Math 476 - Abstract Algebra - Worksheet on Chapter 2

Groups

Definition: Let G be a set and let $*$ be a binary operation defined on G. We say that $(G, *)$ is a *group* if it satisfies the following properties:

1. $*$ is associative;
2. there is an identity e in G;
3. every element of G has an inverse with respect to $*$.

We say that a group $(G, *)$ is *abelian* if we also have that

$$a * b = b * a$$

for all a and b in G, that is to say, if and only if $*$ is *commutative*.

Notation: from now on we will adopt the multiplicative notation for a binary operation in a group, that is to say, we will write xy instead of $x * y$, however we will keep the exponential form x^{-1} for the inverse of an element x (we will see that there is a unique inverse). We will also say "a group G" instead of "a group $(G, *)$", whenever the operation is clear. Sometimes, **but only when the group is abelian** we will use also the additive notation, that is to say, we will write $x + y$ instead of xy; in this notation, the inverse of x is written $-x$ and the identity is written 0.

Group Activity

Important: In the following you may have to prove that some operation is associative. In order to avoid proofs which are too long, you may assume that the following operations are associative: **products and sums of numbers (including $\mathbb{Z}_n$), product and sums of matrices, and composition of functions.**

(a) Say whether the following sets with the given operations are groups (do not forget to check whether the operation is closed). If not explain why, if yes write the identity element and the inverse of a generic element x. Ask whether your answers are correct.

$(\mathbb{Z}, +)$

$(\mathbb{Z}, \cdot)$

$(\mathbb{Q}, +)$

$(\mathbb{Q}^*, \cdot)$ (the * means that we are removing the number 0 from the set)

$(\mathbb{R}, +)$

$(\mathbb{R}^*, \cdot)$

$(\mathbb{C}, +)$

$(\mathbb{C}^*, \cdot)$

$(\mathbb{R}^+, \cdot)$ (the $^+$ means that we are considering only the positive numbers)

$(\mathbb{C}^+, \cdot)$

$(\mathbb{Z}_n, +)$

$(\mathbb{Z}_n, \cdot)$

for every positive integer n, the vector space $\mathbb{R}^n$ (or $\mathbb{C}^n$) but equipped only with the operation "+"

From now on we will write $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*, \mathbb{Q}^+, \mathbb{R}^+, \mathbb{C}^+, \mathbb{Q}^n, \mathbb{R}^n, \mathbb{C}^n$ for the corresponding group with the natural operation for which they are groups.

Are these groups abelian?

(b) **The Group $U(n)$** Now, for every integer $n \geq 2$, we define the group $U(n)$ consisting of all the invertible elements in $\mathbb{Z}_n$ with respect to the product. Let us start with some examples. First of all, write the Cayley tables for $(\mathbb{Z}_5, \cdot)$ and $(\mathbb{Z}_6, \cdot)$.

Write the elements of $\mathbb{Z}_5$ and $\mathbb{Z}_6$ that have an inverse for the product, we will call these two sets $U(5)$ and $U(6)$

$U(5) :=$

$U(6) :=$

Write the Cayley tables for $(U(5), \cdot)$ and $(U(6), \cdot)$

Complete the following proof that $U(5)$ and $U(6)$ are groups by referring to the above tables:

the operation "$\cdot$" is closed in $U(5)$ (and $U(6)$) because

the operation "$\cdot$" is associative because

the identity element is

every element in $U(5)$ (and $U(6)$) has an inverse because

Write the Cayley tables for $U(7)$ and $U(10)$ (from now on, when we write $U(n)$ we mean that the operation is the product).

Did you notice anything interesting?

(c) **The Group GL$(2, F)$** Let F be any of $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, or $\mathbb{Z}_p$ (with p prime). We define $\mathrm{GL}(2, F)$ to be the set of 2×2 invertible (with respect to the product) matrices with entries in F. This is a non-abelian group under matrix multiplication.

Exercise. Say whether the matrix $A := \begin{pmatrix} 5 & 2 \\ 1 & 3 \end{pmatrix}$ is in $\mathrm{GL}(2, \mathbb{R})$. Justify your answer.

Is A in $\mathrm{GL}(2, \mathbb{Z}_{13})$? Justify your answer.

Exercise. Determine two elements A and B of $\mathrm{GL}(2, \mathbb{Q})$ such that $AB \neq BA$. Justify.

Exercise. Determine all the elements of $GL(2, \mathbb{Z}_2)$.

(d) **The Group SL$(2, F)$** Let F be any of $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, or $\mathbb{Z}_p$ (with p prime). We define $\mathrm{SL}(2, F)$ to be the set of 2×2 matrices whose determinant is 1. This is also a non-abelian group under matrix multiplication.

Exercise. Say whether the matrix $A := \begin{pmatrix} 10 & 3 \\ 1 & 3 \end{pmatrix}$ is in $\mathrm{SL}(2, \mathbb{R})$. Justify your answer.

Is A in $\mathrm{SL}(2, \mathbb{Z}_{13})$? Justify your answer.

(e) **The Group D_4** Draw a square and label its vertices A, B, C, and D. Then draw all squares that can be obtained from the first one through rotations and reflections, label the vertices consistently (Hint: you will get a total of 8 squares including the first one.)

List the transformations you have used in the exercise above.

We define D_4 to be the set of rotations and reflections of a square (we call them symmetries of a square). Write the Cayley table for D_4 where the operation is the composition of symmetries.

Show that D_4 with the composition of symmetries is a group by referring to the previous table.

- the composition of symmetries is a closed operation because

- the composition of symmetries is associative because

- the identity element is

- every element has an inverse because

Answer the following questions. You may refer to the Cayley table.

- Is D_4 an abelian group?

- The composition of two rotations is a

- The composition of two reflections is a

- The composition of a rotation and a reflection in either order is a

- The inverse of a rotation h_α is

- The inverse of any reflection L is

- Determine all pairs a, b of elements of D_4 such that $ab = ba$.

Elementary Properties of Groups

Theorem: Cancellation

In a group G we have:

- if $a \cdot b = a \cdot c$ then $b = c$;

- if $b \cdot a = c \cdot a$ then $b = c$.

The above properties are called, respectively, *left and right cancellation laws.*
In your group, prove one of the two cancellation laws. **Keep in mind that you can only use group properties.**

Remark: The cancellation laws can be applied to solve equations in a group. Let G be a group, solving an equation of the form

$$ax = b$$

or

$$xa = b$$

where a and b are in G, means determining all elements x of the group that satisfy the given identity. Show that a solution exists.

Prove that the solution is unique.

Exercise. Solve the following equation in $U(15)$: $2x = 3$.

Theorem: Uniqueness of Inverses

For each element a in a group G, there is a unique element b in G such that $ab = ba = e$.

Prove the above Theorem by using properties of groups and possibly the Cancellation Theorem.

Theorem: Socks-Shoes Property.

Given two elements a and b of a group G, we have $(ab)^{-1} = b^{-1}a^{-1}$.

Prove the above Theorem.

Give an explanation for the name "Sock-Shoes Property"