Introduction to Groups I

Matthew Gherman and Adam Lott

April 14, 2019

1 Introduction

Definition 1. A *group* is a set G together with a binary operation $*$ on the set G (a binary operation means that for any two elements $a, b \in G$, we can combine them to get a new element $a * b \in G$) satisfying the following properties.

(G1) **Associativity**: For all $a, b, c \in G$, we have $(a * b) * c = a * (b * c)$.

(G2) **Identity:** There exists an element $e \in G$ (called an *identity element*) such that for any $a \in G$, $e*a = a*e = a$.

(G3) **Inverse:** For any $a \in G$ there exists some $b \in G$ (called an *inverse* of a) such that $a * b = b * a = e$.

Note that we do not require the operation $*$ to be commutative, i.e. it is allowed for $a * b \neq b * a$. However, this additional property is true in many examples, so it gets its own definition.

Definition 2. An *abelian group* is a group $(G, *)$ that also satisfies the additional property

(A1) **Commutativity:** For all $a, b \in G$, we have $a * b = b * a$.

Exercise 1. For each of the following examples, decide whether or not it is a group. If yes, prove that it satisfies the properties (G1)-(G3). If no, give an example for each property that fails. If it is a group, decide whether or not it is abelian and prove it.

(a) The set of integers with the addition as the operation, denoted $(\mathbb{Z}, +)$

(b) The set of integers with subtraction as the operation, denoted $(\mathbb{Z}, -)$

(c) The set of integers with multiplication as the operation, denoted $(\mathbb{Z}, \times)$

(d) The set of positive real numbers under the operation $x * y = 2xy$

(e) Let X be a set and take our set to be $\mathcal{P}(X) :=$ the *power set* of $X :=$ the set of all subsets of X. For $A, B \subset X$ subsets, define the operation $A * B = A \cup B$.

(f) Take the set of integers modulo n with addition modulo n, denoted $(\mathbb{Z}/n\mathbb{Z}, +)$. (Recall that this is the set $\mathbb{Z}/n\mathbb{Z} = \{0, 1, \ldots, n-1\}$. We add two elements as integers and then take the remainder of the sum when divided by n.)

(g) Take the set of *non-zero* integers modulo n with multiplication modulo n, denoted $((\mathbb{Z}/n\mathbb{Z}) \setminus \{0\}, \times)$. (Note that the definition of a group implies that multiplication of two elements of the set must produce an element of the set.)

(h) (CHALLENGE) For which values of n is $((\mathbb{Z}/n\mathbb{Z}) \setminus \{0\}, \times)$ a group?

(i) As we saw last week, the symmetries of a square index card define a group under composition. We define the dihedral group D_n as the symmetries of a regular n-gon in the plane. Show that D_5 is a group under composition. For this problem, you may assume associativity holds.

(j) Take the set $\{e, a, b, c\}$ and the operation is defined in the table below. For instance, $a * b$ is the element in row a and column b. For this problem, you may assume that associativity holds.

*	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

(k) Take the set $\{e, x_1, x_2, x_3, y_1, y_2\}$ under the operation defined in the table below. For this problem, you may assume that associativity holds.

$*$	e	x_1	x_2	x_3	y_1	y_2
e	e	x_1	x_2	x_3	y_1	y_2
x_1	x_1	e	y_2	y_1	x_3	x_2
x_2	x_2	y_1	e	y_2	x_1	x_3
x_3	x_3	y_2	y_1	e	x_2	x_1
y_1	y_1	x_2	x_3	x_1	y_2	e
y_2	y_2	x_3	x_1	x_2	e	y_1

(l) (CHALLENGE) The set of 2×2 matrices with entries from the real numbers under the operation matrix multiplication. Matrix multiplication is defined as $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{pmatrix}$.

(m) (CHALLENGE) The set of 2×2 matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with entries from the real numbers such that $ad - bc \neq 0$ under matrix multiplication.

2 Properties of groups

In this section, we will investigate some properties that all groups have as consequences of the defining properties.

Exercise 2. Let $(G, *)$ be a group. Using *only* the properties (G1)-(G3) (and (A1) when applicable), prove the following statements. You may also use an earlier statement in the proof of a later statement.

(a) Uniqueness of identity: If e and e' are both identity elements of G (see property (G2)), then $e = e'$.

(b) Uniqueness of inverses: Let $a \in G$. Prove that if b and b' are both inverses of a (i.e. $b * a = b' * a = e$), then $b = b'$.
NOTE: Since we have now proven that inverses are unique, given an element $a \in G$ we will denote its unique inverse by a^{-1}.

(c) Left cancellation: For any $a, b, c \in G$, if $a * b = a * c$, then $b = c$.

(d) Right cancellation: For any $a, b, c \in G$, if $b * a = c * a$, then $b = c$.

(e) For any $a, b \in G$, $(a * b)^{-1} = b^{-1} * a^{-1}$.

(f) For any $a \in G$, $(a^{-1})^{-1} = a$.

Definition 3. For an element $a \in G$ and a positive integer k, we define $a^k := \underbrace{a * a * \cdots * a}_{k \text{ times}}$. We also define $a^{-k} := (a^k)^{-1}$.

(g) For any $a \in G$ and positive integers n, m, we have $a^m * a^n = a^{m+n}$.

(h) For any $a \in G$ and positive integers n, m, we have $(a^m)^n = a^{mn}$.

(i) For any $a \in G$ and positive integers k, we have $a^{-k} = (a^{-1})^k$.

(j) Suppose $(G, *)$ is an abelian group. For any $a, b \in G$ and positive integer k, show that $(a * b)^k = a^k * b^k$. Give an example to show that this is not necessarily true if G is not abelian.

(k) CHALLENGE: Suppose G is a finite group (meaning the set G has finitely many elements) and let $a \in G$. Then there exists some positive integer k such that $a^k = e$.

(l) CHALLENGE: Suppose G is a finite group and let $a \in G$. The *smallest* positive integer k such that $a^k = e$ is called the *order* of a, denoted $\text{ord}(a)$. Prove that for an abelian group G and any $a, b \in G$, $\text{ord}(a * b)$ divides $\text{lcm}(\text{ord}(a), \text{ord}(b))$.

Definition 4. A group G is said to be *cyclic* if there is some $a \in G$ such that $G = \{a^n : n \in \mathbb{Z}\}$, i.e. if every element of G can be written as some power of a.

Exercise 3. Decide whether or not the following groups are cyclic, and prove your answers.

(a) The group in problem 1(**??**)

(b) The group in problem 1(**??**)

(c) The group in problem 1(**??**)

Exercise 4. Prove that all cyclic groups are abelian.

3 Subgroups

Definition 5. Let $(G, *)$ be a group and let H be a subset of G. H is said to be a *subgroup* of G if H is closed under the operation $*$ (meaning that if $a, b \in H$, then $a * b \in H$ also) and H forms a group under the operation $*$.

Exercise 5. Determine whether the subset H is a subgroup of the given group G. If so, prove that the subset is a subgroup. If not, find a counterexample for each property that does not hold.

(a) Let $G = (\mathbb{Z}, +)$ from Exercise 1(a). Let H be the subset of all even integers.

(b) Let $G = (\mathbb{Z}, +)$ from Exercise 1(a). Let H be the subset of all odd integers.

(c) Let $G = D_4$, the group of symmetries of the square. Let H be the subset of all rotations of the square.

(d) Let $G = D_4$, the group of symmetries of the square. Let H be the subset of all reflections of the square.

(e) Let G be the group described in Exercise 1(k). Let $H = \{e, y_1\}$.

(f) Let G be the group described in Exercise 1(k). Let $H = \{e, x_1\}$.

Exercise 6. Let $(G, *)$ be a group and let H be a subset of G that is closed under inverses. Prove that H is a subgroup of G if and only if H is closed under the operation $*$.
(Hint: H being closed under $*$ is part of the definition of subgroup. So what you need to show is that if H is closed under $*$, then the other group properties are automatically also satisfied for H.)

Exercise 7. (a) Find all subgroups of the group $(\mathbb{Z}, +)$.

(b) Find all subgroups of the group $(\mathbb{Z}/n\mathbb{Z}, +)$.

(c) Find all subgroups of the group D_5.