Algebra I: Subgroups

Arjun Vardhan

†

Created: 4th February 2022
Last updated: 14th 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 $C_G(A) = \{g \in G : gag^{-1} = a, \forall a \in A\}$. $C_G(A)$ 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 $gAg^{-1} = \{gag^{-1} : a \in A\}$. The normalizer of A in G, is the set $N_G(A) = \{g \in G : gAg^{-1} = A\}$. 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

- 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 $r < n$, $x^k = x^r \in \{e, x, x^2, ..., x^{n-1}\}$. Thus $\langle x \rangle = \{e, x, x^2, ..., x^{n-1}\}$. 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:* First we must show that f is well-defined. Suppose $x^r = x^s$. Then $x^{r-s} = e \implies n \mid r - s \implies r = tn + s$. So $f(x^r) = f(x^{tn+s}) = y^{tn+s} = y^s = f(x^s)$. So $x^r = x^s \implies f(x^r) = f(x^s)$. It is easy to see that f is a homomorphism by the laws of exponents. Since each y^k has the pre-image x^k in G, f is surjective. And since G and H are finite groups of the same order, f is also injective. Thus $G \cong H$. Now suppose $|G| = \infty$. f is well-defined due to the representation of elements in $\mathbb{Z}$. Since $x^a \neq x^b$ when $a \neq b$, g is injective. By the definition of a cyclic group, g is also surjective. Thus $\mathbb{Z} \cong G$. ■

- **Let $x \in G$, $a \in \mathbb{Z} \setminus \{0\}$. Then,**
  1. **If $|x| = \infty$, then $|x^a| = \infty$.** *Proof:* Suppose $|x^a| = m < \infty$. Then $x^{am} = e$ or $x^{-am} = e$. Either am or $-am$ is positive, which contradicts $|x| = \infty$. So $|x^a| = \infty$. ■
  2. **If $|x| = n < \infty$, then $|x^a| = \dfrac{n}{\gcd(n, a)}$.** *Proof:* Let $y = x^a$, $d = \gcd(n, a)$, $n = db$, $a = dc$, $b, c \in \mathbb{Z}$ with $b > 0$. So $\gcd(b, c) = 1$. Now $y^b = x^{ab} = x^{dcb} = (x^{db})^c = (x^n)^c = e$. So $|y|$ divides b. Let $k = |y|$. Then $x^{ak} = y^k = e$. So $n \mid ak$, i.e, $db \mid dck$. Thus $b \mid ck$. Since $\gcd(b, c) = 1$, $b \mid k$. Thus $b = k$. So $|y| = b \implies |x^a| = \dfrac{n}{d} = \dfrac{n}{\gcd(n, a)}$. ■
  3. **Corollary: If $|x| = n < \infty$ and $a \in \mathbb{N}$, $a \mid n$, then $|x^a| = \dfrac{n}{a}$.**

- **Let $H = \langle x \rangle$. If $|x| = \infty$ then $H = \langle x^a \rangle$ if and only if $a = \pm 1$. If $|x| = n < \infty$ then $H = \langle x^a \rangle$ if and only if $\gcd(a, n) = 1$ (H has $\phi(n)$ generators).** *Proof:* If $a = \pm 1$, then obviously $H = \langle x^a \rangle$. Conversely, let $H = \langle x^a \rangle$. If $|a| > 1$, then $x \notin H$ which is a contradiction. So $a = \pm 1$. Now let $|x| = n$. x^a generates a subgroup of order $|x^a|$, so if $\langle x^a \rangle = \langle x \rangle$, then $|x^a| = |x|$. Thus $|x^a| = n \implies \gcd(a, n) = 1$. ■

- **Let $H = \langle x \rangle$. Then,**
  1. **Every subgroup of H is cyclic. More specifically, if $K \leq H$, then either $K = \{e\}$ or $K = \langle x^d \rangle$ where d is the smallest positive integer such that $x^d \in K$.** *Proof:* Let $K \leq H$. If $K = \{e\}$, then it is of course cyclic, so let $K \neq \{e\}$. Then there exists some integer $a \neq 0$ such that $x^a \in K$. If $a < 0$, then $x^{-a} \in K$. So K always contains some positive power of x. Let $P = \{b \in \mathbb{Z}^+ : x^b \in K\}$. By the well ordering principle, P contains some least element, say d. Since $K \leq H$, any element in K is of the form x^m where $m \in \mathbb{Z}$. By the division algorithm, $m = qd + r$, $0 \leq r < d$. Then $x^r = x^{m-qd} = x^m(x^d)^{-q} \in K$ as x^m, $x^d \in K$. Since d is the minimal element of P, $r = 0$ and $m = qd$, so $x^m = (x^d)^q \in \langle x^d \rangle$. Thus $K = \langle x^d \rangle$. ■
  2. **If $|H| = \infty$, then for any distinct nonnegative integers a, b, $\langle x^a \rangle \neq \langle x^b \rangle$. Also, for all integers m, $\langle x^m \rangle = \langle x^{|m|} \rangle$.** *Proof:* Without loss of generality suppose $|a| < |b|$. If $a \mid b$ then $x^b \in \langle x^a \rangle$ and thus $\langle x^b \rangle \leq \langle x^a \rangle$. But $x^a \notin \langle x^b \rangle$ so $\langle x^a \rangle \neq \langle x^b \rangle$. If a does not divide b, then $x^b \notin \langle x^a \rangle$. If $m > 0$ then $|m| = m$ so let $m < 0$. Then $|m| = -m$. Clearly $\langle x^{-m} \rangle = \langle x^m \rangle$. ■

3. **If $|H| = n < \infty$, then for each positive integer a that divides n, there exists a unique subgroup of order a. This subgroup is $\langle x^d \rangle$, where $d = \frac{n}{a}$. Also, for every integer m, $\langle x^m \rangle = \langle x^{\gcd(m,n)} \rangle$.** *Proof:* Since $d \mid n$, $|x^d| = \frac{n}{d} = a$. Suppose $K \leq H$ and $|K| = a$. Then $K = \langle x^b \rangle$, where b is the smallest positive integer such that $x^b \in K$. Now $\frac{n}{d} = a = |K| = |x^b| = \frac{n}{\gcd(n,b)} \implies d = \gcd(n,b)$. Thus $d \mid b$ and $x^b \in \langle x^d \rangle \implies K = \langle x^b \rangle \leq \langle x^d \rangle$. But $|\langle x^d \rangle| = |K| = a$, so $K = \langle x^d \rangle$ and we are done. Now let $d = \gcd(n,m)$. Since $d \mid m$, $\langle x^m \rangle \leq \langle x^d \rangle$. As $|\langle x^m \rangle| = \frac{n}{d}$, and $|\langle x^d \rangle| = \frac{n}{\gcd(n,d)} = \frac{n}{d}$, we have $\langle x^m \rangle = \langle x^d \rangle$. ■

4 Subgroups Generated by Subsets

5 Lattice of Subgroups