Quotient Groups and Fundamental Theorem of Homomorphisms

Kimsie Phan

Undergraduate of Mathematic at Kamarak University

phankimsie03@gmail.com

Mathematical Association of Cambodia

May 15th, 2021

Introduction

Definition (cosets)

Let G be a group, and H a subgroup of G.

1. The right coset of H in G defined by $Ha = \{ha | h \in H\}, \forall a \in G$.
2. The left coset of H in G defined by $aH = \{ah | h \in H\}, \forall a \in G$.
   Moreover, the set of left and right cosets are denoted respectively by

$$G/H = \{aH | a \in G\} \quad \text{and} \quad H\backslash G = \{Ha | a \in G\}.$$

How to make G/H or $H\backslash G$ a group?

Let G is group and $H \leq G$

And let $G/H = \{aH | a \in G\}$ (is a set)

We define an operation on G/H by coset multiplication:

$(G, *)$: $\quad (aH)(bH) := (ab)H$

$$\begin{aligned} G/H \times G/H &\longrightarrow G/H \\ (aH, bH) &\mapsto (ab)H \end{aligned}$$

Is this operation well-defined?

Answer: If $H \leq G$ then operation is not well-defined.

Via counterexample: if $G = S_3 = \{\epsilon, (12), (13), (23), (123), (132)\}$

And let $H \leq G$ such that $H = \{\epsilon, (12)\}$

We get $\quad (13)H = \{(13), (123)\} = (123)H$

$$(23)H = \{(23), (132)\} = (132)H$$

We get $\quad ((13)H, (23)H) = ((123)H, (132)H)$

Then $\quad ((13)H)((23)H) = [(13)(23)]H = (132)H$

But $\quad ((123)H)((132)H) = [(123)(132)]H = (\epsilon)H$

It means that one element in the domain assign two elements in the range.

So the above operation is not well-defined.

Is the operation on G/H satifies other conditions?

- Associative
  We have $[(aH)(bH)](cH) = [(ab)H](cH)$
  $$= (abc)H = (aH)(bc)H$$
  $$= (aH)[(bH)(cH)]$$
- The identity: $(eH = H)$
  We have $eH = \{eh | h \in H\} = \{h | h \in H\} = H$
  such that $(aH)(eH) = (ae)H = aH$
  $$(eH)(aH) = (ea)H = aH$$
- Inverse:
  $\forall aH \in G/H, \quad \exists a^{-1}H \in G/H$
  such that $(aH)(a^{-1}H) = (aa^{-1})H = eH = H$
  $$(a^{-1}H)(aH) = (a^{-1}a)H = eH = H$$

What condition on H that the operation on G/H defined above well-defined?

Definition (normal subgroups)

A subgroup H of a group G is called a normal subgroup of G if $aH = Ha$ for all $a \in G$. We denote this by $H \triangleleft G$.

Theorem

Let G be a group and $H \triangleleft G$. The set $G/H = \{aH | a \in G\}$ is a group under the operation

$$(aH)(bH) = (ab)H, \forall a, b \in G.$$

*G/H is called the **factor group**, or **quotient group** of G by H.*
Notice that :
$(a+H)(b+H) = (a+b)+H$, we define $(\times)$ on G/H if $(G,+)$.
$(a+H)+(b+H) = (a+b)+H$, we define $(+)$ on G/H if $(G,+)$.

Proof: It is enough to prove that the operation is well-defined.
If $H \triangleleft G$ then coset multiplication (Operation) is well-defined. How?

$$(aH, bH) \in G/H \times G/H$$
$$(cH, dH) \in G/H \times G/H$$

If $(aH, bH) = (cH, dH) \implies (ab)H = (cd)H$?

If $\begin{cases} aH = cH & \text{then} \quad a \in cH \\ bH = dH & \text{then} \quad b \in dH \end{cases}$

Then $\begin{cases} a = ch_1 \\ b = dh_2 \end{cases}$ for some $h_1, h_2 \in H$

Thus $(ab)H = (ch_1)(dh_2)H$
$= c(h_1 d)h_2 H, \quad$ since, $Hd = dH$
$= cdh_3 h_2 H$
$= (cd)H \quad$, since $\quad h_3 h_2 H \iff h_3 h_2 \in H$

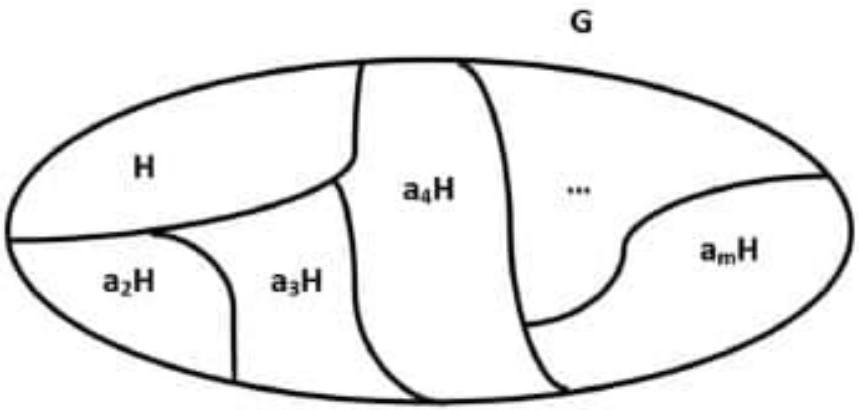
Therefore, $*$ on G/H is well-defined.

Example: From above counterexample $H \not\trianglelefteq S_3$ where $H = \{\epsilon, (12)\}$ because $(12)(123) \neq (123)(12)$ where $(123) \in S_3$.

Application of Quotient Groups

Review: The set of left or right cosets are define respectively by $G/H = \{aH | \forall a \in G\}$ and $H\backslash G = \{Ha | \forall a \in G\}$.
By the theorem of Larange's :

$$|G| = |G : H||H| = \left|G/H\right| |H|$$



Proposition

Let G be a group and $H \triangleleft G$. If G/H and H are finitely generated then G is finitely generated. (A group is said to be finitely generated if it is generated by a finite subset of its elements.)

Proof:
Let $G/H = \langle g_1H, g_2H, ..., g_mH \rangle$ and $H = \langle h_1, h_2, ..., h_n \rangle$ for some positive integer m, n.
Let $x \in G$ then $xH \in G/H = \langle g_1H, g_2H, ..., g_mH \rangle$

$$\implies xH = yH \quad \text{where} \quad y \in \langle g_1, g_2, ..., g_m \rangle$$

Then $y^{-1}x \in H = \langle h_1, h_2, ..., h_n \rangle$

$$\implies y^{-1}x = h, \quad h \in H$$

$$\implies x = yh \in \langle g_1, ..., g_m, h_1, ..., h_n \rangle.$$

Therefore, G is finitely generated.

Proposition

Let G be a group and let $Z(G)$ be the center of G. If $G/Z(G)$ is cyclic, then G is Abelian.

Proof:
Recall that $Z(G) = \{x \in G | xg = gx, \forall g \in G\}$
Let $g \in G$ then $gZ(G) \in G/Z(G) = \langle g_0 Z(G) \rangle$.
Then $\exists n \in \mathbb{Z}$ such that $gZ(G) = (g_0 Z(G))^n = g_0^n Z(G)$

$$\iff g_0^{-n} g = x, \quad x \in Z(G)$$

$$\implies g = g_0^n x$$

Thus, $\forall g_1, g_2 \in G, \exists m, n \in \mathbb{Z}$ such that $g_1 = g_0^m x, g_2 = g_0^n y$ for some $x, y \in Z(G)$.
Then $g_1 g_2 = (g_0^m x)(g_0^n y) = g_0^m g_0^n xy = g_0^m g_0^n yx = g_2 g_1$.
Therefore, G is Abelian.

Proposition

If every element of G/H has a square root, and every element of H has a square root, then every element of G has a square root. (Assume G is abelian.)

Proposition

Let p be a prime number. If G/H and H are p-groups, then G is a p-groups. A group G is called a $p-group$ if the order of every element x in G is a power of p.

Fundamental Theorem of Homomorphisms

Definition

Let G, G' be groups. A map $f : G \longrightarrow G'$ is said to be an **homomorphism** if it preserve the group operator; that is, $f(ab) = f(a)f(b)$ for all $a, b \in G$. In addition, if:

- f is one-one then f is called **monomorphsim**.
- f is onto then f is called **epimorphism**.
- f is bijective then f is called **isomorphism**.
- f is bijective and $G = G'$ then f is called **automorphism**.

Definition

Let $f : G \longrightarrow G'$ be a group homomorphism. Then the sets:

- $\ker(f) = \{x \in G | f(x) = e_{G'}\} \subset G$ is called **the kernel** of homomorphism f.
- $\mathrm{Im}(f) = \{f(x) | x \in G\} \subset G'$ is called **the image** of G in G' via homomorphism f.

Proposition

Let f be a group homomorphism from G to G'. Then
1. $\mathrm{Im}(f) \leq G'$.
2. $\ker(f) \triangleleft G$.

Proof:
1. Let $f(g_1), f(g_2) \in \mathrm{Im}(f)$, such that $g_1, g_2 \in G$.

We have $f(g_1)f(g_2) = f(g_1g_2) \in \mathrm{Im}(f)$.

And $[f(g_1)]^{-1} = f(g_1^{-1}) \in \mathrm{Im}(f)$.

Thus, $\mathrm{Im}(f) \leq G'$.

2. Let $x, y \in \ker(f)$ then $f(x) = e$ and $f(y) = e$
We have $f(xy^{-1}) = f(x)f(y^{-1})$

$$= e[f(y)]^{-1}$$
$$= ee^{-1}$$
$$= e$$

So, $xy^{-1} \in \ker(f)$ then $\ker(f) \leq G$.
From definition of normal subgroups is $aH = Ha, \forall a \in G$.
Observation that $aH = Ha \iff aHa^{-1} = H$

$$\iff \forall a \in G, \forall h \in H, aha^{-1} \in H.$$

If $a \in \ker(f)$ and $x \in G$
Then $f(xax^{-1}) = f(x)f(a)f(x^{-1})$

$$= f(x)f(a)[f(x)]^{-1}$$
$$= f(x)[f(x)]^{-1}, \quad \text{since } f(a) = e$$
$$= e$$

So, $xax^{-1} \in \ker(f)$ then $\ker(f) \triangleleft G$.

Theorem (Fundamental Theorem of Homomorphisms)

Let f be a group homomorphism from G to G'. Then the mapping from $G/\ker(f)$ to G', given by $g\ker(f) \mapsto \mathrm{Im}(f)$, is an isomorphism. In symbols, $G/\ker(f) \cong \mathrm{Im}(f)$.

Proof: Consider the map $f' : G/\ker f \longrightarrow \mathrm{Im} f$

defined by $f'(g\ker f) = f(g), \quad g \in G.$

Now f' is well-defined and injective since

$$a\ker f = b\ker f \iff b^{-1}a \in \ker f \iff f(b^{-1}a) = e \iff f(a) = f(b).$$

And f' is surjective: since

$$f'\left(G/\ker f\right) = \{f'(g\ker f) | g \in G\} = \{f(g) | g \in G\} = \mathrm{Im} f.$$

Moreover f' is homomorphism:

$$\begin{aligned} f'[(a\ker f)(b\ker f)] &= f'(ab\ker f) \\ &= f(ab) = f(a)f(b) \\ &= f'(a\ker f)f'(b\ker f). \end{aligned}$$

Application of Fundamental Theorem of Homomorphisms

Proposition

Let $f : \mathbb{Z} \longrightarrow \mathbb{Z}_n$. For each $n \in \mathbb{N}$ then $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$.

Note: $n\mathbb{Z} \triangleleft \mathbb{Z}$ and so $\mathbb{Z}/n\mathbb{Z} = \{m + n\mathbb{Z} | m \in \mathbb{Z}\}$.
Proof: We have $f : \mathbb{Z} \longrightarrow \mathbb{Z}_n$ given by $f(m) = m(\mod n)$.
Observe that f is a homomorphism from $\mathbb{Z}$ to $\mathbb{Z}_n$.
And f is clearly surjective.
Consider $\ker(f) = \{m \in \mathbb{Z} : m(\mod n) = 0\}$

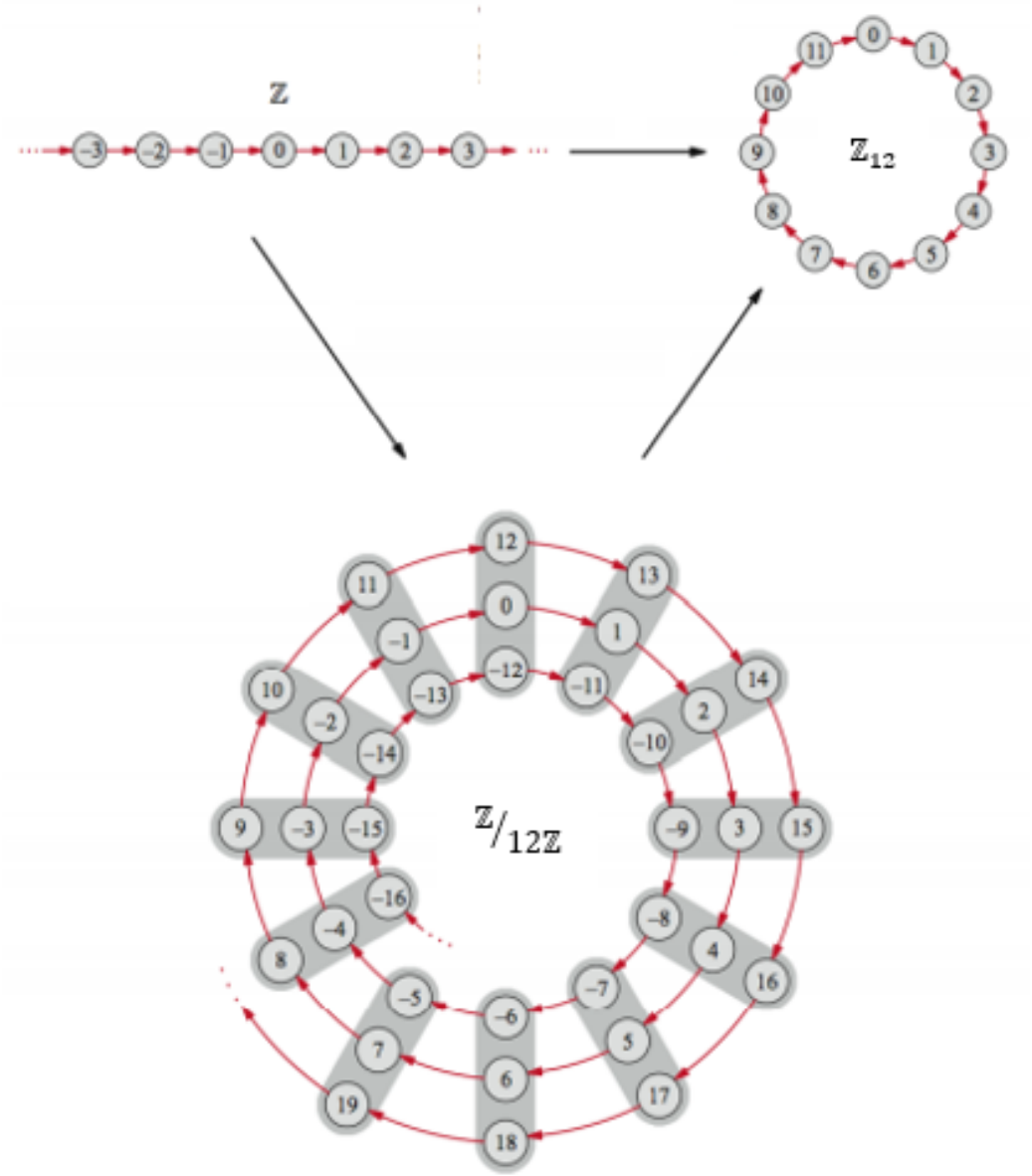
$$= \{m \in \mathbb{Z} : m = kn, k \in \mathbb{Z}\}$$
$$= n\mathbb{Z} = \langle n \rangle.$$

By Fundamental Theorem of Homomorphisms, we have that:

$$\mathbb{Z}/\ker(f) = \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/\langle n \rangle \cong \mathrm{Im}(f) = \mathbb{Z}_n.$$

Therefore, $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$.

A picture of the isomorphism $f : \mathbb{Z}/12\mathbb{Z} \longrightarrow \mathbb{Z}_{12}$:

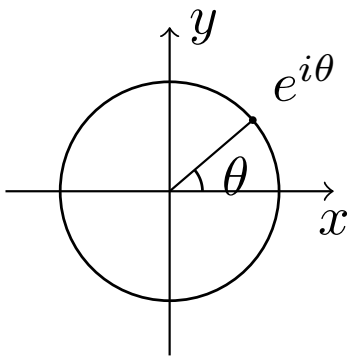


Proposition

Let $(\mathbb{R}, +)$ and $(\mathbb{Z}, +)$ be the additive group. And let $\mathbb{T} = \{z \in \mathbb{C} : |z| = 1\}$ be the circle group. Prove that $\mathbb{R}/\mathbb{Z} \cong \mathbb{T}$.

Review: $(\mathbb{R}, +), (\mathbb{Z}, +)$ are abelian group. Then $\mathbb{Z} \triangleleft \mathbb{R}$ and $\mathbb{R}/\mathbb{Z} = \{x + \mathbb{Z} | x \in \mathbb{R}\}$.

The circle group, denoted by $\mathbb{T}$, is the multiplicative group of all complex numbers with absolute value 1, that is, the unit circle in the complex plane or simply the unit complex numbers.



$$\mathbb{T} = \{z \in \mathbb{C} : |z| = 1\} = \{e^{i2\pi x} | x \in \mathbb{R}\}.$$

Proof: $\mathbb{R}/\mathbb{Z} \cong \mathbb{T}$. Let a map $f : \mathbb{R} \longrightarrow \mathbb{T}$ given by $f(x) = e^{2\pi i x}$. Note that f is well-define since, $a, b \in \mathbb{R}$

$$a = b \Longleftrightarrow 2\pi i a = 2\pi i b \Longrightarrow e^{2\pi i a} = e^{2\pi i b} \Longleftrightarrow f(a) = f(b).$$

Now f is homomorphism because, let $a, b \in \mathbb{R}$ then

$$f(a+b) = e^{2\pi i(a+b)} = e^{2\pi ia} \cdot e^{2\pi ib} = f(a) \cdot f(b)$$

And f is surjective since $\forall y \in \mathbb{T}, \exists x \in \mathbb{R}$ such that $y = e^{i2\pi x}$
$\implies f(x) = e^{i2\pi x} = y$.
Moreover, $\ker(f) = \{x \in \mathbb{R} : e^{i2\pi x} = 1\}$

$$= \{n : n \in \mathbb{Z}\}.$$

Then $\ker(f) = \mathbb{Z}$. By Fundamental Theorem of Homomorphisms :

$$\mathbb{R}/\ker(f) \cong \mathbb{T}.$$

Therefore $\mathbb{R}/\mathbb{Z} \cong \mathbb{T}$.

References

1. **Charles C. Pinter**, *A Book of Abstract Algebra*. Second Edition, McGraw-Hill Publishing Company, Inc., New York, 1982.
2. **Joseph A. Gallian**, *Contemporary Abstract Algebra*. Eight Edition, CENGAGE Learning, United State of America, 2017.
3. **M.Machauley (Clemson)**, *Homomorphisms*, Math 4120, Spring 2014.
4. **Mathematics Stack Exchange**, *Proof the first isomorphism theorem*, 2013.
5. **Edmund F Robertson**, *The first isomorphism theorem*, 11 September 2006.
6. **Proofwiki**, *Quotient Group of Reals by Integers is Circle Group*, 13 December 2019.

THANK YOU FOR YOUR PAYING ATTENTION !

It is tribute to the genius of Galois that he recognized that those subgroups for which the left and right cosets coincide are distinguished ones. Very often in mathematics the crucial problem is to recognize and to discover what are the relevant concepts; once this is accomplished the job may be more than half done.

I.N. HERSTEIN, *Topics in Algebra*

Moreover, I would like to thank my two advisors Seng Monyrathanak and Deom Vanny for providing me guidance and feedback throughout this project work.

Last but not least, I also would like to thank all MAC members who has discussed with me during this project work period.

Q & A !