# Midterm Rivew - Part II

## Mathematical Logic and Algebraic Structure

Logic, Induction, Group Theory

HamHam

University of Michigan-Shanghai Jiao Tong University Joint Institute

April 5, 2022

VE203 - Discrete Mathmatics

# Propositional Logic

A proposition or statement is a declarative sentence that is either **true** or **false**, but not both.

Four binary connectives $\wedge$ (conjunction), $\vee$ (disjunction), $\rightarrow$ (implication), and $\leftrightarrow$ (biconditional).

| $p$ | $q$ | $p \rightarrow q$ |
|---|---|---|
| 0 | 0 | 1 |
| 0 | 1 | 1 |
| 1 | 0 | 0 |
| 1 | 1 | 1 |

| $p$ | $q$ | $p \leftrightarrow q$ |
|---|---|---|
| 0 | 0 | 1 |
| 0 | 1 | 0 |
| 1 | 0 | 0 |
| 1 | 1 | 1 |

$$(p \rightarrow q) \Leftrightarrow (\neg p \vee q)$$

$$(p \leftrightarrow q) \Leftrightarrow ((p \rightarrow q) \wedge (q \rightarrow p))$$

# Important Tautologies

## De-Morgan rules

$$\neg(p \vee q) \Leftrightarrow (\neg p) \wedge (\neg q), \quad \neg(p \wedge q) \Leftrightarrow (\neg p) \vee (\neg q).$$

The contrapositive of $p \to q$ :

$$(p \to q) \Leftrightarrow (\neg p \to \neg q),$$

Proof by contradiction:

$$(p \to q) \Leftrightarrow (p \wedge \neg q) \to 0$$

# Predicates

**Definition**

A function $P : X \to \{\top, \bot\}$ is called a **predicate** on its domain $X$.

It is a declarative sentence involving variables, *i.e.*, a statement involving variables such that when the variables a substituted with appropriate individuals we obtain a **proposition**.

- **Predicate:** $P(x) : x > 1$;
- **Proposition:** $P(0) : 0 > 1$ (false); $P(2) : 2 > 1$ (true).

# Exercise

1. Given logical variables $p$ and $q$, which of the following are tautologies?

(A) $p \wedge \neg p$

(B) $((p \to q) \wedge \neg q) \to \neg q$

(C) $p \vee q \to p$

(D) $p \to (p \wedge q)$

Answer: A B

*Comment.* There is no choice question in this exam.

# Induction

An argument by **strong** induction that shows that a property $A(n)$ holds for all $n \in \mathbb{N}$ with $n \geqslant n_0$ proceeds as follows:

1. Show that $A(n_0)$ holds;
2. Show that for all $n \geqslant n_0$, if $A(n)$ holds, then $A(n+1)$ holds;
   $\rightarrow$ "Assuming the statement is true for $n$, we now show that it is true for $n+1$"
3. Conclude that for all $n \in \mathbb{N}$ with $n \geqslant n_0$, $A(n)$ holds.

## Terminology

- Type-I & Type-II Induction
- IH - Induction Hypothesis

## Interesting Exercise

**If you think the following problem is too hard for you, just ignore it.**

There is a board which is divided into $8 \times 8$ small lattices. One of the lattice is broken (its location is unknown). Prove that we can always place 21 small "L" cards on this board. Note that a "L" card consists of three lattices in the form of "L".

*Hint.* Generalize $8$ to $n$ wouldn't work. Is there another way to generalize the problem?

# Exercise

2. Given a poset $(P, \leq)$. Use induction to show that every finite non-empty set $Q \subset P$ admits a minimal element with respect to $\leq$.

# Exercise

We define the set $S \subset \mathbb{Z}^2$ by the following properties

- $(3, 5) \in S$
- $(x, y) \in S \Rightarrow (x + 2, y) \in S$
- $(x, y) \in S \Rightarrow (-x, y) \in S$
- $(x, y) \in S \Rightarrow (y, x) \in S$

Show that $S = T$, where

$$T = \left\{ (x, y) \in \mathbb{Z}^2 : \underset{m,n \in \mathbb{Z}}{\exists} (x, y) = (2m + 1, 2n + 1) \right\}.$$

## Group

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:

- The law of composition is **associative**: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, c \in G$;
- $G$ contains an **identity** element 1, such that $1 \cdot a = a \cdot 1 = a$ for all $a \in G$;
- 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** $(a \cdot b = b \cdot a)$.

# Subgroup

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

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

## Question

How to prove/disprove $H$ is a subgroup of $G$?

# Subgroup of $(\mathbb{Z}, +)$

For $a \in \mathbb{Z}$, a subgroup of $(\mathbb{Z}, +)$ is given by integers divisible by $a$ as,

$$a\mathbb{Z} = \{n \in \mathbb{Z} \mid n = ka \text{ for some } k \in \mathbb{Z}\}.$$

Given $a, b \in \mathbb{Z}$, then the subgroup $S$ generated by $a$ and $b$, denoted by

$$S = \mathbb{Z}a + \mathbb{Z}b = \{n \in \mathbb{Z} \mid n = ra + sb \text{ for some integers } r, s\}$$

It is also the smallest subgroup that contains both $a$ and $b$.

# Exercise

3. Let $S$ be a subgroup of the additive group $(\mathbb{Z}, +)$. Prove that
   - either $S$ is the trivial subgroup $(\{0\}, +)$,
   - or it has the form $a\mathbb{Z}$, where $a$ is the smallest positive integer in $S$.

# Cyclic Group

A group is cyclic if it can be generated by a single element. The cyclic subgroup generated by $g$ is

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

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

A group $G$ is cyclic if $G = \langle g \rangle$ for some $g \in G$. $g$ is a generator of $\langle g \rangle$.

## Notations

Oder of a element vs. Order of a group: $|g| \quad |\langle g \rangle| \quad |G|$

# Exercise

4. Let $(G, \cdot)$ be a finite. Prove that if $G$ is cyclic and the order of $G$ is even, then $G$ has exactly one element of order 2.

# Symmetric Group

Given $n \in \mathbb{N} \backslash \{0\}$, we have the following symmetric group of degree $n$, $S_n = \{\text{All permutations on } n \text{ letters/numbers}\}$. Note that it is a finite group of order $n!$.

The permutation does not satisfy the law of communication. However, if two permutations $\sigma$ and $\tau$ are **disjoint**, we have $\sigma\tau = \tau\sigma$.

The order of operations is **from right to left**.

## Symmetric Group

A permutation of the form $(ab)$ where $a \neq b$ is a **transposition**.

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 $A_n$, is called the alternating group of degree $n$. $|A_n| = n!/2$ for $n > 1$.

# Exercise

5. Prove that for $n \geqslant 3$, every element of $A_n$ is a product of 3-cycles.

# Homomorphism

Given groups $G, G'$, a homomorphism is a map $f\colon G \to G'$ such that for all $x, y \in G$,

$$f(xy) = f(x)\,f(y)$$

Two important properties:

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

# Image and Kernel

The image of a homomorphism $f\colon G \to G'$, often denoted by 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 $G'$:

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

# isomorphism

Given groups $G$ and $G'$, an isomorphism $f\colon G \to G'$ is a **bijective** group homomorphism, *i.e.*, a bijection $f(xy) = f(x)\,f(y)$ for all $x, y \in G$.

Check if a **homomorphism** $f\colon G \to G'$ is an isomorphism: verify $\ker f = \{1_G\}$ (injection) and $\mathrm{im} f = G'$ (bijection).

# Exericse

6. Given group $G$ and $a \in G$ a fixed element, define $\gamma_a : G \to G$, by $\gamma_a(x) = axa^{-1}$.

(1) Show that $\gamma_a$ is a isomorphism.

(2) If $a, b \in G$, show that $\gamma_a \circ \gamma_b = \gamma_{ab}$

## Cosets

Given a group $G$, if $H$ is a subgroup pf $G$ and $a \in G$, then a left coset of $H$ in $G$ can be defined as

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

The number of left cosets of a subgroup is the index of $H$ in $G$ $[G : H]$ (which could be infinite if $|G| = \infty$). 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 $G$.

# Exericse

7. Prove Lagrange's Theorem.

# 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 $g \in G$, $gag^{-1} \in N$.

$$N \trianglelefteq G \equiv gNg^{-1} = H \text{ for all } g \in G \equiv gN = Ng \text{ for all } g.$$

# Exercise

8. Let $G$ be a group and $N \trianglelefteq G$ be a normal subgroup. We define a binary operation on $G/N$ as follows: for $aN, bN \in G/N$ we set

$$(aN)(bN) = abN.$$

Show that the quotient group $G/N$ exists.

Note: $G/N := \{aN \mid a \in G\}$

# Final Remarks

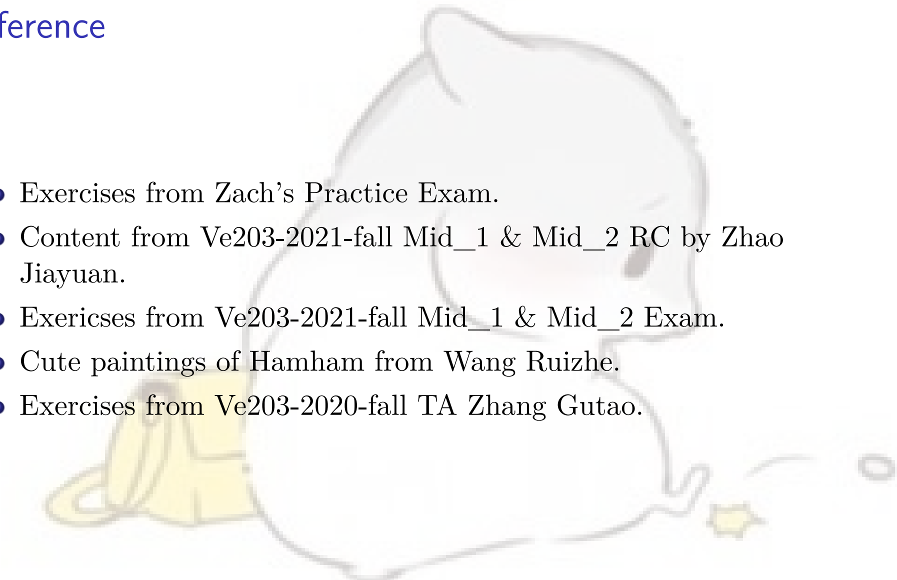
Hmm... Here's something I want to say:

- no choice question in the exam.
- Take a look at last semester's mid1 & mid2 paper.
- Take quiz part I & II.
- Look at our OH feedbacks and questions on piazza.
- DO GET UP! This is an early-eight exam. It's better to have breakfast first.
  - Exam Time: 8:00 - 9:40
  - Submit Time: 9:40 - 9:45
- Be confident! The exam will be easy!



Good Luck For Your Exam!


# Reference




- Exercises from Zach's Practice Exam.
- Content from Ve203-2021-fall Mid_1 & Mid_2 RC by Zhao Jiayuan.
- Exericses from Ve203-2021-fall Mid_1 & Mid_2 Exam.
- Cute paintings of Hamham from Wang Ruizhe.
- Exercises from Ve203-2020-fall TA Zhang Gutao.