

# Math 417 – Sixth Day – Class

Bruce Reznick  
University of Illinois at Urbana-Champaign

September 4, 2020

I've gotten some requests to talk about isomorphisms, and first, an apology. The letter commonly used for the function is  $\Phi$ , and some were trying to connect it to the Euler phi function uses the lower-case version  $\phi$ . There is *no* connection between the two. I'm sorry if this was confusing!

I've gotten some requests to talk about isomorphisms, and first, an apology. The letter commonly used for the function is  $\Phi$ , and some were trying to connect it to the Euler phi function uses the lower-case version  $\phi$ . There is *no* connection between the two. I'm sorry if this was confusing!

I've also gotten a request to talk about isomorphisms and the theorem in the lecture, so let me first review. Let's start with a familiar picture:

I've gotten some requests to talk about isomorphisms, and first, an apology. The letter commonly used for the function is  $\Phi$ , and some were trying to connect it to the Euler phi function uses the lower-case version  $\phi$ . There is *no* connection between the two. I'm sorry if this was confusing!

I've also gotten a request to talk about isomorphisms and the theorem in the lecture, so let me first review. Let's start with a familiar picture:

$C_4$	$e$	$a$	$a^2$	$a^3$
$e$	$e$	$a$	$a^2$	$a^3$
$e$	$e$	$a^2$	$a^3$	$e$
$a^2$	$a^2$	$a^3$	$e$	$a$
$a^3$	$a^3$	$e$	$a$	$a^2$

$(\mathbb{Z}/4\mathbb{Z}, \oplus)$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

I've gotten some requests to talk about isomorphisms, and first, an apology. The letter commonly used for the function is  $\Phi$ , and some were trying to connect it to the Euler phi function uses the lower-case version  $\phi$ . There is *no* connection between the two. I'm sorry if this was confusing!

I've also gotten a request to talk about isomorphisms and the theorem in the lecture, so let me first review. Let's start with a familiar picture:

$C_4$	$e$	$a$	$a^2$	$a^3$
$e$	$e$	$a$	$a^2$	$a^3$
$e$	$e$	$a^2$	$a^3$	$e$
$a^2$	$a^2$	$a^3$	$e$	$a$
$a^3$	$a^3$	$e$	$a$	$a^2$

$(\mathbb{Z}/4\mathbb{Z}, \oplus)$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

The isomorphism implicit from these tables is given by

$$\Phi(e) = [0]_4, \quad \Phi(a) = [1]_4, \quad \Phi(a^2) = [2]_4, \quad \Phi(a^3) = [3]_4.$$

In this case, we can put the isomorphism in words:  $\Phi(a^k) = [k]_4$ .  
This is not always possible.

In this case, we can put the isomorphism in words:  $\Phi(a^k) = [k]_4$ .  
This is not always possible.

Since the divisors of 4 are 1, 2, 4, the group  $C_4 = \langle a \rangle$  has three subgroups:  $\langle a \rangle$ ,  $\langle a^2 \rangle$  and  $\langle a^4 \rangle$ . Of these,  $\langle a \rangle = C_4$  and  $\langle a^4 \rangle = \langle e \rangle = \{e\}$ . The other one is  $\langle a^2 \rangle = \{e, a^2\}$ .

In this case, we can put the isomorphism in words:  $\Phi(a^k) = [k]_4$ . This is not always possible.

Since the divisors of 4 are 1, 2, 4, the group  $C_4 = \langle a \rangle$  has three subgroups:  $\langle a \rangle$ ,  $\langle a^2 \rangle$  and  $\langle a^4 \rangle$ . Of these,  $\langle a \rangle = C_4$  and  $\langle a^4 \rangle = \langle e \rangle = \{e\}$ . The other one is  $\langle a^2 \rangle = \{e, a^2\}$ .

What happens when we apply  $\Phi$  to these sets? First,  $\Phi$  is a bijection, so  $\Phi(C_4) = \mathbb{Z}/4\mathbb{Z}$ . Second,  $\Phi$  maps the identity to the identity, so  $\Phi(\{e\}) = [0]_4$ . The interesting case is



In this case, we can put the isomorphism in words:  $\Phi(a^k) = [k]_4$ . This is not always possible.

Since the divisors of 4 are 1, 2, 4, the group  $C_4 = \langle a \rangle$  has three subgroups:  $\langle a \rangle$ ,  $\langle a^2 \rangle$  and  $\langle a^4 \rangle$ . Of these,  $\langle a \rangle = C_4$  and  $\langle a^4 \rangle = \langle e \rangle = \{e\}$ . The other one is  $\langle a^2 \rangle = \{e, a^2\}$ .

What happens when we apply  $\Phi$  to these sets? First,  $\Phi$  is a bijection, so  $\Phi(C_4) = \mathbb{Z}/4\mathbb{Z}$ . Second,  $\Phi$  maps the identity to the identity, so  $\Phi(\{e\}) = [0]_4$ . The interesting case is

$$\Phi(\{e, a^2\}) = \{\Phi(e), \Phi(a^2)\} = \{[0]_4, [2]_4\}.$$

In this case, we can put the isomorphism in words:  $\Phi(a^k) = [k]_4$ . This is not always possible.

Since the divisors of 4 are 1, 2, 4, the group  $C_4 = \langle a \rangle$  has three subgroups:  $\langle a \rangle$ ,  $\langle a^2 \rangle$  and  $\langle a^4 \rangle$ . Of these,  $\langle a \rangle = C_4$  and  $\langle a^4 \rangle = \langle e \rangle = \{e\}$ . The other one is  $\langle a^2 \rangle = \{e, a^2\}$ .

What happens when we apply  $\Phi$  to these sets? First,  $\Phi$  is a bijection, so  $\Phi(C_4) = \mathbb{Z}/4\mathbb{Z}$ . Second,  $\Phi$  maps the identity to the identity, so  $\Phi(\{e\}) = [0]_4$ . The interesting case is

$$\Phi(\{e, a^2\}) = \{\Phi(e), \Phi(a^2)\} = \{[0]_4, [2]_4\}.$$

Both sides give a cyclic group of order 2, because  $(a^2)^2 = e$  and  $[2]_4 + [2]_4 = [0]_4$ .

Here are the multiplication tables of the subgroups.

Here are the multiplication tables of the subgroups.

	$e$	$a^2$
$e$	$e$	$a^2$
$a^2$	$a^2$	$e$

	$[0]_4$	$[2]_4$
$[0]_4$	$[0]_4$	$[2]_4$
$[2]_4$	$[2]_4$	$[0]_4$

Here are the multiplication tables of the subgroups.

	$e$	$a^2$
$e$	$e$	$a^2$
$a^2$	$a^2$	$e$

	$[0]_4$	$[2]_4$
$[0]_4$	$[0]_4$	$[2]_4$
$[2]_4$	$[2]_4$	$[0]_4$

Let's use a different cyclic group of order 4:  $((\mathbb{Z}/5\mathbb{Z})^*, \odot)$ . Recall that  $(\mathbb{Z}/5\mathbb{Z})^* = \{[1]_5, [2]_5, [3]_5, [4]_5\}$ .

Here are the multiplication tables of the subgroups.

	$e$	$a^2$
$e$	$e$	$a^2$
$a^2$	$a^2$	$e$

	$[0]_4$	$[2]_4$
$[0]_4$	$[0]_4$	$[2]_4$
$[2]_4$	$[2]_4$	$[0]_4$

Let's use a different cyclic group of order 4:  $((\mathbb{Z}/5\mathbb{Z})^*, \odot)$ . Recall that  $(\mathbb{Z}/5\mathbb{Z})^* = \{[1]_5, [2]_5, [3]_5, [4]_5\}$ .

What we found earlier was that  $[1]_5$  is the identity,  $[2]_5$  is a generator, and  $[2]_5^2 = [2^2]_5 = [4]_5$  and  $[2]_5^3 = [2^3]_5 = [8]_5 = [3]_5$  and  $[2]_5^4 = [2^4]_5 = [16]_5 = [1]_5$ .

The multiplication tables, written to emphasize that  $((\mathbb{Z}/5\mathbb{Z}^*, \odot)$  is cyclic.

The multiplication tables, written to emphasize that  $((\mathbb{Z}/5\mathbb{Z}^*, \odot)$  is cyclic.

$C_4$	$e$	$a$	$a^2$	$a^3$
$e$	$e$	$a$	$a^2$	$a^3$
$e$	$e$	$a^2$	$a^3$	$e$
$a^2$	$a^2$	$a^3$	$e$	$a$
$a^3$	$a^3$	$e$	$a$	$a^2$

$((\mathbb{Z}/5\mathbb{Z})^*, \odot)$	1	2	4	3
1	1	2	4	3
2	2	4	3	1
4	4	3	1	2
3	3	1	2	4



The multiplication tables, written to emphasize that  $((\mathbb{Z}/5\mathbb{Z}^*, \odot)$  is cyclic.

$C_4$	$e$	$a$	$a^2$	$a^3$
$e$	$e$	$a$	$a^2$	$a^3$
$e$	$e$	$a^2$	$a^3$	$e$
$a^2$	$a^2$	$a^3$	$e$	$a$
$a^3$	$a^3$	$e$	$a$	$a^2$

$((\mathbb{Z}/5\mathbb{Z})^*, \odot)$	1	2	4	3
1	1	2	4	3
2	2	4	3	1
4	4	3	1	2
3	3	1	2	4

Again, if we define  $\Phi_1$  by

$$\Phi_1(e) = [1]_5, \quad \Phi_1(a) = [2]_5, \quad \Phi_1(a^2) = [4]_5, \quad \Phi_1(a^3) = [3]_5,$$

The multiplication tables, written to emphasize that  $((\mathbb{Z}/5\mathbb{Z}^*, \odot)$  is cyclic.

$C_4$	$e$	$a$	$a^2$	$a^3$
$e$	$e$	$a$	$a^2$	$a^3$
$a$	$e$	$a^2$	$a^3$	$e$
$a^2$	$a^2$	$a^3$	$e$	$a$
$a^3$	$a^3$	$e$	$a$	$a^2$

$((\mathbb{Z}/5\mathbb{Z})^*, \odot)$	1	2	4	3
1	1	2	4	3
2	2	4	3	1
4	4	3	1	2
3	3	1	2	4

Again, if we define  $\Phi_1$  by

$$\Phi_1(e) = [1]_5, \quad \Phi_1(a) = [2]_5, \quad \Phi_1(a^2) = [4]_5, \quad \Phi_1(a^3) = [3]_5,$$

we see that it is an isomorphism, and the proper subgroup of  $((\mathbb{Z}/5\mathbb{Z})^*, \odot)$  is  $\{\Phi_1(e), \Phi_1(a^2)\} = \{[1]_5, [4]_5\}$ .

I'll finish with a request to go over the isomorphism proofs from last night. I will not repeat them in the “Weekly Summary”.

These are unchanged frames. Please stop me if you have questions!

Two groups  $(G, *_G)$  and  $(H, *_H)$  are isomorphic if there is a function  $\Phi$  so that  $\Phi$  is a bijection from  $G$  to  $H$  (as sets) and  $\Phi$  preserves the operation.

Two groups  $(G, *_G)$  and  $(H, *_H)$  are isomorphic if there is a function  $\Phi$  so that  $\Phi$  is a bijection from  $G$  to  $H$  (as sets) and  $\Phi$  preserves the operation.

That is, for  $g_1, g_2 \in G$ ,  $\Phi(g_1 *_G g_2) = \Phi(g_1) *_H \Phi(g_2)$ . From the point of view of multiplication tables, two groups are isomorphic if there is a function  $\Phi$  which relabels the elements so that the tables of the same.

Two groups  $(G, *_G)$  and  $(H, *_H)$  are isomorphic if there is a function  $\Phi$  so that  $\Phi$  is a bijection from  $G$  to  $H$  (as sets) and  $\Phi$  preserves the operation.

That is, for  $g_1, g_2 \in G$ ,  $\Phi(g_1 *_G g_2) = \Phi(g_1) *_H \Phi(g_2)$ . From the point of view of multiplication tables, two groups are isomorphic if there is a function  $\Phi$  which relabels the elements so that the tables of the same.

I didn't mention it explicitly, but there is a useful lemma about isomorphisms.

Two groups  $(G, *_{G})$  and  $(H, *_{H})$  are isomorphic if there is a function  $\Phi$  so that  $\Phi$  is a bijection from  $G$  to  $H$  (as sets) and  $\Phi$  preserves the operation.

That is, for  $g_1, g_2 \in G$ ,  $\Phi(g_1 *_{G} g_2) = \Phi(g_1) *_{H} \Phi(g_2)$ . From the point of view of multiplication tables, two groups are isomorphic if there is a function  $\Phi$  which relabels the elements so that the tables of the same.

I didn't mention it explicitly, but there is a useful lemma about isomorphisms.

LEMMA (i) If  $\Phi : G \mapsto H$  is an isomorphism, and  $e_G$  is the identity in  $G$ , then  $\Phi(e_G) = e_H$ , the identity in  $H$ ;

Two groups  $(G, *_G)$  and  $(H, *_H)$  are isomorphic if there is a function  $\Phi$  so that  $\Phi$  is a bijection from  $G$  to  $H$  (as sets) and  $\Phi$  preserves the operation.

That is, for  $g_1, g_2 \in G$ ,  $\Phi(g_1 *_G g_2) = \Phi(g_1) *_H \Phi(g_2)$ . From the point of view of multiplication tables, two groups are isomorphic if there is a function  $\Phi$  which relabels the elements so that the tables of the same.

I didn't mention it explicitly, but there is a useful lemma about isomorphisms.

LEMMA (i) If  $\Phi : G \mapsto H$  is an isomorphism, and  $e_G$  is the identity in  $G$ , then  $\Phi(e_G) = e_H$ , the identity in  $H$ ;

(ii)  $\Phi(g^{-1})$  is the inverse of  $\Phi(g)$  in  $H$ .



PROOF (i) For  $g \in G$ , we have  $g = e_G *_{G} g$ , so since  $e_H$  is the identity in  $H$ ,

PROOF (i) For  $g \in G$ , we have  $g = e_G *_{G} g$ , so since  $e_H$  is the identity in  $H$ ,

$$e_H *_{H} \Phi(g) = \Phi(g) = \Phi(e_G *_{G} g) = (\Phi(e_G)) *_{H} \Phi(g)$$

PROOF (i) For  $g \in G$ , we have  $g = e_G *_{G} g$ , so since  $e_H$  is the identity in  $H$ ,

$$e_H *_{H} \Phi(g) = \Phi(g) = \Phi(e_G *_{G} g) = (\Phi(e_G)) *_{H} \Phi(g)$$

so by right cancellation,  $e_H = \Phi(e_G)$ .

PROOF (i) For  $g \in G$ , we have  $g = e_G *_{G} g$ , so since  $e_H$  is the identity in  $H$ ,

$$e_H *_{H} \Phi(g) = \Phi(g) = \Phi(e_G *_{G} g) = (\Phi(e_G)) *_{H} \Phi(g)$$

so by right cancellation,  $e_H = \Phi(e_G)$ .

For (ii),  $g *_{G} g^{-1} = e_G \implies \Phi(g) *_{H} \Phi(g^{-1}) = \Phi(e_G) = e_H$ , so  $\Phi(g^{-1})$  is the inverse of  $\Phi(g)$  in  $H$ .

PROOF (i) For  $g \in G$ , we have  $g = e_G *_{G} g$ , so since  $e_H$  is the identity in  $H$ ,

$$e_H *_{H} \Phi(g) = \Phi(g) = \Phi(e_G *_{G} g) = (\Phi(e_G)) *_{H} \Phi(g)$$

so by right cancellation,  $e_H = \Phi(e_G)$ .

For (ii),  $g *_{G} g^{-1} = e_G \implies \Phi(g) *_{H} \Phi(g^{-1}) = \Phi(e_G) = e_H$ , so  $\Phi(g^{-1})$  is the inverse of  $\Phi(g)$  in  $H$ .

To illustrate this, let me prove a theorem I've already announced.

PROOF (i) For  $g \in G$ , we have  $g = e_G *_{G} g$ , so since  $e_H$  is the identity in  $H$ ,

$$e_H *_{H} \Phi(g) = \Phi(g) = \Phi(e_G *_{G} g) = (\Phi(e_G)) *_{H} \Phi(g)$$

so by right cancellation,  $e_H = \Phi(e_G)$ .

For (ii),  $g *_{G} g^{-1} = e_G \implies \Phi(g) *_{H} \Phi(g^{-1}) = \Phi(e_G) = e_H$ , so  $\Phi(g^{-1})$  is the inverse of  $\Phi(g)$  in  $H$ .

To illustrate this, let me prove a theorem I've already announced.

**THEOREM 1:** Suppose the group  $(G, *_{G})$  is isomorphic to the group  $(H, *_{H})$  and suppose  $G_1$  is a subgroup of  $G$ . Then

$$H_1 = \Phi(G_1) := \{\Phi(g) : g \in G_1\}$$

is a subgroup of  $H$ .

PROOF: If  $x \in H_1$ , then there is  $u \in G_1$  so that  $x = \Phi(u)$ .

PROOF: If  $x \in H_1$ , then there is  $u \in G_1$  so that  $x = \Phi(u)$ .

All we have to do is prove the conditions for a subgroup. First closure. Suppose  $x, y \in H_1$ . We need to prove that  $x *_H y \in H_1$ . But  $x, y \in H_1$  means that there exist  $u, v \in G_1$  so that  $x = \Phi(u)$  and  $y = \Phi(v)$ . Because  $\Phi$  is an isomorphism,



PROOF: If  $x \in H_1$ , then there is  $u \in G_1$  so that  $x = \Phi(u)$ .

All we have to do is prove the conditions for a subgroup. First closure. Suppose  $x, y \in H_1$ . We need to prove that  $x *_H y \in H_1$ . But  $x, y \in H_1$  means that there exist  $u, v \in G_1$  so that  $x = \Phi(u)$  and  $y = \Phi(v)$ . Because  $\Phi$  is an isomorphism,

$$\Phi(u *_G v) = \Phi(u) *_H \Phi(v) = x *_H y.$$

PROOF: If  $x \in H_1$ , then there is  $u \in G_1$  so that  $x = \Phi(u)$ .

All we have to do is prove the conditions for a subgroup. First closure. Suppose  $x, y \in H_1$ . We need to prove that  $x *_H y \in H_1$ . But  $x, y \in H_1$  means that there exist  $u, v \in G_1$  so that  $x = \Phi(u)$  and  $y = \Phi(v)$ . Because  $\Phi$  is an isomorphism,

$$\Phi(u *_G v) = \Phi(u) *_H \Phi(v) = x *_H y.$$

Since  $G_1$  is a subgroup,  $u *_G v \in G_1$ , so this means that  $x *_H y$  is the image of an element of  $G_1$  under  $\Phi$ , which means that  $x *_H y \in H_1$ .

PROOF: If  $x \in H_1$ , then there is  $u \in G_1$  so that  $x = \Phi(u)$ .

All we have to do is prove the conditions for a subgroup. First closure. Suppose  $x, y \in H_1$ . We need to prove that  $x *_H y \in H_1$ . But  $x, y \in H_1$  means that there exist  $u, v \in G_1$  so that  $x = \Phi(u)$  and  $y = \Phi(v)$ . Because  $\Phi$  is an isomorphism,

$$\Phi(u *_G v) = \Phi(u) *_H \Phi(v) = x *_H y.$$

Since  $G_1$  is a subgroup,  $u *_G v \in G_1$ , so this means that  $x *_H y$  is the image of an element of  $G_1$  under  $\Phi$ , which means that  $x *_H y \in H_1$ .

The other two are easier. Since  $G_1$  is a subgroup,  $e_G \in G_1$  and so  $\Phi(e_G) \in H_1$ . By the lemma, this means  $e_H \in H_1$ : it has the identity. If  $x \in H_1$ , then  $x = \Phi(u)$  for  $u \in G_1$  and then  $u^{-1} \in G_1$ , because  $G_1$  is a subgroup and by the lemma,  $\Phi(u^{-1}) \in H_1$  is the inverse of  $x = \Phi(u)$ . □

## WORKSHEET PROBLEMS

1. Let  $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} = \{([a]_2, [b]_3)\}$ , and define the operation  $*$  by

## WORKSHEET PROBLEMS

1. Let  $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} = \{([a]_2, [b]_3)\}$ , and define the operation  $*$  by

$$([a]_2, [b]_3) * ([c]_2, [d]_3) = ([a + c]_2, [b + d]_3)$$

## WORKSHEET PROBLEMS

1. Let  $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} = \{([a]_2, [b]_3)\}$ , and define the operation  $*$  by

$$([a]_2, [b]_3) * ([c]_2, [d]_3) = ([a + c]_2, [b + d]_3)$$

Thus, for example

$$([1]_2, [1]_3) * ([1]_2, [1]_3) = ([2]_2, [2]_3) = ([0]_2, [2]_3),$$

because  $2 \equiv 0 \pmod{2}$  and  $2 \equiv 2 \pmod{3}$ .

## WORKSHEET PROBLEMS

1. Let  $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} = \{([a]_2, [b]_3)\}$ , and define the operation  $*$  by

$$([a]_2, [b]_3) * ([c]_2, [d]_3) = ([a + c]_2, [b + d]_3)$$

Thus, for example

$$([1]_2, [1]_3) * ([1]_2, [1]_3) = ([2]_2, [2]_3) = ([0]_2, [2]_3),$$

because  $2 \equiv 0 \pmod{2}$  and  $2 \equiv 2 \pmod{3}$ .

Prove that  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$  is a cyclic group of order 6 by working out  $\langle ([1]_2, [1]_3) \rangle$ .

2. Same situation. Consider  $C_6 = \langle a \rangle, a^6 = e$ .



2. Same situation. Consider  $C_6 = \langle a \rangle, a^6 = e$ .

There is an isomorphism  $\Phi$  which takes  $C_6$  to  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$  and for which  $\Phi(a) = ([1]_2, [1]_3)$ .

2. Same situation. Consider  $C_6 = \langle a \rangle, a^6 = e$ .

There is an isomorphism  $\Phi$  which takes  $C_6$  to  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$  and for which  $\Phi(a) = ([1]_2, [1]_3)$ .

Write out the other values of  $\Phi(a^k)$ , and  $\Phi(\langle a^2 \rangle)$  and  $\Phi(\langle a^3 \rangle)$ .

2. Same situation. Consider  $C_6 = \langle a \rangle, a^6 = e$ .

There is an isomorphism  $\Phi$  which takes  $C_6$  to  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$  and for which  $\Phi(a) = ([1]_2, [1]_3)$ .

Write out the other values of  $\Phi(a^k)$ , and  $\Phi(\langle a^2 \rangle)$  and  $\Phi(\langle a^3 \rangle)$ .

These are subgroups of  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$  that will be “obviously” subgroups.

SOLUTION to 1. From the definition of the group:

SOLUTION to 1. From the definition of the group:

$$([1]_2, [1]_3)^1 = ([1]_2, [1]_3)$$

$$([1]_2, [1]_3)^2 = ([1]_2, [1]_3) * ([1]_2, [1]_3) = ([0]_2, [2]_3)$$

$$([1]_2, [1]_3)^3 = ([1]_2, [1]_3) * ([1]_2, [1]_3)^2 = ([1]_2, [0]_3)$$

$$([1]_2, [1]_3)^4 = ([1]_2, [1]_3) * ([1]_2, [1]_3)^3 = ([0]_2, [1]_3)$$

$$([1]_2, [1]_3)^5 = ([1]_2, [1]_3) * ([1]_2, [1]_3)^4 = ([1]_2, [2]_3)$$

$$([1]_2, [1]_3)^6 = ([1]_2, [1]_3) * ([1]_2, [1]_3)^5 = ([0]_2, [0]_3)$$

SOLUTION to 1. From the definition of the group:

$$([1]_2, [1]_3)^1 = ([1]_2, [1]_3)$$

$$([1]_2, [1]_3)^2 = ([1]_2, [1]_3) * ([1]_2, [1]_3) = ([0]_2, [2]_3)$$

$$([1]_2, [1]_3)^3 = ([1]_2, [1]_3) * ([1]_2, [1]_3)^2 = ([1]_2, [0]_3)$$

$$([1]_2, [1]_3)^4 = ([1]_2, [1]_3) * ([1]_2, [1]_3)^3 = ([0]_2, [1]_3)$$

$$([1]_2, [1]_3)^5 = ([1]_2, [1]_3) * ([1]_2, [1]_3)^4 = ([1]_2, [2]_3)$$

$$([1]_2, [1]_3)^6 = ([1]_2, [1]_3) * ([1]_2, [1]_3)^5 = ([0]_2, [0]_3)$$

So the first five powers are different and the sixth gives the identity and  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$  is a cyclic group of order 6.

SOLUTION to 2.

SOLUTION to 2.

If  $\Phi(a) = ([1]_2, [1]_3)$ , then because  $\Phi$  is an isomorphism.

$\Phi(a^k) = ([1]_2, [1]_3)^k$ , so  $\Phi(a^2) = ([0]_2, [2]_3)$ ,  $\Phi(a^3) = ([1]_2, [0]_3)$ ,

$\Phi(a^4) = ([0]_2, [2]_3)$ ,  $\Phi(a^5) = ([1]_2, [2]_3)$  and

$\Phi(e) = \Phi(a^6) = ([0]_2, [0]_3) = e_G$



SOLUTION to 2.

If  $\Phi(a) = ([1]_2, [1]_3)$ , then because  $\Phi$  is an isomorphism.

$\Phi(a^k) = ([1]_2, [1]_3)^k$ , so  $\Phi(a^2) = ([0]_2, [2]_3)$ ,  $\Phi(a^3) = ([1]_2, [0]_3)$ ,

$\Phi(a^4) = ([0]_2, [2]_3)$ ,  $\Phi(a^5) = ([1]_2, [2]_3)$  and

$\Phi(e) = \Phi(a^6) = ([0]_2, [0]_3) = e_G$

The images of  $\Phi(\langle a^2 \rangle) = \Phi(\{e, a^2, a^4\})$  and  $\Phi(\langle a^3 \rangle) = \Phi(\{e, a^3\})$  are then

$$\{([0]_2, [0]_3), ([0]_2, [1]_3), ([0]_2, [2]_3)\}$$

and

$$\{([0]_2, [0]_3), ([1]_2, [0]_3)\}.$$

You could write these as  $\{[0]_2\} \times \mathbb{Z}/3\mathbb{Z}$  and  $\mathbb{Z}/2\mathbb{Z} \times \{[0]_3\}$