Normal Subgroups and Quotient Groups

R. C. Daileda

To motivate what it means for a subgroup H of a group G to be *normal*, we continue to use the analogy between congruences modulo n in $\mathbb{Z}$ and congruence modulo H in G. We have seen that the congruence classes mod n in $\mathbb{Z}$ are precisely the members of the set

$$\mathbb{Z}/n\mathbb{Z} = \{0 + n\mathbb{Z}, 1 + n\mathbb{Z}, 2 + n\mathbb{Z}, \dots (n-1) + n\mathbb{Z}\},$$

which are in one-to-one correspondence with the members of the set

$$\mathbb{Z}_n = \{0, 1, 2, \dots, n-1\},$$

which are just the possible remainders after division by n. More precisely, the function

$$\begin{aligned} f : \mathbb{Z}_n &\to \mathbb{Z}/n\mathbb{Z}, \\ r &\mapsto r + n\mathbb{Z}, \end{aligned}$$

is (obviously) a bijection. Since $\mathbb{Z}_n$ is known to be a group, Exercise 1 of Assignment 5.3 tells us that we can use f to transfer its group structure to $\mathbb{Z}/n\mathbb{Z}$. Chasing through the details of that exercise, we find that the binary operation on $\mathbb{Z}/n\mathbb{Z}$ becomes

$$(a + n\mathbb{Z}) + (b + n\mathbb{Z}) = (a \oplus b) + n\mathbb{Z} = R_n(a + b) + n\mathbb{Z}, \tag{1}$$

where $R_n(k)$ is the remainder when an integer k is divided by n. Since $a+b = qn+R_n(a+b)$ for some $q \in \mathbb{Z}$, we find (again) that $(a+b)-R_n(a+b)$ is divisible by n. So $a+b \equiv R_n(a+b) \pmod{n}$, which means that

$$R_n(a + b) + n\mathbb{Z} = (a + b) + n\mathbb{Z}, \tag{2}$$

since the cosets of $n\mathbb{Z}$ are just the equivalences classes under congruence mod n. Taken together, equations (1) and (2) tell us that the rule

$$(a + n\mathbb{Z}) + (b + n\mathbb{Z}) := (a + b) + n\mathbb{Z} \tag{3}$$

yields a well-defined binary operation on $\mathbb{Z}/n\mathbb{Z}$ under which $\mathbb{Z}/n\mathbb{Z}$ is a group (isomorphic to $\mathbb{Z}_n$ via f). Once again, we can attempt to generalize this situation by replacing $\mathbb{Z}$ by an arbitrary group G, $n\mathbb{Z}$ by a subgroup $H < G$, and then rewriting (3) in multiplicative notation:

$$(aH)(bH) := (ab)H. \tag{4}$$

It must be understood that we are taking this to be the *definition* of multiplication of cosets in G/H, based solely on our attempt to draw an analogy with the rule (3) that we derived for $\mathbb{Z}/n\mathbb{Z}$. The concatenation $(aH)(bH)$ has *no meaning* until we give it one. Our goal now is to determine whether or not the definition of coset multiplication given in (4) turns the coset space G/H into a group, in the same way that (3) turns $\mathbb{Z}/n\mathbb{Z}$ into a group.

As we will see, the only real question is whether or not (4) is a *well-defined* binary operation. More specifically, if $aH = a'H$ and $bH = b'H$ for some $a, a', b, b' \in G$, we will have $(aH)(bH) = (a'H)(b'H)$ if and only if $(ab)H = (a'b')H$. To see what this requires of H, consider the case in which $a \in H$, $a' = e$, and $b' = b \in G$. The equation $(ab)H = (a'b')H$ becomes

$$(ab)H = (eb)H \;\Leftrightarrow\; (ab)H = bH \;\Leftrightarrow\; (b^{-1}ab)H = H \;\Leftrightarrow\; b^{-1}ab \in H.$$

Because $a \in H$ and $b \in G$ were arbitrary this is equivalent to

$$b^{-1}Hb \subseteq H \quad \text{for all} \quad b \in G. \tag{N2}$$

Although it only arose as a special case, we will soon see that condition (N2) is both necessary *and* sufficient for (4) to be well-defined. But first we provide several convenient reformulations of (N2).

Lemma 1. *Let G be a group and let $H < G$. The following conditions on H are equivalent.*

(N1) $aHa^{-1} \subseteq H$ *for all* $a \in G$.

(N2) $b^{-1}Hb \subseteq H$ *for all* $b \in G$.

(N3) $xHx^{-1} = H$ *for all* $x \in G$.

(N4) $xH = Hx$ *for all* $x \in G$.

Proof. (**N1** $\Rightarrow$ **N2**) Suppose that $aHa^{-1} \subseteq H$ for all $a \in G$. Let $b \in G$ and take $a = b^{-1}$. Then

$$b^{-1}Hb = aHa^{-1} \subseteq H.$$

Since $b \in H$ was arbitrary, this proves N2.

(**N2** $\Rightarrow$ **N3**) Suppose that $b^{-1}Hb \subseteq H$ for all $b \in G$. Let $x \in G$ and set $b = x^{-1}$. Then

$$xHx^{-1} = b^{-1}Hb \subseteq H.$$

But if we take $b = x$ we also have

$$x^{-1}Hx \subseteq H \;\Rightarrow\; H \subseteq xHx^{-1}.$$

We therefore have $xHx^{-1} = H$, by double containment. As $x \in G$ was arbitrary, this proves N3.

(**N3** $\Rightarrow$ **N4**) Clear.

(**N4** $\Rightarrow$ **N1**) Suppose $xH = Hx$ for all $x \in G$. Let $a \in G$ and set $x = a$. Then

$$aH = Ha \;\Rightarrow\; aHa^{-1} = H,$$

which certainly implies $aHa^{-1} \subseteq H$. Once again, since $a \in G$ was arbitrary, we have proven N1. □

Definition. Let G be a group and $H < G$. We say that H is *normal* in G, denoted $H \triangleleft G$, provided it satisfies any of the equivalent conditions N1–N4.

Remarks. Condition N3 is frequently taken as "the" definition of normality. In situations in which the normality of a subgroup needs to be confirmed directly (as opposed to simply invoking a theorem), conditions N1 and N2 are the easiest to check, since they are logically the weakest.

In light of Lemma 1, our work above shows that in order for the binary operation (4) to be well-defined, the subgroup H must be normal in G. We will now prove the converse.

Theorem 1. *Let G be a group and let $H < G$. The rule*

$$(aH)(bH) := (ab)H$$

is a well-defined binary operation on G/H if and only if $H \triangleleft G$.

Proof. Suppose $H \triangleleft G$. Let $a, a', b, b' \in G$ so that $aH = a'H$ and $bH = b'H$. Then

$$(a')^{-1}a \in H \quad \text{and} \quad (b')^{-1}b \in H.$$

Since $H \triangleleft G$, using condition N2 we find that

$$(a'b')^{-1}ab = ((b')^{-1}b)b^{-1}((a')^{-1}a)b \in ((b')^{-1}b)(b^{-1}Hb) \subseteq ((b')^{-1}b)H = H.$$

But $(a'b')^{-1}ab \in H$ if and only if $(ab)H = (a'b')H$. This proves that for all $a, a', b, b' \in G$,

$$aH = a'H \text{ and } bH = b'H \;\Rightarrow\; (ab)H = (a'b')H.$$

This shows that the binary operation in question is indeed well-defined when $H \triangleleft G$. Having already established the converse, this completes the proof of Theorem 1. □

It is now a simple matter to show that G/H is always a group when $H \triangleleft G$.

Corollary 1. *Let G be a group and let $H \triangleleft G$. Then G/H is a group under $(aH)(bH) = (ab)H$. The identity in G/H is the coset $eH = H$ of the identity element $e \in G$, and the inverse of $aH \in G/H$ is $(aH)^{-1} = a^{-1}H$.*

Proof. Now that we know the binary operation on G/H is well-defined, we only need to check that the group axioms are satisfied in G/H. Let $aH, bH, cH \in G/H$. Then

$$((aH)(bH))(cH) = ((ab)H)(cH) = ((ab)c)H = (a(bc))H = (aH)((bc)H) = (aH)((bH)(cH)),$$

which proves associativity. We also have

$$(aH)(H) = (aH)(eH) = (ae)H = aH = (ea)H = (eH)(aH) = (H)(aH),$$

which shows that $H = eH$ is the identity coset. Finally,

$$(aH)(a^{-1}H) = (aa^{-1})H = eH = (a^{-1}a)H = (a^{-1}H)(aH),$$

so that $a^{-1}H$ is the inverse of the coset aH. □

Example 1. If G is a group, its *center* $Z(G) = \{g \in G \,|\, gx = xg \quad \text{for all } x \in G\}$ is always normal, since for any $g \in Z(G)$ and any $x \in G$ we have

$$gx = xg \;\;\Rightarrow\;\; gxg^{-1} = x \in Z(G).$$

Although there's no general rule for what the group $G/Z(G)$ "looks like," there's one special situation that can be useful from time to time. Specifically:

Lemma 2. *If G is a group and $G/Z(G)$ is cyclic, then G is abelian.*

Proof. Choose g so that $G/Z(G)$ is generated by the coset $g\,Z(G)$. Then the elements of $G/Z(G)$ all have the form $(g\,Z(G))^k = g^k\,Z(G)$ for $k \in \mathbb{Z}$. Because every element in G belongs to one of these cosets, any $x \in G$ has the form $x = g^k z$ for some $k \in \mathbb{Z}$ and $z \in Z(G)$. If y is also in G, then we also have $y = g^\ell w$ for some $\ell \in \mathbb{Z}$ and $w \in Z(G)$. Then, because z and w commute with all of G, we find that

$$xy = (g^k z)(g^\ell w) = g^k g^\ell zw = g^{k+\ell} wz = g^{\ell+k} wz = g^\ell g^k wz = (g^\ell w)(g^k z) = yx.$$

Therefore G is abelian, as claimed. □

Example 2. Let $Q = \{\pm 1, \pm i, \pm j, \pm k\}$ denote the *quaternion group*, which was introduced in Exercise 1.2.2 (using matrix notation). The elements ± 1 are central (commute with every other element of Q), and the binary operation in Q is completely determined by the relations

$$i^2 = j^2 = k^2 = ijk = -1.$$

These imply that the elements $\pm i, \pm j$ and $\pm k$ have order 4. We can also see that Q is nonabelian since

$$i^2 = ijk \;\;\Rightarrow\;\; i = jk \;\;\Rightarrow\;\; ji = j^2 k = -k,$$
$$k^2 = ijk \;\;\Rightarrow\;\; k = ij,$$

from which it follows that $ij = k = -ji$. Likewise one can show that $ik = -ki$ and $jk = -kj$. One says that i, j and k *anticommute*.

The computations above imply that $Z(Q) = \{\pm 1\}$, and Example 1 tells us that $Z(Q) \triangleleft Q$. Then, according to Lagrange's theorem, $Q/Z(Q)$ is a group of order

$$|Q/Z(Q)| = [Q : Z(Q)] = \frac{|Q|}{|Z(Q)|} = \frac{8}{2} = 4.$$

The elements of $Q/Z(Q)$ are the cosets $Z(Q)$, $iZ(Q)$, $jZ(Q)$ and $kZ(Q)$. If ϵ is any one of i, j or k, then

$$(\epsilon Z(Q))^2 = (\epsilon Z(Q))\,(\epsilon Z(Q)) = \epsilon^2 Z(Q) = (-1)Z(Q) = Z(Q),$$

since $-1 \in Z(Q)$. This shows that every nonidentity member of the quotient $Q/Z(Q)$ has order 2. In particular, $Q/Z(Q)$ is *not* cyclic. This also follows from Lemma 2, since we know that Q is nonabelian. However, $Q/Z(Q)$ *is* abelian, by homework exercise (???). As we will see later, up to isomorphism the only abelian groups of order 4 are $\mathbb{Z}_4$ and $\mathbb{Z}_2 \oplus \mathbb{Z}_2$. We conclude that $Q/Z(Q) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$.