Group Theory

Arifa Alam

November 25, 2024

1 Basics

Laws of compositions:

- **Associative Law**: $(ab)c = a(bc)$
- **Commutative Law**: $ab = ba$

These two laws shown using the product operation. However, a group may have other operation such as addition.

Let $g \circ f$ denote as the composition of two functions g and f. Then for functions g, f, and h the associativity holds but comutativity necessearly doesn't (take matrix multiplication, for example). In other words–

$$(g \circ f) \circ h = g \circ (f \circ h)$$

Identity of law of compostions is defined as–

$$ae = ea = a$$

(and yes, $a = e$)

> **Definition 1.1: Groups**
>
> A group is a set G which should satisfy these following properties–
>
> - Associative for every element in G.
> - Exist identity element, unique.
> - Exist inverse for all element in G.

A group is *abelian* if its law of compostion is commutative. Such as $\mathbb{Z}^+, \mathbb{R}^+, \mathbb{R}^\times, \mathbb{C}^+, \mathbb{C}^\times$ The $\times$ and $+$ signs are defining the operations, not the set.

Order of a group is defined as its cardinality, $|G|$.

Theorem 1.1: Cancellation Law

Let a, b, and c be elements of G whose law of composition is written multiplicatively. If $ab = ac$ or $ba = ca$ then $b = c$. And if $ab = a$ and $ba = a$ then $b = 1$.

Proof. Just multiply with a^{-1} in both left and right side of the term. □

Definition 1.2: Subgroup

A subset H of a group G must have the following properties:

- *Closure*: If $a \in H \implies ab \in H$.
- *Identity*: $1 \in H$
- *Inverse*: $a \in H \implies a^{-1} \in H$

A subgroup is proper subgroup if it's not trivial subgroup. And they are–

- The group itself
- The subgroup only with identity

Some examples of subgroup are–

- *circle group*: Let group $G = \mathbb{C}$ for which absolute value of every element in $\mathbb{C}$ is equals to 1. The unit circle of the plane is the subgroup of G, which is the circle group.
- *special linear group*: G is the set of $n \times n$ matrices. Matrices with determinant 1 are subgroup of G, which is a special linear group also known as SL_n. And G is known as *general linear group* GL_n

Theorem 1.2

Let S be a subgraoup of the additive group of $\mathbb{Z}^+$. Either S is the trivial subgroup 0, or else it has to be in the form $\mathbb{Z}a$, where a is the smallest positive integer in S.