

Chapter 9

Quotient Groups

“Algebra is the offer made by the devil to the mathematician...All you need to do, is give me your soul: give up geometry.” (Michael Atiyah)

Based on the previous lectures, we now have the following big picture. We know that planar isometries are examples of groups, and more precisely, that finite groups of planar isometries are either cyclic groups or dihedral groups (this is Leonardo Theorem). We also know that there other groups out there, for example the alternating group, but still, most of the groups we have seen can be visualised in terms of geometry. The goal of this lecture is to introduce a standard object in abstract algebra, that of quotient group. This is likely to be the most “abstract” this class will get! Thankfully, we have already studied integers modulo n and cosets, and we can use these to help us understand the more abstract concept of quotient group.

Let us recall what a coset is. Take a group G and a subgroup H . The set $gH = \{gh, g \in H\}$ is a left coset of H , while $Hg = \{hg, h \in H\}$ is a right coset of H . Consider all the distinct cosets of G (either right or left cosets). The question is: does the set of all distinct cosets of G form a group?

Example 31. Consider $G = \{0, 1, 2, 3\}$ to be the set of integers modulo 4, and take the subgroup $H = \{0, 2\}$ (you might want to double check that you remember why this is a subgroup). We have two cosets H and $1+H = \{1, 3\}$. To have a group structure, we need to choose a binary operation. Let us say we start with $+$, the addition modulo 4. How do we add two cosets? Let us try elementwise. To compute $\{0, 2\} + \{1, 3\}$, we have $\{0+1, 0+3, 2+1, 2+3\} = \{1, 3\}$. It seems not bad, the sum of these two cosets does give another coset!

Quotient Group Recipe

Ingredients:

- A group G , a subgroup H , and cosets gH

The set $gH = \{gh, h \in H\}$ is called a **left coset** of H .

The set $Hg = \{hg, h \in H\}$ is called a **right coset** of H .

- Group structure



When does the set of all cosets of H form a group?

1st Example (I)

All cosets of H : $0+H = \{0,2\}$, $1+H = \{1,3\}$, $2+H = \{0,2\}$, $3+H = \{1,3\}$.

The set of cosets is $\{\{0,2\}, \{1,3\}\}$. **Does it form a group?**

We need a **binary operation**, say we keep $+$.

$G = \{0,1,2,3\}$ integers modulo 4
 $H = \{0,2\}$ is a subgroup of G .
 The coset $1+H = \{1,3\}$.

0	2	1	3	G
---	---	---	---	---

Let us compute!

- $\{0,2\} + \{0,2\} = \{0,2\}$
- $\{0,2\} + \{1,3\} = \{1,3\}$
- $\{1,3\} + \{1,3\} = \{0,2\}$

$1 + \{1,3\} = \{2,0\}$, $3 + \{1,3\} = \{0,2\}$

Let us try to do that with both cosets, and summarize it in a Cayley table.

	$\{0, 2\}$	$\{1, 3\}$
$\{0, 2\}$	$\{0, 2\}$	$\{1, 3\}$
$\{1, 3\}$	$\{1, 3\}$	$\{0, 2\}$

We notice that we indeed have a group structure, since the set of cosets is closed under the binary operation $+$, it has an identity element $\{0, 2\}$, every element has an inverse, and associativity holds. In fact, we can see from the Cayley table that this group is in fact isomorphic to the cyclic group C_2 .

In the above example, we defined a binary operation on the cosets of H , where H is a subgroup of a group $(G, +)$ by

$$(g + H) + (k + H) = \{g + h + k + h' \text{ for all } h, h'\}.$$

We now illustrate using the same example that computations could have been done with a choice of a representative instead.

Example 32. We continue with the same setting as in Example 31. Since $0 + H = \{0, 2\}$ and $1 + H = \{1, 3\}$, we have

$$(0 + H) + (1 + H) = (0 + 1) + H = 1 + H$$

using the representative 0 from $0 + H$ and 1 from $1 + H$. Alternatively, if 2 and 3 are chosen as representatives instead, we have

$$(2 + H) + (3 + H) = (2 + 3) + H = 1 + H$$

since $5 \equiv 1 \pmod{4}$. There are in total 4 ways of choosing the coset representatives, since 0 and 2 can be chosen for the first coset, and 1 and 3 could be chosen in the second coset. Any choice will give the same answer as the sum of the two cosets.

1st Example (II)

+	{0,2}	{1,3}
{0,2}	{0,2}	{1,3}
{1,3}	{1,3}	{0,2}

This is the cyclic group C_2 !

We observe

1. The set of cosets is closed under the binary operation $+$.
 2. It has an identity element $\{0,2\}$.
 3. Every element has an inverse.
 4. Associativity
-

1st Example (III)

+	{0,2}	{1,3}
{0,2}	{0,2}	{1,3}
{1,3}	{1,3}	{0,2}

Can be computed using coset representatives!

$G = \{0,1,2,3\}$ integers modulo 4. $H = \{0,2\}$ is a subgroup of G .

All cosets of H : $0+H = \{0,2\}$, $1+H = \{1,3\}$, $2+H = \{0,2\}$, $3+H = \{3,1\}$.

How to compute with cosets:

- $\{0,2\} = 0+H = 2+H$: $\{0,2\} + \{0,2\} = (\mathbf{0}+H) + (\mathbf{0}+H) = (\mathbf{0+0})+H = \mathbf{H} = \{0,2\}$
 $= (\mathbf{0}+H) + (\mathbf{2}+H) = (\mathbf{0+2})+H = \mathbf{H} = \{0,2\}$
 - $\{1,3\} = 1+H = 3+H$: $\{0,2\} + \{1,3\} = (\mathbf{0}+H) + (\mathbf{1}+H) = (\mathbf{0+1})+H = \mathbf{1+H} = \{1,3\}$
 $= (\mathbf{2}+H) + (\mathbf{3}+H) = (\mathbf{2+3})+H = \mathbf{1+H} = \{1,3\}$
-

Let us now revisit integers modulo n . We recall that a and b are said to be congruent modulo n if their difference $a - b$ is an integer which is a multiple of n . We saw that being congruent mod n is an equivalence relation, and that addition modulo n is well defined, which led to the definition of group of integers modulo n with respect to addition.

Now consider the group $G = \mathbb{Z}$ of integers, and the subgroup $H = n\mathbb{Z}$, that is

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

is the set of multiples of n (you might check that this is indeed a subgroup). We now consider the cosets of H , that is

$$-2 + H, -1 + H, 0 + H, 1 + H, 2 + H, \dots$$

Example 33. If $n = 3$, then $H = 3\mathbb{Z}$ consists of the multiple of 3. We have exactly 3 distinct cosets, given by

$$0 + H, 1 + H, 2 + H$$

since \mathbb{Z} is partitioned by these 3 cosets. Indeed, $0 + H$ contains all the multiples of 3, $1 + H$ contains all the multiples of 3 to which 1 is added, and $0 + H$ all the multiples of 3, to which 2 is added, which cover all the integers.

Now when we do computations with integers modulo 3, we choose a coset representative. When we compute $(0 \pmod 3) + (1 \pmod 3)$, we are looking at the sum of the coset $(0 + H)$ and of the coset $(1 + H)$.

2nd Example: Recall integers mod n

For a positive integer n , two integers a and b are said to be **congruent modulo n** if their difference $a - b$ is an integer multiple of n : $a \equiv b \pmod{n}$.

Being congruent mod n is an **equivalence relation**.

Addition modulo n was defined on equivalence classes, since we showed that it is well defined **independently of the choice of the representative!**



Group of integers modulo n

2nd Example: Integers mod n revisited

Consider the group G of integers \mathbb{Z} . Let $H = n\mathbb{Z}$ be the subgroup formed by multiple of n .

All cosets of H : $\dots, -2+H, -1+H, 0+H, 1+H, 2+H \dots$

Check it's a subgroup!

Example: $n = 3$, $0+H$, $1+H$, $2+H$ partition G

... -8 -7 -6 -5 -4 -3 -2 -1 0 1 2 3 4 5 6 7 8 ...

+	$0+H$	$1+H$	$2+H$
$0+H$	$0+H$	$1+H$	$2+H$
$1+H$	$1+H$	$2+H$	$0+H$
$2+H$	$2+H$	$0+H$	$1+H$

Coset representatives are used for coset computations

- $0+H$ = equivalence class of 0 mod 3
- $1+H$ = equivalence class of 1 mod 3
- $2+H$ = equivalence class of 2 mod 3

In the case of integers modulo n , we do have that cosets form a group. Now we may wonder whether this is true in general. To answer this question, let us take a general group G , and its set of cosets. We need to define a binary operation:

$$(gH, g'H) \mapsto (gH)(g'H)$$

multiplicatively, or

$$(g + H, g' + H) \mapsto (g + H) + (g' + H)$$

additively. Now, is the set $\{gH, g \in G\}$ closed under this binary operation, that is, is it true that

$$(gH)(g'H) = gg'H$$

multiplicatively, or

$$(g + H) + (g' + H) = (g + g') + H$$

additively. Let us see what happens multiplicatively. If we choose two elements $gh \in gH$ and $g'h' \in g'H$, then

$$(gh)(g'h') \neq gg'hh'$$

in general. We do have equality if the group is Abelian, but otherwise there is no reason for that to be true. This leads us to the following definition.

Definition 18. A subgroup H of (G, \cdot) is called a **normal subgroup** if for all $g \in G$ we have

$$gH = Hg.$$

We shall denote that H is a subgroup of G by $H < G$, and that H is a normal subgroup of G by $H \triangleleft G$.

One has to be very careful here. The equality $gH = Hg$ is a set equality! It says that a right coset is equal to a left coset, it is not an equality elementwise.

When do Cosets form a Group? (I)

- G a group, H a subgroup, $gH = \{gh, h \text{ in } H\}$ a coset.
- Consider the set $\{gH, g \text{ in } G\}$.
- We need to define a **binary operation**:

map gH and $g'H$ to $(gH)(g'H)$ multiplicatively
map $(g+H)$ and $(g'+H)$ to $(g+H)+(g'+H)$ additively

Is the set $\{gH, g \text{ in } G\}$ **closed** under this binary operation?

$(gH)(g'H) = gg'H$ multiplicatively
 $(g+H)+(g'+H) = (g+g')+H$ additively



When do Cosets form a Group? (II)

$(gH)(g'H) = gg'H$ multiplicatively
 $(g+H)+(g'+H) = (g+g')+H$ additively



Take gh in gH and $g'h'$ in $g'H$.

Do we have that $(gh)(g'h') = gg'h''$?

Not necessarily... True if G is **abelian**, otherwise not clear.

If $\mathbf{gH = Hg}$, then $gh = h'g$, and the set $\{gH, g \text{ in } G\}$ is **closed** under the binary operation.

This does NOT mean $gh = hg$, this means $gh = h'g$.

Now suppose we have (G, \cdot) a group, H a normal subgroup of G , i.e., $H \triangleleft G$, and the set of cosets of H in G , i.e., the set G/H defined by $G/H = \{gH | g \in G\}$.

Theorem 16. *If $H \triangleleft G$, then $(G/H, (g_1H)(g_2H) = (g_1g_2)H)$ is a group.*

Proof. To check what we have a group, we verify the definition.

1. Closure: $(g_1H)(g_2H) = g_1(Hg_2)H = g_1g_2H \in G/H$ using that $g_2H = Hg_2$.
2. Associativity follows from that of G .
3. $eH = H$ is the identity in G/H .
4. Finally $g^{-1}H$ is the inverse of gH in G/H , since

$$(gH)(g^{-1}H) = (gg^{-1})H = H.$$

We also need to show that the operation combining two cosets to yield a new coset is well defined. Notice that

$$(gH, g'H) \mapsto gg'H$$

involves the choice of g and g' as representatives. Suppose that we take $g_1 \in gH$ and $g_2 \in g'H$, we need to show that

$$(g_1H, g_2H) \mapsto gg'H.$$

Since $g_1 \in gH$, then $g_1 = gh$ for some h , and similarly, since $g_2 \in g'H$, then $g_2 = g'h'$ for some h' in H , so that

$$g_1H = ghH = gH, \quad g_2H = g'h'H = g'H$$

and

$$(g_1H)(g_2H) = (gH)(g'H) = gg'H$$

as desired. □

The group G/H is called **quotient group**.

Quotient Group (I)

Let G be a group, with H a subgroup such that $gH=Hg$ for any g in G .
The set $G/H = \{gH, g \text{ in } G\}$ of cosets of H in G is called a **quotient group**.

We need to check that G/H is indeed a group!

Anything missing?

- Binary operation: $G/H \times G/H, (gH, g'H) \rightarrow gHg'H$ is **associative**
 - Since $gH=Hg, gHg'H=gg'H$ and G/H is **closed under binary operation**.
 - The **identity** element is $1H$ since $(1H)(gH)=(1g)H=gH$ for any g in G .
 - The **inverse** of gH is $g^{-1}H$: $(gH)(g^{-1}H)=(g^{-1}g)H=(g^{-1}g)H=H$.
-

Quotient Group (II)

- We need to check the binary operation **does not depend** on the choice of coset representatives.

$(gH, g'H) \rightarrow gHg'H = gg'H$ ← Involves choosing g and g' as respective coset representatives!!

Suppose we take g_1 in gH and g_2 in $g'H$, we need that $g_1g_2H = gg'H$.

g_1 in gH thus $g_1 = gh$ for some h , g_2 in $g'H$ thus $g_2 = g'h'$ for some h' .

Now $g_1H = (gh)H$ for some h , and $g_2H = (g'h')H$ for some h' .

Thus $g_1H g_2H = (gh)H (g'h')H = gHg'H = gg'H$ as desired.

The order of the quotient group G/H is given by Lagrange Theorem

$$|G/H| = |G|/|H|.$$

Example 34. Continuing Example 31, where $G = \{0, 1, 2, 3\}$ and $H = \{0, 2\}$, we have

$$|G/H| = 4/2 = 2$$

and G/H is isomorphic to C_2 .

Example 35. When $G = \mathbb{Z}$, and $H = n\mathbb{Z}$, we cannot use Lagrange since both orders are infinite, still $|G/H| = n$.

Example 36. Consider Dihedral group D_n . The subgroup $H = \langle r \rangle$ of rotations is normal since

1. if r' is any rotation, then $r'r = rr'$,
2. if m is any reflection $\in D_n$, $mr = r^{-1}m$ always.

Hence $rH = Hr$, $mH = Hm$ and $r^i m^j H = r^i H m^j = H r^i m^j$ for $j = 0, 1$ and $i = 0, \dots, n-1$.

Suppose now G is a cyclic group. Let H be a subgroup of G . We know that H is cyclic as well! Since G is cyclic, it is Abelian, and thus H is normal, showing that G/H is a group! What is this quotient group G/H ?

Proposition 10. *The quotient of a cyclic group G is cyclic.*

Proof. Let H be a subgroup of G . Let xH be an element of G/H . To show that G/H is cyclic, we need to show that $xH = (gH)^k$ for some k and gH . Since G is cyclic, $G = \langle g \rangle$ and $x = g^k$ for some k . Thus

$$xH = g^k H = (gH)^k.$$

□

Quotient Group (III)

Let G be a group, H a subgroup of G such that $gH=Hg$ and G/H the quotient group of H in G .

What is the order of G/H ?

By Lagrange Theorem, we have:

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

1st Example Again

$G = \{0,1,2,3\}$ integers modulo 4. $H = \{0,2\}$ is a subgroup of G .

G is abelian, thus $g+H = H+g$.

G/H is thus a group of order 2: $G/H = C_2$.

2nd Example Again

Consider the group G of integers \mathbb{Z} . Let $H = n\mathbb{Z}$ be the subgroup formed by multiple of n .

Since \mathbb{Z} is abelian, $g+H = H+g$ for every g in G .

G/H is thus a group of order n .

Here not from Lagrange since the order is infinite!

3rd Example: the Dihedral Group (I)

$$D_n = \{ \langle r, m \rangle \mid m^2 = 1, r^n = 1, mr = r^{-1}m \}$$

Let r' be a rotation.

- $rr' = r'r$ since the group of rotations is abelian.
- $mr' = (r')^{-1}m$

➡ $H = \langle r \rangle =$ group of rotations, then $rH = Hr$ and $mH = Hm$.

➡ $r^i m^j H = r^i H m^j = H r^i m^j$ for $j=0,1$ and $i=0, \dots, n-1$.

Quotient of Cyclic Groups (I)

- Let G be a cyclic group. Let H be a subgroup of G .
- We know that H is a cyclic group too.
- Since G is **abelian**, we have $gH = Hg$ for every g in G .
- Thus **G/H is a group!**

What is the quotient group of a cyclic subgroup in a cyclic group?

Quotient of Cyclic Groups (II)

Proposition. The quotient of a cyclic group G is cyclic.

Proof. Let H be a subgroup of G , and let xH be an element of G/H .

To show, G/H is cyclic, namely $xH = (gH)^k$ for some k and gH .

Since G is cyclic, we have $G = \langle g \rangle$ and $x = g^k$ for some k .

→ $xH = g^k H = (gH)^k$.

gH is thus the generator of G/H !

The notion of quotient is very important in abstract algebra, since it allows us to simplify a group structure to what is essential!

Example 37. The reals under addition $(\mathbb{R}, +)$, the subgroup $(\mathbb{Z}, +)$ of integers. We have $(\mathbb{Z}, +) \triangleleft (\mathbb{R}, +)$ because of the fact that $(\mathbb{R}, +)$ is abelian! Now


$$\mathbb{R}/\mathbb{Z} = \{r + \mathbb{Z} \mid r \in \mathbb{R}\}.$$

The cosets are $r + \mathbb{Z}$ with $r \in [0, 1)$. \mathbb{R}/\mathbb{Z} is isomorphic to the circle group S of complex numbers of absolute value 1. The isomorphism is $\phi[(r + \mathbb{Z})] = e^{i2\pi r}$.

Why do we care about Quotient Groups?

The notion of quotient allows to **identify** group elements that are “the same” with respect to some criterion, and thus to simplify the group structure to what is **essential**.

Example: Parity

Suppose we only care about the **parity** of an integer. For example, to compute $(-1)^k$, it is enough to know whether k is odd or even.  k modulo 2

Looking at k modulo 2 = to work in the quotient group $\mathbb{Z}/2\mathbb{Z}$.

In this quotient group, every **even number is identified to 0**, and **every odd number to 1**.

This identification is done via equivalence classes! Even numbers are an equivalence class, and so are odd numbers.

Recall Cosets

Recall We have $g_1H=g_2H$ if and only if $g_1^{-1}g_2$ is in H .

Generating the same coset is an **equivalence relation**!

- It is **reflexive**: $g^{-1}g=1$ is in H
- It is **symmetric**: if $g_1^{-1}g_2$ is in H , then $(g_1^{-1}g_2)^{-1}=g_2^{-1}g_1$ is in H .
- It is **transitive**: if $g_1^{-1}g_2$ in H and $g_2^{-1}g_3$, then $(g_1^{-1}g_2)(g_2^{-1}g_3)=g_1^{-1}g_3$ in H .



a coset = an equivalence class

group elements that are "the same"
with respect to some criterion

One more Example (I)

Take $G=(\mathbb{R}, +)$, it has $H=(\mathbb{Z}, +)$ as a subgroup. Since G is abelian, we have that $g+\mathbb{Z}=\mathbb{Z}+g$.

What is the quotient group G/H ?



$G/H = S^1$ (circle)

One more Example (II)

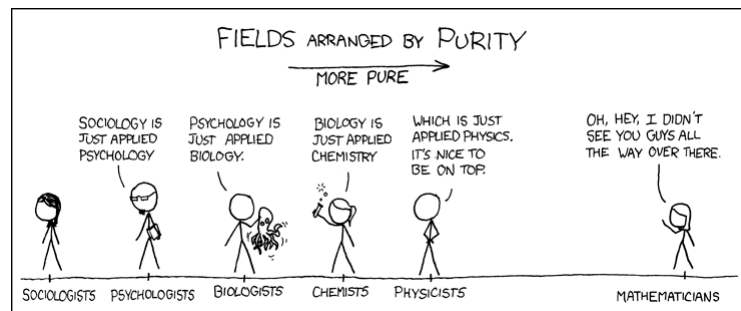
Let us show the isomorphism formally.

We define a map $f: \mathbb{R} / \mathbb{Z} \rightarrow S^1$.

$$r + \mathbb{Z} \rightarrow e^{2i\pi r}$$

- f is a group homomorphism:
 $f((r+\mathbb{Z})+(s+\mathbb{Z}))=f((r+s)+\mathbb{Z})=e^{2i\pi(r+s)} = e^{2i\pi r}e^{2i\pi s} = f(r+\mathbb{Z})f(s+\mathbb{Z})$
 - f is a bijection: it is clearly a surjection, and if $e^{2i\pi r} = e^{2i\pi s}$, then $r = s + \mathbb{Z}$ that is $r-s$ is in \mathbb{Z} , showing that $r+\mathbb{Z} = s+\mathbb{Z}$.
-

Pure Maths...



Exercises for Chapter 9

Exercise 43. Consider the Klein group $G = \{1, f, g, h\}$.

- What are all the possible subgroups of G ?
- Compute all the possible quotient groups of G .

Exercise 44. Consider the dihedral group D_4 . What are all the possible quotient groups of D_4 ?

Exercise 45. Consider A the set of affine maps of \mathbb{R} , that is

$$A = \{f : x \mapsto ax + b, a \in \mathbb{R}^*, b \in \mathbb{R}\}.$$

1. Show that A is a group with respect to the composition of maps.
2. Let

$$N = \{g : x \mapsto x + b, b \in \mathbb{R}\}.$$

Show that the set of cosets of N forms a group.

3. Show that the quotient group A/N is isomorphic to \mathbb{R}^* .