Math 417 – Second Day

Bruce Reznick
University of Illinois at Urbana-Champaign

August 26, 2020

We're going to talk about two main things today: the definition of a group and the definition of modular arithmetic, which will give us many nice examples of a group.

We're going to talk about two main things today: the definition of a group and the definition of modular arithmetic, which will give us many nice examples of a group.

First, some standard notation:

$$\mathbb{Z} = \{\ldots, -4, -3, -2, -1, 0, 1, 2, 3, 4, \ldots\}$$

are the *integers*, and

$$\mathbb{N} = \{1, 2, 3, 4, \ldots\}$$

are the *natural numbers* and

$$\mathbb{Q} = \left\{ \frac{m}{n} : m, n \in \mathbb{Z}, n \neq 0 \right\}$$

are the *rational numbers*.

We're going to talk about two main things today: the definition of a group and the definition of modular arithmetic, which will give us many nice examples of a group.

First, some standard notation:

$$\mathbb{Z} = \{\ldots, -4, -3, -2, -1, 0, 1, 2, 3, 4, \ldots\}$$

are the *integers*, and

$$\mathbb{N} = \{1, 2, 3, 4, \ldots\}$$

are the *natural numbers* and

$$\mathbb{Q} = \left\{ \frac{m}{n} : m, n \in \mathbb{Z}, n \neq 0 \right\}$$

are the *rational numbers*.

As with V, these names come from the German; e.g. "integer" in German is "zahl".

A *group* consists of a pair $(G, *)$, where G is a set of elements and "$*$" is what is called a binary operation: if $x, y \in G$, then $x * y \in G$.

A *group* consists of a pair $(G, *)$, where G is a set of elements and "$*$" is what is called a binary operation: if $x, y \in G$, then $x * y \in G$.

Then $(G, *)$ is a group provided all the following hold:

1. There is an element $e \in G$ so that, for all $x \in G$, $x * e = e * x = x$. (identity)

A *group* consists of a pair $(G, *)$, where G is a set of elements and "$*$" is what is called a binary operation: if $x, y \in G$, then $x * y \in G$.

Then $(G, *)$ is a group provided all the following hold:

1. There is an element $e \in G$ so that, for all $x \in G$, $x * e = e * x = x$. (identity)
2. For every element $x \in G$ there is an element $y \in G$ so that $x * y = y * x = e$. (inverse)

A *group* consists of a pair $(G, *)$, where G is a set of elements and "$*$" is what is called a binary operation: if $x, y \in G$, then $x * y \in G$.

Then $(G, *)$ is a group provided all the following hold:

1. There is an element $e \in G$ so that, for all $x \in G$, $x * e = e * x = x$. (identity)
2. For every element $x \in G$ there is an element $y \in G$ so that $x * y = y * x = e$. (inverse)
3. For all $x, y, z \in G$, $(x * y) * z = x * (y * z)$. (associativity)

A *group* consists of a pair $(G, *)$, where G is a set of elements and "$*$" is what is called a binary operation: if $x, y \in G$, then $x * y \in G$.

Then $(G, *)$ is a group provided all the following hold:

1. There is an element $e \in G$ so that, for all $x \in G$, $x * e = e * x = x$. (identity)
2. For every element $x \in G$ there is an element $y \in G$ so that $x * y = y * x = e$. (inverse)
3. For all $x, y, z \in G$, $(x * y) * z = x * (y * z)$. (associativity)

The following notations are standard: the inverse of x is usually written as x^{-1}. For $n \in N$:

$$x^1 := x, \quad x^2 := x * x, \quad x^n := x * x^{n-1} \quad \text{if } n > 2.$$

We also define $x^0 := e$ and for $n \in N$, $x^{-n} := (x^n)^{-1}$.

A *group* consists of a pair $(G, *)$, where G is a set of elements and "$*$" is what is called a binary operation: if $x, y \in G$, then $x * y \in G$.

Then $(G, *)$ is a group provided all the following hold:

1. There is an element $e \in G$ so that, for all $x \in G$, $x * e = e * x = x$. (identity)
2. For every element $x \in G$ there is an element $y \in G$ so that $x * y = y * x = e$. (inverse)
3. For all $x, y, z \in G$, $(x * y) * z = x * (y * z)$. (associativity)

The following notations are standard: the inverse of x is usually written as x^{-1}. For $n \in N$:

$$x^1 := x, \quad x^2 := x * x, \quad x^n := x * x^{n-1} \quad \text{if } n > 2.$$

We also define $x^0 := e$ and for $n \in N$, $x^{-n} := (x^n)^{-1}$.

It is a boring but true result that $x^m * x^n = x^{m+n}$ for $m, n \in \mathbb{Z}$. I think it's in the book, but if you want me to write it up I can. It uses induction.

Every set with a multiplication table I gave on Monday is a group. I've changed the look a little. Remember

Every set with a multiplication table I gave on Monday is a group. I've changed the look a little. Remember

Combine	Nothing	Flip
Nothing	Nothing	Flip
Flip	Flip	Nothing

Plus	Even	Odd
Even	Even	Odd
Odd	Odd	Even

?

Every set with a multiplication table I gave on Monday is a group. I've changed the look a little. Remember

Combine	Nothing	Flip
Nothing	Nothing	Flip
Flip	Flip	Nothing

Plus	Even	Odd
Even	Even	Odd
Odd	Odd	Even

?

Let me write these tables again in a more abstract way:

$*$	g	h
g	g	h
h	h	g

Every set with a multiplication table I gave on Monday is a group. I've changed the look a little. Remember

Combine	Nothing	Flip
Nothing	Nothing	Flip
Flip	Flip	Nothing

Plus	Even	Odd
Even	Even	Odd
Odd	Odd	Even

?

Let me write these tables again in a more abstract way:

$*$	g	h
g	g	h
h	h	g

This table should be read as saying that $g * g = g$, $g * h = h$, $h * g = h$, and $h * h = g$. I hope you can see that g is the identity here, because whenever you $*$ it with x (x can be g or h), you get x, and since $h * h = g$, this means that h is its own inverse: $h = h^{-1}$.

One thing that isn't obvious is that this table is associative, but we'll find a sneaky way to talk about that later.

One thing that isn't obvious is that this table is associative, but we'll find a sneaky way to talk about that later.

Here's the table for one of the two C_4's we had on Monday

One thing that isn't obvious is that this table is associative, but we'll find a sneaky way to talk about that later.

Here's the table for one of the two C_4's we had on Monday

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

One thing that isn't obvious is that this table is associative, but we'll find a sneaky way to talk about that later.

Here's the table for one of the two C_4's we had on Monday

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

Notice that the element 0 is the identity and $0+0=1+3=2+2=3+1=0$, so the inverses of $0,1,2,3$ in order are $0,3,2,1$.

One thing that isn't obvious is that this table is associative, but we'll find a sneaky way to talk about that later.

Here's the table for one of the two C_4's we had on Monday

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

Notice that the element 0 is the identity and $0+0=1+3=2+2=3+1=0$, so the inverses of $0,1,2,3$ in order are $0,3,2,1$.

As we'll see at the end, this is just addition mod 4.

Just to finish the review, let me remind you of the multiplication table for the Klein 4-group V:

Just to finish the review, let me remind you of the multiplication table for the Klein 4-group V:

$*$	I	X	Y	Z
I	I	X	Y	Z
X	X	I	Z	Y
Y	Y	Z	I	X
Z	Z	Y	X	I

Just to finish the review, let me remind you of the multiplication table for the Klein 4-group V:

$*$	I	X	Y	Z
I	I	X	Y	Z
X	X	I	Z	Y
Y	Y	Z	I	X
Z	Z	Y	X	I

Since the identity is I and $g^2 = g * g = I$ for every $g \in V$, this means that $g = g^{-1}$ for every $g \in V$. Again, it's not obvious that $*$ is associative from the table, but this follows from the interpretation of the elements as motions. I'll return to this later.

I should make the idea of a multiplication table more formal. Suppose we have a group $(G, *)$ and $G = \{g_1, \ldots, g_n\}$ is a finite set. Then we define the *multiplication table of* G as follows:

I should make the idea of a multiplication table more formal. Suppose we have a group $(G, *)$ and $G = \{g_1, \ldots, g_n\}$ is a finite set. Then we define the *multiplication table of* G as follows:

$*$	g_1	g_2	$\cdots$	g_n
g_1	$g_1 * g_1$	$g_1 * g_2$	$\cdots$	$g_1 * g_n$
g_2	$g_2 * g_1$	$g_2 * g_2$	$\cdots$	$g_2 * g_n$
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
g_n	$g_n * g_1$	$g_n * g_2$	$\cdots$	$g_n * g_n$

I should make the idea of a multiplication table more formal. Suppose we have a group $(G, *)$ and $G = \{g_1, \ldots, g_n\}$ is a finite set. Then we define the *multiplication table of* G as follows:

$*$	g_1	g_2	$\cdots$	g_n
g_1	$g_1 * g_1$	$g_1 * g_2$	$\cdots$	$g_1 * g_n$
g_2	$g_2 * g_1$	$g_2 * g_2$	$\cdots$	$g_2 * g_n$
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
g_n	$g_n * g_1$	$g_n * g_2$	$\cdots$	$g_n * g_n$

There are two conventions: we usually write the first element of the product down the left and the second element of the product across the top and in the same order. Usually, $g_1 = e$. There's a convention that we usually put the identity in the first row and the first column and that we have both in the same order.

Now I'm going to prove our first theorem about groups. It's not hard, and you could easily imagine this just being given as part of the definition. But mathematicians practice Jenga. We try to assume as few properties as possible which keep the whole structure intact.

Now I'm going to prove our first theorem about groups. It's not hard, and you could easily imagine this just being given as part of the definition. But mathematicians practice Jenga. We try to assume as few properties as possible which keep the whole structure intact.

THEOREM 1 If $(G, *)$ is a group and $x, y, z \in G$, then

$$x * y = x * z \implies y = z.$$

Now I'm going to prove our first theorem about groups. It's not hard, and you could easily imagine this just being given as part of the definition. But mathematicians practice Jenga. We try to assume as few properties as possible which keep the whole structure intact.

THEOREM 1 If $(G, *)$ is a group and $x, y, z \in G$, then

$$x * y = x * z \implies y = z.$$

The proof won't fit here, so I'll start it on the next page.

PROOF We use all of the properties of the group! First, multiply both sides by x^{-1}

$$x * y = x * z \implies x^{-1} * (x * y) = x^{-1} * (x * z)$$

PROOF We use all of the properties of the group! First, multiply both sides by x^{-1}

$$x * y = x * z \implies x^{-1} * (x * y) = x^{-1} * (x * z)$$

But now, remember that a group is associative, so

$$x^{-1} * (x * y) = (x^{-1} * x) * y; \qquad x^{-1} * (x * z) = (x^{-1} * x) * z$$

PROOF We use all of the properties of the group! First, multiply both sides by x^{-1}

$$x * y = x * z \implies x^{-1} * (x * y) = x^{-1} * (x * z)$$

But now, remember that a group is associative, so

$$x^{-1} * (x * y) = (x^{-1} * x) * y; \qquad x^{-1} * (x * z) = (x^{-1} * x) * z$$

And since x^{-1} is the inverse of x,

$$(x^{-1} * x) * y = e * y = y; \qquad x^{-1} * (x * z) = e * z = z,$$

PROOF We use all of the properties of the group! First, multiply both sides by x^{-1}

$$x * y = x * z \implies x^{-1} * (x * y) = x^{-1} * (x * z)$$

But now, remember that a group is associative, so

$$x^{-1} * (x * y) = (x^{-1} * x) * y; \qquad x^{-1} * (x * z) = (x^{-1} * x) * z$$

And since x^{-1} is the inverse of x,

$$(x^{-1} * x) * y = e * y = y; \qquad x^{-1} * (x * z) = e * z = z,$$

so to review and put it all in two lines:

PROOF We use all of the properties of the group! First, multiply both sides by x^{-1}

$$x * y = x * z \implies x^{-1} * (x * y) = x^{-1} * (x * z)$$

But now, remember that a group is associative, so

$$x^{-1} * (x * y) = (x^{-1} * x) * y; \qquad x^{-1} * (x * z) = (x^{-1} * x) * z$$

And since x^{-1} is the inverse of x,

$$(x^{-1} * x) * y = e * y = y; \qquad x^{-1} * (x * z) = e * z = z,$$

so to review and put it all in two lines:

$$x * y = x * z \implies x^{-1} * (x * y) = x^{-1} * (x * z) \implies$$
$$(x^{-1} * x) * y = (x^{-1} * x) * z \implies e * y = e * z \implies y = z. \quad \square$$

If any part of that is unclear, try to prove it in the opposite direction:

If any part of that is unclear, try to prove it in the opposite direction:

THEOREM 2: $y * x = z * x \implies y = z$.

If any part of that is unclear, try to prove it in the opposite direction:

THEOREM 2: $y * x = z * x \implies y = z$.

But be careful with the order in which you apply the operations. We will have examples later where $y * x = x * z$, but $y \neq z$.

If any part of that is unclear, try to prove it in the opposite direction:

THEOREM 2: $y * x = z * x \implies y = z$.

But be careful with the order in which you apply the operations. We will have examples later where $y * x = x * z$, but $y \neq z$.

By Theorem 1, if $G = \{g_1, \ldots, g_n\}$ and $g_i \in G$, then

$$\{g_i * g_1, \ldots g_i * g_n\}$$

are different elements and they are all in G, so this means that this set is just a rearrangement or *permutation* of G.

If any part of that is unclear, try to prove it in the opposite direction:

THEOREM 2: $y * x = z * x \implies y = z$.

But be careful with the order in which you apply the operations. We will have examples later where $y * x = x * z$, but $y \neq z$.

By Theorem 1, if $G = \{g_1, \ldots, g_n\}$ and $g_i \in G$, then

$$\{g_i * g_1, \ldots g_i * g_n\}$$

are different elements and they are all in G, so this means that this set is just a rearrangement or *permutation* of G.

In other words, each rows of the multiplication table contains the elements of G in some order. Theorem 2 implies that the columns are a permutation too. Those of you who do Sudoku will recognize the pattern.

Let's check this out with V:

Let's check this out with V:

$*$	I	X	Y	Z
I	I	X	Y	Z
X	X	I	Z	Y
Y	Y	Z	I	X
Z	Z	Y	X	I

Let's check this out with V:

$*$	I	X	Y	Z
I	I	X	Y	Z
X	X	I	Z	Y
Y	Y	Z	I	X
Z	Z	Y	X	I

We can use this to identify groups. Suppose $(G, *)$ is a group and $|G|$, the number of elements in G is 2. One of them has to be the identity e. Call the other one g. Let's write out the table knowing this fact and knowing that e is the identity:

Let's check this out with V:

$*$	I	X	Y	Z
I	I	X	Y	Z
X	X	I	Z	Y
Y	Y	Z	I	X
Z	Z	Y	X	I

We can use this to identify groups. Suppose $(G, *)$ is a group and $|G|$, the number of elements in G is 2. One of them has to be the identity e. Call the other one g. Let's write out the table knowing this fact and knowing that e is the identity:

$*$	e	g
e	e	g
g	g	g$*$g

Let's check this out with V:

$*$	I	X	Y	Z
I	I	X	Y	Z
X	X	I	Z	Y
Y	Y	Z	I	X
Z	Z	Y	X	I

We can use this to identify groups. Suppose $(G, *)$ is a group and $|G|$, the number of elements in G is 2. One of them has to be the identity e. Call the other one g. Let's write out the table knowing this fact and knowing that e is the identity:

$*$	e	g
e	e	g
g	g	g$*$g

What can $g * g = g^2$ be? We know from Theorem 1 that the set $\{g * e, g * g\} = \{g, g^2\}$ is a permutation of $G = \{e, g\}$, so we are forced to conclude that $g^2 = e$. In other words the group we wrote down with 2 elements is basically the only one possible.

Now let's look at some infinite groups. Think about $(\mathbb{Z}, +)$, that is, the integers, where if $m, n \in \mathbb{Z}$, then $m * n = m + n$, the usual addition on integers. Is this a group? Sure! What's the identity?

Now let's look at some infinite groups. Think about $(\mathbb{Z}, +)$, that is, the integers, where if $m, n \in \mathbb{Z}$, then $m * n = m + n$, the usual addition on integers. Is this a group? Sure! What's the identity?

$$m \in \mathbb{Z} \implies m + 0 = 0 + m = m.$$

Now let's look at some infinite groups. Think about $(\mathbb{Z}, +)$, that is, the integers, where if $m, n \in \mathbb{Z}$, then $m * n = m + n$, the usual addition on integers. Is this a group? Sure! What's the identity?

$$m \in \mathbb{Z} \implies m + 0 = 0 + m = m.$$

Is there an inverse? Sure:

$$m + (-m) = (-m) + m = 0,$$

and since 0 is the identity, $-m$ is the inverse of m in this group.

Now let's look at some infinite groups. Think about $(\mathbb{Z}, +)$, that is, the integers, where if $m, n \in \mathbb{Z}$, then $m * n = m + n$, the usual addition on integers. Is this a group? Sure! What's the identity?

$$m \in \mathbb{Z} \implies m + 0 = 0 + m = m.$$

Is there an inverse? Sure:

$$m + (-m) = (-m) + m = 0,$$

and since 0 is the identity, $-m$ is the inverse of m in this group.

Addition in $\mathbb{Z}$ is also associative. The exact same argument shows that $(\mathbb{Q}, +)$ and even our friend $(\mathbb{R}, +)$ is a group too.

Now let's look at some infinite groups. Think about $(\mathbb{Z}, +)$, that is, the integers, where if $m, n \in \mathbb{Z}$, then $m * n = m + n$, the usual addition on integers. Is this a group? Sure! What's the identity?

$$m \in \mathbb{Z} \implies m + 0 = 0 + m = m.$$

Is there an inverse? Sure:

$$m + (-m) = (-m) + m = 0,$$

and since 0 is the identity, $-m$ is the inverse of m in this group.

Addition in $\mathbb{Z}$ is also associative. The exact same argument shows that $(\mathbb{Q}, +)$ and even our friend $(\mathbb{R}, +)$ is a group too.

What about $\mathbb{N}$? Several problems: $0 \notin \mathbb{N}$ so there is no identity, and in fact, none of the elements in $\{1, 2, \dots\}$ has an inverse! So, $(\mathbb{N}, +)$ is not a group.

What about $(\mathbb{Z}, \cdot)$, the integers with multiplication, so that $m * n = m \cdot n$? Is there an identity? Yes!

$$m \cdot 1 = 1 \cdot m = m.$$

What about $(\mathbb{Z}, \cdot)$, the integers with multiplication, so that $m * n = m \cdot n$? Is there an identity? Yes!

$$m \cdot 1 = 1 \cdot m = m.$$

Is there an inverse? Well, $1 \cdot 1 = 1$ and $(-1) \cdot (-1) = 1$, so these elements have inverses, but $2 \cdot x = 1$ has no solution for $x \in \mathbb{Z}$ and $0 \cdot x = 1$ has no solution of any kind, so $(\mathbb{Z}, \cdot)$ is not a group.

What about $(\mathbb{Z}, \cdot)$, the integers with multiplication, so that $m * n = m \cdot n$? Is there an identity? Yes!

$$m \cdot 1 = 1 \cdot m = m.$$

Is there an inverse? Well, $1 \cdot 1 = 1$ and $(-1) \cdot (-1) = 1$, so these elements have inverses, but $2 \cdot x = 1$ has no solution for $x \in \mathbb{Z}$ and $0 \cdot x = 1$ has no solution of any kind, so $(\mathbb{Z}, \cdot)$ is not a group.

What about $(\mathbb{Q}, \cdot)$, the rational numbers with multiplication, so that $m * n = m \cdot n$? This has identity element 1, and also

$$\frac{m}{n} \cdot \frac{n}{m} = 1.$$

What about $(\mathbb{Z}, \cdot)$, the integers with multiplication, so that $m * n = m \cdot n$? Is there an identity? Yes!

$$m \cdot 1 = 1 \cdot m = m.$$

Is there an inverse? Well, $1 \cdot 1 = 1$ and $(-1) \cdot (-1) = 1$, so these elements have inverses, but $2 \cdot x = 1$ has no solution for $x \in \mathbb{Z}$ and $0 \cdot x = 1$ has no solution of any kind, so $(\mathbb{Z}, \cdot)$ is not a group.

What about $(\mathbb{Q}, \cdot)$, the rational numbers with multiplication, so that $m * n = m \cdot n$? This has identity element 1, and also

$$\frac{m}{n} \cdot \frac{n}{m} = 1.$$

So inverses exist? Well, almost. This doesn't work with $m = 0$, but every non-zero rational has an inverse. We let $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$ denote the set of non-zero rationals.

What about $(\mathbb{Z}, \cdot)$, the integers with multiplication, so that $m * n = m \cdot n$? Is there an identity? Yes!

$$m \cdot 1 = 1 \cdot m = m.$$

Is there an inverse? Well, $1 \cdot 1 = 1$ and $(-1) \cdot (-1) = 1$, so these elements have inverses, but $2 \cdot x = 1$ has no solution for $x \in \mathbb{Z}$ and $0 \cdot x = 1$ has no solution of any kind, so $(\mathbb{Z}, \cdot)$ is not a group.

What about $(\mathbb{Q}, \cdot)$, the rational numbers with multiplication, so that $m * n = m \cdot n$? This has identity element 1, and also

$$\frac{m}{n} \cdot \frac{n}{m} = 1.$$

So inverses exist? Well, almost. This doesn't work with $m = 0$, but every non-zero rational has an inverse. We let $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$ denote the set of non-zero rationals.

Persuade yourself that $(\mathbb{Q}^*, \cdot)$ satisfies all the conditions, and is a group.

I want to mention a few other infinite groups here, because we'll look at them later. First, suppose $d \in \mathbb{N}$ is a positive integer. Let

I want to mention a few other infinite groups here, because we'll look at them later. First, suppose $d \in \mathbb{N}$ is a positive integer. Let

$$d\mathbb{Z} = \{\ldots, -4d, -3d, -2d, -d, 0, d, 2d, 3d, 4d, \ldots\}$$

Then $(d\mathbb{Z}, +)$ is a group. It's a subset of $\mathbb{Z}$, so we'll be calling this a subgroup before too long.

I want to mention a few other infinite groups here, because we'll look at them later. First, suppose $d \in \mathbb{N}$ is a positive integer. Let

$$d\mathbb{Z} = \{\ldots, -4d, -3d, -2d, -d, 0, d, 2d, 3d, 4d, \ldots\}$$

Then $(d\mathbb{Z}, +)$ is a group. It's a subset of $\mathbb{Z}$, so we'll be calling this a subgroup before too long.

Let me look at the first two non-trivial examples. It's easy to check that there are both groups, with 0 as the identity and the obvious elements as inverses.

I want to mention a few other infinite groups here, because we'll look at them later. First, suppose $d \in \mathbb{N}$ is a positive integer. Let

$$d\mathbb{Z} = \{\ldots, -4d, -3d, -2d, -d, 0, d, 2d, 3d, 4d, \ldots\}$$

Then $(d\mathbb{Z}, +)$ is a group. It's a subset of $\mathbb{Z}$, so we'll be calling this a subgroup before too long.

Let me look at the first two non-trivial examples. It's easy to check that there are both groups, with 0 as the identity and the obvious elements as inverses.

$$2\mathbb{Z} = \{\ldots, -8, -6, -4, -2, 0, 2, 4, 6, 8, \ldots\},$$
$$3\mathbb{Z} = \{\ldots, -12, -9, -6, -3, 0, 3, 6, 9, 12, \ldots\}.$$

I want to mention a few other infinite groups here, because we'll look at them later. First, suppose $d \in \mathbb{N}$ is a positive integer. Let

$$d\mathbb{Z} = \{\ldots, -4d, -3d, -2d, -d, 0, d, 2d, 3d, 4d, \ldots\}$$

Then $(d\mathbb{Z}, +)$ is a group. It's a subset of $\mathbb{Z}$, so we'll be calling this a subgroup before too long.

Let me look at the first two non-trivial examples. It's easy to check that there are both groups, with 0 as the identity and the obvious elements as inverses.

$$2\mathbb{Z} = \{\ldots, -8, -6, -4, -2, 0, 2, 4, 6, 8, \ldots\},$$
$$3\mathbb{Z} = \{\ldots, -12, -9, -6, -3, 0, 3, 6, 9, 12, \ldots\}.$$

Is $(G_1, *) := (2\mathbb{Z}, +) \cup (3\mathbb{Z}, +)$ a group? No, and for a strange reason. Our definition of the binary operation requires that $x * y \in G_1$. This is what fails here! We have $-2 \in (2\mathbb{Z}, +)$ and $3 \in (3\mathbb{Z}, +)$, but $-2 + 3 = 1$ is not in $(2\mathbb{Z}, +) \cup (3\mathbb{Z}, +)$.

Intersections, on the other hand, will always be a group. Let $(G_2, *) = (2\mathbb{Z}, +) \cap (3\mathbb{Z}, +)$. We'll show before too long that this intersection is precisely $(6\mathbb{Z}, +)$, and more generally,

$$(m\mathbb{Z}, +) \cap (n\mathbb{Z}, +) = (LCM(m, n)\mathbb{Z}, +),$$

where $LCM(m, n)$ denotes the least common multiple of m and n.

Intersections, on the other hand, will always be a group. Let $(G_2, *) = (2\mathbb{Z}, +) \cap (3\mathbb{Z}, +)$. We'll show before too long that this intersection is precisely $(6\mathbb{Z}, +)$, and more generally,

$$(m\mathbb{Z}, +) \cap (n\mathbb{Z}, +) = (LCM(m, n)\mathbb{Z}, +),$$

where $LCM(m, n)$ denotes the least common multiple of m and n.

One more infinite group. This is called $\mathbb{Z} \oplus \mathbb{Z}$. The elements are (m, n) where $m, n \in \mathbb{Z}$ and the operation is component-wise addition; that is,

$$(m_1, n_1) * (m_2, n_2) = (m_1 + m_2, n_1 + n_2).$$

You should be able to check that the identity element is (0,0), that the inverse of (m, n) is $(-m, -n)$ and that $*$ is associative.

Time to do some number theory. Based on class Monday, I think this should all be review. (Let me know if I'm wrong.) We'll be working with $\mathbb{Z}$ here.

Time to do some number theory. Based on class Monday, I think this should all be review. (Let me know if I'm wrong.) We'll be working with $\mathbb{Z}$ here.

Suppose $m, n \in \mathbb{Z}$, $m \neq 0$. We say that $m \mid n$ (or m is a *divisor* or a *factor* of n or n is a *multiple* of m) if there exists $t \in \mathbb{Z}$ so that $n = mt$, or equivalently if $\frac{n}{m} \in \mathbb{Z}$. Even though $0 \mid n$ is impossible, it is always the case that if $m \neq 0$, then $m \mid 0$, because $0 = m \cdot 0$. For example, $417 = 3 \cdot 139$; divisors of 417 are 1, 3, 139, and 417.

Time to do some number theory. Based on class Monday, I think this should all be review. (Let me know if I'm wrong.) We'll be working with $\mathbb{Z}$ here.

Suppose $m, n \in \mathbb{Z}$, $m \neq 0$. We say that $m \mid n$ (or m is a *divisor* or a *factor* of n or n is a *multiple* of m) if there exists $t \in \mathbb{Z}$ so that $n = mt$, or equivalently if $\frac{n}{m} \in \mathbb{Z}$. Even though $0 \mid n$ is impossible, it is always the case that if $m \neq 0$, then $m \mid 0$, because $0 = m \cdot 0$. For example, $417 = 3 \cdot 139$; divisors of 417 are 1, 3, 139, and 417.

Suppose $d \in \mathbb{N}$, $d \geq 2$ and $m, n \in \mathbb{Z}$. The notation

$$m \equiv n \mod d$$

means that $d \mid n - m$, or $n - m = dt$ for some integer t or, equivalently $n = m + dt$ or $m = n - dt$.

THEOREM 3: If $n \in \mathbb{Z}$ and $d \in \mathbb{N}$, then there is a unique integer $r \in \{0, 1, \ldots, d-1\}$ so that $n \equiv r \mod d$.

THEOREM 3: If $n \in \mathbb{Z}$ and $d \in \mathbb{N}$, then there is a unique integer $r \in \{0, 1, \ldots, d-1\}$ so that $n \equiv r \mod d$.

PROOF: Use the division algorithm; divide n by d with remainder r. To be precise, let $t = \lfloor \frac{n}{d} \rfloor$, the largest integer $\leq \frac{n}{d}$. Then

$$t \leq \frac{n}{d} < t+1 \implies dt \leq n < dt + d \implies 0 \leq n - dt < d$$

so $n - dt = r$ for some $r \in \{0, 1, \ldots, d-1\}$, and so $n \equiv r \mod d$.

THEOREM 3: If $n \in \mathbb{Z}$ and $d \in \mathbb{N}$, then there is a unique integer $r \in \{0, 1, \ldots, d-1\}$ so that $n \equiv r \mod d$.

PROOF: Use the division algorithm; divide n by d with remainder r. To be precise, let $t = \lfloor \frac{n}{d} \rfloor$, the largest integer $\leq \frac{n}{d}$. Then

$$t \leq \frac{n}{d} < t+1 \implies dt \leq n < dt + d \implies 0 \leq n - dt < d$$

so $n - dt = r$ for some $r \in \{0, 1, \ldots, d-1\}$, and so $n \equiv r \mod d$.

Why is r unique? Suppose $n = dt_1 + r_1$ and $n = dt_2 + r_2$ and $r_1, r_2 \in \{0, 1, \ldots, d-1\}$. Subtract the two equations for n to get $0 = d(t_1 - t_2) + (r_1 - r_2)$, so that $r_1 - r_2 = d(t_2 - t_1)$ is a multiple of d. But $-(d-1) \leq r_1 - r_2 \leq d - 1$, and the only multiple of d in $\{-(d-1), \ldots, d-1\}$ is 0, so $r_1 - r_2 = 0$ and $r_1 = r_2$ and $t_1 = t_2$. □

When $d = 1$, $r = 0$ and this is a boring case we ignore.

When $d = 1$, $r = 0$ and this is a boring case we ignore.

Let's look at this for $d = 2$. I will write $\mathbb{Z}$ and put the elements $\equiv 0 \mod 2$ in red, and the elements $\equiv 1 \mod 2$ in blue. Notice that this is unambiguous. The red elements are the even integers and the blue elements are the odds.

$$\{\ldots, -4, -3, -2, -1, 0, 1, 2, 3, 4, \ldots\}$$

When $d = 1$, $r = 0$ and this is a boring case we ignore.

Let's look at this for $d = 2$. I will write $\mathbb{Z}$ and put the elements $\equiv 0 \mod 2$ in red, and the elements $\equiv 1 \mod 2$ in blue. Notice that this is unambiguous. The red elements are the even integers and the blue elements are the odds.

$$\{\ldots, -4, -3, -2, -1, 0, 1, 2, 3, 4, \ldots\}$$

Now for $d = 3$, I'll write these out in three rows:

$$\begin{aligned}
0 \mod 3 &= \{\ldots, -12, -9, -6, -3, 0, 3, 6, 9 \ldots\}, \\
1 \mod 3 &= \{\ldots, -11, -8, -5, -2, 1, 4, 7, 10 \ldots\}, \\
2 \mod 3 &= \{\ldots, -10, -7, -4, -1, 2, 5, 8, 11 \ldots\},
\end{aligned}$$

When $d = 1$, $r = 0$ and this is a boring case we ignore.

Let's look at this for $d = 2$. I will write $\mathbb{Z}$ and put the elements $\equiv 0 \mod 2$ in red, and the elements $\equiv 1 \mod 2$ in blue. Notice that this is unambiguous. The red elements are the even integers and the blue elements are the odds.

$$\{\ldots, -4, -3, -2, -1, 0, 1, 2, 3, 4, \ldots\}$$

Now for $d = 3$, I'll write these out in three rows:

$$\begin{aligned}
0 \mod 3 &= \{\ldots, -12, -9, -6, -3, 0, 3, 6, 9 \ldots\}, \\
1 \mod 3 &= \{\ldots, -11, -8, -5, -2, 1, 4, 7, 10 \ldots\}, \\
2 \mod 3 &= \{\ldots, -10, -7, -4, -1, 2, 5, 8, 11 \ldots\},
\end{aligned}$$

I hope you can imagine these as forming a *partition* of $\mathbb{Z}$; that is, every integer is in exactly one of these sets.

I now want to formalize this with another bit of notation. First reach back into Math 347 for the definition of equivalence relation and equivalence classes.

I now want to formalize this with another bit of notation. First reach back into Math 347 for the definition of equivalence relation and equivalence classes.

LEMMA The condition $a \sim b \iff a \equiv b \mod d$ forms an equivalence relation.

I now want to formalize this with another bit of notation. First reach back into Math 347 for the definition of equivalence relation and equivalence classes.

LEMMA The condition $a \sim b \iff a \equiv b \mod d$ forms an equivalence relation.

PROOF. We have three things to check. First: is $a \equiv a \mod d$? Yes, because d always divides $a - a = 0$. Second, suppose $a \equiv b \mod d$. Is $b \equiv a \mod d$? Sure. We have $d \mid b - a$, so $b - a = dt$ for some integer t and so $a - b = d(-t)$ and $-t \in \mathbb{Z}$, so $b \equiv a \mod d$. Finally, suppose $a \equiv b \mod d$ and $b \equiv c \mod d$. Then $b - a = dt$ and $c - b = du$ for integers t and u. If we add these, we get that $c - a = (b - a) + (c - b) = d(t + u)$, so $a \equiv c \mod d$. $\square$

So now, suppose $d \in \mathbb{N}$, and $a \in \mathbb{Z}$. We define $[a]_d$ to be

$$\{n \in \mathbb{Z} \mid n \equiv a \mod d\} = \{a + dt \mid t \in \mathbb{Z}\} = a + d\mathbb{Z}.$$

So now, suppose $d \in \mathbb{N}$, and $a \in \mathbb{Z}$. We define $[a]_d$ to be

$$\{n \in \mathbb{Z} \mid n \equiv a \mod d\} = \{a + dt \mid t \in \mathbb{Z}\} = a + d\mathbb{Z}.$$

If $a \equiv b \mod d$, then $[a]_d = [b]_d$, because it's an equivalence relation. We often say that $[a]_d$ is the set of integers *congruent to a mod d*.

So now, suppose $d \in \mathbb{N}$, and $a \in \mathbb{Z}$. We define $[a]_d$ to be

$$\{n \in \mathbb{Z} \mid n \equiv a \mod d\} = \{a + dt \mid t \in \mathbb{Z}\} = a + d\mathbb{Z}.$$

If $a \equiv b \mod d$, then $[a]_d = [b]_d$, because it's an equivalence relation. We often say that $[a]_d$ is the set of integers *congruent to a mod d*.

Theorem 3 can now be rephrased as saying that for all d,

$$\mathbb{Z} = [0]_d \cup [1]_d \cup \cdots \cup [d-1]_d$$

We saw this fact earlier for $d = 2$ and $d = 3$.

The next theorem is critical for our work and the method of proof is a very useful one which is rarely taught explicitly. If you want to prove something, it is often helpful to take one of your hypotheses and parameterize it.

The next theorem is critical for our work and the method of proof is a very useful one which is rarely taught explicitly. If you want to prove something, it is often helpful to take one of your hypotheses and parameterize it.

THEOREM 4: Suppose $a_1, a_2, b_1, b_2 \in \mathbb{Z}$, $d \in \mathbb{N}$ with $d \geq 2$. Then

$$a_1 \equiv a_2 \mod d \quad \textbf{and} \quad b_1 \equiv b_2 \mod d \implies$$
$$a_1 + b_1 \equiv a_2 + b_2 \mod d \quad \textbf{and} \quad a_1 b_1 \equiv a_2 b_2 \mod d.$$

The next theorem is critical for our work and the method of proof is a very useful one which is rarely taught explicitly. If you want to prove something, it is often helpful to take one of your hypotheses and parameterize it.

THEOREM 4: Suppose $a_1, a_2, b_1, b_2 \in \mathbb{Z}$, $d \in \mathbb{N}$ with $d \geq 2$. Then

$$a_1 \equiv a_2 \mod d \quad \textbf{and} \quad b_1 \equiv b_2 \mod d \implies$$
$$a_1 + b_1 \equiv a_2 + b_2 \mod d \quad \textbf{and} \quad a_1 b_1 \equiv a_2 b_2 \mod d.$$

PROOF: We can write $a_2 = a_1 + dt$ and $b_2 = b_1 + du$ for some $t, u \in \mathbb{Z}$. Then

$$(a_2 + b_2) - (a_1 + b_1) = a_1 + dt + b_1 + du - (a_1 + b_1) = d(t + u);$$
$$a_2 b_2 - a_1 b_1 = (a_1 + dt)(b_1 + du) - a_1 b_1 =$$
$$a_1 b_1 + a_1 du + b_1 dt + d^2 tu - a_1 b_1 = d(a_1 u + b_1 t + dtu),$$

so the difference in each case is a multiple of d, and the claimed congruence equations are true.

Why is this important? We now define the set

Why is this important? We now define the set

$$\mathbb{Z}/d\mathbb{Z} = \{[0]_d, [1]_d, \ldots, [d-1]_d\}.$$

Why is this important? We now define the set

$$\mathbb{Z}/d\mathbb{Z} = \{[0]_d, [1]_d, \ldots, [d-1]_d\}.$$

This is a set with d elements, each element is an infinite set. The union of these elements is all of $\mathbb{Z}$, but remember that $\mathbb{Z}/d\mathbb{Z}$ is a finite set. For example

$$\mathbb{Z}/2\mathbb{Z} = \{[0]_2, [1]_2\} = \{\text{even integers, odd integers}\}.$$

Why is this important? We now define the set

$$\mathbb{Z}/d\mathbb{Z} = \{[0]_d, [1]_d, \ldots, [d-1]_d\}.$$

This is a set with d elements, each element is an infinite set. The union of these elements is all of $\mathbb{Z}$, but remember that $\mathbb{Z}/d\mathbb{Z}$ is a finite set. For example

$$\mathbb{Z}/2\mathbb{Z} = \{[0]_2, [1]_2\} = \{\text{even integers, odd integers}\}.$$

The point of the theorem is that we can now define two binary operations of addition and multiplication on $\mathbb{Z}/d\mathbb{Z}$ by

$$[a]_d \oplus [b]_d = [a+b]_d, \qquad [a]_d \odot [b]_d = [ab]_d.$$

Why is this important? We now define the set

$$\mathbb{Z}/d\mathbb{Z} = \{[0]_d, [1]_d, \ldots, [d-1]_d\}.$$

This is a set with d elements, each element is an infinite set. The union of these elements is all of $\mathbb{Z}$, but remember that $\mathbb{Z}/d\mathbb{Z}$ is a finite set. For example

$$\mathbb{Z}/2\mathbb{Z} = \{[0]_2, [1]_2\} = \{\text{even integers, odd integers}\}.$$

The point of the theorem is that we can now define two binary operations of addition and multiplication on $\mathbb{Z}/d\mathbb{Z}$ by

$$[a]_d \oplus [b]_d = [a+b]_d, \qquad [a]_d \odot [b]_d = [ab]_d.$$

This is a subtle point. We have $[a]_d = [a+d]_d = [a-417d]_d$ etc. The set can be given with lot of different names, but it doesn't matter when we are doing the operations, because the sums and the products will always be the same, no matter what name you use.

THEOREM 5. For any $d \geq 2$, $(\mathbb{Z}/d\mathbb{Z}, \oplus)$ is a group.

THEOREM 5. For any $d \geq 2$, $(\mathbb{Z}/d\mathbb{Z}, \oplus)$ is a group.

PROOF. We have the group and the operation. And from the definition,

$$[a]_d \oplus [0]_d = [a+0]_d = [a]_d,$$

so $[0]_d$ is the identity element. Further,

THEOREM 5. For any $d \geq 2$, $(\mathbb{Z}/d\mathbb{Z}, \oplus)$ is a group.

PROOF. We have the group and the operation. And from the definition,

$$[a]_d \oplus [0]_d = [a+0]_d = [a]_d,$$

so $[0]_d$ is the identity element. Further,

$$[a]_d \oplus [-a]_d = [a-a]_d = [0]_d,$$

so every element $[a]_d$ has the inverse $[-a]_d$. Finally,

THEOREM 5. For any $d \geq 2$, $(\mathbb{Z}/d\mathbb{Z}, \oplus)$ is a group.

PROOF. We have the group and the operation. And from the definition,

$$[a]_d \oplus [0]_d = [a+0]_d = [a]_d,$$

so $[0]_d$ is the identity element. Further,

$$[a]_d \oplus [-a]_d = [a-a]_d = [0]_d,$$

so every element $[a]_d$ has the inverse $[-a]_d$. Finally,

$$([a]_d \oplus [b]_d) \oplus [c]_d = [a+b]_d \oplus [c]_d = [a+b+c]_d$$
$$[a]_d \oplus ([b]_d \oplus [c]_d) = [a]_d \oplus [b+c]_d = [a+b+c]_d$$

so associativity holds. □

THEOREM 5. For any $d \geq 2$, $(\mathbb{Z}/d\mathbb{Z}, \oplus)$ is a group.

PROOF. We have the group and the operation. And from the definition,

$$[a]_d \oplus [0]_d = [a+0]_d = [a]_d,$$

so $[0]_d$ is the identity element. Further,

$$[a]_d \oplus [-a]_d = [a-a]_d = [0]_d,$$

so every element $[a]_d$ has the inverse $[-a]_d$. Finally,

$$([a]_d \oplus [b]_d) \oplus [c]_d = [a+b]_d \oplus [c]_d = [a+b+c]_d$$
$$[a]_d \oplus ([b]_d \oplus [c]_d) = [a]_d \oplus [b+c]_d = [a+b+c]_d$$

so associativity holds. □

Remember here $+$ is addition in $\mathbb{Z}$ and $\oplus$ is addition in $\mathbb{Z}/d\mathbb{Z}$.

I will finish up with the group table for $\mathbb{Z}/4\mathbb{Z}$. It will look familiar.

I will finish up with the group table for $\mathbb{Z}/4\mathbb{Z}$. It will look familiar.

$\oplus$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[0]_4$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[1]_4$	$[1]_4$	$[2]_4$	$[3]_4$	$[0]_4$
$[2]_4$	$[2]_4$	$[3]_4$	$[0]_4$	$[1]_4$
$[3]_4$	$[3]_4$	$[0]_4$	$[1]_4$	$[2]_4$

Yes, this is our old friend C_4.

I will finish up with the group table for $\mathbb{Z}/4\mathbb{Z}$. It will look familiar.

$\oplus$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[0]_4$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[1]_4$	$[1]_4$	$[2]_4$	$[3]_4$	$[0]_4$
$[2]_4$	$[2]_4$	$[3]_4$	$[0]_4$	$[1]_4$
$[3]_4$	$[3]_4$	$[0]_4$	$[1]_4$	$[2]_4$

Yes, this is our old friend C_4.

So, for example $[3]_4 \oplus [2]_4 = [5]_4 = [1]_4$. After today, when d is understood, we'll write "$[a]_d$" as "a" to simplify things. It saves me four extra characters in LaTeX!

One last thought. Multiplication? We can write out the binary operation

One last thought. Multiplication? We can write out the binary operation

$\odot$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[0]_4$	$[0]_4$	$[0]_4$	$[0]_4$	$[0]_4$
$[1]_4$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[2]_4$	$[0]_4$	$[2]_4$	$[0]_4$	$[2]_4$
$[3]_4$	$[0]_4$	$[3]_4$	$[2]_4$	$[1]_4$.

One last thought. Multiplication? We can write out the binary operation

$\odot$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[0]_4$	$[0]_4$	$[0]_4$	$[0]_4$	$[0]_4$
$[1]_4$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[2]_4$	$[0]_4$	$[2]_4$	$[0]_4$	$[2]_4$
$[3]_4$	$[0]_4$	$[3]_4$	$[2]_4$	$[1]_4$.

This is not a group! Even though $[1]_4$ is an identity element, neither $[0]_4$ nor $[2]_4$ has an inverse.

One last thought. Multiplication? We can write out the binary operation

$\odot$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[0]_4$	$[0]_4$	$[0]_4$	$[0]_4$	$[0]_4$
$[1]_4$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[2]_4$	$[0]_4$	$[2]_4$	$[0]_4$	$[2]_4$
$[3]_4$	$[0]_4$	$[3]_4$	$[2]_4$	$[1]_4$.

This is not a group! Even though $[1]_4$ is an identity element, neither $[0]_4$ nor $[2]_4$ has an inverse.

What do you think happens with $(\{[1]_4, [3]_4\}, \odot)$?

One last thought. Multiplication? We can write out the binary operation

$\odot$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[0]_4$	$[0]_4$	$[0]_4$	$[0]_4$	$[0]_4$
$[1]_4$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[2]_4$	$[0]_4$	$[2]_4$	$[0]_4$	$[2]_4$
$[3]_4$	$[0]_4$	$[3]_4$	$[2]_4$	$[1]_4$.

This is not a group! Even though $[1]_4$ is an identity element, neither $[0]_4$ nor $[2]_4$ has an inverse.

What do you think happens with $(\{[1]_4, [3]_4\}, \odot)$?

Tune in on Friday.

And remember your job!

And remember your job!

Email me any questions you might have on this presentation, so I can talk about them in class on Wednesday.