

# Homework № 1 for "Basics of abstract algebra and coding theory" course

Artem Petrov

February 13, 2020

## Problem #2

△

Let's select arbitrary  $z \in G$ .

$$z = zzz^{-1} = ez^{-1} = z^{-1}$$

So,  $\forall z \in G : z = z^{-1}$ . Let's select arbitrary  $x, y \in G$ .

$$xy = x^{-1}y^{-1} = (yx)^{-1} = yx$$

□

## Problem #3

△

According to the definition of group  $\forall g \in G, \exists! g^{-1} \in G : gg^{-1} = e$ .

$$g^{-1} = g \Leftrightarrow g^2 = e,$$

so if  $g \neq f$  (and  $g \neq e$ ), then  $g \neq g^{-1}$ . (otherwise we would have  $g^2 = gg^{-1} = e \Rightarrow |g| = 2$ , which is forbidden by problem condition).

$$\prod_{g \in G} g = ef g_1 g_1^{-1} g_2 g_2^{-1} \dots = f$$

□

## Problem #4

△

Suppose  $|h| = m$ .

To prove that  $|ghg^{-1}| = m$  we should prove that  $m = \min\{x \in \mathbb{N} : (ghg^{-1})^x = e\}$ . Let's do this:

1.1)  $(ghg^{-1})^m = gh^m g^{-1} = geg^{-1} = e$ .

1.2) Suppose we have found  $k \in \mathbb{N} : k < m, (ghg^{-1})^k = e$ . Then,  $e = (ghg^{-1})^k = gh^k g^{-1} \Rightarrow g^{-1} = h^k g^{-1} \Rightarrow e = h^k$ , which is impossible since  $|h| = m > k$ .

So, we have proved that  $m = |ghg^{-1}|$

Moving on to the next question:

Suppose  $|gh| = m$ . We will prove that  $|hg| = m$  following the same scheme we have followed in the previous proof:

$$2.1) e = (hg)^m = h(hg)^{m-1}g \Leftrightarrow e = geg^{-1} = gh(hg)^{m-1}gg^{-1} = (gh)^m$$

2.2) Suppose we have found  $k \in \mathbb{N} : k < m, (hg)^k = e$ . Then, similarly to 2.2, we get  $(gh)^k = e$ , which is impossible since  $|h| = m > k$ .

So, we have proved that  $|gh| = m = |hg|$  □

## Problem #6

△

$$] X = \{z \in \mathbb{C} : z^n = 1\} = \{\exp(i2\pi k/n) : k \in \{0, 1, 2, \dots, (n-1)\}\}$$

Clearly,  $(X; *) \cong (\{0, 1, 2, \dots, (n-1)\}, +)$ . And therefore  $(X, *)$  is a group.

$$\forall x \in X \exists y \in X : y^3 = x \Leftrightarrow \forall k \in \{0, 1, \dots, n-1\} \exists m \in \{0, 1, \dots, n-1\} : m * 3 = k.$$

$$] n = 35, k \in \{0, 1, \dots, n-1\}.$$

In this case if  $k \equiv 0 \pmod{3}$ , then  $m = k/3$ . If  $k \equiv 1 \pmod{3}$ , then  $m = (k + 35)/3$ . If  $k \equiv 2 \pmod{3}$ , then  $m = (k + 2 * 35)/3$ . We found corresponding  $m$  for every  $k \in X$ . Hence, every  $x \in X(n = 35)$  is a cube.

]  $n = 36, k \in \{0, 1, \dots, n-1\} : k \equiv 1 \pmod{3}$ . Let's prove by contradiction. Assume,  $\exists m \in \{0, 1, \dots, n-1\} : m * 3 = k$ . Then  $m * 3 \equiv k + 36 * l \pmod{3}; (l \in \mathbb{N}) \Rightarrow 0 \equiv 1 \pmod{3}$ , which is impossible. Therefore not every  $x \in X(n = 36)$  is a cube. □

## Problem #7

△

$(\mathbb{Z}/5\mathbb{Z})^* = (\{1, 2, 3, 4\}, *)$ ;  $(\mathbb{Z}/12\mathbb{Z})^* = (\{1, 5, 7, 11\})$ . Clearly, they have the same amount of elements.

Let's build multiplication tables for both of these groups:

1: Multiplication table for  $(\mathbb{Z}/5\mathbb{Z})^*$

#	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

2: Multiplication table for  $(\mathbb{Z}/12\mathbb{Z})^*$

#	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

Let's prove by contradiction. Suppose  $\exists \phi : (\mathbb{Z}/5\mathbb{Z})^* \rightarrow (\mathbb{Z}/12\mathbb{Z})^*$  - isomorphism. Isomorphism between groups maps 1 to 1.  $\forall x \in (\mathbb{Z}/12\mathbb{Z})^* x^2 = 1$ . Then  $\forall y \in (\mathbb{Z}/5\mathbb{Z})^* \phi(y * y) = \phi(y)\phi(y) = 1 \Rightarrow y * y = 1$ , which is impossible, since  $2^2 = 4$  in  $(\mathbb{Z}/5\mathbb{Z})^*$ . Therefore there are no isomorphisms between this groups. □