Group Theory

Anish Kulkarni, Vavilala Chidvilas

July 1, 2024

1 Preliminaries

1.1 Function

Let A, B be sets. Intuitively a function from A to B takes a value from A and gives a value in B.

Formal Definition

A function f from A to be B, denoted as $f : A \to B$ is a subset U of $A \times B$ such that for all $x \in A$, there is a unique y in B such that $(x, y) \in U$, in this case we write it as

$$f(x) = y$$

- A function $f : A \to B$ is called **surjective** if for every $b \in B$, there is an $a \in A$ such that $f(a) = b$.
- A function $f : A \to B$ is called **injective** if for every $a_1, a_2 \in A$, $f(a_1) = f(a_2)$ implies $a_1 = a_2$.
- A function $f : A \to B$ is called **bijective** if it is both surjective and injective.

2 Binary Operation

2.1 Definition

Consider a set S, a binary operation $< \bullet >$ on S is a function $f : S \times S \to S$.
The operation is denoted by

$$a \bullet b = f(a, b)$$

2.2 Examples

- Natural numbers $\mathbb{N}$ under the operation $+$.
- Natural numbers $\mathbb{N}$ under the operation $\times$.
- Complex numbers $\mathbb{C}$ with absolute value 1 under $\times$.
- Bijective functions from $\mathbb{N}$ to itself under composition. (i.e here the operation is function composition, $f \bullet g = f \circ g$). Note: Composition of bijective functions is bijective.
- Continuous functions from $\mathbb{R}$ to $\mathbb{R}$ under composition. Note this is true because composition of continuous functions is continuous.

2.3 Incorrect Examples

- Surjective functions from $\mathbb{N}$ to itself under composition. Because composition of two surjective functions may not be surjective. (can you find examples?)
- Continuous functions from $[0, 1]$ to $[2, 3]$ under composition. (Why?)

2.4 Exercises

1. Find two surjective functions f, g from $\mathbb{N}$ to $\mathbb{N}$ such that $f \cdot g$ is not surjective.
2. Explain why composition does not form a binary operation on the set of continuous functions from $[0, 1]$ to $[2, 3]$.
3. Now we shall manually define a binary operation on the set $S = \{a, b, c\}$
   Say $a \bullet b = a, b \bullet c = a$ and $c \bullet a = b$. Is this a valid binary operation? Why?

3 Group

3.1 Defintion

A group $< G, \bullet >$ is a set G equiped with a binary operator $\bullet$ such that the following properties are satisfied

1. $\forall a, b, c \in G, (a \bullet b) \bullet c = a \bullet (b \bullet c)$ Associativity of binary operation
2. $\exists e \in G$ such that $\forall a \in G$, $a \bullet e = e \bullet a = a$.
   Such an element e will be called an identity.
3. $\forall a \in G, \exists a' \in G$ such that $a \bullet a' = a' \bullet a = e$, where e is an identity.
   This a' will be called an inverse of a.

3.2 Examples

- The set of integers $\mathbb{Z}$ under addition.
- The set of invertible $n \times n$ matrices under multiplication.
- The set of bijective functions from a set to itself under composition.
- The set of symmetries of a square under composition. [See section 5 about symmetries]

3.3 Exercises

1. In each of the above examples identify the identity and inverses of elements.
2. Prove, using formal argument that in any group G, the identity is unique. That is, if e and f are two identities then show that $e = f$.
3. Prove that for every element $a \in G$, inverse of a is unique.
4. **Cancellation:** If $a \bullet b = a \bullet c$ then $b = c$.

4 Subgroup

4.1 Definition

A subset H of a group G is called a subgroup of G if H is a group under the same operation as G. (Note it is implicit that H is closed under the operation on G.)

4.2 Some Notation

- Due to associativity, $a \bullet (b \bullet c) = (a \bullet b) \bullet c$ and hence we can write $a \bullet b \bullet c$ without any ambiguity. This is sometimes further simplified to just abc when the operation is unambiguous.
- A special case is $a^n = a \bullet a \bullet \cdots \bullet a$ where a occurs n times.
- For $n = 0$ we define $a^0 = e$ and for $n < 0$ we define $a^n = (a^{-1})^{-n}$ where a^{-1} refers to an inverse of a.

4.3 Some Special Subgroups

Let G be a group and $a \in G$, then the set $\{a^n | n \in \mathbb{Z}\}$ is a subgroup of G. This is called the cyclic subgroup generated by a and is denoted by $\langle a \rangle$.
Similarly let S be a subset of G then the subgroup generated by S is the set of elements of form $\{u_1 \bullet u_2 \bullet \cdots \bullet u_n : u_i \in S \text{ or } u_i^{-1} \in S\}$ where the u_i are not necessarily distinct and $n = 0$ corresponds to identity.

4.4 Exercises

1. Let G be a group with identity e, if H is an subgroup show that $e \in H$.
2. Is the set of odd integers a subgroup of integers? What about the set of even integers? Can you classify all subgroups of $\mathbb{Z}$?
3. Let G be a group and S be a set of elements of G. Prove that the subgroup generated by S is the smallest subgroup (under inclusion) of G containing all elements of S.
4. Let H, K be subgroups of a group G. Is $H \cap K$ also a subgroup of G? And what about $H \cup K$? If $\{H_i : i \in I\}$ is an infinite family of subgroups of G then is $\cap_{i \in I} H_i$ a subgroup?
5. Using above two results show that the subgroup generated by a set S is the intersection of all subgroups containing S.

5 Symmetries

5.1 What are symmetries and isometries?

An isometry of $\mathbb{R}^2$ is a mapping $\phi : \mathbb{R}^2 \to \mathbb{R}^2$ that preserves distance, i.e the distance between points P and Q is the same as the distance between the points $\phi(P)$ and $\phi(Q)$ for all points P and Q in $\mathbb{R}^2$. Symmetry of a figure S which lies in a plane $\mathbb{R}^2$ is any isometry(let ω) of $\mathbb{R}^2$ in which the set of points of figure S is mapped onto itself. (i.e the image of set S in the mapping ω is S itself). To put in simple words, a symmetry is a mapping in which the image of the figure under consideration in the $\mathbb{R}^2$ plane overlaps exactly with the figure itself. It can be shown that in a plane any symmetry is a composition of rotation, reflection and translation.
Eg: A mapping $\phi : \mathbb{R}^2 \to \mathbb{R}^2$ given by $\phi(x, y) = (y, -x)$ is an isometry of $\mathbb{R}^2$ and also a symmetry of square centred at origin, whereas another mapping $\phi : \mathbb{R}^2 \to \mathbb{R}^2$ given by $\phi(x, y) = (x + 5, y + 5)$ is an isometry of $\mathbb{R}^2$ but not a symmetry of square centred at origin.

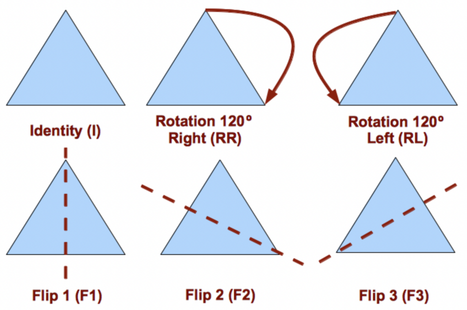
Symmetries and Isometries

5.2 How are groups and symmetries interrelated?

Above we discussed an isometry $\phi : \mathbb{R}^2 \to \mathbb{R}^2$, now if ψ is also an isometry of S, then the distance between $\psi(\phi(P))$ and $\psi(\phi(Q))$ must be the same as the distance between $\phi(P)$ and $\phi(Q)$, which in turn is the distance between P and Q, showing that the composition of two isometries is again an isometry. Since the identity map is an isometry and the inverse of an isometry is an isometry, so the three properties for a group are satisfied hence the **set of isometries of $\mathbb{R}^2$ forms a group**. Given any subset S of $\mathbb{R}^2$(for eg: set of points of a figure), the isometries of $\mathbb{R}^2$ that carry S onto itself form a subgroup of the group of isometries. This subgroup is the **group of symmetries of S in $\mathbb{R}^2$**.
Now comes the thing, the elements of a group can be thought of as the symmetries of a figure, i.e any group can be visualised as Group of Symmetries of some figure S, and surprisingly this can be done for any group(we wont prove this now). For eg: The group as defined below (see its group operations table) can be thought of as the group formed by symmetries of an equilateral triangle in the plane. These symmetries include identity, rotations around center by 120° and 240° and reflections about the axes passing through a vertex and the center. The element ρ_0 can be thought as identity, ρ_1 can be thought as 120 degree rotation, ρ_2 can be thought as 240 degree, μ_1 can be thought as reflection about altitude passing through vertex 1 and similarly others.

	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_0	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_1	ρ_1	ρ_2	ρ_0	μ_3	μ_1	μ_2
ρ_2	ρ_2	ρ_0	ρ_1	μ_2	μ_3	μ_1
μ_1	μ_1	μ_2	μ_3	ρ_0	ρ_1	ρ_2
μ_2	μ_2	μ_3	μ_1	ρ_2	ρ_0	ρ_1
μ_3	μ_3	μ_1	μ_2	ρ_1	ρ_2	ρ_0

(a) A group of 6 elements



(b) Symmetries of triangle

Figure 1: Group as symmetry

5.3 Exercises

1. Draw a plane figure that has a three-element group as its group of symmetries in $\mathbb{R}^2$

2. Let S be the set of integral points on the real line. Consider all the symmetries of the real line that fix S and maintain the rightward increasing order (For example, one possible symmetry is : Mapping x to x+1 for all x on the real line, i.e moving every point to the right by one unit). Show that these form a group under composition and this group has same structure as $\mathbb{Z}$ under addition.

6 Homomorphisms

6.1 Definition

Let U, V be two groups. A function $\phi : U \to V$ is called a homomorphism between U and V if it respects the group operations, that is

$$\phi(u_1 \bullet_U u_2) = \phi(u_1) \bullet_V \phi(u_2)$$

where $\bullet_U$ and $\bullet_V$ respectively denote the group operations in U and V.

6.2 Examples

- Consider R^n to be a group under vector addition. Then any linear transformation from R^n to itself is a group homomorphism.
- Consider $\mathbb{C}, \mathbb{R}$ to be groups under addition. Then $\phi : \mathbb{C} \to \mathbb{R}$ given by $\phi(z) = Re(z)$ is a group homomorphism.

6.3 Proposition

A homomorphism takes identity to identity.

Proof
Let $\phi : U \to V$ be a homomorphism, let e_U and e_V denote the identity elements in U and V.
Note that

$$\phi(e_U) = f(e_U \bullet_U e_U) = \phi(e_U) \bullet_V \phi(e_U)$$

But also

$$\phi(e_U) = e_V \bullet_V \phi(e_U)$$

Now use Cancellation Law to get $f(e_U) = e_V$

6.4 Exercises

1. Prove that homomorphism takes inverse of an element to inverse of its image.
2. Let $\phi : U \to V$ be a homomorphism. Let $K = \{x \in U : \phi(x) = e_V\}$, then show that K is a subgroup of U. This K is called the kernel of the homomorphism ϕ.
3. Let $\phi : U \to V$ be a homomorphism. Let $H = \{y \in V : y = \phi(x) \text{ for some } x \in U\} = Im(\phi)$, then show that H is a subgroup of V. This H is called the image of the homomorphism ϕ.