MATH 405: Assignment 6

Micah Sherry

April 30, 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, $H \neq \varnothing$.
   let $x^2, y^2 \in H$. Consider,

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

   Since,$xy \in G$, $(xy)^2 \in H$ thus H is closed under the operation of the group.
   Let $g^2 \in H$. Notice $(g^{-1})^2 \in H$ because $g^{-1} \in G$. Consider,

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

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

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

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

   $$\begin{aligned} (h_1k_1)(h_2k_2) &= h_1k_1h_2k_2 \\ &= (h_1h_2)(k_1k_2) && \text{(by commutativity of G)} \end{aligned}$$

   Notice $(h_1h_2) \in H$ and (k_1k_2) So, $(h_1h_2)(k_1k_2) \in HK$.
   Let $h \in H$ and $k \in K$, notice $h^{-1}k^{-1} \in HK$ Consider,

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

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

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 order prove each of the following statements:

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

   (b) $ord(g^{-1}) = ord(g)$

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

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

   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,

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

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

5. let a and b be elements of a commutative Group g. If the $ord(a)$ and $ord(b)$ are finite then ord(ab) is finite.

Proof. let $a, b \in G$ with $ord(a) = m$ and $ord(b) = n$. Notice

$$a^m = (a^m)^n = a^{mn} = e^n = e$$

And Similarly

$$b^n = (b^n)^m = b^{nm} = e^m = e$$

Now Consider,

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

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