Math 403 Chapter 9: Normal Subgroups and Factor Groups

1. **Introduction:** A factor group is a way of creating a group from another group. This new group often retains some of the properties of the original group.

2. **Normal Subgroups:**

   (a) **Definition:** A subgroup $H \leq G$ is *normal* if $gH = Hg$ for all $g \in G$. In this case we write $H \triangleleft G$.

   There are a couple of ways to think about normal subgroups:

   - Formally a subgroup is normal if every left coset containing g is equal to its right coset containing g.
   - Informally a subgroup is normal if its elements "almost" commute with elements in g. This means that for any $g \in G$ we don't necessarily get $gh = hg$ but at worst we get $gh = h'g$ for perhaps some other h'.

   Example: In an Abelian group every subgroup H is normal because for all $h \in H$ and $g \in G$ we have $gh = hg$.

   Example: The center of a group is a normal subgroup because for all $z \in Z(G)$ and $g \in G$ we have $gz = zg$.

   Example: Consider the subgroup $H = \{(), (123), (132)\}$ of S_3. Observe that we have the following left cosets:

$$\begin{aligned}
()H &= \{(), (123), (132)\} \\
(12)H &= \{(12), (23), (13)\} \\
(13)H &= \{(13), (12), (23)\} \\
(23)H &= \{(23), (13), (12)\} \\
(123)H &= \{(123), (132), ()\} \\
(132)H &= \{(132), (), (123)\}
\end{aligned}$$

   And we have the following right cosets:

$$\begin{aligned}
H() &= \{(), (123), (132)\} \\
H(12) &= \{(12), (13), (23)\} \\
H(13) &= \{(13), (23), (12)\} \\
H(23) &= \{(23), (12), (13)\} \\
H(123) &= \{(123), (132), ()\} \\
H(132) &= \{(132), (), (123)\}
\end{aligned}$$

   We see that we have $()H = H()$, $(12)H = H(12)$, $(13)H = H(13)$, $(23)H = H(23)$, $(123)H = H(123)$, $(132)H = H(132)$.

   Example: Consider the subgroup $H = \{(), (12)\}$ of S_3. Observe that $(23)H = \{(23), (132)\}$ but $H(23) = \{(23), (123)\}$. Since we have a left coset not equal to a right coset the subgroup is not normal.

(b) **Theorem (Normal Subgroup Test):** A subgroup H of G is normal iff $gHg^{-1} \subseteq H$ for all $g \in G$.
Proof:
$\Rightarrow$: Suppose $H \triangleleft G$. We claim $gHg^{-1} \subseteq H$ for any $g \in G$. Let $g \in G$ and then an element in gHg^{-1} looks like ghg^{-1} for some $h \in H$. Then observe that $ghg^{-1} = h'gg^{-1} = h' \in H$.
$\Leftarrow$: Suppose $gHg^{-1} \subseteq H$ for all $g \in G$. We claim $gH = Hg$. Note that $gH = gHg^{-1}g \subseteq Hg$ and that $Hg = gg^{-1}Hg \subseteq gH$. In the latter we have $g^{-1}Hg \subseteq H$ becaues the supposition is true for g^{-1}.

Example: The subgroup $SL_2\mathbb{R}$ of 2×2 matrices with determinant 1 forms a normal subgroup of $GL_2\mathbb{R}$. To see this note that if $g \in GL_2\mathbb{R}$ and $s \in SL_2\mathbb{R}$ then $\det(gsg^{-1}) = \det(g)\det(s)(1/\det(g)) = \det(s) = 1$ and so $gsg^{-1} \in SL_2\mathbb{R}$.

3. **Factor Groups:**

Definition/Theorem: Let G be a group and let $H \triangleleft G$. Then we define G/H (read "G mod H") to be the set of left cosets of H in G and this set forms a group under the operation $(aH)(bH) = abH$.
Proof: We have a few things to show here:

- Any given left coset will have multiple representatives because we know that aH and $a'H$ can be identical for $a \neq a'$. Consequently we first need to be sure that our operation is well-defined, meaning that if we choose $a'H = aH$ and $b'H = bH$ and we do $(a'H)(b'H) = a'b'H$ we get the same result as if we do $(aH)(bH) = abH$. In other word we must verify that $abH = a'b'H$. Since $a'H = aH$ and since $a' \in a'H$ we have $a' = ah_1$ and likewise $b' = bh_2$ for some $h_1, h_2 \in H$. It follows that $a'b'H = ah_1bh_2H = abh_1'h_2H = abH$.
- The identity is eH.
- The inverse of aH is $a^{-1}H$.
- Associativity follows since $(aH)(bHcH) = (aH)(bcH) = abcH = (abH)(cH) = (aHbH)cH$.

Example: If $G = \mathbb{Z}$ and $h = 4\mathbb{Z}$ then there are four distinct cosets:

$$\begin{aligned}
0 + 4\mathbb{Z} &= \{..., -8, -4, 0, 4, 8, ...\} \\
1 + 4\mathbb{Z} &= \{..., -7, -3, 1, 5, 9, ...\} \\
2 + 4\mathbb{Z} &= \{..., -6, -2, 2, 6, 10, ...\} \\
3 + 4\mathbb{Z} &= \{..., -5, -1, 3, 7, 11, ...\}
\end{aligned}$$

These four cosets form a group with set:

$$\{0 + 4\mathbb{Z}, 1 + 4\mathbb{Z}, 2 + 4\mathbb{Z}, 3 + 4\mathbb{Z}\}$$

The operation is:

$$(a + 4\mathbb{Z}) + (b + 4\mathbb{Z}) = (a + b) + 4\mathbb{Z}$$

So for example:

$$(3 + 4\mathbb{Z}) + (2 + 4\mathbb{Z}) = 5 + 4\mathbb{Z} = 1 + 4\mathbb{Z}$$

We immediately notice that $\mathbb{Z}/4\mathbb{Z} \approx \mathbb{Z}_4$.

Example: If $G = U(32) = \{1, 3, 5, 7, 9, ..., 31\}$ and $H = \{1, 15\}$. then there are eight distinct cosets:

$$
\begin{aligned}
1H &= \{1, 15\} \\
3H &= \{3, 13\} \\
5H &= \{5, 11\} \\
7H &= \{7, 9\} \\
17H &= \{17, 31\} \\
19H &= \{19, 29\} \\
21H &= \{21, 27\} \\
23H &= \{23, 25\}
\end{aligned}
$$

These eight cosets for a group with set:

$$\{1H, 3H, 5H, 7H, 17H, 19H, 21H, 23H\}$$

The operation is $aHbH = abH$. So for example:

$$
\begin{aligned}
5H7H &= 35H = \{35, 525\} = \{3, 13\} = 3H \\
3H19H &= 59H = \{59, 885\} = \{27, 21\} = 21H
\end{aligned}
$$

Note: The terminology "G mod H" arises from the analogy with modular arithmetic. When we work in $\mathbb{Z}$ mod 5, for example, we say that $8 = 3$ mod 5 because $8 = 3{+}5 = 3$ mod 5 because the 5 "gets absorbed" into the modulus. That is, 8 mod $5 = (3 + 5)$ mod $5 = 3 + (5$ mod $5) = 3$ mod 5. Similarly if we're looking at gH and if $g = g'h$ then $gH = g'hH = g'H$ because the h gets absorbed by the H.

4. **Applications:**

   (a) **Theorem:** If $G/Z(G)$ is cyclic then G is Abelian.
   Proof: Since $G/Z(G)$ is cyclic we know there is some $g_0 \in G$ such that $G/Z(G) = \langle g_0 Z(G)\rangle$. Thus every coset has the form $g_0^k Z(G)$ for some k. Given $a, b \in G$ we know that each is in some coset so $a \in g_0^j Z(G)$ and $b \in g_0^k Z(G)$ for some j, k and moreover then $a = g_0^j z_1$ and $b = g_0^k z_2$ for $z_1, z_2 \in Z(G)$. Then observe that:

   $$ab = g_0^j z_1 g_0^k z_2 = g_0^j g_0^k z_1 z_2 = g_0^k g_0^j z_2 z_1 = g_0^k z_2 g_0^j z_1 = ba$$

   $\mathcal{QED}$

   Example: Suppose G is non-Abelian and $|G| = pq$ where p, q are distinct primes then G has trivial center consisting only of $\{e\}$. This is because a bigger center would have to have order p, q or pq by Lagrange's Theorem. The first two fail by this theorem and the third fails because G is non-Abelian.
   Note: This has meaningful results. For example suppose we know that $|G| = pq$ where p, q are prime and suppose we find just one $g_0 \in G$ with $g_0 \in Z(G)$ and $g_0 \neq e$. Since $Z(G) \leq G$ we know that by Lagrange's Theorem we must have $|Z(G)| = 1, p, q$ or pq. Since $|Z(G)| \neq 1$ we know it's p, q or pq. If $|Z(G)| = pq$ then G is Abelian. Without loss of generality if $|Z(G)| = p$ then $|G/Z(G)| = pq/p = q$ and snce groups of prime order are cyclic we have $G/Z(G)$ cyclic and then G Abelian. So this goes to show that in such a group if we find one single non-identity element in the center then the group is Abelian and everything is in the center.