Group Theory

Prepared by Mark on January 19, 2023

Part 1: A Review of Functions

Definition 1:
A *function* or *map* f from a set A (the *domain*, $\mathcal{D}$) to a set B (the *range*, $\mathcal{R}$) is a rule that assigns an element of B to each element of A. We write this as $f : A \to B$.

Consider a function $f : \mathbb{Z} \to \mathbb{Z}$. If $f(1) = 2$, we say that 2 is the *image* of 1 and 1 is a *preimage* of 2 under f.

An element in a function's domain must have exactly one image. However, an element in the range may have more than one preimage.

Problem 1:
Consider the function $f : \mathbb{R} \to \mathbb{R}^+ \cap \{0\}$ defined by $f(x) = x^2$
- What is the image of 2?
- What are the preimages of 9?

Definition 2:
We say a map is *one-to-one* if $a = b \implies f(a) = f(b)$ for all a, b in the domain. In other words, this means that each element of the range has at most one preimage.

Definition 3:
We say a map f is *onto* if, for every $y \in \mathcal{R}$, there exists an $x \in \mathcal{D}$ so that $f(x) = y$. In other words, this means that every y in the range has a preimage in the domain.

Problem 2:
Find a function that is...
- neither one-to-one nor onto
- one-to-one and not onto
- not one-to-one, but onto
- both one-to-one and onto

We say a function that is both one-to-one and onto is *bijective*.

Definition 4:
Let $f : A \to B$ and $g : B \to C$. We can define a new function $(g \circ f) : A \to C$, where $(g \circ f)(a) = g(f(a))$. This is called *composition*.

Problem 3:
Suppose $f : A \to B$ and $g : B \to C$ are both one-to-one. Must $(g \circ f)$ be one-to-one? Provide a proof or a counterexample.

Problem 4:
Suppose $f : A \to B$ and $g : B \to C$ are both onto. Must $(g \circ f)$ be onto? Provide a proof or a counterexample.

Part 2: A Review of Modular Arithmetic

Definition 5:
$\mathbb{Z}_n$ is the set of integers mod n. For example, $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$.
You should all be familiar with modular arithmetic.

Definition 6:
The inverse of an element a in $\mathbb{Z}_n$ is a b so that $a \times b \equiv 1$.
Not all elements of $\mathbb{Z}_n$ have an inverse. Those that do are called *units*.

The set of all units in $\mathbb{Z}_n$ is written $(\mathbb{Z}_n)^\times$
Read this as "$\mathbb{Z}$ mod n cross"

Problem 5:
What are the elements of $(\mathbb{Z}_5)^\times$?

Problem 6:
Create an addition table for $\mathbb{Z}_4$ and a multiplication table for $(\mathbb{Z}_5)^\times$

$+$	0	1	2	3
0	?	?	?	?
1	?	?	?	?
2	?	?	?	?
3	?	?	?	?

Part 3: Groups

Group theory gives us a set tools for understanding complex systems. We can use groups to solve the Rubik's cube, to solve problems in physics and chemistry, and to understand complex geometric symmetries. It's also worth noting that all modern crypography relies heavily on group theory.

Definition 7:
A *group* $(G, *)$ consists of a set G and an operator $*$.
A group must have the following properties:

1. G is closed under $*$. In other words, $a, b \in G \implies a * b \in G$.
2. $*$ is associative: $(a * b) * c = a * (b * c)$ for all $a, b, c \in G$
3. There is an *identity* $e \in G$, so that $a * e = a * e = a$ for all $a \in G$.
4. For any $a \in G$, there exists a $b \in G$ so that $a * b = b * a = e$. b is called the *inverse* of a. This element is written as $-a$ if our operator is addition and a^{-1} otherwise.

Any pair $(G, *)$ that satisfies these properties is a group.

Problem 7:
Is $(\mathbb{Z}_5, +)$ a group?
Is $(\mathbb{Z}_5, -)$ a group?
Hint: $+$ and $-$ refer to our usual definition of modular arithmetic.

Problem 8:
Show that $(\mathbb{R}, \times)$ is not a group, then make it one by modifying $\mathbb{R}$.

Problem 9:
Show that a group has exactly one identity element.

Problem 10:
Show that each element in a group has exactly one inverse.

Problem 11:
Show that $(\mathbb{Z}_n^\times, \times)$ is a group for any $n \in \mathbb{Z}^+$.

Problem 12:
Let $(G, *)$ be a group and $a, b, c \in G$. Show that...

- $a * b = a * c \implies b = c$
- $b * a = c * a \implies b = c$

This means that we can "cancel" operations in groups, much like we do in algebra.

Problem 13:
What is the smallest group we can create?

Problem 14:
Let G be the set of all bijections $A \to A$.
Let $\circ$ be the usual composition operator.
Is $(G, \circ)$ a group?

Definition 8:
Note that our definition of a group does **not** state that $a * b = b * a$.
Many interesting groups do not have this property. Those that do are called *abelian* groups.

One example of a non-abelian group is the set of invertible 2x2 matrices under matrix multiplication.
In this handout, all groups are abelian.

Problem 15:
Show that if G has four elements, $(G, *)$ is abelian.

Problem 16:
Let $(G, *)$ be a finite group (i.e, G has finitely many elements), and let $g \in G$.
Show that $\exists\ n \in \mathbb{Z}^+$ so that $g^n = e$
Hint: $g^n = g * g * ... * g$ n times.

The smallest such n defines the *order* of g.

Problem 17:
What is the order of 5 in $(\mathbb{Z}_{25}, +)$?
What is the order of 2 in $(\mathbb{Z}_{17}^{\times}, \times)$?

Part 4: Isomorphisms

Definition 9:
We say two groups are *isomorphic* if we can create a bijective mapping between them while preserving multiplication structure. This mapping is called an *isomorphism*.

This means that if groups A and B are isomorphic under f,
$a_1 * a_2 = a_3$ in A implies that $f(a_1) * f(a_2) = f(a_3)$ in B.

Problem 18:
Recall your tables from Problem 6:

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\times$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Are $(\mathbb{Z}_4, +)$ and $(\mathbb{Z}_5^{\times}, \times)$ isomorphic? If they are, find a bijection that maps one to the other.

Problem 19:
Let groups A and B be isomorphic under f. Show that $f(e_A) = e_B$, where e_A and e_B are the identities of A and B.

Problem 20:
Let groups A and B be isomorphic under f.
Show that $f(a^{-1}) = f(a)^{-1}$ for all $a \in A$.

Problem 21:
Let groups A and B be isomorphic under f. Show that $f(a)$ and a have the same order.

Problem 22:
Find all distinct groups of two elements.
Find all distinct groups of three elements.
Groups that are isomorphic are not distinct.

Problem 23:
Show that the groups $(\mathbb{R}, +)$ and $(\mathbb{R}^+, \times)$ are isomorphic.

Part 5: Bonus

Problem 24:
Find the inverse of 19 in $\mathbb{Z}_{23}$
Hint: Recall the Euclidean Algorithm

Problem 25:
Prove Lagrange's theorem:

$$a^p = a \pmod{\text{p}}$$

For positive integers a, p

Problem 26:
Let a and m be integers so that $a < m$.
Show that a has an inverse mod m iff $\gcd(a, m) = 1$

Problem 27:
Show that for any integers a, b, c,
$\gcd(ac + b, a) = \gcd(a, b)$