1 Group

Definition: group

A **group** is a binary structure $(G, *)$ s.t.

1) $(G, *)$ is associative
2) (G,*) has an identity: there exists $e \in G$ s.t.

$$e * g = g * e = g \quad \forall g \in G.$$

3) $(G, *)$ has two-sided inverses for all $x \in G$, there exists a $y \in G$ s.t.

$$x * y = y * x = e.$$

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

Definition: abelian group

A group in which $*$ is commutative is called **abelian**.

Example.
- $\mathbb{Z}^+$ under $+$: has no identity.
- N_0 under $+$: 1 doesn't have an inverse.
- $(\mathbb{Q}^*, x)$ nonzero rationals under $\times$: yes
- $(\mathbb{Q}, \times)$: 0 doesn't have an inverse.
- $(\mathbb{Z}^\times, \times)$ nonzero integers under $\times$: 2 doesn't have an inverse.
- $(\mathbb{Z}_n, +_n)$ integers mod n under addition mod n is a group. Associativity is not obvious yet.
- $(\mathbb{Z}_7^*, \times_7)$ is a group.
- $(M_n(\mathbb{R}), +)$ $n \times n$ matrices with real entries under matrix addition: is a group.
- $(M_n(\mathbb{R}), \times)$ under matrix multiplication. The zero matrix have no inverse.
- $(GL_n(\mathbb{R}), \times)$ the invertible $n \times n$ matrices in the general linear group under $\times$.

- $GL_2(\mathbb{R})$ is nonabelian.

$$\begin{pmatrix}1 & 1\\0 & 1\end{pmatrix}\begin{pmatrix}1 & 0\\1 & 1\end{pmatrix}=\begin{pmatrix}2 & 1\\1 & 1\end{pmatrix}$$
$$\begin{pmatrix}1 & 0\\1 & 1\end{pmatrix}\begin{pmatrix}1 & 1\\0 & 1\end{pmatrix}=\begin{pmatrix}1 & 1\\1 & 2\end{pmatrix}$$

Proof

Suppose $a * b = b * c$, then

$$\begin{aligned} a^{-1} * (a * b) &= a^{-1} * (a * c) \\ (a^{-1} * a) * b &= (a^{-1} * a) * c \\ e * b &= e * c \\ b &= c \end{aligned}$$

□

Example (group with 3 elements)**.** $(\mathbb{Z}_3, +_3)$.

G={e,a,b}.

*	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

Remark. Any group with 3 elements is $\rightarrow(\mathbb{R}_3, +_3)$.

Example (groups of order 2)**.**

*	e	a
e	e	a
a	a	e

Example (groups of order 4)**.** See iPad.

Example. $(U, \times)$ (all complex numbers that form unit circle) and $(U_n, \times)$ are groups.