

Qn Find an isomorphism from  $(\mathbb{Z}_5 - \{0\}, \cdot)$  to  $(\mathbb{Z}_4, +)$

Answer  $\mathbb{Z}_5 - \{0\}$  has 4 elements: 1, 2, 3, 4

and  $\mathbb{Z}_4$  has 4 elements: 0, 1, 2, 3.

~~✗~~ We want to find a bijection  $f: \mathbb{Z}_5 - \{0\} \rightarrow \mathbb{Z}_4$   
which respects the operations of multiplication and addition.

$$f(xy) = f(x) + f(y) \quad \text{--- (*)}$$

Now 1 is the identity element in  $\mathbb{Z}_5 - \{0\}$ .

$$1 \cdot 1 = 1$$

$$\Rightarrow f(1 \cdot 1) = f(1)$$

By property (\*) this rewrites as

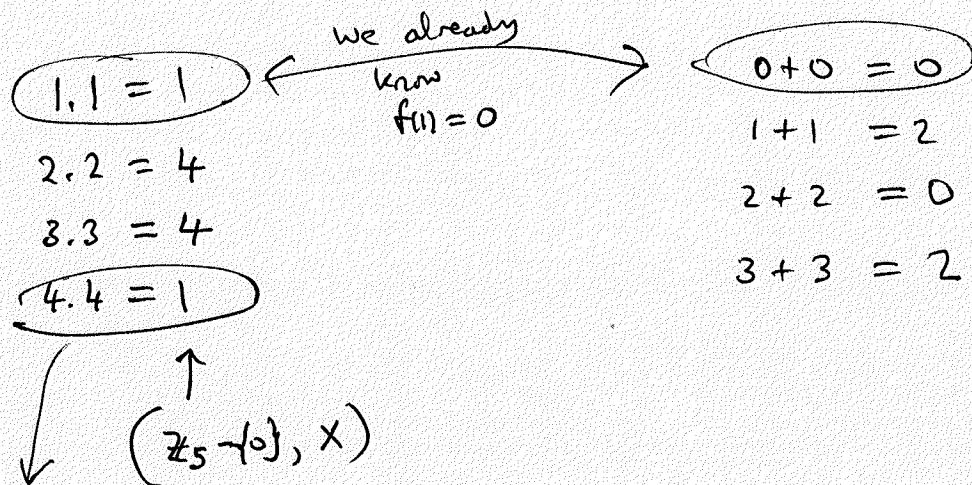
$$f(1) + f(1) = f(1)$$

Subtracting  $f(1)$  (remember we are working with addition  
for the outputs) gives

$$f(1) + \cancel{f(1)} - f(1) = f(1) - f(1) = 0$$

$$\Rightarrow \boxed{f(1) = 0} \quad \leftarrow f \text{ must take } 1 \text{ to } 0.$$

Look at "squares of elements"



$f(4 \cdot 4) = f(1)$  rewrites (using  $(*)$ ) as

$$f(4) + f(4) = f(1) = 0$$

$$f(4) + f(4) = 0,$$

Looking at the right hand column, we see that the only possibilities are  $f(4) = 0$  ( $0 + 0 = 0$ )

and  $f(4) = 2$  ( $2 + 2 = 0$ )

But  $f(1) = 0$  &  $f$  is injective.

$$\Rightarrow f(4) \neq 0$$

$$\Rightarrow \boxed{f(4) = 2}$$

$f$  must send 4 to 2.

There are only 2 possibilities left:

$$f(2) = 1$$

$$f(3) = 3$$



or  $f(2) = 3$

$$f(3) = 1$$

Both work!

$$f_1 : (\mathbb{Z}_5 - \{0\}, \times) \longrightarrow (\mathbb{Z}_4, +)$$

$$: 1 \longmapsto 0$$

$$2 \longmapsto 1$$

$$3 \longmapsto 3$$

$$4 \longmapsto 2$$

$$\& f_2 : (\mathbb{Z}_5 - \{0\}, \times) \longrightarrow (\mathbb{Z}_4, +)$$

$$: 1 \longmapsto 0$$

$$2 \longmapsto 3$$

$$3 \longmapsto 1$$

$$4 \longmapsto 2$$

Remark

inverse

It is perhaps more natural to write out the functions

$$f_1^{-1} : (\mathbb{Z}_4, +) \longrightarrow (\mathbb{Z}_5 - \{0\}, \times)$$

$$: x \longmapsto 2^x$$

(exponential function!)

$$f_2^{-1} : (\mathbb{Z}_4, +) \longrightarrow (\mathbb{Z}_5 - \{0\}, \times)$$

$$: x \longmapsto 3^x$$

(exponential function!)