Chapter 9

<u>Defn</u>: Let G be a group and let $H \leq G$ be a subgroup.
We say H is <u>normal</u> in G if
$$aH = Ha \text{ for all } a \in G.$$
When H is a normal subgroup we write $H \trianglelefteq G$

<u>Note</u>: When H is normal its left cosets are the same as its right cosets, so we refer to them as simply <u>cosets of H</u>.

<u>Note</u>: Recall from Lem. 7.C that $aH = Ha \Leftrightarrow aHa^{-1} = H$.
So H is normal if and only if $aHa^{-1} = H$ for all $a \in G$

<u>Thm 9.1 (Normal Subgroup Test)</u>:
Let H be a subgroup of a group G.
Then H is normal if and only if $aHa^{-1} \subseteq H$ for all $a \in G$.

<u>Pf</u>: ($\Rightarrow$) Follows from Lem 7.C (see Note above)
($\Leftarrow$) Assume $xHx^{-1} \subseteq H$ for all $x \in G$.
By Lem 7.C (or Note above) it suffices to show that $aHa^{-1} = H$ for all $a \in G$.
① Using $x = a$ we obtain $aHa^{-1} \subseteq H$
② Using $x = a^{-1}$ we obtain $a^{-1}Ha \subseteq H$.
Multiplying both sides of ↑ on the left by a and on the right by a^{-1} we obtain $aa^{-1}Haa^{-1} \subseteq aHa^{-1}$, meaning $H \subseteq aHa^{-1}$
① and ② show $aHa^{-1} = H$. $\square$

Examples of normal subgroups

- Every subgroup of an abelian group (for examples all subgroups of $\mathbb{R}, \mathbb{Z}, \mathbb{Z}_n, U(n)$)

- the center $Z(G)$ is always normal in G (for every $x \in G$ $xZ(G)x^{-1} \subseteq Z(G)$, because for each $g \in Z(G)$ we have $xgx^{-1} = xx^{-1}g = g \in Z(G)$)

- A_n is normal in S_n for every n. (If $\beta \in A_n$ is an even permutation then $\alpha\beta\alpha^{-1}$ is an even permutation for every $\alpha \in S_n$, meaning $\alpha\beta\alpha^{-1} \in A_n$)

- Any subgroup of D_n containing only rotations is normal in D_n (Since rotations commute with one another, and we previously showed that if R is a rotation and F is a reflection then $FRF^{-1} = R^{-1}$)

Notation: When $H \triangleleft G$ we write G/H for the set $\{aH : a \in G\}$ of all cosets of H in G.

Thm 9.2: Let G be a group and $H \triangleleft G$ a normal subgroup. Then G/H is a group under the operation

$$aH \cdot bH = \underbrace{ab}_{\text{operation in } G}H$$

Lem 9.A Let H be a normal subgroup of G.
If $a_1 H = a_2 H$ and $b_1 H = b_2 H$ then

$$a_1 b_1 H = a_2 b_2 H$$

Pf: By Lem 7.A $a_1 b_1 H = a_2 b_2 H \iff a_1 b_1 \in a_2 b_2 H$.

Since $a_1 \in a_1 H = a_2 H$, there is $h_a \in H$ with
$$a_1 = a_2 h_a$$
Since $b_1 \in b_1 H = b_2 H$, there is $h_b \in H$ with
$$b_1 = b_2 h_b$$

Since H is normal, $b_2^{-1} H b_2 = H$. In particular
$$b_2^{-1} h_a b_2 \in H.$$
Set $h_* = b_2^{-1} h_a b_2$
Then $b_2 h_* = h_a b_2$

Finally $h_* h_b \in H$ since H is a subgroup.
Set $h = h_* h_b$.

Then we have

$$\begin{aligned} a_1 b_1 &= (a_2 h_a)(b_2 h_b) \\ &= a_2 (h_a b_2) h_b \\ &= a_2 (b_2 h_*) h_b = a_2 b_2 (h_* h_b) \\ &= a_2 b_2 h \in a_2 b_2 H. \quad \square \end{aligned}$$

Pf of Thm 9.1:

In order for the "operation" $aH \cdot bH = abH$ to make sense we need to know that $a_1b_1H = a_2b_2H$ when $a_1H = a_2H$ and $b_1H = b_2H$. Lemma 9.A tells us this.

Now we check this operation makes G/H a group.

(Associative)

$$(aH\,bH)cH = abH\,cH = (ab)cH$$
$$= a(bc)H = aH(bcH) = aH(bH\,cH)$$

G is associative

(Identity) H is the identity: ($=eH$)

for all $aH \in G/H$

$$aH \cdot H = aH \text{ and } H \cdot aH = aH$$

(Inverses) The inverse of aH is $a^{-1}H$ since

$$aH\,a^{-1}H = eH = H \text{ and } a^{-1}H\,aH = eH = H \quad \square$$

Ex: In $\mathbb{Z}$, consider the (normal) subgroup

$$5\mathbb{Z} = \{0, \pm5, \pm10, \pm15, \dots\} = \{n \in \mathbb{Z} : n \bmod 5 = 0\}$$

The cosets of $5\mathbb{Z}$ are

$5\mathbb{Z} = \{n \in \mathbb{Z} : n \bmod 5 = 0\}$
$1+5\mathbb{Z} = \{n \in \mathbb{Z} : n \bmod 5 = 1\}$
$2+5\mathbb{Z} = \{n \in \mathbb{Z} : n \bmod 5 = 2\}$
$3+5\mathbb{Z} = \{n \in \mathbb{Z} : n \bmod 5 = 3\}$
$4+5\mathbb{Z} = \{n \in \mathbb{Z} : n \bmod 5 = 4\}$

The Cayley table for $\mathbb{Z}/5\mathbb{Z}$ is

$\mathbb{Z}/5\mathbb{Z}$	$5\mathbb{Z}$	$1+5\mathbb{Z}$	$2+5\mathbb{Z}$	$3+5\mathbb{Z}$	$4+5\mathbb{Z}$
$5\mathbb{Z}$	$5\mathbb{Z}$	$1+5\mathbb{Z}$	$2+5\mathbb{Z}$	$3+5\mathbb{Z}$	$4+5\mathbb{Z}$
$1+5\mathbb{Z}$	$1+5\mathbb{Z}$	$2+5\mathbb{Z}$	$3+5\mathbb{Z}$	$4+5\mathbb{Z}$	$5\mathbb{Z}$
$2+5\mathbb{Z}$	$2+5\mathbb{Z}$	$3+5\mathbb{Z}$	$4+5\mathbb{Z}$	$5\mathbb{Z}$	$1+5\mathbb{Z}$
$3+5\mathbb{Z}$	$3+5\mathbb{Z}$	$4+5\mathbb{Z}$	$5\mathbb{Z}$	$1+5\mathbb{Z}$	$2+5\mathbb{Z}$
$4+5\mathbb{Z}$	$4+5\mathbb{Z}$	$5\mathbb{Z}$	$1+5\mathbb{Z}$	$2+5\mathbb{Z}$	$3+5\mathbb{Z}$

We can see from the above table that $\mathbb{Z}/5\mathbb{Z} \approx \mathbb{Z}_5$. Specifically, the map $\phi: \mathbb{Z}_5 \to \mathbb{Z}/5\mathbb{Z}$ given by $\phi(r) = r + 5\mathbb{Z}$ is an isomorphism.

Defn: When $H \trianglelefteq G$, G/H is called the factor group (or quotient group) of G by H.

Obs: If H is a normal subgroup of G with index $|G:H| = 2$, then G/H is isomorphic to $\mathbb{Z}_2$

Pf: G/H is a group of order $|G/H| = |G:H| = 2$. Since 2 is prime, Cor. 7.C tells us $G/H \approx \mathbb{Z}_2$. $\square$

Ex: • A_n is a normal subgroup of S_n (exercise)
and $|S_n : A_n| = |S_n| / |A_n| = n! / \frac{1}{2}(n!) = 2$
so S_n / A_n is isomorphic to $\mathbb{Z}_2$

• $K = \{R_0, R_{90}, R_{180}, R_{270}\}$ is normal in D_4 (exercise)
and $|D_4 : K| = |D_4| / |K| = 8/4 = 2$
so D_4 / K is isomorphic to $\mathbb{Z}_2$

Thm 9.5 (Cauchy's Theorem for Abelian Groups):
Let G be a finite abelian group and let p be a prime dividing $|G|$. Then G has an element of order p.

Pf: We'll use (strong) induction on $n = |G|$.

Base Case: $n = 2$. Done in this case because $|G| = 2 \underset{\text{Cor 7.C}}{\Longrightarrow} G \approx \mathbb{Z}_2$ and $\mathbb{Z}_2$ has an element of order 2.

Inductive Step: Assume conclusion of theorem is true for all groups of order strictly smaller than n.

Pick any $y \in G$, $y \neq e$. ~~[illegible]~~
Set m = (order of y). If $p | m$ then $y^{m/p}$ has order p and we are done.
Otherwise, pick any prime divisor $q \neq p$ of m.

Set $z = y^{m/q}$, and $H = \langle z \rangle$. Then H is a subgroup of G of order q. Because G is abelian, H is a normal subgroup. Then G/H has order $|G|/q$ which is strictly smaller than n and $p \mid |G/H|$, so by our inductive hypothesis there is some $xH \in G/H$ having order p. This means that

$$H = (xH)^p = x^p H$$

the identity in G/H

and therefore $x^p \in H = \langle z \rangle = \{e, z, z^2, \dots, z^{q-1}\}$

Case 1: $x^p = e$. Then x has order p and we are done

Case 2: $x^p = z^i$ for some $1 \le i \le q-1$. Since q (the order of z) is prime, we have that z^i has order q. Therefore $x^p = z^i$ has order q and x has order pq. Consequently x^q has order p. $\square$