Algebra I: Subgroups

Arjun Vardhan

†
Created: 4th February 2022
Last updated: 13th June 2022

1 Definition

- Let G be a group. $H \subseteq G$ is a subgroup of G if $H \neq \varnothing$ and if $x, y \in H \implies x^{-1}, xy \in H$. We denote this relation by $H \leq G$, or $H < G$ if the containment is proper.
- Subgroups are just subsets of a group that are also groups themselves with the same operations.
- **Subgroup Criterion: $H \subseteq G$ is a subgroup if and only if $H \neq \varnothing$ and for all $x, y \in H$, $xy^{-1} \in H$.** *Proof:* If $H \leq G$, then $H \neq \varnothing$ and $x, y \in H \implies xy^{-1} \in H$. Conversely, suppose that H satisfies the two conditions. Then $x \in H \implies xx^{-1} = e \in H$. And thus $e, x \in H \implies ex^{-1} = x^{-1} \in H$. Suppose $x, y \in H$. Then, $y^{-1} \in H \implies xy \in H$. ■

2 Centralizers, Normalizers, Stabilizers and Kernels

- Let $A \subseteq G$, $A \neq \varnothing$. Let $C_G(A) = \left\{g \in G : gag^{-1} = a, \forall a \in A\right\}$. $C_G(A)$ is called the centralizer of A in G. Since $gag^{-1} = a$ if and only if $ga = ag$, $C_G(A)$ is the set of all elements in G that commute with all elements in A.
- $C_G(A) \leq G$. *Proof:* Let $a \in A$. $ea = ae$ so $e \in C_G(A)$ and thus $C_G(A) \neq \varnothing$. Suppose $x, y \in C_G(A)$. Then $xax^{-1} = y^{-1}ay = a$ for all $a \in C_G(A) \implies xy^{-1}ayx^{-1} = a \implies xy^{-1} \in C_G(A)$. ■
- The center of G, denoted $Z(G)$ is the set of all elements that commute with all elements of G. So $Z(G) = C_G(G)$. $Z(G) = G$ if and only if G is abelian.
- Let $A \subseteq G$, $A \neq \varnothing$. Let $gAg^{-1} = \left\{gag^{-1} : a \in A\right\}$. The normalizer of A in G, is the set $N_G(A) = \left\{g \in G : gAg^{-1} = A\right\}$. If $g \in C_G(A)$, then $gag^{-1} = a$ for all $a \in A$, so $C_G(A) \leq N_G(A)$.
- $N_G(A) \leq G$. *Proof:* Clearly, $e \in N_G(A)$ so $N_G(A) \neq \varnothing$. Suppose $x, y \in N_G(A)$. Then $xAx^{-1} = yAy^{-1} = A$.
- If G is a group acting on a set S, and $s \in S$, then the stabilizer of s in G is the set $G_s = \{g \in G : g \cdot s = s\}$.
- $G_s \leq G$. *Proof:* Since $e \in G_s$, $G_s \neq \varnothing$. Suppose $x, y \in G_s$. Then, $s = e \cdot s = y^{-1}y \cdot s = y^{-1}(y \cdot s) = y^{-1} \cdot s$, so $y^{-1} \in G_s$. Also, $(xy) \cdot s = x(y \cdot s) = x \cdot s = s$, so $xy \in G_s$. ■
- It can similarly be shown that the kernel of a group action is also a subgroup.

3 Cyclic Groups and Subgroups

- A group H is cyclic if it can be generated by a single element, i.e, $H = \{x^n : n \in \mathbb{Z}\}$ for some $x \in H$. In this case we say H is generated by x and $H = \langle x \rangle$.
- **All cyclic groups are abelian.** *Proof:* Let $H = \langle x \rangle$. Let $a, b \in H$. Then $a = x^k$ and $b = x^m$ for some $k, m \in \mathbb{Z}$. Thus, $ab = x^k x^m = x^{k+m} = x^{m+k} = x^m x^k = ba$. ■

- **If $H = \langle x \rangle$, then $|H| = |x|$. More specifically, if $|H| = n < \infty$, then $x^n = e$ and $e, x, x^2, ..., x^{n-1}$ are all distinct and are precisely the elements of H. If $|H| = \infty$ then $x^n \neq e$ for all $n \in \mathbb{Z}$ and all elements of H are distinct.** *Proof:* Suppose $|x| = n < \infty$. Then $e, x, x^2, ..., x^{n-1}$ are distinct because if $x^a = x^b$ where $0 \leq a < b < n$, then $x^{b-a} = e$ which contradicts $|x| = n$. So H has at least n elements. Let $x^k \in H$. By the division algorithm, there exist integers q, r such that $k = qn + r$ with $0 \leq r < n$. So $x^k = x^{qn+r} = x^{qn}x^r = ex^r = x^r$. Since $r < n$, $x^k = x^r \in \left\{e, x, x^2, ..., x^{n-1}\right\}$. Thus $\langle x \rangle = \left\{e, x, x^2, ..., x^{n-1}\right\}$. Now suppose $|x| = \infty$. Then there is no integer n such that $x^n = e$. Let $a < b$ and $x^a = x^b$. Then $x^{b-a} = e$ which is a contradiction. So all powers of x are distinct, and $|H| = \infty$. ■

- **Let $x \in G$, and $m, n \in \mathbb{Z}$. If $x^m = e$ and $x^n = e$, then $x^d = e$ where $d = \gcd(m, n)$. If $x^k = e$ for some $k \in \mathbb{Z}$, then $|x|$ divides k.** *Proof:* There exist integers r, s such that $d = mr + ns$. Thus $x^d = x^{mr+ns} = e$. If $x^k = e$, let $|x| = n$. If $k = 0$, then n obviously divides k, so let $k \neq 0$. Thus $n < \infty$. Let $\gcd(k, n) = d$. Since $0 < d \leq n$, $d = n$ and thus $n \mid k$. ■

- **Any cyclic groups of the same order are isomorphic. In particular, if $G = \langle x \rangle$ and $H = \langle y \rangle$ and $|G| = |H| = n$, then the map $f : G \to H$, $f(x^k) = y^k$ is an isomorphism. If $|G| = \infty$, then the map $g : \mathbb{Z} \to G$, $g(k) = x^k$ is an isomorphism.** *Proof:*

-

4 Subgroups Generated by Subsets

5 Lattice of Subgroups