Normal Subgroups and Quotients

Notation.

$\mathbf{S} \subset \mathbf{G}$. S is a **subset** if every element in S is also in G.

$\mathbf{H} < \mathbf{G}$. H is a **subgroup** if it is a subset and also it is a group.

$\mathbf{N} \lhd \mathbf{G}$. N is a **normal subgroup** if it is a subgroup and also its cosets are a group!

G/N. The **group of cosets** for a normal subgroup is called the **quotient group**.

Normal Subgroups.

Definition. A **normal subgroup** H of G (written $H \lhd G$) is a subgroup where $\boldsymbol{gH = Hg}$ for all $g \in G$. When the group G is clear from context, we will just say "H is normal."

Remark. This is *almost* a statement about commutativity. The requirement $gH = Hg$ means that for each $h \in H$ there is $h' \in H$ so that $\boldsymbol{gh = h'g}$ (and vice versa). This is *slightly weaker* than being commutative.

There are a number of equivalent formulations for this requirement.

Proposition. *The following are all equivalent to* $\boldsymbol{H \lhd G}$.

(i) For all $g \in G$, $\boldsymbol{gH = Hg}$.

(ii) For all $g \in G$ *and* $h \in H$, $\boldsymbol{hg \in gH}$ *(i.e.* $Hg \subset gH$ *for all* g*).*

(iii) For all $g \in G$, $\boldsymbol{gHg^{-1} = H}$.

(iv) For all $g \in G$ *and* $h \in H$, $\boldsymbol{ghg^{-1} \in H}$ *(i.e.* $gHg^{-1} \subset H$ *for all* g*).*

*(v) Every **left coset** is also a **right coset** (for each* $g \in G$ *there is* $g' \in G$ *so that* $gH = Hg'$*).*

Proof. For all of these, the ($\Rightarrow$) direction is trivial.
(i) is a restatement of the definition.
(iv) was in the homework last week.
(ii) is equivalent to *(iv)* since $hg = gh' \iff h = gh'g^{-1}$.
(iii) ($\Leftarrow$) is implied by *(iv)*
(v) ($\Leftarrow$) is proven as follows.
If $gH = Hg'$ then $g \in gH = Hg'$. So there is $h \in H$ with $g = hg'$. Then $g'g^{-1} = h^{-1} \in H$. This is our key!

Given $h \in H$ use $gH = Hg'$ to get $h' \in H$ with $gh = h'g'$. Multiplying on right by g^{-1}, we have $ghg^{-1} = h'g'g^{-1} = h(g'g^{-1}) \in H$, connecting to *(iv)*. □

Let's look at some examples! Below are some examples and propositions comparing normality with commutativity in various settings.

Example. All subgroups are normal if G is abelian (because $hg = gh$ is stronger than normality).

Example. The center of a group is always normal (because center commutes with everything).

Proposition. *The commutator subgroup* $[G, G] < G$ *defined by* $[G, G] = \{aba^{-1}b^{-1} \mid a, b \in G\}$ *is normal.*

Proof. Recall that $g[a, b]g^{-1} = [gag^{-1}, gbg^{-1}] \in [G, G]$. □

Commutator subgroups are used to build the **lower central series** for **nilpotent groups** (connecting to Lie algebras, topology, and knot theory). They are also used to build the **derived series** for **solvable groups** (connecting to solving degree n equations in algebra). These series measure "how close" a group is to being abelian. Abelian groups are the best! Lots of love for those guys! ❤

Example. The **quaternions** $\mathbb{H}$ are numbers of the form $a + b\boldsymbol{i} + c\boldsymbol{j} + d\boldsymbol{k}$ with the rules $\boldsymbol{i}^2 = \boldsymbol{j}^2 = \boldsymbol{k}^2 = -1$ and $\boldsymbol{k} = \boldsymbol{i}\boldsymbol{j} = -\boldsymbol{j}\boldsymbol{i}$ and $\boldsymbol{j} = \boldsymbol{k}\boldsymbol{i} = -\boldsymbol{i}\boldsymbol{k}$ and $\boldsymbol{i} = \boldsymbol{j}\boldsymbol{k} = -\boldsymbol{k}\boldsymbol{j}$. These are complex numbers with an "extra imaginary direction" $\mathbb{C} + \mathbb{C}\boldsymbol{j}$. Quaternion multiplication is not commutative, but the subgroups generated by $\boldsymbol{i}$, $\boldsymbol{j}$, and $\boldsymbol{k}$ are all normal, since e.g. $\langle \boldsymbol{i} \rangle = \{1, \boldsymbol{i}, -1, -\boldsymbol{i}\}$ and the $\boldsymbol{i}, \boldsymbol{j}, \boldsymbol{k}$ all *anti-commute*. (These play an important role in describing 3D rotations.)

Note. Continuing this ["Cayley–Dickson"] pattern would generate the **octonians** $\mathbb{O}$. But their multiplication isn't associative, so they don't form a group. (Luckily we don't care about 7D rotations...)

At the other end of the spectrum, consider S_n. In the previous homework set, you proved the following.

Proposition. *If $H < G$ with index $[G : H] = 2$, then H is a normal subgroup.*

Corollary. *The alternating group of even permutations A_n is normal in the symmetric group S_n.*

Most other things aren't normal in S_n, though.... S_n is **very** non-commutative!

Example. In S_3 the subgroup generated by transposition $\big\langle (1\ 2) \big\rangle = \big\{(1),\ (1\ 2)\big\}$ is **not** normal because conjugating with $(1\ 3)$ moves outside the subgroup. $(1\ 3)\,(1\ 2)\,(1\ 3) = (3\ 2) \notin \big\langle (1\ 2) \big\rangle$.

Index arguments, like the one above, are about counting elements. Lets look more at normality vs order!

Begin with the following statement which is useful for analyzing normal subgroups. We proved this during our subgroup week, but I'll repeat the proof again.

Proposition. *If $H < G$ then $gHg^{-1} < G$ as well (i.e. conjugation preserves subgroup).*

Proof. Verify nonempty, closed under product, closed under inverse.

(Nonempty.) If H is a group then $e \in H$, so $e = geg^{-1} \in gHg^{-1}$.
(Product.) $(gh_1g^{-1})\,(gh_2g^{-1}) = g(h_1h_2)g^{-1} \in gHg^{-1}$.
(Inverse.) $(ghg^{-1})^{-1} = (g^{-1})^{-1}h^{-1}g^{-1} = gh^{-1}g^{-1} \in gHg^{-1}$. $\square$

Corollary. *If $H < G$ is the **only** subgroup with order $\big|H\big|$, then it is normal.*

Proof. Note that $\big|gHg^{-1}\big| = \big|H\big|$ because $gh_1g^{-1} = gh_2g^{-1} \iff h_1 = h_2$. If H is the only subgroup with order $|H|$, then $gHg^{-1} = H$. $\square$

Corollary. *The intersection of **all** subgroups of a given order (if nonempty) is a normal subgroup.*

Proof. Let $K = \bigcap\limits_{|H|=k} H$ and suppose $x \in K$ and $g \in G$. For H any given subgroup of order k, $x \in H$. Since $g^{-1}Hg$ is also a subgroup with the same order, $x \in g^{-1}Hg$ as well. So there is $h \in H$ with $x = g^{-1}hg$. Thus $gxg^{-1} = h \in H$. Therefore gxg^{-1} must be in every subgroup of order k. So $gxg^{-1} \in K$. $\square$

There is a very interesting construction related to this.

Definition. The **core** of a subgroup $H < G$ is $\operatorname{core}_G(H) = \bigcap\limits_{g \in G} gHg^{-1}$.

Proposition. *If $H < G$ then the core of H is the largest normal subgroup of G contained in H.*

(i) $\operatorname{core}_G(H) \lhd G$ *and* $\operatorname{core}_G(H) < H$.

(ii) If $K \lhd G$ with $K < H$ then $K < \operatorname{core}_G(H)$.

Quotient Groups.

The job of normal subgroups is to have nice cosets!

Recall that we previously defined cosets as equivalence classes of an equivalence relation.

Definition. If $H < G$, define the **quotient set** $G/H = G/\sim$ where $a \sim b$ if $a = hb$ for some $h \in H$.

Notation. Elements of G/H are cosets. We use bracket notation for the coset generated by $g \in G$.

We say g is a **representative** of the coset $[g] = gH \in G/H$. *Some people* write $\bar{g}$ instead of $[g]$.

Theorem. *If $H \lhd G$ then G/H is a **group**.*

Proof. Once we know that multiplication is well-defined we will have $[e] = eH = H$ and $[g]^{-1} = [g^{-1}] = g^{-1}H$.

Suppose $a \sim a'$ and $b \sim b'$. Then there are $h_a, h_b \in H$ so that $a = h_a a'$ and $b = h_b b'$. Substituting $ab = (h_a a')(h_b b') = h_a(a' h_b)b'$. Since H is normal there exists $h_b' \in H$ so that $a' h_b = h_b' a'$. Therefore $ab = h_a(a' h_b)b' = (h_a h_b')(a' b')$. So $ab \sim a'b'$. □

Normality is the **minimum** requirement to get a group structure on cosets.

Proposition. *A subgroup is normal if and only if cosets have a product structure.*

I.e. $H \lhd G$ if and only if $(aH)(bH) = (ab)H$ for all $a, b \in G$.

Proof. The theorem gives the $(\Rightarrow)$ direction.

For $(\Leftarrow)$ note that setting $a = e$ implies $(eH)(bH) = (eb)H = bH$. But $(eH)(bH) = HbH = (Hb)H$. Thus $(Hb)H = bH$, which implies $Hb \subset bH$. This is formulation *(ii)* for normality. □

Example. Recall that $n\mathbb{Z} \lhd \mathbb{Z}$ has the following cosets.

$$\begin{array}{rcrcl}
[\mathbf{0}] &=& \mathbf{0} + n\mathbb{Z} &=& \{\ldots, \mathbf{0}, n, \ldots\} &= [n] \\
[\mathbf{1}] &=& \mathbf{1} + n\mathbb{Z} &=& \{\ldots, \mathbf{1}, n+1, \ldots\} &= [n+1] \\
\vdots & & \vdots & & & \vdots \\
[\boldsymbol{n-1}] &=& (\boldsymbol{n-1}) + n\mathbb{Z} &=& \{\ldots, \boldsymbol{n-1}, 2n-1, \ldots\} &= [2n-1]
\end{array}$$

The group operation on $\mathbb{Z}/n\mathbb{Z}$ is $[a] + [b] = [a+b] = [a + b \pmod{n}]$. So $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$!

Example. Recall that if $[G : H] = 2$ then $H \lhd G$. In this case, $G/H = \mathbb{Z}_2$ (the cyclic group of order 2).

More generally, we often think about G/H as "$G/(H \sim e)$" as if we formally *squished* H down to the identity element, deforming G slightly in the process. A similar operation appears in **many** different areas of mathematics!

Quotient operations allow us to separate the group structure of G into "stuff due to H" and "other stuff." Ideally we can combine our understanding of H and G/H in order to understand G itself.

Most of all, we like when G/H is abelian. Because we understand abelian stuff.

Example. The quotient by the commutator $G/[G, G]$ is abelian because $gh = (hg)\big(g^{-1}h^{-1}gh\big) \in (hg)\,[G, G]$.

In fact, the commutator is the **smallest** subgroup so that G/H is abelian!

♥ ♥ ♥ Lots of love for commutators! ♥ ♥ ♥

Let's look at how multiple subgroups play together! We previously proved the following.

Proposition. *If $H, K < G$ (nothing normal) then the following are true.*

(i) $H < HK \subset G$

(ii) $(H \cap K) < K$

When something is normal, everything gets upgraded!

Proposition. *If $H, K < G$ and $H \lhd G$ (one normal) then the following are true.*

(i) $H \lhd HK < G$

(ii) $(H \cap K) \lhd K$

(iii) $HK/H \;\cong\; K/(H \cap K)$ *("2nd Isomorphism Theorem.")*

$$\begin{array}{ccc} H & \lhd & HK \\ \vee & & \vee \\ H\cap K & \lhd & K \end{array} \qquad \begin{array}{c} HK/H \\ \wr\| \\ K/(H\cap K) \end{array}$$

When everything is normal, then everything is normal!

Proposition. *If $H, K \lhd G$ (both normal) then the following are true.*

(i) $H \lhd HK \lhd G$

(ii) $(H \cap K) \lhd \boldsymbol{G}$

You have to try really hard to lose normality. [Don't try really hard.]

We can similarly consider strings of subgroups $K < H < G$.

Proposition. *If $K < H < G$ with $K \lhd G$ (bottom is normal) then the following are true.*

(i) $K \lhd H$

(ii) $H/K < G/K$

(iii) $\{\text{subgroups } H \mid K < H < G\} \;\cong\; \{\text{subgroups of } G/K\}$ *("Correspondence Theorem")*

When everything is normal, then beauty abounds! ❤

Proposition. *If $K \lhd H \lhd G$ with $K \lhd G$ (everything is normal) then the following are true.*

(i) $H/K \lhd G/K$

(ii) $\dfrac{G/K}{H/K} \;\cong\; G/H$ *("3rd Isomorphism Theorem." – generalizes $[G:K] = [G:H]\,[H:K]$)*

We will prove the isomorphism theorems after introducing group homomorphisms.

Warning. Normality is **not** a **transitive** relationship! $K \lhd H \lhd G$ does **not** imply $K \lhd G$!

Example. Consider $\langle (1\ 2)\,(3\ 4)\rangle \lhd K_4 \lhd S_4$. The Klein 4-group sits inside $A_4 < S_4$ as the disjoint cycle products:

$$K_4 \cong \{(1),\ (1\ 2)\,(3\ 4),\ (1\ 3)\,(2\ 4),\ (1\ 4)\,(2\ 3)\}$$

(We know this is K_4 because there are only two order 4 groups, and the other one is cyclic.) Since K_4 is abelian, everything is normal in K_4. To show K_4 is normal in S_4, it is enough to show conjugation preserves disjointness of cycles.

But $\langle (1\ 2)\,(3\ 4)\rangle$ is **not normal** in S_4 because we can directly show that

$$(2\ 3)\ (1\ 2)\,(3\ 4)\ (2\ 3) \;=\; (1\ 3)\,(2\ 4) \;\notin\; \langle (1\ 2)\,(3\ 4)\rangle$$

We can think of normal subgroups like factors of numbers. Corresponding to prime numbers are the groups which contain no normal subgroups.

Definition. A group is **simple** if it contains no nontrivial proper normal subgroups.

In 2004 the classification of all finite simple groups was completed. This is popularly called the "enormous theorem," with a proof requiring multiple books. It was one of the first instances of computer aided proof verification **(very controversial!)**. One of the larger finite simple groups (the largest *sporadic simple group*), called the "monster group," has order $\approx 10^{53}$ and was proven to exist in 1983; though it was predicted to exist in 1973 when the "baby monster"[1] (order $\approx 10^{33}$) was found.

[1] Not to be confused with the 2020's South Korean girl band "Babymonster" aka *Baemon*.