Math 541 - Fall 2017
HW2 - Notion of a group and some examples
For the Friday 9/22/17 "10 min." test

Remark. Answers should be written in the following format:
i) Statement and/or Result.
ii) Main points that will appear in your explanation or proof or computation.
iii) The actual explanation or proof or computation.

Definition. A group is a triple $(G, \cdot, 1_G)$, where G is a set, $\cdot : G \times G \to G$, $(g, h) \mapsto g \cdot h$, is a map, called operation, and $1_G \in G$ a specific element, called identity, such that the following axioms are satisfied:

- Associativity. We have $g_1 \cdot (g_2 \cdot g_3) = (g_1 \cdot g_2) \cdot g_3$ for every $g_1, g_2, g_3 \in G$.
- Identity. The element 1_G satisfies $1_G \cdot g = g \cdot 1_G = g$ for every $g \in G$.
- Inverse. For every $g \in G$ there exists $g' \in G$ such that $g \cdot g' = g' \cdot g = 1_G$. We will denote such a g' (it turns out that it is unique see 3.*b.* below) usually by g^{-1}.

1. Check which of the following is a group:

   (a) The set $\mathbb{R}$ with the standard operation of addition $+$ and identity element 0.

   (b) The set $\mathbb{N} = \{0, 1, 2, ...\}$ of natural numbers, with the standard operation of addition and the element 0 as identity.

   (c) The set $\mathbb{Z} = \{..., -2, -1, 0, 1, 2, ...\}$ of integers, with the standard operation of addition and the element 0 as identity.

   (d) The triple $(\mathbb{R}^\times, \cdot, 1)$ where $\mathbb{R}^\times = \mathbb{R} - 0$ the set of all non-zero real numbers, $\cdot$ is the usual multiplication of real numbers, and 1 is the usual number 1.

   (e) Denote by $GL_2(\mathbb{R})$ the set of all 2×2 invertible matrices with real entries

   $$GL_2(\mathbb{R}) = \left\{ A = \begin{pmatrix} a & b \\ c & d \end{pmatrix};\ a, b, c, d \in \mathbb{R} \text{ and there exists } A^{-1} \right\}.$$

   Show that with the operation $\circ$ of matrix multiplication the triple $(GL_2(\mathbb{R}), \circ, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix})$ is a group.

   (f) The triple $(M_2(\mathbb{R}), +, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix})$ where $M_2(\mathbb{R})$ denotes the set of all 2×2 matrices with real entries, and $+$ denotes standard addition of matrices.

2. *The integers modulo n.*

(a) Suppose m, n are integers, $m \geq 0$, $n \geq 1$. Show that we can divide m by n with a remainder in a unique way, i.e., show that there exist unique integers q, r, with $0 \leq r < n$, such that

$$m = qn + r. \tag{1}$$

We will call the r appearing in (1), the remainder after dividing m by n.

(b) For $n \geq 0$, consider the set $\mathbb{Z}_n = \{0, \ldots, n-1\}$. Define $\underset{\text{mod } n}{+}$ (called addition modulo n) and $\underset{\text{mod } n}{\cdot}$ (called multiplication modulo n) on $\mathbb{Z}_n$ as follows

$$\begin{cases} x \underset{\text{mod } n}{+} y = \text{ the remainder after dividing } x \underset{\mathbb{Z}}{+} y \text{ by } n; \\ x \underset{\text{mod } n}{\cdot} y = \text{ the remainder after dividing } x \underset{\mathbb{Z}}{\cdot} y \text{ by } n; \end{cases}$$

1. Show that $(\mathbb{Z}_n, \underset{\text{mod } n}{+}, 0)$ is a group. It is called the group of integers modulo n, or the group $\mathbb{Z}$ mod n.
2. Assume $n \geq 1$. Denote by $\mathbb{Z}_n^* = \{x \in \mathbb{Z}_n$, such that there is $y \in \mathbb{Z}_n$ with $x \underset{\text{mod } n}{\cdot} y = 1\}$. Show that $(\mathbb{Z}_n^*, \underset{\text{mod } n}{\cdot}, 1)$ is a group. It is called the multiplicative group of the integers modulo n.

(c) (not for the test) Define the notion of a field and solve the following:

1. Suppose $p \geq 2$ is a prime. Show that $\left(\mathbb{Z}_p, \underset{\text{mod } p}{+}, 0, \underset{\text{mod } p}{\cdot}, 1\right)$ is a field.
2. Suppose $n \geq 2$. Show that if $\left(\mathbb{Z}_n, \underset{\text{mod } n}{+}, 0, \underset{\text{mod } n}{\cdot}, 1\right)$ is a field, then n is a prime.

3. *Properties of groups.* Let $(G, \cdot, 1)$ be a group. Show that:

(a) If e and e' are elements of G which satisfy $e \cdot g = g \cdot e = g$ and $e' \cdot g = g \cdot e' = g$ for all $\in G$, then $e = e'$.

(b) If g,g', g'' are elements of G, and $g \cdot g' = g' \cdot g = 1$ and $g'' \cdot g = g \cdot g'' = 1$ then $g' = g''$.

(c) If $g, g' \in G$ and $g \cdot g' = 1$ then $g' \cdot g = 1$.

(d) For every $g \in G$ we have $(g^{-1})^{-1} = g$.

(e) For every $g, h \in G$ we have $(g \cdot h)^{-1} = h^{-1} \cdot g^{-1}$.

Definition. Let G be a group. We say that G is finite if $\#G < \infty$, i.e., it has finitely many elements. Otherwise, we say that G is infinite. The cardinality $\#G$ (whether finite of infinite) is called the order of G.

4. *Commutative and non-commutative groups.*

(a) Define the notions of:

1. Commutative group.

2. Non-commutative group.

(b) Give examples of two non-commutative groups: One which is finite, i.e., with finitely many elements, and one which is not finite.

(c) Give examples of two commutative groups: One finite and the other infinite.

Definition. A group C is called cyclic if there is $g \in C$ such

$$C =< g >^{\text{def}} \{g^k;\ k \in \mathbb{Z}\},$$

where

$$g^k = \begin{cases} \overbrace{g \cdot \ldots \cdot g}^{k \text{ times}}, & \text{if } k > 0; \\ 1_C\ , & \text{if } k = 0; \\ (g^{-1})^{-k}\ , & \text{if } k < 0. \end{cases}$$

(d) Show that any cyclic group is commutative. Give example of a commutative group which is not cyclic.

(e) Give two example of infinite cyclic groups.

(f) Give for every $n \geq 0$ two examples of cyclic groups of order n.

Remarks

- You are very much encouraged to work with other students on the HW.
- We encourage you at attend the **Discussion meeting every Wed. 4-5pm at B333.**
- We will be happy to help you with the home works. Please visit us in our office hours.

Good Luck!