Review VII(Slides 458 - 521)

Group Theory

This is the most difficult part!

HamHam

University of Michigan-Shanghai Jiao Tong University Joint Institute

July 21, 2023

VE203 - Discrete Mathmatics

Why group theory?

Group theory is soooooo abstract. Why we need it?

From GPT:

- Philosophical view of Number theory: Group theory is used to study properties of numbers and explore topics such as modular arithmetic, Diophantine equations, and primality testing.
- Particle physics: Group theory is crucial in the field of particle physics, particularly in the study of the fundamental forces and particles. Symmetry groups, like the Standard Model gauge group, describe the interactions between particles.
- Geometry: Group theory is used to study the symmetries and transformations of geometric objects, leading to a deeper understanding of geometry and its applications in computer graphics and computer-aided design (CAD).

Why group theory?

Fron GPT:

- Coding theory: Group theory is employed in coding theory to construct error-correcting codes used in data transmission and storage systems.
- Music theory: Group theory has applications in music theory to analyze musical structures, symmetries, and chord progressions.

More reference:

- `https://www.zhihu.com/question/29102364`
- `https://www.scienceforums.net/topic/51581-real-life-applications-of-group-theory/`

Groups

A **group** is a pair $(G, \cdot)$, where G is a set, and $\cdot : G \times G \to G$ is a law of composition that has the following properties:

- Closure: The generalized product is defined as $\cdot : G \times G \to G$
- Associativety: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, c \in G$;
- Identity: G contains an identity element 1, such that $1 \cdot a = a \cdot 1 = a$ for all $a \in G$;
- Inverse: Every element $a \in G$ has an inverse, an element b such that $a \cdot b = b \cdot a = 1$.

An **abelian group** is a group whose law of composition is commutative $(a \cdot b = b \cdot a)$.

Properties

Given a group G, $a, b, c \in G$, then

- there exists a **unique** identity element;
  $\rightarrow$ suppose there are two distinct identity i and j, then $i \cdot j = i = j$
- $ba = ca \Rightarrow b = c$ and $ab = ac \Rightarrow b = c$;
  $\rightarrow$ multiply by a^{-1} on both sides, note that a group does not necessarily satisfy the commutative law
- For all $a \in G$, there **exists** a **unique** element $b \in G$ such that $ab = ba = 1$;
  $\rightarrow$ prove existence ($b = a^{-1}$) first, then prove uniqueness by contradiction
- $(ab)^1 = b^{-1}a^{-1}$.
  $\rightarrow (ab)^1(ab) = 1$; $(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b = 1$

Subgroup

A subset H of a group G is a subgroup if it has the following properties:

- Closure: If $a, b \in H$, then $ab \in H$;
- Identity: $1 \in H$;
- Inverses: If $a \in H$, then $a^{-1} \in H$.

Look carefully at the identity and inverse axioms for a subgroup:

- In verifying the identity axiom for a subgroup, the issue is not the existence of an identity but **whether the identity for the group is actually contained in the subgroup**.
- Likewise, for subgroups the issue of inverses is not whether inverses exist (every element of a group has an inverse) but **whether the inverse of an element in the subgroup is actually contained in the subgroup**.

Exercise

1. Given a group G and its two distinct subgroups H_1 and H_2. Check whether the following sentences are true or false:

- The identity element in G and H_1 must be the same.
- $H_1 \cup H_2$ is a group.
- $H_1 \cap H_2$ cannot be empty and it is a group.
- A subset in G that is not a subgroup may be a group.

Comment. Compare to the concept of **vector space** in Vv186.

Exercise

2. $\mathbb{Z}^2 = \mathbb{Z} \times \mathbb{Z}$ denotes the set of pairs of integers:

$$\mathbb{Z}^2 = \{(m, n) \mid m, n \in \mathbb{Z}\}.$$

It is a group under "vector addition", that is,

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

Consider the set

$$H = \{(x, y) \mid x + y \geqslant 0\}.$$

Check if H is a subgroup of $\mathbb{Z}^2$.

Exercise

3. Let G be a group and let $H \subset G$ with $H \neq \varnothing$. If $\forall a, b \in H$ we have $ab^{-1} \in H$ then H is a subgroup of G.

Solution:

Since $H \subset G$, any operation in H has associativity. Then, we need to verify closure, identity, and inverses requirements but we need to do these **in a particular order**.

1. Since $H \neq \varnothing$, pick any $a \in H$. Then $aa^{-1} = e \in H$, so H has the identity.
2. Pick any $a \in H$. Since the identity $e \in H$, then $ea^{-1} = a^{-1} \in H$ so we have inverses.
3. Pick any $a, b \in H$. Then $b^{-1} \in H$ and denote as $c \in H$. So, $ac^{-1} \in H$ according to the problem statement. So, $ab = a(b^{-1})^{-1} = ac^{-1} \in H$ and we have closure.

Exercise

4. Let G be a group. If $\forall x \in G : x^2 = e$, show that G is an abelian group.

Solution:

From $\forall x \in G : x^2 = e$, we obtain $x = x^{-1}$.
Therefore, taking $\forall x, y \in G$, we have

$$xy = (xy)^{-1} = y^{-1}x^{-1} = yx.$$

This completes the proof.

Cyclic Group

The cyclic subgroup generated by g is

$$\langle g \rangle = \{g^k \mid k \in \mathbb{Z}\}.$$

In other words, $\langle g \rangle$ consists of all (positive or negative) powers of g.

$$\langle g \rangle = \{k \cdot g \mid k \in \mathbb{Z}\}.$$

Be sure you understand that the difference between the two forms is simply **notational**: It's the same concept.

Let G be a group, $g \in G$. The order of g is the smallest positive integer n such that $g^n = 1$ $(ng = 0)$. If there is no positive integer n such that $g^n = 1$ $(ng = 0)$, then g has **infinite** order.

Exercise

5. List the elements of the subgroups generated by elements of $\mathbb{Z}_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$.

Solution:

$$\langle 0 \rangle = \{0\}$$
$$\langle 2 \rangle = \langle 6 \rangle = \{0, 2, 4, 6\}$$
$$\langle 4 \rangle = \{0, 4\}$$
$$\langle 1 \rangle = \langle 3 \rangle = \langle 5 \rangle = \langle 7 \rangle = \{0, 1, 2, 3, 4, 5, 6, 7\} = \mathbb{Z}_8$$

Question

What is the identity? Order?

Exercise

6. Prove that
   1. Let $G = \langle g \rangle$ be a finite cyclic group, where g has order $n \neq 0$. Then the powers $\{1, g, \cdots, g^{n-1}\}$ are distinct.
   2. Let $G = \langle g \rangle$ be infinite cyclic. If m and n are integers and $m \neq n$, then $g^m \neq g^n$.

Solution:

1. Since g has order n, $g, g^2, \cdots, g^{n-1}$ are all different from 1. Suppose $g^i = g^j$ where $0 \leqslant j < i < n$. Then $0 < i - j < n$ and $g^{i-j} = 1$, contrary to the preceding observation. Therefore, the powers $\{1, g, \cdots, g^{n-1}\}$ are distinct.
2. Suppose without loss of generality that $m > n$. We want to show that $g^m \neq g^n$. Suppose this is false, so $g^m = g^n$. Then $g^{m-n} = 1$, so g has finite order $m - n$. This contradicts the fact that a generator of an infinite cyclic group has infinite order. Therefore, $g^m \neq g^n$.

Symmetric Group

Definition

Given $n \in \mathbb{N}\backslash\{0\}$, we have the following symmetric group of degree n,

$$\begin{aligned} S_n &= \{\text{All permutations on } n \text{ letters/numbers}\} \\ &= \mathsf{Sym}\{1, 2, 3, \ldots, n\} \\ &= \{f : [n] \to [n] \mid f \text{ bijective}\} \end{aligned}$$

Note that it is a finite group of order $n!$ (the number of bijections from $[n]$ to $[n]$), *i.e.*, $|S_n| = n!$.

- A subgroup of S_n is called a **permutation group**.
- A permutation of the form (ab) where $a \neq b$ is called a **transposition**.

Permutation

A permutation that can be expressed as a product of an **even/odd number of transpositions** is called an even/odd permutation.

The set of even permutations in S_n forms a subgroup of S_n, denoted as A_n, is called the alternating group of degree n.

Permutation $\rightarrow$ transportation: $(132)(5648) = (13)(32)(56)(64)(48)$ (not unique, but only can be either all odd or all even).

Inverse of permutation: $\sigma = (132)(5648) \Rightarrow \sigma^{-1} = (8465)(231)$ (Separate permutations to be **disjoint** first. Since $\sigma(a_i) = a_j$ implies $\sigma^{-1}(a_j) = a_i$, we only need to reverse the order of the cyclic pattern).

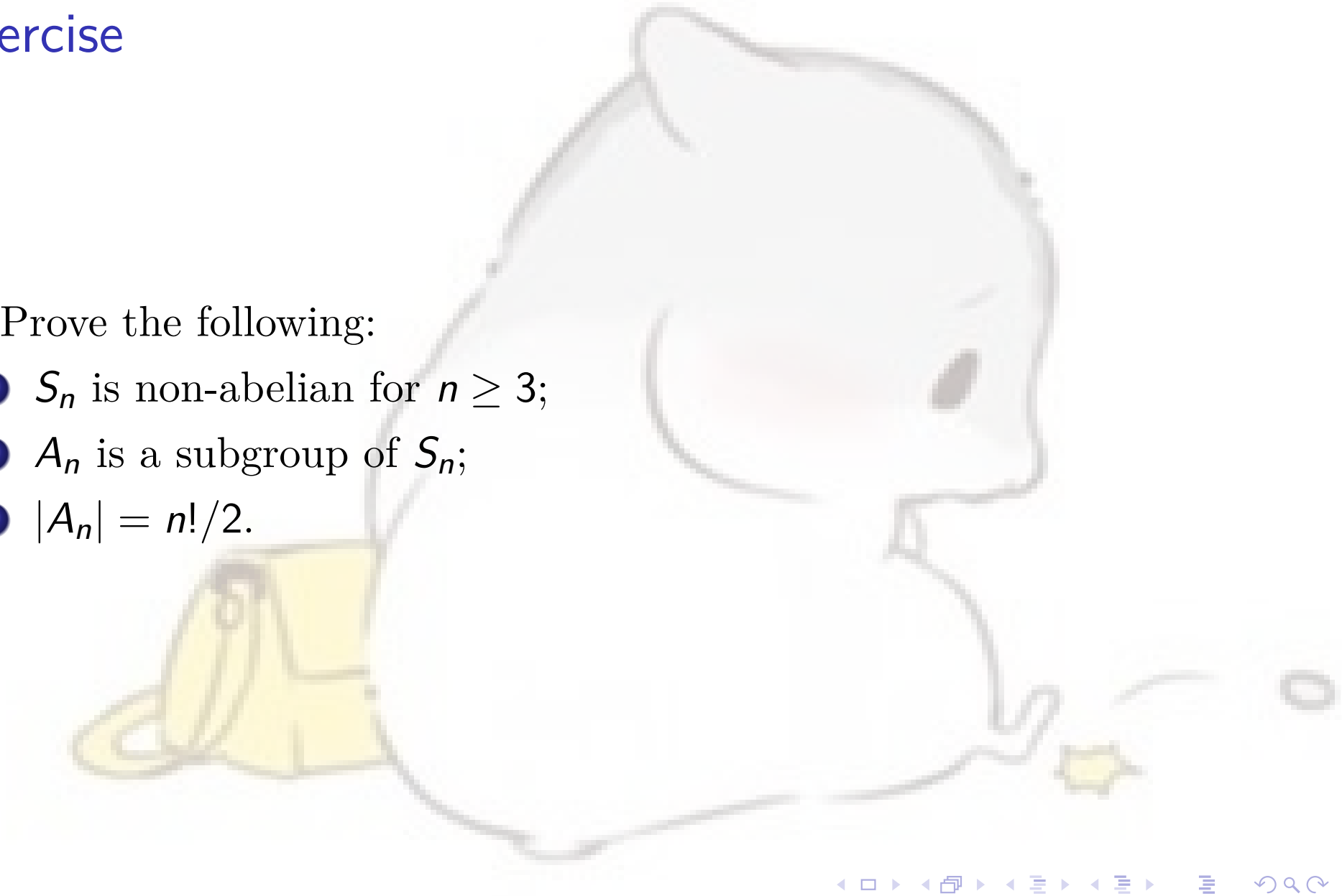
Composition: $(12)(245)(13)(125) = (14532)$.
(Apply the **right** permutation first. Demo!).

Exercise

7. True or false:
   - Can an abelian group have a non-abelian subgroup?
   - Can a non-abelian group have an abelian subgroup?
   - Can a non-abelian group have a non-abelian subgroup?

Exercise

8. Prove the following:
   1. S_n is non-abelian for $n \geq 3$;
   2. A_n is a subgroup of S_n;
   3. $|A_n| = n!/2$.



Homomorphism

Given groups G, G', a homomorphism is a map $f : G \to G'$ such that for

$$f(x \cdot y) = f(x) \cdot f(y)$$

We have:

- $f(a_1 \cdots a_k) = f(a_1) \cdots f(a_k)$
- $f(1_G) = 1_{G'}$
- $f\left(a^{-1}\right) = (f(a))^{-1}$

Compare and Contrast

Recall the concept of **structure preserving**

$$\begin{array}{ccc} y & \xrightarrow{f} & f(y) \\ x \cdot \downarrow & & \downarrow f(x) \cdot \\ x \cdot y & \xleftarrow{f^{-1}} & f(x \cdot y) \end{array}$$

Image & Kernel

The **image** of a homomorphism $f: G \to G'$, often denoted by $\operatorname{im} f$, or $f(G)$, is simply the image of as a map of sets:

$$\operatorname{im} f = \left\{ x \in G' \mid x = f(a) \text{ for some } a \in G \right\}.$$

The **kernel** of f, denoted by $\ker f$, is the set of elements of G that are mapped to the identity in G':

$$\ker f = \{ a \in G \mid f(a) = 1_{G'} \}.$$

Comapre and Contrast

Let U, V be real or complex vector spaces and $L \in \mathscr{L}(U, V)$, then we define the range and kernel of L by:

$$\operatorname{ran} L := \{ v \in V : \exists_{u \in U} \; v = Lu \}$$

$$\ker L := \{ u \in U : Lu = 0 \}$$

Properties

Let $f: G \to G'$ be a group homomorphism, and let $a, b \in G$. Let $K = \ker f$. The following are equivalent:

1. $f(a) = f(b)$
2. $a^{-1}b \in K$
3. $b \in aK$
4. $aK = bK$

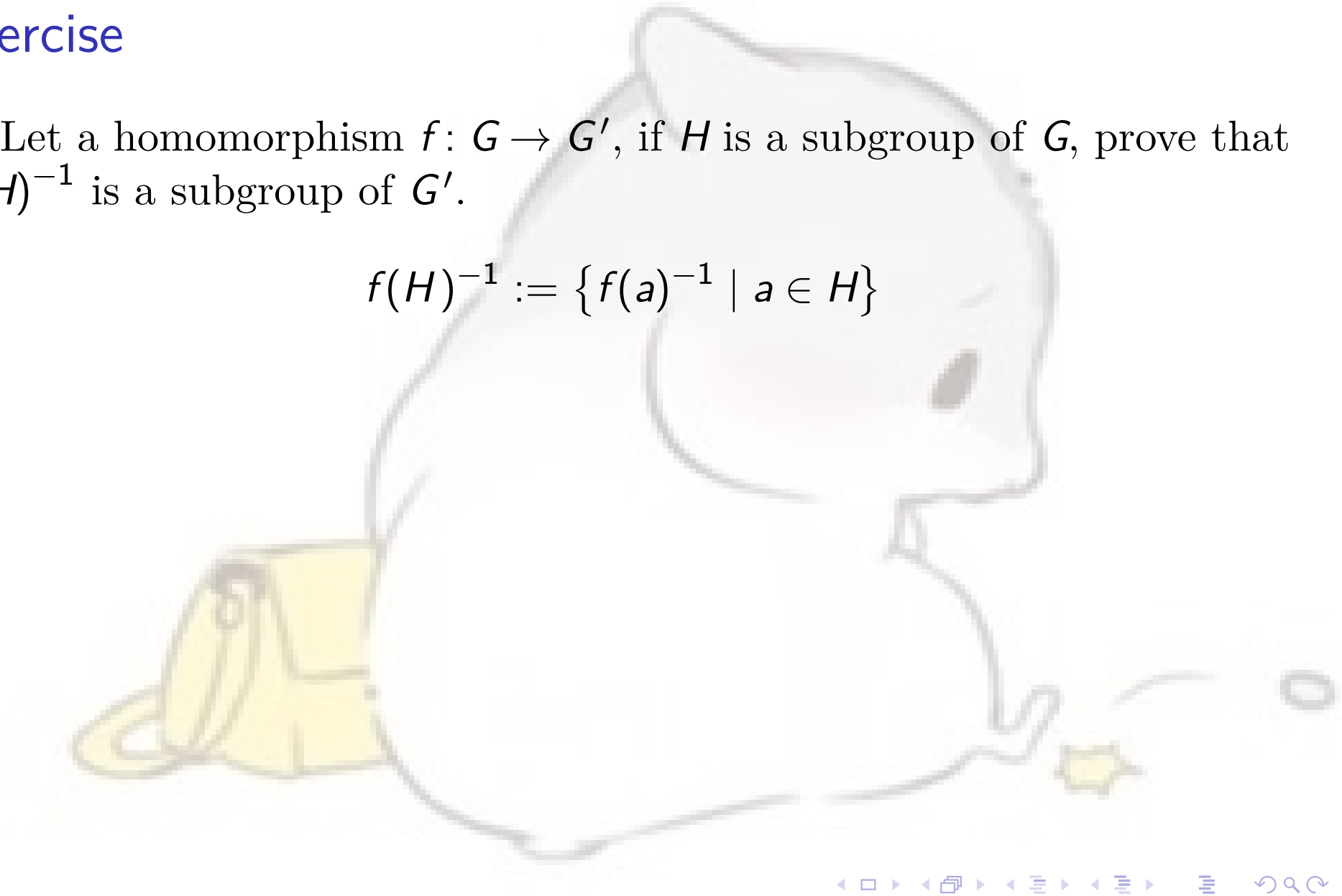
! A homomorphism $f: G \to G'$ is injective iff $\ker f = \{1_G\}$.
! Isomorphism $G \cong G' \quad \Leftrightarrow \quad f$ is **bijective**.
! How to check if a **homomorphism** is an **isomorphism**:

verify $\ker f = \{1_G\}$ (injection) and $\operatorname{im} f = G'$ (surjection)

Exercise

9. Let a homomorphism $f: G \to G'$, if H is a subgroup of G, prove that $f(H)^{-1}$ is a subgroup of G'.

$$f(H)^{-1} := \left\{ f(a)^{-1} \mid a \in H \right\}$$



Exercise

9. Let a homomorphism $f: G \to G'$, if H is a subgroup of G, prove that $f(H)^{-1}$ is a subgroup of G'.

$$f(H)^{-1} := \left\{ f(a)^{-1} \mid a \in H \right\}$$

Solution:

Let $x, y, a \in H$.

1. Closure:
   $f(x)^{-1} f(y)^{-1} = f(x^{-1}) f(y^{-1}) = f\left(x^{-1} y^{-1}\right) = f\left((yx)^{-1}\right) = f(yx)^{-1}$.
2. Identity: $1_G \in H, 1_{G'} = f(1_G) = f(1_G)^{-1} \in f(H)^{-1}$.
3. Inverse: $f(a)^{-1} = f\left(a^{-1}\right) \in f(H)^{-1}$.

Exercise

10. Let $(G, \cdot)$ be a group. Let $g, h \in G$ both have order n, prove that $\langle g \rangle \cong \langle h \rangle$.

Solution:

Define $f : \langle g \rangle \to \langle h \rangle$ by $f(g) = h$ and for all $0 \leq k \leq n$, $f\left(g^k\right) = f(g)^k$. So, f is a well-defined function, and, by definition, f preserves the group product. It is clear that the function f sends $1_G \mapsto 1_G$, $g \mapsto h$, $\ldots$, $g^{n-1} \mapsto h^{n-1}$, and so f is a bijection.

(Directly taken from Zach's slides)

Cosets

Given a group G, if H is a subgroup of G and $a \in G$, the notation aH will stand for the set of all products ah with $h \in H$,

$$aH = \{g \in G \mid g = ah \text{ for some } h \in H\}$$

This set is called a **left coset** of H in G.

The number of left cosets of a subgroup is called the **index** of H in G. The index is denoted by $[G : H]$ (can be infinite, why?).

All left cosets aH of a subgroup H of a group G have the same **order**.

- Counting formula: $|G| = |H| \cdot [G : H]$.
- Lagrange's Theorem: Let H be a subgroup of a finite group G. The order of H divides the order of G.

Exercise

11. Verify Lagrange's Theorem for the subgroup $H = \{0, 3\}$ of $\mathbb{Z}_6$.

Solution:

The cosets are

$$0 + H = \{0, 3\}, \quad 1 + H = \{1, 4\}, \quad 2 + H = \{2, 5\}.$$

Notice there are 3 cosets, each containing 2 elements, and that the cosets form a **partition** of the group.

An important consequence of Lagrange's Theorem

Theorem

Let $(G, \cdot)$ be a group and let $g \in G$ have order n. If there exists $m, k \in \mathbb{N}\backslash\{0\}$ with $n = mk$, then the order of g^m is k.

Proof.

Let $m, k \in \mathbb{N}\backslash\{0\}$ with n = mk. Now, $(g^m)^k = g^{mk} = g^n = 1_G =$. If $0 < q < k$ is such that $(g^m)^q = 1_G$, then $g^{mq} = 1_G$. But $mq < mk = n$, which is a contradiction.

Theorem

If $(G, \cdot)$ is a finite group with order n, then for all $g \in G, g^n = 1_G$.

Proof.

Let $(G, \cdot)$ be a finite group with order n. Let $g \in G$. We know that the order of g must be finite, so let k be the order of g. Now, k must divide n, so the exists $m \in N$ such that $n = mk$. So $g^n = g^{mk} = (g^k)^m = 1_G^m = 1_G$.

Exercise

12. Prove that for any subgroup $H \leq G$, the (left) cosets of H partition the group G.

Hint:

We need to show that the union of the left cosets is the whole group, and that different cosets do not overlap.

Normal Subgroup

Given group G, and $a, g \in G$, the element $gag^{-1} \in G$ is called the **conjugate** of a by g.

A subgroup N of G is a **normal subgroup**, denoted by $N \trianglelefteq G$, if for all $a \in N$ and $g \in G$, $gag^{-1} \in N$.

Properties:

- $f : G \to G'$ a homomorphism, then $\ker f \trianglelefteq G$.
- Every subgroup of an abelian group is normal.
- The **center** is always a normal subgroup.
- $gH = Hg$ for all $g \in G$ iff $H \trianglelefteq G$.
- $A_n \trianglelefteq S_n$.

Exercise

Important result:

13. Show that any subgroup of index 2 in a group is a normal subgroup.

Solution:

Denote the subgroup as H. Obviously, the left cosets of a subgroup of index 2 are $1_H H = H$ and aH, where $a \notin H$; (why?) the right cosets are $H1_H = H$ and Ha. Since the cosets form a partition of the origin group, and $1_H H = H1_H = H$, so the remaining is another coset, namely $aH = Ha$. (left=right) So H is normal.

University of zhihu: https://zhuanlan.zhihu.com/p/163548084

Reference

- Examples From Zach's Slides (P196)
- Exercises/graphics from 2021-Fall-Ve203 TA Xue Runze
- Exercises from 2021-Fall-Ve203 TA Zhao Jiayuan
- Yan Shijian, etc. *Basic Number Theory*, fourth edition. Beijing: Higher Education Press, 2020.5 print.


THANKS!