LECTURE NOTES ON GROUP THEORY

SHIYUE LI
MATHCAMP 2019

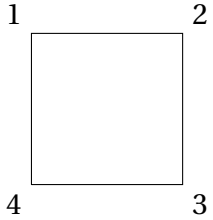
ABSTRACT. This document serves as the class notes for Group Theory class taught by Shiyue Li in Week 1 of Canada/USA Mathcamp 2019. They are based on Mira's notes from Mathcamp 2018, improved and completed via conversations with Mira, Jeff, campers, and many other Mathcamp staff.

CONTENTS

1. DAY 1

1.1. **Symmetries, groups, and examples.** A group is a set...with some extra structures.

Example 1.1. Consider a square sitting on a plane. We consider the set of operations composed out of the rotation that rotates the square by 90 degrees clockwise, denoted by r, and the flip along the "northwest-southeast" diagonal.



(a) Denote the rotation as r and the flip as f. Is the set of all operations composed out of r and f a group with some appropriate operation? This is called the set of symmetries (i.e. transformations that preserve the square in the space) of a square, denoted by Sym($\square$), denoted as D_4.

In general, the symmetry group of an n-gon is denoted as D_n, called **dihedral group**.

(b) What is the size of the symmetry group D_4?

(c) Write the elements of D_4 as compositions of r and f.

Example 1.2. Consider 3 points numbered as $1,2,3$ on the plane and the operations of permuting the 3 points.

(a) Write down the elements of S_3 as bijective maps from [3] to [3].

(c) In general, we call the set of all permutations of an n-set the symmetric group S_n. Prove that

$$|S_n| = n!.$$

(d) We can see that D_4 is a subset of S_4 under the same group operation.

Observation 1.3. From the examples we have, we can see the followings.

(a) Given any two transformations, the composition of the two is always a legitimate transformation that preserves the underlying shape.

(b) There is always the "do nothing" operation.

(c) Any transformation has a corresponding "undo" transformation that it composes to go back to "do nothing".

(d) If you do transformation A, then do B and C altogether, that would be the same as doing A and B altogether, and then do C. (Consider the example of $f(rr)$ and $(fr)r$ in D_4.)

Definition 1.4. A **group** $(G,*)$ is a set G with a binary operation $*$ that satisfies the following axioms:

(a) For any $x, y \in G$, $x * y \in G$. ("Closed under the binary operation")

(b) The set G has an **identity element** denoted as e_G such that $x * e_G = e_G * x = x$.

(c) For any $x \in G$, there exists an element y such that $x * y = e_G$; we call y the **inverse** of x. ("Inverses exist")

(d) For any $x, y, z \in G$,

$$(x * y) * z = x * (y * z).$$

(Associativity)

Proposition 1.5 (Uniqueness of the identity)**.** *Let $(G,+)$ be a group. Then the identity element is unique.*

Proof. Let e, e' be two elements such that $x + e = e + x = x$ and $x + e' = e' + x = x$ for all x. In particular, $e = e + e' = e'$. Thus the identity is unique. □

Proposition 1.6 (Uniqueness of inverses)**.** *Let G be a group. Let x be an element in G. Then the inverse of x is unique.*

Example 1.7. Consider the integers $\mathbb{Z}$ with addition as its operation. Prove that $(\mathbb{Z},+)$ is a group.

Example 1.8. Consider the set

$$5\mathbb{Z} := \{5x : x \in \mathbb{Z}\} = \{0,5,-5,10,-10,\ldots\}$$

with the usual addition on $\mathbb{Z}$. Prove that $(5\mathbb{Z},+)$ is a group.

In general, for any integer n, $(n\mathbb{Z},+)$ is a group.

Example 1.9. Consider the set $\{0,1,2,3\}$ under the usual addition with the rule that $x+y := x+y \mod 4$ for all $x,y \in \{0,1,2,3\}$.

- Is this a group?
- If so, with what identity and inverses?

This is denoted as $\mathbb{Z}_4$ (reads "$\mathbb{Z}$ four") or $\mathbb{Z}/4\mathbb{Z}$ (reads "$\mathbb{Z}$ mod four $\mathbb{Z}$").

Let us construct the **Cayley Table** for $\mathbb{Z}/4\mathbb{Z}$.

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

In general, the set

$$\mathbb{Z}/n\mathbb{Z} \text{ or } \mathbb{Z}_n := \{0,1,\ldots,n-1\}$$

is a group under addition with the rule that $x+y := x+y \mod n$.

Example 1.10. Consider $\mathbb{Z}_4$. It is important when talking about a group to talk about its operations.

(a) Is $\mathbb{Z}_4$ under multiplication under the rule that $x\,y = x\,y \mod 4$ a group?
(b) How about $\mathbb{Z}_4 \setminus \{0\}$?
(c) How would you modify $\mathbb{Z}_4$ to make a group under multiplication? Call the resultant group $\mathbb{Z}_4^*$
(d) What is the size of $\mathbb{Z}_4^*$ (*Hint:* You might need Bézout's Lemma from Number Theory)?

Example 1.11. Are all groups commutative? Performing $r\,f$ and $f\,r$ on a square does not give us the same symmetry of the square.

Mathcamp's alma mater-performed every year in the talent show by the Contrapositones, our camp choir-was penned by Chris & Meep in the summer of 2000, and is sung to the tune of Cecilia by Simon and Garfunkel (See the Youtube video performed by Contrapositones at Mathcamp 2012, `https://youtu.be/pKNVdiP6WYY`):

```
Nonabelian, you're breaking my heart
You're wreckin' my multiplication
Nonabelian, I'm down on my knees
I'm beggin' you please, please commute
Please commute
```

```
Thinking groups in the afternoon, nonabelian
Up in my classroom (thinking groups!)
There are things that just can't be done
When a b a inverse b inverse is not one

Nonabelian, you're breaking my heart
You're wreckin' my multiplication
Nonabelian, I'm down on my knees
I'm beggin' you please, please commute
Please commute

Jubilation, it commutes again,
divide out by all commutators
Jubilation, it commutes again,
Divide out by all commutators

Oh oh oh oh....
```

Definition 1.12. A group G is abelian if $x * y = y * x$ for all $x, y \in G$.

Definition 1.13. Let G be a group and $x \in G$. The minimal integer n such that $x^n = e_G$ is **order** of x.

1.2. **Exercises for Day 1.**

Exercise 1.14. Let us focus on the dihedral group D_4 and generalize to other groups.

(a) What are the elements of D_4, in terms of r, f, where r denotes rotation clockwise 90 degrees, and f denotes flipping along the northwest-southeast diagonal?
(b) Read the notes for **Cayley Table** for $(\mathbb{Z}_4, +)$. Complete the **Cayley Table** for D_4.
(c) What can you say about entries in the same row or the same column? (*Hint:* how many times does each element appear in one row?)
(d) **Cancellation Property.** Let G be a group and $a, b, c \in G$. Prove that

$$ab = ac \implies b = c,$$

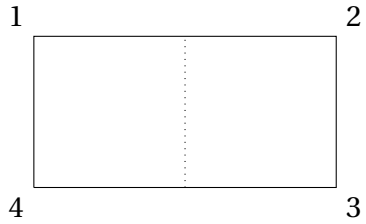
and that

$$ba = ca \implies b = c.$$

Exercise 1.15. Let G be a group. Denote the inverse of $x \in G$ as x^{-1}.

(a) Prove that the identity of a group and inverse of an element $x \in G$ is unique. (*Hint*: you might need to use use Cancellation Properties)
(b) Prove that $e^{-1} = e$ and $(x^{-1})^{-1} = x$.
(c) Prove that $(x^{-1})^k = (x^k)^{-1}$.
(d) How else could you write $(ab)^{-1}$? Prove it. (*Hint:* Say you have your socks and shoes on. What do you have to do to get back to barefoot?)

Exercise 1.16. Consider the symmetry set of a rectangle.



Denote the clockwise rotation by 180 degrees as r and the vertical flip along the dotted line as f.

(a) What is the symmetry set of the rectangle in terms of r and f?
(b) Show that the symmetry set of a rectangle is a group.
(c) List out all its element in terms of r, f.

This group is called the **Klein n-group**, denoted by V_n, where n is the size of the group you derived from part (c) above.

Exercise 1.17. Recall that the dihedral group D_4 that captures the symmetry of a square.

(a) What are the subgroups of order 2 of D_4? (Hint: there are five of them.)
(b) What are the subgroups of size 4 in D_4? Do they have the same structure as some other groups we already know?

Exercise 1.18. Find a geometric object whose symmetry group is $\mathbb{Z}_4$.

Exercise 1.19. We gave a seemingly different definition of **abelian groups** from the one in Mathcamp's alma mater. Prove that G is abelian if and only if $xyx^{-1}y^{-1} = e_G$, where x^{-1} and y^{-1} are the inverses of x and y respectively.

2. Day 2

2.1. **Subgroups, Cyclic Groups, Lagrange's Theorem.** Recall definition of group. Recall the definition of order of a group element and order (size) of a group.

Definition 2.1. Let G be a group. Suppose x is an element of G. Then the minimum positive integer n such that $x^n = e_G$ is the **order** of x in G, denoted as $\text{ord}(x)$. If no such integer exists for x, the order of x is said to be ∞.

Definition 2.2. The order of a group G is the size of the set G, denoted as $|G|$.

Recall the following examples.

(a) The symmetry group of a square D_4 is a subset of S_4, both equipped with composition as group operation.
(b) The symmetry group of a rectangle is Klein Four group, V, and is a subset of D_4 with the same group operation.
(c) Despite both having size 4, V and $\mathbb{Z}_4$ have sort of different structures.

Definition 2.3. Given a group G, a subgroup of G is a subset H of G that is also a group, with the same group operation as G. The group containment relation is denoted by $H \leq G$.

Example 2.4. (a) D_4 is a subgroup of S_4.
(b) The group $\{e, rf, fr, rr\}$, which has the same structure as V, is a subgroup of D_4.

(c) The group $\{e, r, r^2, r^3\}$, which "has the same structure" as $\mathbb{Z}_4$, is a subgroup of D_4.

Non-Example 2.5. The set of integers $\mathbb{Z}$ under addition does not contain $\mathbb{Z}_4$ as its subgroup. Why?

In (c) of our recollection, we said that $\mathbb{Z}_4$ and V has different structures, by analyzing the orders of their elements. On the other hand, we could see this by analizing the composition of the elements of $\mathbb{Z}_4$ and V. We have written $\mathbb{Z}_4$ as a subgroup of D_4 by identifying 1 as rotating clockwise by 90 degrees, r. Hence

$$\mathbb{Z}_4 = \{e, r, r^2, r^3\} \neq V_4 = \{e, rf, fr, rr\}.$$

Definition 2.6. Let G be a group. If there exists an element $g \in G$ such that for any nontrivial element $x \in G$ (i.e. $x \neq e_G$),

$$x = \underbrace{g * \cdots * g}_{g \text{ appears } n \text{ times}} = g^n \text{ or } x = \underbrace{g^{-1} * \cdots * g^{-1}}_{g^{-1} \text{ appears } n \text{ times}} = (g^{-1})^n = (g^n)^{-1}$$

for some $n \in \mathbb{Z}_{>0}$, then we say that G is cyclic, or generated (under group axioms) by one generator g. We write $G = \langle g \rangle$.

Example 2.7. (a) The integers $\mathbb{Z} = \langle 1 \rangle$ is a cyclic group.
(b) The group $\mathbb{Z}_4 = \langle 1 \rangle$ is a cyclic group.
(c) V is not cyclic; D_4 is not cyclic.

Proposition 2.8. *Let G be a group. If G is cyclic, then G is abelian.*

Proof. Let G be a cyclic group. By definition, $G = \langle g \rangle$ for some $g \in G$. Then for any $x, y \in G$, there exist integers n, m such that

$$x = g^n \text{ and } y = g^m,$$

where if n (or m) is negative, we think of g^n (or g^m) as $\underbrace{g^{-1} * \cdots * g^{-1}}_{n \text{ times}}$. Therefore,

$$\begin{aligned} x * y &= \underbrace{g * \cdots * g}_{n \text{ times}} * \underbrace{g * \cdots * g}_{m \text{ times}} \\ &= \underbrace{g * \cdots * g}_{n+m \text{ times}} (\text{ by Associativity}) \\ &= \underbrace{g * \cdots * g}_{m \text{ times}} * \underbrace{g * \cdots * g}_{n \text{ times}} \\ &= y * x. \end{aligned}$$

□

Proposition 2.9. *Let G be a group. Given an element $g \in G$, then the set*

$$H = \{e_G, g, g^{-1}, g^2, g^{-2}, \ldots\}$$

with the same group operation is a subgroup of G.

Example 2.10. Consider the group $(\mathbb{Z},+)$ and the subgroup generated by 4; that is,

$$4\mathbb{Z} := \{0,4,-4,8,-8,\ldots\}.$$

This is a subgroup of $\mathbb{Z}$. In general, for any integer n, $(n\mathbb{Z},+)$ is a subgroup of $(\mathbb{Z},+)$.

Proposition 2.11. *Any subgroup of* $(\mathbb{Z},+)$ *is of the form* $n\mathbb{Z}$ *for some integer* n.

Theorem 2.12 (Lagrange)**.** *Let* G *be a finite group and* $H \leq G$*. Then* $|H|$ *divides* G*.*

To prove Lagrange's Theorem, we need the definition of cosets.

Example 2.13. We define that

$$\overline{0} = \{0,4,-4,8,-8,\ldots\}$$
$$\overline{1} = \{1,5,-3,9,-7,\ldots\}$$
$$\overline{2} = \{2,6,-2,10,-6,\ldots\}$$
$$\overline{3} = \{3,7,-1,11,-5,\ldots\}$$

Consider the set

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

with the group operation $+^4$ that

$$\overline{x} +^4 \overline{y} := \overline{x+y \mod 4}.$$

We can check that $(\{\overline{0},\overline{1},\overline{2},\overline{3}\},+^4)$ is a group.

We have the following observations.

(a) All the sets $\overline{0},\overline{1},\overline{2},\overline{3}$ have the same size; we have partitioned $\mathbb{Z}$ into equally sized sets.
(b) If the group that we are partitioning has finite size, then size of each "bucket" is $|H|$, and it will devide $|G|$, since the number of buckets is an integer.

2.2. **Exercises for Day 2.** This problem set contains lots of formal proof writing. You are encouraged to talk to Shiyue, other staff or your peers to make sure if your proofs are well-written and logically sound.

Exercise 2.14. Prove that any subgroup of $(\mathbb{Z},+)$ is of the form $n\mathbb{Z}$ for some integer n.

Exercise 2.15. Let G be a group and let $g \in G$. Let $\mathrm{ord}(g)$ denote the order of g and let $|H|$ denote the size of a subgroup H.

(a) Show that the cyclic group generated $\langle g\rangle$ by g is a subgroup of G.
(b) Show that $\mathrm{ord}(g) = |\langle g\rangle|$.
(c) Show that $g^k = e_G$ if and only if $\mathrm{ord}(g)|k$. (*Hint:* One direction is easy; for the other direction, use integer division.)
(d) Use Lagrange's Theorem and the previous part, show that $g^{|G|} = e_G$.
(e) Let $G = \mathbb{Z}_n^*$ (See Notes on Day 1), what theorem from number theory is the previous statement equivalent to?

Exercise 2.16. Let G be a group. Prove that if $|G|$ is prime, then G is cyclic. (*Hint:* Use Lagrange's Theorem.)

Exercise 2.17. Prove that every group of size 4 has the same structure either with $\mathbb{Z}_4$ or with V. (*Hint:* We have seen in class that "showing that two things have the same structure" amounts to proving that they are really the same thing up to relabeling of elements. Use Lagrange's Theorem.).

Exercise 2.18. Revisit Day 1's Exercises and understand D_4:

(a) (Revisit) What are the subgroups of size 2 in D_4? (*Hint:* there are 5 of them.)
(b) (Revisit) What are the subgroups of size 4 in D_4?
(c) Use Lagrange's Theorem and casework, show that these subgroups, plus $\{e_{D_4}\}$ and D_4, are the only subgroups of D_4.

3. Day 3

3.1. Cosets, Normal Subgroups, and Quotient Groups.

Definition 3.1 (Cosets of subgroups)**.** Let G be a group, H be a subgroup of G and $g \in G$. A **left coset** of H with respect to g is defined to be

$$gH := g * H := \{g * h : h \in H\}.$$

A **right coset** of H with respect to g is defined to be

$$Hg := H * g := \{h * g : h \in H\}.$$

Example 3.2. In our example, we considered $G = \mathbb{Z}$, $H = 4\mathbb{Z}$, and the following cosets

$$\overline{0} = 0 + 4\mathbb{Z} = \{0, 4, -4, 8, -8, \ldots\}$$
$$\overline{1} = 1 + 4\mathbb{Z} = \{1, 5, -3, 9, -7, \ldots\}$$
$$\overline{2} = 2 + 4\mathbb{Z}\{2, 6, -2, 10, -6, \ldots\}$$
$$\overline{3} = 3 + 4\mathbb{Z} = \{3, 7, -1, 11, -5, \ldots\}$$

Are there more cosets if we consider cosets of H with respect to elements of $\mathbb{Z}$ other than $0, 1, 2, 3$? Consider

$$\overline{17} = 17 + 4\mathbb{Z} = \{17 + 4n : n \in \mathbb{Z}\} = \{1, 5, -3, \ldots\}.$$

Therefore, after putting the numbers to the "buckets" or "cosets", we don't see the difference between $1, 17, -3$ and 29781. The only thing we see is that they are all $1 \mod 4$. They are **congruent** $\mod 4$ or **equivalent** $\mod 4$.

Definition 3.3. The set of left cosets of H in G is denoted as G/H.

Proof of Lagrange's Theorem. Let G be a finite group; that is $|G| < \infty$. Let H be a subgroup of G. Then $|H|$ is finite.

Consider the set of cosets G/H of H in G. We claim that all the cosets have the same size. Indeed, given any two cosets aH and bH for $a, b \in G$, define a map $f : aH \to bH$ by

$$f(ah) = ba^{-1}(ah) = bh \in bH.$$

We check that this map is well-defined and bijective.

(a) *Well-defined:* Let $ah = ah'$, then by Cancellation Property, $h = h'$. Hence $f(ah) = bh = bh' = f(ah')$.

(b) *Bijective:* Define a map $g : bH \to aH$ by

$$g(bh) = ab^{-1}(bh) = ah.$$

Check that for any $h \in H$,

$$(f \circ g)(bh) = f(ah) = bh,$$
$$(g \circ f)(ah) = g(bh) = ah.$$

Hence f, g are inverses of each other, and both are bijective.

Therefore, all cosets of H in G have the same size.

Since all cosets of H has the same size, and the coset eH has the same size as H, all cosets of H has the size of H.

Since there are finitely many cosets (othewise, G is infinite), and

$$|H| \cdot |G/H| = |G|,$$

$|H|$ divides G. □

Proposition 3.4 (A Wrong Proposition)**.** *Let G be a group and H be a subgroup. The set of left cosets G/H is a group.*

Fake Proof of the Wrong Proposition. Let $(G, *)$ be a group and H be a subgroup. Consider the set of left cosets G/H of H in G. To see that the set G/H is a group, we define a group operation $\diamond$ and show that $(G/H, \diamond)$ satisfies the group axioms.

The binary operation $\diamond$ on G/H is defined as follows. For any $aH, bH \in G/H$,

$$aH \diamond bH := (a * b)H.$$

We now check the group axioms.

(a) For any $aH, bH \in G/H$,

$$aH \diamond bH = (a * b)H \in G/H$$

since $a * b \in G$.

(b) The coset eH is the identity of G/H. For any $aH \in G/H$, $aH \diamond eH = eH \diamond aH = (a * e)H = aH$.

(c) For any $aH \in G/H$, there exists $a^{-1}H$ such that

$$aH \diamond a^{-1}H = eH.$$

(d) Associtivity follows from associativity of G.

□

Non-Example 3.5. Let $G = D_4$ and $H = \{e, f\}$. We claim that G/H is not a group under $\diamond$.

The set G/H of left cosets consists of the followings.

$$eH = fH = \{e, f\}$$
$$rH = rfH = \{r, rf\}$$
$$r^2H = r^2fH = \{r^2, r^2f\}$$
$$r^3H = r^3fH = \{r^3, r^3f\}.$$

Notice that $rH = rfH$, and if $\diamond$ were well-defined, multiplying rH and rfH with the same element, say rH should yield the same result. However,

$$rH \diamond rH = r^2H \neq fH = (rf)H \diamond rH.$$

Question 3.6. What is the desired property that we want?

3.2. **Exercises for Day 3.** In today's exercises, we will practice writing formal proofs while understanding cosets, equivalence relations, normal subgroups of examples we have seen, and direct product of groups. Finally, we will get to understand the last verse in Mathcamp's alma mater *Nonabelian*!

Exercise 3.7. Let G be a group and H be a subgroup of G. Consider the set of left cosets of H.

(a) Show that any two cosets $aH = bH$ if and only if $b \in aH$.
(b) Show that given any two cosets aH, bH, either $aH = bH$ or $aH \cap bH = \varnothing$.

Exercise 3.8. Given a set S, an **equivalence relation** $\sim$ is a binary relation on S such that

- *Reflexive:* $a \sim a$ for all $a \in S$;
- *Symmetric:* if $a \sim b$, then $b \sim a$ for all $a, b \in S$;
- *Transitivie:* if $a \sim b$ and $b \sim c$, then $a \sim c$ for all $a, b, c \in S$.

In **partition** of S is a set of nonempty subsets of S such that each $x \in S$ is in exactly one of the subsets.

(a) Prove that S has an equivalence relation if and only if there is a partition of S.
(b) Using part (a) and previous exercise, show that cosets define an equivalence relation on the group G.

Exercise 3.9. At the end of class, we have seen that the set of left cosets of $H = \{e, f\}$ in $G = D_4$ is not a group under $\diamond$ operation. Because the operation $\diamond$ is not **well-defined** on G/H. This exercise leads you to the desired property of H for G/H to be a group.

(a) Let G be a group, and $H \leq G$. Consider any two cosets aH and bH, and the $\diamond$ operation that
$$aH \diamond bH := (a * b)H = (ab)H.$$
Suppose we have $ah \in aH$ and bh' in bH, we would want $(ah) * (bh') = ahbh'$ to land in $(ab)H$. How would you formulate the desired property of H? (*Hint:* what if hb can be written as bh'' for some $h'' \in H$?)
(b) If $aH = Ha$ for all $a \in G$ (i.e. for any $ah \in aH$, there exists h' such that $ah = h'a$), then H is a **normal subgroup** of G, denoted as $H \trianglelefteq G$.
Suppose $H \trianglelefteq G$. Prove that $(G/H, \diamond)$ is a group. (*Hint:* we have done the harder part of the work in class. Now you only need to show that $\diamond$ operation is well-defined on G/H.)

Exercise 3.10. Consider $(\mathbb{Z}, +)$. Prove that $4\mathbb{Z}$ is normal. Conclude that $\mathbb{Z}/4\mathbb{Z}$ is a group and write down the group elements.

Exercise 3.11. Consider the Klein 4-Group V.

(a) Prove that subgroup $H = \{e, v\}$, where v is flipping the rectangle along the vertical axis, is normal.

(b) Which familiar group can V/H be identified with?

Exercise 3.12. Consider D_4.

(a) Prove that the subgroup $R_4 = \{e, r, r^2, r^3\}$ is normal in D_4.
(b) What familiar group can D_4/R_4 be identified with?

Exercise 3.13. Let G be an abelian group. Show that any subgroup of G is normal.

Exercise 3.14. Let $(G, *)$ and $(H, \star)$ be two groups. Then we define the **direct product** of G and H to be the set

$$G \times H = \{(g, h) : g \in G, h \in H\}$$

with the group operation $\diamond$ defined as follows: for any $(a, b), (c, d) \in G \times H$,

$$(a, b) \diamond (c, d) := (a * c, b \star d).$$

(a) Prove that $(G \times H, \diamond)$ is a group.
(b) Prove that if G and H are abelian, then $G \times H$ is abelian.
(b) Realize that $V = \mathbb{Z}_2 \times \mathbb{Z}_2$.
(d) Is $\mathbb{Z}$ identified with $\mathbb{Z}_4 \times 4\mathbb{Z}$?

Exercise 3.15. We are now ready to understand the final verse of *Nonabelian:*

```
Jubilation, it commutes again,
Divide out by all commutators!
```

Let G be a group. Let $S = \{aba^{-1}b^{-1} : a, b \in G\}$. The **commutator subgroup** G' of G is the subgroup generated by all the element of S; in other words, G' consists of all the elements of S and all possible products of such elements and their inverses. This automatically makes G' into a group.

(a) Show that if G is abelian then G' is trivial (i.e. $G' = \{e\}$).
(b) Show that G' is normal in G.
(c) Show that G/G' is abelian. This kind of make sense intuitively: you're "getting rid" of all the things that prevent G from being abelian, by putting them all into the identity coset. In other words, G "commutes again" (I'm not sure why "again") when you "divide out by all commutators"! The group G/G' is called the *abelianization of* G, denoted G_{ab}.
(i) Let $G = D_4$. Find G' and figure out the isomorphism class of G/G'.
(ii) Show that if H is normal in G and G/H is abelian then $G' \subseteq H$. In other words, the only way to "make" G into an abelian group is to mod out by G'. You can mod out by more (a bigger group H), but G' is the minimum required to get something abelian.

4. DAY 4

Recall that we have seen many examples of groups that have the same structure.

4.1. **Group Homomorphisms and First Isomorphism Theorem.**

Example 4.1. Let V be the Klein 4-Group, or the symmetry group of an rectangle, and H be the subgroup $\{e, v\}$ where v corresponds to the flip along the vertical axis. The set of left cosets V/H contains the following elements:

$$eH = \{e, v\} = vH$$
$$hH = \{h, vh\} = (vh)H.$$

Note that V/H has a group structure under the $\diamond$ operation defined in Day 3, and is identifiable with $\mathbb{Z}_2$ (treating eH as 0, and hH as 1 in $\mathbb{Z}_2$, and using the addition operation).

Example 4.2. Consider D_4 and $R_4 = \{e, r, r^2, r^3\}$. Then the set of left cosets D_4/R_4 contains the elements:

$$eR_4 = rR_4 = r^2R_4 = r^3R_4 = \{e, r, r^2, r^3\},$$
$$fR_4 = rfR_4 = r^2fR_4 = r^3fR_4 = \{f, rf, r^2f, r^3f\}.$$

The set of left cosets form a group under the $\diamond$ operation, and is identifiale with $\mathbb{Z}_2$ by treating eR_4 as 0 and fR_4 as 1 under the addition operation.

In general, we identify groups using maps.

Definition 4.3. Let $(G, *)$ and $(H, \star)$ be two groups, a set map $f : G \to H$ is a **group homomorphism** if $f(x * y) = f(x) \star f(y)$ for all $x, y \in G$.

Example 4.4. Consider the map $f : \mathbb{Z} \to \mathbb{Q}$ defined by $f(x) = x$. Show that this is a group homomorphism.

Example 4.5. Consider the map $f : \mathbb{Z} \to \mathbb{Q}$ defined by $f(x) = \lfloor x \rfloor$. Show that this is **not** a group homomorphism.

Example 4.6. Consider the map $f : \mathbb{Z} \to \mathbb{Z}_4$ defined by $f(x) = x \mod 4$. Show that this is a group homomorphism.

Example 4.7. Consider the map $f : \mathbb{Z} \to 4\mathbb{Z}$ defined by $f(x) = 4x$. Show that this is a group homomorphism.

Proposition 4.8. *Let $(G, *)$, $(H, \star)$ be two groups, and f is a group homomorphism $f : G \to H$. Then the followings are true:*

(a) $f(e_G) = e_H$;
(b) $f(g^{-1}) = f(g)^{-1}$.

Definition 4.9. A group homomorphism $f : G \to H$ is an isomorphism if f is injective and bijective (i.e. f is bijective). We say that G and H are isomorphic, denoted as $G \cong H$.

Example 4.10. The set of integers $\mathbb{Z}$ under addition is isomorphic to any of its subgroups.

Example 4.11. We have witnessed the following isomorphisms:

(a) $D_4/R_4 \cong \mathbb{Z}_2$;
(b) $V/H \cong \mathbb{Z}_2$.
(c) Sym(3 points) $\cong S_3$.

(d) $V \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ via the isomorphism, $f : V \to \mathbb{Z}_2 \times \mathbb{Z}_2$ defined by

$$\begin{aligned} e &\mapsto (0,0), \\ v &\mapsto (1,0), \\ h &\mapsto (0,1), \\ vh &\mapsto (1,1). \end{aligned}$$

Definition 4.12. Let G and H be two groups and f is a group homomorphism $G \to H$. Then the set

$$\{x \in G : f(x) = e_H\}$$

is called the kernel of f, denoted by $\ker(f)$.

We extract some ideas from these quotient groups identifications; By modding out a subgroup of a group, we declare that we don't care about the subgroup and just want to see the rest of the operations, regarding the subgroup as the identity.

Proposition 4.13. *Let G, H be two groups and $f : G \to H$ is a group homomorphism. The set* $\ker(f)$ *is a normal subgroup of G.*

Proposition 4.14. *Let G and H be groups and f be a group homomorphism $f : G \to H$. Then f is injective if and only if* $\ker(f) = e_G$.

Theorem 4.15 (First Isomorphism Theorem of Groups)**.** *Let G and H be groups and $f : G \to H$ is a group homomorphism. Then*

$$G/\ker(f) \cong \mathrm{Im}(f).$$

4.2. **Exercises for Day 4.**

Exercise 4.16. Given G, H two groups and a group homomorphism $f : G \to H$.

(a) Prove that $\ker(f)$ is a subgroup of G.
(b) Prove that $\ker(f)$ is a normal subgroup of G.
(c) Denote the subset

$$\{f(g) : g \in G\} \subseteq H$$

the **image of** f, or $\mathrm{Im}(f)$. Prove that $\mathrm{Im}(f)$ is a subgroup of H.

Exercise 4.17. Let G and H be groups and f be a group homomorphism $f : G \to H$. Then f is injective if and only if $\ker(f) = e_G$.

Exercise 4.18. Consider the symmetric group S_3.

(a) Which subgroup of S_3 is normal? Call it H.
(b) What familiar group is S_3/H identified with?

Exercise 4.19 (Hard)**.** Classify all groups of size n where n ranges from 1 to 8.

5. Day 5

5.1. First Isomorphism Theorem of Groups.

Theorem 5.1. *Let G, H be two groups and $f : G \to H$ is a group homomorphism. Then*

$$G/\ker(f) \cong \mathrm{Im}(f).$$

Recall definitions and results from Day 4's exercises that we need for the proof.

Definition 5.2. Let G and H be two groups and f is a group homomorphism $G \to H$. Then the set

$$\{x \in G : f(x) = e_H\}$$

is called the kernel of f, denoted by $\ker(f)$.

To make sense of the statement of the theorem, we want to show that $\ker(f)$ is a normal subgroup of G and $\mathrm{Im}(f)$ is a subgroup of H. We leave it to the reader to check that $\ker(f)$ is a subgroup of G.

Proposition 5.3. *Given two groups G, H and a group homomorphism $f : G \to H$. Then* $\ker(f)$ *is normal.*

Proof. Let $\ker(f) = K$. Then to show that K is normal in G is equivalent to showing that for all $a \in G$, $aKa^{-1} = K$ (i.e., for all $a \in G$ and for all $k \in K$, there exists k' such that $ak = k'a$, or $aka^{-1} \in K$.) For any $a \in G, k \in K$,

$$f(aka^{-1}) = f(a)f(k)f(a^{-1}) = f(a)e_H f(a^{-1}) = f(a * a^{-1}) = f(e_G) = e_H.$$

Hence $aka^{-1} \in K$ and K is normal. □

Proposition 5.4. *Let G be a group and H is a subgorup of G. Show that given any two cosets aH, bH, either $aH = bH$ or $aH \cap bH = \varnothing$.*

Proof. Let aH and bH be two cosets. Suppose $aH \cap bH \neq \varnothing$. Then we want to show that $aH = bH$. Since $aH \cap bH = \varnothing$, we know that there exists $x \in aH \cap bH$; in particular, $x = ah = bh'$ for some $h, h' \in H$. This implies that $a = bh'h$ and $b = ahh'^{-1}$. Therefore, $aK = bK$. □

Proof of First Isomorphism Theorem of Groups. Let $\ker(f) = K$. Define a map $\phi : G/K \to \mathrm{Im}(f)$ by

$$aK \mapsto f(a).$$

We check the followings:

(a) *Well-defined:* Let $aK = bK$. We want to show that $\phi(aK) = \phi(bK)$, which is the same as showing that $f(a) = f(b)$. Since $aK = bK$, by previous proposition, $a \in bK$. Then $a = bk$ for some $k \in K$. Hence $f(a) = f(bk) = f(b)f(k) = f(b)e_H = f(b)$.

(b) *Injective:* Suppose $\phi(aK) = \phi(bK)$ (i.e. $f(a) = f(b)$). Then we want to show that $aK = bK$. Since

$$e_H = f(a)^{-1}f(a) = f(a)^{-1}f(b) = f(a^{-1} * b),$$

we know that $a^{-1}b \in K$. Hence $b \in aK$ and $aK = bK$.

(c) *Surjective:* Let $y \in \mathrm{Im}(f)$, and this implies that there exists $x \in G$ such that $f(x) = y$. Then $\phi(xK) = f(x) = y$.

(d) *Group Homomorphism:* Let $aK, bK \in G/K$. Then

$$\phi(aK \diamond bK) = \phi((ab)K) = f(ab) = f(a)f(b) = \phi(aK)\phi(bK).$$

Therefore, ϕ is a group isomorphism. □

Example 5.5 (Geometry and Group Theory)**.** Consider the punctured complex plane

$$\mathbb{C}^* = \mathbb{C} \setminus \{0\} = \{re^{i\theta} : r \in \mathbb{R}_+, \theta \in [0, 2\pi)\}.$$

This is a group under multiplication. For any complex number, which has a modulus and an angle, we could care not about its modulus, but only care about its angle. We can contrive a stereographic projection to do so:

$$f : \mathbb{C}^* \to S^1 = \{z \in \mathbb{C} : |z| = 1\}$$

by

$$f(re^{i\theta}) = e^{i\theta}.$$

The kernel of this map is $\mathbb{R}_+$ and the image is S^1. By First Isomorphism Theorem of Groups, $\mathbb{C}^*/R_+ \cong S^1$, which matches up with our intuition.

The S^1 as the image is often referred to as the **complex projective space** of dimension 1, denoted as $\mathbb{CP}^1$. It being compact is one of the reasons why geometers like complex projective spaces.

Example 5.6 (Linear Algebra and Group Theory)**.** The previous example can be seen in linear algebraic way. Let $\mathbb{C}$ be a 2-dimensional vector space over $\mathbb{R}$, and the set of all vectors in $\mathbb{C}$ is a group under addition. We want to study the set of all nonzero vectors in relation with a chosen 1-dimensional vector space. Therefore,

$$\mathbb{C}/\mathbb{R} \cong \mathbb{R},$$

or in otherwords, the quotient space of $\mathbb{C}$ mod $\mathbb{R}$ is a 1-dimenisional real vector space.