Class 3: Groups - 2022/09/14

Motivating Examples

1. The set of integers $\mathbb{Z}$, we have addition defined on it: $a+b$
   - Associative: $(a+b)+c=a+(b+c)$
   - Commutative: $a+b=b+a$
   - $0 \in \mathbb{Z}$. such that $a+0=0+a=a$ for any $a \in \mathbb{Z}$.
   - $\forall a \in \mathbb{Z}$, it has an "inverse": $-a \in \mathbb{Z}$

     such that $a+(-a)=(-a)+a=0$
2. The set of $n \times n$ invertible matrices with $\mathbb{R}-entries$
   - **Denoted** by $GL_n(\mathbb{R})$
   - On $GL_n(\mathbb{R})$, a matrix multiplication can be defined.
     - $GL_n(\mathbb{R}) \times GL_n(\mathbb{R}) \to GL_n(\mathbb{R})$
     - $(A,B) \mapsto AB$

> Note that $AB \in GL_n(\mathbb{R})$ since A and B invertible $\Rightarrow$ AB invertible.
>
> $|A|=0, |B|=0$, so $|AB|=|A||B|=0$

   - Associative: $(AB)C=A(BC)$
   - Commutative: Holds only when $n=1$.
     - In general we know $AB \neq BA$
   - Identity Matrix :

$$I=\begin{bmatrix} 1 & \dots & \dots \\ \dots & 1 & \dots \\ \dots & \dots & 1 \end{bmatrix}$$

     - $\forall A \in GL_n(\mathbb{R}), IA=AI=A$
     - $\forall A \in GL_n(\mathbb{R})$, it has inverse matrix A^{-1}, $AA^{-1}=A^{-1}A=I$

Group

Definition

- A Group is a nonempty set G with an operation (also called Law of Composition) on it.
    - $G \times G \to G$ (means an operation, not necessarily multiplication)
    - $(g_1, g_2) \mapsto g_1 g_2$
- It satisfies the conditions below
    - Associative: $\forall x, y, z \in G, (xy)z = x(yz)$
    - $\exists 1 \in G, \quad \forall g \in G, \quad 1 \cdot g = g \cdot 1 = g$. ($1$ is called the identity)
    - $\forall g \in G, \quad \exists g^{-1} \in G, \quad gg^{-1} = g^{-1}g = 1$. ($g^{-1}$ is called the inverse of g)
- If a groups is also commutative (i.e. $\forall g_1, g_2 \in G, g_1 h_2 = g_2 g_1$), then we say it's an **abelian group** (named after Abel)
- We see the two motivating examples are groups
- Remarks on notation:
    - e is also often used to denote identity
    - If G is abelian, we can use 0 for identity and $+$ for composition
    - In general, the composition is usually denoted by ab, $a \cdot b$, $a * b$, ...

Example of Groups:

1. The trivial group: $G = \{1\}$
    - Composition: $1 \cdot 1 = 1$
2. $\mathbb{R}^x = \mathbb{R} - \{0\}$ with multiplication is a group.
    - Set: the real number except 0
    - Law of Composition: multiplication
    - Associative: $(ab)c = a(bc)$
    - identity: $1 \in \mathbb{R}^x: \ \forall a \in \mathbb{R}^x, \ a \cdot 1 = 1 \cdot a = a$
    - inverse: $\forall a \in \mathbb{R}^x, \ a\frac{1}{a} = \frac{1}{a}a = 1$

    > We delete 0 because 0 doesn't have an inverse.

    - Furthermore, $\mathbb{R}^x$ is an abelian group.
3. Let S be a set of n elements. Say $S = \{1, 2, \ldots n\}$

    Let G be the set of all bijections on S. Each element is a function $S \to S$.

    Then G with the function composition forms a group:

    $$G \times G \to G$$
    $$(f_1, f_2) \mapsto f_1 \circ f_2$$

    > Note that $f_1 \circ f_2$ is also bijective, so it's in G.

    - associative: $(f_1 \circ f_2) \circ f_3 = f_1 \circ (f_2 \circ f_3)$
    - identity: identity function id_s
        - $\forall f \in G, \ \ f \circ id_s = id_s \circ f = f$
    - inverse: $\forall f \in G$, its invers function f^{-1} is its inverse:
        - $f \circ f^{-1} = f^{-1} \circ f = id_s$

Remarks:

- We will use S_n to denote this group.
- Called the symmetric groups or permutation group.

Theorems

- **Theorem**: In a group G, the identity is unique

  Proof:

  - If 1, 1' are both identities of G, then $1 = 1 \cdot 1' = 1'$

> “
>
> Inverse of $g \in G$ is also unique

- **Theorem** (Cancellation Law): If G is a group, $x, y, z \in G$, the $xy = xz \Rightarrow y = z$

  Proof:

$$
\begin{aligned}
xy &= xz \\
x^{-1}(xy) &= x^{-1}(xz) \\
(x^{-1}x)y &= (x^{-1}x)z \\
1 \cdot y &= 1 \cdot z \\
y &= z
\end{aligned}
$$

> “
>
> **NOTE**: $\mathbb{R}$ with multiplication is NOT a group.
>
> - Because $0 \in \mathbb{R}$ has no inverse, cancellation law is not true on $\mathbb{R}$
>   - Ex: $x(x-1) = 2x$
> - On the other hand, $\mathbb{R}$ with addition is a group, so cancellation law holds.
>   - $a + b = a + c \quad \Rightarrow \quad b = c$