Chapter 1

Groups

Additive Group	Multiplicative Group
Let G be a set, and $+$ be an operation, then $(G, +)$ is an additive group provided	Let G be a set, and be an operation, then $(G, \circ)$ is an multiplicative group provided
1. $\forall a, b \in G,\ a + b \in G$	6. $\forall a, b \in G,\ a \circ b \in G$
2. $\forall a, b, c \in G,\ a + (b + c) = (a + b) + c$	7. $\forall a, b, c \in G,\ a \circ (b \circ c) = (a \circ b) \circ c$
3. $\forall a \in G, \exists 0 \in G$ (identity) s.t. $$a + 0 = a = 0 + a$$	8. $\forall a \in G, \exists 1 \in G$ (unity) s.t. $$a \circ 1 = a = 1 \circ a$$
4. $\forall a \in G, \exists -a \in G$ (additive inverse) s.t. $$a + (-a) = 0 = (-a) + a$$	9. $\forall a \in G, \exists a^{-1} \in G$ (unity) s.t. $$a \circ a^{-1} = 1 = a^{-1} \circ a$$
5. (Commutative) $\forall a, b \in G,\ a + b = b + a$	10. (Commutative) $\forall a, b \in G,\ a \circ b = b \circ a$

Joining additive and multiplicative groups together, we form a ring with **distributive laws**

$$\begin{aligned} &11. \quad \forall a, b, c \in G, (a + b) \circ c = (a \circ c) + (b \circ c) \\ &12. \quad \forall a, b, c \in G, c \circ (a + b) = (c \circ a) + (c \circ b) \end{aligned}$$

- Abelian group: (1-5) or (6-10)
- Associative Ring: 1-6, with 11 and 12
- Semigroup: 1, 2 only
- Monoid: 1, 3 only
- Commutative ring: 1-5, 6, 10, 11, and 12

- Ring: 1-5, with 11 and 12
- Ring with unity: 1-6, with 8, 11, and 12
- Field: 1-12

Theorem 1.1 Socks-shoes property

$$(a \circ b)^{-1} = b^{-1} \circ a^{-1} \tag{1.1}$$

Remark. In abstract algebra, the position of inputs in binary operator is very important! The commutative property no necessary hold. $a \circ b \neq b \circ a$. E.g. matrix multiplication $AB \neq BA$.

Theorem 1.2
The following statements are equivalent.

1. Every subgroup of a cyclic group (multiplicative group) is cyclic.
2. If $|\langle a \rangle| = n$, then the order of any subgroup of $\langle a \rangle$ is a divisor of n.
3. For each positive divisor $k|n$, $\langle a \rangle$ has exactly one subgroup of order k. $\langle a^{n/k} \rangle$ if multiplicative group, $\langle \frac{n}{k} a \rangle$ if additive group.

Proof. Let G be a cyclic group and H be a subgroup of G. We need to show that H is also cyclic. Example: $H = \langle a^m \rangle$ s.t. m is the least positive integer.

By randomly pick integer $b \in H$, $b = a^k, k \in \mathbb{Z}^+$. By division algorithm, $k = qm + r$, where $0 \leq r < m$.

$$\begin{aligned} b = a^k = a^{qm+r} = (a^m)^q a^r &\Rightarrow a^r = (a^m)^{-q} b \in H \\ &\Rightarrow a^r \in H, \quad 0 \leq r < m \\ &\Rightarrow r = 0 \end{aligned}$$

$\square$