1. OVERVIEW

1.1 What is Mathematics?

- Mathematics per se consists of discovering and proving **theorems** (정리) from **definitions** (정의).
- Axiomatic approach a.k.a. deductive system
- Axiom (공리): the starting point of mathematical studies with undefined terms
- Mathematical objects: numbers, structures, sets, manifolds, relations, etc.

1.2 Hierarchy of Mathematical Studies

[Algebra] [Analysis] [Topology] [Number Theory] [Discrete Math] [Probability & Statistics]

[Set Theory] [Logic] [Mathematical Philosophy]

1.3 Set Theory (집합론, 集合論)

- Why? To resolve many paradoxes, esp. Russell's paradox
- What? Foundation of mathematics; sets, relations, functions, etc.
- Subfields: Axioms, Category Theory, Set Theory, etc.

1.4 Logic (논리, 論理)

- Why? To make firm foundation of mathematics
- What? Propositions, Formulas, Syntax, Semantics, etc.
- Subfields: Model Theory, Proof Theory, Propositional Logic, 1^{st}/ 2^{nd}/ High-Order Logic, Lambda Calculus, etc.

1.5 Algebra (대수학, 代數學)

- Why? To find the solutions of polynomials (다항식).
- What? Structures of Set associated with one or two operations; group, ring, field, vector spaces, modules, etc.
- Subfields: Group/Ring/Field Theory, Linear Algebra(선형대수학), Algebraic Geometry, etc.

1.6 Analysis (해석학, 解哲學)

- Why? To make firm foundation of Calculus (미적분학)
- What? Microscopic viewpoint, special case of topology; limit, differentiation(미분), integration(적분), continuity of functions, epsilon-delta reasoning, etc.
- Subfields: Calculus, Real/Complex Analysis(실/복소해석학), Differential Equations(미분방정식), Differential Geometry(미분기하학), Functional Analysis, Harmonic Analysis, Measure Theory, etc.

1.7 Topology (위상수학, 位相數學)

- Why? To study analysis with geometric concept; general viewpoint of Analysis
- What? Classification of n-dimensional manifolds; open/closed set, compact space, connected space, etc.
- Subfields: Algebraic Topology, Knot Theory (매듭이론), Low-Dimensional Topology, etc.

1.8 Number Theory (정수론, 正數論)

- Why? What? To study the properties of numbers, esp. integers
- Subfields: Algebraic/Analytic/Transcendental Number Theory, Congruence, Elliptic Curves, Prime Numbers, etc.

1.9 Discrete Mathematics (이산수학, 離散數學)

- Why? What? To study characteristics of discrete objects; <-> continuous math
- Subfields: Automata, Coding Theory, Combinatorics, Computer Science, Finite Groups, Graph Theory, Information Theory, Recurrence Relations, etc.

1.10 Probability and Statistics (확률과 통계, 確率과 統計)

- Why? What? To study randomness in the real world
- Subfields: Stochastic Process, Queuing Theory, Bayesian Analysis, Error Analysis, Markov Processes, Moments, Multivariate Statistics, Random Numbers, Random Walks, Statistical Tests, etc.

1.11 References

- “A First Course in Abstract Algebra” (Fraleigh)
- “Topology” (Munkres)
- “Real Analysis & Foundations” (Krantz)
- “Elementary Number Theory” (Rosen)
- “Discrete Mathematics” (Johnsonbaugh)
- Lecture Notes of Comp 409 “Logic in Computer Science” (Vardi)

2. SET THEORY

2.1 Preliminaries

Undefined Terms set and element (with some condition) cf. class (without condition)

Quantifiers ∃ : there exists, !∃ : not exist, ∃!: uniquely exist, and ∀ : for all

Equality (1) element: a = b iff a, b: symbols for the same object, (2) set: A = B iff a ∈ A ⇔ a ∈ B

Set Relations A ⊆ B (subset), A ∩ B (intersection), A ∪ B (union), and A×B (Cartesian product)

N = {0, 1, 2, 3 …}, **Z** = {…, -2, -1, 0, 1, 2 …}, $\mathbf{Z}_+$ = set of positive integers,

Q = {a/b | a, b ∈ **Z**}, **R** = set of real numbers, **C** = {x + y *i* | x, y ∈ **R**}

Notations Def = Definition, Thm = Theorem, Ex = Example, Rmk = Remark

2.2 Relations

Def A *relation* R of set A and B is a subset of A×B. That is, R ⊆ A×B.

2.2.1 Equivalent Relations

Let R be a relation on A, that is, R ⊆ A×A.

Def A relation R on a set A is *reflexive* if ∀x∈A, xRx.

Def A relation R on a set A is *symmetric* if xRy, then yRx.

Def A relation R on a set A is *transitive* if xRy and yRz, then xRz.

Def A relation R is an *equivalent relation* if it is reflexive, symmetric, and transitive

Thm By an equivalence relation, we can make *equivalent classes*, and *partition*.

2.2.2 Order Relations

Def A relation R is *comparable* if ∀x, y ∈ A such that x≠y, either xRy or yRx.

Def A relation R is *nonreflexive* if !∃x in A such that xRx.

Def A relation R is *order relation* if it is comparable, non-reflexive, and transitive.

Let A be a set of order relation and A' ⊆ A.

Def (immediate) predecessor, (immediate) successor.

Ex Compare $\mathbf{Z}_+$×[0, 1) and [0, 1)×$\mathbf{Z}_+$ with dictionary order relations

Def b: *largest element*(*smallest*) or *maximum*(*minimum*) of A' if b∈A' and if x ≤(≥) b for ∀x∈A'.

Def A' is *bounded above (below)* if b∈A such that x ≤(≥) b for ∀x∈A'. Say b: *upper (lower) bound*

Def If the set of all upper (lower) bounds for A' has a smallest (largest) element,

then this element is called *least upper bound* (*greatest lower bound*) or *supremum* (*infimum*).

Def A set satisfies *least upper bound property* if ∀nonempty bounded-above subset has a supremum.

Ex [0, 1]×[0, 1] and [0, 1)×[0, 1] : satisfy but [0, 1]×[0, 1) and [0, 1)×[0, 1) : not satisfy

2.2.3 Examples

P = set of all people in the world and **R** = set of real numbers

D = {(x,y) ∈ P×P | x is descendent of y}. (nonreflexive, transitive)

B = {(x,y) ∈ P×P | x has an ancestor who is also an ancestor of y}. (reflexive, symmetric)

S = {(x,y) ∈ P×P | the parents of x are the parents of y}. (reflexive, symmetric, transitive)

"$X^1<Y^1$" = {(x,y) ∈ **R**×**R** | x < y}. (comparable, nonreflexive, transitive) → order relation

"$X^2<Y^2$" = {(x,y) ∈ **R**×**R** | $x^2<y^2$}. (nonreflexive, transitive)

"$X^2=Y^2$" = {(x,y) ∈ **R**×**R** | $x^2=y^2$}. (transitive)

2.3 Functions

Def A relation f ⊂A×B is a *function* if, ∀x∈A, ∃! y∈B such that (x, y)∈ f.

In other words, if x = y, then f(x) = f(y). (*Well-defined*) Write f: A→B.

Def Let f: A → B, then say that A: *domain*, B: *codomain*, and f(A): *range*.

Def A function f is *injective (one-to-one)* if f(x) = f(y), then x = y.

Def A function f is *surjective (onto)* if ∀y∈B, ∃x∈A such that f(x) = y.

Def A function f is *bijective (one-to-one correspondence)* if it is injective and surjective

Thm If ∃injective f: A→B and ∃injective g: B→A, then ∃bijective k: A→B

Def Let f: A→B and g: B→C. *Composite* of f and g is g∘f: A→C by (g∘f)(a) = g(f(a)).

Rmk Composite of 2 injective (surjective) functions is injective (surjective).

Def Let f: A→B be bijective. *Inverse function* of f is a function defined by f^{-1}: B→A by $f^{-1}(b)$ = a such that f(a) = b.

Def A *binary operation* on a set A is a function f: A×A→A

Ex Let f: A→B and A_0, A_1 ⊆ A, B_0, B_1 ⊆ B. Then the followings hold.

If $A_0 \subseteq A_1$, then $f(A_0) \subseteq f(A_1)$. If $B_0 \subseteq B_1$, then $f^{-1}(B_0) \subseteq f^{-1}(B_1)$.

$f(A_0 \cup A_1) = f(A_0) \cup f(A_1)$ and $f^{-1}(B_0 \cup B_1) = f^{-1}(B_0) \cup f^{-1}(B_1)$.

$f(A_0 \cap A_1) \subseteq f(A_0) \cap f(A_1)$ and $f^{-1}(B_0 \cap B_1) \subseteq f^{-1}(B_0) \cap f^{-1}(B_1)$. "=" holds if f is injective.

$A_0 \subseteq f^{-1}(f(A_0))$, and "=" holds if f is injective. $B_0 \subseteq f(f^{-1}(B_0))$, and "=" holds if f is surjective.

2.4 Countable and Uncountable Sets

Def A set A is *finite* if ∃ bijective function of A with some selection of positive integers.

That is, if it is empty or if ∃bijection f: A→{1, ..., n} for some n ∈ $\mathbf{Z}_+$.

Thm If A is finite, then !∃bijection of A with a proper subset of itself.

Def A set is *infinite* if it is not finite.

Ex $\mathbf{Z}_+$ is infinite because ∃bijection such that f: $\mathbf{Z}_+$→ $\mathbf{Z}_+$-{1} by f(n) = n+1.

Def A set *A* is *countably infinite* if ∃bijection f: *A*→ $\mathbf{Z}_+$.

Ex **Z** is countably infinite because ∃bijection such that f(n) = 2n (if n>0) or -2n+1 (if n≤0)

Ex $\mathbf{Z}_+ \times \mathbf{Z}_+$, **Q**, the set of all polynomials, and the set of algebraic numbers are countable.

Def A set is *countable* if it is either finite or countably infinite.

Thm A countable union of countable set is countable.

Thm A finite product of countable set is countable.

Def A set is *uncountable* if it is not countable.

Ex **R** is uncountable by Cantor's diagonal method.

Ex $\{0, 1\}^{\omega}$ is uncountable, where $X^{\omega} = \{ f: \mathbf{Z}_+ \to X \mid f: \text{function}\}$.

Thm Let A be a set and *P*(A) be the power set of A. Then $|A| < |P(A)|$ (strictly larger).

Rmk Continuum Hypothesis (Cantor) "! ∃ A such that $|\mathbf{Z}_+| < A < |\mathbf{R}|$."

2.5 References

"Set Theory: An Intuitive Approach" (Y. Lin and S. Lin)

"Topology" (Munkres)

"Mystery of Aleph" (Aczel, 한역판: "무한의 신비")

"Gödel, Escher, Bach: an Eternal Golden Braid" (Hofstadter, 한역판: "괴델, 에셔, 바흐")

3. LOGIC

3.1 Definition of Logic

(1) The ability to determine correct answers through a standardized process

(2) The study of formal inference

(3) A sequence of verified statements

(4) Reasoning, as opposed to intuition

(5) The deduction of statements from a set of statements

3.2 Short History of Logic

(1) Philosophical Logic (500 B.C. to 19th Century)

- Some problems due to the ambiguity of natural language
- Liar's paradox ("This sentence is a lie"), Sophist' paradox (a trial between student and school), Surprise Paradox

(2) Symbolic Logic (mid to late 19th Century)

- George Boole tried to formulate logic in terms of a mathematical language
- Venn Diagram was developed as a means of reasoning about sets

(3) Mathematical Logic (late 19th to mid 20th Century)

- As mathematical proofs became more sophisticated, paradoxes began to show up
- Russell's paradox ("T = {S| S not belongs to S}, then T∈T?"), Cantor's Continuum Hypothesis
- Gödel's First and Second Incompleteness Theorems, Church and Turing's undecidable problems

(4) Logic in Computer Sciences (mid 20th Century to current time)

- Computability Theory (1930s), Computational Complexity Theory (1970s)
- Boolean logic, Database design, Semantics in Programming Languages, Design Validation/Verification, AI, etc.

3.3 The Syntax of Propositional Logic

A language consists of two parts: syntax and semantics.

<u>Metadef</u> The *syntax* of a language is the way to make a concrete representation of the meaning

<u>Metadef</u> The *semantics* of a language is our understanding of words or how the words relate to real world objects.

<u>Metadef</u> A *metalanguage* is a language that talks about both the syntax and the semantics of a language.

Now, let's start studying about the syntax propositional logic with our metalanguage English.

<u>Def</u> A *proposition* is a sentence which is either true or false. *Prop* is the set of all propositions.

<u>Def</u> An *expression* is a string composed of propositions, connectives ($\neg$, $\wedge$, $\vee$, $\rightarrow$), and parenthesis. <u>Ex</u> ")$\rightarrow$p ".

<u>Def</u> The set of formulas, *Form*, is defined as the smallest set of expressions such that: (here, $\circ$: $\wedge$, $\vee$ and, $\rightarrow$)

(1) $Prop \subseteq Form$, and (2) (closure property) If $\alpha, \beta \in Form$, then $(\neg\alpha) \in Form$ and $(\alpha\circ\beta) \in Form$.

<u>Def</u> The *primary connective* and *immediate sub-formula(s)* of a given formula φ are defined as follows:

(1) If φ is atomic, then it has no primary connective and no immediate sub-formula(s).

(2) If φ is $(\neg\psi)$, then $\neg$ is a primary connective and ψ is an immediate sub-formula.

(3) If φ is $(\theta\circ\psi)$, then $\circ$ is a primary connective and, θ and ψ are immediate sub-formulas.

<u>Thm</u> (Unique Readability) A composite formula has a unique primary connective and unique immediate sub-formulas

3.4 The Semantics of Propositional Logic

Def A *truth assignment*, τ, is an element of 2^{Prop}.

Rmk There are two ways to think of truth assignments:

(1) 2^{Prop} can be thought of as the power set of *Prop*, and a truth assignment X is an element of it, i.e., X ⊆ *Prop*.

(2) We can think of 2^{Prop} as set of all functions from *Prop* to {0, 1}. A truth assignment is a function τ: *Prop*→{0, 1}.

Let's consider now three different, but equivalent, perspectives of semantics.

3.4.1 Philosopher's view

For a philosopher, semantics is a binary relation ⊨ between structures and formulas.

τ ⊨ φ means (1) τ satisfies φ or (2) τ is true of φ or (3) τ holds at φ or (4) τ is a model of φ.

Def ⊨ ⊆ (2^{Prop} ×*Form*) is a binary relation, where the left side has a truth assignment and the right side has a formula. ⊨ is called the *satisfaction relation*, or the *truth relation*. We shall define it inductively:

(1) τ ⊨ p for some proposition p if τ(p) = 1

(2) τ ⊨ ¬ φ if it is not the case that τ ⊨ φ, that is, τ ⊨! φ (Note: this is so only in 2-valued world)

(3) τ ⊨ θ∨ψ if τ ⊨ θ or τ ⊨ ψ, (4) τ ⊨ θ∧ψ if τ ⊨ θ and τ ⊨ ψ, (5) τ ⊨ θ→ψ if τ ⊨! θ or τ ⊨ ψ.

Ex Let τ = {p, q, r, t}, then τ ⊨ (p→q)∧r and τ ⊨! p∧s.

3.4.2 Electrical Engineer's view

To an electrical engineer, the truth assignment is simply a mapping of voltages on a wire: τ: *Prop*→{0, 1}.

Operations are carried out by gates, which represent logical connectives.

Def ¬:{0, 1}→{0, 1} is a function defined by ¬(0) = 1 and ¬(1) = 0.

Def ∧: $\{0, 1\}^2$→{0, 1} is a function defined by ∧(0, 0) = ∧(0, 1) = ∧(1, 0) = 0 and ∧(1, 1) = 1.

Def ∨: $\{0, 1\}^2$→{0, 1} is a function defined by ∨(1, 1) = ∨(1, 0) = ∨(0, 1) = 1 and ∨(0, 0) = 0.

Def →: $\{0, 1\}^2$→{0, 1} is a function defined by →(1, 1) = →(0, 0) = →(0, 1) = 1 and →(0, 1) = 0.

Def Let p ∈*Prop*, τ ∈2^{Prop}. Then the semantics is defined according to the following rules:

(1) p(τ) = τ (p) (meaning of a wire), (2) (¬φ)(τ) = ¬(φ(τ)), (3) (θ∘ψ)(τ) = ∘(θ(τ), ψ(τ)).

Thm Let φ ∈*Form* and τ ∈2^{Prop}, then τ ⊨ φ if and only if φ(τ) = 1.

3.4.3 Software Engineer's view

A software engineer describes truth assignments in which a given formula is true.

Def This mapping from formula to sets of truth assignments is called *models*, where *models*: *Form*→$2^{2^{Prop}}$.

Def Let φ be a formula, then *models*(φ) is defined as follows:

(1) φ = p: *models*(p) = {τ | τ (p) = 1}, where p ∈*Prop*.

(2) φ = (¬θ): *models*(¬θ) = 2^{Prop} – *models*(θ).

(3) φ = (θ∧ψ): *models*(θ∧ψ) = *models*(θ) ∩ *models*(ψ).

(4) φ = (θ∨ψ): *models*(θ∨ψ) = *models*(θ) ∪ *models*(ψ).

(5) φ = (θ→ψ): *models*(θ→ψ) = (2^{Prop} – *models*(θ)) ∪ *models*(ψ).

Thm Let φ ∈*Form* and τ ∈2^{Prop}, then φ(τ) = 1 if and only if τ ∈*models*(φ). That is, *models*(φ) = {τ | φ(τ) = 1}.

4. ALGEBRA

4.1 Preliminaries

Def A *binary operation* * on S is a function *: $S \times S \rightarrow S$ defined by $(a, b) \mapsto a*b$.

Def $H \subseteq S$ and * on S. Say that H is closed under * if $h, k \in H \rightarrow h*k \in H$.

Def * on S is *commutative*, if a*b = b*a for $\forall a, b \in S$; * on S is *associative*, if (a*b)*c = a*(b*c) for $\forall a, b, c \in S$.

Let (S, *) and (S', *') be binary algebraic structures.

Def An *isomorphism* of S into S' is a bijective function f: $S \rightarrow S'$ such that f(x*y) = f(x) *' f(y)

Def S and S' are *isomorphic* if $\exists$ an isomorphism from S to S'. Write $S \approx S'$.

Rmk If two algebraic structures are isomorphic, then they share the same algebraic properties.

Rmk The isomorphism is an equivalent relation on the set of algebraic structures

Ex (**R**, +) and (**R+**, *) are isomorphic.

4.2 Groups

Def A *group* is a set G with an operation * that satisfies the following conditions (cf. *semigroup*, *monoid*)

(1) * is associative, (2) $\exists$ identity e in G, and (3) $\forall g \in G$, $\exists$ g'(inverse)$\in$G such that g*g' = e.

Def An element $e \in S$ is an *identity* for * if s*e = e*s = s for $\forall s \in S$.

Def A group G is *abelian* if the operation is commutative.

Thm A group has a unique identity, and all inverses are unique.

Ex $\mathbf{Z_p}$, **Z, Q**, **R**, **C** are abelian groups with addition operations. {e}: trivial group. But <N, +> is not a group.

Ex GL_2 = {2 by 2 matrices with non-zero determinant}. GL_2 is a non-abelian group.

Def Let <G, *> be a group. $H \subset G$ is a subgroup of G if H is a group under the same operation *.

Thm A subset H of G is a *subgroup* of G (write $H < G$) if and only if

(1) H is closed under the operation of G, (2) the identity e of G is in H, and (3) for $\forall a \in H$, $a^{-1} \in H$.

Ex T = {2 by 2 matrices with determinant 1} $\subset GL_2$, and $T < GL_2$.

Def A group G is *cyclic* if $\exists a \in G$ such that $\forall g \in G$, $g = a^n$ for some $n \in \mathbf{Z+}$.

Thm Every cyclic group is abelian.

Ex $\mathbf{Z_p}$, **Z, Q**, **R**, **C** are cyclic groups; but V ($\approx Z_2 \times Z_2$) is not cyclic. Compare the structures of V and Z_4

4.3 Groups of Permutations

Def A *permutation* on a nonempty set S is a bijective function f: $S \rightarrow S$.

Thm A collection of all permutations on A is a group under permutation multiplication.

Def The group in the preceding theorem is called a *symmetric group*.

Ex S_3 (symmetric group of 3 letters) and S_4 (symmetric group of 4 letters) are symmetric groups.

The structure of group S_3 is shown in the following table.

Z_4

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

V

+	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

S_3

	P0	P1	P2	M1	M2	M3
P0	P0	P1	P2	M1	M2	M3
P1	P1	P2	P0	M3	M1	M2
P2	P2	P0	P1	M2	M3	M1
M1	M1	M2	M3	P0	P1	P2
M2	M2	M3	M1	P2	P0	P1
M3	M3	M1	M2	P1	P2	P0

4.4 Homomorphism

<u>Def</u> A function f: G→G' of groups is a *homomorphism* if f(a*b) = f(a)*'f(b) for ∀a, b ∈G.

<u>Ex</u> Let g: G→G' be defined by g(a) = e' for ∀a ∈G. Then g is a *trivial homomorphism*.

<u>Ex</u> Let (**F**, +), (**R**, +) be groups and c ∈**R**, where **R** is the set of real numbers and **F** = {f | f: **R**→**R**}.

Then E_c: **F**→**R**, defined by E_c(f) = f(c) for f ∈**F**, is the *evaluation homomorphism*.

<u>Ex</u> Let GL(n, **R**) be the multiplicative group of all invertible n*n matrices.

Then the *determinant* function det: GL(n, **R**)→**R** is a homomorphism because det(AB) = det(A)det(B).

<u>Ex</u> Let $\mathbf{C}_{[0, 1]}$ be the additive group of *continuous* functions with domain [0, 1].

Then I: $\mathbf{C}_{[0, 1]}$→**R**, defined by I(f) = $\int_0^1 f(x)dx$, is a homomorphism.

<u>Ex</u> Let **D** be the additive group of all *differentiable* functions mapping **R** into **R**.

Then the *derivative* function der: **D**→**F**, defined by der(f) = f', is a homomorphism because (f + g)' = f' + g'.

<u>Thm</u> Let f: G→G' be a homomorphism of groups, then

(1) f(e) = e', (2) $f(a^{-1}) = f(a)^{-1}$, (3) H<G → f(H)<G', (4) H'<G'→ f^{-1}(H')<G.

4.5 Factor Groups

<u>Def</u> Let f: G→G' be a homomorphism of groups. Then f^{-1}[{e'}] = {x ∈G | f(x) = e'} is the *kernel* of f. Write Ker(f).

<u>Def</u> Let H<G. Then aH = {ah | h ∈H} is the *left coset* of H, and Ha = {ha | h ∈H} is the *right coset* of H.

<u>Def</u> A subgroup H of G is *normal* if aH = Ha for ∀a ∈G. (↔ aHa^{-1} = H ↔ aha^{-1} H for h ∈H). Write H◁G.

<u>Thm</u> All subgroups of abelian groups are normal.

<u>Thm</u> The kernel of a homomorphism f: G→G' is a normal subgroup of G.

<u>Thm</u> Let H◁G. Then the set of cosets forms a group G/H under the binary operation (aH)(bH) = (ab)H.

<u>Def</u> The group G/H is the *factor group* (or *quotient group*) of G modulo H.

<u>Ex</u> r: **Z**→**Z**, defined by r(m) = the remainder of m/3, is a homomorphism, and Ker(r) = 3**Z**, which is a normal subgroup.

The set of cosets of 3**Z** forms a group **Z**/3**Z**, i.e., {3**Z**, 1+3**Z**, 2+3**Z**} with coset addition operations.

<u>Ex</u> The trivial subgroup {0} of Z is normal, then Z/{0}≈ Z.

<u>Ex</u> Compute $(Z_4 \times Z_6)$ / <(0, 2)>. <(0, 2)> = {(0,0), (0,2), (0,4)}. $(Z_4 \times Z_6)$ / <(0, 2)> ≈ $Z_4 \times Z_2$.

<u>Def</u> A group is *simple* if it has no proper nontrivial normal subgroups.

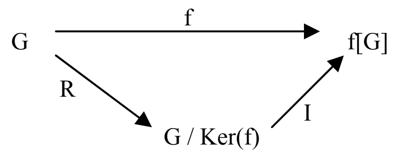
<u>Ex</u> S_n is simple for n ≥ 5. In 1980, Griess constructed a simple group of order more than $808 * 10^{17}$.

<u>Def</u> A *maximal normal subgroup* of a group G is a normal subgroup M s.t. M<N◁G → N=M or N=G.

4.6 Advanced Group Theory

Thm Let $f:G \to G'$ be a group homomorphism and $R:G \to G/\ker(f)$ be the canonical homomorphism.

Then $\exists !$ isomorphism $I: G/\ker(f) \to f[G]$ such that $f = I \circ R$.



Thm If $H<G$ and $N \triangleleft G$, then $(HN) / N \approx H / (H \cap N)$.

Thm If $H, K \triangleleft G$ with $H<K$, then $G / H \approx (G/K) / (H/K)$.

Thm Let G be a group with $|G| = p^n m$ and p not divide m.

Then $\exists H<G$ such that $|H| = p^k$ for $1 \le k \le n$, and $H_i \triangleleft H_j$ when $|H^i|=p^i$, $|H^j|=p^j$, and $i \le j \le n$.

Thm Let P_1 and P_2 be *Sylow p-subgroups* of a finite group G. Then $P_1 = xP_2x^{-1}$ for some $x \in G$.

Thm Let G is a finite group with $p \mid |G|$ and s be the number of Sylow p-subgroups. Then $s \equiv 1 (\mathrm{mod}\ p)$ and $s \mid |G|$.

4.7 Rings

Def A *ring* <R, +, *> is a set R with binary operations + and *, such that

(1) <R, +> : abelian group, (2) * is associative, (3) $a*(b + c) = a*b + a*c$ for $\forall a, b, c \in R$ (distributive law)

Ex {0} is the *zero ring* because 0 + 0 = 0 and (0)(0) = 0.

Ex <**Z**, +, *> is a ring. So are **Q**, **R**, and **C**.

Ex $M_2(\mathbf{Z})$ = {2 by 2 matrices with integer entries} is a ring with matrix addition and multiplication.

Ex $P[\mathbf{Z}] = \{a_0 + a_1x^1 + \dots + a_nx^n \mid a_i \in \mathbf{Z}$ and $n \in \mathbf{Z+}\}$ is a ring with polynomial addition and multiplication.

Ex $n\mathbf{Z} = \{na \mid a \in \mathbf{Z}\}$ is a ring with + and *.

Thm Let R be a ring and $a, b \in R$. Then $a*(-b) = (-a)*b = -(a*b)$ and $(-a)*(-b) = a*b$ for $\forall a, b \in R$.

Def A *subring* of a ring is a subset of the ring that is ring under induced operations from the whole ring.

Def A function $f: R \to R'$ of rings is a *ring homomorphism* if $f(a + b) = f(a) + f(b)$ and $f(a*b) = f(a)*f(b)$ for $\forall a, b \in R$.

Ex Let $g: \mathbf{Z} \to \mathbf{Z}$ defined by $g(a) = -a$. g is a group homomorphism but not a ring homomorphism.

Ex Let $f_1: \mathbf{Z} \to \mathbf{Z}$ by $f_1(a)=a$, $f_2: \mathbf{Z} \to \mathbf{Z}$ by $f_2(a)=0$, and $f_3: \mathbf{Z} \to \mathbf{Z}$ by $f_3(a)=2a$. Only f_1 and f_2 are ring homomorphisms.

4.8 Integral Domains and Fields

Def A ring in which the multiplication is commutative is a *commutative ring*.

Def Let R be a ring, then $i \in R$ is *unity* if $a*i = i*a = a$, for $a \in R$, and $b \in R$ is a *unit* if $b^{-1} \in R$ such that $b*b^{-1} = i$.

Ex Let (**Z**, +, *) be a ring, then 1 is a unity, -1 is a unit ((-1)(-1) = 1), and 2 is not a unit.

Def A ring with a multiplicative identity (unity) is *a ring with unity*.

Def A ring R is a *division ring* if every nonzero element is a unit.

Def A ring is a *field* if it is a commutative division ring, and a noncommutative division ring is called a *skew field*.

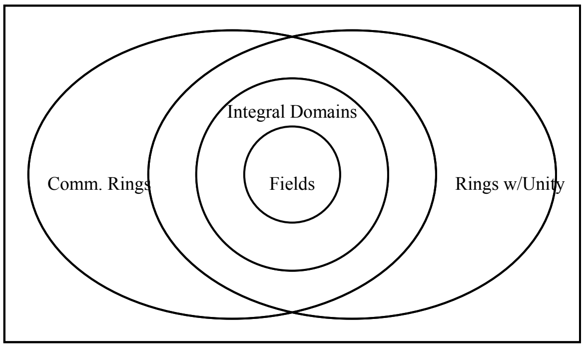
Def A *subfield* of a field is a subset of the field that is field under induced operations from the whole field.

Ex **Z** is a ring with unity but not division ring. **Q** and **R** are division rings and commutative, so fields.

Ex $\mathbf{H} = \{a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} \mid a, b, c, d \in \mathbf{R}\}$ is a division ring but not commutative because $\mathbf{ij} = \mathbf{k}$ and $\mathbf{ji} = -\mathbf{k}$.

Def Let R be a ring. If $a, b \in R$ such that $a \neq 0$, $b \neq 0$, and $a*b=0$, then a, b are *zero divisors*.

Def A commutative ring with unity and without zero divisors is an *integral domain*.



Ex $\mathbf{Z}_5$ is an integral domain, but $\mathbf{Z}_6$ is not because 2*3=0 in $\mathbf{Z}_6$.

Thm Every field is an integral domain.

Thm Every finite integral domain is a field.

Cor If p is a prime, then $\mathbf{Z}_p$ is a field.

4.9 Vector Spaces

Def A *vector space* V over a field F consists of the following:

(1) F: a field of *scalars*;

(2) (V, +): an abelian group where V is set of *vectors* and + is *vector addition* +: V×V→V

(3) Scalar multiplication *: F×V→V satisfying the following conditions; (a) 1***v** = **v** for ∀**v** ∈V, (b) (ab)***v** = a(b***v**), (c) a*(v + w) = a*v + a*w, (d) (a + b)*v = a*v + b*v, where a, b ∈F and **v** ∈V.

Ex $\mathbf{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbf{Q}\}$ is a vector space over **Q** with a *basis* $\{1, \sqrt{2}\}$.

Ex For any field F, F[x] is a vector space over F, where $F[x] = \{a_0 + a_1x^1 + \ldots + a_nx^n \mid a_i \in F \text{ and } n \in \mathbf{Z}+\}$.

4.10 References

"A First Course in Abstract Algebra" (John B. Fraleigh)

"Algebra" (Thomas W. Hungerford)

"Linear Algebra" (Hoffman and Kunze)

"Linear Algebra and its Applications" (Gilbert Strang)

5. ANALYSIS

5.1 Sequences

Def A *sequence* of real (or complex) numbers is a function f: **N**→**R** (or **C**). Write $\{f_n\}^{\infty}_{n=1}$.

Def $\{a_n\}$ *converges* to α if ∀ε >0, ∃N∈**N** such that $|a_n - \alpha| < \varepsilon$ if n ≥ N. Write $a_n \to \alpha$ or $lim_{n\to\infty} a_n = \alpha$.

Def $\{a_n\}$ *diverges* to +∞ (or -∞) if ∀M ∈**R**, ∃N∈**N** such that $a_n > M$ (or $a_n < M$) if n ≥ N. Write $a_n \to +\infty$(or -∞).

Def $\{a_n\}$ is *bounded* if ∃M > 0 such that $a_n < M$ for ∀n ∈**N**.

Def $\{a_n\}$ is *monotone* if $a_n \le a_{n+1}$ for ∀n ∈**N** (increasing) or $a_n \ge a_{n+1}$ for ∀n ∈**N** (decreasing).

Thm If $a_n \to \alpha$ and $b_n \to \beta$, then

(1) α is unique, (2) $\{a_n\}$ is bounded, (3) $ca_n \to c\,\alpha$, (4) $(a_n + b_n) \to \alpha + \beta$, (5) $(a_n \cdot b_n) \to \alpha\cdot\beta$, (6) $(a_n/b_n) \to \alpha / \beta$.

Ex $lim_{n\to\infty} (1+1/n)^n = \sum^{\infty}_{n=0} 1/(n!) = e$ and $\sum^{\infty}_{n=0} (-1)^n\, 1/(2n+1) = \pi/3$.

5.2 Basic Topology

Def (a, b) = {x ∈**R** | a < x < b}, (a, b] = {x ∈**R** | a < x ≤ b}, [a, b] = {x ∈**R** | a ≤ x ≤ b}

Def A set S ⊆ **R** is *open* if ∀x ∈S, ∃ε>0 such that x ∈ (x-ε, x+ε) ⊆ S.

Def A set V ⊆ **R** is *closed* if V^c is open.

Thm Let $\{U_a \mid a \in A\}$, $\{U_i \mid 1 \le i \le n\}$ be collections of open sets, then $\cup_{a\in A} U_a$ and $\cap^{n}_{i=1} U_i$ are also open sets.

Ex Let $U_n = (-1/n, 1/n + 1)$, then $\cap^{\infty}_{n=1} U_n = [0, 1]$, which is closed.

Ex Let **Q** = $\{q_1, q_2 \ldots\}$ and $U_n = (q_n - \varepsilon/2^n, q_n + \varepsilon/2^n)$, then $U = \cup^{\infty}_{n=1} U_n$ is open. **Q** ⊆ U but the length of U is just 2ε!

Def A point x is an *accumulation point* of S if ∀ε>0, (x-ε, x+ε) contains infinitely many elements of S.

Def A point x is an *isolated point* of S if x ∈S and ∃ε>0 such that (x-ε, x+ε) ∩ S = {x}.

Def A point x is a *boundary point* of S if ∀ε>0, (x-ε, x+ε) ∩ S ≠ {} and (x-ε, x+ε) ∩ S^c ≠ {}.

Def A point x is an *interior point* of S if ∃ε>0 such that (x-ε, x+ε) ⊆ S.

Def A set S ⊆ **R** is *compact* if every sequence in S has a subsequence that converges to an element of S.

Thm A set S ⊆ **R** is compact if and only if S is closed and bounded.

Def $\{O_a\}_{a\in A}$ is an *open covering* of S if O_a is open and $S \subseteq \cup_{a\in A} O_a$.

Thm S is compact if and only if every open covering has a finite subcovering.

Ex $O_n = (1/n, 1+1/n)$, S = (0, 1]; S is bounded, not closed; $\{O_n\}$ is an open covering, but doesn't have finite subcovering.

Ex $O_n = (n-2, n)$, S = [1, ∞); S is closed, not bounded; $\{O_n\}$ is an open covering, but doesn't have finite subcovering.

Def S is *disconnected* if ∃disjoint nonempty U, V such that S = (U∩S)∪(V∩S). S is *connected* if it is not disconnected.

Ex The Cantor Set $C = \cap^{\infty}_{n=1} C_n$; C is compact, has zero length, is uncountable, and {x + y | x, y ∈C} = [0, 2].

5.3 Limits and Continuity of Functions

Def Let f: [a, b]→R, then $lim_{x\to c} f(x) = L$ if ∀ε>0, ∃δ>0 such that if |x – c| < δ , then |f(x) – L| < ε.

Thm Let $lim_{x\to c} f(x) = L$ and $lim_{x\to c} g(x) = M$, then

(1) L is unique, (2) $lim_{x\to c} (f(x) + g(x)) = L+M$, (3) $lim_{x\to c} (f(x)\cdot g(x)) = L\cdot M$, (4) $lim_{x\to c} (f(x)/g(x)) = L/M$ if M ≠0.

Def A function f is *continuous at p* if $\mathit{lim}_{x \to p}$ f(x) = f(p).

Thm If f and g are continuous at p, then f+g, f-g, αf, f/g, fg are also continuous at p.

Thm A function f: E→**R** is continuous if and only if $f^{-1}(O) = E \cap O'$ for all open sets O, where O' is also open.

Thm If f is a continuous function and K is a compact set, then f(K) is compact.

Thm If f is a continuous function and L is a connected set, then f(L) is connected.

5.4 Differentiation of Functions

Let f , g be real functions. In other words, f: S→**R** and g: S→**R**.

Def f is *differentiable at p* if ∃ the *derivative* of f at p; f'(p) := $\mathit{lim}_{h \to 0}$ {(f(p + h)-f(p)) / h}.

Def f is *differentiable* if it is differentiable at each a in its domain.

Def C^n (I) is the collection of real functions whose n-th derivatives exist and are continuous on I.

Thm If f is differentiable at p, then f is continuous at p.

Ex h(x) = |x| is continuous at 0 but not differentiable there.

Thm Let f and g are differentiable at p, then

(1) (f + g)'(x) = f'(x) + g'(x), (2) (f·g)'(x) = f'(x)·g(x) + f(x)·g'(x), (3) (f/g)'(x) = {g(x)·f'(x) – f(x)·g'(x)} / $g^2(x)$.

Thm If f is differentiable at p and g is differentiable at f(p), then g∘f is differentiable at p with (g∘f)'(p) = g'(f(p))·f'(p).

Thm (L'Hopital) Let f and g are differentiable on an open interval I, p ∈I, f(x) 0 for x ∈ I –{p}.

If $\mathit{lim}_{x \to p}$f(x) = $\mathit{lim}_{x \to p}$g(x) = 0 and ∃ $\mathit{lim}_{x \to p}$(f'(x) / g'(x)) = L, then $\mathit{lim}_{x \to p}$(f(x) / g(x)) = L

Thm Let f be an invertible function on an interval (a, b) with nonzero derivative at a point x ∈ (a, b), and X = f(x).

Then $(f^{-1})'(X)$ exists and equals 1/f'(x).

Thm (Mean Value) Let f be a continuous function on the closed interval [a, b] that is differentiable on (a, b).

Then ∃ a point ξ ∈(a, b) such that f'(ξ) = (f(b) – f(a)) / (b – a).

5.5 Integral of Functions

Let f be a function on a closed interval [a, b] in **R**. In other words, f: [a, b]→**R**.

Def A finite, ordered set of points $P = \{x_0, x_1 \ldots , x_{k-1}, x_k\}$ such that $a=x_0 \le x_1 \le \ldots \le x_{k-1} \le x_k = b$ is a *partition* of [a, b].

Def Let P is a partition of [a, b]. I_j denotes the interval $[x_{j-1}, x_j]$, Δj denotes the length of I_j, and the *mesh* $m(P)$ is max Δj .

Def Let $P = \{x_0, x_1 \ldots , x_{k-1}, x_k\}$ is a partition of [a, b] and s_j is an element of I_j for each j.

Then the corresponding *Riemann sum* is $R(f, P) = \sum_{i=1}^{k} f(s_j)\, \Delta j$.

Def We say that *the Riemann sums of f tend to a limit L as m(P) tends to zero* if

∀ε>0, ∃δ>0 such that if *P* is any partition of [a, b] with $m(P) < \delta$ then $|R(f, P) – L| < \varepsilon$ for every choice of $s_j \in I_j$.

Def A function f is *Riemann integrable* on [a, b] if the Riemann sums of *R*(f, *P*) tend to a limit as *m*(*P*) tends to zero.

The value of the limit, when it exists, is *Riemann integral* of f over [a, b] and is denoted by $\int_a^b f(x)dx$.

Thm Let f be a continuous function on a nonempty closed interval [a, b], then f is Riemann integrable on [a, b].

Thm Let [a, b] be a nonempty interval, f and g be Riemann integrable functions on the interval, and α ∈**R**.

Then f + g, and α f are integrable; (1) $\int_a^b \{f(x) + g(x)\}dx = \int_a^b f(x)dx + \int_a^b g(x)dx$., (2) $\int_a^b \alpha\cdot f(x)dx = \alpha\cdot\int_a^b f(x)dx$.

Thm If f and g are Riemann integrable on [a, b], then so is the function f·g.

Thm If f is Riemann integrable on [a, b] and φ is a continuous function on a compact interval containing the range of f. Then $\varphi \circ f$ is Riemann integrable.

Thm (Fundamental Theorem of Calculus) Let [a, b] be a closed, bounded interval and f: [a, b] → **R**.

(1) If f is continuous on [a, b] and $F(x) = \int_a^x f(t)dt$, then $F \in C^1[a, b]$ and F'(x) = f(x).

(2) If f is differentiable on [a, b] and f' is integrable on [a, b], then $\int_a^x f'(t)dt = f(x) - f(a)$ for each $x \in [a, b]$.

5.6 References

"Real Analysis & Foundations" (Krantz)
"An Introduction to Analysis" (Wade)

6. TOPOLOGY

6.1 Topological Spaces

Def A *topology* on a set X is a collection ***T*** of subsets of X having the following properties:

(1) Ø, X ∈ ***T***, (2) $\forall \{U_a \mid a \in A\} \subseteq T$, $\cup_{a \in A} U_a \in$ ***T***, and (3) $\forall \{U_1, U_2, \ldots, U_n\} \subseteq$ ***T***, $\cap^n_{i=1} U_i \in$ ***T***.

Ex Let X = {a, b, c}. Then T_1 = {X, Ø}, T_2 = {X, Ø, {a}, {b}, {a, b}, {c}, {a, c}}, and $T_3 = 2^X$ are topologies on X.

Def If X is any set, the collection of all subsets is the *discrete topology* on X, and {Ø, X} is the *indiscrete topology* on X.

Ex Let X ≠ Ø and T_f = {U⊆X | X –U is finite, or U is X}. T_f is called *finite complement topology* on X.

Def Let T_1 and T_2 be topologies on X, with $T_1 \subset T_2$. Then T_2 is *finer* than T_1.

6.2 Basis for a Topology

Def If X is a set, a *basis* for a topology on X is a collection ***B*** of subsets of X such that

(1) ∀x∈X, ∃B∈***B*** such that x∈B, and (2) If $x \in B_1 \cap B_2$, then $\exists B_3 \in$ ***B*** such that $x \in B_3 \subseteq B_1 \cap B_2$.

Thm If ***B*** is a basis, the topology ***T*** on X generated by ***B*** is described as follows;

A subset U of X is open in X if ∀x∈U, ∃B∈***B*** such that x∈B⊆U.

Def Let ***B*** = {(a, b) | a ≤ b}. The topology generated by ***B*** is called the *standard topology* (**R**) on **R**.

Def Let ***B'*** = {[a, b) | a ≤ b}. The topology generated by ***B'*** is called the *lower limit topology* ($\mathbf{R}_l$) on **R**.

Def Let K = {1/n | n ∈**Z+**}, ***B''*** = ***B*** ∪ {(a, b) – K}. The topology generated by ***B''*** is called the *K-topology* ($\mathbf{R}_k$) on **R**.

Def Let ***B'''*** = {[a, b] | a ≤ b}. The topology generated by ***B'''*** is called the *discrete topology* on **R**.

Thm The K-topology and the lower limit topology are finer than the standard topology.

6.3 Order Topology, Product Topology, and Subspace Topology

Let X be a set with a simple order relation with more than two elements

Def Let ***B*** be the collection of all sets of the following types: (here, a_0, b_0 are the smallest and largest in X, if any)

(1) All open intervals (a, b) in X, (2) All intervals of form $[a_0, b)$ of X, and (3) All intervals of form $(a, b_0]$ of X.

Then the collection ***B*** is a basis for a topology on X, which is called the *order topology* on X.

Ex The standard topology on **R** is just the order topology derived from the usual order on **R**.

Let X and Y be topological spaces.

Def The *product topology* on X×Y is the topology $T_{X\times Y}$ defined by {U×V | U is open in X, V is open in Y}.

Ex The product of the standard topology on **R** is a topology on $\mathbf{R}\times\mathbf{R} = \mathbf{R}^2$.

Let X be a topological space with topology ***T***.

Def If Y ⊆ X, the collection T_Y = {Y ∩ U | U ∈***T***} is a topology on Y, called the *subspace topology*.

Ex Let (**R**, ***T***) be the standard topology and Y = [0, 1) ∪ {2}. Then T_Y = {Y ∩ U | U ∈***T***} is a subspace topology on Y.

6.4 The Metric Topology

Def A *metric* on a set X is a function d: X×X→**R** satisfying the followings: for ∀x, y, z ∈X

(1) d(x, y) ≥ 0 ("=" holds if and only if x = y), (2) d(x, y) = d(y, x), and (3) d(x, y) + d(y, z) ≥ d(x, z).

Ex Let X be a set and d: X×X→**R** defined by d(x, y) = 0 (if x = y), or 1 (if x ≠ y). d is called the *discrete metric* on X.

Ex Let X = **R** and d: **R**×**R**→**R** defined by d(x, y) = | x – y |. d is called the *Euclidean metric* on **R**.

Def Let (X, d) be a set X with a metric d. The *ε-ball centered at x* is $B_d(x, \varepsilon)$ = {y | d(x, y) < ε}, where ε > 0.

Thm {$B_d(x, \varepsilon)$ | x ∈X and ε >0} forms a basis of a topological space on X.

Def A topology (X, ***T***) is *metrizable* if ∃ a metric on X such that the topology generated by the metric equals to ***T***.

Ex A discrete topology (X, ***D***) is metrizable because the discrete metric induces the discrete topology on X.

Ex The standard topology **R** is metrizable because the Euclidean metric induces the standard topology on **R**.

Let **x** = $(x_1, x_2\ldots, x_n) \in \mathbf{R}^n$,

Def The *Euclidean metric* d on $\mathbf{R}^n$ is defined by $d(x, y) = [(x_1- y_1)^2 +\ldots+ (x_n- y_n)^2]^{1/2}$.

Def The *square metric* ρ on $\mathbf{R}^n$ is defined by $\rho(x, y) = \max \{|x_1- y_1| \ldots, |x_n- y_n|\}$.

Thm The topologies on $\mathbf{R}^n$ induced by the d and ρ are the same as the product topology on $\mathbf{R}^n$.

6.5 Continuous Functions and Homeomorphisms

Def (In Analysis) A function f: **R**→**R** is *continuous* if ∀x, y∈**R**, ∀ε>0, ∃δ>0 such that if |x–y| < δ, then |f(x)–f(y)| < ε.

Def (In Topology) A function f: (X, ***T***)→(Y, ***U***) is *continuous* if ∀open set A ∈***U***, $f^{-1}(A)$ is open in X, i.e., $f^{-1}(A)$ ∈***T***.

Rmk The continuity defined by "ε–δ" method is equivalent to the topological definition.

Ex A function f: **R**→$\mathbf{R}_l$ defined by f(x) = x is not continuous because $f^{-1}[a, b) = [a, b)$ is not open in R.

Ex A function f: $\mathbf{R}_l$→**R** defined by f(x) = x is continuous because $f^{-1}(a, b) = (a, b) = \cup^{\infty}_{n=k} [a+1/n, b)$.

Def A function f: (X, ***T***)→(Y, ***U***) is a *homeomorphism* if (1) f is bijective, (2) f is continuous, and (3) f^{-1} is continuous.

Def Two topologies ***T*** and ***T'*** are *homeomorphic* if ∃ a homeomorphism from ***T*** to ***T'***.

Ex A function f: (-1, 1)→**R** defined by f(x) = *tan*(π·x/2) and f = 2/π · $tan^{-1}(x)$ is a homeomorphism.

Ex A function f: [0,1)→S⊆$\mathbf{R}^2$ defined by f(t)=(*cos*(2π·t), *sin*(2π·t)) is not a homeomorphism, where S={(x, y) |$x^2+y^2=1$}.

6.6 Connectedness

Let X be a topological space.

Def A *separation* of X is a pair {U, V} of disjoint nonempty open subsets of X such that U ∪ V= X.

Def X is *connected* if there is no separation for X.

Ex A = {p, q} with discrete topology is not connected, but A with indiscrete topology is connected.

Ex $\mathbf{R}_l$ is disconnected because R = (-∞, a) ∪ [a, ∞) = {$\cup_{n\in \mathbf{Z}+}$(-n, a)} ∪ {$\cup_{m\in \mathbf{Z}+}$[a, m)}.

Thm If {A_a | a∈J} is a collection of connected subsets of X with $\cap_{a\in J} A_a \neq \emptyset$, then $\cup_{a\in J} A_a$ is also connected.

Thm If f: X→Y is a continuous function and X is connected, then f(X) is a connected subspace of Y.

Thm If X and Y are connected, then X×Y is also connected.

6.7 Compactness

Let X be a topological space.

Def A collection ***A*** = {$A_a \subseteq X$ | a∈J} is an *open covering* of X if $\cup_{a \in J} A_a = X$ and each A_a is open in X.

Def X is *compact* if ∀ open covering of X, ∃ a finite subcollection {$A_1 \ldots A_n$} ⊆A such that $\cup^n_{i=1} A_i = X$.

Def (In Analysis) A set S ⊆ **R** is *compact* if every sequence in S has a subsequence that converges to an element of S

Ex Let X = **R** with finite complement topology, then X is compact.

Ex Let X = **R** with standard topology and Y = {0} ∪ {1/n | n ∈**Z+**}, then Y is compact.

Thm If X is compact and Y is a closed subspace of X, then Y is compact.

Thm If X is compact and f: X→Y is a continuous function, then f(X) is compact in Y.

Thm If X and Y are compact, then X×Y is also compact.

6.8 References

"Topology" (James R. Munkres),

"General Topology" (Seymour Lipschutz).