

MATH 405: Assignment 6

Micah Sherry

April 29, 2025

1. if G is a commutative Group Then $H = \{\alpha \in G | \alpha = g^2 \text{ for some } g \in G\}$ is a Subgroup of G .

Proof. let G be a commutative Group and let $H = \{\alpha \in G | \alpha = g^2 \text{ for some } g \in G\}$.

Notice $e = e^2 \in H$. So, $H \neq \emptyset$.

let $x^2, y^2 \in H$

$$\begin{aligned} x^2 y^2 &= x x y y \\ &= x y x y && \text{(By commutativity of } G) \\ &= (x y)^2 \end{aligned}$$

So, $(xy)^2 \in H$ thus H is closed under the operation of the group.

let $g^2 \in H$ and let $(g^{-1})^2 \in H$ where g^{-1} is the inverse of g . Consider,

$$\begin{aligned} (g^{-1})^2 g^2 &= g^{-1} g^{-1} g g \\ &= e && \text{(By definition of inverses)} \end{aligned}$$

Therefore $(g^{-1})^2$ is the inverse of g^2 . So H contains inverses for each element of H . Thus H is a Subgroup. \square

2. let H and K be Subgroup of a commutative group G . Define $HK = \{hk | h \in H \text{ and } k \in K\}$

Proof. Notice $e \in H$ and $e \in K$ therefore $e^2 = e \in HK$. So $HK \neq \emptyset$. let $h_1, h_2 \in H$ and $k_1, k_2 \in K$. Consider,

$$\begin{aligned} (h_1 k_1)(h_2 k_2) &= (h_1 k_1)(h_2 k_2) \\ &= (h_1 h_2)(k_1 k_2) && \text{(by commutativity of } G) \end{aligned}$$

Notice $(h_1 h_2) \in H$ and $(k_1 k_2) \in K$ So, $(h_1 h_2)(k_1 k_2) \in HK$. Let $h \in H$ and $k \in K$, notice $h^{-1} k^{-1} \in HK$ Consider,

$$\begin{aligned} (h^{-1} k^{-1})(hk) &= h^{-1} k^{-1} h k \\ &= h^{-1} h k^{-1} k && \text{(by commutativity)} \\ &= e && \text{(by definition of inverses)} \end{aligned}$$

Therefore $h^{-1} k^{-1}$ is the inverse of hk . Thus HK is a Subgroup of G . \square

3. Find the order of each element in U_{20}

element of U_{20}	order
1	1
3	4
7	4
9	2
11	2
13	4
17	4
19	2

4. Let G be a group and $g \in G$ be an element with finite ord prove each of the following statements:

- (a) $\text{ord}(g^{-1})$ is finite. proof of this follows from proof of part b
- (b) $\text{ord}(g^{-1}) = \text{ord}(g)$

Proof. let $g \in G$ with $\text{ord}(g) = n \in \mathbb{N}$

$$\begin{aligned} g^n &= e \\ (g^n)^{-1} &= e^{-1} \\ (g^{-1})^n &= e \end{aligned} \quad \text{(by properties of exponents and since e is self inverse)}$$

Assume for the sake of contradiction that there exist $r \in \mathbb{N}$ such that $0 < r < n$ such that $(g^{-1})^r = e$. So,

$$\begin{aligned} (g^{-1})^r &= e \\ ((g^{-1})^r)^{-1} &= e^{-1} \\ g^r &= e \end{aligned} \quad \text{(by properties of exponents and since e is self inverse)}$$

since $0 < r < n$ this implies that $\text{ord}(g) = r$ which contradicts the assumption therefore $\text{ord}(g^{-1}) = n$ \square

5. let a and b be elements of a commutative Group G . If the $\text{ord}(a)$ and $\text{ord}(b)$ are finite then $\text{ord}(ab)$ is finite.

Proof. let $a, b \in G$ with $\text{ord}(a) = m$ and $\text{ord}(b) = n$ Notice $a^m = (a^m)^n = a^{mn} = e^n = e$ and $b^n = (a^m)^n = b^{nm} = e^m = e$. Now Consider,

$$\begin{aligned} e &= a^{nm} b^{nm} \\ &= (ab)^{nm} \end{aligned} \quad \text{(since G is commutative)}$$

Therefore the $0 < \text{ord}(ab) < mn$, which is finite. \square