

QUOTIENT GROUPS

KEITH CONRAD

1. INTRODUCTION

By thinking carefully about how we build the group $\mathbf{Z}/(m)$ from the group \mathbf{Z} and its subgroup $m\mathbf{Z}$ we will be led to an analogous “modular arithmetic” in an arbitrary group. The catch is that the subgroups we are allowed to mod out by in a general group are not arbitrary as in the case of \mathbf{Z} (where every subgroup is some $m\mathbf{Z}$), but are a special type of subgroup called a normal subgroup, which we’ll describe in Section 2. A group modulo a normal subgroup is called a quotient group and we’ll look at some examples and properties of quotient groups in Section 3.

2. NORMAL SUBGROUPS

The elements of $\mathbf{Z}/(m)$ are congruence classes, and a congruence class mod m is a 2-sided arithmetic progression

$$a + m\mathbf{Z} = \{\dots, a - 2m, a - m, a, a + m, a + 2m, \dots\}.$$

We add two elements in $\mathbf{Z}/(m)$ by adding representatives of the congruence classes:

$$(2.1) \quad \bar{a} + \bar{b} := \overline{a + b},$$

where \bar{a} is shorthand for $a + m\mathbf{Z}$. The point about (2.1) is that it is well-defined, *i.e.*, it’s independent of the choice of representatives used from the two congruence classes: if $\bar{a} = \bar{a}'$ and $\bar{b} = \bar{b}'$ then $\bar{a} + \bar{b} = \bar{a}' + \bar{b}'$. That is, if $a \equiv a' \pmod{m}$ and $b \equiv b' \pmod{m}$ then $a + b \equiv a' + b' \pmod{m}$.

Since $a + m\mathbf{Z}$ is the same thing as a coset of $m\mathbf{Z}$ in \mathbf{Z} , we want to carry over the idea of addition of integers modulo m to a multiplication of left cosets (or of right cosets) of a subgroup of a group: if G is a group and H is a subgroup, could we define the product of two left cosets of H to be another left coset of H by the rule

$$(2.2) \quad g_1H \cdot g_2H \stackrel{?}{=} g_1g_2H.$$

Unfortunately this sometimes makes no sense, since it can depend on the *choice* of representatives for the left cosets.

Example 2.1. Take $G = D_3$ and $H = \langle s \rangle = \{1, s\}$. Then

$$rH = \{r, rs\} = rsH \quad \text{and} \quad r^2H = \{r^2, r^2s\} = r^2sH$$

However

$$r \cdot r^2H = H$$

while

$$rs \cdot r^2sH = rr^{-2}ssH = r^{-1}H \neq H.$$

So even though r and rs are in the same left H -coset, and r^2 and r^2s are in the same left H -coset, $r \cdot r^2$ and $rs \cdot r^2s$ are not in the same left H -coset, so the left H -cosets they are in don’t match.

A similar problem happens for a definition like (2.2) with right cosets: $Hr = Hr^2s$ and $Hr^2 = Hrs$, but $Hr \cdot r^2 = H$ while $Hr^2s \cdot rs = Hr \neq H$.

It turns out that for (2.2) to make sense as an operation on left cosets of H we need H to be a special type of subgroup: one for which left and right cosets by each element are the same thing.

Definition 2.2. A subgroup N of a group G is called *normal* if $gN = Ng$ for every $g \in G$. Equivalently, N is normal if $gNg^{-1} = N$ for every $g \in G$.¹

The condition $gN = Ng$ is **not** saying $gn = ng$ for all $n \in N$, but rather than for each $n \in N$ we can write $gn = n'g$ for some $n' \in N$, and $ng = n''g$ for some $n'' \in N$: the sets gN and Ng agree, but not necessarily by having gn equal ng all the time.

Remark 2.3. Unlike cyclic subgroups or abelian subgroups, which are subgroups that happen to be cyclic or abelian groups on their own, a normal subgroup is not a subgroup that's a "normal group," since there is no such thing as a "normal group." Whether or not a subgroup N of a group G is a normal subgroup (that is, whether or not $gN = Ng$ for every $g \in G$) is not an internal property of N , but depends on how N interacts with the larger group G it lies inside.

Example 2.4. In every group G both G and its trivial subgroup $\{e\}$ are normal subgroups of G .

Example 2.5. If G is an abelian group then every subgroup of G is a normal subgroup, since the order of multiplication doesn't matter: $gN = Ng$ because $gn = ng$ for all $g \in G$ and $n \in N$.

Example 2.6. The center Z of a group G is a normal subgroup since each element of Z commutes with each element of G : $gz = zg$ for all $g \in G$ and $z \in Z$, so $gZ = Zg$. By similar reasoning, each *subgroup of the center* of G is a normal subgroup of G . (This last part subsumes the previous example, since if G is abelian its center is G , so subgroups of the center are all subgroups of G .)

Remark 2.7. The reasoning in the previous example depends on how the center Z interacts with the whole group G . In particular, it is generally *false* that abelian subgroups are normal subgroups. For example, $\langle s \rangle = \{1, s\}$ is an abelian (and in fact cyclic) subgroup of D_n for $n \geq 3$ but it is *not* normal in D_n since $r\{1, s\} = \{r, rs\}$, $\{1, s\}r = \{r, sr\}$, and $rs \neq sr$: $sr = r^{-1}s = r^{n-1}s \neq rs$ since r has order n and $n > 2$. Thus $r\{1, s\} \neq \{1, s\}r$.

Example 2.8. In D_n the subgroup $H = \langle r \rangle = \{1, r, r^2, \dots, r^{n-1}\}$ is normal. To check $gH = Hg$ for each $g \in D_n$, this is immediate if $g \in H$ since then $gH = H$ and $Hg = H$. If $g \notin H$ then g is not a rotation so it is a reflection, say $g = r^i s$. Then

$$gH = r^i sH = sr^{-i}H = sH$$

because $r^{-i} \in H$, and

$$Hg = Hr^i s = Hs$$

because $r^i \in H$, so we are reduced to checking $sH = Hs$:

$$sH = \{s, sr, sr^2, \dots, sr^{n-1}\} = \{s, r^{-1}s, r^{-2}s, \dots, r^{-(n-1)}s\}$$

and

$$Hs = \{s, rs, r^2s, \dots, r^{n-1}s\},$$

and the lists of elements in sH and Hs are the same (just in a different order) since $r^{-i} = r^{n-i}$.

Example 2.8 is a special case of the following theorem.

¹In the late 19th and early 20th centuries, normal subgroups had many other names, such as "invariant subgroups" and "self-conjugate subgroups". See <https://math.stackexchange.com/questions/898977> for further synonyms, which are all obsolete. The term "normal" is famous in mathematics for the wide number of unrelated meanings it has in different areas, as shown at <https://en.wikipedia.org/wiki/Normal>, but it's not as bad as regular: <https://en.wikipedia.org/wiki/Regular>.

Theorem 2.9. *Every subgroup of index 2 in a group is a normal subgroup.*

Proof. Let H have index 2 in the group G . For each $g \in G$ we want to show $gH = Hg$. If $g \in H$ then this is immediate since $gH = H$ and $Hg = H$. If $g \notin H$ then $gH \neq H$, so from H having index 2 in G the coset gH is the other coset of H besides H , i.e., $gH = G - H$. For the same reason, using right cosets, we have $Hg \neq H$ so $Hg = G - H$. Thus $gH = G - H = Hg$. \square

Example 2.10. Since $[S_n : A_n] = 2$, A_n is a normal subgroup of S_n .

The standard notation to indicate a subgroup H of a group G is normal is: $H \triangleleft G$ (not $H \Delta G$). For example, $m\mathbf{Z} \triangleleft \mathbf{Z}$ (\mathbf{Z} is abelian), $\langle r \rangle \triangleleft D_n$ (index-2 subgroup), and $A_n \triangleleft S_n$ (index-2 subgroup).

Let's show that multiplying cosets of a normal subgroup by the rule (2.2) is well-defined: it is independent of the choice of representative.

Theorem 2.11. *Let $N \triangleleft G$. If $g_1N = g'_1N$ and $g_2N = g'_2N$ for some $g_1, g'_1, g_2, g'_2 \in G$ then $g_1g_2N = g'_1g'_2N$.*

Proof. Since $g_1N = g'_1N$ and $g_2N = g'_2N$, we can write $g_1 = g'_1n_1$ and $g_2 = g'_2n_2$ for $n_1, n_2 \in N$. Then

$$g_1g_2 = g'_1n_1g'_2n_2 = g'_1(n_1g'_2)n_2.$$

Since N is a normal subgroup, $n_1g'_2 = g'_2n'_1$ for some $n'_1 \in N$. Then

$$g_1g_2 = g'_1(g'_2n'_1)n_2 = g'_1g'_2(n'_1n_2),$$

and $n'_1n_2 \in N$, so $g_1g_2N = g'_1g'_2N$. \square

We will build on this result in the next section to show the operation $g_1N \cdot g_2N = g_1g_2N$ makes the cosets of N in G into a (new) group.

To verify that a subgroup H of a group G is a normal subgroup, often it is useful to think about the condition $gH = Hg$ as $gHg^{-1} = H$, and it turns out that to check $gHg^{-1} = H$ for all $g \in G$, just checking the containment of the left side in the right side (for all g) is sufficient.

Theorem 2.12. *A subgroup H of a group G is normal if and only if $gHg^{-1} \subset H$ for all $g \in G$. That is, $gHg^{-1} = H$ for all $g \in G$ if and only if $gHg^{-1} \subset H$ for all $g \in G$.*

Proof. The direction (\Rightarrow) is immediate: if $gHg^{-1} = H$ for all $g \in G$ then obviously $gHg^{-1} \subset H$ for all $g \in G$. For the more interesting direction (\Leftarrow), suppose $gHg^{-1} \subset H$ for all $g \in G$. Replacing g with g^{-1} (which we can do since the containment is assumed to hold for all g in G) we get $g^{-1}Hg \subset H$ for all g too. Multiplying both sides of $gHg^{-1} \subset H$ on the right by g gives us $gH \subset Hg$, and multiplying both sides of $g^{-1}Hg \subset H$ on the left by g gives us $Hg \subset gH$. From $gH \subset Hg$ and $Hg \subset gH$ we get $gH = Hg$. \square

Example 2.13. We will show $SL_2(\mathbf{R}) \triangleleft GL_2(\mathbf{R})$. By Theorem 2.12 it is sufficient to show $ASL_2(\mathbf{R})A^{-1} \subset SL_2(\mathbf{R})$ for each $A \in GL_2(\mathbf{R})$. For $B \in SL_2(\mathbf{R})$, is $ABA^{-1} \in SL_2(\mathbf{R})$? Well,

$$\det(ABA^{-1}) = \det(A) \det(B) \det(A^{-1}) = \det(A) \det(B) \frac{1}{\det A} = \det B = 1,$$

so $ABA^{-1} \in SL_2(\mathbf{R})$.

Example 2.14. In D_n , $\langle r \rangle$ is a normal subgroup since it has index 2 (Theorem 2.9), while $\langle s \rangle = \{1, s\}$ is not a normal subgroup of D_n since $r\langle s \rangle r^{-1} \not\subset \langle s \rangle$:

$$rsr^{-1} = rrs = r^2s \notin \langle s \rangle.$$

To prove a subgroup H of a group G is *not* normal, it suffices to show $gHg^{-1} \not\subset H$ for some $g \in G$, which means $ghg^{-1} \notin H$ for some $g \in G$ and some $h \in H$.²

Example 2.15. The subgroup $\text{Aff}(\mathbf{R})$ of $\text{GL}_2(\mathbf{R})$ is *not* normal, since $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in \text{GL}_2(\mathbf{R})$ and

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 0 \\ b & a \end{pmatrix},$$

which is not in $\text{Aff}(\mathbf{R})$ if $b \neq 0$ (and a is nonzero, say $a = 1$).

With Theorem 2.12 we can show a converse to Theorem 2.11 holds: if the rule (2.2) is well-defined then H *must* be a normal subgroup of G . Indeed, for $g \in G$ and $h \in H$, $hH = H = eH$ and $gH = gH$, so having (2.2) be well-defined at least requires $hgH = egH$, so $hg \in gH$. Thus $g^{-1}hg \in H$ for all $h \in H$ and $g \in G$. Since this is supposed to hold for all g , we can replace g with g^{-1} to get $ghg^{-1} \in H$ for all $h \in H$, so $gHg^{-1} \subset H$ for all $g \in G$. Thus $H \triangleleft G$ by Theorem 2.12.

Remark 2.16. It is crucial in Theorem 2.12 that the quantification runs over *all* $g \in G$, since for *some* H and $g \in G$ it can happen that $gHg^{-1} \subset H$ without having $gHg^{-1} = H$.³ For example, let $G = \text{GL}_2(\mathbf{R})$ (or $G = \text{GL}_2(\mathbf{Q})$) and $H = \{\begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} : m \in \mathbf{Z}\}$. Then H is a subgroup of G , and if $g = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$ then

$$\begin{aligned} g \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} g^{-1} &= \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}^{-1} \\ &= \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1/2 & 0 \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 2 & 2m \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1/2 & 0 \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2m \\ 0 & 1 \end{pmatrix} \in H \end{aligned}$$

for all $m \in \mathbf{Z}$, so $gHg^{-1} \subset H$, while

$$\begin{aligned} g^{-1} \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} g &= \begin{pmatrix} 1/2 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1/2 & m/2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix}, \end{aligned}$$

which is not in H if $m = 1$, so $g^{-1}Hg \not\subset H$. Therefore $gHg^{-1} \neq H$: the subgroup H of G is not a normal subgroup.

More generally, if $g = \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}$ for an integer $a \geq 2$ then

$$g \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} g^{-1} = \begin{pmatrix} 1 & am \\ 0 & 1 \end{pmatrix} \in H$$

for all $m \in \mathbf{Z}$ while

$$g^{-1} \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} g = \begin{pmatrix} 1 & m/a \\ 0 & 1 \end{pmatrix}$$

²The property of a subgroup being normal is called its normality, not its normalcy, even though “normalcy” comes from math: <https://www.merriam-webster.com/words-at-play/did-warren-harding-coin-normalcy>.

³This is impossible if H is finite, since then $|gHg^{-1}| = |H|$, so a containment $gHg^{-1} \subset H$ forces equality.

is not in H if $m = 1$, so gHg^{-1} is a proper subset of H .

3. QUOTIENT GROUPS

By Theorem 2.11, we can meaningfully multiply cosets of a normal subgroup N of a group G by multiplying representatives for two cosets and passing to the coset of N the product lies in.

Definition 3.1. If $N \triangleleft G$, define the product of two cosets g_1N and g_2N to be $g_1N \cdot g_2N := g_1g_2N$.

Nothing would change if we use right cosets of N because for a normal subgroup $gN = Ng$, so the above definition is exactly the same thing as defining $Ng_1 \cdot Ng_2 = Ng_1g_2$.

Theorem 3.2. *Using the above operation, the set of cosets of N in G is a group.*

Proof. It is easy to see N is an identity for this operation on cosets of N :

$$N \cdot gN = 1N \cdot gN = 1gN = gN, \quad gN \cdot N = gN = 1N = g1N = gN.$$

The inverse of gN is $g^{-1}N$ since their product in either order is the identity coset N :

$$gN \cdot g^{-1}N = gg^{-1}N = 1N = N, \quad g^{-1}N \cdot gN = g^{-1}gN = 1N = N.$$

Associativity of this multiplication on cosets follows from associativity of multiplication in G :

$$(gN \cdot hN) \cdot kN = ghN \cdot kN = (gh)kN, \quad gN \cdot (hN \cdot kN) = gN \cdot hkN = g(hk)N,$$

so from $(gh)k = g(hk)$ we get $(gh)kN = g(hk)N$. □

The collection of all cosets of a normal subgroup N of a group G is denoted G/N (and this is pronounced “ $G \bmod N$ ”). Its construction generalizes that of $\mathbf{Z}/(m)$: if $G = \mathbf{Z}$ and $N = m\mathbf{Z}$ then $\mathbf{Z}/m\mathbf{Z}$ under addition is exactly the same thing as congruence classes mod m under addition.

The group G/N is called the *quotient group* of G modulo N . Another term for G/N , which was more widely used many years ago, is *factor group* (and that is still the standard term in some other languages, e.g., Faktorgruppe in German.)⁴ While the collection of (left) cosets $G/H = \{gH : g \in G\}$ for an arbitrary subgroup H in G is always a *set*, only when H is a normal subgroup does G/H form a group using the rule (2.2), because if (2.2) is well-defined then H must be a normal subgroup of G .⁵ The name “quotient group” is explained at <https://math.stackexchange.com/questions/857539/who-named-quotient-groups> and the following short theorem shows that the size of G/N is related to quotients of integers when G is finite.

Theorem 3.3. *If $N \triangleleft G$ with finite index then $|G/N| = [G : N]$. In particular, $|G/N| = |G|/|N|$ if G is finite.*

Proof. The size of G/N is the number of cosets of N in G (left or right), which is $[G : N]$. If G is finite and $[G : N] = t$, then $t|N| = |G|$, so $|G/N| = t = |G|/|N|$. □

The notion of congruent integers in modular arithmetic carries over to all groups: in \mathbf{Z} we say $a \equiv b \pmod m$ when $a - b \in m\mathbf{Z}$, or equivalently when $a = b + mk$ for some $k \in \mathbf{Z}$, so if $N \triangleleft G$ we write $g_1 \equiv g_2 \pmod N$ when $g_1g_2^{-1} \in N$, which is equivalent to $g_1 = ng_2 = g_2n'$ for some $n, n' \in N$, which is equivalent to $g_1N = g_2N$ (we have $g_1g_2^{-1} \in N \Leftrightarrow g_1 \in Ng_2 = g_2N \Leftrightarrow g_1N = g_2N$ since two cosets of N that overlap must be equal).

⁴Quotient groups were introduced by Hölder in 1889. He wrote $G|N$ and called it a quotient of groups: see p. 31 in <https://eudml.org/doc/157433>.

⁵If (2.2) is well-defined then for all $g \in G$ and $h \in H$, $gH = ghH$ and $g^{-1}H = g^{-1}H$. Thus $gg^{-1}H = ghg^{-1}H$, so $H = ghg^{-1}H$. Thus $ghg^{-1} \in H$ for all $g \in G$ and $h \in H$, so $gHg^{-1} \subset H$ for all $g \in G$. Thus $H \triangleleft G$ by Theorem 2.12.

As in $\mathbf{Z}/(m)$, where \bar{a} denotes the congruence class $a + m\mathbf{Z}$, we may write \bar{g} for gN in G/N and call \bar{g} the reduction of g modulo N . In this notation, the group law in G/N is $\boxed{\overline{g_1 g_2} = \overline{g_1} \overline{g_2}}$, with identity $\bar{1}$ and $\overline{g^{-1}} = \overline{g}^{-1}$. In additive notation, $\overline{g_1 + g_2} = \overline{g_1} + \overline{g_2}$, the identity is $\bar{0}$, and $\overline{-g} = -\overline{g}$.

Theorem 3.4. *Let G be a group and $N \triangleleft G$. For $g \in G$, $\overline{g^k} = \overline{g}^k$ for all $k \in \mathbf{Z}$.*

Proof. The case $k \geq 1$ follows by induction. The case $k = 0$ is trivial. For $k < 0$, write $k = -K$ where $K \geq 1$, so $\overline{g^K} = \overline{g^K}$. Then $\overline{g^k} = \overline{g^{-K}} = (\overline{g^K})^{-1} = \overline{g^K}^{-1} = \overline{(g^K)^{-1}} = \overline{g^{-K}} = \overline{g^k}$. \square

Corollary 3.5. *Let $N \triangleleft G$ and $[G : N] < \infty$. For each $g \in G$, $g^{[G:N]} \in N$.*

Proof. Let $t = [G : N]$, so the group G/N has order t . For each $g \in G$ we have $\overline{g^t} = \bar{1}$ in G/N . Therefore by Theorem 3.4, $\overline{g^t} = \bar{1}$, so $g^t \in N$. \square

Example 3.6. If $G = S_n$ and $N = A_n$, so $|G|/|N| = 2$, the corollary says $g^2 \in A_n$ for all $g \in S_n$. Indeed, whether or not g is an even or odd permutation, g^2 is even since its sign is $(\pm 1)^2 = 1$.

Remark 3.7. In the setting of Corollary 3.5, the power map $f : G \rightarrow G$ where $f(g) = g^{[G:N]}$ has values in N , but it is not necessarily a homomorphism! Consider $G = S_n$ and $N = A_n$, so $[G : N] = 2$. The mapping $S_n \rightarrow S_n$ where $\sigma \mapsto \sigma^2$ has values in A_n and is not a homomorphism when $n \geq 3$ since the squaring map on a group is a homomorphism if and only if the group is abelian: see Nonexample 5.2 in <https://kconrad.math.uconn.edu/blurbs/grouptheory/homomorphisms.pdf>. However, if G is finite and $N \subset Z(G)$ then $g \mapsto g^{[G:N]}$ is a homomorphism from G to N : see <https://math.stackexchange.com/questions/842500>.

When H is a non-normal subgroup of G with finite index, the conclusion of Corollary 3.5 with H in place of N may have counterexamples: it need not be true that $g^{|G|/|H|} \in H$ for all $g \in G$. For instance, if $G = S_3$ and $H = \{(1), (12)\}$, so $H \not\triangleleft G$ and $[G : H] = 3$, then $g^3 \notin H$ if g is (13) and (23) .⁶

Theorem 3.8. *Let G be a group and $N \triangleleft G$.*

- (1) *If G is abelian then G/N is abelian.*
- (2) *If G is cyclic then G/N is cyclic.*

Proof. (1) Pick two elements \bar{g} and \bar{g}' of G/N . Then

$$\overline{g g'} = \overline{g g'}, \quad \overline{g' g} = \overline{g' g},$$

Since G is commutative, $g g' = g' g$ in G , so $\overline{g g'} = \overline{g' g}$ in G/N . Thus $\overline{g} \overline{g'} = \overline{g'} \overline{g}$.

(2) Let G be cyclic with generator x , so every element of G has the form x^k for some $k \in \mathbf{Z}$. Thus every element of G/N is $\overline{x^k}$ for some $k \in \mathbf{Z}$, and $\overline{x^k} = \overline{x}^k$ by Theorem 3.4, so \overline{x} is a generator of G/N . \square

For the rest of this section we will look at some examples of quotient groups.

Example 3.9. $\mathbf{Z}/m\mathbf{Z}$: the quotient group $\mathbf{Z}/m\mathbf{Z}$ is $\mathbf{Z}/(m)$, the integers modulo m under addition.

Example 3.10. $\mathbf{R}/2\pi\mathbf{Z}$: angles on the circle in radians are real numbers up to adding an integer multiple of 2π . This is $\mathbf{R}/2\pi\mathbf{Z}$. For example, when we say “ $\pi = -\pi$ in radians” or “ $3\pi/2 = -\pi/2$ in radians”, we are working with real numbers modulo $2\pi\mathbf{Z}$: in $\mathbf{R}/2\pi\mathbf{Z}$, $\overline{\pi} = \overline{-\pi}$ and $\overline{3\pi/2} = \overline{-\pi/2}$. In trigonometry you get used to adding angles while ignoring integer multiples of 2π , and that is

⁶If $|G|$ is a prime power then $g^{[G:H]} \in H$ for all subgroups H of G and all $g \in G$, whether or not $H \triangleleft G$. The key term to look up is “subnormal subgroup.” All subgroups of a group of prime-power order are subnormal.

what addition and equality in $\mathbf{R}/2\pi\mathbf{Z}$ are all about: a number in $2\pi\mathbf{Z}$ is effectively treated like 0. Angles in degrees would be $\mathbf{R}/360\mathbf{Z}$ under addition.

Example 3.11. $\mathbf{R}^\times/\{\pm 1\}$: when working with nonzero real numbers known only up to a sign, you should be comfortable multiplying them while ignoring the sign: $(\pm x)(\pm y) = \pm xy$ where the signs are chosen arbitrarily. For example if $a = \pm 3$ and $b = \pm 5$ for some unknown signs then definitely $ab = \pm 15$. This type of multiplication up to a choice of sign is the same as working in $\mathbf{R}^\times/\{\pm 1\}$, since a coset of the subgroup $\{\pm 1\}$ in \mathbf{R}^\times is $\{\pm x\} = \{x, -x\}$ for $x \in \mathbf{R}^\times$.

So far our examples have been quotient groups of abelian groups, where every subgroup is normal. Our remaining examples will be G/N where G is a nonabelian group.

Example 3.12. S_n/A_n : there are two cosets for A_n in S_n , namely $\overline{(1)} = (1)A_n = A_n$ (the even permutations) and $\overline{(12)} = (12)A_n$ (the odd permutations). Therefore $S_n/A_n = \{\overline{(1)}, \overline{(12)}\}$. The group operation in S_n/A_n has $\overline{(12)}\overline{(12)} = \overline{(12)(12)} = \overline{(1)}$. This group is cyclic of order 2.

Example 3.13. $D_8/Z(D_8)$: the 16 elements of D_8 are

$$1, r, r^2, \dots, r^7, s, rs, r^2s, \dots, r^7s$$

and the center $Z(D_8)$ is $\{1, r^4\}$, with $r^{-4} = r^4$. Let $\bar{g} = gZ(D_8) = \{g, r^4g\}$. The size of $D_8/Z(D_8)$ is $16/2 = 8$, and the cosets in $D_8/Z(D_8)$ are

$$\begin{aligned} \bar{1} &= \{1, r^4\}, & \bar{r} &= \{r, r^5\}, & \bar{r^2} &= \{r^2, r^6\}, & \bar{r^3} &= \{r^3, r^7\}, \\ \bar{s} &= \{s, r^4s\}, & \bar{rs} &= \{rs, r^5s\}, & \bar{r^2s} &= \{r^2s, r^6s\}, & \bar{r^3s} &= \{r^3s, r^7s\}. \end{aligned}$$

What does the group $D_8/Z(D_8)$ look like?

Since $\bar{r}^4 = \bar{r^4} = \bar{1}$ and smaller powers of \bar{r} are not $\bar{1}$, \bar{r} has order 4 in $D_8/Z(D_8)$. The coset \bar{s} is not the identity since $s \notin Z(D_8)$ and $\bar{s}^2 = \bar{s^2} = \bar{1}$, so \bar{s} has order 2. Since $rs = sr^{-1}$ in D_8 , we have in $D_8/Z(D_8)$

$$\bar{r}\bar{s} = \bar{rs} = \overline{sr^{-1}} = \bar{s}\overline{r^{-1}} = \bar{s}\bar{r}^{-1},$$

so the multiplicative relations among \bar{r} and \bar{s} make $D_8/Z(D_8)$ look like the group D_4 .

Example 3.14. $\text{GL}_2(\mathbf{R})/\text{SL}_2(\mathbf{R})$: first we will show every coset has a unique representative of the form $\begin{pmatrix} \delta & 0 \\ 0 & 1 \end{pmatrix}$ where $\delta \in \mathbf{R}^\times$.

For $A \in \text{GL}_2(\mathbf{R})$, let \bar{A} be the coset $A\text{SL}_2(\mathbf{R}) = \{AB : B \in \text{SL}_2(\mathbf{R})\}$ and set $\delta = \det A$. Then $\begin{pmatrix} \delta & 0 \\ 0 & 1 \end{pmatrix}$ has determinant δ too, so $\begin{pmatrix} \delta & 0 \\ 0 & 1 \end{pmatrix}^{-1}A$ has determinant $(1/\delta)\delta = 1$. Thus $\begin{pmatrix} \delta & 0 \\ 0 & 1 \end{pmatrix}^{-1}A \in \text{SL}_2(\mathbf{R})$, so $A \in \begin{pmatrix} \delta & 0 \\ 0 & 1 \end{pmatrix}\text{SL}_2(\mathbf{R})$. That shows $\bar{A} = \overline{\begin{pmatrix} \delta & 0 \\ 0 & 1 \end{pmatrix}}$, so each coset in $\text{GL}_2(\mathbf{R})/\text{SL}_2(\mathbf{R})$ is represented by a matrix of the form $\begin{pmatrix} \delta & 0 \\ 0 & 1 \end{pmatrix}$. This δ is unique: if

$$\overline{\begin{pmatrix} \delta & 0 \\ 0 & 1 \end{pmatrix}} = \overline{\begin{pmatrix} \delta' & 0 \\ 0 & 1 \end{pmatrix}}$$

then $\begin{pmatrix} \delta & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \delta' & 0 \\ 0 & 1 \end{pmatrix}B$ with $\det B = 1$, so taking determinants of both sides implies $\delta = \delta' \det B = \delta'$.

Having shown the matrices $\begin{pmatrix} \delta & 0 \\ 0 & 1 \end{pmatrix}$ represent the cosets in $\text{GL}_2(\mathbf{R})/\text{SL}_2(\mathbf{R})$, the multiplicative rule $\begin{pmatrix} \delta & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} \delta' & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \delta\delta' & 0 \\ 0 & 1 \end{pmatrix}$ for matrices implies the rule $\overline{\begin{pmatrix} \delta & 0 \\ 0 & 1 \end{pmatrix}} \cdot \overline{\begin{pmatrix} \delta' & 0 \\ 0 & 1 \end{pmatrix}} = \overline{\begin{pmatrix} \delta\delta' & 0 \\ 0 & 1 \end{pmatrix}}$ for cosets, so the quotient group $\text{GL}_2(\mathbf{R})/\text{SL}_2(\mathbf{R})$ resembles the group \mathbf{R}^\times under multiplication.

Example 3.15. $\text{GL}_2(\mathbf{Z}/(m))/\text{SL}_2(\mathbf{Z}/(m))$: reasoning like in the previous example, with \mathbf{R}^\times replaced by $(\mathbf{Z}/(m))^\times$, each coset in $\text{GL}_2(\mathbf{Z}/(m))/\text{SL}_2(\mathbf{Z}/(m))$ has a unique representative of the form $\begin{pmatrix} \delta & 0 \\ 0 & 1 \end{pmatrix}$ with $\delta \in (\mathbf{Z}/(m))^\times$, and the quotient group $\text{GL}_2(\mathbf{Z}/(m))/\text{SL}_2(\mathbf{Z}/(m))$ resembles $(\mathbf{Z}/(m))^\times$ under multiplication.

Don't confuse quotient groups and subgroups! Even though the elements of $\mathbf{Z}/m\mathbf{Z}$ have representatives in \mathbf{Z} , such as $\{0, 1, \dots, m-1\}$, the group $\mathbf{Z}/m\mathbf{Z}$ is *not* a subgroup of \mathbf{Z} : elements of $\mathbf{Z}/m\mathbf{Z}$ have finite order while nonzero elements of \mathbf{Z} do not. For example, $\{0, 1, \dots, m-1\}$ for $m \geq 2$ is not closed under addition, so this set of integers is in no way a subgroup of \mathbf{Z} . Subgroups are inside a group while quotient groups are a type of collapsing of a group, generalizing the way \mathbf{R} can be wrapped around to form the circle group $\mathbf{R}/2\pi\mathbf{Z}$.

4. ORDERS OF ELEMENTS IN A QUOTIENT GROUP

Let's compare the order of an element in G to its order in G/N . To say \bar{g} in G/N has order k means $\bar{g}^k = \bar{1}$ and no smaller power has that property. In terms of G itself, this is saying $g^k \in N$ and k is the smallest positive integer with that property. Passing from G to G/N , the order of an element can *drop*: from infinite to finite or from finite to a smaller finite value.

Example 4.1. In the additive group \mathbf{Z} , 1 has infinite order while in $\mathbf{Z}/6\mathbf{Z}$, $\bar{1} = 1 + 6\mathbf{Z}$ has order 6.

Example 4.2. In the quaternion group Q_8 , the subgroup $\{\pm 1\}$ is normal (it is the center of Q_8)⁷. The order of i in Q_8 is 4 and the order of \bar{i} in $Q_8/\{\pm 1\}$ is 2 since $\bar{i}^2 = \overline{-1} = \bar{1}$ and $\bar{i} \neq \bar{1}$.

Example 4.3. For $n \geq 3$, the n -cycle $(12 \dots n)$ has order n in S_n , while its reduction in S_n/A_n has order 1 or 2 since S_n/A_n is a group of order 2. For a permutation $\sigma \in S_n$, the reduction $\bar{\sigma} = \sigma A_n$ in S_n/A_n is trivial if σ is even and nontrivial if σ is odd, so $\bar{\sigma}$ has order 1 if σ is even and order 2 if σ is odd.

Example 4.4. Let $G = \mathbf{Z}/20\mathbf{Z}$ and $N = 10\mathbf{Z}/20\mathbf{Z}$. Then G is cyclic of order 20 and $N = \{0, 10 \bmod 20\}$ is a normal subgroup of order 2 (all subgroups of a cyclic group are normal). The quotient group G/N is a cyclic group of order $20/2 = 10$ by Theorem 3.8 and its proof shows each generator of G reduces in G/N to a generator of G/N . For example, $1 \bmod 20$ has order 20 in G , while in G/N , $\overline{1 \bmod 20}$ has order 10. An element's order dropped from 20 to 10 when we pass from G to G/N . The order of $5 \bmod 20$ in G is 4, while the order of $\overline{5 \bmod 20}$ in G/N is 2. The order of $4 \bmod 20$ in G and the order of $\overline{4 \bmod 20}$ in G/N are both 5.

Theorem 4.5. *If G is a group with a normal subgroup N and g in G has finite order m , then the order of \bar{g} in G/N is a factor of m .*

Proof. In G we have $g^m = 1$, so in G/N we have $\bar{g}^m = (gN)^m = g^m N = N = \bar{1}$. Therefore \bar{g} has order dividing m . \square

If \bar{g} in G/N has finite order k , then Theorem 4.5 tells us each coset representative of \bar{g} in G has order divisible by k (if the representative has finite order, *e.g.*, if G is finite). There may or may not be a representative of \bar{g} with order k .

Example 4.6. Let $G = \mathbf{Z}/12\mathbf{Z} = \{0, 1, \dots, 11 \bmod 12\}$ and $N = 2\mathbf{Z}/12\mathbf{Z} = \{0, 2, 4, 6, 8, 10 \bmod 12\}$. In G/N , $\overline{1 \bmod 12}$ has order 2 and its coset representatives in G are $\{1, 3, 5, 7, 9, 11 \bmod 12\}$, where the representatives have order 12, 4, 12, 12, 4, and 12: no coset representative has order 2.

Example 4.7. In $Q_8/\{\pm 1\}$ the element \bar{i} has order 2 and its coset representatives in Q_8 are $\pm i$, which both have order 4.

⁷In fact every subgroup of Q_8 is a normal subgroup, even though Q_8 is not abelian.

Example 4.8. In $(\mathbf{Z}/35\mathbf{Z})^\times$, which has size 24, 11 mod 35 has order 3: $\langle 11 \rangle = \{1, 11, 16 \text{ mod } 35\}$. In $(\mathbf{Z}/35\mathbf{Z})^\times$ the order of 2 is 12, and the order of 2 drops from 12 to 4 when we pass to the quotient group $(\mathbf{Z}/35\mathbf{Z})^\times / \langle 11 \rangle$, since the least positive power of 2 mod 35 that is inside $\langle 11 \rangle = \{1, 11, 16 \text{ mod } 35\}$ is 2^4 .

Corollary 4.9. *If G is a finite group with a normal subgroup N such that the order $|N|$ and index $[G : N]$ are relatively prime, then N is the only subgroup of G having its size: if H is a subgroup of G such that $|H| = |N|$ then $H = N$.*

Proof. Let $|N| = n$. For $h \in H$ we have $h^n = 1$ since $|H| = n$. In the quotient group G/N we get $\bar{h}^n = \bar{1}$, so the order of \bar{h} divides n . Also the order of \bar{h} divides $|G/N|$, so from $(|N|, |G/N|) = 1$ we get $\bar{h} = \bar{1}$ in G/N . Thus $h \in N$. This holds for all $h \in H$, so $H \subset N$, and thus $H = N$ because $|H| = |N|$. \square

Remark 4.10. This corollary does not say a subgroup with relatively prime order and index is the only subgroup of its size, but rather that a *normal* subgroup with relatively prime order and index is unique for its size. For instance, when $G = S_3$, the subgroup A_3 is normal in G and is the only subgroup of its size (order is 3, index is 2), but $\{(1), (12)\}$ is not normal in G and is not the only subgroup of its size (order is 2, index is 3).

Although the order of \bar{g} in a quotient group G/N might not “lift” to the order of some coset representative of \bar{g} in G , the next theorem shows the property of having p -power order (but not a specific p -power order) can be lifted from G/N to G when G is finite.

Theorem 4.11. *If G is a finite group, $N \triangleleft G$, and \bar{g} has p -power order in G/N for a prime p , then some coset representative for \bar{g} has p -power order in G .*

Proof. Let \bar{g} have order p^r in G/N and g have order m in G , so $p^r \mid m$ by Theorem 4.5. Write $m = p^s n$ where $p \nmid n$, so $r \leq s$. We will show $g = ab$ where a and b are powers of g such that $a^{p^s} = 1$ and $b \in N$ with $b^n = 1$, so $\bar{g} = \bar{a}$ and a has p -power order.

Since p^s and n are relatively prime, we can write $1 = p^s x + ny$ for some integers x and y . Then

$$g = g^1 = g^{p^s x} g^{ny} = g^{ny} g^{p^s x}$$

where $a := g^{ny}$ satisfies $a^{p^s} = g^{p^s ny} = g^{mxy} = 1$ and $b := g^{p^s x}$ satisfies $b^n = g^{p^s nx} = g^{mxy} = 1$. Since $r \leq s$ and $\bar{g}^{p^r} = \bar{1}$, we have $\bar{g}^{p^s} = \bar{1}$, so $g^{p^s} \in N$. Thus $b = g^{p^s x} \in N$, so $g = ab \Rightarrow \bar{g} = \bar{a}$ in G/N with a having order dividing p^s , which means a has p -power order. \square

In this proof, it turns out that a has order p^s and b has order n . This is explained by Theorem 6.1 in <https://kconrad.math.uconn.edu/blurbs/grouptheory/order.pdf>, which shows a and b are the unique commuting elements of G with orders p^s and n that have product g .

Example 4.12. Let $G = \mathbf{Z}/90\mathbf{Z}$ and $N = 15\mathbf{Z}/90\mathbf{Z}$, so $G/N \cong \mathbf{Z}/15\mathbf{Z}$.

- In G/N , 5 has (additive) order 3 while in G , 5 has order 18 but $5 = 20$ in G/N and 20 in G has order 9.
- In G/N , 6 has (additive) order 5 while in G , 6 has order 30 but $6 = 36$ in G/N and 36 in G has order 5.