1 Subgroups

1.1 Definition and Examples

Definition. Let G be a group. The subset H of G is a *subgroup* of G if H is nonempty and H is closed under products and inverse (i.e, $x, y \in H$ implies $x \in H$ and $xy \in H$). If H is a subgroup of G we shall write $H \leq G$.

Proposition 1. (The Subgroup Criterion) A subset H of a group G is a subgroup if and only if

1. $H \neq \emptyset$, and
2. for all $x, y \in H, xy^{-1} \in H$

1.2 Centralizers and Normalizers, Stabilizers and Kernels

Let G be a group and A a nonempty subset of G.

Definition. The *centralizer* of A in G is $C_G(A) = \{g \in G \mid gag^{-1} = a \text{ for all } a \in A\}$. Note that this is the set of elements of G which commute with every element of A. Note that $C_g(A) \leq G$.

Definition. The *center* of G is the set $Z(G) = \{g \in G \mid gx = xg \text{ for all } x \in G\}$. Note that, $Z(G) = C_G(G)$, thus $Z(G) \leq G$.

Definition. Define $gAg^{-1} = \{gag^{-1} \mid a \in A\}$. The *normalizer* of A in G is the set $N_G(A) = \{g \in G \mid gAg^{-1} = A\}$. Note that, $C_G(A) \leq N_G(A) \leq G$.

1.3 Cyclic Groups and Cyclic Subgroups

Definition. A group H is *cyclic* if H can be generated by a single element, i.e, there exist some $x \in H$ such that $H = \{x^n \mid n \in \mathbb{Z}\}$ when using multiplicative notation and $H = \{nx \mid n \in \mathbb{Z}\}$ when using additive notation. In either case we write $H = \langle x \rangle$.

Proposition 2. If $H = \langle x \rangle$, then $|H| = |x|$. Moreover,

1. if $|H| = n < \infty$, then $x^n = 1$ and $1, x, x^2, \ldots, x^{n-1}$ are all distinct elements of H, and
2. if $|H| = \infty$, then $x^n \neq 1$ for all $n \neq 0$ and $x^a \neq x^b$ for all $a \neq b \in \mathbb{Z}$.

Proposition 3. Let G be an arbitrary group, $x \in G$ and let $m, n \in \mathbb{Z}$. If $x^n = 1$ and $x^m = 1$ then $x^d = 1$ where $d = (m, n)$. In particular, if $x^m = 1$ for some $m \in \mathbb{Z}$ then $|x|$ divides m.

Theorem 4. Any two cyclic groups of the same order are isomorphic. Moreover,

1. if $n \in \mathbb{Z}^+$ and $\langle x \rangle$ and $\langle y \rangle$ are both cyclic groups of order n, then the map

$$\begin{aligned} \phi \colon \langle x \rangle &\to \langle y \rangle \\ x^k &\mapsto y^k \end{aligned}$$

   is well defined and is an isomorphism

2. if $\langle x\rangle$ is an infinite cyclic group, the map

$$\begin{aligned} \phi\colon \mathbb{Z} &\to \langle x\rangle \\ k &\mapsto x^k \end{aligned}$$

is well defined and is an isomorphism

Proposition 5. Let G be a group, let $x \in G$ and let $a \in \mathbb{Z} - \{0\}$.

1. If $|x| = \infty$, then $|x^a| = \infty$.
2. If $|x| = n < \infty$, then $|x^a| = \frac{n}{(n,a)}$.
3. In particular, if $|x| = n < \infty$ and a is a positive integer dividing n, then $|x^a| = \frac{n}{a}$.

Proposition 6. Let $H = \langle x\rangle$.

1. Assume $|x| = \infty$. Then $H = \langle x^a\rangle$ if and only if $a = \pm 1$.
2. Assume $|x| = n < \infty$. Then $H = \langle x^a\rangle$ if and only if $(a, n) = 1$. In particular, the number of generators of H is $\phi(n)$ (where ϕ is Euler's ϕ-function)

Theorem 7. Let $H = \langle x\rangle$ be a cyclic group.

1. Every subgroup of H is cyclic. More precisely, if $K \leq H$, then either $K = \{1\}$ or $K = \langle x^d\rangle$, where d is the smallest positive integer such that $x^d \in K$.
2. If $|H| = \infty$, then for any distinct nonnegative integers a and b, $\langle x^a\rangle \neq \langle x^b\rangle$. Furthermore, for every integer m, $\langle x^m\rangle = \langle x^{|m|}\rangle$, where $|m|$ denotes the absolute value of m, so that the nontrival subgroups of H correspond bijectively with the integers $1, 2, 3, \ldots$.
3. If $|H| = n < \infty$, then for each positive integer a dividing n there is a unique subgroup of H of order a. This subgroup is the cyclic group $\langle x^d\rangle$, where $d = \frac{n}{a}$. Furthermore, for every integer m, $\langle x^m\rangle = \langle x^{(n,m)}\rangle$, so that the subgroups of H correspond bijectively with the positive divisors of n.

1.4 Subgroups Generated by Subsets of a Group

Proposition 8. If $\mathcal{A}$ is any nonempty collection of subgroups of G, then the intersection of all members of $\mathcal{A}$ is also a subgroup of G.

Definition. If A is any subset of the group G define

$$\langle A\rangle = \bigcap_{\substack{A\subseteq H \\ H\leq G}} H.$$

This is called the *subgroup of G generated by A*.

Note. $\langle A\rangle = \{a_1^{\epsilon_1} a_2^{\epsilon_2} \ldots a_n^{\epsilon_n} \mid n \in \mathbb{Z}, n \geq 0 \text{ and } a_i \in A, \epsilon_i = \pm 1 \text{ for each } i\}$.