Math 417 – Third Day – Class

Bruce Reznick
University of Illinois at Urbana-Champaign

August 28, 2020

First. How to view cyclic groups. One was is formally. Suppose $G = C_6$, the cyclic group of order 6. Then the elements of G are e, g, g^2, g^3, g^4, g^5 and $g^6 = e$.

First. How to view cyclic groups. One was is formally. Suppose $G = C_6$, the cyclic group of order 6. Then the elements of G are e, g, g^2, g^3, g^4, g^5 and $g^6 = e$.
What happens when you look at $g^3 * g^5$, for example? Because of associativity, we don't have to think about how we group the elements

$$(g * g * g) * (g * g * g * g * g)$$

First. How to view cyclic groups. One was is formally. Suppose $G = C_6$, the cyclic group of order 6. Then the elements of G are e, g, g^2, g^3, g^4, g^5 and $g^6 = e$.
What happens when you look at $g^3 * g^5$, for example? Because of associativity, we don't have to think about how we group the elements

$$(g * g * g) * (g * g * g * g * g)$$
$$= g * g * g * g * g * g * g * g$$

First. How to view cyclic groups. One was is formally. Suppose $G = C_6$, the cyclic group of order 6. Then the elements of G are e, g, g^2, g^3, g^4, g^5 and $g^6 = e$.

What happens when you look at $g^3 * g^5$, for example? Because of associativity, we don't have to think about how we group the elements

$$\begin{aligned}(g * g * g) * (g * g * g * g * g) \\ = g * g * g * g * g * g * g * g \\ = g * g * g * g * g * g * g * g\end{aligned}$$

First. How to view cyclic groups. One was is formally. Suppose $G = C_6$, the cyclic group of order 6. Then the elements of G are e, g, g^2, g^3, g^4, g^5 and $g^6 = e$.

What happens when you look at $g^3 * g^5$, for example? Because of associativity, we don't have to think about how we group the elements

$$\begin{aligned}
&(g * g * g) * (g * g * g * g * g) \\
&= g * g * g * g * g * g * g * g \\
&= g * g * g * g * g * g * g * g \\
&= (g * g * g * g * g * g) * g * g
\end{aligned}$$

First. How to view cyclic groups. One was is formally. Suppose $G = C_6$, the cyclic group of order 6. Then the elements of G are e, g, g^2, g^3, g^4, g^5 and $g^6 = e$.
What happens when you look at $g^3 * g^5$, for example? Because of associativity, we don't have to think about how we group the elements

$$\begin{aligned}
&(g * g * g) * (g * g * g * g * g) \\
&= g * g * g * g * g * g * g * g \\
&= g * g * g * g * g * g * g * g \\
&= (g * g * g * g * g * g) * g * g \\
&= e * g * g = g^2
\end{aligned}$$

Or, you can think of a C_6 as the rotations of a regular hexagon, where g is clockwise rotation by $\frac{2\pi}{6} = 60$ degrees. Then g^k is rotation by $60 \cdot k$ degrees. So g^3 is rotation by 180 degrees and g^5 is rotation by 300 degrees, so $g^3 * g^5 = g^8$ is rotation by 480 degrees, but g^6 is rotation by 360 degrees, which is like doing nothing, so the net effect is rotation by $480 - 360 = 120$ degrees.

Another way to do this is to think of the cyclic group of order 6 as addition mod 6, and then $3 + 5 = 8 \equiv 2 \mod 6$.

Another way to do this is to think of the cyclic group of order 6 as addition mod 6, and then $3 + 5 = 8 \equiv 2 \mod 6$.

You could also think of an elaborate 6×6 multiplication table, which might take me 10 minutes to write, so think of those southwest to northeast diagonals.

I want to do the isomorphism argument from C_4 to V again. I'll bring back what I wrote:.The elements of C_4 are $\{e, g, g^2, g^3\}$; the elements of V are $\{I, X, Y, Z\}$.

I want to do the isomorphism argument from C_4 to V again. I'll bring back what I wrote:.The elements of C_4 are $\{e, g, g^2, g^3\}$; the elements of V are $\{I, X, Y, Z\}$.
Here are their multiplication tables, which we've seen before.

I want to do the isomorphism argument from C_4 to V again. I'll bring back what I wrote:.The elements of C_4 are $\{e, g, g^2, g^3\}$; the elements of V are $\{I, X, Y, Z\}$.
Here are their multiplication tables, which we've seen before.

$*_1$	e	g	g^2	g^3
e	e	g	g^2	g^3
g	g	g^2	g^3	e
g^2	g^2	g^3	e	g
g^3	g^3	e	g	g^2

$*_2$	I	X	Y	Z
I	I	X	Y	Z
X	X	I	Z	Y
Y	Y	Z	I	X
Z	Z	Y	X	I

I want to do the isomorphism argument from C_4 to V again. I'll bring back what I wrote:.The elements of C_4 are $\{e, g, g^2, g^3\}$; the elements of V are $\{I, X, Y, Z\}$.
Here are their multiplication tables, which we've seen before.

$*_1$	e	g	g^2	g^3
e	e	g	g^2	g^3
g	g	g^2	g^3	e
g^2	g^2	g^3	e	g
g^3	g^3	e	g	g^2

$*_2$	I	X	Y	Z
I	I	X	Y	Z
X	X	I	Z	Y
Y	Y	Z	I	X
Z	Z	Y	X	I

Suppose Φ is the isomorphism map. We have by definition for all i,

$$\Phi(g^i) = \Phi(e *_1 g^i) = \Phi(e) *_2 \Phi(g^i),$$

so $\Phi(e)$ has to be the identity element in V and so $\Phi(e) = I$.

Remember that Φ is a bijection on the elements of C_4 and V, so $\{\Phi(g), \Phi(g^2), \Phi(g^3)\} = \{X, Y, Z\}$. Since Φ is an isomorphism, we have three cases: $\Phi(g) = X$, $\Phi(g) = Y$ and $\Phi(g) = Z$.

Remember that Φ is a bijection on the elements of C_4 and V, so $\{\Phi(g), \Phi(g^2), \Phi(g^3)\} = \{X, Y, Z\}$. Since Φ is an isomorphism, we have three cases: $\Phi(g) = X$, $\Phi(g) = Y$ and $\Phi(g) = Z$.

$$\Phi(g) = X \implies$$

$$\Phi(g^2) = \Phi(g *_1 g) = \Phi(g) *_2 \Phi(g) = X *_2 X = I = \Phi(e),$$

Remember that Φ is a bijection on the elements of C_4 and V, so $\{\Phi(g), \Phi(g^2), \Phi(g^3)\} = \{X, Y, Z\}$. Since Φ is an isomorphism, we have three cases: $\Phi(g) = X$, $\Phi(g) = Y$ and $\Phi(g) = Z$.

$$\Phi(g) = X \implies$$

$$\Phi(g^2) = \Phi(g *_1 g) = \Phi(g) *_2 \Phi(g) = X *_2 X = I = \Phi(e),$$

$$\Phi(g) = Y \implies$$

$$\Phi(g^2) = \Phi(g *_1 g) = \Phi(g) *_2 \Phi(g) = Y *_2 Y = I = \Phi(e),$$

Remember that Φ is a bijection on the elements of C_4 and V, so $\{\Phi(g), \Phi(g^2), \Phi(g^3)\} = \{X, Y, Z\}$. Since Φ is an isomorphism, we have three cases: $\Phi(g) = X$, $\Phi(g) = Y$ and $\Phi(g) = Z$.

$$\Phi(g) = X \implies$$
$$\Phi(g^2) = \Phi(g *_1 g) = \Phi(g) *_2 \Phi(g) = X *_2 X = I = \Phi(e),$$
$$\Phi(g) = Y \implies$$
$$\Phi(g^2) = \Phi(g *_1 g) = \Phi(g) *_2 \Phi(g) = Y *_2 Y = I = \Phi(e),$$
$$\Phi(g) = Z \implies$$
$$\Phi(g^2) = \Phi(g *_1 g) = \Phi(g) *_2 \Phi(g) = Z *_2 Z = I = \Phi(e)$$

Remember that Φ is a bijection on the elements of C_4 and V, so $\{\Phi(g), \Phi(g^2), \Phi(g^3)\} = \{X, Y, Z\}$. Since Φ is an isomorphism, we have three cases: $\Phi(g) = X$, $\Phi(g) = Y$ and $\Phi(g) = Z$.

$$\Phi(g) = X \implies$$
$$\Phi(g^2) = \Phi(g *_1 g) = \Phi(g) *_2 \Phi(g) = X *_2 X = I = \Phi(e),$$
$$\Phi(g) = Y \implies$$
$$\Phi(g^2) = \Phi(g *_1 g) = \Phi(g) *_2 \Phi(g) = Y *_2 Y = I = \Phi(e),$$
$$\Phi(g) = Z \implies$$
$$\Phi(g^2) = \Phi(g *_1 g) = \Phi(g) *_2 \Phi(g) = Z *_2 Z = I = \Phi(e).$$

There is no way to define $\Phi(g)$ that works and so there is no isomorphism.

The last thing that seemed confusing to several was proving that $D(m) \cap D(n) = D(m) \cap D(n - km)$.

The last thing that seemed confusing to several was proving that $D(m) \cap D(n) = D(m) \cap D(n - km)$.

Suppose $d \in D(m) \cap D(n)$. Then $d \mid m$ and $d \mid n$, so $m = dt$ and $n = du$ and $n - km = d(u - kt)$, so $d \mid n - km$. Thus $D(m) \cap D(n) \subseteq D(m) \cap D(n - km)$.

The last thing that seemed confusing to several was proving that $D(m) \cap D(n) = D(m) \cap D(n - km)$.

Suppose $d \in D(m) \cap D(n)$. Then $d \mid m$ and $d \mid n$, so $m = dt$ and $n = du$ and $n - km = d(u - kt)$, so $d \mid n - km$. Thus $D(m) \cap D(n) \subseteq D(m) \cap D(n - km)$.

In the other direction, suppose $d \in D(m) \cap D(n - km)$. Then, again, $d \mid m$, but also $d \mid n - km$. We have $m = dt$ and $n - mk = dv$, so $n = (n - mk) + km = d(v + kt)$, so the other inclusion holds: $D(m) \cap D(n - km) \subseteq D(m) \cap D(n)$. Thus the two sets are equal.

The last thing that seemed confusing to several was proving that $D(m) \cap D(n) = D(m) \cap D(n - km)$.

Suppose $d \in D(m) \cap D(n)$. Then $d \mid m$ and $d \mid n$, so $m = dt$ and $n = du$ and $n - km = d(u - kt)$, so $d \mid n - km$. Thus $D(m) \cap D(n) \subseteq D(m) \cap D(n - km)$.

In the other direction, suppose $d \in D(m) \cap D(n - km)$. Then, again, $d \mid m$, but also $d \mid n - km$. We have $m = dt$ and $n - mk = dv$, so $n = (n - mk) + km = d(v + kt)$, so the other inclusion holds: $D(m) \cap D(n - km) \subseteq D(m) \cap D(n)$. Thus the two sets are equal.

Let $A = D(m)$, $B = D(n)$ and $C = D(n - km)$. The logic is that if $x \in A \cap B$, then $x \in A, x \in B$. Work implies that $x \in C$, so $x \in A \cap C$, and this means formally that $A \cap B \subseteq A \cap C$. Similarly, if $x \in A \cap C$, then $x \in B$ so $x \in A \cap B$ and $A \cap C \subseteq A \cap B$ so $A \cap B = A \cap C$.

A return to the Euclidean algorithm. We'll prove a surprisingly important result on Monday: if $gcd(m, n) = g$, then there exist integers r, s so that $g = rm + ns$. Recall:

A return to the Euclidean algorithm. We'll prove a surprisingly important result on Monday: if $gcd(m, n) = g$, then there exist integers r, s so that $g = rm + ns$. Recall:

$$417 = 34 \cdot 12 + 9,$$
$$12 = 1 \cdot 9 + 3,$$
$$9 = 3 \cdot 3,$$

A return to the Euclidean algorithm. We'll prove a surprisingly important result on Monday: if $gcd(m, n) = g$, then there exist integers r, s so that $g = rm + ns$. Recall:

$$417 = 34 \cdot 12 + 9,$$
$$12 = 1 \cdot 9 + 3,$$
$$9 = 3 \cdot 3,$$

We have $gcd(12, 417) = 3$, and we want to write 3 as a linear combination of 12 and 417. First, $3 = 12 - 1 \cdot 9$. Then, $9 = 417 - 34 \cdot 12$, so

$$3 = 12 - 1 \cdot (417 - 34 \cdot 12) = 35 \cdot 12 - 417 = 420 - 417.$$

A return to the Euclidean algorithm. We'll prove a surprisingly important result on Monday: if $gcd(m, n) = g$, then there exist integers r, s so that $g = rm + ns$. Recall:

$$417 = 34 \cdot 12 + 9,$$
$$12 = 1 \cdot 9 + 3,$$
$$9 = 3 \cdot 3,$$

We have $gcd(12, 417) = 3$, and we want to write 3 as a linear combination of 12 and 417. First, $3 = 12 - 1 \cdot 9$. Then, $9 = 417 - 34 \cdot 12$, so

$$3 = 12 - 1 \cdot (417 - 34 \cdot 12) = 35 \cdot 12 - 417 = 420 - 417.$$

The same thing works in general. We have $x_{n-1} = c_{n-1}x_n + x_{n+1}$, so this gives the x_{n+1} the gcd, in terms of x_{n-1} and x_n. But also $x_{n-2} = c_{n-2}x_{n-1} + x_n$, so we have x_n in terms of x_{n-2} and x_{n-1}; plug it in to get x_{n+1} in terms of x_{n-2} and x_{n-1}. You just work your way back up the ladder.

I did a pathetic job of explaining this on Whiteboard; here's a better version. We define $(\mathbb{Z}/d\mathbb{Z})^*$ to be the set of integers a in $\{1, \ldots, d-1\}$ which are relatively prime to d, and then we're going to show that this is a group under $\odot$.

I did a pathetic job of explaining this on Whiteboard; here's a better version. We define $(\mathbb{Z}/d\mathbb{Z})^*$ to be the set of integers a in $\{1, \ldots, d-1\}$ which are relatively prime to d, and then we're going to show that this is a group under $\odot$.

Let $d = 12$, so $a \in \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$ and $D(12) = \{1, 2, 3, 4, 6, 12\}$. Notice that 2 divides 12 and $\{2, 4, 6, 8, 10\}$ and 3 divides 12 and $\{3, 6, 9\}$ and this leaves $(\mathbb{Z}/12\mathbb{Z})^* = \{1, 5, 7, 11\}$.

I did a pathetic job of explaining this on Whiteboard; here's a better version. We define $(\mathbb{Z}/d\mathbb{Z})^*$ to be the set of integers a in $\{1, \ldots, d-1\}$ which are relatively prime to d, and then we're going to show that this is a group under $\odot$.

Let $d = 12$, so $a \in \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$ and $D(12) = \{1, 2, 3, 4, 6, 12\}$. Notice that 2 divides 12 and $\{2, 4, 6, 8, 10\}$ and 3 divides 12 and $\{3, 6, 9\}$ and this leaves $(\mathbb{Z}/12\mathbb{Z})^* = \{1, 5, 7, 11\}$.

We have $5 \cdot 5 = 25 \equiv 1 \mod 12$, $5 \cdot 7 = 35 \equiv 11 \mod 12$, $5 \cdot 11 = 55 \equiv 7 \mod 12$, $7 \cdot 7 = 49 \equiv 1 \mod 12$, $7 \cdot 11 = 77 \equiv 5 \mod 12$, $11 \cdot 11 = 121 \equiv 1 \mod 12$, so, on the next page:

Here is the multiplication table for $(\mathbb{Z}/12\mathbb{Z})^*$, where the elements are to be technical, $[1]_{12}$, $[5]_{12}$, $[7]_{12}$, $[11]_{12}$.

Here is the multiplication table for $(\mathbb{Z}/12\mathbb{Z})^*$, where the elements are to be technical, $[1]_{12}$, $[5]_{12}$, $[7]_{12}$, $[11]_{12}$.

$\odot$	$[1]_{12}$	$[5]_{12}$	$[7]_{12}$	$[11]_{12}$
$[1]_{12}$	$[1]_{12}$	$[5]_{12}$	$[7]_{12}$	$[11]_{12}$
$[5]_{12}$	$[5]_{12}$	$[1]_{12}$	$[11]_{12}$	$[7]_{12}$
$[7]_{12}$	$[7]_{12}$	$[11]_{12}$	$[1]_{12}$	$[5]_{12}$
$[11]_{12}$	$[11]_{12}$	$[7]_{12}$	$[5]_{12}$	$[1]_{12}$

I hope you can see that this is isomorphic to one of our popular groups!