Chapter 10

Given a group G and a subgroup H, we are going to construct a new group called the quotient and denoted G/H. However, our construction will only work if the left and right cosets of H are equal: That is, $gH = Hg$ for all $g \in G$.

Definition: A subgroup $H \subset G$ is called normal in G if $gH = Hg$ for all $g \in G$.

Example: If G is an abelian group, then $gH = Hg$ for every subgroup $H \subset G$ and every $g \in G$. Therefore every subgroup of an abelian group is normal.

Example: Consider the subgroup $H = \{\text{identity}, (1,2)\}$ of S_3. Then

$$(1,2,3)H = \{(1,2,3), (1,3)\}$$

and $$H(1,2,3) = \{(1,2,3), (2,3)\}$$

so H is not a normal subgroup. On the other hand, if we consider the subgroup $K \subset S_3$ where

$K = \{\text{identity}, (1,2,3), (1,3,2)\}$

then $[S_3 : K] = 2$ and so the two cosets of K are:

- K itself, and
- $\sigma K = S_3 \setminus K$, where σ is any permutation not in K. Similarly $K\sigma = S_3 \setminus K$ for any $\sigma \notin K$, so $\sigma K = K\sigma$ for all $\sigma \in S_3$

Therefore K is normal.

Here's how we check whether or not a given subgroup is normal:

Theorem 10.3 Let G be a group and N a subgroup. The following statements are equivalent:

1. N is a normal subgroup of G
2. For all $g \in G$, $gNg^{-1} \subseteq N$
3. For all $g \in G$, $gNg^{-1} = N$.

Proof: We do $(1) \Rightarrow (2) \Rightarrow (3) \Rightarrow (1)$.

To show $(1) \Rightarrow (2)$, we first assume N is normal in G. Fix an element $n \in N$. Since $gN = Ng$ for all $g \in G$ there exists an element $n' \in N$ such that

$gn = n'g$. In other words, for all $g \in G$ we have $gng^{-1} = n' \in N$. This shows $gNg^{-1} \subset N$, so (2) holds.

Now assuming (2) is true, we need to show the reverse containment $N \subseteq gNg^{-1}$ in order to conclude (3), $gNg^{-1} = N$. So let $n \in N$ be given, and let $g \in G$. Then $g^{-1}ng = \underbrace{g^{-1}n(g^{-1})^{-1}}_{\text{an element of } g^{-1}N(g^{-1})^{-1}} \in N$, so there exists $n' \in N$ such that $g^{-1}n(g^{-1})^{-1} = n'$, meaning $n = gn'g^{-1}$ is an element of gNg^{-1}. So (3) holds.

Finally, (3) $\Rightarrow$ (1). Assuming $gNg^{-1} = N$ for all $g \in G$, let $n \in N$. Then there exists n' such that $gng^{-1} = n'$. Consequently $gn = n'g$, so $gN \subset Ng$. By an identical argument we get $Ng \subset gN$, so $gN = Ng$ and (1) holds.

Example: Consider

$$G = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \;\middle|\; a,b,c \in \mathbb{R},\ \underbrace{ac \neq 0}_{ac=1} \right\}$$

Then G is a subgroup of $GL(2,\mathbb{R})$ (this basically follows from the fact that the product of upper triangular matrices is upper triangular)

Set $H = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \;\middle|\; b \in \mathbb{R} \right\}$. Then $H \subset G$

and it is not hard to check that H is a subgroup. In fact, it is a normal subgroup since for any $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in G$, we have for every $\begin{pmatrix} 1 & b' \\ 0 & 1 \end{pmatrix} \in H$

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\begin{pmatrix} 1 & b' \\ 0 & 1 \end{pmatrix}\begin{pmatrix} c & -b \\ 0 & a \end{pmatrix}$$

$$= \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\begin{pmatrix} c & -b+ab' \\ 0 & a \end{pmatrix}$$

$$= \begin{pmatrix} ac & a(ab'-b)+ab \\ 0 & ac \end{pmatrix} = \begin{pmatrix} 1 & a^2b' \\ 0 & 1 \end{pmatrix}.$$

Thus $gHg^{-1} \subset H$ for all $g \in G$, so H is normal

Here is why we want to study normal subgroups: When $N \subseteq G$ is normal, we can define the quotient group G/N as follows:

Definition: If G is a group and N a normal subgroup, let G/N denote the set of left cosets of N. Define a binary operation on the cosets by

$$(gN) * (hN) = ghN$$

that is, you multiply cosets by multiplying representatives. Then with this operation, G/N becomes a group,

called the quotient group of G by N.

Remark: It's not immediately clear that the operation above is well-defined. A coset can be written with many different representatives, so if $gN = g'N$ and $hN = h'N$, how do we know that

$$(hN)(gN) = hgN$$

gives the same result as

$$(h'N)(g'N) = h'g'N \quad ?$$

The proof of this fact requires N to be normal, and it is exactly the proof that shows why we restrict our attention to normal subgroups.

Theorem: Let N be a normal subgroup of G. Then G/N defined above is indeed a group.

Proof: First we show that $(aN)*(bN) = abN$ is well-defined. So let $aN = a'N$ and $bN = b'N$.

Then $a = a'n_1$ and $b = b'n_2$ for some $n_1, n_2 \in N$.

Therefore
$$\begin{aligned} abN &= a'n_1 b'n_2 N \\ &= a'n_1 b'N \quad (\text{since } n_2 N = N) \\ &= a'n_1 Nb' \quad (\text{since } b'N = Nb', N \text{ is normal}) \\ &= a'Nb' \quad (\text{since } n_1 N = N) \\ &= a'b'N \quad (\text{since } N \text{ is normal}). \end{aligned}$$

so indeed, our operation is well-defined.

- It is associative since the operation in G is associative.
- It has an identity: eN, because

$$(gN)(eN) = (ge)N = gN$$
$$(eN)(gN) = egN = gN \quad \text{for all } g \in G,$$

- It has inverses since

$(gN)^{-1} = g^{-1}N$, because $(gN)(g^{-1}N) = eN$.

Remark: Remember, the elements of G/N are sets of elements of G. They are cosets!

Example: $G/\{1\}$ is the set of cosets

$g \cdot \{1\} = \{g\}$ for all $g \in G$, with multiplication

$$(g \cdot \{1\})(h \cdot \{1\}) = gh \cdot \{1\}$$

or $\{g\} \cdot \{h\} = \{gh\}$. So $G/\{1\} \cong G$.

Similarly trivial is G/G, then there is only one coset (G itself), so G/G is a group with one element, namely $\{e\}$.

Example: We saw that the subgroup $N = \langle (1,2,3) \rangle$ of S_3 is normal. So the set S_3/N of left cosets becomes a group. Since N has only two cosets in S_3, the group S_3/N must have only two elements, so $S_3/N \cong \mathbb{Z}_2$.

Example: The cosets of $n\mathbb{Z} \subset \mathbb{Z}$ are

$$0 + n\mathbb{Z} = \{\ldots, -2n, -n, 0, n, 2n, \ldots\}$$

$$1 + n\mathbb{Z} = \{\ldots, -2n+1, -n+1, 1, n+1, 2n+1, \ldots\}$$

$$\vdots$$

etc, ending with $(n-1) + n\mathbb{Z}$.

Since the subgroup $n\mathbb{Z}$ is normal ($\mathbb{Z}$ is abelian), we can form the group $\mathbb{Z}/n\mathbb{Z}$ and the operation is

$$(j + n\mathbb{Z}) + (i + n\mathbb{Z}) = (j+i) + n\mathbb{Z}.$$

This is exactly our definition of $\mathbb{Z}_n$. Thus $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$.

Example: Let

$GL(2,\mathbb{R})$ = invertible 2×2 matrices, and

$SL(2,\mathbb{R})$ = invertible 2×2 matrices with determinant 1.

Then $SL(2,\mathbb{R})$ is normal, because if $A \in SL(2;\mathbb{R})$ then for every $B \in GL(2,\mathbb{R})$ we compute

$$\det(BAB^{-1}) = \det(A) = 1$$

so that $B(SL(2;\mathbb{R}))B^{-1} \subset SL(2;\mathbb{R})$ for all B.

Therefore we can take the quotient $GL(2;\mathbb{R})/SL(2;\mathbb{R})$.

Define a map $\phi : GL(2;\mathbb{R})/SL(2;\mathbb{R}) \longrightarrow \mathbb{R}^*$ by

$$\phi(A \cdot SL(2;\mathbb{R})) = \det(A).$$

Claim: ϕ is well-defined.

Suppose $A \cdot SL(2;\mathbb{R}) = B \cdot SL(2;\mathbb{R})$. Then $AP = BQ$ for some $P, Q \in SL(2;\mathbb{R})$. Thus,

$$\det(A) = \det(AP) = \det(BQ) = \det(B)$$

So that $\phi(A \cdot SL(2;\mathbb{R})) = \phi(B \cdot SL(2;\mathbb{R}))$, and ϕ is well-defined.

Claim: ϕ is bijective:

If $\phi(A \cdot SL(2;\mathbb{R})) = \phi(B \cdot SL(2;\mathbb{R}))$, then $\det(A) = \det(B)$, therefore $A^{-1}B^{+1} \in SL(2;\mathbb{R})$.

So $A^{-1}B \cdot SL(2;\mathbb{R}) = SL(2;\mathbb{R})$

$\Rightarrow B \cdot SL(2;\mathbb{R}) = A \cdot SL(2;\mathbb{R})$, so ϕ is 1-to-1.

ϕ is surjective since $\phi\left(\begin{pmatrix} r & 0 \\ 0 & 1 \end{pmatrix} \cdot SL(2,\mathbb{R})\right) = r$ for every $r \in \mathbb{R}^*$.

So ϕ is bijective.

Last, ϕ respects the group operation since

$$\phi(A \cdot SL(2;\mathbb{R}) * B \cdot SL(2;\mathbb{R})) = \phi(A \cdot SL(2;\mathbb{R})) \cdot \phi(B \cdot SL(2;\mathbb{R}))$$

$$\| \qquad\qquad\qquad\qquad\qquad\qquad \|$$

$$\phi(AB \cdot SL(2;\mathbb{R})) \qquad\qquad \det A \cdot \det(B)$$

$$\|$$

$$\det(AB) \qquad\qquad \det(AB).$$

Example. The group A_n is normal in S_n, since it has only two cosets: A_n itself and $S_n \setminus A_n$.

So $\sigma A_n = A_n \sigma = S_n \setminus A_n$ whenever $\sigma \notin A_n$.

Since $|S_n| / |A_n| = 2$, $S_n / A_n \simeq \mathbb{Z}_2$.

Theorem: Let G be a group and N a normal subgroup. If G is finite, then

$$|G/N| = |G|/|N| = [G : N].$$

Proof: Apply Lagrange's theorem.

So, in order for a group to have a nontrivial quotient, it must have a proper nontrivial normal subgroup.

Definition: A group with no proper, nontrivial normal subgroups is called simple.

Example: Consider the group $\mathbb{Z}_p$. Since any subgroup $H \subset \mathbb{Z}_p$ must satisfy: $|H|$ divides $|\mathbb{Z}_p| = p$, if p is prime then $|H| = \{1\}$ or p.

$\Rightarrow$ When p is prime, $\mathbb{Z}_p$ is a simple group.

Remark: One of the largest projects in "modern day" group theory was to classify all finite simple groups (ie, write a list of them). We've just started the list:

- $\mathbb{Z}_p$ where $p \in \mathbb{Z}$ is prime.

The next item on the list is:

- A_n for $n \geq 5$.

So let us sketch the proof, leaving in some of the details but omitting some of the longer calculations.

Lemma 1 Every element in A_n can be written as a product of 3-cycles.

Proof: Since every element of A_n can be written as an even product of transpositions, it suffices to show that any pair $(a,b)(c,d)$ of transpositions is a product of 3-cycles. Taking into account that $(ab) = (ba)$, there are only 3 possible pairs:

$$(a,b)(a,b) = id$$
$$(a,b)(c,d) = (a,c,b)(a,c,d)$$
$$(a,b)(a,c) = (a,c,b).$$

And since they're all products of 3-cycles, done.

Lemma 2 Let N be a normal subgroup of A_n. If N contains a 3-cycle, then $N = A_n$.

Proof. Fix $i,j \in \{1,2,\dots,n\}$. We'll first show that every element in A_n can be written as a product of 3-cycles of the form (i,j,k), where k varies over $\{1,2,\dots,n\}$.

First, we show every 3-cycle is a product of such elements by considering cases:

Case 1: A three cycle containing both i and j. Then we can assume it is of the form (i,a,j), and observe

$$(i,a,j) = (i,j,a)^2.$$

Case 2: The 3-cycle contains only j. Then we can assume it is of the form (j,a,b), and

$$(j,a,b) = (i,j,b)^2(i,j,a).$$

Case 3: The 3-cycle contains only i. Then we can assume it is of the form (i,a,b), and

$$(i,a,b) = (i,j,b)(i,j,a)^2.$$

Case 4: Neither i, nor j appears in the 3-cycle. Then

$$(a,b,c) = (i,j,a)^2(i,j,c)(i,j,b)^2(i,j,a).$$

= end cases =

Now suppose N is a nontrivial normal subgroup, and contains a 3-cycle (a,b,c). Then since N is normal, N must also contain

$$\left[(a,b)(c,k)\right](a,b,c)^2\left[(a,b)(c,k)\right]^{-1} = (a,b,k)$$

for all k. So N contains all 3-cycles of the form (a,b,k), $k \in \{1,\ldots,n\}$. But the cycles of this form allow us to get every 3-cycle in A_n

by using the previous cases and taking products. So every 3-cycle is in N.

By our previous lemma, every element of A_n is a product of 3-cycles; but every product of 3-cycles is in N. So $A_n \subset N$, and $N = A_n$.

Lemma 3: For $n \geq 5$, every nontrivial normal subgroup N of A_n contains a 3-cycle.

Proof: Another very long case argument with heavy calculations. Five cases total, see the text for all the details.

Theorem: The group A_n for $n \geq 5$ is simple.

Proof: Let N be a normal subgroup of A_n. By Lemma 3, N contains a 3-cycle. By Lemma 2, this forces $N = A_n$. Thus A_n contains no proper, nontrivial normal subgroups, and so is simple.

A remarkable effort to classify all finite simple groups concluded in 2004, the proof ~~covers~~ is several tens of thousands of pages long and is the work of about 100 authors.

Their final list was:

- $\mathbb{Z}_p$ for $p \geq 2$ prime
- A_n for $n \geq 5$
- 16 other infinite families of simple groups

+ 26 groups which do not fit into any family and are therefore called "sporadic groups".

The 26 sporadic groups are really remarkable. The final one was found in 1981(ish) building on the work of many authors. It has order:

808017424794512875886459904961710757005

754368000000000 (54 digits).

It is a group of matrices of size

$$196882 \times 196882.$$

with entries in $\mathbb{Z}_2$.

Exercises: 1, 4, 5, 6, 7, 8, 9, 10, 11.