Binary Operation

Definition: Let S be a non-empty set. A map $*: S \times S \to S$ is called a binary operation on S.

For example, if $S = \mathbb{R}$, then $* = \cdot$ is a binary operation. We also have $* = +$ is a binary operation on $\mathbb{R}$.

Groups

Definition: Let G be a non-empty set a $*$ a binary operation on G. We say $(G, *)$ is a group if it satisfies:

(i) We have $g_1 * g_2 \in G$ for all $g_1, g_2 \in G$, i.e., G is closed under $*$;

(ii) We have $(g_1 * g_2) * g_3 = g_1 * (g_2 * g_3)$ for all $g_1, g_2, g_3 \in G$ i.e., $*$ is associative;

(iii) There exists $e \in G$ so that $g * e = g = e * g$ for all $g \in G$. We call e the identity element of G

(iv) For each $g \in G$, there exists $g^{-1} \in G$ so that $g * g^{-1} = e = g^{-1} * g$. We refer to g^{-1} as the inverse of g.

Note we often write G for a group instead of $(G, *)$ when $*$ is clear from the context.

Example: Consider the set $\mathbb{Z}_{<0}$ of negative integers and the binary operation $\cdot$.

We have $-1 \in \mathbb{Z}_{<0}$, but $(-1) \cdot (-1) = 1 \notin \mathbb{Z}_{<0}$.

Thus, $\mathbb{Z}_{<0}$ is not closed under multiplication.

Example: Let $G = \mathbb{Z}$ and $* = + =$ addition. We have that $\mathbb{Z}$ is non-empty.

(i) If you add two integers, you get another integer so $\mathbb{Z}$ is closed under addition.
(ii) We know addition in $\mathbb{Z}$ is associative.
(iii) In this case we have $e=0$ because $0+n=n=n+0$ for all $n \in \mathbb{Z}$.
(iv) Let $n \in \mathbb{Z}$. We have $(-n)+n=0=n+(-n)$, so $-n$ is the inverse of n under $+$.

Thus, $(\mathbb{Z},+)$ is a group.

Example: Let $G=\mathbb{Z}$ and $* = \cdot =$ multiplication. We again have $\mathbb{Z}$ is non-empty.

(iii) In this case we have $e=1$ because $1 \cdot n = n = n \cdot 1$ for all $n \in \mathbb{Z}$.
(iv) Consider $n = 2 \in \mathbb{Z}$. There is no integer m so that $2m=1$. In fact, we know $m = 1/2$, but $1/2 \notin \mathbb{Z}$. Thus, not all elements in $\mathbb{Z}$ have inverses.

Thus, $(\mathbb{Z},\cdot)$ is NOT a group.

Abelian

Definition: Let $(G,*)$ be a group. If $g*h = h*g$ for all $g,h \in G$ we say $(G,*)$ is abelian.

The group $(\mathbb{Z},+)$ is an abelian group.

special linear group of 2x2   s.t. det. = 1

Example: Let $G = SL_2(\mathbb{R}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a,b,c,d \in \mathbb{R},\ ad-bc=1 \right\}$. Let $*$ be matrix multiplication, i.e.

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} * \begin{bmatrix} s & t \\ u & v \end{bmatrix} = \begin{bmatrix} as+bu & at+bv \\ cs+du & ct+dv \end{bmatrix}$$

We have G is non-empty as $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in SL_2(\mathbb{R})$

(i) Let $g_1 = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, $g_2 = \begin{bmatrix} s & t \\ u & v \end{bmatrix} \in SL_2(\mathbb{R})$. We have $g_1 g_2$ is still a 2x2 matrix with real entries.

Note that $\det\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) = ad - bc$.

Since $\det(g_1 g_2) = \det(g_1)\det(g_2) = 1 \cdot 1 = 1$, we have $SL_2(\mathbb{Z})$ is closed under multiplication.

(ii) Checking that multiplication is associative is a huge pain.

Recall that each matrix corresponds to a linear transformation and matrix multiplication corresponds to composition of linear transformations — and then its easier to check compositions of functions are associative

(iii) The identity in this case is $e = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

(iv) The inverse of $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is $\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$.

Thus, G is a group.

However, G is NOT abelian as we have

$$g_1 = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}, \quad g_2 = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \in SL_2(\mathbb{R}) \text{ but}$$

$$g_1 g_2 = \begin{bmatrix} -1 & 2 \\ -1 & 1 \end{bmatrix} \neq \begin{bmatrix} 1 & 1 \\ -2 & -1 \end{bmatrix} = g_2 g_1$$