Math 403 Chapter 3: Finite Groups and Subgroups

---

1. **Finite versus Infinite Groups and Elements:** Groups may be broadly categorized in a number of ways. One is simply how large the group is.

   (a) **Definition:** The order of a group G, denoted $|G|$, is the number of elements in a group. This is either a finite number or is infinite. We will not distinguish beetween various infinite cardinalities.

   - **Example:** If $G = \mathbb{Z}$ then $|G| = \infty$.
   - **Example:** If $G = (\mathbb{Z}_7, + \bmod 7)$ then $|G| = 7$.
   - **Example:** If $G = U(8) = (\{1,3,5,7\}, \cdot \bmod 8)$ then $|G| = 4$.

   (b) **Definition:** Given a group G and an element $g \in G$, we define *the order of* g, denoted $|g|$, to be the smallest positive integer n such that $g^n = e$. If there is no such n then we say $|g| = \infty$. Notice that if the operation is addition then g^n means $g + ... + g = ng$.

   - **Example:** If $G = \mathbb{R} - \{0\}$ then $|1| = 1$, $|-1| = 2$, and otherwise $|g| = \infty$.
   - **Example:** If $G = \mathbb{Z}_{10}$ then check out all the elements.
   - **Example:** If $G = U(8)$ then check out all the elements.

2. **Subgroups:** When we're trying to understand the structure of a particular group it can be helpful to note that sometimes a group will have other groups as subsets of them. For example the group $2\mathbb{Z}$ sits inside the group $\mathbb{Z}$.

   (a) **Definition:** If G is a group and if $H \subseteq G$ is a group itself using G's operation then G *is a subgroup of* G. We write $H \leq G$.

   - **Example:** $2\mathbb{Z}$ is a subgroup of $\mathbb{Z}$.
   - **Example:** $\{-1, 1\}$ is a subgroup of $\mathbb{R} - \{0\}$.
   - **Example:** $\mathbb{Z}_5$ is not a subgroup of $\mathbb{Z}$. It is a subset but the operations are different.

   (b) **Theorem (One-Step Subgroup Test):** Let G be a group and let $H \subseteq G$ with $H \neq \emptyset$. If $\forall a, b \in H$ we have $ab^{-1} \in H$ then $H \leq G$.
   Proof: We need to verify closure and the additional three requirements but we need to do these in a particular order. We have associativity because the operation of H is the same as G. Since $H \neq \emptyset$ pick any $a \in H$. Then $aa^{-1} = e \in H$ so H has the identity. Pick any $a \in H$ then $ea^{-1} \in H$ so we have inverses. Pick any $a, b \in H$ Then $b^{-1} \in H$ and so $ab = a\left(b^{-1}\right)^{-1} \in H$ and we have closure. $\mathcal{QED}$
   Example: If G is an Abelian group then $H = \{x \mid x^2 = e\} \leq G$.
   Proof: $\mathcal{QED}$

   (c) **Theorem (Two-Step Subgroup Test):** Let G be a group and let $H \subseteq G$ with $H \neq \emptyset$. If $\forall a, b \in H$ we have $ab \in H$ and $a^{-1} \in H$ then $H \leq G$.
   Proof: Given $a, b \in H$ since $b^{-1} \in H$ we have $ab^{-1} \in H$ and so the One-Step Subgroup Test is satisfied. $\mathcal{QED}$
   Example: If G is an Abelian group then $H = \{x \mid |x| < \infty\} \leq G$.
   Proof: $\mathcal{QED}$

   (d) **Theorem (Finite Subgroup Test):** Let G be a group and let $H \subseteq G$ with $|H| < \infty$. If $\forall a, b \in H$ we have $ab \in H$ then $H \leq G$.
   Proof: We need to show that $a^{-1} \in H$ for all $a \in H$ and then the Two-Step Subgroup

Test is satisfied. Given $a \in H$ if $a = e$ then $a^{-1} = e$ and we're done. If $a \neq e$ consider $S = \{a, a^1, a^2, ...\} \subseteq H$ by closure. Since H is finite two of these must be identical, say $a^j = a^k$ for $1 \leq j < k$. Then by canceling a^j we get $e = a^{k-j} = aa^{k-j-1}$ and so a^{k-j-1} is the inverse of a and is in S hence in H. $\mathcal{QED}$

3. **Special Subgroups:** There are certain subgroups of groups which will be particularly useful to us.

   (a) **Definition/Theorem:** For $g \in G$ define the set:

   $$\langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}$$

   Then $\langle g \rangle \leq G$, this is called *the subgroup generated by g*.
   Note: When we write something like g^{-2} we mean the inverse of g^2. $\mathcal{QED}$
   Proof: Omit. Easy. Try it! $\mathcal{QED}$
   Example: $\langle 3 \rangle \subseteq \mathbb{R} - \{0\}$.
   Note: If the operation is addition then this is the set of multiples of g as well as multiples of the inverse of g.
   Example: $\langle 3 \rangle \subseteq \mathbb{Z}$.

   (b) **Definition/Theorem:** For a group G define *the center of* G:

   $$Z(G) = \{g \in G \mid \forall x \in G, gx = xg\}$$

   Then $Z(G) \leq G$.
   Note: $Z(G)$ is the set of things in G which commute with everything in G.
   Note: The Z stands for "Zentrum", a German word for "Center".
   Proof: We'll use the two-step subgroup test. Assume $a, b \in Z(G)$ so that for all $x \in G$ we have $ax = xa$ and $bx = xb$. Let $x \in G$. First note that since $xa = ax$ we have $a^{-1}xaa^{-1} = a^{-1}axa^{-1}$ and so $a^{-1}x = xa^{-1}$ and so $a^{-1} \in Z(G)$. Second note $abx = axb = xab$ so $ab \in Z(G)$. $\mathcal{QED}$

   (c) **Definition/Theorem:** For a group G and a specific $g \in G$ define *the centralizer of g in* G:

   $$C(g) = \{x \in G \mid xg = gx\}$$

   Then $C(g) \leq G$.
   Note: $C(g)$ is the set of things in G which commute with g specifically.
   Proof: We'll use the two-step subgroup test. Assume $a, b \in C(g)$ so that $ag = ga$ and $bg = gb$. The rest is the same as the previous proof except we're only using g specifically and not an arbitrary $x \in G$. $\mathcal{QED}$

It's worth taking a second to consider the difference between the center and a centralizer. The center consists of all the elements which commute with everything. For a centralizer we take a specific element and find all the elements which commute with that specific element. It's fairly clear that $Z(G) \subseteq C(g)$ (can you prove it?) and counterexamples can be found with $C(g) \not\subseteq Z(G)$.