Chapter 3 Finite groups and Subgroups

Definition Let G be a group.

- The *order* of G, denoted by $|G|$ is the cardinality (finite or infinite) of G.
- The *order* of an element $g \in G$ is the smallest positive integer n such that $g^n = e$ if n exists.
- Else, the order of g, denoted by $|g|$, is infinite.
- A subset $H \subseteq G$ is a *subgroup* of G, denoted by $H \leq G$, if H is a group under the same binary operation.

Examples ...

More terminology and notation

- If $H \leq G$ and $H \neq G$, then H is a **proper subgroup** of G and we write $H < G$;
- otherwise, H is the **improper subgroup**.
- If $H = \{e\}$, then H is the **trivial subgroup**;
- otherwise, H is a **non-trivial subgroup**.

Theorem 3.1 Let G be a group and H be a **non-empty** subset of G.
Then H is a subgroup of G if and only if $ab^{-1} \in H$ whenever $a, b \in H$.

Theorem 3.2 Let G be a group and H be a **non-empty** subset of G.
Then H is a subgroup of G if and only if

(1) $ab \in H$ whenever $a, b \in H$, and (2) $a^{-1} \in H$ whenever $a \in H$.

Theorems 3.4 – 3.6 Let G be a group, and let $a \in G$. The following are subgroups of G.

(1) The cyclic subgroup generated by a is $\langle a \rangle = \{a^n : n \in \mathbb{Z}\}$.

(2) The centralizer of a is $C(a) = \{g \in G : ga = ag\}$.

(3) The center of G is $Z(G) = \{x \in G : xg = gx \text{ for all } g \in G\}$.

Remarks

- Intersection of subgroups of G is always a subgroup.
- The union of two subgroups of G is a subgroup if and only if one of the subgroups contains the other subgroup.
- The center of a group is Abelian.
- The centralizer of an element may not be Abelian.

More results on subgroups

Theorem 3.3 Let G be a group and H be a **non-empty finite** subset of G.

Then H is a subgroup of G if and only if $ab \in H$ whenever $a, b \in H$.

Chapter 4 Cyclic groups

Theorem 4.1 Let G be a group and $a \in G$.

(1) Suppose a has infinite order. Then $a^i = a^j$ if and only if $i = j$.

(2) Suppose a has finite order n. Then $a^i = a^j$ if and only if n divides $i - j$.

Corollary Let G be a group, and $a \in G$. Then $H = \langle a \rangle = \{a^k : k \in \mathbb{Z}\} \leq G$ is Abelian.

(1) $|a| = |\langle a \rangle|$.

(2) If $|a| = n$, then H is isomorphic to $\mathbb{Z}_n$.

(3) If $|a|$ is infinite, then H is isomorphic to $\mathbb{Z}$.

Remarks

- The group $H = \langle a \rangle$ is called the cyclic subgroup of G generated by a.
- If $H = G$, then G is a cyclic group generated by a.
- Every cyclic group is either isomorphic to $\mathbb{Z}_n$ or isomorphic to $\mathbb{Z}$.
- If $G = \langle a \rangle$ is isomorphic to $\mathbb{Z}$, then every subgroup has the form $\langle a^k \rangle = \langle a^{-k} \rangle$, which is isomorphic to $\mathbb{Z}$ is $k \neq 0$.

Theorem 4.2 Suppose $a \in G$ has order n, and $H = \langle a \rangle$, which is isomorphic to $\mathbb{Z}_n$.

- Every subgroup of H is generated by a^k for some $k \in \{0, 1, \ldots, n-1\}$.
- For any $k \in \{0, 1, \ldots, n-1\}$, $\langle a^k \rangle = \langle a^d \rangle$ with $d = \gcd(n, k)$ so that $|a^k| = n/d$, which is a factor of n.
- For every factor m of n, there is a unique subgroup of H of order m.

Corollary Let $a \in G$ has order n. The following conditions are equivalent.

(1) $\langle a^i \rangle = \langle a^j \rangle$.

(2) $|a^i| = |a^j|$.

(3) $\gcd(n, i) = \gcd(n, j)$.

Corollary Let $a \in G$ has order n. Then $\langle a \rangle = \langle a^j \rangle$ if and only if $\gcd(n, j) = 1$.

Definition (Euler ϕ function) Define $\phi(1) = 1$ and $\phi(n)$ equals the number of integers smaller than n are relatively prime to n for every positive integer $n > 1$.

Theorem Let $G = \langle a \rangle$ be a cyclic group of order n.

- If d is a divisor of n, the number of elements of order d in G is $\phi(d)$.
- Consequently, in a finite group, the number of elements of order d is a multiple of $\phi(d)$.