bH = \emptyset$

4. $aH = bH$ if and only if $a^{-1}b \in H$

5. $|aH| = |bH|$

Proof. **1.** Since H is a subgroup, the identity element of G, let's call it e, belongs to H. Therefore

$$a = ae \in \{ah : h \in H\} = aH.$$

2. First, suppose $aH = H$. By statement 1, $a \in aH$ and therefore $a \in H$.

On the other hand, suppose $a \in H$. To show $aH = H$ we have to show containment in both directions. First, let $b \in aH$. Then $b = ak$ for some $k \in H$. Since $a \in H$ and $k \in H$, and H is closed under the operation since it's a subgroup, this shows $b \in H$. Therefore $aH \subseteq H$. Next, let $b \in H$. We can write $b = (aa^{-1})b = a(a^{-1}b)$. Since $a \in H$ and H is a subgroup, $a^{-1} \in H$. And since $b \in H$ and H is closed under the operation, $a^{-1}b$ is equal to some element $k \in H$. Therefore $b = a(a^{-1}b) = ak \in \{ah : h \in H\} = aH$. Therefore $H \subseteq aH$. Since we have containment in both directions, $aH = H$.

3. We will show that if $aH \cap bH \neq \emptyset$, then $aH = bH$ must be true.

Suppose $aH \cap bH \neq \emptyset$. Then there exists some $x \in G$ such that $x \in aH \cap bH$. This means that $x = ah_1$ for some $h_1 \in H$, and also that $x = bh_2$ for some $h_2 \in H$. Therefore

$$ah_1 = bh_2, \quad h_1, h_2 \in H. \tag{1}$$

Now we will show containment both ways. Let $y \in aH$, so that $y = ak$ for some $k \in H$. By Equation 1, $a = bh_2h_1^{-1}$ so we can rewrite $y = ak = bh_2h_1^{-1}k$. Since h_2, h_1^{-1}, and k are all elements of H, y is equal to b times an element of H so $y \in bH$. Therefore $aH \subseteq bH$.

On the other hand let $y \in bH$, so that $y = bk'$ for $k' \in H$. Now we'll use Equation 1 to write $b = ah_1h_2^{-1}$ and substitute $y = bk' = ah_1h_2^{-1}k'$. Since $h_1h_2^{-1}k'$ is the product of three elements of H, it is an element of H, so $y \in aH$. Therefore $bH \subseteq aH$ and we have shown $aH = bH$.

4. This is a homework problem. Fun fact: more than once when I've taught 4170, this was an exam problem.

5. To show that the cosets aH and bH have the same cardinality, we will define a function $\phi : aH \to bH$ and prove that ϕ is a bijection. Let $\phi : aH \to bH$ be defined by $\phi(ah) = (bh)$ for all $ah \in aH$.

To show ϕ is one-to-one: Suppose that $\phi(ah_1) = \phi(ah_2)$. Then by the function's definition $bh_1 = bh_2$. Since b, h_1, h_2 are elements of a group G, we can use the cancellation law of groups to see $h_1 = h_2$. Therefore $ah_1 = ah_2$ so ϕ is one-to-one.

To show ϕ is onto: Let $y \in bH$. Then by definition there exists $h \in H$ such that $y = bh$. If we let $x = ah$, then $x \in aH$ by definition, and $\phi(x) = \phi(ah) = bh = y$. Therefore for every $y \in bH$, there exists $x \in aH$ such that $\phi(x) = y$, so ϕ is onto.

□

7.3 Lagrange's Theorem

Theorem. (Lagrange's Theorem.) If G is a finite group and H is a subgroup of G, then $[G : H] = |G|/|H|$. Hence $|H|$ divides $|G|$.

Proof. Suppose G is a finite group and $H \leq G$. By definition there are $[G : H]$ distinct left cosets of H in G, one of which is H itself. By Theorem 7.2 part 5, $|aH| = |H|$ for every left coset aH. Since the cosets partition G into $[G : H]$ sets, each of which has $|H|$ elements, $|G| = [G : H] \cdot |H|$. □

Corollary. If G is a finite group and $a \in G$, then $|a|$ divides $|G|$.

Proof. Suppose G is a finite group and $a \in G$. Consider $\langle a \rangle$, the cyclic subgroup generated by a. Since G is finite, $|a|$ is finite, say $|a| = n$. Then $\langle a \rangle$ has exactly n elements:

$$\langle a \rangle = \{a^0 = e, a^1, a^2, a^3, \dots, a^{n-1}\},$$

so by Lagrange's Theorem $|\langle a \rangle| = n$ divides $|G|$.

□

8 Isomorphisms and homomorphisms

8.1 Definitions and examples

Definition. Two groups $(G, \cdot)$ and $(H, \circ)$ are **isomorphic** if there exists a bijection (one-to-one and onto function) $\phi : G \to H$ such that

$$\phi(a \cdot b) = \phi(a) \circ \phi(b) \text{ for all } a, b \in G. \tag{2}$$

We call ϕ an **isomorphism**. If G is isomorphic to H, we write $G \cong H$.

Note: Since we often omit symbols when we write group operations, we might have said: Two groups G and H are isomorphic if there exists a bijection $\phi : G \to H$ such that

$$\phi(ab) = \phi(a)\phi(b) \text{ for all } a, b, \in G.$$

This is correct, but be careful: On the left, ab denotes multiplication in G. On the right, $\phi(a)\phi(b)$ denotes multiplication in H. These are different operations! Using two different symbols, like in the boxed definition, can help you keep track of which operation is which.

Example: Let $\mathbb{R}_{>0}$ denote the positive real numbers. Then $(\mathbb{R}, +) \cong (\mathbb{R}_{>0}, \cdot)$.

Proof. Define the function $f : \mathbb{R} \to \mathbb{R}_{>0}$ by $f(x) = e^x$. Note that for any $x \in \mathbb{R}$, e^x is a positive real number, so this function is well-defined. First we will show that f satisfies Equation 2; in other words that f is operation-preserving.

Let $x_1, x_2 \in \mathbb{R}$. Then

$$f(x_1 + x_2) = e^{x_1 + x_2} = e^{x_1}e^{x_2} = f(x_1)f(x_2)$$

so f satisfies Equation 2. Notice that we are *adding* x_1 and x_2 on the left-hand side of this equation, and *multiplying* $f(x_1)$ and $f(x_2)$ on the right-hand side, to match the different operations of $\mathbb{R}$ and $\mathbb{R}_{>0}$.

To show that f is injective: suppose $f(a) = f(b)$ for some $a, b \in \mathbb{R}$. Then $e^a = e^b$. Taking the natural log of both sides, we get $\ln(e^a) = \ln(e^b) \quad \implies \quad a = b$.

To show that f is surjective: let $c \in \mathbb{R}_{>0}$ be arbitrary. Since $c > 0$, $\ln c$ exists and is a real number, and it satisfies $f(\ln c) = e^{\ln c} = c$.

Thus f is an isomorphism, and $(\mathbb{R}, +) \cong (\mathbb{R}_{>0}, \cdot)$. □

Example: Let $C_4 = \{1, i, -1, -i\}$ under complex multiplication. Then $C_4 \cong \mathbb{Z}_4$.

Proof. Let $g : C_4 \to \mathbb{Z}_4$ be given by $g(1) = 0$, $g(i) = 1$, $g(-1) = 2$, and $g(-i) = 3$. This is clearly a bijection between the two groups of order four. To check that Equation 2 is satisfied, we can check all sixteen products individually:

$$\begin{aligned} g(i \cdot -1) &= g(-i) = 3 = 1 + 2 = g(i) + g(-1) \\ g(1 \cdot -1) &= g(-1) = 2 = 0 + 2 = g(1) + g(-1) \\ &\textit{etc.} \end{aligned}$$

An easier way to organize this information is simply to show that the bijection $g : C_4 \to Z_4$ preserves all entries of the Cayley table.

$\cdot$	1	i	-1	$-i$
1	1	i	-1	$-i$
i	i	$-i$	1	-1
-1	-1	1	$-i$	i
$-i$	$-i$	-1	i	1

C_4

$$\xrightarrow{\quad g \quad}$$

$+_4$	0	1	2	3
0	0	1	2	3
1	1	3	0	2
2	2	0	3	1
3	3	2	1	0

$\mathbb{Z}_4$

The definition of g says where the heading rows and columns are mapped to. To check that g is operation-preserving, we check that within the table entries, every 1 is sent to a 0, every i sent to a 2, etc. Since this holds, we know all sixteen products are preserved as desired, and g is indeed an isomorphism.

Thus $C_4 \cong \mathbb{Z}_4$. □

8.2 Homomorphisms

This "operation-preserving" property of a function between groups is so important, we have a name for this kind of function, whether or not it is a bijection.

Definition. Let $(G, \cdot)$ and $(H, \circ)$ be groups. A function $\phi : G \to H$ is called a **homomorphism** if

$$\phi(a \cdot b) = \phi(a) \circ \phi(b) \text{ for all } a, b \in G.$$

Notice that a function is an isomorphism if and only if it is a homomorphism that is also a bijection. This means that isomorphisms are a special case of homomorphisms. Every isomorphism is a homomorphism.

Is every homomorphism of groups also an isomorphism? No. For example, consider $h : \mathbb{R} \to \mathbb{R}^*$ given by $h(x) = e^x$. Then h is a homomorphism, because it's still that case that

$$h(x_1 + x_2) = e^{x_1+x_2} = e^{x_1}e^{x_2} = h(x_1)h(x_2)$$

for all $x_1, x_2 \in \mathbb{R}$. But h is not surjective, since $h(x) > 0$ for all $x \in \mathbb{R}$. In particular, there is no $x \in \mathbb{R}$ such that $h(x) = -2$, even though $-2 \in \mathbb{R}^*$.

8.3 Solutions to Worksheet: Isomorphisms and Homomorphisms I

1. For each function ϕ, determine **(i)** if ϕ is a homomorphism, and **(ii)** if ϕ is an isomorphism.

a. $\phi : \mathbb{Z} \to \mathbb{Z}_6$, given by $\phi(n) = n \pmod 6$
Let $a, b \in \mathbb{Z}$. Then

$$\begin{aligned}\phi(a+b) &= (a+b) \pmod 6\\ &= a \pmod 6 +_6 b \pmod 6\\ &= \phi(a) +_6 \phi(b),\end{aligned}$$

So ϕ is a homomorphism. But ϕ is not an isomorphism because it is not one-to-one. For example, $6 \neq 12$, but $\phi(6) = \phi(12)$.

b. $\phi : \mathbb{Z} \to \mathbb{Z}$, given by $\phi(n) = n - 1$
Let $n, m \in \mathbb{Z}$. Then $\phi(n + m) = n + m - 1$, while $\phi(n) + \phi(m) = (n - 1) + (m - 1) = n + m - 2$. This is not a homomorphism because (citing a concrete example):

$$\phi(2 + 3) = 4 \neq 3 = \phi(2) + \phi(3).$$

Therefore it cannot be an isomorphism.

c. $\phi : \mathbb{R}^* \to \mathbb{R}^*$, given by $\phi(x) = 3x$
This is not a homomorphism, because

$$\phi(1 \cdot 2) = \phi(2) = 6 \neq 18 = (3 \cdot 1)(3 \cdot 2) = \phi(1)\phi(2).$$

Therefore it cannot be an isomorphism.

d. $\phi : \mathbb{Z}_{12} \to \mathbb{Z}_{12}$ given by $\phi(n) = -n$.
This is both a homomorphism and an isomorphism. In general to prove a function is bijective, the strategy is:

- Show one-to-one by assuming $\phi(x) = \phi(y)$, then showing that $x = y$.
- Show onto by letting $y \in H$ (or whatever the codomain is), and showing there exists an $x \in G$ (or whatever the domain is) satisfying $\phi(x) = y$.

In this case, because both groups are finite, we can show that ϕ is a bijection by drawing a diagram matching x with $\phi(x)$ for all x in the domain:

$$\begin{aligned}
0 &\longrightarrow 0\\
1 &\longrightarrow 11\\
2 &\longrightarrow 10\\
3 &\longrightarrow 9\\
4 &\longrightarrow 8\\
5 &\longrightarrow 7\\
6 &\longrightarrow 6\\
7 &\longrightarrow 5\\
8 &\longrightarrow 4\\
9 &\longrightarrow 3\\
10 &\longrightarrow 2\\
11 &\longrightarrow 1
\end{aligned}$$

Since no element in the codomain has more than one arrow pointing to it, the function is one-to-one. And since every element of the codomain has some arrow pointing to it, the function is onto.

e. $\phi : \mathbb{R}^* \to \mathbb{R}^*$ given by $\phi(x) = x^{-1}$

This is both a homomorphism and an isomorphism. Here we will use the standard strategy to prove the bijective part of the definition.

- One-to-one: suppose $\phi(x) = \phi(y)$. Then $x^{-1} = y^{-1}$. Taking the inverse of both sides, we get $x = y$.
- Onto: let $y \in \mathbb{R}^*$. Since $\mathbb{R}^*$ is a group, y^{-1} exists in $\mathbb{R}^*$, which is also the domain of ϕ, and $\phi(y^{-1}) = (y^{-1})^{-1} = y$.

f. $\phi : \mathbb{R}_{>0} \to \mathbb{R}_{>0}$ given by $\phi(x) = x^2$

This function is a homomorphism, because for all $x_1, x_2 \in \mathbb{R}_{>0}$, $\phi(x_1x_2) = (x_1x_2)^2 = (x_1)^2(x_2)^2 = \phi(x_1)\phi(x_2)$. It is an isomorphism (left as exercise).

g. $\phi : S_4 \to S_4$, given by $\phi(\sigma) = (14)\sigma$

Not a homomorphism (left as exercise).

h. $\phi : S_4 \to S_4$, given by $\phi(\sigma) = \sigma^2$

Not a homomorphism (left as exercise).

Something to think about: What is different between this function and the one in part **f**?

2. Show that if G and H are any groups, there is always at least one homomorphism $\phi : G \to H$.

The trivial homomorphism, $\phi(g) = e_H$ for all $g \in G$, is always a homomorphism.

3. Suppose $\phi : G \to H$ is a homomorphism. Prove that $\phi(e_G) = e_H$ (where e_G and e_H are the identities of G and H, respectively).

$$\begin{aligned}
e_H\phi(e_G) &= \phi(e_G) \text{ since } e_H \text{ is the identity of } H\\
&= \phi(e_Ge_G) \text{ since } e_G \text{ is the identity of } G\\
&= \phi(e_G)\phi(e_G) \text{ since } \phi \text{ is a homomorphism}
\end{aligned}$$

Since $e_H\phi(e_G) = \phi(e_G)\phi(e_G)$, by right cancellation in groups, $e_H = \phi(e_G)$.

4. True or false: if $\phi : G \to H$ is not an isomorphism, then $G \ncong H$.

False. Just because a particular function is not an isomorphism, doesn't mean there are no isomorphisms. For example, $\phi : \mathbb{Z} \to \mathbb{Z}$ defined by $\phi(x) = 0$ for all x is not an isomorphism, but $\mathbb{Z} \cong \mathbb{Z}$.

8.4 Solutions to Worksheet: Isomorphisms and Homomorphisms II

Theorem. (Judson 9.6). Suppose $\phi : G \to H$ is an isomorphism. Then:

1. $\phi^{-1} : H \to G$ is an isomorphism.

2. $|G| = |H|$.

3. If G is abelian, then H is abelian.

4. If G is cyclic, then H is cyclic.

5. If G has a subgroup of order n, then H has a subgroup of order n.

Theorem. (Additional properties of isomorphisms.) Suppose $\phi : G \to H$ is an isomorphism. Then:

6. $|a| = |\phi(a)|$ for all $a \in G$.

7. For any positive integer n, G and H have the same number of elements of order n.

8. For any positive integer n, G and H have the same number of subgroups of order n.

Proof. **1.** Since ϕ is an isomorphism, it is by definition a bijection, therefore ϕ^{-1} exists and is a bijection. Let $h_1, h_2 \in H$. Since ϕ is an isomorphism, there exist $g_1, g_2 \in G$ satisfying $\phi(g_1) = h_1$ and $\phi(g_2) = h_2$. We also know $\phi(g_1g_2) = \phi(g_1)\phi(g_2) = h_1h_2$. Therefore

$$\phi^{-1}(h_1h_2) = g_1g_2 = \phi^{-1}(h_1)\phi^{-1}(h_2)$$

so ϕ^{-1} is an isomorphism.

2. Since a bijection exists between G and H, the sets have the same cardinality.

3. Suppose G is abelian. Then $g_1g_2 = g_2g_1$ for all $g_1, g_2 \in G$. To prove that H is abelian, let $h_1, h_2 \in H$. Then since ϕ is a bijection, there exist $g_1, g_2 \in G$ such that $\phi(g_1) = h_1$ and $\phi(g_2) = h_2$. Then

$$h_1h_2 = \phi(g_1)\phi(g_2) = \phi(g_1g_2) = \phi(g_2g_1) = \phi(g_2)\phi(g_1) = h_2h_1$$

so H is abelian.

4. Suppose G is cyclic, so there exists $a \in G$ such that

$$G = \{a^k : k \in \mathbb{Z}\}.$$

Let $b = \phi(a)$. We will show that b is a cyclic generator of H; in other words, any $h \in H$ can be written as $h = b^k$ for some $k \in \mathbb{Z}$.

Let $h \in H$. Since ϕ is a bijection, there exists $g \in G$ such that $\phi(g) = h$. And since $G = \langle a \rangle$, we know $g = a^k$ for some $k \in \mathbb{Z}$. Therefore

$$h = \phi(g) = \phi(a^k) = \phi(a)^k = b^k.\text{*}$$

5. Let K be a subgroup of G with $|K| = n$. We will show that

$$\phi(K) := \{\phi(k) : k \in K\}$$

is a subgroup of H using the 3-step subgroup test.

*Prove the equality $\phi(a^k) = \phi(a)^k$ using induction and the homomorphism property.

First, note that $e_G \in K$ since K is a subgroup of G. By Problem 3 from the previous worksheet, $\phi(e_G) = e_H$ so $e_H \in \phi(K)$.

Second, suppose that $h_1, h_2 \in \phi(K)$. Then by definition of $\phi(K)$, there exist $k_1, k_2 \in K$ such that $\phi(k_1) = h_1$ and $\phi(k_2) = h_2$. Since K is a subgroup, it is closed under the operation, so $k_1k_2 \in K$. Now $h_1h_2 = \phi(k_1)\phi(k_2) = \phi(k_1k_2)$ (by homomorphism property) so $h_1h_2 \in \phi(K)$. Therefore $\phi(K)$ is closed under the operation of H.

Third, suppose that $h \in \phi(K)$. Then $h = \phi(k)$ for some $k \in K$. since K is a subgroup, the element $k^{-1} \in G$ belongs to K. We will show that $h^{-1} = \phi(k^{-1})$ by the following:

$$e_H = \phi(e_G) = \phi(kk^{-1}) = \phi(k)\phi(k^{-1}) = h\phi(k^{-1})$$

and

$$e_H = \phi(e_G) = \phi(k^{-1}k) = \phi(k^{-1})\phi(k) = \phi(k^{-1})h.$$

Therefore $h^{-1} = \phi(k^{-1}) \in \phi(K)$ so $\phi(K)$ is closed under inverses.

Hence $\phi(K)$ is a subgroup of H.

6. Suppose $|a| = n$, so that n is the smallest positive integer satisfying $a^n = e_G$. Then

$$\phi(a)^n = \phi(a^n) = \phi(e_G) = e_H.$$

Suppose toward a contradiction that $\phi(a)^m = e_H$ for some $0 < m < n$. Then

$$\phi(e_G) = e_H = \phi(a^m)$$

and since ϕ is one-to-one, this implies $e_G = a^m$, contradicting that n is the order of a. Thus $\phi(a)^m \neq e_H$ for any $0 < m < n$ so $|\phi(a)| = n$.

7. This follows immediately from Part **6.**

8. This follows immediately from Part **7.**

□

Ways to prove that two groups G and H are isomorphic:

- There is only one way: find a function $\phi : G \to H$ that you can prove is an isomorphism!
- The only "other way," which is really the same way, is to draw the Cayley tables of G and H, assuming they are finite and reasonably small, and find an explicit bijection between the elements of G and H. If the bijection correctly labels every inner entry of the Cayley table as well as its labels, this shows it satisfies the homomorphism property and therefore is a bijection.

Ways to prove that two groups G and H are *not* isomorphic:

- If $|G| \neq |H|$, then $G \ncong H$.
  - Example: $\mathbb{Z}_5 \ncong \mathbb{Z}_6$ because $|\mathbb{Z}_5| \neq |\mathbb{Z}_6|$.
- If one of G, H is abelian and the other is not, then $G \ncong H$.
  - Example: Even though they both have order 6, $S_3 \ncong \mathbb{Z}_6$ because $\mathbb{Z}_6$ is abelian and S_3 is not.
- If one of G, H is cyclic and the other is not, then $G \ncong H$.
  - Example: Even though they both have order 4 and are both abelian, $\mathbb{Z}_2 \times \mathbb{Z}_2 \ncong \mathbb{Z}_4$ because $\mathbb{Z}_4$ is abelian and $\mathbb{Z}_2 \times \mathbb{Z}_2$ is not.

- For any n, if G and H have different numbers of subgroups of order n, then $G \ncong H$.
  - Example: even though D_4 and Q_8 both have order 8, both are non-abelian, and both are non-cyclic, we know $Q_8 \ncong D_4$ because Q_8 has only one subgroup of order 2, and D_4 has 5 subgroups of order 2.
- For any n, if G and H have different numbers of elements of order n, then $G \ncong H$.
  - Example: even though $\mathbb{R}^*$ and $\mathbb{C}^*$ have the same cardinality, are both abelian, and both non-cyclic, we know $\mathbb{R}^* \ncong \mathbb{C}^*$ because $\mathbb{C}^*$ has two elements of order four (namely, i and $-i$), but $\mathbb{R}^*$ has zero elements of order four.

8.5 Solutions to Worksheet: Kernels and images of homomorphisms

Definitions

Let $\phi : G \to H$ be a homomorphism and let e_H denote the identity of H. The **kernel** of ϕ, written $\ker(\phi)$, is the set

$$\ker(\phi) = \{x \in G : \phi(x) = e_H\}.$$

Let $\phi : G \to H$ be a homomorphism and let K be a subgroup of G. The **image** of K, written $\phi(K)$ is the set

$$\phi(K) = \{\phi(k) : k \in K\}.$$

When we consider the image of G itself, we may write $\text{Im}(\phi)$ or $\phi(G)$ interchangeably.

Examples

1. Consider the homomorphism $\phi : \mathbb{Z} \to \mathbb{Z}$, where $\phi(n) = 7n$.

a. Find $\ker(\phi)$. Solution: $\ker(\phi) = \{0\}$

b. Find $\phi(\langle 3\rangle)$. Solution: $\phi(\langle 3\rangle) = \langle 21\rangle$

c. Find $\phi(\mathbb{Z})$. Solution: $\phi(Z) = \langle 7\rangle$

d. Is ϕ an isomorphism? Solution: No, it is not onto.

2. Consider the homomorphism $\phi : \mathbb{Z} \to \mathbb{Z}_6$, where $\phi(n) = n \pmod 6$.

a. Find $\ker(\phi)$. Solution: $\ker(\phi) = \langle 6\rangle \leq \mathbb{Z}$

b. Find $\phi(\langle 3\rangle)$. Solution: $\phi(\langle 3\rangle) = \{0, 3\} \leq \mathbb{Z}_6$

c. Find $\phi(\langle 5\rangle)$. Solution: $\phi(\langle 5\rangle) = \mathbb{Z}_6$

d. Is ϕ an isomorphism? Solution: No, it is not one-to-one.

3. Let $\phi : G \to H$ be a homomorphism, and let e_G, e_H denote the identity elements of G and H, respectively. Show that $\phi(e_G) = e_H$. That is, show that $e_G \in \ker(\phi)$.

Solution: Consider $e_H\phi(e_G) = \phi(e_G) = \phi(e_Ge_G) = \phi(e_G)\phi(e_G)$. By cancelling $\phi(e_G)$ from the right side of the first and last equalities, we obtain $e_H = \phi(e_G)$.

Important theorems.

- Suppose $\phi : G \to H$ is a homomorphism. Then $\ker(\phi)$ is a subgroup of G.

  Solution: Use 3-step subgroup test:

  1. Need to show $e_G \in \ker(\phi)$. This is just problem 3 above.

  2. Suppose $g \in \ker(\phi)$; we need to show $g^{-1} \in \ker(\phi)$.
  Since $g \in \ker(\phi)$, $\phi(g) = e_H$, so $\phi(g^{-1}) = \phi(g)^{-1} = e_H^{-1}$, so $g^{-1} \in \ker(\phi)$.

  3. Suppose $a, b \in \ker(\phi)$. Then

  $$\begin{aligned}\phi(ab) &= \phi(a)\phi(b) \text{ (since } \phi \text{ is a homom.)}\\ &= e_He_H \text{ (since } a, b \in \ker(\phi))\\ &= e_H\end{aligned}$$

  So $ab \in \ker(\phi)$ by definition.

  Therefore $\ker(\phi) \leq G$.

- Suppose $\phi : G \to H$ is a homomorphism. Then for any $K \leq G$, $\phi(K) \leq H$.

  Solution: Use 3-step subgroup test:

  1. Need to show $e_H \in \phi(K)$. Since K is a subgroup of G, $e_G \in K$. So $e_H = \phi(e_G) \in \phi(K)$.

  2. Suppose $h \in \phi(K)$; we need to show $h^{-1} \in \phi(K)$.
  Since $h \in \phi(K)$, there exists $a \in K$ such that $\phi(a) = h$. Since K is a subgroup, $a^{-1} \in K$, and therefore $\phi(a^{-1}) \in K$.
  Now $\phi(a^{-1}) = \phi(a)^{-1} = h^{-1}$, so $h^{-1} \in \phi(K)$.

  3. Suppose $c, d \in \phi(K)$. Then there exist $e, f \in K$ such that $\phi(e) = c$ and $\phi(f) = d$.
  Now $\phi(ef) = \phi(e)\phi(f) = cd$, so $cd \in \phi(K)$, showing that $\phi(K)$ is closed under the operation.

  Therefore $\phi(K) \leq H$.

- A homomorphism $\phi : G \to H$ is one-to-one if and only if $\ker(\phi) = \{e_G\}$.

  Solution: First, suppose ϕ is one-to-one. Suppose toward a contradiction that $\ker(\phi) = \{e_G, g\}$ with $g \neq e_G$; i.e. that there is more than element in $\ker(\phi)$. Then $\phi(e_G) = \phi(g) = e_H$ but $e_G \neq g$, contradiction that the function is one-to-one. So $\ker(\phi)$ cannot have more than one element. (And we've already proven that e_G is in the kernel.

  In the other direction, suppose $\ker(\phi) = \{e_G\}$. Suppose toward a contradiction that ϕ is not one-to-one, so there exist $g_1, g_2 \in G$ such that $g_1 \neq g_2$ but $\phi(g_1) = \phi(g_2)$.

  Now consider $\phi(g_1g_2^{-1}) = \phi(g_1)\phi(g_2^{-1}) = \phi(g_1)\phi(g_2)^{-1}$.

  Since $\phi(g_1) = \phi(g_2)$, $\phi(g_1)^{-1} = \phi(g_2)^{-1}$. So $\phi(g_1g_2^{-1}) = \phi(g_1)\phi(g_2)^{-1} = \phi(g_1)\phi(g_1)^{-1} = e_H$, showing that $g_1g_2^{-1} \in \ker(\phi)$. But $g_1 \neq g_2$, so $g_1g_2^{-1} \neq e_G$ by uniqueness of inverses, and this contradicts that $\ker(\phi) = \{e_G\}$ only. Thus ϕ must be one-to-one.

- A homomorphism $\phi : G \to H$ is onto if and only if $\phi(G) = H$.

  Solution: This is true basically by the definition of "onto": a function is onto if and only if the image of the function is equal to the entire codomain.

- Suppose $\phi : G \to H$ is a homomorphism. Then ϕ is an isomorphism if and only if Solution: $\ker(\phi) = \{e_G\}$ and $\phi(G) = H$.

9 Normal subgroups and quotient groups (a.k.a. factor groups)

Note: see the slides on this topic posted on Canvas—I have collected some of the important results from that here, and am still working on it, but there is more in the slides that isn't in this document yet.

We've talked a lot about left cosets and right cosets, and examples of when they agree—or don't.

From homework: $G = A_4$, $H = A_3 = \{(), (123), (132)\}$.

$$(12)(34)H = \{(12)(34), (143), (243)\}$$
$$H(12)(34) = \{(12)(34), (134), (234)\}$$

$$(12)(34)H \neq H(12)(34), \text{ so left cosets do not equal right cosets}$$

Also from homework: $G = Q_8$, $H = \{1, -1\}$.

$$(-1)H = 1H = \{1, -1\} = H1 = H(-1)$$
$$(-i)H = iH = \{i, -i\} = Hi = H(-i)$$
$$(-j)H = jH = \{j, -j\} = Hj = H(-j)$$
$$(-k)H = kH = \{k, -k\} = Hk = H(-k)$$

$$aH = Ha \text{ for all } a \in Q_8$$

9.1 Normal subgroups

Some subgroups have the property that $aH = Ha$ for all $a \in G$ and some subgroups don't. We call the ones that do have this property **normal**.

Definition. A subgroup H of a group G is called a **normal subgroup** of G if $aH = Ha$ for all $a \in G$. We write $H \trianglelefteq G$.

Warning!! $aH = Ha$ does **not** mean that $ah = ha$ for all $h \in H$.

Examples:

- $\{1, -1\} \trianglelefteq Q_8$

- $A_3 \ntrianglelefteq A_4$

We've already (secretly) seen a few conditions that guarantee a subgroup is normal!

From "Cosets and Lagrange's Theorem" worksheet: Suppose that H is a subgroup of G with $[G : H] = 2$. Show that $gH = Hg$ for all $g \in G$.

That was this in disguise:

Proposition. If $H \leq G$ and $[G : H] = 2$, then $H \trianglelefteq G$.

This gives plenty of examples of normal subgroups:

- $\{id, r, r^2, r^3\} \trianglelefteq D_4$
- $\{1, -1, i, -i\} \trianglelefteq Q_8$
- $A_n \trianglelefteq S_n$
- etc.

Here's another condition we saw.

Proposition. All subgroups of abelian groups are normal.

Proof. Suppose G is an abelian group and H is a subgroup of G. Then for any $a \in G$,

$$aH = \{ah : h \in H\} = \{ha : h \in H\} = Ha.$$

Therefore $H \trianglelefteq G$. □

Corollary. All subgroups of cyclic groups are normal.

9.2 Normal subgroup test

Proposition. (Normal subgroup test) $H \trianglelefteq G$ if and only if $gHg^{-1} \subseteq H$ for all $g \in G$.

Proof. This was a homework problem. □

Theorem. (Theorem 10.3 from Judson)
The following statements are equivalent:

1. $H \trianglelefteq G$

2. For all $g \in G$, $gHg^{-1} \subseteq H$

3. For all $g \in G$, $gHg^{-1} = H$

9.3 Quotient groups

under construction

9.4 First Isomorphism Theorem

under construction

9.5 Normal subgroups = kernels of homomorphisms

under construction

10 Rings

Definition. Let R be a set and let $+$ and $\cdot$ be binary operations on R. $(R, +, \cdot)$ is a **ring** if

1. $(R, +)$ is an abelian group.
2. For all $a, b, c \in R$, $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.
   (multiplication is **associative**)
3. For all $a, b, c \in R$, $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(b + c) \cdot a = b \cdot a + c \cdot a$.
   (multiplication **distributes** across addition)

10.1 Notation

- We call $+$ addition and $\cdot$ multiplication even if the operations aren't the "usual" addition and multiplication.
- Since $(R, +)$ is an abelian group:
  - We use 0 to denote the additive identity of the ring.
  - For $a \in R$ we denote the additive inverse of any element as $-a$.
  - For a, b in R we write $a - b$ as a shortcut for $a + (-b)$.
- To shorten our writing we often write $a \cdot b = ab$.
- For $n \in \mathbb{Z}$, write na to mean $\underbrace{a + a + \cdots + a}_{n}$.
- For $n \in \mathbb{Z}$, write a^n to mean $\underbrace{a \cdot a \cdot \cdots \cdot a}_{n}$.
- We often write "R is a ring" instead of "$(R, +, \cdot)$ is a ring" when the operations are clear from context. (Just as we often call groups G instead of $(G, *)$.)

A ring may or may not have a multiplicative identity. If it does; i.e., if there is an element $1 \in R$ such that $1 \neq 0$ and $1 \cdot a = a \cdot 1 = a$ for all $a \in R$, we say R is a **ring with unity** or **unital ring**.

Multiplication in a ring may or may not be commutative. If it is; i.e., if $ab = ba$ for all $a, b \in R$, we call R a **commutative ring.**

10.2 Units, zero divisors, integral domains, and fields.

- An element $a \in R$ is called a **unit** if there exists $b \in R$ such that $ab = ba = 1$.
  - In other words, if $ab = ba = 1$ then a and b are both units.
  - We usually write $b = a^{-1}$ and $a = b^{-1}$.
  - This definition only makes sense if the ring is unital.
- A nonzero element $a \in R$ is called a **zero divisor** if there is a nonzero $b \in R$ such that $ab = 0$ or $ba = 0$.
  - In other words, if $ab = 0$ with $a \neq 0$, $b \neq 0$, then a and b are both zero divisors.

Definition. An **integral domain** is a unital commutative ring R that has the property: for all $a, b \in R$, if $ab = 0$ then either $a = 0$ or $b = 0$.

In other words: If R is a unital commutative ring with no zero divisors, then R is an integral domain.

Definition. A **field** is a unital commutative ring such that every nonzero element has a multiplicative inverse.

In other words: If R is a unital commutative ring and every nonzero element is a unit, then R is a field.

Let R^* denote the non-zero elements of the ring R. Then R is a field if it is a unital commutative ring and R^* forms a group under multiplication.

10.3 Examples.

1. $(\mathbb{Z}, +, \cdot)$.

- Integral domain? Yes. This ring is commutative and unital (unity=1), and it has no zero divisors.
- Field? No, not every element is a unit. In fact, the only units are 1 and -1.

2. $(\mathbb{Z}_{12}, +_{12}, \cdot_{12})$.

- Integral domain? No. This ring has many zero divisors. Actually, every integer that shares a common factor with 12 is a zero divisor, so 2, 3, 4, 6, 8, and 9 are all zero divisors in $\mathbb{Z}_{12}$.
- Field? No, the units of $\mathbb{Z}_n$ are the $0 < a < n$ such that $\gcd(a, n) = 1$, by 5.1, so not every nonzero element is a unit.

3. $(2\mathbb{Z}, +, \cdot)$.

- Integral domain? No, because this ring is not unital.
- Field? No.

4. $\mathcal{C}[0, 1] = \{f : [0, 1] \to \mathbb{R} : f \text{ is continuous}\}$ under pointwise addition and multiplication of functions. E.g., if $f(x) = x^2$ and $g(x) = \cos(x)$, then $(f + g)(x) = x^2 + \cos(x)$, and $(fg)(x) = x^2 \cos x$.

- Integral domain? No. There are many zero divisors. For instance, consider the following two piecewise linear (and thus continuous) functions:

$$f(x) = \begin{cases} 0 & 0 \leq x < 1/2 \\ x - 1/2 & 1/2 \leq x \leq 1, \end{cases} \quad \text{and} \quad g(x) = \begin{cases} 1/2 - x & 0 \leq x < 1/2 \\ 0 & 1/2 \leq x \leq 1. \end{cases}$$

Both $f(x)$ and $g(x)$ are nonzero functions, but $f(x)g(x)$ is zero everywhere on $[0,1]$.

- Field? No. The units of this ring are $f \in \mathcal{C}[0,1]$ such that $f(x) \neq 0$ for all $x \in [0,1]$.

5. $\mathbb{R}[x] = \{a_n x^n + \cdots + a_1 x + a_0 : a_i \in \mathbb{R}\}$, the set of polynomials in the variable x with real coefficients, under the usual addition and multiplication of polynomials.

- Integral domain? Yes.
- Field? No. For instance, the polynomial x^2+2 does not have a multiplicative inverse.
  Note: the expression $\frac{1}{x^2+2}$, which is called a **rational function**, is *not* an element of $\mathbb{R}[x]$.

6. $\mathbb{Z}_{12}[x] = \{a_n x^n + \cdots + a_1 x + a_0 : a_i \in \mathbb{Z}_{12}\}$, the set of polynomials in the variable x with coefficients that are elements of $\mathbb{Z}_{12}$, where addition and multiplication of polynomials is done normally and then coefficients are reduced modulo 12.

- Integral domain? No. For example, let $p(x) = 3 + 3x^2$, $q(x) = 4 + 4x^2 + 4x^4$. Then $p(x)q(x) = 0$.
- Field? No.

7. Here is an example of a set which is **not a ring**. Consider the subset S of $\mathbb{R}[x]$ (previous example) consisting of those polynomials with degree at most d. I.e.,

$$S = \{r_d x^d + r_{d-1} x^{d-1} \cdots + r_1 x + r_0 : r_i \in \mathbb{R}\}$$

where d is a fixed integer. This is not a ring, because it is not closed under the multiplication operation. For example, x^d is a polynomial in this set, but $(x^d)(x^d) = x^{2d}$ and x^{2d} does not belong to the subset.

8. The set $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$, where $i = \sqrt{-1}$, under the usual addition and multiplication of complex numbers.

- Integral domain? Yes, since it is commutative, unital with unity $1 = 1 + 0i$, and there are no zero divisors. (The easiest way to see this is that $\mathbb{C}$ has no zero divisors.)
- Field? No, not every element is a unit. In fact, the only units are 1, -1, i, and $-i$.

$\mathbb{Z}[i]$ is known as the *Gaussian integers.*

9. $(\mathbb{Q}, +, \cdot)$, rational numbers with usual addition and multiplication.

- Integral domain? Yes, since there are no zero divisors.
- Field? Yes, since for every nonzero rational number $\frac{p}{q}$, the rational number $\frac{q}{p}$ is its multiplicative inverse.

10. $(R, \oplus, \odot)$ where $R = \mathbb{R} \cup \{\infty\}$ is the set of real numbers together with infinity, $\oplus$ is the "max" operation $a \oplus b = \max(a,b)$, and $\odot$ is usual addition: $a \odot b = a + b$.

- Not a ring. This set has no zero element, because there is no $r \in R$ satisfying $\max(r,a) = a$ for all $a \in R$.

11. $(R, \oplus, \odot)$ where $R = \mathbb{R} \cup \{-\infty\}$ is the set of real numbers together with negative infinity, $\oplus$ and $\odot$ as in the last example.

- Still not a ring. This time the set has a zero element, because $-\infty$ satisfies $\max(-\infty, a) = a$ for all $a \in \mathbb{R}$, and $\max(-\infty, -\infty) = -\infty$.
  However, this set lacks additive inverses. For instance, 4 has no additive inverse because $-\infty$ is the zero element, but there is no $r \in R$ such that $\max(4, r) = -\infty$.

12. $\mathbb{Z} \times \mathbb{Z}$ with component-wise addition and multiplication. I.e.,

$$(a,b) + (c,d) = (a+c, b+d), \text{ and } (a,b)(c,d) = (ac, bd).$$

- Integral domain? No! This ring is commutative and unital, but it has many zero divisors. Keep in mind that the zero element of $\mathbb{Z} \times \mathbb{Z}$ is $(0, 0)$. Then, for instance, we have

  $$(1, 0)(0, 1) = (0, 0)$$

  but $(1, 0)$ and $(0, 1)$ are nonzero elements.
- Field? No, it can't be because it's not an integral domain.

The last example illustrates the next theorem, which says that the Cartesian product of rings is a ring.

Theorem. If $(R, +, \cdot)$ and $(R', +', \cdot')$ are both rings, then $R \times R'$ is a ring under the coordinate-wise operations:

$$(r, r') + (s, s') = (r + s, r' +' s')$$

and

$$(r, r')(s, s') = (r \cdot s, r' \cdot' s').$$

Proof. This one is left as an exercise. □

Proposition. Properties of rings (Prop. 16.8 in Judson).
Let R be a ring with $a, b \in R$. Then

1. $a0 = 0a = 0$

2. $a(-b) = (-a)b = -ab$

3. $(-a)(-b) = ab$

A word about proving propositions such as this. The only ring axiom which involves *both* addition and multiplication, and has rules for their interactions, is the axiom of the *distributive laws.* Thus statements like this, which involve the interaction of multiplication with additive inverses and the additive identity, will have to come from the distributive laws.

Proof. **1.** $a0 = a(0 + 0) = a0 + a0 \implies a0 = 0$

2. $ab + a(-b) = a(b - b) = a0 = 0 \implies -ab = a(-b)$
Similarly, $ab + (-a)b = (a - a)b = 0b = 0 \implies -ab = (-a)b$

3. Since $a(-b) = -ab$ by **2.**, and this holds for any ring elements a and b, replace a with the ring element $-a$ to get $(-a)(-b) = -(-a)b = ab$

□

10.4 Subrings

Definition. A **subring** S of a ring R is a subset $S \subseteq R$ such that S is also a ring under the $+$ and $\cdot$ operations of R.

As with subgroups, to check that something is a subring is usually less work than checking that it's a ring. Properties like associativity, distributive laws, and existence of additive inverses are inherited from the ring R. The main properties to check are that $(S, +)$ is a subgroup of the abelian group $(R, +)$, and that S is closed under multiplication.

Proposition. Four-Step Subring Test. A subset S of a ring R is a subring if:

- $0 \in S$ where 0 is the zero of the ring R.
- S is closed under addition; i.e., $a + b \in S$ for all $a, b \in S$.
- S is closed under additive inverses; i.e., for all $a \in S$, $-a \in S$.
- S is closed under multiplication; i.e., $ab \in S$ for all $a, b \in S$.

Proposition. Two-Step Subring Test. A nonempty subset S of R is a subring if:

- S is closed under subtraction; i.e., $a - b \in S$ for all $a, b \in S$.
- S is closed under multiplication; i.e., $ab \in S$ for all $a, b \in S$.

The Two-Step Subring Test simply replaces the Three-Step Subgroup Test (first three conditions of Prop. 10.4) with the One-Step Subgroup Test. (That is why we have to add the requirement of *nonempty*.)

Examples.

- $\{0\}$ is a subring of any ring R, called the *trivial subring*.
- R is a subring of any ring R, called the *improper subring*.

Is it a subring, true/false voting. Answers are given below.

3. $3\mathbb{Z}$ is a subring of $\mathbb{Z}$.
True

4. $\{1, -1, i, -i\}$ is a subring of $\mathbb{C}$.
False

5. $\mathbb{R}$ is a subring of $\mathbb{C}$.
True

6. $\mathbb{Z}_6$ is a subring of $\mathbb{Z}$.
False

7. $\{0, 2, 4\}$ is a subring of $\mathbb{Z}_6$.
True

8. The subring $\{0, 2, 4\}$ of $\mathbb{Z}_6$ is unital.
True

9. The subring $\{0, 2, 4\}$ of $\mathbb{Z}_6$ is an integral domain.
True

10. The subring $\{0, 2, 4\}$ of $\mathbb{Z}_6$ is a field.
True

11. If R is a unital ring, and S is a subring of R, then S is unital.
False, for example by #**3**.

12. If R is a unital ring, and S is a unital subring of R, then R and S have the same unity.
False, for example by #**8**.

13. If R is *not* an integral domain, and S is a subring of R, then S is *not* an integral domain.
False, for example by #**9**.

The subring $\{0, 2, 4\}$ of $\mathbb{Z}_6$ illustrates the following theorem.

10.5 More about integral domains and fields

Inside any integral domain we can solve equations in familiar ways. For instance:

Find all solutions $x \in \mathbb{Z}$ to the equation $x^2 - 4x + 3 = 0$.

We can write $0 = x^2 - 4x + 3 = (x - 3)(x - 1)$ and conclude that $x = 1$ and $x = 3$ are the integer solutions.

Here we are relying on the fact that for $a, b \in \mathbb{Z}$, $ab = 0$ implies $a = 0$ or $b = 0$. In other words, relying on $\mathbb{Z}$ being an integral domain. Consider a similar problem, this time not working over an integral domain:

Find all solutions $x \in \mathbb{Z}_{12}$ to the equation $x^2 - 4x + 3 = 0$.

Because $\mathbb{Z}_{12}$ has zero divisors, so does $\mathbb{Z}_{12}[x]$. We can still write $0 = x^2 - 4x + 3 = (x - 3)(x - 1)$, but because of the existence of zero divisors, we cannot conclude that $x - 3 = 0$ or $x - 1 = 0$. You can verify that over $\mathbb{Z}_{12}$. there are four solutions to the equation: $x = 1$, 3, 7, and 9.

Another technique we'd like use to solve equations is *cancellation* of common factors (if $ab = ac$ and $a \neq 0$, then $b = c$). For instance:

Find all solutions $x \in \mathbb{Z}$ to the equation $6x^2 - 24x + 18 = 0$.

We can "cancel the 6" to conclude that this equation holds if and only if $x^2 - 4x + 3 = 0$ holds, so the solutions are $x = 1$ and 3 like before. But what about:

Find all solutions $x \in \mathbb{Z}_{12}$ to the equation $6x^2 - 24x + 18 = 0$.

Now this equation has *six* solutions, $x = 1, 3, 5, 7, 9, 11$. If we try to "cancel the 6" we lose two solutions!

We will see next that the ability to cancel goes hand-in-hand with the absence of zero divisors; in fact, these are two equivalent conditions that characterize integral domains.

Proposition. (Prop. 16.15 in Judson). Let D be a commutative unital ring. Then D is an integral domain if and only if we have the cancellation property. More precisely, D is an integral domain if and only if for every nonzero $a \in D$, $ab = ac$ implies $b = c$.

Proof. First suppose D is an integral domain. Suppose $a \in D$ is nonzero and that $ab = ac$. Then $ab - ac = 0$, so $a(b - c) = 0$. Since D has no zero divisors and $a \neq 0$, $b - c = 0$ must be true.

On the other hand, suppose D is a commutative unital ring with the cancellation property. Let a be an arbitrary nonzero element of D, and suppose $ab = 0$. Then $ab = a0$, so by cancellation b must be 0. We have proved that for any $a, b \in D$, if $ab = 0$ then either $a = 0$ or $b = 0$, which is the exact definition of an integral domain. □

Every field F is an integral domain. This follows from the fact that F^* is a group under multiplication, and therefore cancellation holds. Alternatively, it follows from the following proposition.

Proposition. Let R be a ring. If $a \in R$ is a unit, then a is not a zero divisor.

Proof. Suppose $a \in R$ is a unit, so by definition there exists $a^{-1} \in R$ such that $aa^{-1} = a^{-1}a = 1$.

Now suppose there exists $b \in R$ such that $ab = 0$. Then $a^{-1}ab = a^{-1}0 \implies b = 0$. Similarly, if there exists $b \in R$ such that $ba = 0$, we have $baa^{-1} = 0a^{-1} \implies b = 0$.

Thus a cannot be a zero divisor. □

It's important to remember that the converse of Proposition 10.5 is not true; just because a ring element isn't a zero divisor, that doesn't mean it's a unit. In $\mathbb{Z}$, for instance, every nonzero element other than 1 and -1 is neither a unit nor a zero divisor.

However, in the special case where R is a finite ring, it is true that every nonzero element is either a unit or (this is the exclusive or!) a zero divisor. In particular this means that if there are no zero divisors, every nonzero element is a unit. In other words:

Theorem. (Thm. 16.16 in Judson). Every finite integral domain is a field.

Proof. Let D be a finite integral domain with unity element 1. Let a be any nonzero element of D. WTS a is a unit. If $a = 1$ we are done, so suppose $a \neq 1$, and consider the following sequence of elements of D:

$$\{a, a^2, a^3, \ldots\}.$$

Since D is finite, this list must be finite, so there must exist positive integers $i \neq j$ such that $a^i = a^j$. WLOG suppose $i > j$. Then by cancellation $a^{i-j} = 1$, which means $a \cdot a^{i-j-1} = 1$. (Note: we know $i - j$ is at least 2 since $a \neq 1$.) So a is a unit. □

Corollary. For every prime p, $\mathbb{Z}_p$ is a field.

Proof. This follows from Proposition 5.1. □

Example. There are finite fields other than $\mathbb{Z}_p$. For instance, $\mathbb{Z}_3[i] = \{a + bi : a, b \in \mathbb{Z}_3\}$ is a finite field with 9 elements.

10.6 Ring homomorphisms and isomorphisms

Is $\mathbb{Z}$ is a subring of $\mathbb{Z} \times \mathbb{Z}$? This is **false**, because the zero element of $\mathbb{Z} \times \mathbb{Z}$ is $(0, 0)$, and $(0, 0) \notin \mathbb{Z}$.

Even though $\mathbb{Z}$ isn't technically a subring of $\mathbb{Z} \times \mathbb{Z}$, it is *isomorphic* to one. For instance, $\mathbb{Z} \cong \mathbb{Z} \times \{0\} = \{(n, 0) : n \in \mathbb{Z}\} \subseteq \mathbb{Z} \times \mathbb{Z}$.

To prove this, we need the definition of a **ring isomorphism**. This is very similar to the previous notion of group isomorphism, but now we require that *both* binary operations are preserved.

Definition. Let R and S be rings. A **ring homomorphism** $\phi : R \to S$ is a map satisfying:

1. $\phi(a + b) = \phi(a) + \phi(b)$, and

2. $\phi(ab) = \phi(a)\phi(b)$.

If $\phi : R \to S$ is a bijective homomorphism, then ϕ is called a **ring isomorphism**.

Examples.

1. The subring $\mathbb{Z} \times \{0\}$ of $\mathbb{Z} \times \mathbb{Z}$ is isomorphic to $\mathbb{Z}$.

2. Let $C[0, 1]$ be the ring of continuous real-valued functions on the domain $[0, 1]$. For $\alpha \in [0, 1]$, define the **evaluation homomorphism** $\phi_\alpha : C[0, 1] \to \mathbb{R}$ by $\phi_\alpha(f) = f(\alpha)$. Prove this is a ring homomorphism. Is it an isomorphism?

3. True or false: $\mathbb{Z}[i] \cong \mathbb{Z}\times\mathbb{Z}$. Recall: $\mathbb{Z}[i] = \{a+bi : a, b \in \mathbb{Z}\}$, where $i = \sqrt{-1}$, under the usual addition and multiplication of complex numbers.

4. True or false: $\mathbb{Z}[\sqrt{2}] \cong \mathbb{Z}[i]$, where $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$.

Proposition. (Prop. 16.22 in Judson). Properties of ring homomorphisms.
Let $\phi : R \to S$ be a ring homomorphism. Then

1. If R is a commutative ring, then $\phi(R)$ is a commutative ring.

2. $\phi(0) = 0$.

3. Let 1_R and 1_S denote the unity elements of R and S, respectively. If ϕ is onto, then $\phi(1_R) = 1_S$.

4. If R is a field and $\phi(R) \neq \{0\}$, then $\phi(R)$ is a field.

Examples.

1. True or false: $\mathbb{Z}[i] \cong \mathbb{Z}\times\mathbb{Z}$. Recall: $\mathbb{Z}[i] = \{a+bi : a, b \in \mathbb{Z}\}$, where $i = \sqrt{-1}$, under the usual addition and multiplication of complex numbers.

False. For example, the element i has (multiplicative) order 4 in $\mathbb{Z}[i]$, but there are no elements in $\mathbb{Z} \times \mathbb{Z}$ of multiplicative order 4.

2. True or false: $\mathbb{Z}[\sqrt{2}] \cong \mathbb{Z}[i]$, where $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$.

False. Suppose $\phi : \mathbb{Z}[\sqrt{2}] \to \mathbb{Z}[i]$ were an isomorphism. By Prop. 10.6, $\phi(1) = 1$. This forces $\phi(2) = \phi(1 + 1) = \phi(1) + \phi(1) = 2$. Now suppose $\phi(\sqrt{2}) = a \in \mathbb{Z}[i]$. Because ϕ is a homomorphism $2 = \phi(2) = \phi(\sqrt{2} \cdot \sqrt{2}) = \phi(\sqrt{2}) \cdot \phi(\sqrt{2}) = a^2$. But there is no $a \in \mathbb{Z}[i]$ such that $a^2 = 2$ so this is impossible.

11 Polynomial Rings

We are already familiar with:
- $\mathbb{R}[x]$, the ring of polynomials in one variable x, with real coefficients
- $\mathbb{Q}[x]$, the ring of polynomials in x with rational coefficients
- $\mathbb{Z}[x]$, the ring of polynomials in x with integer coefficients.

We can also define polynomials over less familiar rings, such as $\mathbb{Z}_{12}[x]$, the ring of polynomials in x with coefficients in $\mathbb{Z}_{12}$.

In general...

Definition. Let R be a ring. A **polynomial** over R with indeterminate (or variable) x is an expression of the form

$$p(x) = \sum_{i=0}^{n} a_i x^i = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0,$$

where the **coefficients** a_i are elements of R.
If n is the largest positive integer such that $a_n \neq 0$, we say the **degree** of $p(x)$ is n, and write $\deg p(x) = n$.

Note: by convention, we say that the zero polynomial, $p(x) = 0$, has degree $-\infty$.

Proposition. $R[x]$ is a ring under the usual addition and multiplication of polynomials.

Writing addition and multiplication of polynomials abstractly.

Let $p(x) = a_0 + a_1 x + \cdots + a_n x^n$, and let $q(x) = b_0 + b_1 x + \cdots b_m x^m$. Then:

- $p(x) + q(x) = c_0 + c_1 x + \cdots + c_k x^k$, where $k = \max(m, n)$, and $c_i = (a_i + b_i)$.
- $p(x)q(x) = c_0 + c_1 x + \cdots + c_k x^k$, where $k = m + n$, and

$$c_i = \sum_{k=0}^{i} a_k b_{i-k} = a_0 b_i + a_1 b_{i-1} + \cdots + a_{i-1} b_1 + a_i b_0.$$

The next two theorems show that when R is an integral domain, the polynomials in $R[x]$ behave in familiar ways. For instance, $p(x)q(x) = 0$ implies that $p(x) = 0$ or $q(x) = 0$, and $\deg(p(x)q(x)) = p(x) + q(x)$.

Theorem. (Thm. 17.3 in Judson)
Let R be a commutative unital ring. Then $R[x]$ is a commutative unital ring.

Theorem. (Thm. 17.4 in Judson)
Let R be an integral domain. Then $R[x]$ is an integral domain.
Furthermore, if $p(x)$ and $q(x)$ are polynomials in $R[x]$, then $\deg p(x) + \deg q(x) = \deg(p(x)q(x))$.

Note: if R is not an integral domain, then degrees of polynomials may do very unexpected things! For example, let $p(x) = 3 + 3x^2$, $q(x) = 4 + 4x^2 + 4x^4$ in $\mathbb{Z}_{12}[x]$. Then $\deg p(x) = 2$, $\deg q(x) = 4$, and $\deg p(x)q(x) = -\infty$.

Theorem. Division Algorithm. Let $f(x)$ and $g(x) \neq 0$ be polynomials in $F[x]$, where F is a field. Then there exist unique polynomials $q(x), r(x) \in F[x]$ such that

$$f(x) = g(x)q(x) + r(x),$$

and $\deg r(x) < \deg g(x)$ or $r(x) = 0$.

Proof. If $f(x) = 0$ or $\deg f(x) < \deg g(x)$, then we must have $q(x) = 0$ and $r(x) = f(x)$.

Note: we are relying on the fact that F is an integral domain and therefore $\deg g(x)q(x) = \deg g(x) + \deg q(x)$.

So we can assume that $\deg f(x) \geq \deg g(x)$. Let $f(x) = a_n x^n + \cdots + a_0$, $g(x) = b_m x^m + \cdots + b_0$ with $n \geq m$. We are going to prove this using induction on n. We will prove existence, and then uniqueness.

Base case: $n = 0$, which means $m = 0$. Then $f(x) = a_0 \neq 0$ and $g(x) = b_0 \neq 0$, so

$$f(x) = a_0 b_0^{-1} g(x) + 0.$$

Note: we are relying on the fact that F is a field and therefore b_0^{-1} exists.

Inductive hypothesis: suppose the statement is true when $\deg f(x) \leq n - 1$.

Inductive step: now suppose $\deg f(x) = n$. Then let

$$f'(x) = f(x) - a_n b_m^{-1} x^{n-m} g(x).$$

Then $\deg f'(x) < \deg f(x)$ so by the inductive hypothesis, there exists $q'(x)$ and $r'(x)$ in $F[x]$ such that

$$f'(x) = q'(x)g(x) + r'(x)$$

and $r'(x) = 0$ or $\deg r'(x) < \deg g(x)$. Therefore

$$\begin{aligned} f(x) &= a_n b_m^{-1} x^{n-m} g(x) + f'(x) \\ &= a_n b_m^{-1} x^{n-m} g(x) + q'(x)g(x) + r'(x) \\ &= (a_n b_m^{-1} x^{n-m} + q'(x))g(x) + r'(x) \end{aligned}$$

so the polynomials $q(x) = a_n b_m^{-1} x^{n-m} + q'(x)$ and $r(x) = r'(x)$ satisfy the desired properties.

Now to prove uniqueness, suppose that $f(x) = q_1(x)g(x) + r_1(x)$ and $f(x) = q_2(x)g(x) + r_2(x)$ both satisfy the properties. Then

$$0 = (q_1(x) - q_2(x))g(x) + (r_1(x) - r_2(x))$$

or

$$(q_1(x) - q_2(x))g(x) = (r_2(x) - r_1(x)).$$

Since $r_2(x) - r_1(x)$ has smaller degree than $g(x)$, this is only possible if both sides are 0.

Note: we are again using the fact that F is an integral domain.

□

Corollary. Let F be a field. An element $\alpha \in F$ is a zero of $p(x) \in F[x]$ if and only if $x - \alpha$ is a factor of $p(x)$.

Proof. Using the division algorithm:

$$p(x) = q(x)(x - \alpha) + r(x)$$

where $\deg r(x) < \deg(x - \alpha) = 1$. So $r(x)$ is some constant c. Therefore

$$0 = p(\alpha) = q(\alpha)(\alpha - \alpha) + c = 0 + c$$

so $c = 0$ and $x - \alpha$ is a factor of $p(x)$.

On the other hand if $x - \alpha$ is a factor of $p(x)$ then $p(x) = f(x)(x - \alpha)$ so $p(\alpha) = 0$.

□

Corollary. Let F be a field. A nonzero polynomial $p(x)$ of degree n in $F[x]$ can have at most n distinct roots in F.

Proof. By induction: if $\deg p(x) = 0$ then $p(x)$ is a constant polynomial and has no roots. If $\deg p(x) = 1$, then $p(x) = ax + b$ for some $a, b \in F$. If α_1 and α_2 are zeros of $p(x)$, then $a\alpha_1 + b = a\alpha_2 + b \implies \alpha_1 = \alpha_2$.

Now suppose $\deg p(x) > 1$. If $p(x)$ doesn't have a zero in F, we're done. OTOH suppose α is a zero of $p(x)$. Then $p(x) = (x - \alpha)q(x)$ for some $q(x) \in F[x]$ by the previous corollary. The degree of $q(x)$ is $n - 1$ since we're in an integral domain.

Let β be a zero of $p(x)$ distinct from α. Then β is also a zero of $q(x)$. This is because $0 = p(\beta) = (\beta - \alpha)q(\beta)$. Since $\beta - \alpha \neq 0$, and $F[x]$ is an integral domain, $q(\beta) = 0$. By induction hypothesis, $q(x)$ has at most $n - 1$ zeros in F. Therefore $p(x)$ has at most n distinct zeros in F. □

11.1 Note about CSET Standards

Here are some of the specific CSET standards, in their words, that seem relevant to this last portion of 4170. I was curious about 4170 being a requirement for the CSET waiver and thought the answer was interesting; maybe you will too.

- Demonstrate knowledge of why the real and complex numbers are each a field, and that particular rings are not fields (e.g., integers, polynomial rings, matrix rings)
- Identify and translate between equivalent forms of algebraic expressions and equations using a variety of techniques (e.g., factoring, applying properties of operations)
- Justify the steps in manipulating algebraic expressions and solving algebraic equations and inequalities
- Analyze and solve polynomial equations with real coefficients using the Fundamental Theorem of Algebra (related to Corollary 11)
- Prove and use the Factor Theorem (Corollary 11)
- Demonstrate knowledge that the rational numbers and real numbers can be ordered and that the complex numbers cannot be ordered, but that any polynomial equation with real coefficients can be solved in the complex field (we didn't talk about ordered fields, but ask me if you're interested)

11.2 Ideals

Definition. Let R be a ring. An **ideal** of R is a subring I that satisfies: for all $a \in I$ and for all $r \in R$, both $ar \in I$ and $ra \in I$.

You can think of an ideal as an additive subgroup which also *absorbs products*.

Proposition. Four-Step Subring Test. A subset I of a ring R is an ideal of R if:

- $0 \in I$ where 0 is the zero of the ring R.
- I is closed under addition; i.e., $a + b \in I$ for all $a, b \in I$.
- I is closed under additive inverses; i.e., for all $a \in I$, $-a \in I$.
- I absorbs products ($ra, ar \in I$ whenever $a \in I$ and $r \in R$).

Proposition. (Two-Step Ideal Test.)
A nonempty subset I of a ring R is an ideal of R if:

1. I is closed under subtraction ($a - b \in I$ whenever $a, b \in I$).

2. I absorbs products ($ra, ar \in I$ whenever $a \in I$ and $r \in R$).

The Two-Step Ideal Test simply replaces the Three-Step Subgroup Test (first three conditions of Prop. 11.2) with the One-Step Subgroup Test.

Examples.

1. $\{0\}$ is an ideal of any ring R, called the *trivial ideal*.

2. R is an ideal of any ring R, called the *improper ideal*.

3. $n\mathbb{Z}$ is an ideal of $\mathbb{Z}$ for any n.

4. If a is an element of a ring R, the *principal ideal generated by* a is the smallest ideal of R containing a.

5. Let R be a commutative ring with unity and let $a \in R$. The *principal ideal generated by* a is the set $\langle a \rangle = \{ra : r \in R\}$.

Why do we require a commutative ring with unity here?

6. $\langle x \rangle \subseteq \mathbb{R}[x]$ is the set of all polynomials with constant term 0.

7. Let R be a commutative ring with unity and let $a_1, \ldots, a_n \in R$. The *ideal generated by* $a_1, \ldots, a_n$ is the set $\langle a_1, \ldots, a_n \rangle = \{r_1 a_1 + r_2 a_2 + \cdots r_n a_n : r_i \in R\}$.

8. $\langle x, 2 \rangle \subseteq \mathbb{Z}[x]$.

9. Subset of differentiable functions is not an ideal of set of continuous functions.

Appendix: some Cayley tables

$\mathbb{Z}_4$

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\mathbb{Z}_6$

$+_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$\mathbb{Z}_2 \times \mathbb{Z}_2$

$(+_2, +_2)$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,0)$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,1)$	$(0,1)$	$(0,0)$	$(1,1)$	$(1,0)$
$(1,0)$	$(1,0)$	$(1,1)$	$(0,0)$	$(0,1)$
$(1,1)$	$(1,1)$	$(1,0)$	$(0,1)$	$(0,0)$

$U(8)$

$\cdot_8$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

$U(10)$

$\cdot_{10}$	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

S_3

	()	(12)	(23)	(13)	(123)	(132)
()	()	(12)	(23)	(13)	(123)	(132)
(12)	(12)	()	(123)	(132)	(23)	(13)
(23)	(23)	(132)	()	(123)	(13)	(12)
(13)	(13)	(123)	(132)	()	(12)	(23)
(123)	(123)	(13)	(12)	(23)	(132)	()
(132)	(132)	(23)	(13)	(12)	()	(123)

A_3

	()	(123)	(132)
()	()	(123)	(132)
(123)	(123)	(132)	()
(132)	(132)	()	(123)

D_3

	1	r	r^2	s	rs	r^2s
1	1	r	r^2	s	rs	r^2s
r	r	r^2	1	rs	r^2s	s
r^2	r^2	1	r	r^2s	s	rs
s	s	r^2s	rs	1	r^2	r
rs	rs	s	r^2s	r	1	r^2
r^2s	r^2s	rs	s	r^2	r	1

D_4

	1	r	r^2	r^3	s	rs	r^2s	r^3s
1	1	r	r^2	r^3	s	rs	r^2s	r^3s
r	r	r^2	r^3	1	rs	r^2s	r^3s	s
r^2	r^2	r^3	1	r	r^2s	r^3s	s	rs
r^3	r^3	1	r	r^2	r^3s	s	rs	r^2s
s	s	r^3s	r^2s	rs	1	r^3	r^2	r
rs	rs	s	r^3s	r^2s	r	1	r^3	r^2
r^2s	r^2s	rs	s	r^3s	r^2	r	1	r^3
r^3s	r^3s	r^2s	rs	s	r^3	r^2	r	1

Q_8

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

S_4

*	()	(34)	(23)	(234)	(243)	(24)	(12)	(12)(34)	(123)	(1234)	(1243)	(124)	(132)	(1342)	(13)	(134)	(13)(24)	(1324)	(1432)	(142)	(143)	(14)	(1423)	(14)(23)
()	()	(34)	(23)	(234)	(243)	(24)	(12)	(12)(34)	(123)	(1234)	(1243)	(124)	(132)	(1342)	(13)	(134)	(13)(24)	(1324)	(1432)	(142)	(143)	(14)	(1423)	(14)(23)
(34)	(34)	()	(234)	(23)	(24)	(243)	(12)(34)	(12)	(1234)	(123)	(124)	(1243)	(1342)	(132)	(134)	(13)	(1324)	(13)(24)	(142)	(1432)	(14)	(143)	(14)(23)	(1423)
(23)	(23)	(243)	()	(24)	(34)	(234)	(123)	(1243)	(12)	(124)	(12)(34)	(1234)	(13)	(13)(24)	(132)	(1324)	(1342)	(134)	(143)	(1423)	(1432)	(14)(23)	(142)	(14)
(234)	(234)	(24)	(34)	(243)	()	(23)	(1234)	(124)	(12)(34)	(1243)	(12)	(123)	(134)	(1324)	(1342)	(13)(24)	(132)	(13)	(14)	(14)(23)	(142)	(1423)	(1432)	(143)
(243)	(243)	(23)	(24)	()	(234)	(34)	(1243)	(123)	(124)	(12)	(1234)	(12)(34)	(13)(24)	(13)	(1324)	(132)	(134)	(1342)	(1423)	(143)	(14)(23)	(1432)	(14)	(142)
(24)	(24)	(234)	(243)	(34)	(23)	()	(124)	(1234)	(1243)	(12)(34)	(123)	(12)	(1324)	(134)	(13)(24)	(1342)	(13)	(132)	(14)(23)	(14)	(1423)	(142)	(143)	(1432)
(12)	(12)	(12)(34)	(132)	(1342)	(1432)	(142)	()	(34)	(13)	(134)	(143)	(14)	(23)	(234)	(123)	(1234)	(1423)	(14)(23)	(243)	(24)	(1243)	(124)	(13)(24)	(1324)
(12)(34)	(12)(34)	(12)	(1342)	(132)	(142)	(1432)	(34)	()	(134)	(13)	(14)	(143)	(234)	(23)	(1234)	(123)	(14)(23)	(1423)	(24)	(243)	(124)	(1243)	(1324)	(13)(24)
(123)	(123)	(1243)	(13)	(13)(24)	(143)	(1423)	(23)	(243)	(132)	(1324)	(1432)	(14)(23)	()	(24)	(12)	(124)	(142)	(14)	(34)	(234)	(12)(34)	(1234)	(1342)	(134)
(1234)	(1234)	(124)	(134)	(1324)	(14)	(14)(23)	(234)	(24)	(1342)	(13)(24)	(142)	(1423)	(34)	(243)	(12)(34)	(1243)	(1432)	(143)	()	(23)	(12)	(123)	(132)	(13)
(1243)	(1243)	(123)	(13)(24)	(13)	(1423)	(143)	(243)	(23)	(1324)	(132)	(14)(23)	(1432)	(24)	()	(124)	(12)	(14)	(142)	(234)	(34)	(1234)	(12)(34)	(134)	(1342)
(124)	(124)	(1234)	(1324)	(134)	(14)(23)	(14)	(24)	(234)	(13)(24)	(1342)	(1423)	(142)	(243)	(34)	(1243)	(12)(34)	(143)	(1432)	(23)	()	(123)	(12)	(13)	(132)
(132)	(132)	(1432)	(12)	(142)	(12)(34)	(1342)	(13)	(143)	()	(14)	(34)	(134)	(123)	(1423)	(23)	(14)(23)	(234)	(1234)	(1243)	(13)(24)	(243)	(1324)	(24)	(124)
(1342)	(1342)	(142)	(12)(34)	(1432)	(12)	(132)	(134)	(14)	(34)	(143)	()	(13)	(1234)	(14)(23)	(234)	(1423)	(23)	(123)	(124)	(1324)	(24)	(13)(24)	(243)	(1243)
(13)	(13)	(143)	(123)	(1423)	(1243)	(13)(24)	(132)	(1432)	(23)	(14)(23)	(243)	(1324)	(12)	(142)	()	(14)	(24)	(124)	(12)(34)	(1342)	(34)	(134)	(234)	(1234)
(134)	(134)	(14)	(1234)	(14)(23)	(124)	(1324)	(1342)	(142)	(234)	(1423)	(24)	(13)(24)	(12)(34)	(1432)	(34)	(143)	(243)	(1243)	(12)	(132)	()	(13)	(23)	(123)
(13)(24)	(13)(24)	(1423)	(1243)	(143)	(123)	(13)	(1324)	(14)(23)	(243)	(1432)	(23)	(132)	(124)	(14)	(24)	(142)	()	(12)	(1234)	(134)	(234)	(1342)	(34)	(12)(34)
(1324)	(1324)	(14)(23)	(124)	(14)	(1234)	(134)	(13)(24)	(1423)	(24)	(142)	(234)	(1342)	(1243)	(143)	(243)	(1432)	(34)	(12)(34)	(123)	(13)	(23)	(132)	()	(12)
(1432)	(1432)	(132)	(142)	(12)	(1342)	(12)(34)	(143)	(13)	(14)	()	(134)	(34)	(1423)	(123)	(14)(23)	(23)	(1234)	(234)	(13)(24)	(1243)	(1324)	(243)	(124)	(24)
(142)	(142)	(1342)	(1432)	(12)(34)	(132)	(12)	(14)	(134)	(143)	(34)	(13)	()	(14)(23)	(1234)	(1423)	(234)	(123)	(23)	(1324)	(124)	(13)(24)	(24)	(1243)	(243)
(143)	(143)	(13)	(1423)	(123)	(13)(24)	(1243)	(1432)	(132)	(14)(23)	(23)	(1324)	(243)	(142)	(12)	(14)	()	(124)	(24)	(1342)	(12)(34)	(134)	(34)	(1234)	(234)
(14)	(14)	(134)	(14)(23)	(1234)	(1324)	(124)	(142)	(1342)	(1423)	(234)	(13)(24)	(24)	(1432)	(12)(34)	(143)	(34)	(1243)	(243)	(132)	(12)	(13)	()	(123)	(23)
(1423)	(1423)	(13)(24)	(143)	(1243)	(13)	(123)	(14)(23)	(1324)	(1432)	(243)	(132)	(23)	(14)	(124)	(142)	(24)	(12)	()	(134)	(1234)	(1342)	(234)	(12)(34)	(34)
(14)(23)	(14)(23)	(1324)	(14)	(124)	(134)	(1234)	(1423)	(13)(24)	(142)	(24)	(1342)	(234)	(143)	(1243)	(1432)	(243)	(12)(34)	(34)	(13)	(123)	(132)	(23)	(12)	()

A_4

	()	(123)	(124)	(132)	(134)	(142)	(143)	(234)	(243)	(12)(34)	(13)(24)	(14)(23)
()	()	(123)	(124)	(132)	(134)	(142)	(143)	(234)	(243)	(12)(34)	(13)(24)	(14)(23)
(123)	(123)	(132)	(13)(24)	()	(234)	(143)	(14)(23)	(12)(34)	(124)	(134)	(243)	(142)
(124)	(124)	(14)(23)	(142)	(134)	(13)(24)	()	(243)	(123)	(12)(34)	(143)	(132)	(234)
(132)	(132)	()	(243)	(123)	(12)(34)	(14)(23)	(142)	(134)	(13)(24)	(234)	(124)	(143)
(134)	(134)	(124)	(12)(34)	(14)(23)	(143)	(234)	()	(13)(24)	(132)	(123)	(142)	(243)
(142)	(142)	(234)	()	(13)(24)	(132)	(124)	(12)(34)	(14)(23)	(143)	(243)	(134)	(123)
(143)	(143)	(12)(34)	(123)	(243)	()	(13)(24)	(134)	(142)	(14)(23)	(124)	(234)	(132)
(234)	(234)	(13)(24)	(134)	(142)	(14)(23)	(12)(34)	(123)	(243)	()	(132)	(143)	(124)
(243)	(243)	(143)	(14)(23)	(12)(34)	(124)	(132)	(13)(24)	()	(234)	(142)	(123)	(134)
(12)(34)	(12)(34)	(243)	(234)	(143)	(142)	(134)	(132)	(124)	(123)	()	(14)(23)	(13)(24)
(13)(24)	(13)(24)	(142)	(143)	(234)	(243)	(123)	(124)	(132)	(134)	(14)(23)	()	(12)(34)
(14)(23)	(14)(23)	(134)	(132)	(124)	(123)	(243)	(234)	(143)	(142)	(13)(24)	(12)(34)	()