Definition 2.1

A *group* is set G equipped with an operation that assigns to each pair of elements $a, b \in G$ an element $a \cdot b \in G$ in such way, that the following conditions are satisfied:

1) For any $a, b, c \in G$ we have

$$(a \cdot b) \cdot c = a \cdot (b \cdot c)$$

(associativity).

2) There exists an element $e \in G$ such that

$$e \cdot a = a \cdot e = a$$

for all $a \in G$. The element e is called the *identity element* or the *trivial element*.

3) For each element $a \in G$ there exists an element $b \in G$ such that

$$a \cdot b = b \cdot a = e$$

Such element b is called the *inverse* of a and it is denoted by a^{-1}.

Definition 2.2

A *abelian group* is a group G where the multiplication is commutative:

$$a \cdot b = b \cdot a$$

for all $a, b \in G$.

<u>Notation</u>

Multiplicative:

- $a \cdot b, \quad a \times b, \quad a * b, \quad a \circ b, a \odot b, \ldots$
- **Inverse element:** a^{-1}.
- **The identity element:** e, 1, ...

Additive:

- $a + b$
- **Inverse element:** $-a$.
- **The identity element:** 0.

Note: The additive notation is only used for abelian groups.

Some examples of groups

Example: General linear groups $GL(n, \mathbb{R})$.

Example: **Groups $\mathbb{Z}_n$**

Example: **Groups $U(n)$**

Recall:

- If m, n are integers then the *greatest common divisor* of m and n, denoted $\gcd(m, n)$, is the greatest integer that divides both m and n.

- $\gcd(m, n) = \gcd(m + kn, n)$ for any $k \in \mathbb{Z}$.

- For any $m, n \in \mathbb{Z}$ there exists $p, q \in \mathbb{Z}$ such that

$$pm + qn = \gcd(m, n)$$

  Moreover, $\gcd(m, n)$ is the smallest positive integer that can be obtained for any choice of p and q.