Math 417 Homework 2 Solutions Due Friday, September 11, 2020

---

1. ($\mathcal{E}$) Consider the integers $\mathbb{Z}$ with the binary operation $\circ$ defined by

$$a \circ b = a + b - 4.$$

We want to prove that $(\mathbb{Z}, \circ)$ is a group.

a. Prove that $\circ$ is associative.

$$(a \circ b) \circ c = (a + b - 4) \circ c = (a + b - 4) + c - 4 = a + b + c - 8$$
$$a \circ (b \circ c) = a \circ (b + c - 4) = a + (b + c - 4) - 4 = a + b + c - 8$$

These are equal, so $\circ$ is associative.

b. Find the identity element for $\circ$.

We want e so that $a \circ e = a$; that is, $a + e - 4 = a$, so $e = 4$ will work, and $a \circ 4 = a + 4 - 4 = a$.

c. Find an inverse element (with respect to $\circ$) for $a \in \mathbb{Z}$.

We need to solve $a \circ b = e$, or $a + b - 4 = 4$, so the inverse element of a is $b = 8 - a$.

2. ($\mathcal{E}$) Let $G = (\mathbb{Z}/6\mathbb{Z}, \oplus)$ and $H = ((\mathbb{Z}/9\mathbb{Z})^*, \odot)$. Write down one explicit isomorphism Φ from G to H; that is, determine the values of $\Phi([0]_6)$, $\Phi([1]_6)$, $\Phi([2]_6), \ldots$ as elements in H. Your answer should include an explanation of why you know that Φ is an isomorphism.

The first thing you need to do is check that H is a cyclic group. I'll write down the powers of $[2]_9$, reducing mod 9 to keep the numbers small (or look at the multiplication table):

$$[2]_9^0 = e = [1]_9, \quad [2]_9^1 = [2]_9, \quad [2]_9^2 = [2^2]_9 = [4]_9, [2]_9^3 = [2^3]_9 = [8]_9$$
$$[2]_9^4 = [2^4]_9 = [16]_9 = [7]_9, \quad [2]_9^5 = [2]_9[2^4]_9 = [2]_9[7]_9 = [14]_9 = [5]_9,$$
$$[2^6]_9 = [2]_9[2^5]_9 = [2]_9[5]_9 = [10]_9 = [1]_9 = e.$$

So we see that $H = \langle [2]_9 \rangle = \{[1]_9, [2]_9, [4]_9, [8]_9, [7]_9, [5]_9\}$. Isomorphisms between cyclic groups of the same order take generators to generators. We have

$$\Phi([0]_6) = [1]_9, \quad \Phi([1]_6) = [2]_9, \quad \Phi([2]_6) = [4]_9,$$
$$\Phi([3]_6) = [8]_9, \quad \Phi([4]_6) = [7]_9, \quad \Phi([5]_6) = [5]_9.$$

Or, to be brief, $\Phi([k]_6) = [2^k]_9$. This is an isomorphism by previous discussion or as follows: it is a bijection, and

$$\Phi([i]_6 \oplus [j]_6) = \Phi([i + j]_6) = [2^{i+j}]_9 = [2^i]_9 \odot [2^j]_9 = \Phi([i]_6) \odot \Phi([j]_6)$$

In terms of the original definition of isomorphism, $*_G = \oplus$ and $*_H = \odot$.

3. and 4. ($\mathcal{E}$) (counts as two problems) Define in the usual way the set

$$S = (\mathbb{Z}/5\mathbb{Z})^* = \{[1]_5, [2]_5, [3]_5, [4]_5\},$$

and define the binary operation $*$ on S by $[a]_5 * [b]_5 = [2ab]_5$. (For example $[1]_5 * [4]_5 = [2 \cdot 1 \cdot 4]_5 = [8]_5 = [3]_5$.) For your convenience, the multiplication table is given above. (The table shows that $*$ is a binary operation, and you do **not** have to prove this!) Instead, your task in this problem is to prove that $G = (S, *)$, with **this** strange definition, is a group.

G	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$
$[1]_5$	$[2]_5$	$[4]_5$	$[1]_5$	$[3]_5$
$[2]_5$	$[4]_5$	$[3]_5$	$[2]_5$	$[1]_5$
$[3]_5$	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$
$[4]_5$	$[3]_5$	$[1]_5$	$[4]_5$	$[2]_5$

a. Show that $*$ is associative in G.

$$([a]_5 * [b]_5) * [c]_5 = [2ab]_5 * [c]_5 = [4ab]_5,$$
$$[a]_5 * ([b]_5 * [c]_5) = [a]_5 * [2bc]_5 = [4ab]_5.$$

b. Determine the identity element in $(S, *)$. (The table will be helpful.)

It seems from the table that $[3]_5$ is the identity, and in fact, $[a]_5 * [3]_5 = [6a]_5 = [a]_5$,

c. Find the inverses of the four elements in S. (I want four answers here.)

Again from the table, $[1]_5 * [4]_5 = [2]_5 * [2]_5 = [3]_5 * [3]_5 = [3]_5$, so the inverses of $([1]_5, [2]_5, [3]_5, [4]_5)$, in order,are $([4]_5, [2]_5, [3]_5, [1]_5)$

d. Write down enough powers of $[1]_5$ to show that $(S, *)$ is a cyclic group and explain your answer.

$[1]_5^2 = [1]_5 * [1]_5 = [2]_5$, $[1]_5^3 = [1]_5 * [1]_5^2 == [1]_5 * [2]_5 = [4]_5$, $[1]_5^4 = [1]_5 * [1]_5^3 = [1]_5 * [4]_5 = [3]_5$. So $[1]_5^4 = [3]_4$ is the identity, and if I write $a = [1]_5$, the elements of G are $\{e, a, a^2, a^3\}$ and $a^4 = e$. This gives a cyclic group of order 4.

5. (Followup to 9/4 Worksheet) Let $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} = \{([a]_2, [b]_4)\}$, and define the operation $*$ by

$$([a]_2, [b]_4) * ([c]_2, [d]_4) = ([a+c]_2, [b+d]_4).$$

Thus, for example

$$([1]_2, [2]_4) * ([1]_2, [3]_4) = ([2]_2, [5]_4) = ([0]_2, [1]_4),$$

because $2 \equiv 0 \mod 2$ and $5 \equiv 1 \mod 4$.

a. Determine $\langle([1]_2, [1]_4)\rangle$, $\langle([1]_2, [2]_4)\rangle$ and $\langle([1]_2, [3]_4)\rangle$.

First, I'll observe that $([0]_2, [0]_4)$ is the identity, so I'll keep adding until I get to it. I will also not explicitly reduce mod 2 and mod 4.

$$([1]_2, [1]_4) * ([1]_2, [1]_4) = ([0]_2, [2]_4), ([1]_2, [1]_4) * ([0]_2, [2]_4) = ([1]_2, [3]_4),$$
$$([1]_2, [1]_4) * ([1]_2, [3]_4) = ([0]_2, [0]_4)$$

$$([1]_2, [2]_4) * ([1]_2, [2]_4) = ([0]_2, [0]_4)$$

$$([1]_2, [3]_4) * ([1]_2, [3]_4) = ([0]_2, [2]_4), ([1]_2, [3]_4) * ([0]_2, [2]_4) = ([1]_2, [1]_4),$$
$$([1]_2, [3]_4) * ([1]_2, [1]_4) = ([0]_2, [0]_4)$$

Notice that the inverse of $([1]_2, [1]_4)$ is $([1]_2, [3]_4)$, so they generate the same finite group:

$$\langle([1]_2, [1]_4)\rangle = \langle([1]_2, [3]_4)\rangle = \{([0]_2, [0]_4), ([1]_2, [1]_4), ([0]_2, [2]_4), ([1]_2, [3]_4)\}$$
$$\langle([1]_2, [2]_4)\rangle = \{([0]_2, [0]_4), ([1]_2, [2]_4)\}$$

b. Show that $H = \{([0]_2, [0]_4), ([0]_2, [2]_4), ([1]_2, [0]_4), ([1]_2, [2]_4)\}$ is a subgroup for G, and give an isomorphism from H to the Klein 4-group V.

The set H is closed under $*$, as the table shows (writing ab for $([a]_2, [b]_4)$):

G	00	02	10	12
00	00	02	10	12
02	02	00	12	10
10	10	12	00	02
12	12	10	02	00

I hope the family resemblance to V is clear. Here is one isomorphism:

$$\Phi(([0]_2, [0]_4)) = I, \quad \Phi(([0]_2, [2]_4)) = X, \quad \Phi(([1]_2, [0]_4)) = Y, \quad \Phi(([1]_2, [2]_4)) = Z$$